NEW SYLLABUS
CBCS PATTERN

S.Y. B.B.A. (C.A.)
SEMESTER - IV

NETWORKING

Dr. Ms. MANISHA BHARAMBE
VIKAS TAYADE
Mrs. VEENA GANDHI

NIRALI PRAKASHAN

Syllabus ...

1. Introduction to Computer Network (10 Hrs.)

- 1.1 Basics of Computer Network
  - 1.1.1 Definition
  - 1.1.2 Goals
  - 1.1.3 Applications
  - 1.1.4 Network Hardware –Broadcast, Point to Point
  - 1.1.5 Components of Data Communication
- 1.2 Network Topologies
  - 1.2.1 Mesh
  - 1.2.2 Star
  - 1.2.3 Bus
  - 1.2.4 Ring
- 1.3 Types of Networks
  - 1.3.1 LAN, MAN, WAN
  - 1.3.2 Internetwork
  - 1.3.3 Wireless Network
- 1.4 Modes of Communication
  - 1.4.1 Simplex
  - 1.4.2 Half Duplex
  - 1.4.3 Full Duplex
- 1.5 Server Based LANs & Peer-to-Peer LANs
- 1.6 Protocols and Standards
- 1.7 Network Software
  - 1.7.1 Protocol Hierarchies, Layers, Peers, Interfaces
  - 1.7.2 Design Issues of the Layers
  - 1.7.3 Connection Oriented and Connectionless Service

2. Network Models (8 Hrs.)

- 2.1 OSI Reference Model : Functions of each Layer
- 2.2 TCP/IP Reference Model, Comparison of OSI and TCP/IP Reference Model
- 2.3 TCP/IP Protocol Suite
- 2.4 Addressing
  - 2.4.1 Physical Addresses

- 2.4.2 Logical Addresses
- 2.4.3 Port Addresses,
- 2.4.4 Specific Addresses

2.5 IP Addressing

- 2.5.1 Classfull Addressing
- 2.5.2 Classless Addressing

3. Transmission Media (8 Hrs.)

3.1 Introduction, Types of Transmission Media

3.2 Guided Media:

- 3.2.1 Twisted Pair Cable - Physical Structure, Categories, Connectors &Applications
- 3.2.2 Coaxial Cable – Physical Structure, Standards, Connectors & Applications
- 3.2.3 Fiber Optic Cable- Physical Structure, Propagation Modes, Connectors & Applications

3.3 Unguided Media:

- 3.3.1 Electromagnetic Spectrum for Wireless Communication
- 3.3.2 Propagation Modes Ground, Sky, Line-of-Sight
- 3.3.3 Wireless Transmission: Radio Waves, Microwaves, Infrared

4. Wired and Wireless LAN (8 Hrs.)

4.1 IEEE Standards

4.2 Standard Ethernet MAC Sublayer, Physical Layer

4.3 Fast Ethernet – Goals, MAC Sublayer, Topology, Implementation

4.4 Gigabit Ethernet – Goals, MAC Sublayer, Topology, Implementation

4.5 Ten-Gigabit Ethernet – Goals, MAC Sublayer, Physical Layer

4.6 Backbone Networks -Bus Backbone, Star Backbone

4.7 Virtual LANs Membership, IEEE standards advantages

4.8 Wireless LAN

- 4.8.1 IEEE 802.11 Architecture
- 4.8.2 Bluetooth Architecture (Piconet, Scatternet)

5. Network Devices (6 Hrs.)

5.1 Network Connectivity Devices

- 5.1.1 Active and Passive Hubs
- 5.1.2 Repeaters
- 5.1.3 Bridges - Types of Bridges

5.1.4 Switches
5.1.5 Router
5.1.6 Gateways

6. Network Security (8 Hrs.)

6.1 Introduction
6.2 Need for Security
6.3 Security Services
6.3.1 Message - Confidentiality, Integrity, Authentication, Non repudiation.
6.3.2 Entity (User) - Authentication.
6.4 Types of Attack
6.5 Cryptography, PlainText, Cipher Text, Encryption, Decryption, Symmetric Key and Asymmetric Key Cryptography
6.6 Substitution Techniques, Caesar Cipher, and Transposition Cipher (Problems should be covered.)
6.7 Firewalls- Packet Filter firewall, Proxy firewall
6.8 Steganography, Copyright

❖❖❖

Contents ...

❖❖❖

1... Introduction to Computer Network

Objectives...

- To learn basics of Computer Network.
- To understand various Network topologies and Network types.
- To know about Modes of communication.
- To get information of Server based and Peer to Peer LANs.
- To study about Protocols and standards and Network Software.

1.1 BASICS OF COMPUTER NETWORK (W-18, S-19)

- Today every business in the world needs a computer network for smooth operations, flexibly, instant communication and data access. Just imagine if there is no network communication in the university campuses, hospitals, multinational Organizations and educational institutes then how difficult are to communicate with each other.
- A computer network is comprised of connectivity devices and components. To share data and resources between two or more computers is known as Networking.

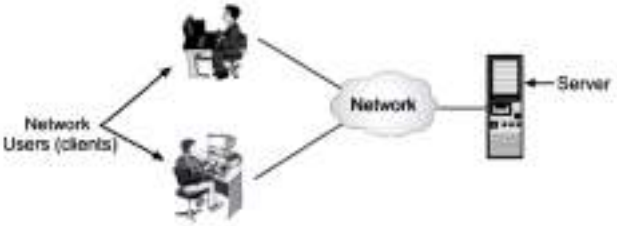


Fig. 1.1: A Typical Computer Network

- The purpose of a computer network is to link two or more "clients" together in order to exchange information.

1.1.1 Definition

- A computer network is a system for communication among two or more computers.

OR

- A computer network is defined as two computers that are linked together through either a physical cable, or a wireless device. This link then allows the computers on the network to share resources such as an Internet connection, printers, files, and programs.

OR

- A computer network is a collection of computer systems which can communicate or interact with each other.

OR

- Networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.

1.1.2 Goals

- The computer networks are playing an important role in providing services to large or small or medium organizations as well as to the individual common man.
- Network services are the things that a network can do.

Like human being computer network provides following goals:

1. **Resource Sharing:**

- It is the main goal of the computer network. The goal is to provide data and hardware to all programs on network regardless of physical location of resources and users.
- In computer network, one of the machines can work as a server. So whatever important data we want, can be stored on server. This data (files, documents) can be shared by users. One hard disk will fulfill the need of all users.
- This allows us to extract co-relation about the whole network. For example, we can manage all the users from server. We can copy data of one user to other user. We can send similar information to all users and so on.
- In short, Networks used to provide sharing of resources such as information or processors.

2. **High Reliability:**

- Network provides high reliability by having alternative sources of data.
- For example, all files could be replicated on more than one machines, so if one of them is unavailable due to hardware failure or any other reason, the other copies can be used.

3. **Minimize Cost:**

- Small computers have a much better price to performance ratio as compared to large ones. So it is always minimizing the cost to set up a network of large or small number of computers than the large ones.

- As well as by sharing the resources like printer, we can save the cost. While designing cost of a network is an important factor.

4. **High Performance:**

- Computer network provides the network user with maximum performance at minimum cost. The network performance can be measured by its transit time and response time.
  (i) Transit time is the amount of time required for a message to travel from one device to another device in network.
  (ii) Response time is the time elapsed between an inquiry and a response.
- Network performance depends on a number of factors including, network transmission medium, network hardware, network software and traffic load. Computer network have provided means to increase system performance as the work load increases.

5. **Scalability:**

- We can easily extend computer network just by adding more computers, printers or any other devices without disturbing others and affecting overall performance.

6. **Powerful Communication Medium:**

- A computer network provides a powerful communication medium.
- Computer network helps people who live or work apart to report together. So, when one user prepared some documentation, he can make the document online enabling other to read and convey their opinions.
- From the server, we can send same information to all users and users can also communicate with the server. For this reason, computer network is a powerful communication medium.

7. **Distribution of Workload:**

- By using computer network, large work can be distributed among different network users.

8. **Security:**

- Network security issues comprise of prevention from virus attacks and protecting data from unauthorized access. Only authorized user can access resource in a computer network.

9. **Backups:**

- Similarly, in computer network taking backup is very easy. Because data is stored on server. By using a single floppy drive or CD writer we can take backups.

1.1.3 Network Structure

- In any network, there are collections of machines intended for application user programs.

- Any network should have following elements:
  1. **Hosts:** Hosts are the machines intended for running user application. They are also called end systems because they are the end users.
  2. **Communication subnet:** Hosts are connected with each other by communication subnet. The job of the subnet is to carry messages from host to host. The subnet plays an important role in network addressing which is needed in internetworking.
  - In most WANs, subnet consists of two different elements:
    - **Transmission lines:** These are also referred as circuits, channels or trunks. These move bits between machines. For communication these lines are very important.
    - **Switching element:** This is also called as IMP i.e. Interface Message Processors. IMPs are specialized computers used to connect two or more transmission lines. Some may called them packet switched node, intermediate system and data switching exchange, routers.

Components of Network:

- A computer network comprises the following components:
  1. Computers (at least two).
  2. Cables that connect the computers to each other.
  3. A network interface device on each computer (This is called a Network Interface Card or NIC).
  4. A switch (Note: hubs are no longer recommended).
  5. Network operating system software.
  6. Uninterruptible power supply (optional).

1.1.4 How Does a Computer Network Work ?

- Following figure shows how simple network to send information from one computer send to another:

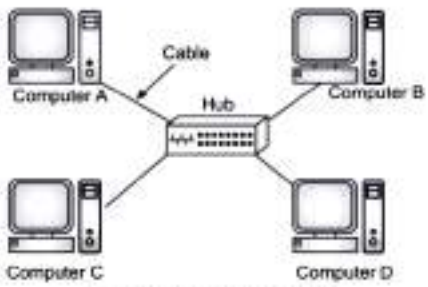


Fig. 1.2: A Typical Network

- If Computer A wants to send a file to Computer B, the following would take place:
  1. Based on a protocol that both computers use, the NIC in Computer A translates the file, (which consists of binary data 1's and 0's) into pulses of electricity.
  2. The pulses of electricity pass through the cable with a minimum (hopefully) of resistance.
  3. The hub takes in the electric pulses and shoots them out to all of the other cables.
  4. Computer B's NIC interprets the pulses and decides if the message is for it or not. In this case, it is so Computer B's NIC translates the pulses back into the 1's and 0's that make up the file.
- If Computer A sends the message to the network using NetBEUI, a Microsoft protocol, but Computer B only understands the TCP/IP protocol, it will not understand the message; no matter how many times Computer A sends it. Computer B also would not get the message if the cable is getting interference from the fluorescent lights or if the network card has decided not to turn on today etc.

1.1.5 Applications

A computer network has of following applications:

1. **Resource Sharing:** Enables users to share hardware like scanners and printers. This reduces costs by reducing the number of hardware items bought. Resources are available to anyone on the network without regard to the physical location of the resource and the user.

   For example: Printers, scanners, CD burners, etc.
2. **Information Sharing:** Allows users access to data stored on others computers. This keeps everyone up-to-date on the latest data, since it's all in the same file, rather than having to make copies of the files, which are immediately out-of-date.

   For example: Files, database, records etc.
3. **Person-to-Person Communication:** For example, e-mail (electronic mail). Voice and Video conferencing is also available to perform virtual meetings.
   - Online reservations for airlines, railways and online examination systems are available because of network.
   - We can access remote information for bank transaction, MSEB bill paying, by reading newspapers.
   - **For example:** GIS [Geographical Information System] is available from which we can get the information of soil details, water detail, rivers, oceans maps, area wise details of our earth.
4. **Electronic Business:** Users can place orders electronically as needed. In the industries or Organizations, management can keep track of all inventories, sales, production, personnel information through network. By using electronic mail facility, messages, documents, memos can be send to different people and immediately get the delivery report.

5. **Interactive Entertainment:** Users can play real-time simulation games, like flight simulators, Age of empires etc. Also allows user to chat, watch movies, solve quiz, etc.
6. **Manufacturing**: Computer network is used in manufacturing and in manufacturing process also.
   For example: CAD (Computer Aided Design) and CAM (Computer Aided Manufacturing).
7. **Marketing and Sales**: Sales application-teleshopping is one of the computer network's applications. This application uses order-entry computers or the telephones are connected to an order processing network. The network is used to transmit and receive critical sales, administrator and research data by the travelling salesman and remote employees.
8. **Banking:** Computers are instrumental to the way the banking industry performs its business. This technology allows banks to be able to take banking transactions and update accounts in real time.
9. **Financial services**: It include credit history searches, foreign exchange and investment services and Electronic Fund Transfer (EFT) which allows a user to transfer money without going to bank.
10. **Insurance:** The world of insurance relies on computers to the same extent as banks. With the use of the Internet, insurance companies are able to access information which will determine whether they accept clients or not.

1.1.6 Network Hardware - Broadcast and Point to Point

- Network hardware structure is a design required for developing any computer network.
- For classification of computer network, transmission technology is important.
- Transmission technology refers how two devices are connected and how they are communicating. In transmission technology, a link is the physical communication pathway that transfers data from one device to another.
- For communication to occur, two devices must be connected in same way to the same link at the same time.
- The transmission technology can be broadly categorized into two types:
  1. Broadcast networks (multipoint)
  2. Point-to-Point networks

1.1.6.1 Broadcast Network

- The networks having multipoint configuration are called as Broadcast Network.
- Broadcast network has single communication channel that is shared by all the machines on the network. Short messages called packets in certain contexts, sent by any machine, are received by all the others.

- An address field within the packet specifies for whom it is intended. After receiving a packet, a machine checks the address field.
- If the packet is intended for itself, it processes the packet; if packet is intended for some other machine, it is just ignored. Example: LAN
- It is normally a connection of hosts and repeaters. Here if packet is not responded, then it will be lost.
- A broadcast network is an organization, such as a corporation or other association, that provides live or recorded content, such as movies, newscasts, sports, and public affairs programs for broadcast over a group of radio or television stations.
- They are generally primarily either a television network or a radio network, although some organizations run both types of networks.
- A broadcast network avoids the complex routing procedures of a switched network by ensuring that each node's transmissions are received by all other nodes in the network.
- Therefore, a broadcast network has only a single communications channel.
- A wired Local Area Network (LAN), for example, may be set up as a broadcast network, with one user.

Modes of operations:

- Broadcast network supports two modes of operations:
  1. **Broadcasting:** Broadcast systems generally use a special code in the address field for addressing a packet to all the concerned computers. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called Broadcasting.
  2. **Multicasting:** Some broadcast systems also support transmission to a subset of the machines known as Multicasting. When a packet is sent to a certain group, it is delivered to all machines of that group. Examples of this network are Ethernet and Bus topology based on LAN.

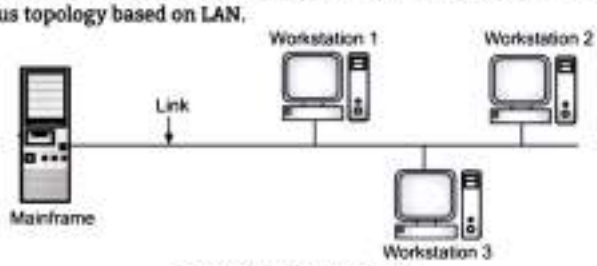


Fig. 1.3: Broadcast Network

1.1.6.2 Point-to-Point Network

- In contrast, Point-to-Point network consists of many connections between individual pairs of machines to go from the source to destination.

- A packet on this type of network may have to visit one or more intermediate machine. Often multiple routes of different lengths are possible.
- So routing algorithms play an important role in Point-to-Point communication. Example: WAN
- It is normally a connection of routers, called as Subnet.
- If two routers, that are not connected by a direct cable and wish to communicate, they must do it via other routers. A packet is sent from one to another via. Intermediate router.
- The packet is stored until there required output line is free and then forwarded.
- A subnet using this principle is called as point to point store and forward or packet switched network.
- A Point-to-Point network with one sender and one receiver is sometimes called Unicasting.
- Examples of Point-to-Point networks are LAN (Local Area Networks), MAN (Metropolitan Area Network), WAN (Wide Area Network), Internet, etc.

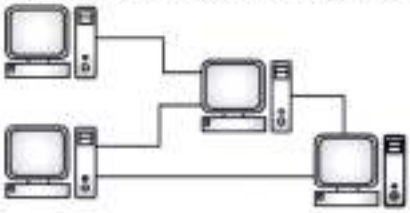


Fig. 1.4: Point-to-Point Network

Advantages:

1. **Simple:** A Point-to-Point network is one of the simplest networks because it only involves two nodes.
2. **Cheapest and effective:** This is one of the cheapest and most effective network architectures because it doesn't involve the cost of redundancies.
3. **Less Complex:** It does not add the complexity of needing several nodes functioning to make a connection.

Disadvantages:

1. **Lack of security:** You have limited number of concurrent connections and anyone with access to the network can access all shared files/folders. You open yourself up to viruses/spyware/adware/rootkits and lots of other 'malware'.
2. **More expensive:** As it requires lots of transmission lines and switching elements to connect remote hosts. It also requires a lot of bandwidth.

1.1.7 Components of Data Communication (W-18)

- The five components of data communication are:

1. **Message/Data:** The message is nothing but the data or information which is to be communicated. It may have texts, numbers, pictures, sound or video or combination of anything from these.
2. **Sender:** This is the device which sends the data message. It can be a computer, workstation, telephone handset, video camera and so on. Data is in human readable form, gets converted into machine form i.e. 0's and 1's.
3. **Receiver:** The receiver is the device which receives the message. Again it can be a computer, workstation, telephone handset, television and so on.

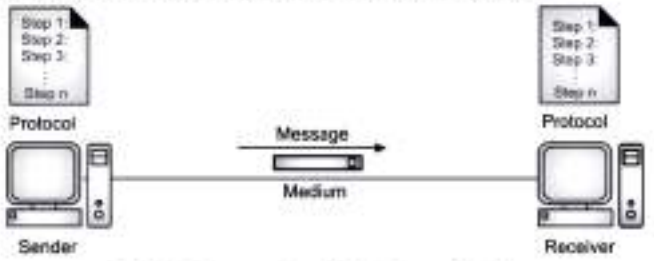


Fig. 1.5: Components of Data Communication

4. **Transmission Medium:** The transmission medium is the physical path by which a message travels from sender to receiver. It may be twisted-pair wire, coaxial cable, fiber-optic cable, laser or radio waves and so on. The radio waves may be terrestrial or satellite microwave.
5. **Protocol:** A protocol is a set of rules required for data communication. It represents the agreement between the two communicating devices. Without protocol, we can connect two devices but they cannot communicate with each other. For example, without a translator, a Japanese cannot communicate with a French person. The job of protocol is similar to the translator.

1.1.8 Advantages and Disadvantages of Network

- Computer Network consist of following Advantages:

1. **Speed:** Networks provide a very rapid method for sharing and transferring files. Without a network, files are shared by copying them to floppy disks, than carrying or sending the disks from one computer to another. This method of transferring files (referred to as Sneaker-net) is very time-consuming.
2. **Cost:** Networkable versions of many popular software programs are available at considerable savings when compared to buying individually licensed copies. Besides monetary savings, sharing a program on a network allows for easier upgrading of the

program. The changes have to be done only once, on the file server, instead of on all the individual workstations.

3. **Security:** Files and programs on a network can be designated as "copy inhibit," so that you do not have to worry about illegal copying of programs. Also, passwords can be established for specific directories to restrict access to authorized users.
4. **Centralized Software Management:** One of the greatest benefits of a network is the fact that all of the software can be loaded on one computer (the *file server*). This eliminates the need to spend time and energy installing updates and tracking files on independent computers throughout the building or campus.
5. **Resource Sharing:** Sharing resources is another area in which a network exceeds stand-alone computers. Most organizations cannot afford enough laser printers, fax machines, modems, scanners, and CD-ROM players for each computer. However, if these or similar peripherals are added to a network, they can be shared by many users.
6. **Sharing Software:** Users can share software within the network easily. Networkable versions of software are available at considerable savings compared to individually licensed version of the same software. Therefore large companies can reduce the cost of buying software by networking their computers.
7. **Easy Communication:** It is very easy to communicate through a network. People can communicate efficiently using a network with a group of people. Person to person communication became easy due to e-mail systems, instant messaging, telephony, video conferencing, chat rooms etc.
8. **Flexible Access:** Some organization's networks allow authorized users to access their files from computers throughout the network of organization.
9. **Workgroup Computing:** Workgroup software (such as *Microsoft BackOffice*) allows many users to work on a document or project concurrently. For example, educators located at various schools within a state could simultaneously contribute their ideas about new curriculum standards to the same document and spreadsheets.

Disadvantages of Network:

- A computer network consist of following disadvantages:

1. **Expensive to Install:** Although a network will generally save money over time, the initial costs of installation can be prohibitive. Cables, network cards and software are expensive, and the installation may require the services of a technician.
2. **Requires Administrative Time:** Proper maintenance of a network requires considerable time and expertise.
3. **Breakdowns and Possible Loss of Resources:** Although a file server is no more susceptible to failure than any other computer in the network. When the files server "goes down," the entire network may come to a halt. When this happens, the entire organization may lose access to necessary programs and files.

4. **Security Threats:** Security threats are always problems with large networks. There are hackers who are trying to steal valuable data of large companies for their own benefit. So it is necessary to take utmost care to facilitate the required security measures.
5. **Bandwidth Issues:** In a network, there are users who consume a lot more bandwidth than others. Because of this some other people may experience difficulties.

1.2 NETWORK TOPOLOGIES (S-18, W-18)

- Topology is the physical layout of computers, cables, switches, routers and other components of a network. This term can also refer to the underlying network architecture such as Ethernet or Token Ring.
- The word "topology" comes from "topos", which is Greek word for "place". When you design a network, your choice of topology will be determined by the size, architecture, cost and management of the network.
- A node is an active device connected to the network, such as a computer or a printer. It can be a piece of networking equipment such as a hub, switch or a router.
- The topology of a network is the geometric representation of the relationship of all the links and linking devices, (usually called *nodes*) to one another.

Note: The term "topology" can refer to either a network's physical topology, which is the actual physical layout or pattern of the cabling or its logical topology, which is the path that signals actually take around the network. This difference is most evident in Token Ring networks, whose cabling is physically arranged in a star, but whose signal flows in a ring from one component to the next. The term "topology" without any further description is usually assumed to mean the physical layout.

Types of Network Topologies:

- Fig. 1.6 shows different categories of topologies in computer network. In the following section we will see description of some of them.

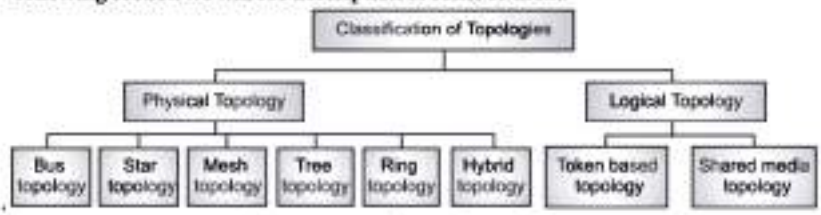


Fig. 1.6: Types of Network Topologies

- Topology defines the physical or logical arrangement of links in a network.
- The **Physical Topology** of a network refers to the configuration of cables, computers and other peripherals. This includes the arrangement and location of network nodes and how they are connected.

- The **Logical Topology** refers to the paths that messages take to get from one user on the network to another.
- Now let us see types of Physical Topology of a network.

1.2.1 Mesh Topology

- Each device in mesh topology has a dedicated point-to-point link to every other device. Dedicated means that link carries traffic only between the two devices it connects.
- The mesh topology connects each computer on the network to the complex in a redundant pattern.
- This topology is generally used only in Wide Area Networks (WANs) in which different networks are connected using routers.

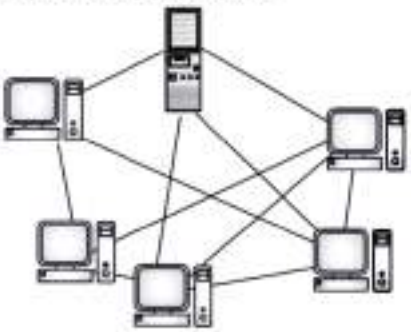


Fig. 1.7: Mesh Topology

- Fully connected mesh network has **n(n – 1)/2** links for **n** devices. To accommodate n(n-1)/2 links, every device on the network must have **n – 1** input/output (I/O) ports. Meshes use a significantly larger amount of network cabling than do the other network topologies, which makes it more expensive. The mesh topology is highly fault tolerant.
- That is, every computer has multiple possible connection paths to the other computers on the network, so a single cable break will not stop network communications between any two computers.
- A network topology in which every device is connected by a cable to every other device on the network. Multiple links to each device are used to provide network link redundancy.

Advantages:

1. Each connection can carry its own data load due to dedicated link.
2. Eliminates traffic problem.

3. Mesh topology is robust. If one link becomes unusable, it does not affect other systems.
4. Privacy or Security because of dedicated line.
5. Point-to-point link make fault identification easy.

Disadvantages:

1. More cables are required than other topologies.
2. Installation and reconfiguration is very difficult because each device must be connected to every other device.
3. Expensive due to hardware requirements such as cables and input/output ports.

1.2.2 Star Topology

- Each device in star topology has a dedicated point-to-point link to central controller, usually called a **hub** or **switch.**
- The controller acts as an exchange that means if one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.
- At the center of the star is a wiring hub or concentrator and the nodes or workstations are arranged around the central point representing the points of the star.
- The hub manages and controls all functions of the network. It also acts as a repeater for the data flow.

Fig. 1.8(a): Star Topology

- The devices are not directly linked to one another in star topology.
- Wiring costs tend to be higher for star networks than for other configurations, because each node requires its own individual cable.
- This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.
- The protocols used with star configurations are usually *Ethernet* or *LocalTalk*. Computers are connected by cable segments to a centralized hub.
- Signal travels through the hub to all other computers. Star topology requires more cable.

- **Illustration of Star topology:** In star topology, each station or node attached to central node (may be hub or switch) (Ref. Fig. 1.8(b)). Suppose node "C" wants to transfer data to node "A". If hub is use as a central node then it will broadcast packet to each every other node but only station/node "A" copies the packet and all other nodes discard the packet. But if switch is used as a central node then it will directly sent the packet only to node "A".

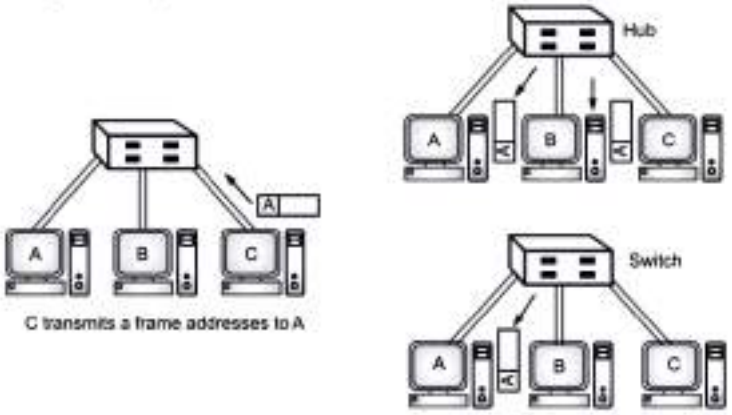


Fig. 1.8(b): Example of Star Topology

Advantages:

1. Easy to install, reconfigure and wire.
2. Robustness i.e. if one link fails, only that link is affected.
3. Fast as compare to ring topology.
4. Multiple devices can transfer data without collision.
5. Eliminates traffic problem.
6. No disruptions to the network then connecting or removing devices.
7. Easy to detect faults and to remove parts.
8. Supported by several hardware and software venders.

Disadvantages:

1. If central node (hub or switch) goes down then entire network goes down.
2. More cabling is required than bus topology, so expensive than bus topology.
3. Performance is depending on capacity of central device.

1.2.3 Bus Topology

- In networking, a topology that allows all network nodes to receive the same message through the network cable at the same time is called as bus topology.

- In this topology, all nodes are connected to a central cable which is called a bus. This bus is also called as a Trunk or sometimes it is also referred to as Backbone cable.
- Trunk cable is then connected to the branch cables which were further connected to the PCs. Every network device communicates with the other device through this Bus.
- Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- A node (computer) that wants to send data, it puts the data on the bus which carries it to the destination node.
- When one computer sends a signal on the wire, all the computers on the network receive the information, but only one accepts the information. The rest regrets the message. One computer can send a message at a time. A computer must wait until the bus is free before it can transmit.

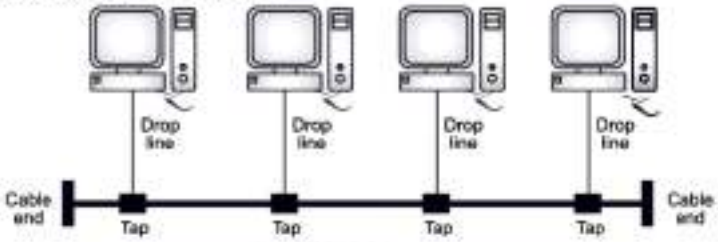


Fig. 1.9(a): Bus Topology

- In bus topology, communications goes both directions along the line. It is a multipoint configuration.
- Examples: Ethernet and LocalTalk networks use a linear bus topology.
- A network that uses a bus topology is referred to as a "Bus Network".

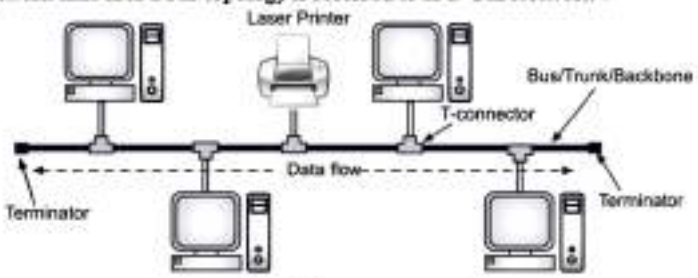


Fig. 1.9(b): A Bus Network

- **Illustration of Bus Topology:** Suppose node "A" wants to transfer data to node "D" as shown in Fig. 1.9(c). In bus topology all nodes will receive the packet sent by node "A" to node "D" because of common/same medium/link used by all nodes. Node "B" and node "C" will reject the packet while node "D" will accept the packet.

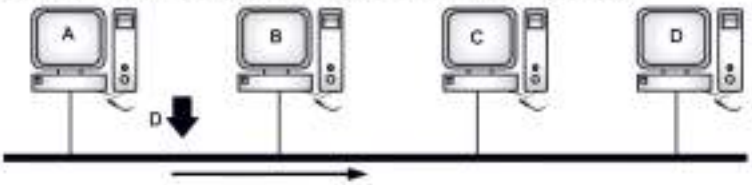


Fig. 1.9 (c): Example of Bus Topology

Advantages:

1. Easy to install. It's very easy to connect a computer or peripheral to a bus.
2. Bus topology is the cheapest way of connecting computers to form a workgroup or departmental LAN because it requires less cabling length.
3. Any one computer or device being down does not affect the others.
4. Fast as compare to ring topology.

Disadvantages:

1. Can not connect a large number of computers.
2. A fault or break in the bus cable stops all transmission.
3. Difficult to identify the problem if the entire network shuts down.
3. Collision may occur.
4. Signal reflection at the taps can cause degradation in quality.
5. Used for only small network.
6. Heavy network traffic can slow a bus considerably.

1.2.4 Ring Topology

- Each device in Ring topology has a dedicated point-to-point line configuration only with the two devices on either side of it, (Dedicated means that the link carries traffic only between the two devices is connects.)
- In ring topology, the computers in the network are connected in circular fashions which form of a ring.
- In other words, in ring topology, each computer is connected to the next computer, with the last one connected to the first, or we can say each device is connected to other two devices with dedicated link in one direction, from device to device.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.

- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along. Computers are connected on a single circle of cable.
- Ring networks normally use some form of token-passing protocol to regulate network traffic. The token is passed from one computer to the next, only the computer with the token can transmit.
- The receiving computer strips the data from the token and sends the token back to the sending computer with an acknowledgment.
- After verification, the token is regenerated. Ring topology is a network topology in the form of a closed loop or circle, with each node in the network connected to the next. Messages move in one direction around the system.
- When a message arrives at a node, the node examines the address information in the message. If the address matches the node's address, the message is accepted; otherwise, the node regenerates the signal and places the message back on the network for the next node in the system.
- This regeneration allows a ring network to cover greater distances than star networks or bus networks.
- The failure of a single node can disrupt network operations; however, fault tolerant techniques have been developed to allow the network to continue to function in the event one or more nodes fail.

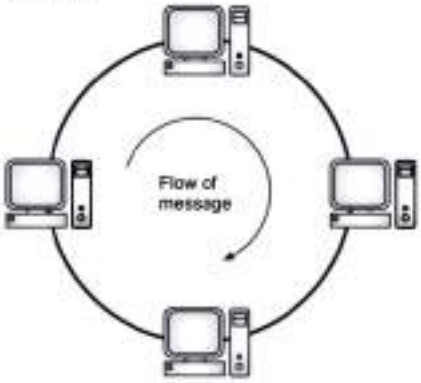


Fig. 1.10(a): Ring Topology

- **Examples:** Ring topology usually seen in a Token Ring or FDDI (Fiber Distributed Data Interface) network.

Illustration of Ring Topology:

- In ring topology, each node functions as a repeater. Suppose, in Fig 1.10(b) ring operates in clockwise direction i.e. data is transferred from one node to another in

clockwise direction and node "B" wants to transmit data to node "A". Node "B" will first prepare the frame, and then forward it towards node "C". Node "C" examines the frame and ignores it. Node "C" simply forwards it to node "A". Node "A" accepts the frame, because its intended for it.

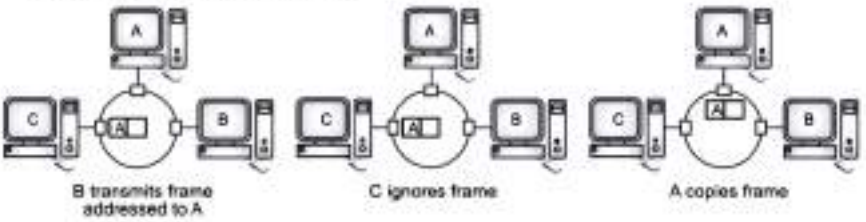


Fig. 1.10 (b): Example of Ring topology

Advantages:

1. Require less cabling so is less expensive.
2. Fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.
4. Reduces chances of collision.
5. Each computer has equal access to resources.
6. There is no need for network server to control the connectivity between workstations.

Disadvantages:

1. The major disadvantage of a physical ring topology is its sensitivity to single link failure. If one connection between two stations fails or a bypass for a particular inactive station is malfunctioning, the ring traffic is down.
2. Traffic is unidirectional.
3. Slow in speed.
4. Reconfiguration is required i.e. to add one node, whole network must be down first.

1.2.5 Tree Topology

- **A tree topology** is variation of a star topology. In tree topology not every device plugs to the central hub. The majority of devices connect to a secondary hub that in turn is connected to the central hub.
- A tree topology can also combines characteristics of linear bus and star topologies.
- It consists of groups of star-configure workstations connected to a linear bus backbone cable.
- Tree topologies allow for the expansion of an existing network and enable schools to configure a network to meet their needs.

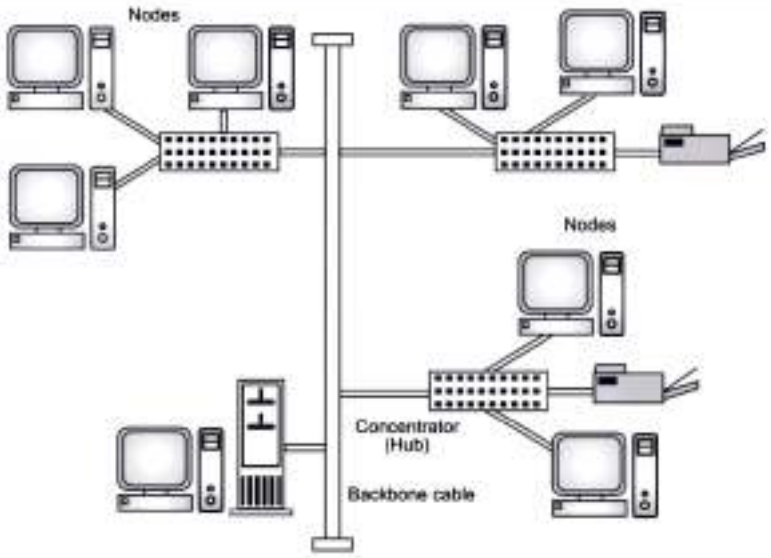


Fig. 1.11: A Tree Network

Advantages:

1. Easy to install, reconfigure and wire.
2. Robustness: If one link fails, only that link is affected.
3. Fast as compare to ring topology.
4. Multiple devices can transfer data without collision.
5. Eliminates traffic problem.
6. No disruptions to the network then connecting or removing devices.
7. Easy to detect faults and to remove parts.
8. Supported by several hardware and software venders.

Disadvantages:

1. If central node (hub or switch) goes down then entire network goes down.
2. More cabling is required than bus topology, so expensive than bus topology.
3. More expensive than bus topologies because of the cost of the concentrators (hub or switch).

1.2.6 Hybrid Topology

- A hybrid topology is combination of two or more network topologies. Fig. 1.12 shows a hybrid star and Bus topologies.

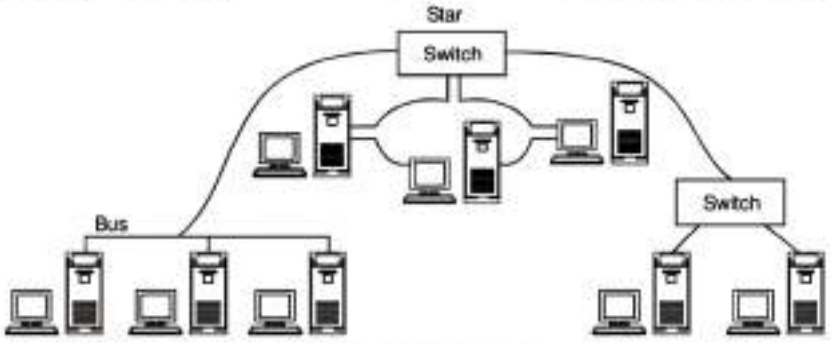


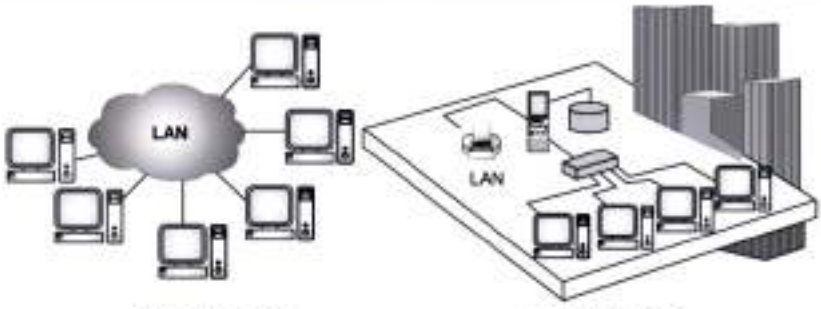
Fig. 1.12: Hybrid Topology

1.3 TYPES OF NETWORK

- Computer networks fall into three classes regarding the size, distance and the structure namely LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).

1.3.1 Local Area Network (LAN) (S-19)

- LAN is a group of computers and associated peripheral devices connected by a communications channel, capable of sharing files and other resources among several users.
- Local area networks are privately-owned networks covering a small geographical area, (less than 1 km) like a home, office, or groups of buildings.
- Depending on the needs of the organization and the type of technology used, a LAN can be as simple as two PCs and a printer or it can extend throughout an organization.
- LANs are widely used to connect personal computers and workstations to share resources like printers and exchange information.
- LANs are distinguished from other kind of networks by three characteristics i.e., their size, their transmission technology and their topology.
- Generally, LAN will use only one type of transmission medium wired or wireless. The most common LAN topologies are bus, ring or star.
- Early LAN had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 to 1000 mbps. Wireless LANs are the newest evolution in LAN technology.
- At present, LANs are being installed using wireless technologies. Such a system makes use of access point or APs to transmit and receive data. One of the computers in a network can become a server serving all the remaining computers called clients.
- For example, a library will have a wired or wireless LAN network for users to interconnect local networking devices. For example, Printers and Servers to connect to the Internet.



(a) Typical LAN (b) Building LAN

Fig. 1.13

1.3.1.1 Components of LAN [W-18]

- LAN components are configurable in a variety of ways, but a LAN always requires the same basic components.
- PCs/workstations and servers.
- Network Interface Card (NIC): A network card is a component that allows the computer to communicate across a network. This component is frequently built into the motherboard of today's computers, but it can also be a separate card for use in a PCI slot, or part of an external unit that connects to the computer via a USB port.
- Cabling and connectors, for example, coaxial cable and BNC connector, Unshielded Twisted Pair (UTP) and RJ-45 connector.
- Hub, concentrator, and more complicated network devices such as Bridge, LAN Switch and Router.

1.3.1.2 Working of LAN [S-18; W-19]

- Before you can link computers into a LAN, you must install a network-aware operating system on them to enable them to share resources.
- The choice of operating system depends on whether the network will be a peer-to-peer network or a server-based network.
- Microsoft Windows 98 is a good choice for peer-to-peer workgroup LANs, while Windows NT and Windows 2000 offer the security and scalability needed to support a server-based network.
- Next, you choose a networking architecture. Then you must install a suitable Network Interface Card (NIC) in an available slot on the motherboard of each node (computer) in the network.
- You must also install a software driver to control the card's functions. You use cabling to join the NICs in order to enable the computers to communicate with each other.

- The most common type of cabling used in LANs is unshielded twisted-pair (UTP) cabling.
- The cabling is installed in some kind of topology or layout, the most popular of which is the cascaded star topology used in the 10BaseT version of Ethernet.
- You then choose a protocol to enable the nodes on the network to speak a common "language"; the most popular protocol is TCP/IP, especially for Internet connectivity, although for small stand-alone workgroup LANs that use Windows 95 or Windows 98/Me, NetBEUI is still popular.

1.3.1.3 Advantages and Disadvantages of LAN

Advantages:

1. The reliability of network is high because the failure of one computer in the network does not effect the functioning for other computers.
2. Addition of new computer to network is easy.
3. High rate of data transmission is possible.
4. Peripheral devices like magnetic disk and printer can be shared by other computers.
5. Less expensive to install.

Disadvantages:

1. Used for small geographical Areas.
2. Limited computers are connected in LAN.
3. Special security measures are needed to stop users from using programs and data that they should not have access to network.
4. Networks are difficult to set up and need to be maintained by skilled technicians.
5. If the file server develops a serious fault, all the users are affected, rather than just one user in the case of a stand-alone machine.

1.3.1.4 Uses of LAN

- Following are the major areas where LAN is normally used:
  1. File transfers and Access
  2. Word and Text processing
  3. Electronic message handling
  4. Remote database access
  5. Personal computing
  3. Digital voice transmission and Storage
  7. Office automation
  8. Factory automation
  9. Distributed computing

10. Fire and Security systems
11. Process control
12. Document distribution.

1.3.2 Metropolitan Area Network (MAN)

- If a network spanning a physical area larger than a LAN but smaller than a WAN, such as a city then this network is called Metropolitan Area Network (MAN).
- MAN is an extended face of LAN, in which computing devices spread over a city are interconnected with communication mediums to form a network.
- Geographical area for MAN lies between 16 km to 50 km generally covers towns and cities. In this type of networks data is transmitted over one or two cables.

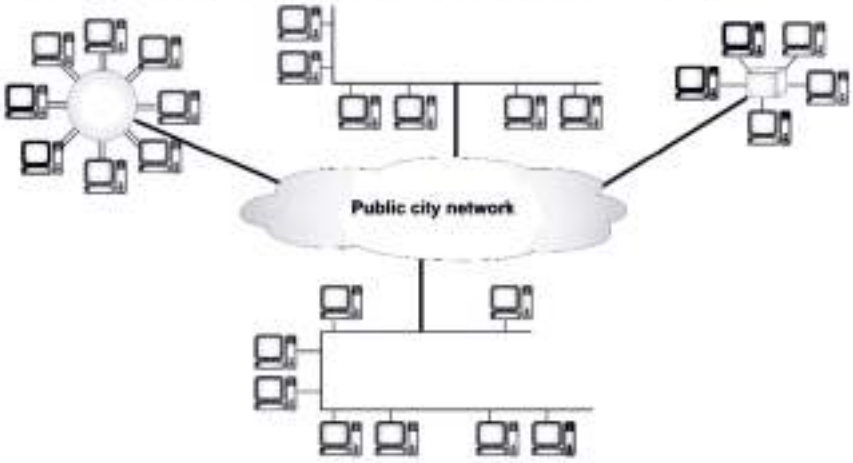


Fig. 1.14: Metropolitan Area Network

- Multiple networks that are connected within the same city to form a citywide network for a specific government or industry.
- By interconnecting smaller networks within a large geographic area, information is easily disseminated throughout the network. Local libraries and government agencies often use a MAN to connect to citizens and private industries. ATM (Asynchronous Transfer Modes), FDDI (Fiber Distributed Data Interface) etc. are the technologies used in MAN.
- A MAN may be wholly owned and operated by a private company. Number of LANs connected so that resources may be shared LAN-to-LAN as well as device-to-device. For example, cable television network.

1.3.2.1 Advantages and Disadvantages of MAN

Advantages:

1. MAN spans large geographical area than LAN.
2. MAN falls in between the LAN and WAN therefore, increases the efficiency of handling data.
3. MAN saves the cost and time attached to establish a wide area network.
4. MAN offers centralized management of data.
5. MAN enables us to connect many fast LANs together.

Disadvantages:

1. Cost is high.
2. Speed is slow.

1.3.3 Wide Area Network (WAN)

- A network that connects users across large distances, often crossing the geographical boundaries of cities or states.
- WANs utilize public, leased, or private communication devices.
- A WAN provides long-distance transmission of data, voice, image, and video information over large geographical areas that may comprise a country, or even whole world.
- A geographically distributed network composed of Local Area Networks (LANs) joined into a single large network using services provided by common carriers.
- WANs are commonly implemented in enterprise networking environments in which company offices are in different cities, states, or countries or on different continents.

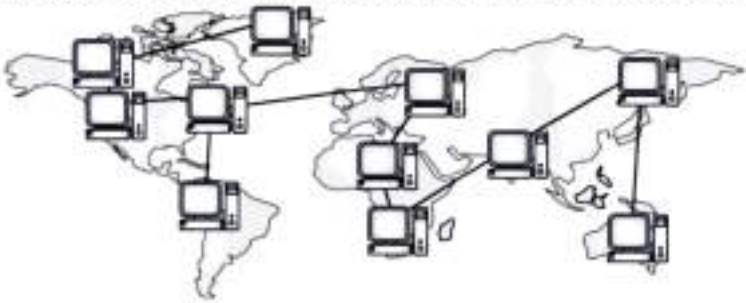


Fig. 1.15: Wide Area Network

- A WAN that is entirely owned and used by a single company is often referred to as an enterprise network.

- Wide area networking combines multiple LANs that are geographically separate. This is accomplished by connecting the different LANs using services such as dedicated leased phone lines, dial-up phone lines (both synchronous and asynchronous), satellite links, and data packet carrier services.
- Wide area networking can be as simple as a modem and remote access server for employees to dial into, or it can be as complex as hundreds of branch offices globally linked using special routing protocols and filters to minimize the expense of sending data sent over vast distances.
- A WAN is a geographically dispersed collection of LANs. A wide area network is simply a LAN of LANs or Network of Networks.
- WAN are characterized by the slowest data communication rates and the largest distances.
- Wide Area Networks are commonly connected either through the Internet or special arrangements made with phone companies or other service providers.
- WAN may use advanced technologies like Asynchronous Transfer Mode (ATM), Frame Relay and SONET.
- Internet, Indian Railway Reservation System, Bank Networks that supported core banking, etc. are some good examples of WAN. The Internet is the largest WAN, spanning the World today.
- LAN's and WAN's come in many different flavors. The most popular type of network is Ethernet. Ethernet networks have speeds of 10 Mbps, 100 Mbps, or 1 Gbps.

1.3.3.1 Architecture of Wide Area Network

- WAN contains a collection of machines used for running user (i.e. application) programs. All the machines called hosts are connected by a communication subnet.

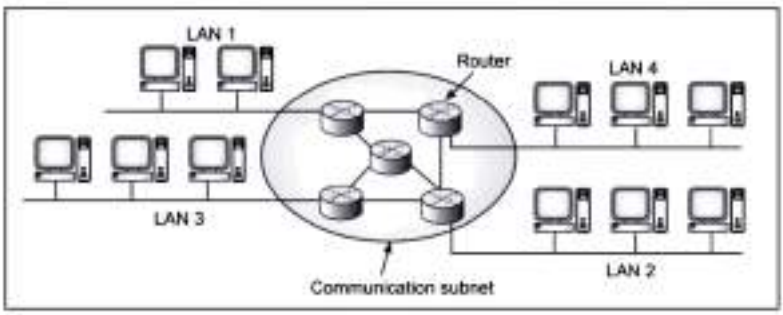


Fig. 1.16: Communication Subnet in WAN

- The function of the subnet is to carry messages from host to host. The subnet consists of two important components; transmission lines and switching elements.

- Transmission lines move bits from one machine to another. The switching elements are specialized computers used to connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line to forward them.
- The switching elements are either called as packet switching nodes, intermediate systems, data switching exchanges or routers.
- When a packet is sent from one router to another via one or more intermediate routers, the packet is received at intermediate router. It is stored in the routers until the required output line is free and then forwarded. A subnet using this principle is called a Point to Point, store-forward or Packet Switched Subnet.
- WAN's may use public, leased or private communication devices, and can spread over a wide geographical area. A WAN that is entirely owned and used by a single company is often called as an Enterprise Network.

1.3.3.2 Characteristics of WAN

- Followings are the major characteristics of WAN.

1. **Communication Facility:**
   - For a big company spanning over different parts of the country the employees can save long distance phone calls and it overcomes the time lag in overseas communications.
   - Computer conferencing is another use of WAN where users communicate with each other through their computer system.
2. **Remote Data Entry:**
   - Remote data entry is possible in WAN. It means sitting at any location you can enter data, update data and query other information of any computer attached to the WAN but located in other cities.
   - For example, suppose you are sitting at Madras and want to see some data of a computer located at Delhi, you can do it through WAN.
3. **Centralized Information:**
   - In modern computerized environment you will find that big organizations go for centralized data storage.
   - This means if the organization is spread over many cities, they keep their important business data in a single place.
   - As the data are generated at different sites, WAN permits collection of this data from different sites and save at a single site.

Advantages:

1. Allows many people to use the same network from many different locations.

2. Used for Large Geographical Area.
3. Expensive devices (like printers or phone lines to the internet etc.) can be shared by all the computers on the network.
4. Adds fluidity to user's information communication.

Disadvantages:

1. Protection against hackers and viruses adds more complexity and expense.
2. Setting up a network can be time consuming.
3. Can be expensive.
4. Slow in speed than LAN and MAN.
5. WANs need a good firewall to restrict outsiders from entering and disrupting the network.

Difference between various types of Networks:

Table 1.1: Difference between LAN, MAN and WAN

Sr. No.	Parameters	LAN	WAN	MAN
1.	Stands for	Local Area Network.	Wide Area Network.	Metropolitan Area Network.
2.	Area covered	Covers small area i.e. within the building (less than 1 km).	Covers large geographical area, like country, state etc.	Covers larger area than LAN and smaller than WAN like city, campus.
3.	Error rates	Lowest.	Highest.	Moderate.
4.	Transmission speed	High.	Low.	Moderate.
5.	Equipment cost	Uses inexpensive equipment.	Uses most expensive equipment.	Uses moderately expensive equipment.
6.	Example	Offices, Cyber Café.	Internet.	ATM, FDDI etc.
7.	Data transfer rate	High.	Low.	Moderate.
8.	Setup cost	Low.	High.	Moderate.

1.3.4 Internetwork (S-19)

- Today, it is very rare to see a LAN, a MAN in isolation, they are connected to one another. When two or more networks are connected, they become an Internetwork or Internet.

- An internetwork is formed when distinct networks are interconnected. The Internet is a structured organized system.
- Internetworking started as a way to connect different types of computer networking technology.
- Computer network term is used to describe two or more computers that are linked to each other. When two or more computer networks or computer network segments are connected using devices such as a router then it is called as Computer Internetworking.
- Internetworking is a term used by Cisco. Any interconnection among or between public, private, commercial, industrial, or governmental computer networks may also be defined as an internetwork or Internetworking.
- An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.
- Internetworking refers to the industry, products, and procedures that meet the challenge of creating and administering internetworks.
- The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made-up of many wide and local area networks joined by connecting devices and switching stations.

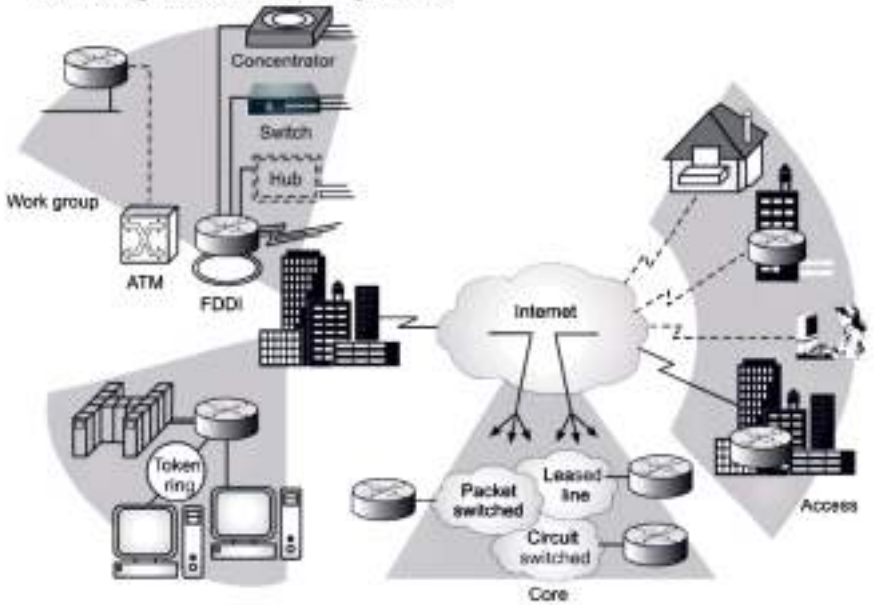


Fig. 1.17: Internetworking

- Today, most end users who want Internet connection use the services of Internet Service Providers (ISPs). There are international, national, regional and local service providers.
- There are following variants of Internetwork or Internetworking:
  1. **Intranet:** An intranet is a set of interconnected networks or Internetworking, using the Internet Protocol and uses IP-based tools such as web browsers and FTP tools that are under the control of a single administrative entity.
  2. **Extranet:** An extranet is a network of internetwork or Internetworking, that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities.
  3. **Internet:** It is a network of networks based on many underlying hardware technologies, but unified by an internetworking protocol standard, the Internet Protocol Suite. It is often also referred as TCP/IP.

Advantages of Internetworking:

1. Internetworks reduce network traffic.
2. The benefit of reduced traffic is optimized performance.
3. Network problems can be more easily identified and isolated in smaller networks, as opposed to one large network.
4. We can more efficiently span long distance by connecting multiple smaller networks.

1.3.5 Wireless Network

- Wireless communication is one of the fastest growing technologies. The demand for connecting devices without the use of cables is increasing everywhere.
- The word wireless is dictionary defined as "having no wires".
- In networking terminology, wireless is the term used to describe any computer network where there is no physical wired connection between sender and receiver, but rather the network is connected by radio waves and/or microwaves to maintain communications.
- The basis of wireless systems is radio waves, an implementation that takes place at the physical level of network structure.

1.3.5.1 Types of Wireless Network

- Wireless networks can be divided into three main categories as System Interconnection, Wireless LANs, and Wireless WANs.

1. **System Interconnection:**

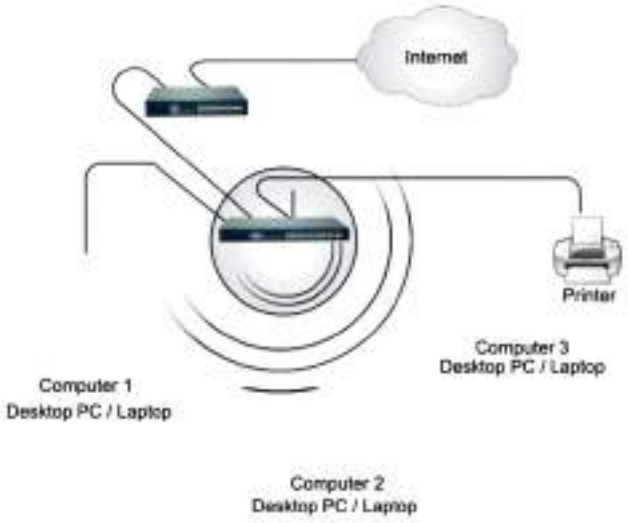
- System interconnection means connecting the components of computer using short range radio.
- All components can also be connected by a short range wireless network called Bluetooth. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer.

- The system interconnection networks use the Master-Slave paradigm as shown in Fig. 1.18.

Fig. 1.18: Bluetooth Configuration

2. Wireless LANs:

- The next step in wireless networking is the wireless LANs. WLANs are systems in which every computer has a radio modem and antenna with which it can communicate with other system.
- Wireless LANs are becoming increasingly common in small offices and homes.
- IEEE 802.11 is a standard for wireless LANs.



- A Wireless Local Area Network (WLAN) links two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for Internet access.

3. Wireless WANs:

- The third kind of wireless network is used in wide area system.
- The radio network used for cellular telephones is an example of a low-bandwidth wireless system.
- Cellular wireless networks are like wireless LANs except that the distances involved are much greater and the bit rates are much lower.
- In addition to low-speed networks, high bandwidth wide area wireless networks are also being developed. The initial use is high speed wireless internet access from homes and business bypassing the telephone system.
- Wireless Wide Area Networks (WWANs) are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public internet access system.

Fig. 1.20: WWAN

1.4 MODES OF COMMUNICATION (S-18, 19 W-18)

- In data communication, the exchange of information takes place through transmission modes which defines the direction of the flow of information between two communication devices i.e. it tells the direction of signal flow between the two devices.
- Communication between two devices can be Simplex, Half-duplex or Full duplex transmission modes..

1.4.1 Simplex

- In simplex mode, the communication is unidirectional, as on a one-way street.
- Only, one of the two devices on a link can transmit; the other can only receive.

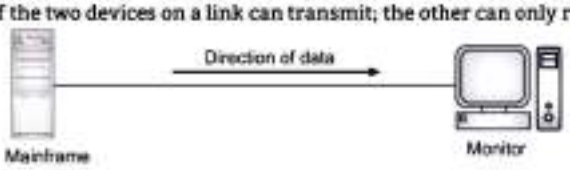


Fig. 1.21: Simplex Mode

- Simplex means communication runs in one direction. The examples includes:
  (i) TV and radio broadcasting or pager.
  (ii) Keyboards and traditional monitors are both examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.
- Simplex transmission occurs in many common communication applications, the most obvious being broadcast and cable television.
- It is not used in true network communication because stations on a network generally need to communicate both ways.
- Some forms of network communication might seem to be simplex in nature, such as streaming audio or video, but the communication actually takes place using bidirectional network traffic, usually Transmission Control Protocol (TCP) traffic.

1.4.2 Half Duplex

- In half-duplex mode, each station can both transmit and receive, but not at the same time. For half-duplex, both end devices can send and receive, (they must alternate). When one device is sending, the other can only receive, and vice versa.

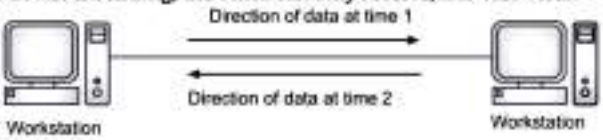


Fig. 1.22: Half-duplex Mode

- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- The simplest example is a walkie-talkie: You have to press a button to talk and release the button to listen. When two people use walkie-talkies to communicate, at any given moment, only one of them can talk while the other listens. If both try to talk simultaneously, a collision occurs and neither hears what the other says.
- Communication through traditional Ethernet networks is another example of half-duplex communication. When one station on an Ethernet transmits, the other stations detect the carrier signal and listen instead of transmitting. If two stations transmit signals simultaneously, a collision occurs and both stations stop transmitting and wait random intervals of time before retransmitting.

1.4.3 Full Duplex

- In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously. The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time.
- In full-duplex mode, signals going in either direction share the capacity of the link.

Fig. 1.23: Full-duplex Mode

- Sharing of link can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals travelling in both directions.
- For example, mobile phones operate in full-duplex mode when two persons talk on mobile phone, both can listen and speak simultaneously.
- In full-duplex communication, both stations send and receive at the same time, and usually two communication channels are required. However, you can also achieve full-duplex communication using a multiplexing technique whereby signals travelling in different directions are placed into different time slots.
- The disadvantage of this technique is that it cuts the overall possible transmission speed by half.

1.5 SERVER BASED LANS & PEER-TO-PEER LANS (S-18, 19 W-18)

- The PC requires operating system to manage the files and hardware. Similarly, LAN needs the NOS (Network Operating System) which controls the transmission of data and messages between workstations.

- In the simplest case, the NOS makes the disk drive on the server appear to be an extra drive (F:) on each workstation.
- The NOS also make a LAN printer appears as a locally attached printer at your workstation.
- The LAN's are of two types.
  1. Server-based LAN.
  2. Peer-to-peer LAN.
- The server-based LAN, a separate, unattended computer acts as a file server. Whereas in peer-to-peer LAN, a workstation may acts as a workstation and file server simultaneously.

1.5.1 Server-Based LAN

- These LAN's offer better performance and increased the reliability.
- Network operating system such as Novell network is installed on a file server which replaces the DOS completely.
- The file server organizes the disk in a way that performs well for large files. This is referred as dedicated server LAN.
- Companies that offer server based LAN's are Apple Talk, Wrap Server, Vines, Netware, and Windows NT Server.
- The diagrammatic representation of server based LAN is as shown in Fig. 1.24.

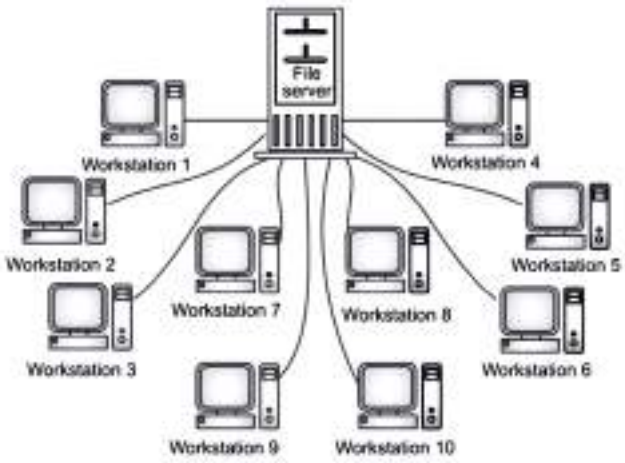


Fig. 1.24: Server Based LAN's

1.5.2 Peer-to-Peer LAN

- In this LAN, only one machine will work as workstation and a file server.
- This is not a dedicated machine. Fig. 1.25 shows peer-LAN environment, in which three desktop computers acts as both file server and workstation.
- In a peer LAN, the disk space and files on your computer become communal property. Peer LAN's are cost effective for small, lightly loaded networks.
- The advantage of this LAN is that user don't have to remember to copy files from their computers be a separate file server for other people to access.
- Obviously this access is depends upon the security and rights given to the users.

Fig. 1.25: Peer-to-Peer LAN

- The companies that offer peer LAN's are 10NETplus, EasyNet, AppleTalk, GVLANOS, Ready Link, NET/30 etc.
- The NOS is installed on a file server machine and this network software is installed on each machine. They communicate through protocol.
- A list of NOS is given below in Table. But most popular NOS is Novell Netware.

Table 1.2: List of Various Network Operating Systems

Operating system	Manufacturer
AppleTalk	Apple
LANtastic	Artisoft
Netware	Novell
Network File System (NFS)	Sun microsystem
Wrap server	IBM
Wrap connect	IBM
Vines	Banyan
Window NT server	Microsoft
Windows for workgroup	Microsoft

1.5.3 Comparison of Server-based LAN and Peer-to-Peer LAN (S-19)

Table 1.3: Difference between Server-based LAN and Peer-to-Peer LAN

Sr. No.	Server-based LAN	Peer-to-Peer LAN
1.	Server-based LAN a separate, unattended computer acts as a file server.	Peer-to-peer LAN, a workstation may acts as a workstation and file server.
2.	Server-based LAN also referred as dedicated server LAN.	Peer-to-peer LAN is not dedicated machine.
3.	High performance.	Low performance.
4.	More reliable.	Less reliable.
5.	Costly for small network.	Cost effective for small networks.
6.	Examples: (i) Apple Talk, (ii) WrapServer	Examples: (i) EasyNet, (ii) 10NetPlus

1.6 PROTOCOLS AND STANDARDS (S-18, W-18)

- Protocol is very important for networking without a protocol network is meaningless. The sender and the receiver, the two parties in data communication must agree on a common set of rules, i.e. protocols before they can communicate with each other.
- A protocol is a set of rules that governs the communications between computers on a network. The sender and the receiver, the two parties in data communication must agree these rules before they can communicate with each other.
- These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.
- In networking many protocols are available, some of which are more popular than others.
- Two networking devices wishing to communicate with each other cannot just begin data transmission arbitrarily, i.e. one device cannot simply start sending bit streams to the other. The two networking devices must agree on a set of rules before this transmission can begin.

Terms:

- A protocol defines the following terms:
  1. **Timing:** Timing refers to an agreement between the sender and the receiver about the data transmission rates and duration.

2. **Syntax:** The syntax of protocol defines the structure or format of data. This means that the order in which it is to be sent is decided. A protocol could define that the first 16 bits of a data transmission must always contain the receiver's address.
3. **Semantics:** Protocol semantics defines the interpretation of the data that is being sent. For example: The semantics could define that if the last two bits of the receiver's address field contain a 00, it means that the sender and the receiver are on the same network.

1.6.1 Examples of Protocols

- The most common protocols are:
  1. Ethernet
  2. LocalTalk
  3. Token Ring
  4. FDDI
  5. ATM

1. Ethernet:

- The Ethernet protocol is by far the most widely used. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection).
- This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear.
- Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs.
- Each computer then backs off and waits a random amount of time before attempting to retransmit.
- With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.
- The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over wireless access points, twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps up to 1000 Mbps.
- To allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps. This is commonly called **Fast Ethernet**.
- Fast Ethernet requires the use of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary.
- Fast Ethernet is becoming common in organizations that have been recently wired.

2. LocalTalk:

- LocalTalk is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers.
- The method used by LocalTalk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).
- It is similar to CSMA/CD except that a computer signals its intention to transmit before it actually does so.
- LocalTalk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software.
- With the addition of the server version of AppleShare software, a client/server network can be established.
- The LocalTalk protocol allows for linear bus, star, or tree topologies using twisted pair cable. A primary disadvantage of LocalTalk is speed. Its speed of transmission is only 230 Kbps.

3. Token Ring:

- The Token Ring protocol was developed by IBM in the mid-1980s. The access method used involves token-passing.
- In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring.
- A single electronic token moves around the ring from one computer to the next.
- If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token.
- The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer.
- The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring has decreased.

4. FDDI:

- Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances.
- The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology.
- Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring.
- A major advantage of FDDI is speed. It operates over fiber optic cable at 100 Mbps.

5. ATM:

- Asynchronous Transfer Mode (ATM) is a network protocol that transmits data at a speed of 155 Mbps and higher.
- ATM works by transmitting all data in small packets of a fixed size; whereas, other protocols transfer variable length packets.
- ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology, which can work with fiber optic as well as twisted pair cable.
- ATM is most often used to interconnect two or more local area networks. It is also frequently used by Internet Service Providers to utilize high-speed access to the Internet for their clients.
- As ATM technology becomes more cost-effective, it will provide another solution for constructing faster local area networks.

Table 1.4: Summary of Protocols

Protocol	Cable	Speed	Topology
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	0.23 Mbps (or 230 Kbps)	Linear Bus or Star
Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

- Protocols also define procedures for handling lost or damaged transmissions or "packets." TCP/IP (for UNIX, Windows NT, Windows 95 and other platforms), IPX (for Novell NetWare), DECnet (for networking Digital Equipment Corp. computers), AppleTalk (for Macintosh computers), and NetBIOS/NetBEUI (for LAN Manager and Windows NT networks) are the main types of network protocols in use today.

1.6.2 Protocol Standards

- Standards are necessary in daily life. Everything that we use in our daily life has some common features, some standards. In the absence of standards, every manufacturer can theoretically manufacture a set of goods or services that are incompatible with other manufactures.
- To avoid such anomalies or problems a set of standards is established which governs the rules that manufactures must obey. In exactly the same way standards for data communications have been set or developed.

- A lot of incompatibility issues have no place in data communications, which is highly desirable.
- Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.
- Setting standards, rules that all manufacturers of hardware and software will follows, are important for a number of reasons:
  - Standards describe accurately and unambiguously how information is transmitted.
  - A manufacturer's products will work successfully with other manufacturer's products if they all follow the same standards.
  - By defining a set of standards, you are providing a framework within which all manufacturers can design new, successful products.
  - Standards break down complex ideas into smaller, methodical, and easier to understand components.
- Data communications standards can be classified into two types: De facto (i.e., meaning "by fact" or "by convention") and De jure (meaning "by law" or "by regulation").

1. De facto:

- The standards that have not been approved by an organized body but have been adopted as standards through widespread use are De facto standards. De facto standards are often established originally by manufactures who seek to define the functionality of a new product of technology.
- **De facto** data communication standards can be further divided into **proprietary** and **non-proprietary** standards. The proprietary standards are invented and owned by an organization who first uses them, and which gain popularity.
- Proprietary standards are closed, because they close-off communication with devices/systems of other vendors. Non-proprietary standards are those that are developed by an organization/ committee/group, which become popular and vendors start supporting them.
- Non-proprietary standards are open standards because anybody adhering to those automatically gains access to all others following those standards.

Examples:

1. The most important De facto organization involved in establishing communication standards and protocols is CCITT (Consultative Committee for International Telegraph and Telephone) is United Nations agency responsible for defining standards for Telegraph and Telephone. X.25 is most common standard for WAN.

2. IBM (International Business Machines): SNA (System Network Architecture) protocol is example of De facto protocol. The IBM developed this protocol in 1974 for its mainframe computers, still being used by large number of organizations all over the world.

2. De jure:

- These standards have been legislated by an official body. These are usually led by governments or government-appointed agencies.

Examples:

- For example, the IEEE (Institute of Electrical and Electronic Engineers) has the authority to create electrical standards such as wireless communication.
- On a global level ISO, the International Standards Organization was setup to create standards. They have produced over 18,500 formal standards covering everything from quality control to making tractors.

1.6.3 Standards Organizations

- Standards organizations can be classified into three categories:
  1. Standards creation committees
  2. Forums
  3. Regulatory agencies
- There is lot of organizations serving as standards creation committees.

1. American National Standards Institute (ANSI):

- ANSI is a private non-profit organization that does not have any direct ties with the US federal government. Generally, all ANSI projects are undertaken for the social benefit of the US citizens. Professional groups, regulatory bodies, government, and consumer groups represent ANSI.

2. Electronic Industries Association (EIA):

- EIA is a non-profit organization that is aligned with ANSI. EIA focus is public awareness and lobbying for standards. The main contributions to the data communications technology are the development of interfaces for physical connections and electronic signal specifications for data communications.

3. International Telecommunications Union-Telecommunications Standards Sector (ITU-T):

- ITU-T was earlier known as the Consultative Committee for International Telegraphy and Telephony (CCITT). ITU-T was formed by the United Nations in response to the demands from some nations who were developing their own national standards for data communications in the early 1970s and which led to issues of incompatibility with each other.

4. **Institute of Electrical and Electronics Engineers (IEEE):**

- IEEE is the biggest professional engineering body in the world. IEEE focus areas are developments in the areas of electric and electronic engineering and radio sciences. IEEE also covers the development and adoption of international computer and communications standards.

5. **International Standards Orgnisation (ISO):**

- ISO is a well-known multi-national standards body. Open Systems Interconnection (OSI) model as a networking protocol is a major contribution of the ISO to the data communications world. Most members of ISO are their respective government representatives. ISO created in 1947, the ISO is a non-profitable standards creation organisation. Members from over eighty developed nations actively represent the ISO.

Forums:

- The main drawback of standards committees is notorious for the slow speed of developments and decision-making.
- Forums generally concentrate on a particular technology, and this specialization helps them to achieve a great amount of throughput with contributions from a variety of forum members.
- User groups, industry representatives, university students, and experts come together and set up forums to address the various issues and concerns of data communications technology, and come up with standards from time to time.
- **Examples:**
  1. Internet Society (ISOC)
  2. Internet Engineering Task Force (IETF)
  3. Frame Relay Forum
  4. ATM Forum
- These are Government appointed agencies. For example, Federal Communications Commission (FCC) of the US are always involved in regulating standards.
- These agencies help to protect the interests of the general public in areas such as radio, television and wired communications.
- Every portion of communications technology must be approved by FCC before it can be sold in the market.
- FCC periodically reviews the rates changed by service providers, technical specifications of communication hardware and divides and allocates ratio frequencies, etc.

1.7 NETWORK SOFTWARE

- Network software interacts, increases and faciliates the functions of a computer network. It has become integral part of today's computing world where shared information, effective communication and reliable productivity is needed.

1.7.1 Protocol Hierarchies, Layers, Peers, Interfaces

Protocol Hierarchy:

- Networks are set up with a protocol hierarchy that divides the communication task into several layers. A protocol is a set of rules for communication within a layer.
- Design of protocols should be simple. To reduce the design complexity of a protocol, most of the networks are organized as a series of **layers** or levels. Each layer is built upon its predecessor i.e. previous layer.
- The number of layers used, name of each layer, contents of each layer and function of each layer are different from one network to other network. But the purpose of each layer is to offer services to the higher layers is same in all networks.
- Layer n on one machine communicates with its corresponding layer n of another machine. That is layer 1 communicates with layer 1 of other machine. The rules and the conventions which are used for this conversation/communication are known as layer 'n' protocol. Fig. 1.26 illustrates 7-layer network.

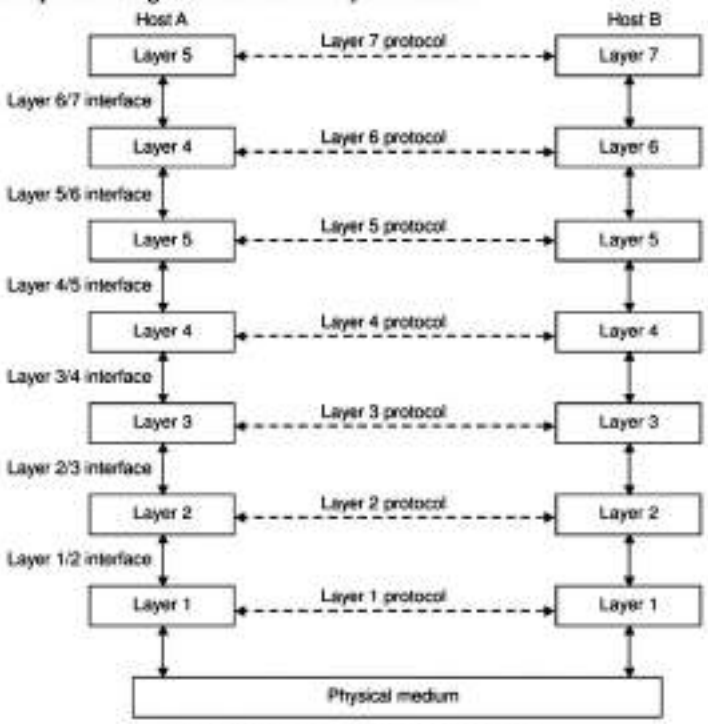


Fig. 1.26: Layers, Protocols and Interfaces

- **Peers:** The corresponding layer entities on different machines are called **peer** processes. We can say that each peer communicates through protocol.
- Actually, speaking, no data can directly transfer from layer n of one machine to layer n of another machine. Each layer passes data and control information to the lower level. For example, layer 6 passes data to layer 5.
- When it reaches to lowest layer i.e. layer 1 it transfers data to the physical medium which is the medium through which actual communication occurs. We can say that layer 5 of one machine has virtual communication with layer 5 of another machine.
- This virtual communication is shown by dotted lines and physical communication, [occurs in layer 2 and layer 1] is shown by solid lines.

Interface:

- The physical communication between each pair of adjacent layers is known as **Interface**. The interface defines the primitive operations and services which a lower layer offer to the upper one.
- Most important considerations are defining clean interfaces between the layers. So that if we want to replace a layer with different implementation, it must be possible. For example, all telephone lines we replaced by satellite channels. The amount of information passed between layers should be smallest.
- The set of layers and protocol together is called the **Network Architecture**. The architecture must have enough information. So that the software and hardware can be designed to follow the protocols.
- But the details of the implementation and specification of interfaces are not considered as a part of architecture. It is because these are not visible from outside and are within the machines.

Multi-layer Communication:

- Let's consider the idea of multi-layer communication. Two persons (layer 3), one speaking French and other speaking Japanese want to communicate. As they have to common language they require a translator (layer 2) who translates their messages into the respective language (English).
- The translators contact with engineers (layer 1) for transmission by telegram, telephone, computer network etc. And the message is passed across 2/3 interface to second person.
- Here, the protocol is completely independent of the other ones. If both translators switch from English to German, it will not affect the other protocol.

Example:

- Now let's consider the technical example of 7-layer network. A message M is produced by host A in layer 7. The message is passed from layer 7 to layer 6 according to the definition of layer 6/7 interface. Layer 6 transforms the message in certain ways for example text compression. Then it passes the new message M to layer 5 across layer 5/6 interface. Layer 5 just regulates the direction of flow.

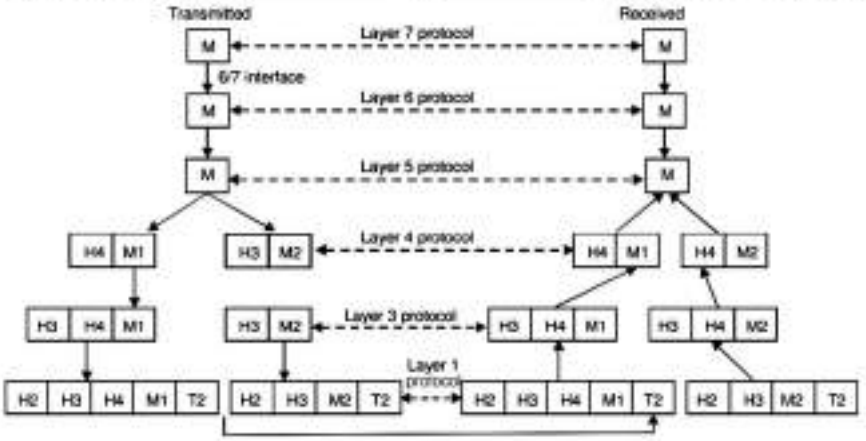


Fig. 1.27: Information Flow in 7 Layer Network

- In many networks, layer 4 does not have restrictions or limits to the size of the message. But layer 3 may have limits. So layer 4 breaks up the message into smaller units, by writing a header to each unit. Header allows reconnecting the message in the original form at destination machine. Header contains the sequence number. Sometime, in many layers header contains sizes, times and other control fields with the sequence number.
- Layer 3 decides about the outgoing line and attaches its own header and then passes the data to layer 2.
- Layer 2 adds a header to each piece and a trailer and then gives this resulting message in the form of unit to layer 1 for physical transmission. This message is converted back again into the original message with the same procedure from lower layer to upper layer.
- The peer process abstraction is very crucial to all network design. This abstraction technique allows partitioning the design at complete network i.e. unmanageable problem into several smaller and manageable layers.

1.7.2 Design Issues of the Layers

(W-18)

- Some of the key design issues that occur in computer netoworking are present in severeal layers. Below, we will briefly mention some of the more important ones.

1. **Connection Establishment and Termination:** In a network, there are many computers available. Each machine has multiple processes. A process of one machine specifies with which computer connection is established. Therefore every layer must have a mechanism for connection establishment. When the

connection is not needed, it should be terminated. That is why there should be a mechanism available to terminate the connection.

2. **Addressing:** Every layer needs a mechanism for identifying senders and receivers. Since a network normally has many computers, some of which have multiple processes, a means is needed for a process on one machine to specify with whom it wants to talk. As a consequence of having multiple destinations, some form of addressing is needed in order to specify a specific destination. That is the facility of acknowledgement can be provided.
3. **Direction of Data Transfer:** There are some rules for data transfer. These rules should be present in the design issue. Data transfer may be simplex, half-duplex or full-duplex. Simplex communication means the data travels in one direction. For example: data transfer from CPU to monitor. Half-duplex means data can transfer in either direction but not simultaneously. For example: data transfer from one workstation to other workstation. Full-duplex means data transfer is possible in both directions at once.
4. **Error Control:** The physical communication circuits are not perfect. So control is an important issue. The receiver and sender, both ends of the connection must agree upon the error-detecting and error-correcting code. The receiver can gives acknowledgement to the sender about which message has been received or not.
5. **Avoid loss of sequencing:** Proper sequencing must be allowed. This is needed because in the communication channels the messages are not delivered in the same order as they were sent. So by providing sequence number provision, a receiver can put them back in order.
6. **Ability of receiving Long Messages:** Several layers cannot accept very long messages. So there should be a mechanism to disassemble that message, transmit it and reassemble it again. Similarly, if the message is very small or a data unit is very small, it is inefficient to transmit them separately. So several small messages to the same destination are gathered into a single message, transmitted and then afterwards separated at last end.
7. **To use Multiplexing and De-multiplexing:** There are various processes available; it is very expensive or inconvenient to set up a separate connection for each pair of communicating process. So it is necessary to have multiplexing and de-multiplexing. This is needed to share a single communication channel among several unrelated conversations. For example: Client/ Server model.
8. **Routing:** It is a network structure. So for reaching a particular destination, multiple paths are available. One or two layers can be split up and have a routing technique. A route can be chosen for communication. For example, if we want to go to ShivajiNagar, we can go from Fergusson college Road or from Jangali Maharaj Road etc.

Layers:

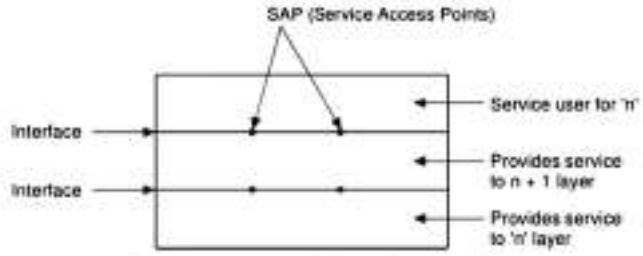


Fig. 1.28: Layers to Reduce Design Complexity

- To reduce design complexity, most networks are to achieve as a series of layers or levels. Each one built upon the one below it.
- **SAP (Service Access Points):** SAP is generally used as an identifier label for endpoints of network in OSI networking or model. It is a data structure and identifier also for a buffer area in memory of system. It is a point in a layer of a layered architecture where a network is usually provided and where layer just above layer that provides service can probably have access to it.
- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differs from network to network. However, in all networks, the purpose of each layer is to offer certain services to the higher layer.
- The function of each layer is to provide services to the layer above it. The active elements in each layer are often called entities. Entity can be software entity or hardware entity.
- The layered architecture concept redefines the way networks are conceived and creates significant cost savings and managerial benefits.
- Instead of building a separate network for each service, user can have multiple services sharing a common core network.
- Adding new services and managing the network infrastructure must be easy.
- That is why the layered architecture concept will become increasingly important for user.
- It offers opportunities to reduce capital and operating expenditure by offering a smooth step-by-step migration to IP.
- Key advantage is that network resources can be used more effectively in terms of simplicity and fewer equipment sites leading to lower total cost of ownership.
- Also, the need for transmission connections in the network can, in many cases, be reduced by more than 50 %.

1.7.2.1 Advantages and Disadvantages of Layered Designs

Advantages:

- Layered designs issues consist of following advantages:

1. Segmentation of high-level from low-level issues. Complex problems can be broken into smaller more manageable pieces.
2. Since, the specification of a layer says nothing about its implementation, the implementation details of a layer are hidden, (abstracted) from other layers.
3. Easier exchange of parts at a later date.
4. Development by teams is aided because of the logical segmentation.
5. Many upper layers can share the services of a lower layer. Thus layering allows us to reuse functionality.

Disadvantages:

- Layered designs consist of following disadvantages:

1. Layering can lead to poor performance. To avoid this penalty, in situations where an upper layer can optimize its actions by knowing what a lower layer is doing, we can reveal information that would normally be hidden behind a layer boundary.
2. The layers must be engineered at the outset, before the system is built.
3. Layering is a form of information hiding. A "layering violation" occurs in situations where a layer uses knowledge of the implementation details of another layer in its own operations. At the limit this leads to changes to one layer resulting in changes to every other layer, which is an expensive and error prone proposition.
4. The trouble with layers of computer software is that sooner or later you loose touch with reality. Layers are abstraction boundaries and the more they encapsulate their works the more one is unaware of the application's inner works.

1.7.3 Connection Oriented and Connectionless Services [S-19]

- Layers can offer two different types of service to the layers are:
  1. Connection-oriented
  2. Connectionless

1.7.3.1 Connection-oriented Services

- In general, transport protocols can be characterized as being either connection-oriented or connectionless.
- Connection-oriented services must first establish a connection with the desired service before passing any data.
- A connectionless service can send the data without any need to establish a connection first.

Phases in Connection-oriented service:

- Connection-oriented service involves three phases: Connection Establishment, Data Transfer, and Connection Termination.

- **Connection Establishment:** During connection establishment phase, the end nodes may reserve resources for the connection.
- The end nodes also may negotiate and establish certain criteria for the transfer, such as a window size used in TCP connections. This resource reservation is one of the things exploited in some denial of service (DOS) attacks.

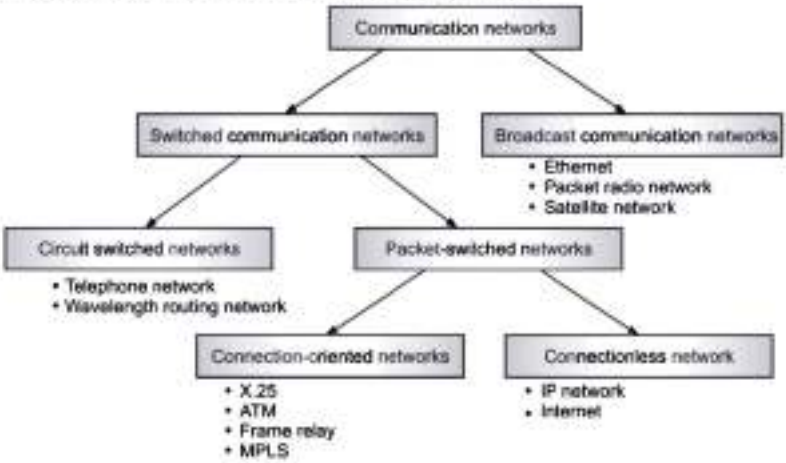


Fig. 1.29: Types of Communication Networks

- An attacking system will send many requests for establishing a connection but then will never complete the connection. The attacked computer is then left with resources allocated for many never-completed connections. Then, when an end node tries to complete an actual connection, there are not enough resources for the valid connection.
- **Data Transfer:** The data transfer phase occurs when the actual data is transmitted over the connection. During data transfer, most connection-oriented services will monitor for lost packets and handle resending them.
- **Connection Termination:** The protocol is generally also responsible for putting the packets in the right sequence before passing the data up the protocol stack. When the transfer of data is complete, the end nodes terminate the connection and release resources reserved for the connection.
- **Session connection:** A Connection-oriented service requires a session connection be established before any data can be sent with a direct physical connection between the sessions. This often considered being a more reliable network service than the alternative connectionless service.

Advantages:

1. These services provide guarantee delivery of data.
2. This service is more reliable then connectionless services.
3. Some connection oriented services will monitor for lost packets and handle resending them.

Disadvantages:

1. A connection must require.
2. These services have more overhead than connectionless service.
3. Complex method for data transferring.

1.7.3.2 Connectionless Services

- It does not require a session connection between sender and receiver.
- The sender simply starts sending packets, (called datagrams) to the destination. TCP(Transmission Control Protocol) is a connection-oriented transport protocol.
- While UDP(User Datagram Protocol) is a connectionless network protocol. Neither system must maintain state information for the systems that they send transmission to or receive transmission from.
- A connectionless network provides minimal services.
- Connection-oriented methods may be implemented in the data link layers of the protocol stack and/or in the transport layers of the protocol stack, depending on the physical connections in place and the services required by the systems that are communicating.
- This service does not have the reliability of the connection-oriented method, but it is useful for periodic burst transfers. Both operate over IP.
- The physical, data link, and network layer protocols have been used to implement guaranteed data delivery. For example, X.25 packet-switching networks perform extensive error checking and packet acknowledgment because the services were originally implemented on poor-quality telephone connections.
- Today, networks are more reliable. It is generally believed that the underlying network should do what it does best, which is deliver data bits as quickly as possible.
- Therefore, connection-oriented services are now primarily handled in the transport layer by end systems, not the network. This allows lower-layer networks to be optimized for speed.
- LANs operate as connectionless systems. A computer attached to a network can start transmitting frames as soon as it has access to the network.
- It does not need to set up a connection with the destination system ahead of time. However, a transport-level protocol such as TCP may set up a connection-oriented session when necessary.

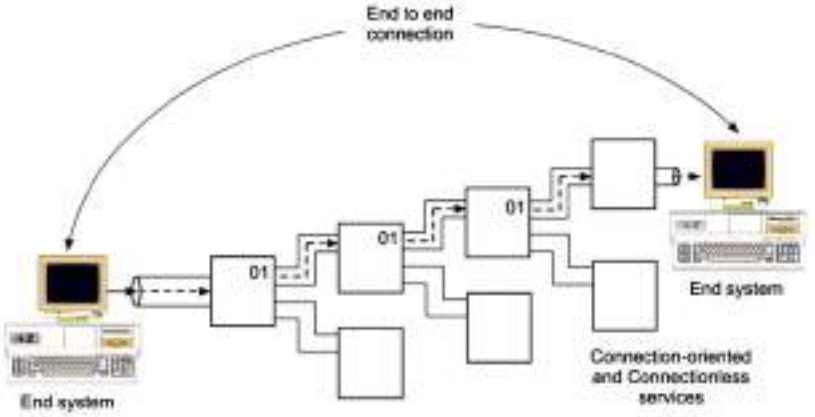


Fig. 1.30: Connection Services

- The Internet is one big connectionless packet network in which all packets delivers are handled by IP.
- However, TCP adds connection-oriented services on top of IP. TCP provides all the upper-level connection-oriented session requirements to ensure that data is delivered properly.
- MPLS is a relatively new connection-oriented networking scheme for IP networks that sets up fast label-switched paths across routed or layer 2 networks.
- A WAN service that uses the connection-oriented model is frame relay. The service provider sets up PVCs (Permanent Virtual Circuits) through the network as required or requested by the customer.
- ATM is another networking technology that uses the connection-oriented virtual circuit approach.

Advantages:

1. Does not require any connection.
2. These services are very simple and easy for data transfer.
3. Used for periodic burst data transfer.
4. Less overhead then connection oriented services.

Disadvantages:

1. Less reliable than connection-oriented services.
2. No guarantee for delivery of data.
3. It provides minimal services.

Examples of Services:

Table 1.5: Different types of Services and Example

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connectionless	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

- Observe that each layer in the OSI model may offer different kinds of service. Often there is datagram service on the lower layers while e.g. the transport layer offers a reliable message stream.

Service Primitives:

- A service is formally specified by a set of primitives (operations) available to a user process to access the service.

Table 1.6: Service Primitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection.
CONNECT	Establish a connection with a waiting peer.
RECEIVE	Block waiting for an incoming message.
SEND	Send a message to the peer.
DISCONNECT	Terminate a connection.

Table 1.7: Comparison between Connection-oriented and Connectionless services

Sr. No.	Connection-oriented Service	Connectionless Services
1.	Connection-oriented services must first establish a connection with the desired service before passing any data.	A connectionless service can send the data without any need to establish a connection first.
2.	Connection - oriented services provide some level of delivery guarantee.	Connectionless services do not provide some level of delivery guarantee.

Contd..

3.	Connection-oriented network services have more overhead.	Connectionless network have less overhead.
4.	TCP (Transmission Control Protocol) is a connection-oriented transport protocol.	While UDP (User Datagram Protocol) is a connectionless network protocol.
5.	This method is often called a "reliable" network service.	This service does not have the reliability of the connection-oriented method, but it is useful for periodic burst transfers.
6.	Examples: MPLS is a relatively new connection - oriented networking scheme for IP networks that sets up fast label-switched paths across routed or layer 2 networks. A WAN service that uses the connection-oriented model is frame relay. ATM is another networking technology that uses the connection-oriented virtual circuit approach.	Examples: LANs operate as connectionless systems. The Internet is one big connectionless packet network in which all packet deliveries are handled by IP.

Summary

- Computer network is a set or collection of computing devices that are linked to each other in order to communicate and share their resources with each other.
- The interconnected computers can share resources, which called networking.
- Computer network is divided into wired and wireless network. A wired network is simply a collection of two or more computers, printers, and other computing devices linked by cables like Ethernet, coaxial cables. A wireless network, which uses high-frequency radio waves or micro wave rather than wires to communicate between nodes.
- Nowadays, computer networks have become an essential part of industry, entertainment world, business as well as our daily lives. Some of the applications of computer network in different fields are: Business applications, Home applications and Mobile application.
- Remote access is the ability to get access to a computer or a network from a remote distance. For example, Home users get access to the Internet through remote access to an Internet Service Provider (ISP).
- Transmission Technology refers how two devices are connected and how they are communicating.

- The transmission technology can be categorized broadly into two types i.e. Point-to-Point networks and Broadcast networks (multipoint).
- Communication between two directly interconnected devices is referred to as point-to-point communication.
- Point-to-point networks consist of many connections between individual pairs of computers or machines.
- Point-to-point transmission with one sender and one receiver is sometime called unicasting.
- The networks having multipoint configuration are called Broadcast Networks.
- A collection of interconnected networks is called an internetwork or internet. The Internet is a global network connecting millions of computers.
- Network topology defines the geographic arrangement of computer networking devices.
- Topology defines the physical (describes the placement of network nodes and the physical connections between them) or logical (the paths that take messages to get from one place on the network to another place) arrangement of links in a network.
- Network topology is defined as, "the physical interconnection between various elements on computer network, such as links and nodes".
- There are number of different network topologies in networking like star, ring, mesh, tree, bus etc.
- In bus topology, all nodes are connected to a central cable which is called a bus. This bus is also called as a Trunk or sometimes it was also referred to as Backbone cable.
- In ring topology, the computers in the network are connected in a circular fashion which forms of a ring.
- In star topology all the cables run from the computers to a central location, where they are all connected by a device called a hub/switch.
- Computer networks fall into three classes regarding the size, distance and the structure namely LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).
- Local Area Network (LAN) is a privately-owned network covering a small geographic area (10 m to 1 km), like a home, office, building or group of buildings (For example: campus).
- Metropolitan Area Network (MAN) covers a larger geographical area than a LAN (1 km to 10 km), ranging from several blocks of buildings to entire cities.
- Wide Area Networks (WAN) covers a large geographical area (100 km to 1000 km), often a country. IT can be divided into three main categories system interconnection (connecting the components of computer using short range radio like Bluetooth.

7. Communication channel is shared by all the machines on the network in _____.
   (a) broadcast network (b) unicast network
   (c) multicast network (d) none of the mentioned
8. _____ is the technology that connects the machines and people within a site in a small area .
   (a) LAN (b) MAN
   (c) WAN (d) None of these
9. _____ is a network that covers geographic areas that are larger, such as districts or cities.
   (a) LAN (b) MAN
   (c) WAN (d) None of these

ANSWERS

(1) a	(2) c	(3) b	(4) b	(5) c	(6) c	(7) a
(8) a	(9) b					

Practice Questions

Q.I Answer the following questions in short.

1. Define Computer Network.
2. How are networks classified?
3. State applications of computer networks.
4. Enlist various advantages and disadvantages of network.
5. What is topology?
6. What is Protocol?
7. What are the modes of communications? Explain with example.

Q.II Answer the following questions.

1. What is Computer Network? What are its goals?
2. Define topology. Explain any one topology with its advantages and disadvantages.
3. Write a note on point-to-point and broadcast transmission.
4. What are the applications of computer networks?
5. How are networks classified?
6. What is an internetwork? Explain its structure in brief.
7. Write a short note on: (a) WAN, and (b) MAN.
8. What are standards? What is their need? What are the two types of standards?
9. Define protocol.

10. Compare WAN and MAN.
11. Compare peer-to-peer LAN and server-based LAN.
12. With suitable diagram describe network components
13. Explain the layered network model. What are the advantages?
14. Explain different types of LAN? How do they differ in functionality?
15. Explain the classification of services. Also explain them.
16. Explain the relationship between services and protocol.
17. What are the types of topologies?

Q.III Define the following terms:

1. LAN
2. Communication Modes
3. Network Components
4. Peers
5. Interfaces
6. Network software
7. Wireless Network

Previous Exams Questions

Summer 2018

1. Define network topology. List different types of topologies. Explain any one in detail. **5 M**

Ans. Please refer to section 1.2.

2. What are different modes of communication? Explain any one in detail. **5 M**

Ans. Please refer to section 1.4.

3. Write a note on protocols and standards. **5 M**

Ans. Please refer to section 1.6.

Winter 2018

1. Define Network Topology. List different types of Topologies. Explain any one in detail. **5 M**

Ans. Please refer to section 1.2.

2. Explain different components of LAN. **5 M**

Ans. Please refer to section 1.3.1.1.

3. Define Computer Network. Explain goals of Computer Network. **5 M**

Ans. Please refer to section 1.1.

4. Explain server based and peer to peer LAN's. **5 M**

Ans. Please refer to section 1.5.

5. What are different modes of communication? Explain any one. **5 M**

Ans. Please refer to section 1.4.

6. Write a note on protocols and standards. **5 M**

Ans. Please refer to section 1.6.

7. Write note on: SAP. **5 M**

Ans. Please refer to section 1.7.2.

Summer 2019

1. Compare connection oriented and connectionless Network Models. **5 M**

Ans. Refer to section 1.7.3.

2. Explain Server Based and Peer-To-Peer LANs. **5 M**

Ans. Refer to section 1.5.3.

3. Define Computer Networks. Explain goals of Computer Networks. **5 M**

Ans. Refer to section 1.1.

4. Write short notes on:

(a) Modes of communication **5 M**

Ans. Refer to section 1.4.

(b) Intranet and Extranet **5 M**

Ans. Refer to section 1.3.4.

❖❖❖

2... Network Models

Objectives...

- To learn about OSI and TCP/IP reference Models
- To study TCP/IP Protocol Suite
- To get information about IP addressing

2.1 NETWORK MODELS

- A Network Model reflects a design or architecture to accomplish communication between different systems. Network models are also referred to as network stacks or protocol suites. Examples of network models includes TCP/IP, Sequenced Packet Exchange/Internet Packet Exchange (SPX/ IPX) used by Novell Netware, the Network Basic Input Output System (Net-BIOS), which comprises the building blocks for most Microsoft networking and network applications; and AppleTalk, the network model for Apple Macintosh computers.
- A network model usually consists of layers. Each layer of a model represents specific functionality. Within the layers of a model, there are usually protocols specified to implement specific tasks. You may think of a protocol as a set of rules or a language. Thus, a layer is normally a collection of protocols.
- There are several different network models depending on what organization or company started them. The most important two models are:
  1. **OSI Network Model:** The International Standards Organization (ISO) has defined a standard called the International Organization for Standardization/Open System Interconnection Reference Model (ISO/ OSI-RM, or more simply, OSI-RM). This is a seven layer architecture explained in the next section. This model dominated data communication and networking literature before 1990. The OSI model was never fully implemented.
  2. **TCP/IP Model:** It is also called the Internet Model because TCP/IP is the protocol used on the internet. The TCP/IP protocol suite became the dominant commercial architecture because it was used and tested extensively in the Internet.

2.2 OSI REFERENCE MODEL

- The International Organization for Standardization (ISO) is a worldwide body that promotes standards internationally. ISO-OSI describes the architecture, protocols and services that are needed to achieve this goal. There are multiple ISO-OSI standards. Some of these are complete, while others are still evolving.
- The term open system in ISO-OSI defines a computer system that can communicate with another computer system using the OSI protocol.

Fig. 2.1: The ISO-OSI Reference Model

- Each layer in the ISO-OSI Reference Model has a name, a number, protocols that provide specific functions, and defined services.
- Because the various intended uses of ISO-OSI are very broad, spanning terminals, personal computers, and very large mainframes, different services and protocol options are available at each layer. This range of support can accommodate different connection requirements and environments.
- Although there are many different architectures, standards and models the ISO-OSI Reference Model is mostly used to explain the different functions implemented in protocols from different layers and how these protocols work together.
- It is a layered framework for the design of network systems that allows for communication across all types of computer systems.
- Seven layered model, higher layers have more complex tasks. Each layer provides services for the next higher layer. Each layer communicates logically with its associated layer on the other computer.
- Packets are sent from one layer to another in the order of the layers, from top to bottom on the sending computer and then in reverse order on the receiving computer. Each layer performs a unique, generic, and well-defined function.
- Layer boundaries are designed so that the amount of information flowing between any two adjacent layers is minimized. This is accomplished by having each layer within an open system use the services provided by the layer below. Conversely, each layer provides a sufficient number of services to the layer immediately above it.

2.2.1 Layers in the OSI Model

(S-18,19; W-18)

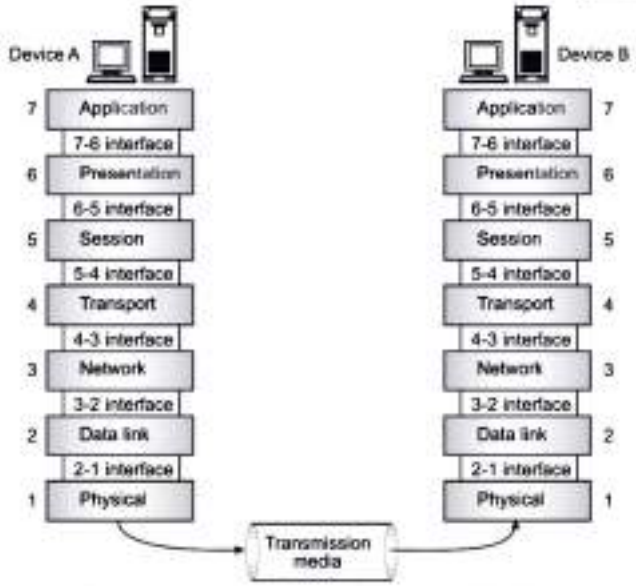


Fig. 2.2: Layered Architecture of the ISO-OSI Model

- Each interface defines what information and services a layer must provide for the layer above it. Layers 1, 2, and 3 are the network support layers; they deal with physical aspect of moving data from one device to another (such as electrical specification, physical connection). Layer 4 ensures end-to-end reliable data transmission. Layers 5, 6, and 7 are user support layers.
- The upper OSI layers are almost always implemented by software; lower layers are a combination of hardware and software, except physical layer, which is mostly hardware.
- This layered approach was selected as a basis for the OSI Reference Model to provide flexibility and open-ended capability through defined interfaces.
- The interfaces permit some layers to be changed while leaving other layers unchanged. In principle, as long as standard interfaces to the adjacent layers are adhered to, an implementation can still work.
- For example, a system implementation could use either HDLC or local area network protocols as the data link layer. Similarly, a particular layer such as the presentation layer can be implemented as a null layer for the time being.

- This means the layer is functionally empty, providing only the mandatory interfaces between the upper and lower layers (application and session layers respectively).

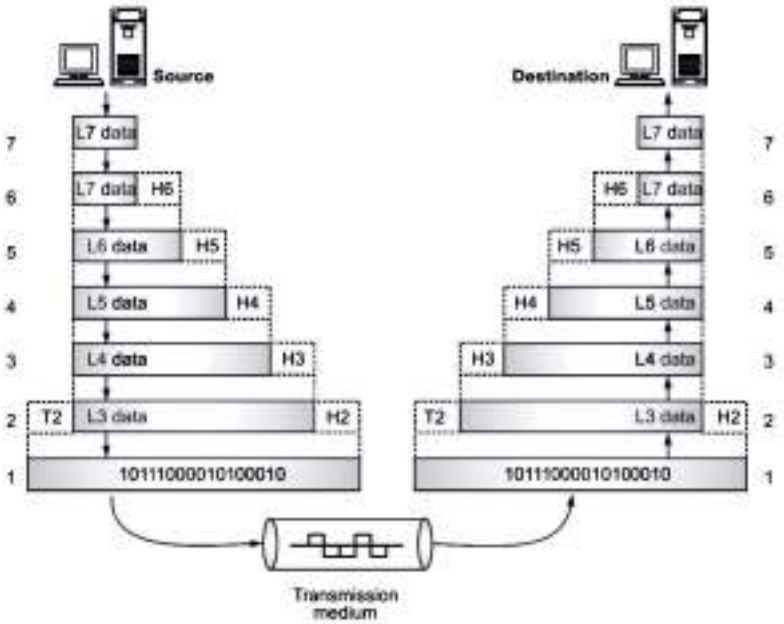


Fig. 2.3: Data Exchange using OSI Model

2.2.2 Functions of Each Layer

- In this section, we will discuss the functions of each layer in the OSI model.

1. **Physical Layer:**
   - The **Physical Layer** is the lowest layer (1st) of the OSI model.
   - Physical layer deals with the mechanical and electrical specifications of the interface and transmission medium.
   - Transmits the unstructured raw bit stream over a physical medium.
   - Relates the electrical, optical mechanical and functional interfaces to the cable.
   - Physical layer also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
   - Defines data encoding and bit synchronization.

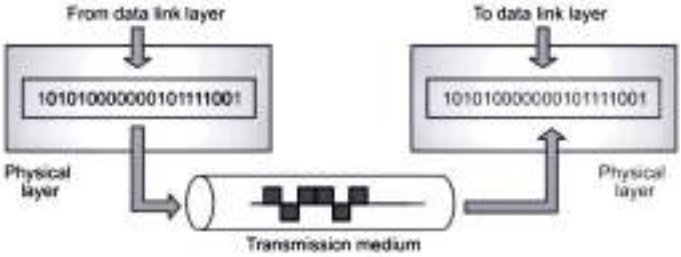


Fig. 2.4: Physical Layer

Responsibilities or functions of the Physical Layer:

(i) **Physical characteristics of Interfaces and Medium:** Physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

(ii) **Representation of Bits (Data Encoding):** Data consist of a stream of bits (0's and 1's). Any transmission medium doesn't understand about computer data i.e. 0 and 1, it understands only about signal. Physical layer converts binary data into signals and vice versa. To be transmitted, bits must be encoded into signals- electrical or optical. The physical layer defines the different types of encoding methods.

(iii) **Data rate:** The transmission rate i.e. the number of bits sent per second.

(iv) **Synchronization of bits:** The sender and receiver must use the same bit rate as well as must be synchronized at the bit level. The sender and receiver clocks must be synchronized.

(v) **Physical Topology:** It defines how devices are connected to make a network. For example, a *star topology* (devices are connected through a central device), a *ring topology* (every device is connected to the next).

(vi) **Transmission mode:** It defines the way in which the data flows between the two connected devices. The various transmission modes possible are simplex, half-duplex and full-duplex.

2. **Data Link Layer:**
   - The 2nd layer of the OSI model is the Data link layer.
   - It makes the physical layer appear error free to the upper layer.
   - Sends data frames from the Network layer to the Physical layer.
   - Packages raw bits into frames for the Network layer at the receiving end.
   - Responsible for providing error free transmission of frames through the Physical layer.

- This layer is often divided into two parts:

(i) **Media Access Control (MAC):** The MAC sub layer controls the means by which multiple devices share the same media channel. This includes contention methods and other media access details. The MAC layer also provides addressing information for communication between network devices.

(ii) **Logical Link Control (LLC):** The LLC sub layer establishes and maintains links between communicating devices.

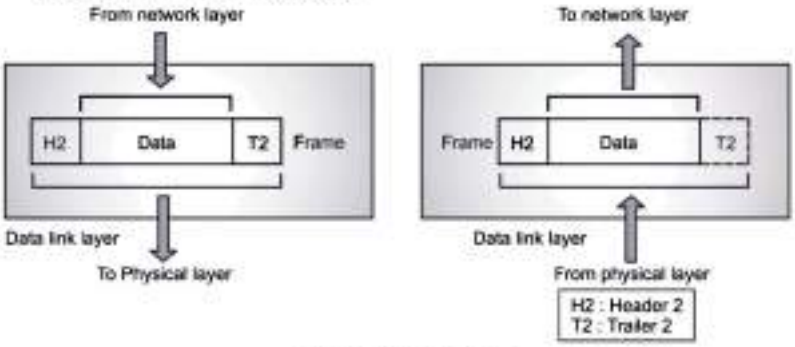


Fig. 2.5: Data Link Layer

Responsibilities or Functions of the Data Link Layer:

(i) **Framing:** The data link layer divides the stream of bits received from the network layer into manageable data units called frames. Data link layer performs various framing functions like Frame Traffic Control, Frame Sequencing, Frame Delimiting and so on.

(ii) **Physical addressing:** If frames are distributed to different system on the network, the data link layer adds header to the frame to define the physical address of the sender (source address) and receiver address (destination address) of the frame. If the frame is intended for the system outside the sender's network, the receiver address is the address of device that connects one network to the next.

(iii) **Flow control:** Flow control is the traffic regulatory mechanism implemented by Data Link layer. If the rate at which the data are absorbed by receiver is less than the rate produced in the sender, the data link layer imposes a flow control mechanism.

(iv) **Error control:** It adds reliability to the physical layer by adding mechanism to detect and retransmit damaged or lost frames. It also prevents duplication of frames.

(v) **Access control:** When two or more devices are connected to the same link, data link layer protocols determine which device has control over the link at any given time.

3. Network Layer:

- The 3rd layer of the OSI model is the Network Layer.
- The network layer is responsible for the source-to-destination delivery of a packet possibly across multiple networks (links). Whereas, the data link layer oversees the delivery of the packet between two systems on the same network (links). If two systems are connected to the same link, there is usually no need for a network layer.

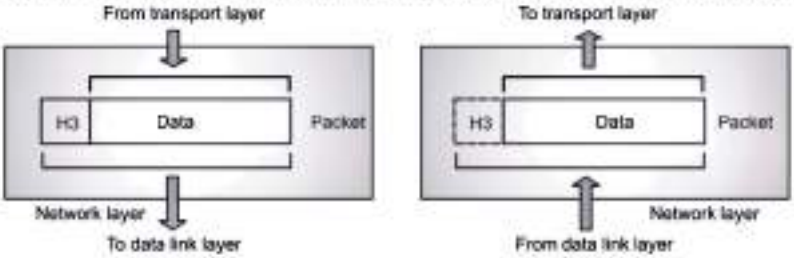


Fig. 2.6: Network Layer

Responsibilities or Functions of Network Layer:

(i) **Logical addressing:** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, then need of another addressing system to help to distinguish the source and destination systems.

(ii) **Routing:** When independent networks or links are connected together to create an internetwork (a network of networks), the connecting devices (called router or gateway) route the packets to their final destination.

(iii) **Congestion Control:** This layer is also responsible for handling the congestion problem at the node, when there are too many packets stored at the node to be forwarded to the next node.

(iv) **Internetworking:** One of the main responsibilities of network layer is to provide internetworking between different networks. It provides logical connection between different types of network.

4. Transport Layer:

- The 4th layer of the OSI model is the Transport Layer.
- The transport layer is responsible for source-to-destination, (end-to-end) delivery of the entire message.

- Network layer treats each packet independently, as though each packet belonged to a separate message, whether or not it does.

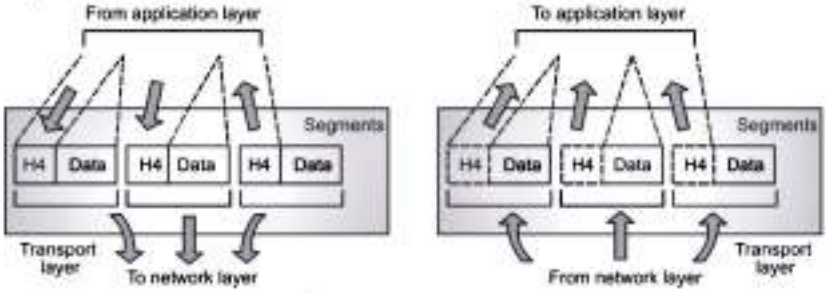


Fig. 2.7: Transport Layer

- Whereas, the transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the Source-to-destination level.

Responsibilities or Functions of the Transport Layer:

(i) **Service-point Addressing (Port Addressing):** Computers often run multiple programs at the same time.

- Source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on the other. The transport layer header therefore must include a type of address called a Service-point address (or port address).
- Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process on destination machine.

(ii) **Segmentation and Reassembly:** A message is divided into transmittable segments, each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in the transmission.

(iii) **Connection control:** It creates a connection between the two end ports. A connection is a single logical path between the source and destination that is associated with all packets in a message. The transport layer can provide connection oriented or connectionless services for connection control.

- A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination.
- A connection oriented transport layer makes a connection with destination transport layer first and then delivers data. After all data transfer is done, the connection is terminated.

(iv) **Flow control:** Transport layer makes sure that the sender and receiver communicate at the rate they both can handle. Flow control at this level is performed end to end rather than across a single link.

(v) **Error control:** Error control at this level is performed end to end. The transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss or duplication).

5. Session layer:

- The 5th layer of the OSI model is the Session Layer.
- Session layer has the primary responsibility of beginning, maintaining and ending the communication between two devices, which is called Session.
- It also provides for orderly communication between devices by regulating the flow of data.
- The session layer is the network *dialog controller*. It establishes, maintains, and synchronizes the interaction between communicating systems.

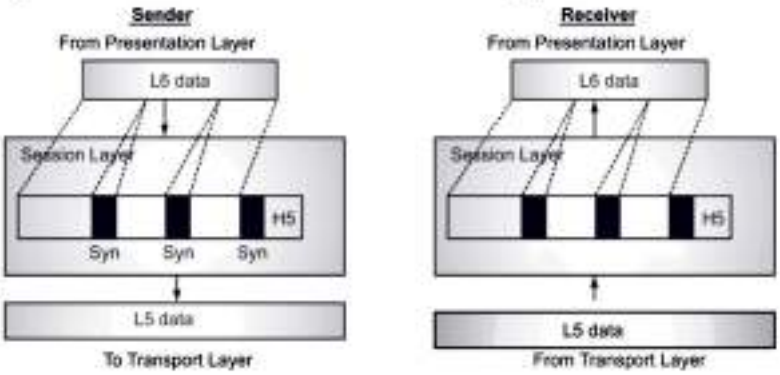


Fig. 2.8: Session Layer

- Above figure shows the relationship of the Session layer to the transport layer and presentation layer.

Responsibilities of the Session Layer:

(i) **Dialog control:** Dialog control is the function of session layer that determines which device will communicate first and the amount of data that will be sent. It also decides the communication between two processes to take place in either half duplex or full duplex mode.

(ii) **Token management:** Preventing two parties from attempting the same critical operation at the same time.

(iii) **Synchronization:** It allows a process to add checkpoints (synchronization points) into a stream of data. Use of checkpoints for long transmission allows them to continue from where they were after a crash.

For example, if a system sending a file of 2000 pages and process inserts checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. If crash happens during transmission of page 545, retransmission begins at page 501; pages 1 to 500 need not be retransmitted.

6. Presentation Layer:

- The 6th layer of the OSI model is the presentation layer. Presentation Layer is also called Translation layer.
- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. The presentation layer is concerned with the representation of user or system data. This includes necessary conversions, (For example, printer control characters) and code translation (For example, ASCII to or EBCDIC).

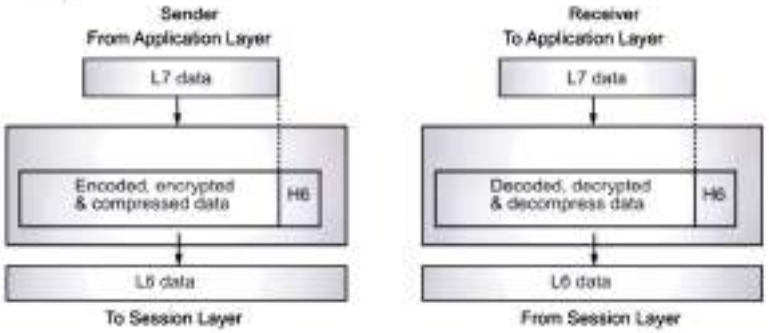


Fig. 2.9: Presentation Layer

Responsibilities or functions of the Presentation layer:

(i) **Translations:** Different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependant format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependant format.

(ii) **Encryption:** Converting computer data into non-readable form is encryption. It is required for important data transmission. Decryption reverses the original process to transform the message back to its original form.

(iii) **Compression:** Reduces the number of bits to be transmitted. Saves network bandwidth. Data compression becomes particularly important in the transmission of multimedia such as text, audio and video.

7. **Application Layer:**

- The 7th layer of the OSI model is the Application Layer.
- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as e-mail, remote file access and transfer, shared database management and other types of distributed information services. Application layer is responsible for providing services to the user.

Services provided by the Application Layer:

(i) **Network Virtual Terminal (NVT):** A network virtual terminal is a software version of a physical terminal and it allows a user to log onto a remote host. The remote host believes it is communicating with one of its own terminal and allows the user to log on.

(ii) **File Transfer, Access and Management (FTAM):** This application layer protocol allows a user to access files in remote computer (to make changes or read data), to retrieve files from a remote computer and to manage or control files in a remote computer.

(iii) **Mail services:** This application provides the basis for e-mail forwarding and storage.

(iv) **HTTP (HyperText Transfer Protocol):** A standard Internet protocol that specifies the client/server interaction processes between Web browsers such as Microsoft Internet Explorer and Web servers such as Microsoft Internet Information Services (IIS).

2.2.3 Summary of ISO-OSI Layer Functions

Table 2.1: Summary of ISO-OSI Model Layers

OSI Layers	Functions
APPLICATION Message/data	Service advertisement, service availability. Manages communications between applications. (FPDAM) File, Print, Database, Application, and Messaging services. Allows applications to use the network. Handles network access, flow control and error recovery.

Contd..

PRESENTATION Message/data	Translation, compression, encryption, data conversion. Translates data into a form usable by the application layer. The redirector operates here. Responsible for protocol conversion, translating and encrypting data, and managing data compression.
SESSION Message/data RPC (Remote Procedure calls) functions here.	Connection establishment, data transfer, connection release (Half-duplex, Full- duplex, Simplex). Allows applications on connecting systems to establish a session. Provides synchronization between communicating computers.
TRANSPORT Segments (or Datagrams)	Service addressing, segmentation and transport control, flow control, end-to-end data integrity. Responsible for packet handling. Ensures error-free delivery. Repackages messages, divides messages into smaller packets and controls error handling.
NETWORK Packets (or Datagrams)	Logical addressing, switching, routing, network control. Translates system names into addresses. Determines routes for sending data and manages network traffic problems, packet switching, routing, data congestion and reassembling data.
DATA LINK Frames	Sends data from network layer to physical layer. Manages physical layer communications between connecting systems. LLC Layer (Logical Link Control): flow control and timing (802.2). Manages link control and defines SAPs (Service Access Points). MAC Layer (Media Access Control): framing and physical addressing (802.3, 802.4, 802.5, 802.12). Communicates with adapter card.
PHYSICAL Bits is concerned with definition of low level functions (voltage, media types)	Transmits data over a physical medium. Defines cables, cards and physical aspects as well as electrical properties, transmission media, transmission devices, physical topology, data signaling, data synchronization and data bandwidth. Manages data placement on and data removal from the network media.

2.3 TCP/IP REFERENCE MODEL W-18

- The TCP/IP Reference Model is sometimes called the *Internet Reference Model* or the *DoD Model*. The TCP/IP model or Internet Protocol Suite, describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network.

- TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. Protocols exist for a variety of different types of communication services between computers.

2.3.1 What is TCP/IP ?

- The name TCP/IP refers to a suite of data communication protocols. Its name comes from two of the more important protocols in the suite: the *Transmission Control Protocol (TCP)* and the *Internet Protocol (IP)*.
- TCP/IP originated out of the investigative research into networking protocols that the Department of Defense (DoD) initiated in 1969. In 1968, the DoD Advanced Research Projects Agency (ARPA) began researching the network technology that is now called *packet switching*.
- The original focus of this research was to facilitate communication among the DoD community. However, the network that was initially constructed as a result of this research then called ARPANET, gradually became known as the Internet.
- The TCP/IP protocols played an important role in the development of the Internet. In the early 1980s, the TCP/IP protocols were developed. In 1983, they became standard protocols for ARPANET.
- Because of the history of the TCP/IP protocol suite, it is often referred to as the **DoD protocol suite** or the **Internet Protocol Suite**.
- It is built into UNIX, and is available for most other operating systems.
- TCP/IP is not one protocol, but is a suite of many protocols. The protocols define applications, transport controls, networking, routing, and network management. It is today's most widely used multivendor interoperability protocol. (The other major multivendor interoperability protocol, OSI, is not yet completely defined and not widely used.)
- TCP/IP is a routable protocol that is suitable for connecting dissimilar systems (such as Microsoft Windows and UNIX) in heterogeneous networks, and it is the protocol of the worldwide network known as the Internet.

2.3.2 Layers of TCP/IP Model

- TCP/IP Model contains following Layers:

1. **Application Layer:**

- The top layer in the Internet reference model is the *application layer*. This layer provides functions for users or their programs, and it is highly specific to the application being performed.
- It provides the services that user applications use to communicate over the network, and it is the layer in which user-access network processes reside.

- These processes include all of those that users interact with directly, as well as other processes of which the users are not aware.
- This layer includes all applications protocols that use the host-to-host transport protocols to deliver data. Other functions that process user data, such as data encryption and decryption and compression and decompression, can also reside at the application layer.
- The application layer also manages the sessions, (connections) between cooperating applications.
- In the TCP/IP protocol hierarchy, sessions are not identifiable as a separate layer, and these functions are performed by the host-to-host transport layer.
- Instead of using the term "session," TCP/IP uses the terms "socket" and "port" to describe the path (or virtual circuit) over which cooperating applications communicate.
- Most of the application protocols in this layer provide user services, and new user services are added often.
- For cooperating applications to be able to exchange data, they must agree about how data is represented.
- The application layer is responsible for standardizing the presentation of data.

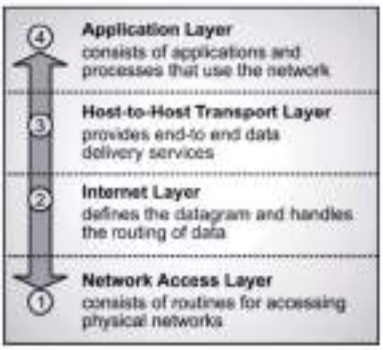


Fig. 2.10: Layers in the TCP/IP Protocol Architecture

2. Host-to-Host Transport Layer:

- The protocol layer just above the internet layer is the *host-to-host transport layer*. It is responsible for providing end-to-end data integrity and provides a highly reliable communication service for entities that want to carry out an extended two-way conversation.
- In addition to the usual transmit and receive functions, the host-to-host transport layer uses *open* and *close* commands to initiate and terminate the connection.

- This layer accepts information to be transmitted as a *stream* of characters, and it returns information to the recipient as a stream.
- The service employs the concept of a connection (or *virtual circuit*). *A connection* is the state of the Host-to-Host transport layer between the time that an open command is accepted by the receiving computer and the time that the close command is issued by either computer.

3. Internet Layer:

- In the Internet reference model, the layer above the network access layer is called the *internetwork layer*.
- This layer is responsible for routing messages through internetworks. Two types of devices are responsible for routing messages between networks.
- The first device is called a *gateway*, which is a computer that has two network adapter cards.
- This computer accepts network packets from one network on one network card and routes those packets to a different network via the second network adapter card. The second device is a *router*, which is a dedicated hardware device that passes packets from one network to a different network.
- The internetwork layer protocols provide a datagram network service. *Datagrams* are packets of information that comprise a header, data, and a trailer. The header contains information, such as the *destination address*, that the network needs to route the datagram.
- A header can also contain other information, such as the *source address* and *security labels*. Trailers typically contain a *checksum value*, which is used to ensure that the data is not modified in transit.
- The communicating entities which can be computers, operating systems, programs, processes or people that use the datagram services must specify the destination address (using control information) and the data for each message to be transmitted.
- The internetwork layer protocols package the message in a datagram and send it off. A datagram service does not support any concept of a session or connection.
- Once, a message is sent or received, the service retains no memory of the entity with which it was communicating. If such a memory is needed, the protocols in the Host-to-Host transport layer maintain it.
- The abilities to retransmit data and check it for errors are minimal or nonexistent in the datagram services. If the receiving datagram service detects a transmission error during transmission using the checksum value of the datagram, it simply ignores, (or drops) the datagram without notifying the receiving higher-layer entity.

4. Network Access Layer:

- The Network Access Layer is the lowest layer in the Internet reference model. This layer contains the protocols that the computer uses to deliver data to the other computers and devices that are attached to the network.
- The protocols at this layer perform three distinct functions:
  1. They define how to use the network to transmit a *frame*, which is the data unit passed across the physical connection.
  2. They exchange data between the computer and the physical network.
  3. They deliver data between two devices on the same network. To deliver data on the local network, the network access layer protocols use the physical addresses of the nodes on the network. A physical address is stored in the network adapter card of a computer or other device, and it is a value that is "hardcoded" into the adapter card by the manufacturer.
- Unlike higher level protocols, the network access layer protocols must understand the details of the underlying physical network, such as the packet structure, maximum frame size, and the physical address scheme that is used. Understanding the details and constraints of the physical network ensures that these protocols can format the data correctly so that it can be transmitted across the network.

2.4 TCP/IP PROTOCOL SUITE

- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having four layers i.e. Host-to-Network, internet, transport, and application.
- However, when TCP/IP is compared to OSI, we can say that the Host-to-Network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer. So in this section, we assume that the TCP/IP protocol suite is made of five layers: Physical, Data Link, Network, Transport and Application.
- The first four layers provide physical standards, network interfaces, internetworking and transport functions that correspond to the first four layers of the OSI model.
- The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the Application Layer as shown in Fig. 2.11.
- TCP/IP is a hierarchical protocol made up of interactive modules with specific functionality. These modules are not interdependent. In OSI model, every layer is having predefined functions. The layers in TCP/IP protocol suite contain relatively

independent protocols that can be mixed and matched depending on the needs of the system. Every upper layer protocol is supported by one or more lower level protocols.

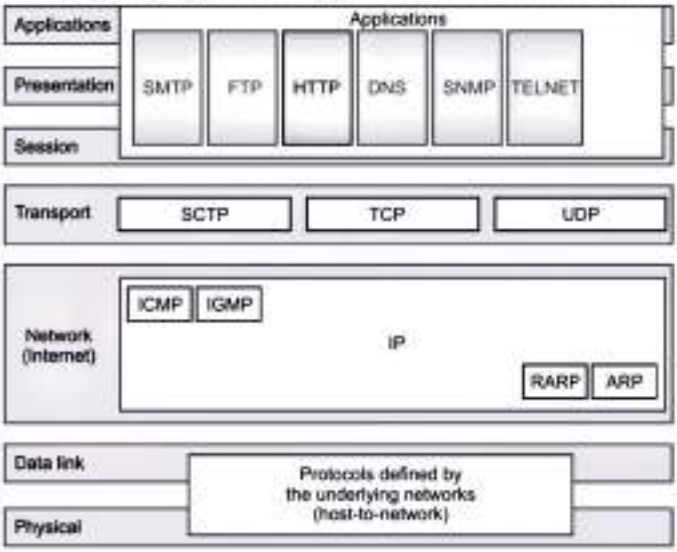


Fig. 2.11: TCP/IP and OSI Model

2.5 COMPARISON OF OSI & TCP/IP REFERENCE MODEL (S-19)

- The OSI and TCP/IP reference models have many things common. Both are based on concept of a stack of independent protocols.
- Functionality of the layers is almost same. The layers above transport are application oriented users of the transport service.
- Despite these fundamental similarities, the two models also have many differences as shown in following table.

Table 2.2: Comparison between ISO-OSI and TCP/IP model

Sr. No.	ISO-OSI Reference Model	TCP/IP Model
1.	7 layer model.	4 layer model.
2.	OSI model is useful in describing networks, but protocols are too general.	TCP/IP model is weak, but protocols are specific and widely used.

Contd...

3.	Model was conceptual, designers didn't know what functionality to put in the layers.	Model is practical, designers knows the functionality of each layer and used in real world network.
4.	Model is general, and easier to replace protocols.	Model is not general, and difficult to replace protocols.
5.	Model had to adjust when networks did not match the service specifications (wireless networks, internetworking).	Model need not require to adjust too much in this scenario.
6.	Model describes any type of network.	Model only describes TCP/IP which is not useful for describing any other networks.
7.	Network layer supports both Connection-oriented and connection-less service.	Network layer supports only connection-less service.
8.	Transport layers supports only connection-oriented service.	Transport layers supports both Connection oriented and connectionless service.

2.6 ADDRESSING (W-18, S-18)

- A network address serves as a unique identifier for a computer on a network.
- When set up correctly, computers can determine the addresses of other computers on the network and use these addresses to send messages to each other.

Levels of Addresses used in TCP/IP protocol:

- In TCP/IP, different levels of addresses are used, (Ref. Fig. 2.12).
  1. Physical Address (Hardware Address or Link Address).
  2. Logical Address (IP Address).
  3. Port Address.
  4. Specific Address

Fig. 2.12: Addresses in TCP/IP

- Physical address is basically a part of data link layer.
- Logical address is a part of network layer.

- Port address is a part of transport layer.
- Specific address is supported by application layer.
- Each address is related to a specific layer in the TCP/IP architecture, as shown in Fig. 2.13.

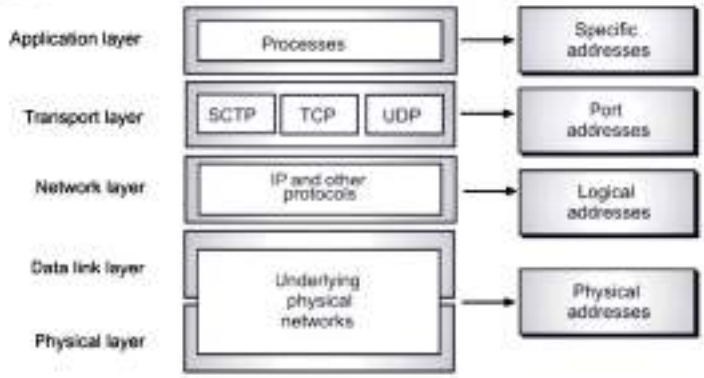


Fig. 2.13: Addresses related to layers in TCP/IP Architecture

2.6.1 Physical Addresses

- The physical addresses also known as the link address. This is the address of the node that defined by its LAN and WAN.
- Data link layer includes this address into data frame.
- Physical address is used when source and destination are from same network. It is lowest level address.
- The physical addresses have authority over the network i.e. LAN or WAN. The address size and format depend on the network.
- For example, Ethernet uses 6 byte (48 bit) physical address which is imprinted on the network interface card (LAN card).

Example:

- In Fig. 2.14, a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link i.e., bus topology LAN.
- At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection.
- Fig. 2.14 shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver. The data link layer at the sender

receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses.

Fig. 2.14: Physical Addresses

- We have shown a bus topology for an isolated LAN. In a bus topology, the frame is propagated in both directions (left and right).
- The frame propagated to the left dies when it reaches the end of the cable if the cable end is terminated appropriately. The frame propagated to the right is sent to every station on the network. Each stations with physical addresses other than 87 drops the frame because the destination address in the frame does not match its own physical address.
- The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.

Example of Physical Address:

- Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B

2.6.2 Logical Addresses

- The logical addresses also known as the IP address.
- When source and destination are from different networks or in on internetworking environment, physical addresses are not adequate where different networks can have different address format.
- A unique universal addressing system is needed in which every computer can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose.
- Logical addresses in a network model are necessary for universal communications that are independent of underlying physical networks.

- A logical address can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have same IP addresses. Logical addresses are necessary for universal communications.
- An IP addresses is 32 bit address usually written in dotted decimal format A.B.C.D. where each number is in the range 0 to 255. For example, 192.9.100.2.

Example:

- Fig. 2.15 shows a part of an Internet with two routers connecting three LANs.

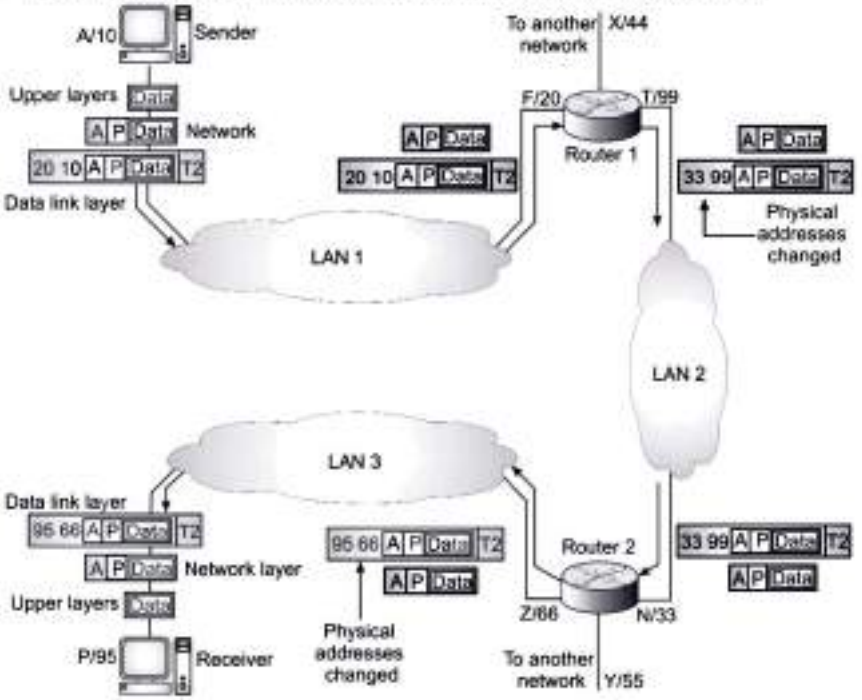


Fig. 2.15: Logical (IP) Addresses

- Each device/node like computer or router has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses.
- Each router, however, is connected to three network models for this reason each router has three pairs of addresses, one for each connection. Although it may obvious that each router must have a separate physical address for each connection, it may not be obvious why it needs a logical address for each connection.

2.6.3 Port Addresses

- The IP address and the physical address in a network model are necessary for a quantity of data to travel from a source host to the destination host.
- However, arrival at the destination host is not the final objective of data communications on the Internet.
- A system that sends nothing but data from one computer to another is not complete.
- Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process.
- For example, computer x can communicate with computer z by using TELNET. At the same time, computer x communicates with computer y by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes. In other words, they need addresses. In the TCP/IP network model architecture, the label assigned to a process is called a Port address.

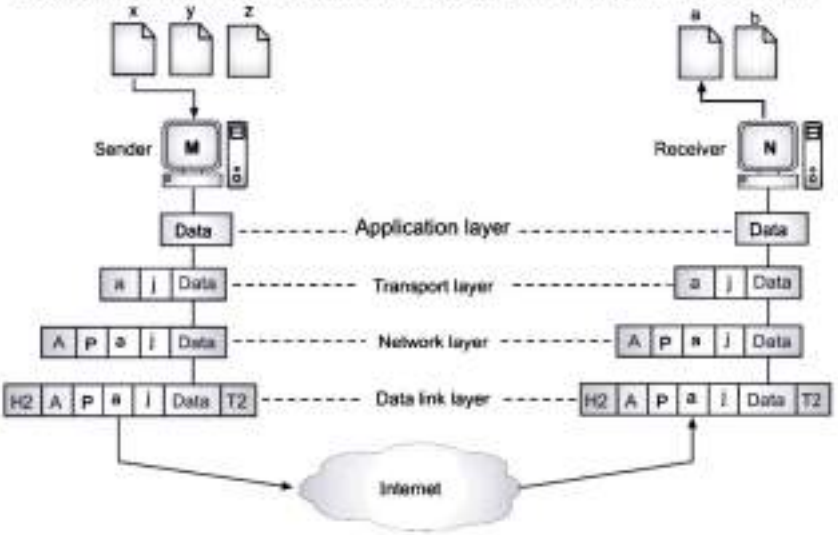


Fig. 2.16: Port Addresses

- A port address in TCP/IP network model is 16 bits in length. For example, A port address is a 16-bit address represented by one decimal number as 753.
- IANA (Internet Assigned Numbers Authority) has divided port numbers into three ranges:
  - (i) **Well Known Ports:** Ports ranging from 0 to 1023 are assigned and controlled by IANA.

(ii) **Registered Ports:** Ports from 1024 to 49,151 can be registered with IANA to prevent duplication.

(iii) **Dynamic Ports:** Ports from 49,152 to 65,535. They can be used by any process.

- In Fig. 2.16, two computers are communicating via Internet are shown. The sender is running three processes with port addresses x, y and z.
- The receiver is running two processes with port addresses a and b. Process 'x' wants to communicate with process 'a'. Both computers are using the same application. Process x's data must be delivered to process a and not b.
- For this, transport layer encapsulates data from the application layer in a packet and adds two port addresses x and a, as source port and destination port addresses.
- The packet is then given to network layer with adds logical addresses M and N and then data link layer adds physical addresses of the next hop. Although physical addresses change from hop to hop, logical and port addresses remain the same.

2.6.4 Specific Addresses

- Addresses are user friendly addresses and are called specific addresses.
- Some applications use friendly addresses that are designed for that specific address. However, this address gets changed according to the required logical and port addresses sent from the sender computer.
- For example, e-mail address and URL, for example: iamheremg@gmail.com, www.educationindia.edu and so on.

2.7 IP ADDRESSING

- An IP address is a binary number that uniquely identifies computers and other devices on a TCP/IP network.
- There are two kinds of IP addresses, public (also called globally unique IP addresses) and private.

1. **Public IP addresses** are assigned by the Internet Assigned Numbers Authority (IANA). The addresses are guaranteed to be globally unique and reachable on the Internet. This assures that multiple computers do not have the same IP address. An Internet service provider (ISP) obtains a range of public IP addresses from IANA, and then the ISP assigns the addresses to customers to use when they connect to the Internet through the ISP.

- Public IP addresses are routable on the Internet, which means that a computer with a public IP address is visible to other computers on the Internet.

2. **Private IP addresses** cannot be used on the Internet. IANA has set aside three blocks of IP addresses that cannot be used on the global Internet. These three blocks of addresses are private IP addresses, and they are used for networks that do not directly connect to the Internet.

- A private IP address is within one of the following blocks or range of addresses:
  - 192.168.0.0/16: This block allows valid IP addresses within the range 192.168.0.1 to 192.168.255.254.
  - 172.16.0.0/12: This block allows valid IP addresses within the range 172.16.0.1 to 172.31.255.254.
  - 10.0.0.0/8: This block allows valid IP addresses within the range 10.0.0.1 to 10.255.255.254.
- Network ID is used to identify the subnet upon which the host resides. The host ID is used to identify the host itself within the given subnet.

Fig. 2.17: IDs of IP Address

Parts of an IP Address:

- Any TCP/IP network will require a unique network number and every host on a TCP/IP network will require a unique IP address. Let us understand how IP addresses are constructed.
- An IP address is a 32-bit number that uniquely identifies a network interface on a machine. IP addresses are typically written in decimal digits, formatted as four 8-bit fields separated by periods. Each 8-bit field represents a byte of the IP address. This form of representing the bytes of an IP address is often referred to as the dotted-decimal format.
- The bytes of an IP address can be further classified into two parts: the **Network part** and the **Host part**. The example below shows the components of the Class B network 192.168.1.100.

Fig. 2.18: Parts of an IP Address

1. **Network Part:**
   This part specifies the unique number assigned to your particular network. It is also the part that identifies the class of network assigned. In the above example, the network part takes up two bytes of the IP address, namely 192.168.
2. **Host Part:**

- This is the part of the IP address that you assign to each host, and uniquely identifies each host on your network. Note that for each host on your network, the network part of the address will be the same, but the host part must be different.

- IP addresses can be displayed in three typical formats:
  - **Binary notation:** Binary notation is the format that systems on the network use to process the address. An example of binary notation is 11000000.10101000.00000001.01100100.
  - **Hexadecimal notation:** Hexadecimal notation is the format typically used when identifying IPv6 addresses. An example of hexadecimal notation of an IPv4 address is C0.A8.01.64
  - **Dotted-decimal notation:** Dotted-decimal notation is the format that is typically used for displaying the IP address in a human-readable format. An example of dotted-decimal notation is 192.168.1.100.
- The IP addressing scheme is integral to the process of routing IP datagrams through an internetwork.

2.7.1 Classful Addresses

- Classful addressing is a concept that divides the available address space of IPv4 into five classes namely A, B, C, D & E. Nowadays, this concept has become obsolete and has been replaced with classless addressing.
- The most complicated part of an IP address is that the division between the network identifier and the host identifier is not always in the same place.
- A hardware address, for example, consists of 3 bytes assigned to the manufacturer of the network adapter and 3 bytes that the manufacturer itself assigns to each card.
- IP addresses can have various numbers of bits assigned to the network identifier, depending on the size of the network.
- The IANA defines several different classes of IP addresses, which provide support for networks of different sizes, as shown in Fig. 2.19 (a).

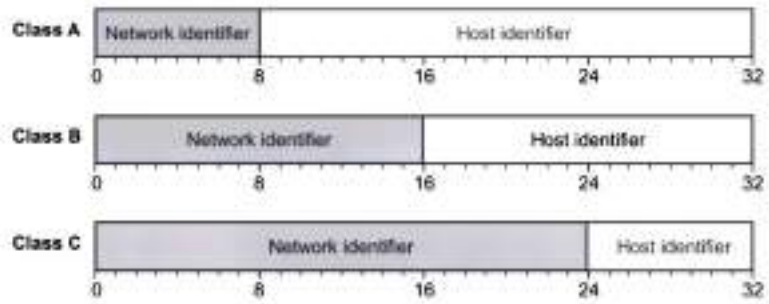


Fig. 2.19 (a): Three Classes of IP addresses with different sized network and host identifiers

Network Addressing and IP Address Classes:

- IP addresses are broken into 4 octets (IPv4) separated by dots called dotted decimal notation. An octet is a byte consisting of 8 bits. The IPv4 addresses are in the following form:

  192.168.10.1

- There are two parts of an IP address:
  - Network ID
  - Host ID
- The various classes of networks specify additional or fewer octets to designate the network ID versus the host ID.

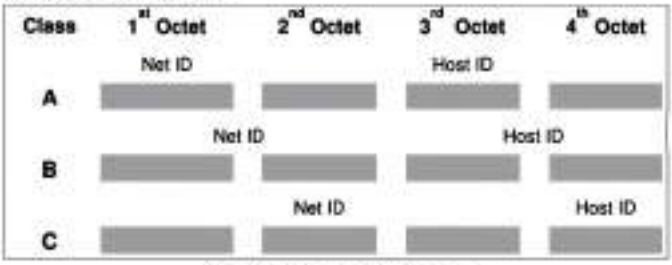


Fig. 2.19 (b): Octets in Classes

- Network address is an address that defines the network itself.
- The addressing scheme for class A through E networks is shown below.

Table 2.3: Addressing Scheme for Classes

Network Type	Address Range	Normal Netmask	Comments
Class A	001.x.x.x to 126.x.x.x	255.0.0.0	For very large networks
Class B	128.1.x.x to 191.254.x.x	255.255.0.0	For medium size networks
Class C	192.0.1.x to 223.255.254.x	255.255.255.0	For small networks
Class D	224.x.x.x to 239.255.255.255		Used to support multicasting
Class E	240.x.x.x to 247.255.255.255		Reserved for future use

Note: We use the 'x' character here to denote 'don't care situations' which includes all possible numbers at the location. It is many times used to denote networks.

1. **Class A Addressing:**

- First byte specifies the network portion (8 bits).
- Remaining bytes specify the host portion (24 bits).

- The highest order bit of the network byte is always 0.
- Network values of 0 and 127 are reserved.
- This class is used for large addressing networks.
- There are 126 Class A networks.
- There are more than 16 million host values for each Class A network.

Fig. 2.20: Class A Addressing

2. Class B Addressing:

- The first two bytes specify the network portion (16 bits).
- The last two bytes specify the host portion (16 bits).
- The highest order bits 6 and 7 of the network portion are 10.
- This class is used for medium sized addressing networks.
- There are more than 16 thousand Class B networks.
- There are 65 thousand nodes in each Class B network.

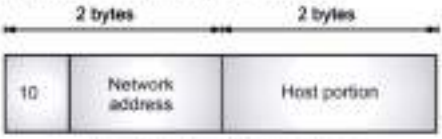


Fig. 2.21: Class B Addressing

3. Class C Addressing:

- The first three bytes specify the network portion (24 bits).
- The last byte specifies the host portion (8 bits).
- The highest order bits 5, 6 and 7 of the network portion are 110.
- This class is used for addressing small sized networks.
- There are more than 2 million Class C networks.
- There are 254 nodes in each Class C network.

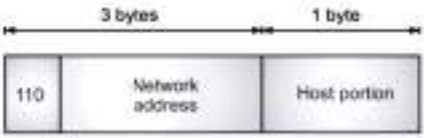


Fig. 2.22: Class C Addressing

4. Class D Addressing:

- Class D address defines a group-ID and used for multicasting.
- Internet authorities have designated some multicast addresses to specific groups.

Fig. 2.23: Class D Addressing

Table 2.4: Categories of Class D addresses.

Address	Group
224.0.0.0	Reserved
224.0.0.1	ALL SYSTEMS on this SUBNET
224.0.0.2	ALL ROUTERS on this SUBNET
224.0.0.4	DVMRP ROUTERS
224.0.0.5	OFPFIGP ALL ROUTERS
224.0.0.6	OSPFIGP Designated ROUTERS
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	RIP2 Routers
224.0.0.10	IGRP Routers
224.0.0.11	Mobile Agents

5. Class E Addressing:

- Fig. 2.24 shows address format of class E addressing.
- This format begins with 1110 that shows it is reversed for the future use.

Fig. 2.24: Class E addressing

Subnetting and Supernetting:

- To overcome the flaws of classful addressing, these two solutions were introduced to compensate for the wastage of addresses. Let us discuss them one by one.

Subnetting:

- IP networks can be divided into smaller networks called subnetworks (or subnets).
- Subnetting is the process of breaking down a main class A, B, or C network into subnets for routing purposes.

- A subnet mask is the same basic thing as a netmask with the only real difference being that you are breaking a larger organizational network into smaller parts, and each smaller section will use a different set of address numbers.
- This will allow network packets to be routed between subnetworks. When subnetting, the number of bits in the subnet mask determines the number of available subnets.
- Two to the power of the number of bits minus two is the number of available subnets.

Number of available subnets = $2^n - 2$ Where, n: Number of bits

- When setting up subnets the following must be determined:
  - Number of segments
  - Hosts per segment.
- Subnetting provides the following advantages:
  - **Network traffic isolation:** There is less network traffic on each subnet.
  - **Simplified Administration:** Networks may be managed independently.
  - **Improved security:** Subnets can isolate internal networks so they are not visible from external networks.

Subnet Masks:

- A 14 bit subnet mask on a class B network only allows 2 node addresses for WAN links. A routing algorithm like OSPF (Open Shortest Path First) must be used for this approach.
- These protocols allow the Variable Length Subnet Masks (VLSM). RIP (Routing Information Protocol) and IGRP (Interior Gateway Routing Protocol) don't support this. Subnet mask information must be transmitted on the update packets for dynamic routing protocols for this to work.
- The router subnet mask is different than the WAN interface subnet mask.
- One network ID is required by each of:
  - Subnet
  - WAN connection.
- One host ID is required by each of:
  - Each NIC on each host.
  - Each router interface.

Types of Subnet Masks:

- **Default:** Fits into a Class A, B, or C network category.
- **Custom:** Used to break a default network such as a Class A, B, or C network into subnets.

Fig. 2.25: Masking Concept

Fig. 2.26: AND Operation

Table 2.5: Default Masks

Class	Mask in Binary	Mask in dotted-decimal
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

(a) Without Subnetting **(b) With Subnetting**

Fig. 2.27: Default mask and Subnet mask

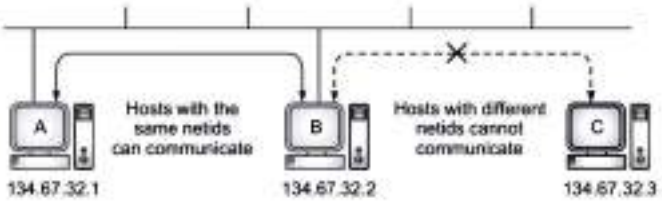


Fig. 2.28: Host Communication on a Local Network

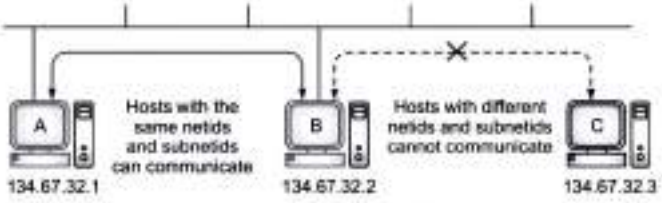


Fig. 2.29: Host Communication with Subnetting

- A subnet is defined by applying a bitmask, the subnet mask, to the IP address. If a bit is on the mask, the equivalent bit in the address is interpreted as a network bit.
- If the bit in the mask is off, the bit belongs to the host part of the address. The subnet is only known locally. To the rest of the Internet, the address is still interpreted as a standard IP address.

Supernetting:

- As the blocks in class A and B were almost consumed so, new organizations consider class C. But, the block of class C is too small then the requirement of the organization. In this case, the solution which came out is supernetting which grants to join the blocks of class C to form a larger block which satisfies the address requirement of the organization.

2.7.2 Classless Addresses

- Classless addressing is a concept of addressing the IPv4 addresses. It was adopted after the failure of classful addressing. The classful addressing leads to wastage of addresses as it assigns a fixed-size block of addresses to the customer. But, the classless addressing assigns a block of addresses to the customer according to its requirement which prevents the wastage of addresses.
- Classless addressing is also called **Classless Inter-Domain Routing (CIDR)**. This addressing type helps to allocate IP addresses more efficiently. When the user requires a particular number of IP addresses, this method assigns a block of IP addresses concerning certain rules. And, this block is called a CIDR block and has the required number of IP addresses.

Properties:

1. Addresses in a block must be in contiguous form.
2. The number of address in a block must be the power of 2 i.e. 2, 4, 8, 16, ...
3. The first address must be evenly divisible by the number of addresses.

Representation:

- In Classless addressing a block, IP address is given like 192.168.10.1/28 (after "/" number of the mask bit is given).
- We can find a mask for the whole block by putting the given after bits out of 32 as 1 and rest of the bits as 0.

- Here, we have 28 bits. So, we need to put 28 bits out of 32 bits as 1 and rest of bits as 0 will give us the mask for the IP address block.

  11111111.11111111.11111111.11100000

  255. 255. 255. 240

  Mask is 255.255.255.240

Important points:

1. To get the first IP address of the block set the rightmost (32 - n) bits to 0s.
2. Last IP address of the block can be found by setting the rightmost bits to 1s.
3. Number of IP addresses of the given block can be found by 232 - n.

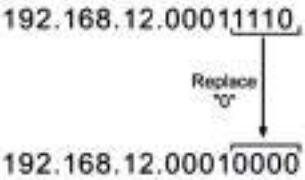
Example:

192.168.12.30/28

Mask value : 255.255.255.240

- In the above example, if we want to find the first address of the given blocks then have to put 0 to set a rightmost bit of the given IP.
- To make it is easy to convert only the last octet into binary and then set 1 or 0 accordingly and rest will remain the same.

  Binary of 30 = 11110



- Hence, the first IP address of the block is 192.168.12.16 (Satisfying Property no. 3).
- Again, to get the last IP address of the block we have to replace all the rightmost bit to 1.
- 192.168.12.00011110
- After replacing all the rightmost bits to 1 we obtain 192.168.12.00011111 i.e. 192.168.12.31.

Table 2.6: Difference between Classful and Classless Addressing

Sr. No	Classful Addressing	Classless Addressing
1.	This alloctes IP addresses according to five major classess.	It is designed to replace classful addressing. It minimizes the rapid exhaustion of IP addresses.
2.	The network ID and host ID changes depending on the classes	There is no boundary on network ID and host ID
3.	Less Practical and useful	More practical and useful

Summary

- A Network Model is a combination of hardware and software that sends data from one location to another.
- The hardware consists of the physical equipment that carries signals from one point of the network model to another. The software consists of instruction sets that make possible the services that we expect from a network model.
- A reference model is a conceptual framework for understanding relationships.
- The International Standards Organization (ISO) has defined a standard called the Open Systems Interconnection (OSI) reference model.
- OSI reference model is a logical framework for standards for the network communication. OSI reference model is now considered as a primary standard for internetworking and inter computing.
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.
- The ISO-OSI model consists of seven layers i.e. Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, and Application Layer.
- Physical layer activates, maintain and deactivate the physical connection. It converts the digital bits into electrical signal.
- Data link layer synchronizes the information which is to be transmitted over the data it also provides error and flow controlling.
- The Network Layer routes the signal through different channels to the other end.
- Transport Layer decides if data transmission should be on parallel path or single path. Functions such as multiplexing, segmenting or splitting on the data done by layer four that is transport layer.
- Session layer manages and synchronize the conversation between two different applications.
- Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data. Languages (syntax) can be different of the two communicating systems.
- Manipulation of data (information) in various ways is done in Application Layer. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc. are services provided by application layer.
- TCP/IP is also called as Internet Model. It has four layers.
- The TCP/IP (Transmission Control Protocol and Internet Protocol) is a set of protocols, or a protocol suite, that defines how all transmission are exchanged across the Internet.
- TCP/IP protocol suite uses four different types of addresses i.e. Physical addresses (also known as the link address, is the address of the node as defined by its LAN and WAN), Logical Addresses (also called as IP address, is a unique universal addressing system is needed in which every computer can be identified uniquely, regardless of

the underlying physical network), Port addresses (a port address is a 16-bit address represented by one decimal number), Specific addresses (user friendly addresses).

- A network address is an identifier for a node or network interface of a computer network. A network address is simply a code used by computers as a means of identification.
- Addressing is the mechanism for identifying senders and receivers, on the network.
- IP address is an address having information about how to reach a specific host, especially outside the LAN.
- Classful and classless addressing are two IP addressing types. The main difference between classful and classless addressing is that classless addressing allows allocating IP addresses more efficiently than classful addressing.

Check Your Understanding

1. Which layer of the OSI reference model corresponds to the IP protocol of the TCP/IP protocol stack ?
   (a) Transport (b) Network
   (c) Internet (d) Data link
2. The entities in the same layer on different machines are called _____.
   (a) hosts (b) peers
   (c) protocols (d) IMP's
3. As the data packet moves from the lower to the upper layers, headers are _____.
   (a) Added (b) Rearranged
   (c) Modified (d) Subtracted
4. Which of the following is a TCP/IP transport layer protocol ?
   (a) IP (b) FTP
   (c) UDP (d) ICMP
5. What is the main function of the transport layer ?
   (a) Process-to-process delivery
   (b) Note-to-node delivery
   (c) Synchronization
   (d) Updating and maintenance of routing tables
6. Which of the following device operates at the network layer of the OSI model ?
   (a) repeater (b) router
   (c) bridge (d) hub
7. The length of an IP address if IPv4 is _____ bits.
   (a) 46 (b) 32
   (c) 16 (d) 64
8. Which of the following is a NOT an Internet layer protocol in the TCP/IP stack ?
   (a) IP (b) UDP
   (c) ARP (d) ICMP
9. The OSI model has ___ layers.
   (a) 4 (b) 5
   (c) 6 (d) 7

10. TCP/IP model does not have _____ layer but OSI model have this layer.
    (a) session layer (b) presentation layer
    (c) application layer (d) both (a) and (b)
11. Which layer links the network support layers and user support layers
    (a) session layer (b) data link layer
    (c) transport layer (d) network layer
12. Which address is used in an internet employing the TCP/IP protocols?
    (a) physical address and logical address
    (b) port address
    (c) specific address
    (d) all of the mentioned
13. TCP/IP model was developed _____ the OSI model.
    (a) prior to (b) after
    (c) simultaneous to (d) none of the mentioned
14. Which layer is responsible for process to process delivery?
    (a) network layer (b) transport layer
    (c) session layer (d) data link layer
15. Which address identifies a process on a host?
    (a) physical address (b) logical address
    (c) port address (d) specific address
16. Which layer provides the services to user?
    (a) application layer (b) session layer
    (c) presentation layer (d) none of the mentioned
17. Transmission data rate is decided by _____.
    (a) network layer (b) physical layer
    (c) data link layer (d) transport layer
18. The physical layer concerns with _____.
    (a) bit-by-bit delivery
    (b) process to process delivery
    (c) application to application delivery
    (d) none of the mentioned

ANSWERS

(1) b	(2) b	(3) d	(4) c	(5) a	(6) b	(7) b
(8) b	(9) d	(10) d	(11) c	(12) d	(13) a	(14) b
(15) c	(16) a	(17) b	(18) a			

Practice Questions

Q.I Answer the following questions in short.

1. What is network model?
2. Write name of addresses used in TCP/IP protocol.

3. Differentiate between physical address and logical address.
4. Which device operates at the network layer of the OSI model?
5. What is subnetting?

Q.II Answer the following questions.

1. Explain functions of each layer ISO-OSI reference model.
2. What is addressing? Explain logical addressing in network.
3. Explain the functions of Transport Layer in OSI-Reference Model.
4. Draw TCP/IP model and state the functions of each layer.
5. Compare OSI and TCP/IP reference Model.
6. Describe protocol hierarchy in brief.
7. What are the similarities available in TCP/IP and OSI model ?
8. Explain classful addressing of TCP/IP model in detail.
9. Explain IP address in detail.

Q.III Define the Terms:

1. Physical address
2. Broadcast address
3. Port address
4. HTTP
5. Framing

Previous Exams Questions

Summer 2018

1. Explain functions of each layer of ISO-OSI reference model. 5 M

Ans. Please refer to section 2.2.1.

2. Explain different types of addresses. 5 M

Ans. Please refer to section 2.6.

Winter 2018

1. Explain functions of each layer ISO-OSI reference model. 5 M

Ans. Please refer to section 2.2.1.

2. Explain different types of addresses. 5 M

Ans. Please refer to section 2.6.

3. Explain TCP/IP protocol in detail. 5 M

Ans. Please refer to section 2.3.

Summer 2019

1. Draw TCP/IP model and state the functions of each layer. 5 M

Ans. Please refer to section 2.2.1.

2. Compare ISO/OSI reference model and TCP/IP. 5 M

Ans. Please refer to section 2.5.

❖❖❖

3... Transmission Media

Objectives...

- To introduce Transmission Media and its types
- To learn about Guided Media such as Twisted Pair Cable, Coaxial Cable, Fiber Optic Cable.
- To study of various Unguided Media such as Wireless Transmission.

3.1 INTRODUCTION

- Computers and other telecommunication devices use signals to represent data. These signals are transmitted from one device to another in the form of electromagnetic energy.
- Electromagnetic signals can travel through a vacuum, air or other transmission media.
- Transmission Medium is used to carry data from the transmitter to the receiver. It is a physical path between sending machine and receiving machine in data communication means it provides a pathway over which the data can travel from sender-to-receiver.
- Each of the messages can be sent in the form of data by converting them into binary digits. These binary digits are then encoded into a signal that can be transmitted over the appropriate medium.
- For example, a copper cable network uses bits as electrical signals while bits in a fiber network are available as light pulses.

3.1.1 Types of Transmission Media

- Transmission media can be divided into two broad categories: Guided (wired) and Unguided (wireless).
- Fig. 3.1 shows types of Transmission Media.

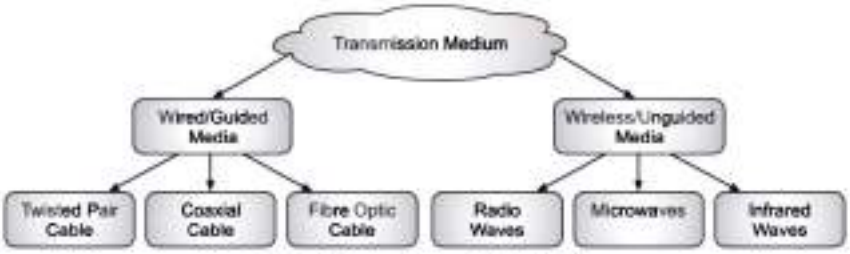


Fig. 3.1: Types of Transmission Media

Types of Transmission Media:

1. Wired or Guided Media or Bound Transmission Media
   - Twisted Pair Cable
   - Coaxial Cable
   - Fiber Optic Cable
2. Wireless or Unguided Media or Unbound Transmission Media
   - Radio Waves
   - Microwaves
   - Infrared Waves

Design factors of Transmission Medium:

- A number of design factors relating to the transmission medium and the signal determine the data rate and distance:
  - **Bandwidth:** All other factors remaining constant, the greater the bandwidth of a signal, the higher the data rate that can be achieved.
  - **Transmission impairments:** Impairments, such as attenuation, limit the distance. For guided media, twisted pair generally suffers more impairment than coaxial cable, which in turn suffers more than Optical fiber.
  - **Interference:** Interference from competing signals in overlapping frequency bands can distort or wipe out a signal. Interference is of particular concern for unguided media but is also a problem with guided media. For guided media, interference can be caused by discharges from nearby cables. For example, twisted pairs are often bundled together and channels often carry multiple cables. Interference can also be experienced from unguided transmissions. Proper shielding of a guided medium can minimize this problem.
  - **Number of receivers:** A guided medium can be used to construct a point-to-point link or a shared link with multiple attachments. In the latter case, each attachment introduces some attenuation and distortion on the line, limiting distance and/or data rate.

3.1.2 Characteristics of Transmission Media

1. **Medium and signal:** Characteristics and Quality determined by medium and signal. For guided (wired), the medium is more important. For unguided (wireless) the bandwidth produced by the antenna is more important.
2. **Data Rate:** Higher data rate needs higher bandwidth. For guided medium, higher data rate needs closer repeaters. For same signal bandwidth, data rate is much lower in unguided media compared to optical fiber or coaxial cable.

3.2 GUIDED MEDIA (W-18)

- Guided media also known as Bounded media.
- Guided transmission media uses a "cabling" system that guides the data signals along a specific path. Cabling is meant in a generic sense in the previous sentences and is not meant to be interpreted as copper wire cabling only.
- Cable is the medium through which information usually moves from one network device to another.

Types:

- There are four basic types of Guided Media are:
  1. Open Wire
  2. Twisted Pair
  3. Coaxial Cable
  4. Fiber-optic Cable

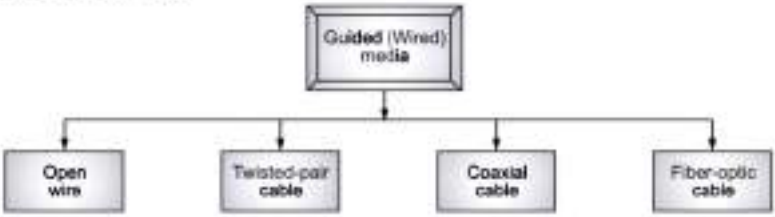


Fig. 3.2: Types of Guided Media

- Twisted Pair cable and Coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a glass or plastic cable that accepts and transports signals in the form of light.

3.2.1 Open Wire

- Open wire is traditionally used to describe the electrical wire strung along power poles.
- There is a single wire strung between poles. No shielding or protection from noise interference is used.

- We are going to extend the traditional definition of Open Wire to include any data signal path without shielding or protection from noise interference. This can include multiconductor cables or single wires.
- This media is susceptible to a large degree of noise and interference and consequently not acceptable for data transmission except for short distances under 20 ft.

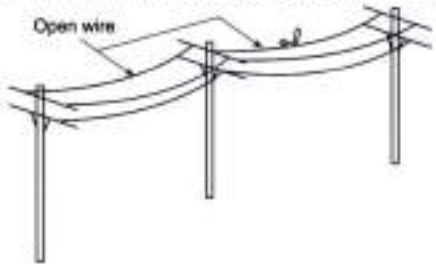


Fig. 3.3: Open Wire

3.2.2 Coaxial Cable

- A form of network cabling used primarily in older Ethernet networks and in electrically noisy industrial environments.
- The name "coax" comes from its two-conductor construction in which the conductors run concentrically with each other along the axis of the cable.
- Coaxial cabling has been largely replaced by twisted-pair cabling for Local Area Network (LAN) installations within buildings, and by fiber-optic cabling for high-speed network backbones.
- Coaxial cable (or coax) carries signals of higher frequency ranges than twisted-pair cable.

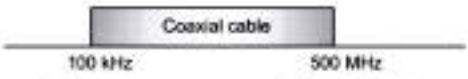


Fig. 3.4: Frequency Range of Coaxial Cable

3.2.2.1 Physical Structure

- Instead of having two wires, coax has a central core conductor of solid or standard wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid or a combination of the two (also usually copper).
- The outer metallic wrapping serves both as a shield against and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

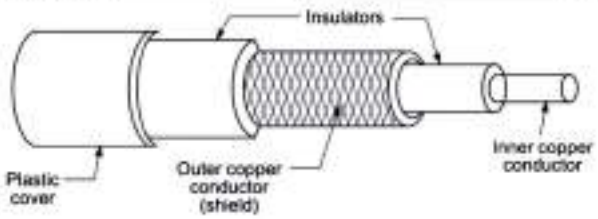


Fig. 3.5: Physical structure of Coaxial Cable

- Shielded concentric construction reduces interference and crosstalk.
- This cable can be used over longer distances and support more stations on a shared line than twisted pair.

3.2.2.2 Categories

- Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable.
- **Radio Government (RG) rating:** Coaxial cables are categorized by Radio Government (RG) rating. Each RG number denotes a unique set of physical specifications, including the wire gauge (gauge is the measure of the thickness of the wire) of the inner conductor, the thickness and type of inner insulator, the construction of the shield, and the size and type of the outer casting.
- Coaxial cabling comes in various types and grades. The most common types are:

1. **Thicknet Cabling:** This is an older form of cabling used for legacy 10Base5 Ethernet backbone installations. This cabling is generally yellow in color and is referred to as RG-8 or N-series cabling. Strictly speaking, only cabling labelled as IEEE 802.3 cabling is true thicknet cabling. RG-9, RG-11 are used in thick Ethernet.

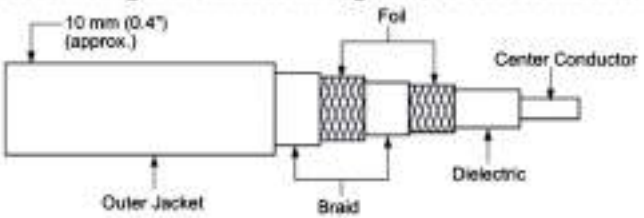


Fig. 3.6: Thicknet Coaxial Cable

2. **Thinnet Coaxial Cabling:** This is used in 10Base2 networks for small Ethernet installations. This grade of coaxial cabling is generally designated as RG-58A/U cabling, which has a stranded conductor and 53-ohm impedance. This kind of cabling uses BNC connectors for connecting to other networking components and must have terminators at free ends to prevent signal bounce.

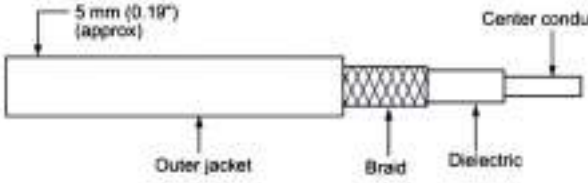


Fig. 3.7: Thinnet Coaxial Cable

3. **ARCNET Cabling:** This uses thin coaxial cabling called RG-62 cabling with an impedance of 93 ohms.
4. **RG-59 Cabling:** This is used for Cable Television (CATV) connections.

3.2.2.3 Advantages and Disadvantages

Advantages:

- Coaxial cable supports both analog and digital signals.
- It has superior frequency characteristics compared to twisted pair.
- It can support higher frequencies and data rates.
- Shielded concentric construction makes it less susceptible to interference and crosstalk than twisted pair.
- Constraints on performance are attenuation, thermal noise and intermodulation noise.
- Requires amplifiers every few kilometers for long distance transmission.
- Usable spectrum for analog signaling up to 500 MHz.
- For both analog and digital transmission, closer spacing is necessary for higher frequencies/data rates.

Disadvantages:

- They are more prone to lightning strikes.
- Single cable failure can disrupt the entire network

3.2.2.4 Connectors

- To connect coaxial cable to devices, we need coaxial connector. The most common type of connector used today is the Bayone-Neill-Concelman or BNC connector.

BNC Connector:

- The BNC (Bayonet Neill-Concelman) connector is a very common type of RF connector used for terminating coaxial cable.

Fig. 3.8: BNC Connector

- The BNC connector is used for RF signal connections, for analog and Serial Digital Interface video signals, amateur radio antenna connections, aviation electronics (avionics) and many other types of electronic test equipment.
- It is an alternative to the RCA connector when used for composite video on commercial video devices, although many consumer electronics devices with RCA jacks can be used with BNC-only commercial video equipment via a simple adapter.
- BNC connectors were commonly used on 10base2 thin Ethernet networks, both on cable interconnections and network cards; though these have largely been replaced by newer Ethernet devices whose wiring does not use coaxial cable. Some ARCNET networks use BNC-terminated coax.

Fig 3.9 (a) Photograph of BNC Connector

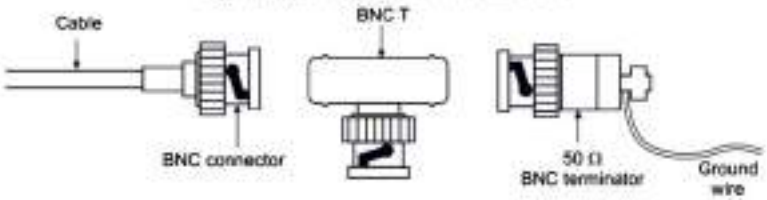


Fig. 3.9 (b): Types of BNC connector

- Fig. 3.9(b) shows 3 popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator.
- The BNC is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.
- BNC connectors exist in 50 and 75 ohm versions. Originally all were 50 ohm and were used with cables of other impedances, the small mismatch being negligible at lower frequencies. The 75 ohm types can sometimes be recognized by the reduced or absent dielectric in the mating ends.
- The different versions are designed to mate with each other, although the impedance mismatch in the cable may lead to signal reflections.

- Typically, they are specified for use at frequencies up to 4 and 2 GHz, respectively.
- 75 ohm BNC Connectors are primarily used for video and DS3 Telco central office applications whereas 50 ohm connectors are used for data and RF.

3.2.2.5 Applications of Coaxial Cable

1. The use of coaxial cable started in analog telephone networks where a single coaxial network could carry 10,000 voice signals.
2. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. (However, coaxial cable in telephone networks has largely been replaced toady with fiber-optic cable).
3. Most common use is in cable TV.
4. Coaxial cabling is often used in heavy industrial environments where motors and generators produce a lot of Electromagnetic Interference (EMI) and where more expensive fiber-optic cabling is unnecessary because of the slow data rates needed.
5. Another common application of coaxial cable is in traditional Ethernet LANs. Because of its high bandwidth and consequently high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs.
6. 10Base-2 or Thin Ethernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10 Mbps with a range of 185 m.
7. 10Base5 or Thick Ethernet, uses RG-11 to transmit 10 Mbps with a range of 5000 m.

3.2.3 Twisted-Pair Cable

- Twisted-pair cable is least expensive and most widely used for data transmission. Twisted-pair cables are most effectively used in systems that use a balanced line method of transmission: Polar Line Coding (Manchester Encoding) as opposed to Unipolar Line Coding (TTL logic).

3.2.3.1 Physical Structure

- A twisted pair cable consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
- One of the wire is used to carry signals to the receiver and the other is used only a ground reference.

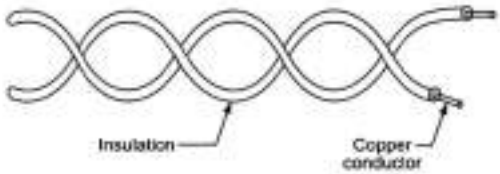


Fig. 3.10: Twisted-Pair Cable

- These cables are color coated to identify each cable.
- Any noise that appears on one wire of the pair would occur on the other wire. Because the wires are of opposite polarities, they are 180 degrees out of phase. When the noise appears on both wires, it cancels or nulls itself out at the receiving end.
- The twists in the cabling reduce the effects of crosstalk and make the cabling more resistant to electromagnetic interference (EMI), which helps maintain a high signal-to-noise ratio for reliable network communication.

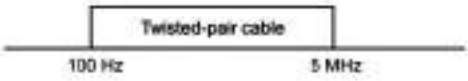


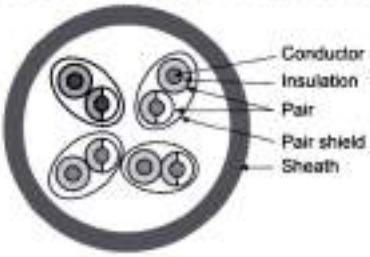
Fig. 3.11: Frequency Range for Twisted-Pair Cable

3.2.3.2 Categories of Twisted Pair Cable

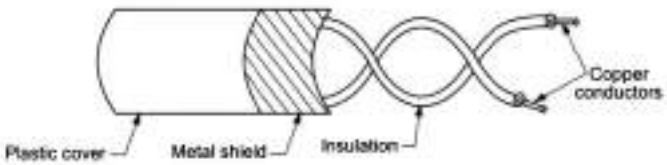
- Twisted Pair cable can be either *Unshielded TP (UTP)* cable or *Shielded TP (STP)* cable.

1. **Shielded TP (STP):**

- IBM produced a version of TP cable for its use called Shielded Twisted Pair (STP).
- These are cables with a shield. Shielding means metallic material added to cabling to reduce susceptibility to noise due to electromagnetic interference (EMI).
- STP cables have a metal foil covering each pair of insulator conductors.



(a) Internal structure of STP cable



(b)

Fig. 3.12: STP cable

Categories of STP:

- STP cabling comes in various grades or categories defined by the EIA/TIA wiring standards, as shown in the Table 3.1.

Table 3.1: STP Cabling Categories

Category	Description
IBM Type 1	Token Ring transmissions on AWG #22 wire up to 20 Mbps.
IBM Type 1A	Fiber Distributed Data Interface (FDDI), Copper Distributed Data Interface (CDDI), and Asynchronous Transfer Mode (ATM) transmission up to 300 Mbps.
IBM Type 2A	Hybrid combination of STP data cable and CAT3 voice cable in one jacket.
IBM Type 6A	AWG #26 patch cables.

Effect of Noise on Twisted-Pair Lines:

- Metal casing used in STP improves the quality of cable by preventing the penetration of noise. It also can eliminate a phenomenon called **Crosstalk**.

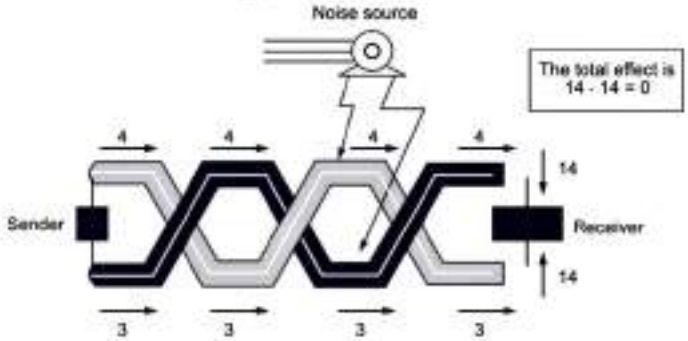


Fig. 3.13: Effect of Noise on Twisted-Pair Lines

- **Crosstalk** is the undesired effect of one circuit (or channel) on another circuit (or channel). It occurs when one line picks up some of the signal traveling down another line.
- Crosstalk effect can be experienced during telephone conversations when one can hear other conversations in the background.

Characteristics:

- It has an impedance of 150 ohms, has a maximum length of 90 meters and is used primarily in networking environments with a high amount of EMI due to motors, air conditioners, power lines or other noisy electrical components. STP cabling is the default type of cabling for IBM Token Ring networks.
- The data transmission rate is higher in STP.
- Due to metal foil covering, STP is more expensive as compared to UTP.

2. Unshielded Twisted Pair (UTP):

- Cables without a shield are called Unshielded Twisted Pair or UTP.
- UTP is cheap, flexible, and easy to install. It is used in many LAN technologies, including *Ethernet* and *Token Ring*.
- Twisted-pair cabling used in Ethernet networking is usually Unshielded Twisted-Pair (UTP) cabling, while Shielded Twisted-Pair (STP) cabling is typically used in Token Ring networks.

Categories of UTP:

- UTP cabling comes in different grades for different purposes.
- The Electronic Industries Association (EIA) has developed standards to classify UTP cable into seven categories. Categories are determined by cable quality, with CAT 1 as the lowest and CAT 7 as the highest.

Table 3.2: Categories of UTP cables

Category	Data Rate	Digital/Analog	Use
CAT 1	< 100 Kbps	Analog	Telephone systems
CAT 2	4 Mbps	Analog/Digital	Voice + Data transmission
CAT 3	10 Mbps	Digital	Ethernet 10BaseT LANs
CAT 4	20 Mbps	Digital	Token based or 10baseT LANs
CAT 5	100 Mbps	Digital	Ethernet 100BaseT LANs
CAT 6	200 Mbps	Digital	LANs
CAT 7	600 Mbps	Digital	LANs

Characteristics:

- The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket.

- Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices.
- The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot.

3.2.3.3 Connectors

- The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector.

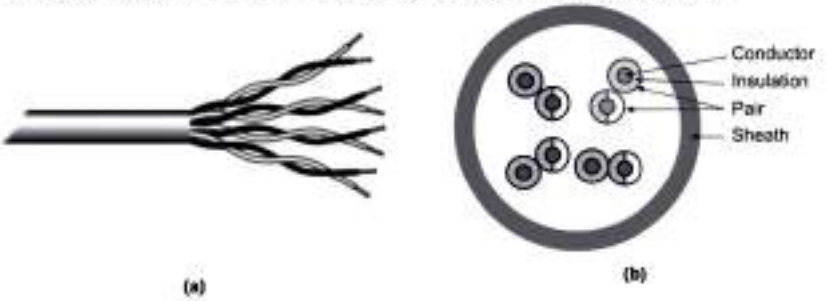


Fig. 3.14: Unshielded Twisted Pair Cable

- A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry.
- This standard designates which wire goes with each pin inside the connector.

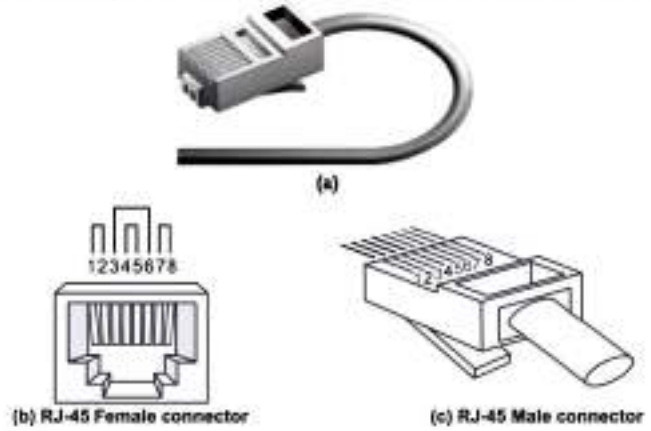


Fig. 3.15: RJ-45 connector

3.2.3.4 Transmission Characteristics

- Requires amplifiers every 5-6 km for analog signals.
- Requires repeaters every 2-3 km for digital signals.
- Attenuation is a strong function of frequency.
- Higher frequency implies higher attenuation.
- Susceptible to interference and noise.
- Improvement possibilities.
- Shielding with metallic braids or sheathing reduces interference.
- Twisting reduces low frequency interference.
- Different twist length in adjacent pairs reduces crosstalk.

3.2.3.5 Comparison of Unshielded and Shielded Twisted Pairs

Table 3.3: Difference between UTP and STP

BASIS OF COMPARISON	UTP	STP
Electromagnetic Interference	Electromagnetic interference and noise is more in UTP.	STP cable reduce electrical noise within the cable and from outside of the cable (e.g. EMI, RFI).
Speed	It offers speed or throughput of about 10 to 1000 Mbps.	It offers speed or throughput of about 10 to 100 Mbps.
Distance	It offers maximum cable length of about 100 meters.	It supports maximum segment of length about 100 meters.
Characteristic	Each of the 8 individual copper wires in UTP cable is covered by insulating material. In addition, wires in each pair are twisted around each other.	Each pair of wires in STP cable is wrapped in an overall metallic foil usually 150 Ohm cable.
Attenuation	Attenuation is high when compared to STP.	Attenuation is low when compared to UTP.
Application	Widely used for data transmission within short distance and is very popular for home network connecting.	Mainly used for connection of enterprises over a long distance.
Crosstalk Generation	The generation of crosstalk is high when compared to STP.	The generation of crosstalk is quite less when compared to UTP.

Contd...

Cost	Cheaper in cost	Costlier than UTP.
Grounding	Grounding cable is not required.	Grounding cable is required.

3.2.3.6 Applications of Twisted Pair Cable

1. This is the most common transmission media for both digital and analog signals.
2. TP cables are used in telephone lines to provide voice and data channels.
3. The DSL lines that are used by the telephone companies to provide high data rate connections also use high bandwidth capability UTP cable.
4. Local Area Network (LAN) also uses twisted-pair cable.

3.2.4 Fiber-optic Cable

(W-18; S-19)

- Fiber-optic is a glass cabling media that sends network signals using light.
- Fiber-optic cabling has higher bandwidth capacity than copper cabling and is used mainly for high-speed network Asynchronous Transfer Mode (ATM) or Fiber Distributed Data Interface (FDDI) backbones, long cable runs and connections to high-performance workstations.
- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- The use of fiber-optics was generally not available until 1970 when Corning Glass Works was able to produce a fiber with a loss of 20 dB/km.
- Today's optical fiber attenuation ranges from 0.5 dB/km to 1000 dB/km depending on the optical fiber used. Attenuation limits are based on intended application.

Fig. 3.16: Fiber-optic Cable

3.2.4.1 Characteristics of Optical Fiber

1. **Capacity:**
   - Much higher bandwidth.
   - Transmits data over long distances.
2. **Smaller size and lightweight:**
   - Very thin for similar data capacity.
   - Much lighter and easy to support in terms of weight (structural properties).

3. **Significantly lower attenuation.**
4. **EM isolation (Resistance to noise):**
   - Not affected by external EM (Electromagnetic) fields.
   - Not vulnerable to interference, impulse noise or crosstalk.
   - No energy radiation; little interference with other devices; security from eavesdropping.
5. **Greater repeater spacing:** Lower cost and fewer error sources.
6. **Speed:** Fiber optic networks operate at high speeds - up into the Gigabits.
7. **Distance:** Signals can be transmitted further without needing to be "refreshed" or strengthened.
8. **Maintenance:** Fiber-optic cable costs much less to maintain.

3.2.4.2 Physical Structure

- The cable consists of one or more strands of glass. The center of each strand is called a core. This core provides pathway for light to travel. A glass or plastic core is surrounded by layer of glass known as **Cladding.**
- Optical fiber uses reflection to guide light through a channel. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it. Information is encoded onto a beam of light as a series of on-off flashes that represents 1's and 0's.
- Looking at the components in a fiber-optic chain will give a better understanding of how the system works in conjunction with wire based systems.
- At one end of the system is a transmitter. This is the place of origin for information coming on to fiber-optic lines.
- The transmitter accepts coded electronic pulse information coming from copper wire. It then processes and translates that information into equivalently coded light pulses.
- A Light-Emitting Diode (LED) or an Injection-Laser Diode (ILD) can be used for generating the light pulses.
- Using a lens, the light pulses are funneled into the fiber-optic medium where they transmit themselves down the line.

Fig. 3.17: Fiber Optic Cable Construction

- Think of a fiber cable in terms of very long cardboard roll (from the inside roll of paper towel) that is coated with a mirror. If you shine a flashlight in one you can see light at the far end - even if bent the roll around a corner.
- Light pulses move easily down the fiber-optic line because of a principle known as total internal reflection. "This principle of total internal reflection states that when the angle of incidence exceeds a critical value, light cannot get out of the glass; instead, the light bounces back in.
- When this principle is applied to the construction of the fiber-optic strand, it is possible to transmit information down fiber lines in the form of light pulses.
- The light is "guided" down the center of the fiber called the "core". The core is surrounded by an optical material called the "cladding" that traps the light in the core using an optical technique called "total internal reflection."
- The core and cladding are usually made of ultra-pure glass, although some fibers are all plastic or a glass core and plastic cladding.
- The fiber is coated with a protective plastic covering called the "primary buffer coating" that protects it from moisture and other damage.

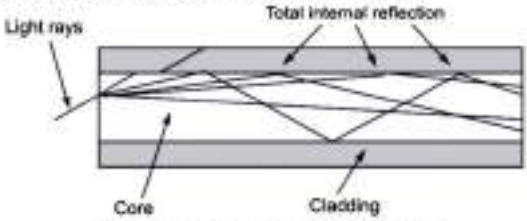


Fig. 3.18: Inner structure of Fiber Optic

- Transparent glass or plastic fibers, which allows light to be guided from one end to the other with minimal loss.

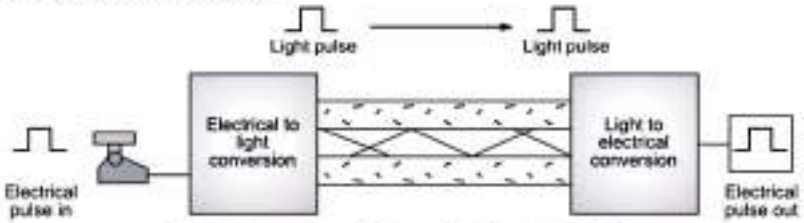


Fig. 3.19: Data Transmission using Fiber Optic Cable

- Fiber-optic cable functions as a "light guide," guiding the light introduced at one end of the cable through to the other end. The light source can either be a Light-Emitting Diode (LED) or a laser.

- The light source is pulsed on and off, and a light-sensitive receiver on the other end of the cable converts the pulses back into the digital ones and zeros of the original signals.
- While fiber-optic cable itself has become cheaper over time - an equivalent length of copper cable cost less per foot but not in capacity.
- Fiber-optic cable connectors and the equipment needed to install them are still more expensive than their copper counterparts.
- The bndwidth of a fiber-optic cable depends on the distance as well as the frequency. Bandwidth is usually expressed in frequency distance form, for example in MHz-km. In other words, a 500-MHz-km fiber-optic cable can transmit a signal a distance of 5 kilometers at a frequency of 100 MHz (5 × 100 = 500) or a distance of 50 kilometers at a frequency of 10 MHz (50 × 10 = 500). In other words, there is an inverse relationship between frequency and distance for transmission over fiber-optic cables.

3.2.4.3 Propagation Modes

- There are two different modes for propagating light along optical channels: *multimode* and *single mode*.

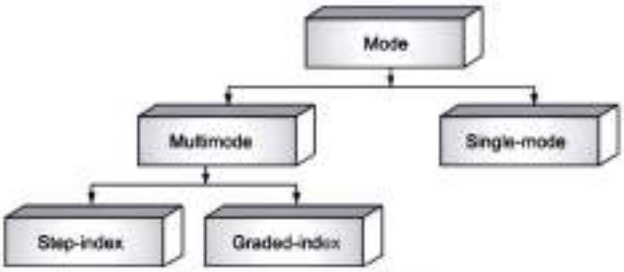


Fig. 3.20: Propagation Modes

1. Multimode:

- Multimode is so named because multiple beams from a light source move through the core in different paths. Multimode cable is made of glass fibers, with a common diameters in the 50-100 micron range for the light carry component, (the most common size is 62.5).
- Multimode fiber gives high bandwidth at high speeds over medium distances. Light waves are dispersed into numerous paths or modes, as they travel through the cable's core typically 850 or 1300 nm. Typical multimode fiber core diameters are 50, 62.5 and 100 micrometers. However, in long cable runs (greater than 3000 feet [914.4 meter]), multiple paths of light can cause signal distortion at the receiving end, resulting in an unclear and incomplete data transmission.

a. **Step-index Multimode Fiber**: In multimode step-index fiber, the density of the core remains constant from the center to the edges.

- A beam of light moves through this constant density in straight line until it reaches the interface of the core and the cladding. At the interface, there is an sudden change to a lower density that alters the angle of beam's motion. The term **step-index** refers to the suddenness of this change.

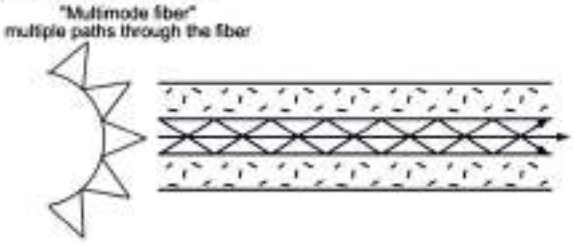


Fig. 3.21: Multimode, Step-Index Fiber

- Step-index multimode fiber has a large core up to 100 microns in diameter. As a result, some of the light rays that make up the digital pulse may travel a direct route, whereas others zigzag as they bounce off the cladding. These alternative pathways cause the different groupings of light rays, referred to as modes, to arrive separately at a receiving point. The pulse, an aggregate of different modes, begins to spread out, losing its well-defined shape. The need to leave spacing between pulses to prevent overlapping limits bandwidth that is, the amount of information that can be sent.
- Consequently, this type of fiber is best suited for transmission over short distances, in an endoscope, for instance. It is less costly variety of multimode fiber, it uses a wide core with a uniform index of refraction, causing the light beams to reflect in mirror fashion off the inside surface of the core by the process of total internal reflection. Because light can take many different paths down the cable and each path takes a different amount of time, signal distortion can result when step-index fiber is used for long cable runs. Use this type only for short cable runs.

b. **Multimode Graded-Index Fiber**:

- A second type of fiber, called *multimode graded-index fiber*, decreases this distortion of the signal through the cable. The word *index* here refers to the index of refraction.
- Index of refraction is related to density. A graded-index fiber, therefore, is one with varying density. Density is highest at the center of the core and decreases gradually to its lowest at the edge.
- Graded-index multimode fiber contains a core in which the refractive index diminishes gradually from the center axis out toward the cladding. The higher refractive index at the center makes the light rays advance moving slowly down the

axis more than those near the cladding. Also, rather than zigzagging off the cladding, light in the core curves helically because of the graded index, reducing its travel distance. The shortened path and the higher speed allow light at the periphery to arrive at a receiver about the same time as the slow, but straight rays in the core axis. In the result, a digital pulse suffers less dispersion.

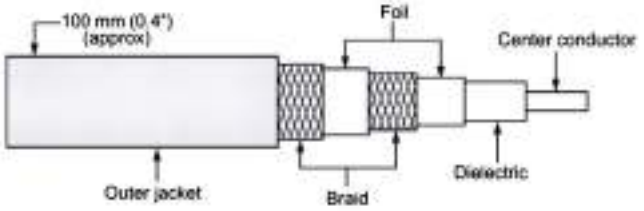


Fig. 3.22: Multimode Graded-Index Fiber

2. Single Mode:

- Single mode uses step-index fiber and a highly focused source of light that limits beams to small range of angles, all close to the horizontal.
- Single Mode cable is a single stand of glass fiber with a diameter of 8.3 to 10 microns that has one mode of transmission.
- Single Mode Fiber with a relatively narrow diameter, through which only one mode will propagate typically 1310 or 1550 nm.
- Carries higher bandwidth than multimode fiber, but requires a light source with a narrow spectral width. Single-mode fiber is also called as Mono-mode optical fiber, Single-mode optical waveguide, Unimode fiber.
- The single mode fiber is manufactured with a much smaller diameter than that of multimode fibers and with substantially lower density (index of refraction). The decrease in density results in a critical angle that is close enough to 90 degrees to make the propagation of beams almost horizontal.

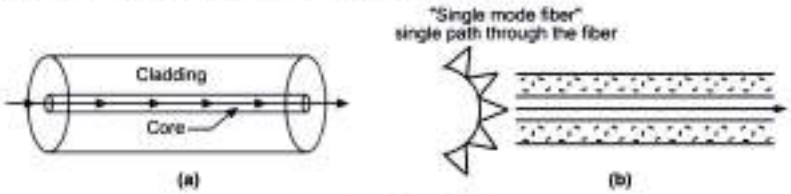


Fig. 3.23: Single-Mode Fiber

- Single-mode fiber gives you a higher transmission rate and up to 50 times more distance than multimode, but it also costs more. Single-mode fiber has a much smaller core than multimode.

- The small core and single light-wave virtually eliminate any distortion that could result from overlapping light pulses, providing the least signal attenuation and the highest transmission speeds of any fiber cable type.

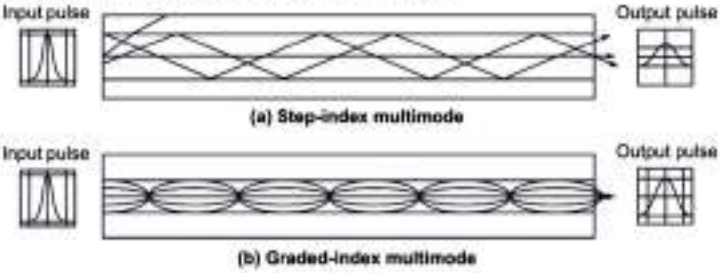


Fig. 3.24: Optical Fiber Transmission Modes

Table 3.4: Single Mode and Multimode Characteristics

Parameters	Single Mode Fiber	Multimode Fiber
Bandwidth	High	Lower
Signal Quality	High	Lower
Main Source of Attenuation	Chromatic Dispersion	Modal Dispersion
Fiber Designs	Step index and Dispersion shifted	Step index and Graded index
Application	Long transmission, higher bandwidth	Short transmission, lower bandwidth
Core/cladding	8.3/125	62.5/125
Light source	ILD	LED/ILD

3.2.4.4 Types of Optical Fiber

- Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in microns (micrometer).

Table 3.5: Optical Fiber Types

Fiber Type	Core	Cladding
62.5/125	62.5	125
50/125	50.0	125
100/140	100.0	140
8.3/125	8.3	125

- The last size listed is used only for single mode. Single mode fiber has a very small core causing light to travel in a straight line and typically has a core size of 8 or 10 microns.
- Multimode fiber supports multiple paths of light and has a much larger core and has a core size of 50 or 62.5 microns.

3.2.4.4 Connectors

- Fiber connector, also called fiber optic cable connectors, are often used to link optical fibers where connect or disconnect capability is needed.
- Fiber optic cable connectors come in many configurations and usages. Some of them are given below:

1. **SC (Subscriber Channel) Fiber Optic Connector:** SC, also called a square connector or subscriber connector. It was developed by Nippon Telegraph and Telephone. It is used for cable TV and uses a push/pull locking system.
2. **ST (Straight Tip) Fiber Optic Connector:** It is used for connecting cable to networking devices. SC is mainly used in multimode fiber optic cable, campuses and buildings.
3. **MT-RJ Fiber Optic Connector:** MT-RJ stands for Mechanical Transfer Registered Jack. MT-RJ is a fiber-optic cable connector that is very popular for small form factor devices due to its small size. The MT-RJ utilizes two fibers and integrates them into a single design that looks similar to a RJ45 connector.
4. **LC Fiber Optic Connector:** LC refers to Lucent Connector. It is a push-pull, small form factor connector that uses a 1.25mm ferrule, half the size of the SC. LC, due to the combination of small size and latch feature, is ideal for high-density connections
5. **FC Fiber Optic Connector:** FC is short for Ferrule Connector. It is a round, threaded fiber optic connector that was designed by Nippon Telephone and Telegraph in Japan. The FC connector is applied for single-mode optic fiber and polarization-maintaining optic fiber. The FC is a screw type connector with a 2.5mm ferrule, which was the first fiber optic connector to use a ceramic ferrule. However, FC is becoming less common and mostly replaced by SC and LC because of its vibration loosening and insertion loss.
6. **MPO/MTP fiber connector:** This connector is a multi-fiber connector which combines fibers from 12 to 24 fibers in a single rectangular ferrule. It's often used in 40G and 100G optical parallel connections. Compared with other fiber connectors mentioned above, MPO/MTP fiber connectors are more complicated. Because there are key-up and key-down, male and female MPO/MTP connectors.

Fig. 3.25: Fiber optic cable connectors

3.2.4.6 Applications of Fiber-optic Cable

1. Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. SONET network provides such backbone.
2. Some cable TV companies use a combination of optical-fiber and coaxial cable.
3. Telephone companies also using optical-fiber cable.
4. The continuing improvements in performance and decline in prices, together with the inherent advantages of optical fiber, have made it increasingly attractive for local area networking. Local Area Networks (LANs) such as 100BaseFx network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.
5. In military applications, it is used for long-distance telecommunications.

3.2.4.7 Advantages

- Advantages of fiber-optic cables are given below:
  1. **Higher Bandwidth:** Higher data rate than TP and coaxial cable.
  2. **Less signal attenuation:** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters after every 5 km for coaxial or TP cable.
  3. **Noise resistance:** Because fiber-optic transmission uses light rather than electricity, noise is not a factor. External light, the only possible interference, is blocked from the channel by the outer jacket.
  4. **Light-weight:** Fiber-optic cables are much lighter than copper cables.
  5. **More immune to tapping (or Security):** Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antennas that can easily be tapped.

6. **Amount of data transfer:** Optical fiber can carry thousands of times more information than copper wire. For example, a single-strand fiber strand could carry all the telephone conversations in the United States at peak hour Fiber is more lightweight than copper.
7. **Reliability:** Fiber is more reliable than copper and has a longer life span.
8. **General capacity:** Fiber optic cable can carry signals for longer distance without repeater than co-axial cable.

3.2.4.8 Disadvantages

- Disadvantages of fiber-optic cable are listed below:

1. **Installation/Maintenance expertise:** Installation and Maintenance need expertise that is not yet available everywhere.
2. **Unidirectional:** Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
3. **Cost:** Fiber-optic cable is more expensive.
4. **Fragility:** Glass fiber is more easily broken than wire, making it less useful for applications where hardware portability is required.
5. **Limited physical arc of cable:** It is breakable, if bend it too much.

3.2.4.9 Comparison of Guided Medias

- **Trade-offs between Electrical and Optical cable:**

1. Electrical is cheaper, especially for short distances, because silicon circuits can send and receive over wires directly. Other semiconductor materials are required to implement the lasers for optical communication. Thus, optical requires multiple die and has a higher base cost.
2. Optical provides better performance at high-bandwidths and long distances. Glass propagates light better than copper propagates electrical currents.

Table 3.6: Comparison of Guided Medias

Sr. No.	Twisted-Pair Cable	Coaxial Cable	Fiber Optic Cable (FOC)
1.	It uses electrical signals for transmission.	It uses electrical signals for transmission.	It uses optical form of signal (i.e. light) for transmission.
2.	It uses metallic conductor to carry the signal.	It uses metallic conductor to carry the signal.	It uses glass or plastic to carry the signal.
3.	Noise immunity is low. Therefore more distortion.	Higher noise immunity than twisted-pair cable due to the presence of shielding conductor.	Highest noise immunity as the light rays are unaffected by the electrical noise.

4.	Affected due to external magnetic filed.	Less affected due to external magnetic filed.	Not affected by the external magnetic filed.
5.	Cheapest	Moderately costly	Costly
6.	Can support low data rates.	Moderately high data rates.	Very high data rates.
7.	Power loss due to conduction and radiation.	Power loss due to conduction.	Power loss due to absorption, scattering, dispersion.
8.	Short circuit between two conductors is possible	Short circuit between two conductors is possible	Short circuit is not possible
9.	Low bandwidth	Moderately high bandwidth	Very high bandwidth

3.3 UNGUIDED MEDIA (S-18)

- Unguided media are natural parts of the Earth's environment that can be used as physical paths to carry electrical signals.
- The atmosphere and outer space are examples of unguided media that are commonly used to carry signals.
- These media can carry electromagnetic signals such as microwaves, infrared light waves and radio waves.
- Network signals are transmitted through all transmission media as a type of waveform. When transmitted through wire and cable, the signal is an electrical waveform.
- When transmitted through fiber-optic cable, the signal is a light wave: either visible or infrared light. When transmitted through Earth's atmosphere or outer space, the signal can take the form of waves in the radio spectrum, including VHF and microwaves, or it can be light waves, including infrared or visible light (For example, lasers).
- Recent advances in radio hardware technology have produced significant advancements in wireless networking devices: the cellular telephone, wireless modems, and wireless LANs.
- Typically, a wireless network uses infrared light or radio transmissions to distribute data. Infrared networks communicate by using beams of infrared light. They have a maximum range of 100 meters.
- Theoretically, they can transmit at 10 Mbps, but 1-3 Mbps is more typical. Narrow band radio networks can cover an area up to 5,000 square meters at up to 4.8 Mbps.

- Their disadvantage is that they offer little security. Spread-spectrum radio networks use multiple frequencies. These multiple channels provide network security.
- They can transmit data at up to 1 Mbps at a range of 800 feet indoors, though 300 Kbps is more typical.

Applications:

- Some common applications of wireless data communication are:
  1. Accessing the Internet using a cellular phone.
  2. Establishing a home or business Internet connection over satellite.
  3. Beaming data between two hand-held computing devices.
  4. Using a wireless keyboard and mouse for the PC.

3.3.1 Electromagnetic Spectrum for Wireless Communication

(W-18; S-18, 19)

- All electromagnetic waves travel at the speed of light (300,000,000 metres per second) in a vacuum, whatever their frequency (in copper or fibre, the speed drops to approximately two thirds of this value, and is slightly frequency dependent).
- The relationship between frequency, wavelength and the speed of light (c) in a vacuum is given by:

$$F\lambda = C$$

- Since, C is a constant, if wavelength is known, then frequency can be calculated and vice versa. Thus, a frequency of 1 MHz would give a wavelength of approximately 300 meters, and a 1 cm wavelength would give a frequency of approximately 30 GHz. The Electromagnetic Spectrum is shown in Fig. 3.37.

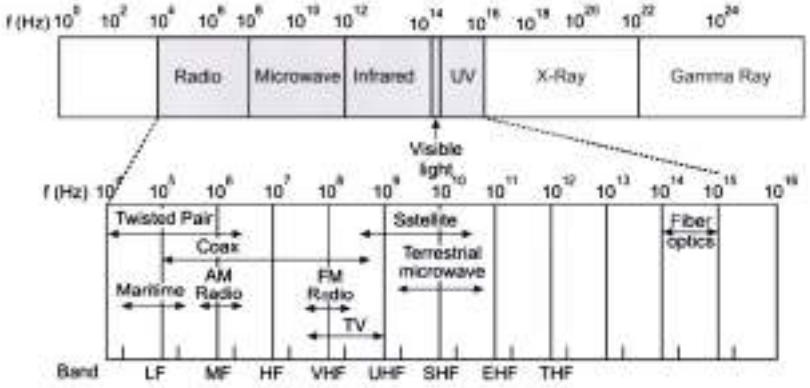


Fig. 3.26: The Electromagnetic Spectrum

- The parts of the electromagnetic spectrum which can be used for transmitting information using amplitude, frequency or phase modulation are shown using a darker shading and include radio, microwave, infrared and visible light.

3.3.2 Propagation Methods

(W-18, S-18, 19)

- Basically, the propagation method classified into three categories:
  1. Ground wave propagation
  2. Sky wave propagation
  3. Line-of-Sight (LOS)

3.3.2.1 Ground Wave Propagation

- Radio waves in the VLF (Very Low Frequency) band propagate in a ground, or surface wave.
- The wave is connected at one end to the surface of the earth and to the ionosphere at the other. The ionosphere is the region above the troposphere (where the air is), from about 50 to 250 miles above the earth.
- It is a collection of ions, which are atoms that have some of their electrons stripped off leaving two or more electrically charged objects.
- The sun's rays cause the ions to form which slowly recombine. The propagation of radio waves in the presence of ions is drastically different than in air, which is why the ionosphere plays an important role in most modes of propagation.
- Ground waves travel between two limits, the earth and the ionosphere, which acts like a duct. Since the duct curves with the earth, the ground wave will follow. Therefore, very long range propagation is possible using ground waves.
- Ground wave propagation more or less follows the contour of the earth and can propagate considerable distances, well over the visual horizon. This effect is found in frequencies up to about 2 MHz.

Fig. 3.27: Ground Waves

- Electromagnetic waves in this frequency range are scattered by the atmosphere in such a way that they do not penetrate the upper atmosphere. The best-known example of ground wave communication is AM radio.

3.3.2.2 Sky Wave Propagation

- Radio waves in the LF (Low Frequency) and MF (Medium Frequency) ranges may also propagate as ground waves, but suffer significant losses, or are attenuated, particularly at higher frequencies. But as the ground wave mode fades out, a new mode develops the sky wave.
- Sky waves are reflections from the ionosphere.
- While the wave is in the ionosphere, it is strongly bent or refracted, ultimately back to the ground. From a long distance away this appears as a reflection.
- Long ranges are possible in this mode also, up to hundreds of miles. Sky waves in this frequency band are usually only possible at night, when the concentration of ions is not too great since the ionosphere also tends to attenuate the signal.
- However, at night, there are just enough ions to reflect the wave but not reduce its power too much.
- The HF (High Frequency) band operates almost exclusively with sky waves. The higher frequencies have less attenuation and less refraction in the ionosphere as compared to MF (Medium Frequency).
- At the high end, the waves completely penetrate the ionosphere and become space waves. At the low end, they are always reflected.
- The HF band operates with both these effects almost all of the time.

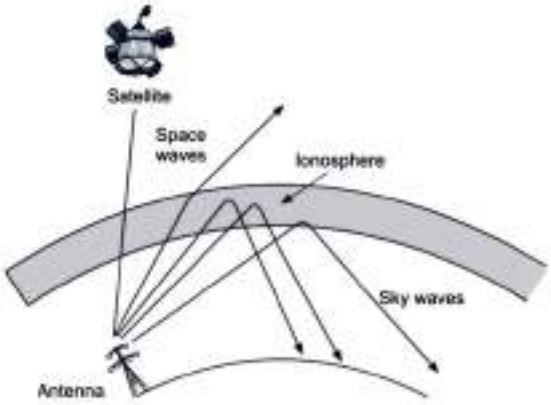


Fig. 3.28: Sky Wave Propagation

- The characteristics of the sky wave propagation depend on the conditions in the ionosphere which in turn are dependent on the activity of the sun.

Layers in Ionosphere:

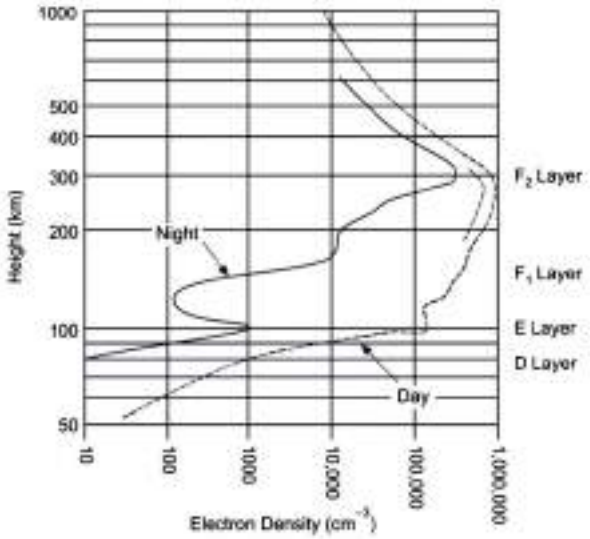


Fig. 3.29: Layers in Ionosphere

- The ionosphere has several well-defined regions in altitude.
  - **D-region:** About 75-95 km. Relatively weak ionization. Responsible for strong absorption of MF during daylight.
  - **E-region:** 95-150 km. An important player in ionospheric scatter of VHF.
  - **F-region:** 150-400 km. This region has separate F1 and F2 layers during the day. The strongest concentration of ions. Responsible for reflection of HF radio waves. Since, the propagation characteristics depend on frequency, several key frequencies can de defined.
  - **Critical frequency:** The minimum frequency that will penetrate the ionosphere at vertical incidence. The critical frequency increases during the daylight and decrease at night. At other angles, the wave will be reflected back. At frequencies above the critical frequency, some range of waves from vertical incidence and down will become space waves.
  - This will cause a gap in coverage on the ground known as a skip zone. In Fig. 3.29, the skip zone extends to about 1400 miles. The transmitted frequency was 5 MHz and the critical frequency was 3 MHz in this example.
  - **Maximum Useable Frequency (MUF):** This defined for two stations. The maximum frequency that will reflect back to the receiving station from the transmitter. Beyond the MUF, the wave will become a space wave. At MUF the skip

zone extends to just short of the receiver. In Fig. 3.29, the MUF for a receiver at 1400 miles is 5 MHz.

- **Lowest Useable Frequency (LUF):** This again defined for two stations. At low frequencies, the signal will be attenuated before it can be reflected. The LUF increases with sunlight and is a maximum near noon.
- **Optimum Frequency for Traffic (OFT):** This frequency for two stations, taking into account the exact conditions in the ionosphere. There will be the perfect frequency that gives the strongest signal. This can be predicted by powerful modeling programs and is the best guarantee of success in HF. The daytime variation if HF propagation is characterized a simple rule-of-thumb: the frequency follows the sun. At noon, the OFT is generally higher than at night.

3.3.2.3 Line-of-Sight

- Above 30 MHz neither ground wave nor sky wave propagation modes operate and then the communication must be by line of sight. For satellite communication, a signal above 30 MHz is not reflected by the ionosphere and therefore a signal can be transmitted between an earth station and a satellite overhead that is not beyond the horizon.

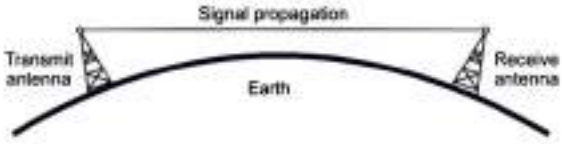


Fig. 3.30: Line-of-sight (LOS) propagation (above 30 MHz)

Effects in Line-of-sight Propagation:

- In the VHF (Very High Frequency) band and up, the propagation tends to straighten out into Line-Of-Sight (LOS) waves. However, the frequency is still low enough for some significant effects.

1. **Ionospheric Scatter:** The signal is reflected by the E-region and scattered in all directions. Some energy makes it back to the earth's surface. This seems to be most effective in the range of 600-1000 miles.

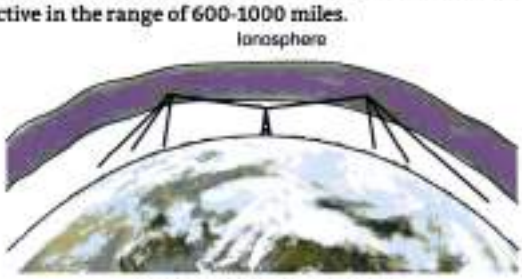


Fig. 3.31: Ionospheric Scatter

2. **Tropospheric Scatter:** Again, the wave is scattered, but this time, by the air itself. This can be visualized like light scattering from fog. This is a strong function of the weather but can produce good performance at ranges fewer than 400 miles.

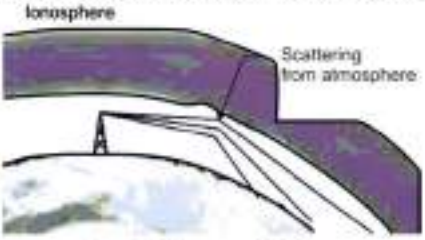


Fig. 3.32: Toposperic Scatter

3. **Tropospheric ducting:** The wave travels slower in cold dense air than in warm air. Whenever, inversion conditions exist, the wave is naturally bent back to the ground. When the refraction matches the curvature of the earth, long ranges can be achieved. This ducting occurs to some extend always and improves the range over true the line-of-sight by about 10 %.
4. **Diffraction:** When the wave is block by a large object, like a mountain, is can diffract around the object and give coverage where no line-of-sight exists.

   Beyond VHF, all the propagation is line-of-sight. Communications are limited by the visual horizon.

   The line-of-sight range can be found from the height of the transmitting and receiving antennas by:

$$R = \sqrt{13h_t} + \sqrt{13h_r}$$

   Where, h_t and h_r are the heights of the antennas in meters, and R will be in km.

3.3.3 Wireless Transmission

(S-18, 19)

- The wireless transmission is the sending and receiving of the data packets over the distance without the use of wires.
- The wireless network transmission is the ideal for the locations where the physical medium like coaxial cables, UPT/STP and fiber optic is not possible to deploy.
- The demand of the wireless communications is increasing exponentially.
- The wireless communication can be performed in a variety of ways such as wireless Ethernet, GSM, Bluetooth, Infrared, Wi-Fi and Wi-Max.
- Similarly, the broadband wireless is an emerging wireless technology that allows the simultaneous delivery of the voice, video and data signals.
- All these technologies based on the different standards and specifications. The wireless communication standards are based on the 802.11 specifications.

- Wireless transmission is the transfer of information over a distance without the use of electrical conductors or "wires".
- The distances involved may be short such as a few meters as in television remote control or long such as thousands or millions of kilometers for radio communications.

3.3.3.1 Radio Waves

- Radio waves are widely used for both indoor and outdoor communication because they are easy to generate, can travel over long distances and can penetrate buildings easily.
- Radio waves used omnidirectional antennas that send out signals to all directions.
- Radio waves are omni-directional. When an antenna transmits radio waves, they are propagated in all directions. This means the sending and receiving antennas do not have to be aligned.
- The properties of radio waves are dependent on frequency.
  - At **low frequencies**, they pass through obstacles well, but the power falls off sharply as the distance from the transmitter increases.
  - At **high frequencies**, radio waves tend to travel in straight lines and bounce off obstacles. They are also absorbed by rain.
  - At **all frequencies**, they are subject to electromagnetic interference from electrical equipment such as electric motors.
- The ability to travel over large distances means that radio transmissions can also interfere with each other, which is one of the main reasons why the use of radio transmitters is tightly controlled by governments.

Radio Transmission Using Ground Wave Propagation:

- In the very low to medium frequency bands, radio waves follow the ground, as illustrated below, and can be detected at distances of up to about 1000 kilometers (Also called as Ground wave Propagation).

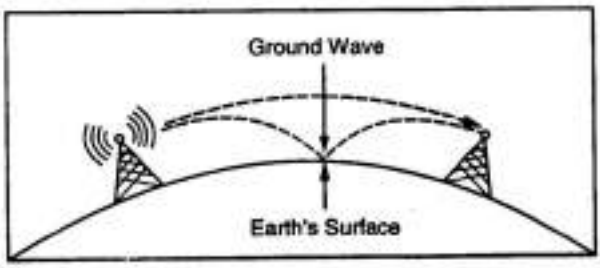


Fig. 3.33: Radio Transmission Using Ground Wave Propagation

- Radio waves at these frequencies can easily pass through buildings and are subsequently widely used by terrestrial radio stations.
- The relatively low bandwidth, however, means that they are not suitable for data communication.

Radio waves radiated by a Base Station's antenna:

- RF is part of electromagnetic spectrum that ranges from 3 Hz – 300 GHz. Radio wave is radiated by an antenna and produced by alternating currents fed to the antenna.
- RF is used in many standard as well as proprietary wireless communication systems.
- RF has long been used for radio and TV broadcasting, wireless local loop, mobile communications, and amateur radio.
- High (HF) and very high (VHF) frequency radio waves that reach the ionosphere, which is a layer of charged particles approximately 100-500 km above the earth's surface, are refracted by it and sent back to earth.
- These bands are used by amateur radio operators to talk over long distances, and are also used for military radio communications.
- Radio waves have virtually no distance limitations. However, the radio waves are government regulated, expensive, and can be tapped into. This can be used across continents.

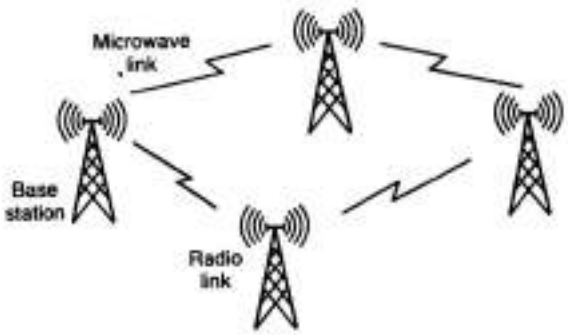


Fig. 3.34: Radio waves radiated by a Base Station's antenna

Applications:

- The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.
- Microwaves are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones, satellite networks and wireless LANs.

3.3.3.2 Infrared Waves

- Unguided infrared waves are widely used for short-range communication. Infrared technology allows computing devices to communicate via short-range wireless signals.
- With infrared, computers can transfer files and other digital data bi-directionally.
- The infrared transmission technology used in computers is similar to that used in consumer product (Television and VCRs) remote control units.
- Used for very short line of sight transmission, remote car locking systems, wireless security alarms. Infrared light is part of electromagnetic spectrum that is shorter than radio waves but longer than visible light.
- Computer infrared network adapters both transmit and receive data through ports on the rear or side of a device.
- Infrared adapters are installed in many laptops and handheld personal devices. Its frequency range is between 300 GHz and 400 THz that correspond to wavelength from 1 mm to 750 nm.
- Infrared is also one of the physical media in the original wireless LAN standard, that's IEEE 802.11.
- Infrared networks were designed to support direct two-computer connections only, created temporarily as the need arises. However, extensions to infrared technology also support more than two computers and semi-permanent networks.
- Infrared communications work by sending and receiving pulses of infrared light. These pulses consist of periods of light and darkness.

IrDA specifications for Infrared technology:

- Infrared use in communication and networking was defined by the IrDA (Infrared Data Association).

Fig. 3.35: TV Remote Control uses Infrared

- Using IrDA specifications, infrared can be used in a wide range of applications, For example, file transfer, synchronization, dial-up networking, and payment. However, IrDA is limited in range (up to about 1 meter).
- It also requires the communicating devices to be in LOS (Line of Sight) and within its 30-degree beam-cone. Infrared technology used in local networks exists in three different forms:
  1. **IrDA-SIR** (slow speed) infrared supporting data rates up to 115 Kbps.
  2. **IrDA-MIR** (medium speed) infrared supporting data rates up to 1.15 Mbps.
  3. **IrDA-FIR** (fast speed) infrared supporting data rates up to 4 Mbps.

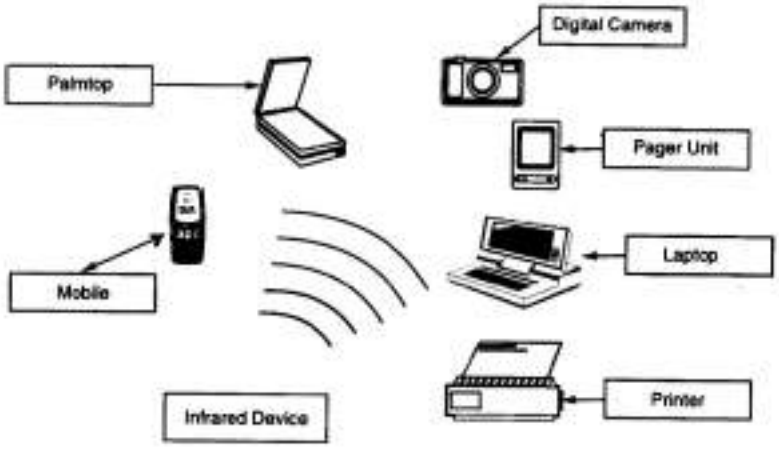


Fig. 3.36: Device Communicates using Infrared

Advantages:

- Infrared transmitters are (relatively) directional, cheap, and easy to manufacture.
- Infrared data and communication is a mode of communication that now plays an important role in wireless data communication.
- It suits the use of laptop computers, wireless data communication and other digital equipment such as personal assistants, cameras, mobile telephones and pagers.
- An infrared system in one room of a building will not interfere with similar systems in nearby rooms, and the possibility of eavesdropping is far lower than with radio based systems.
- IR can be used over longer interconnections and has applicability to Local Area Networks (LANs). However, the maximum effective distance is approximately 1 mile, with a maximum bandwidth of 16 Mbps.

- Infrared is therefore a realistic alternative for indoor wireless LANs, and the computers and offices within a building can be equipped with infrared transmitters and receivers which can be designed to be either directional or diffuse. In the latter case, signals bounce off walls and other objects to reach the receiver.

Disadvantages:

- The major drawback is that infrared waves will not pass through solid objects. The communication between the devices requires that each have a transceiver, (a combination of a transmitter and a receiver) in order to communicate. This capability is provided by microchip technology.
- However, devices may also require further, specialized software allowing communication to be synchronized.
- Infrared communication is now common as a means of wireless communication between devices. It will not penetrate buildings and therefore is secure. Infrared communication is more secure than other options, such as radio, but it cannot be used outside due to interference by the Sun.

Applications of IR (Infrared):

- The short distance of interconnection drives the main application of this technology between appliances.
- Thus, according to the IrDA, at present, the main benefits and applications are:
  - Sending a document from a notebook computer to a printer.
  - Co-ordinating schedules and telephone books between desktop and hand-held (notebook) computers.
  - Sending faxes from a hand-held computer, via a public telephone, to a distant fax machine.
  - Beaming images from digital cameras to a desktop computer.
  - Exchanging messages, business cards and other information between hand-held personal computers.
- For some of these functions, an interconnection between the hand-held or laptop computer and the desktop PC/printer in the form of an IR port is required. Alternatively an IR adapter can be used.

3.3.3.3 Microwave

- At frequencies of 1 GHz and above, electromagnetic waves travel in straight lines and can be narrowly focused. Microwave is the upper part of RF spectrum.
- Because of the availability of larger bandwidth in microwave spectrum, microwave is used in many applications such as wireless PAN, wireless LAN, fixed broadband wireless access (wireless MAN), satellite communications, radar and as backhaul in cellular networks.

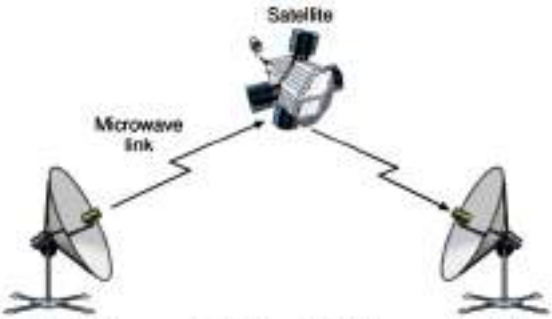


Fig. 3.37: Microwave Link using Dish Antenna and Satellite

- A parabolic dish antenna can be used to focus the transmitted power into a narrow beam to give a high signal to noise ratio, and before the advent of optical fiber, some long distance telephone transmission systems were heavily dependent on the use of a series of microwave towers.
- Because microwaves travel in a straight line, the curvature of the earth limits the maximum distance over which microwave towers can transmit, so repeaters are needed to compensate for this limitation.

Fig. 3.38: Microwave Transmission with Repeater

Propogation Losses:

- As a general rule, the higher the towers are, the further apart they can be. At these higher frequencies, the transmitted waves do not easily pass through buildings.
- Moreover, even though the beam may be well focused at the transmitter, there is still some divergence in space. Some waves may be refracted by low-lying atmospheric and will take longer to arrive at their destination than direct waves.
- Therefore, the delayed waves may arrive out of phase with the direct waves and cancel out the signal. This effect known as *Multipath Fading*.
- Rain can also be a problem, as frequencies around 8 GHz are absorbed by water.
- At higher frequencies, more expensive electronics are required, and transmissions can be subject to interference from radar installations and microwave ovens. Microwave does, however, have several advantages over fiber.

Advantages of Microwave Transmission:

- Obstacles such as roads, railways and rivers may make laying cables difficult whereas, these problems do not exist for microwave and rights of way are not an issue.
- Erecting simple towers or mounting antenna on top of tall buildings is usually far cheaper than laying several kilometers of cable. Microwave also removes the need for reliance on telephone companies. In addition, governments worldwide have set aside the frequency band from 2.400 GHz to 2.484 GHz for unlicensed transmissions, so use of these frequencies does not require a license, and is therefore popular for various forms of short range wireless networking.
- Microwaves have a medium distance limitation and require line of sight. This is good between buildings or between satellites and satellite dishes. Weather and Solar conditions may affect transmission.
- Microwaves are used for long distance communication like cellular phones, garage door openers, and much more.
- Microwave transmission is line of sight transmission. The Transmit station must be in visible contact with the receive station.
- This sets a limit on the distance between stations depending on the local geography. Typically the line of sight due to the Earth's curvature is only 50 km to the horizon. Repeater stations must be placed so the data signal can hop, skip and jump across the country.
- Microwaves operate at high operating frequencies of 3 to 10 GHz. This allows them to carry large quantities of data due to the large bandwidth.

A. Terrestrial Microwave Transmission

- Communication is accomplished through line of sight parabolic dish antenna located on elevated sites.
- Long distance communication is possible by using a series of relay stations. The distance between the stations is dependent on the height above the ground.
- Used for voice and television transmission and private communications and telephone networks For example: emergency services, utilities etc. Utilizes a wide frequency band, 2 to 40 GHz but is susceptible to attenuation and interference.
- Attenuation can rise markedly in poor atmospheric conditions e.g. rain. But adversely affects the higher end of the frequency band, which is only used for short distance transmission.
- Natural noise severely affects transmission frequencies below 2 GHz. Quick to install and overcomes the problems of laying cables in congested locations or over difficult terrain.

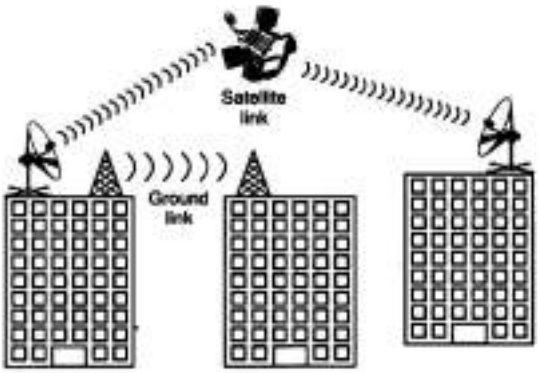


Fig. 3.39: Example of Terrestrial and Satellite Microwave Links

Applications:

- The primary use for terrestrial microwave systems is in long haul telecommunications service. Microwave is commonly used for both voice and television transmission.
- Use of microwave is for short point-to-point links between buildings. This can be used for closed-circuit TV or as a data link between Local Area Networks.
- A business can establish a microwave link to a long-distance telecommunications facility in the same city, bypassing the local telephone company.
- Another important use of microwave is in cellular systems.

B. Satellite Microwave Transmission

- Overcomes the line of sight problems of terrestrial microwave and can be used for point-to-point or broadcast transmission.

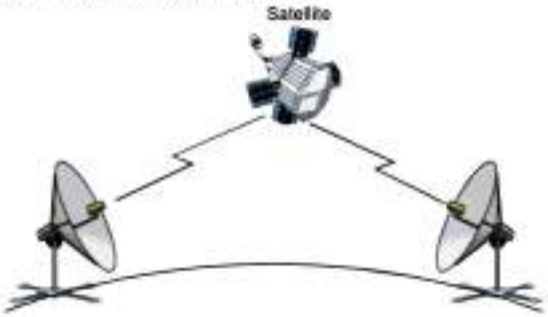


Fig. 3.40: Point-to-Point Link via Satellite Microwave

- Uses an uplink and downlink frequency, a common frequency set is referred to as the 4/6 range which uses a downlink frequency of 4 GHz and an uplink frequency of 6 GHz.
- A microwave transmitter uses the atmosphere or outer space as the transmission medium to send the signal to a microwave receiver.
- The microwave receiver then either relays the signal to another microwave transmitter or translates the signal to some other form, such as digital impulses, and relays it on another suitable medium to its destination.
- Originally, this technology was used almost exclusively for satellite and long-range communication. Recently, however, there have been developments in cellular technology that allow you complete wireless access to networks, intranets and the Internet.
- IEEE 802.11 defines a MAC and physical access control for wireless connection to networks. Used for TV distribution, long-distance telephone, and business networks.

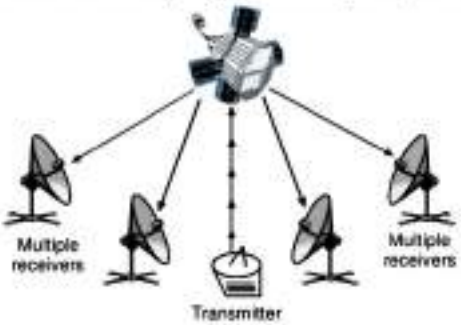


Fig. 3.41: Broadcast Link via Satellite Microwave

- One important difference between infrared and microwave transmission is that the former does not penetrate walls. Thus the security and interference problems encountered in microwave systems are not present. Furthermore, there is no frequency allocation issue with infrared, because no licensing is required.

Advantages of satellite microwave transmission:

1. They require no right of way acquisition between towers.
2. They can carry high quantities of information due to their high operating frequencies.
3. Low cost land purchase: each tower occupies small area.
4. High frequency/short wavelength signals require small antenna.

Disadvantages:

1. Attenuation by solid objects such as birds, rain, snow and fog.

2. Reflected from flat surfaces like water and metal.
3. Diffracted (split) around solid objects.
4. Refracted by atmosphere, thus causing beam to be projected away from receiver.

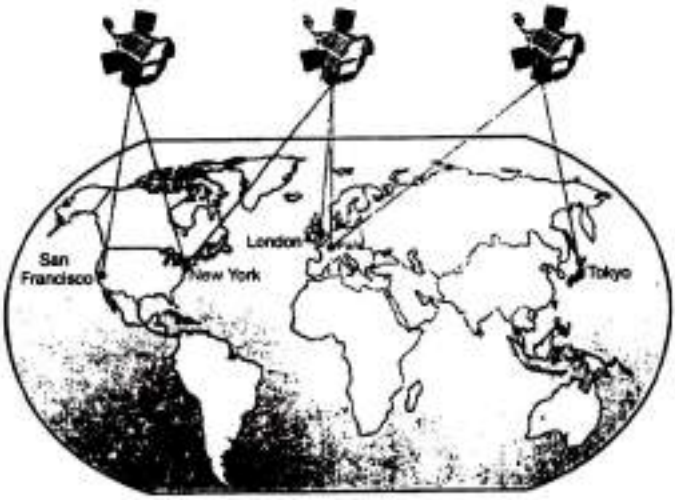


Fig. 3.42: Satellite Microwave Link for Worldwide Communication

Applications:

- The most important applications for satellites are the following:
  1. Television distribution
  2. L ong-distance telephone transmission
  3. Private business networks for global organizations.
  4. Microwave transmitters and receivers, especially satellite systems, are commonly used to transmit network signals over great distances.

3.4 COMPARISON OF GUIDED AND UNGUIDED MEDIA

Table 3.7: Difference between Guided Media and Unguided Media

Sr. No.	Guided Media	Unguided Media
1.	The signal energy is contained and bounded within a solid medium.	The signal energy propagates in the form of unbounded electromagnetic waves.
2.	Used for point-to-point communication	Used for broadcasting.

Contd..

3.	Twisted-pair cable, coaxial cable, fiber optical cables are example of bounded media.	Radio and infrared light are the examples of unbounded media.
4.	Attenuation depends exponentially on the distance.	Attenuation is proportional to square of distance.

Summary

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- Types of transmission Media are: Guided (wired) and Unguided Media (wireless).
- Examples of Wired transmission media are: Twisted pair, Fiber-optic, Coaxial cable.
- Twisted Pair is the least expensive and most widely used guided transmission medium. It consists of two insulated copper wires arranged in a regular spiral pattern.
- Types of twisted pair : Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP).
- Coaxial cable consists of two conductors, but is constructed differently to permit it to operate over a wider range of frequencies. It consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor.
- Coaxial cable is widely used as a means of distributing TV signals to individual homes — cable TV.
- An optical fiber is a thin, flexible medium capable of guiding an optical ray.
- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as wireless transmission.
- Examples of wireless transmission media are Radio waves, Microwaves, Bluetooth, Wi-Fi, Satellites, Infrared.
- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are of two types: Terrestrial microwave and Satellite microwave.
- The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.
- An infrared transmission is a wireless technology used for communication over short ranges. The frequency of this in the range from 300 GHz to 400 THz.

- Wireless transmissions propagate in three modes: ground-wave, sky-wave, and line-of-sight.
- Ground wave propagation follows the contour of the earth, while sky wave propagation uses reflection by both earth and ionosphere. Line of sight propagation requires the transmitting and receiving antennas to be within line of sight of each other.
- Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multi- mode can be implemented in two forms: step-index or graded-index.

Check Your Understanding

1. BNC stands for _____.
   (a) Bayonet Neill–Concelman (b) Boys Net–Concelman
   (c) Bayonet Neill–Connector (d) Bayonet Network–Concelman
2. The "RJ" in RJ45 stands for _____.
   (a) Resistance Jet (b) Registered Jack
   (c) Routing Jack (d) Radio Jack
3. Which of following is not Unguided Media?
   (a) Microwaves (b) Radio Waves
   (c) Ifrared (d) Fiber Optic
4. _____cables carry data signals in the form of Light.
   (a) Coaxial (b) Fiber optic
   (c) Twisted Pair (d) None of these
5. _____cables consists of two insulated copper wire twisted together.
   (a) Coaxial (b) Fiber optic
   (c) Twisted Pair (d) one of these
6. _____ cable consists of an inner copper core and a second conducting outer sheath.
   (a) Twisted-pair (b) Coaxial
   (c) Fiber-optic (d) Shielded twisted-pair
7. In fiber optics, the signal is _____.
   (a) light (b) radio
   (c) infrared (d) very low-frequency waves.
8. Signals with a frequency between 2 MHz and 30MHz use _____propagation.
   (a) ground (b) Sky
   (c) line-of-sight (d) none of the above

9. A parabolic dish antenna is a(n) _____ antenna.
   (a) omnidirectional (b) bidirectional
   (c) unidirectional (d) horn
10. Which of the following is not a guided medium?
   (a) twisted-pair cable (b) coaxial cable
   (c) fiber-optic cable (d) atmosphere

ANSWERS

(1) a	(2) b	(3) d	(4) b	(5) c	(6) d	(7) a
(8) b	(9) c	(10) d				

Practice Questions

Q.I Answer the following questions in short.

1. What is transmission media?
2. What are types of transmission media?
3. Which are types of twisted-pair cables?
4. Write the types of wireless data transmission?
5. What is propagation mode in fiber-optic cable?
6. What is infrared?
7. What is Wireless LAN?
8. What is unguided media?

Q.II Answer the following questions.

1. With suitable diagram describe transmission media.
2. Explain coaxial cable with diagram.
3. Enlist various characteristics of transmission media.
4. State various applications of TP cable.
5. With suitable diagram describe STP and UTP cables.
6. Enlist various applications of fiber optic cable.
7. Explain guided media in brief.
8. With suitable diagram describe electromagnetic spectrum in brief.
9. Compare guided and unguided media.
10. State advantages and disadvantages of wireless LAN.
11. State various applications Infrared.
12. Differentiate between Fiber Optic and Twisted Pair Cable.
13. Write a short note on.
    i) BNC Connector ii) Propagation Mode iii) Guided Media
14. Explain in detail 'Line of-sight'
15. Explain wireless transmission and explain any one media in detail.

16. What is Connector? Explain RJ-45 and BNC connector.
17. What is Wireless Communication? Explain need of Wireless Communication in transmission.
18. Explain Radio waves as a wireless transmission.

Q.III Define following Terms:

1. Ground wave propagation
2. Sky wave propagation
3. Wireless LAN
4. Guided and unguided media
5. Radio waves

Previous Exams Questions

Summer 2018

1. Explain wireless transmission and explain any one media in detail. 5M

Ans. Please refer to Section 3.3.3

2. Explain propagation method. 5M

Ans. Please refer to Section 3.3.2

3. Write notes on Unguided Media 5M

Ans. Please refer to Section 3.3

Winter 2018

1. Explain Optic Fiber Cable in detail. 5M

Ans. Please refer to Section 3.2.4.

2. What are different propagation methods? Explain any one. 5M

Ans. Please refer to Section 3.3.2.

3. Write notes on Guided Media. 5M

Ans. Please refer to Section 3.2

Summer 2019

1. Explain wireless transmission. Explain any one media in detail. 5M

Ans. Please refer to Section 3.3.3.

2. Explain optic fiber cable in detail. 5M

Ans. Please refer to Section 3.2.4.

3. Explain propagation method. 5M

Ans. Please refer to Section 3.3.2.

❖❖❖

4... Wired and Wireless LANs

Objectives...

- To learn about IEEE Standards
- To study Standard Ethernet, Fast Ethernet, Gigabit Ethernet, Ten-Gigabit Ethernet
- To know Backbone Networks and its types
- To get knowledge of Virtual LANs Membership and IEEE standards advantages
- To learn about Wireless LAN
- To get knowledge of IEEE 802.11 Architecture and Bluetooth Architecture (Piconet Scattemet)

4.1 IEEE STANDARDS

- IEEE 802.3 is a collection of IEEE standards defining the physical layer, and the media access control (MAC) sublayer of the data link layer, of wired Ethernet. This is generally a LAN technology with some WAN applications. Physical connections are made between nodes and/or infrastructure devices (hubs, switches, routers) by various types of copper or fiber cable.
- 802.3 is a technology that can support the IEEE 802.1 network architecture.
- The maximum packet size is 1518 bytes, although to allow the Q-tag for Virtual LAN and priority data in 802.3ac it is extended to 1522 bytes. If the upper layer protocol submits a protocol data unit (PDU) less than 46 bytes, 802.3 will pad the data field to achieve the minimum 46 bytes. The minimum frame size will then always be of 64 bytes.
- Although it is not technically correct, the terms packet and frame are often used interchangeably. The ISO/IEC 8802-3 and ANSI/IEEE 802.3 standards refer to MAC sub-layer frames consisting of the destination address, the source address,

length/type, data payload, and frame check sequence (FCS) fields. The preamble and start frame delimiter (SFD) are (usually) together considered a header to the MAC frame. This header and the MAC frame constitute a packet.pad

- The original Ethernet is called Experimental Ethernet today. It was developed by Robert Metcalfe in 1972 (patented in 1978) and was based in part on the wireless ALOHA net protocol. It is not in use anywhere, but is thought to be the only Ethernet by some purists. The first Ethernet that was generally used outside Xerox was the DIX Ethernet. However, as DIX Ethernet was derived from Experimental Ethernet, and as many standards have been developed that are based on DIX Ethernet, the technical community has accepted the term Ethernet for all of them. Therefore, the term Ethernet can be used to name networks using any of the following standardized media and functions.
- In the last several years, the demand on the network has increased drastically. The old 10Base5 and 10Base2 Ethernet networks were replaced by 10BaseT hubs, allowing for greater manageability of the network and the cable plant. As applications increased the demand on the network, newer, high-speed protocols such as FDDI and ATM became available. However, in the last two years, Fast Ethernet has become the backbone of choice because its simplicity and its reliance on Ethernet. The primary goal of Gigabit Ethernet is to build on that topology and knowledge base to build a higher-speed protocol without forcing customers to throw away existing networking equipment.
- The standards body working on Gigabit Ethernet is the IEEE 803.2z Task Force, which has established an aggressive timetable for development of the Gigabit Ethernet standard. The possibility of a Gigabit Ethernet Standard was raised in mid-1995 after the final ratification of the Fast Ethernet Standard. By November 1995 there was enough interest to form a high-speed study group. This group met at the end of 1995 and several times during early 1996 to study the feasibility of Gigabit Ethernet. The meetings grew in attendance, reaching 150 to 200 individuals. Numerous technical contributions were offered and evaluated.
- In July 1996, the 802.3z Task Force was established with the charter to develop a standard for Gigabit Ethernet. Basic concept agreement on technical contributions for the standard was achieved at the November 1996 IEEE meeting. The first draft of the standard was produced and reviewed in January 1997; the final standard was approved in June 1998.
- CSMA/CD (Carrier Sense Multiple Access/Collision Detection) based LAN proposed by the IEEE 802.3 subcommittee, commonly known as Ethernet.
- In this section we shall discuss Ethernet (CSMA/CD), Token bus, Token ring based LANs proposed by the IEEE 802. 3, IEEE 802.4 and IEEE 802.5, subcommittees.

Fig. 4.1: IEEE Standards in OSI Layer

4.1.1 IEEE Standard 802.3 (Ethernet)

- The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. Ethernet is the most widely-installed Local Area Network technology.
- This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By following to the IEEE standard, network equipment and network protocols can communicate efficiently.
- An Ethernet LAN typically uses coaxial cable or twisted pair wires. It provides speeds up to 10 Megabits per second (10 Mbps).
- The devices connected to the LAN compete for access using CSMA/CD protocol.

Example:

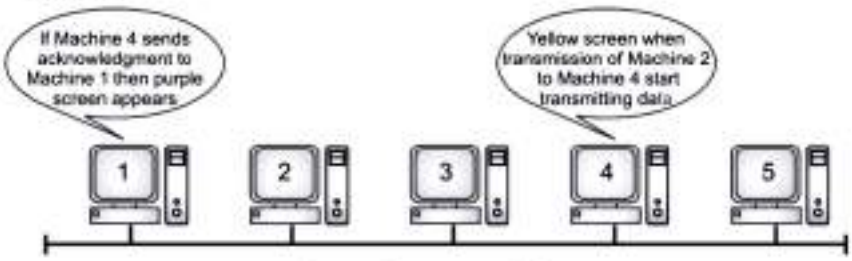


Fig. 4.2: Ethernet Transmission

- In above fig., Machine 2 wants to send a message to Machine 4, but first it listens to the cable to make sure that no one else is using the network.

- If it is all clear it starts to transmit its data on to the network (represented by the yellow screens). Each packet of data contains the destination address, the senders address and the data to be transmitted.
- The signal moves down the cable and is received by every machine on the network but because it is only addressed to number 4, the other machines ignore it.
- Machine 4 then sends a message back to number 1 acknowledging receipt of the data (represented by the purple screens).
- As we stated before, there is a possibility of two machines try to transmit simultaneously over the cable. The result can be observed in the Fig. 4.3.

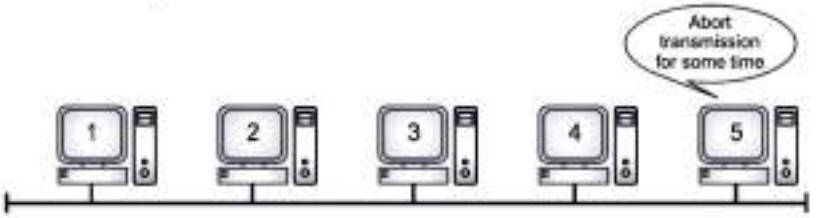


Fig. 4.3: Abort Transmission

- What happens is that Machine 2 and 5 decide to transmit at the same time. The packets collide and each machine has the ability to detect the collision and immediately abort transmission. Then they wait for random period of time and transmit again.

Protocols:

1. CSMA/CD:

- Carrier Sense Multiple Access with Collision Detection is a protocol used to sense whether a medium is busy before transmission but is the ability to detect whether a transmission has collided with another.
- CSMA/CD is the protocol used in Ethernet networks to ensure that only one network node is transmitting on the network wire at any one time.
- Carrier Sense means that every Ethernet device listens to the Ethernet wire before it attempts to transmit. If the Ethernet device senses that another device is transmitting, it will wait to transmit.
- Multiple Access means that more than one Ethernet device can be sensing (listening and waiting to transmit) at a time.
- Collision Detection means that when multiple Ethernet devices accidentally transmit at the same time, they are able to detect this error.
- The collision detection in CSMA/CD that was mentioned earlier functions when the interfaces start relaying out signals simultaneously. This can happen because the

transmission of data is not instantaneous. In other words, if the Ethernet system gets clogged up, the CSMA/CD will take the necessary steps to unblock it.

- The collision detector of the CSMA/CD functions by releasing its own signal. In some Ethernet systems it is the 24 mA.

Working of CSMA/CD:

- A method called CSMA/CD was used to send data over shared single coaxial cable connected to all computers on a network.
- In this method, the computer terminals (also called as stations) transmit the data over cable whenever the cable is idle, if more than one station transmits at same time and if they collide, the transmission will be stopped by such stations. They will wait for some random time and restart transmission.
- The concept of sharing single cable or wire between multiple stations was used for first time in Hawaiian Islands. It was called ALOHA systems; built to allow radio communication between machines located at different places in Hawaiian Islands. Later Xerox PARC built a 2.94 mbps CSMA/CD system to connect multiple personal computers on a single cable. It was named as Ethernet.
- Ethernet or IEEE 802.3 standards only define MAC (Data link) and Physical layer of standard OSI model.

2. CSMA/CA:

- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is a protocol for carrier transmission in 802.11 networks.
- Unlike CSMA/CD which deals with transmissions after a collision has occurred, CSMA/CA acts to prevent collisions before they happen.
- In CSMA/CA, as soon as a node receives a packet that is to be sent, it checks to be sure the channel is clear (no other node is transmitting at the time). If the channel is clear, then the packet is sent. If the channel is not clear, the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear.
- This period of time is called the back-off factor, and is counted down by a back-off counter. If the channel is clear when the back-off counter reaches zero, the node transmits the packet. If the channel is not clear when the back-off counter reaches zero, the back-off factor is set again, and the process is repeated.

4.1.2 IEEE Standard 802.4 (Token Bus)

- IEEE 802.4 standard evolved from the needs of companies like General Motors implementing terminals for factory automation.
- 802.3 was not suitable for them as a station in ethernet has to wait for a long time to send a frame in worst case. 802.3 frames do not have priorities which makes important frames waiting for unimportant frames.

- A token bus system is a medium access control technique for bus/tree stations form a logical ring around which a token is passed.
- A station receiving the token may transmit data and then must pass the token on to next station in the ring.
- Though it is similar to token ring it does not implement the ring physically as it has drawback of getting entire network down in case one terminal is down.
- If there are n stations the token bus network and TP seconds are required to send a frame. It will take not more than n TP seconds to get a turn for a station.

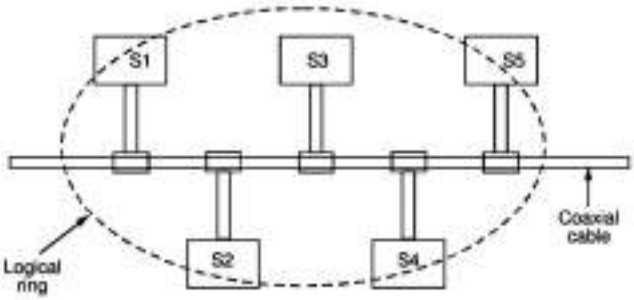


Fig. 4.4: Token Bus

- The stations can be configured so that they can be a part of the logical ring or may opt out of the ring.
- Initially highest number station gets the token. Then it passes the token to its neighbour (right or left).
- Token thus moves around the ring with token holder permitted send the frame.
- If station has no data it must pass the token to next station.
- The 85 ohm broadband cable is used at physical layer.

Frame Format of Token Bus Protocol:

- The token bus frame format is shown in Fig. 4.5

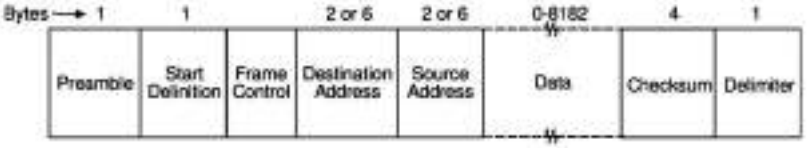


Fig. 4.5: Token Bus (802.4) Frame Format

- Fields of 802.4 (token bus) frame format are listed below:
  1. **Preamble:** It is used to synchronize the receiver's clock as in case of Ethernet (802.3).
  2. **Starting and ending delimiter:** These fields are for frame synchronization mark the frame boundaries.
  3. **Frame control:** This field is used to indicate whether the frame is data frame or control frame. For data frames, it carries frame's priority. Token bus defines four classes of priorities 0, 2, 4, and 6 for traffic with 0 lowest and 6 highest. Each station puts the data as per their priority in the substations. Each substation with different priority maintains its own queue of frames to be transmitted. When token comes to a station, it is first given to the substation with priority 6, so that it can transmit the frames first, and then it is given to substation with priority 4 and so on. In this field, there can be indicator of whether destination is allowed to acknowledge the frame or not.
     In case of control, the frames have token passing and ring maintenance frames. They also manage the job of letting new stations enter the ring or existing ones to leave the ring.
  4. **Source address and destination address:** It is similar to 802.3. These fields are 2 byte or 6 byte long. But they should either all byte or 6 byte on source cable for all stations.
  5. **Data field:** It can be extended upto 8182 bytes when 2 byte address is used and 8174 bytes when 3 bytes address is used.
  6. **Checksum:** It is used to detect transmission errors. CRC polynomial as in 802.3 is used.

4.1.3 IEEE Standard 802.5 (Token Ring)

- The token ring protocol is the second most widely-used protocol on Local Area Networks (LANs) after Ethernet.
- The IEEE 802.5 token ring technology provides for data transfer rates of either 4 or 16 Mbps. It is a collection of individual point-to-point links, connecting each terminal, that happen to form a circle.
- Token Ring is formed by the nodes connected in ring format as shown in the Fig. 4.6.

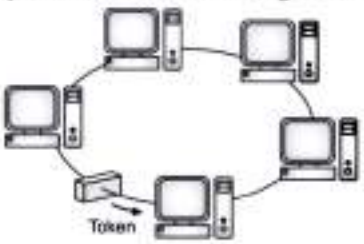


Fig. 4.6: Token Ring (802.5)

- The principle used in the token ring network is that a token is circulating in the ring and whichever node grabs that token will have right to transmit the data.
- Whenever, a station wants to transmit a frame it inverts a single bit of the 3-byte token which instantaneously changes it into a normal data packet. Because there is only one token, there can at most be one transmission at a time.
- Since, the token rotates in the ring it is guaranteed that every node gets the token within some specified time. So there is an upper bound on the time of waiting to grab the token so that starvation is avoided.
- There is also an upper limit of 250 on the number of nodes in the network. To distinguish the normal data packets from token (control packet) a special sequence is assigned to the token packet. When any node gets the token it first sends the data it wants to send, then recirculates the token.
- If a node transmits the token and nobody wants to send the data the token comes back to the sender. If the first bit of the token reaches the sender before the transmission of the last bit, then error situation arises. So to avoid this we should have: propagation delay + transmission of n-bits (1-bit delay in each node) > transmission of the token time.
- A station may hold the token for the token-holding time which is 10 ms unless the installation sets a different value. If there is enough time left after the first frame has been transmitted to send more frames, then these frames may be sent as well.
- After all pending frames have been transmitted or the transmission frame would exceed the token-holding time, the station regenerates the 3-byte token frame and puts it back on the ring.

Modes of Operation:

1. **Listen Mode:** In this mode the node listens to the data and transmits the data to the next node. In this mode there is a one-bit delay associated with the transmission.

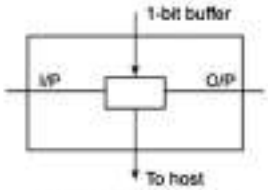


Fig. 4.7: Listen Mode

2. **Transmit Mode:** In this mode the node just discards the any data and puts the data onto the network.

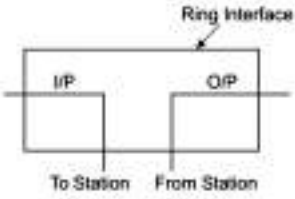


Fig. 4.8: Transmit Mode

3. **By-pass Mode:** When the node is down, By-pass mode is reached. Any data is just bypassed. There is no one-bit delay in this mode.

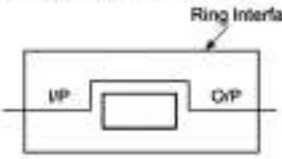


Fig. 4.9: By-pass Mode

Transactions of Token Ring:

- A special 'three-byte' frame pattern called a "token" circulates around the ring (See Fig. 4.10). A station wishing to transmit on the ring must seize the token.
- The station then alters one bit of the token which then becomes the first part of the normal data frame the station wishes to transmit.
- Only having one token on the ring means that only one station can transmit at a time. This solves the problem of contention and access to the common media.
- In the example, Machine 1 wants to send some data to Machine 4. It captures the token, writes its data and the recipient's address onto the Token (indicated by the yellow screen).
- The packet of data travels first to Machines 2 and 3 that read the address, realize it is not its own, and pass the token to Machine 4. This time it is the correct address and so number 4 stores the packet (represented by the yellow screen).
- Then Machine 4 sends an acknowledgement back to Machine 1 to say that it has received the packet (represented by the purple screen).
- Machines 5 and 6 forward the acknowledgement to Machine 1, who sent the original message.
- As soon as Machine 1 receives the acknowledgement (ACK) from machine 4 (indicated by the purple flashing screen) regenerates the free token back on to the ring ready for the next machine to use.

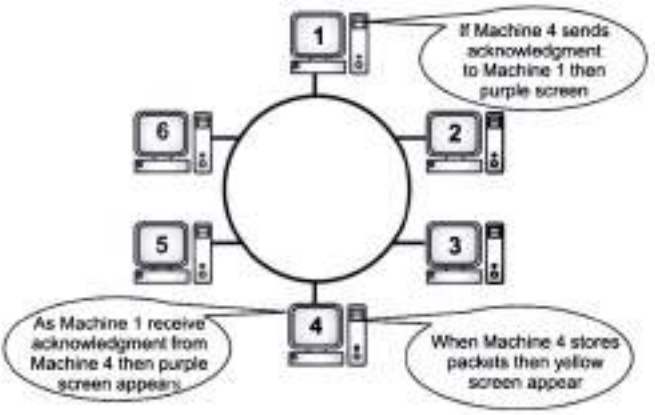


Fig. 4.10: Token Ring Transactions

Priority System:

- Token Ring networks use a sophisticated priority system that permits certain user-designated, high-priority stations to use the network more frequently. Token Ring frames have two fields that control priority: the priority field and the reservation field.
- Only stations with a priority equal to or higher than the priority value contained in a token can seize that token. After the token is seized and changed to an information frame, only stations with a priority value higher than that of the transmitting station can reserve the token for the next pass around the network. When the next token is generated, it includes the higher priority of the reserving station. Stations that raise a token's priority level must reinstate the previous priority after their transmission is complete.

Fault-Management Mechanisms:

- Token Ring networks employ several mechanisms for detecting and compensating for network faults. For example, one station in the Token Ring network is selected to be the active monitor. This station, which potentially can be any station on the network, acts as a centralized source of timing information for other ring stations and performs a variety of ring-maintenance functions. One of these functions is the removal of continuously circulating frames from the ring. When a sending device fails, its frame may continue to circle the ring. This can prevent other stations from transmitting their own frames and essentially can lock up the network. The active monitor can detect such frames, remove them from the ring, and generate a new token.

- The IBM Token Ring network's star topology also contributes to overall network reliability. Because all information in a Token Ring network is seen by active MSAUs, these devices can be programmed to check for problems and selectively remove stations from the ring, if necessary.
- A Token Ring algorithm called beaconing detects and tries to repair certain network faults. Whenever a station detects a serious problem with the network (such as a cable break), it sends a beacon frame, which defines a failure domain. This domain includes the station reporting the failure, its Nearest Active Upstream Neighbor (NAUN), and everything in between. Beaconing initiates a process called autorecon figuration, in which nodes within the failure domain automatically perform diagnostics in an attempt to reconfigure the network around the failed areas. Physically, the MSAU can accomplish this through electrical reconfiguration.

Frame Format:

- Token Ring and IEEE 802.5 support two basic frame types: tokens and data/command frames.
- Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter.
- Data/command frames vary in size, depending on the size of the information field.
- Data frames carry information for upper layer protocols, while command frames contain control information and have no data for upper layer protocols.
- Both formats are shown in Fig. 4.11.

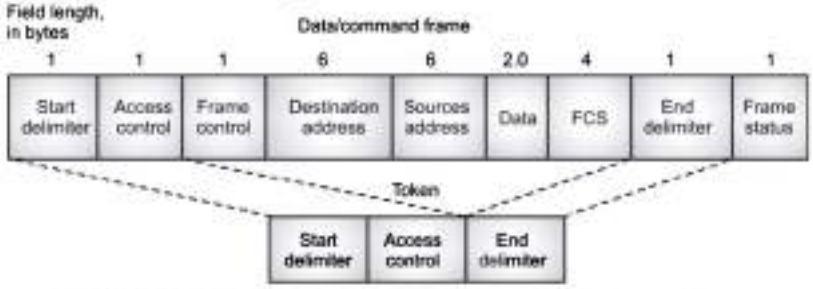


Fig. 4.11: IEEE 802.5 and token ring specify tokens and data/command frames

(i) Token Frame Fields:

- The three token frame fields illustrated in Fig. 4.11 are summarized in the descriptions that follow:
  1. **Start delimiter:** This field alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from

the rest of the frame by violating the encoding scheme used elsewhere in the frame.

2. **Access-control byte:** This field contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
3. **End delimiter:** This field signals the end of the token or data/command frame. This field also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.

(ii) Data/Command Frame Fields:

- Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields illustrated in Fig. 4.11 are described in the following summaries:
  - **Start delimiter:** Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
  - **Access-control byte:** Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
  - **Frame-control bytes:** This field indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
  - **Destination and source addresses:** This field consists of two 6-byte address fields that identify the destination and source station addresses.
  - **Data:** This field indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.
  - **Frame check sequence (FCS):** This field is filled by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
  - **End Delimiter:** signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.
  - **Frame Status:** This field is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

4.2 STANDARD ETHERNET (S-19)

- The Standard Ethernet defines several physical layer implementations; four of the most Common.

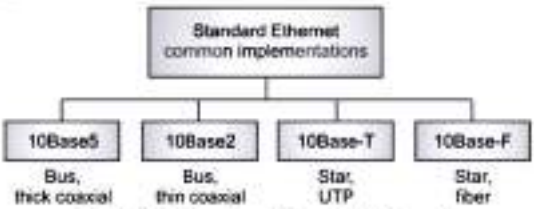


Fig. 4.12: Categories of Standard Ethernet

Encoding and Decoding:

- All standard implementations use digital signalling (baseband) at 10 Mbps. At the sender, data are converted to a digital signal using the Manchester scheme; at the receiver, the received signal is interpreted as Manchester and decoded into data. Manchester encoding is self-synchronous, providing a transition at each bit interval. Fig. 4.13 shows the encoding scheme for Standard Ethernet.

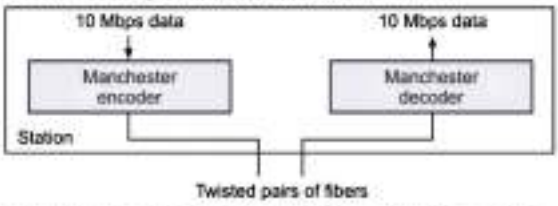


Fig. 4.13: Encoding in a Standard Ethernet implementation

a. 10Base5: Thick Ethernet

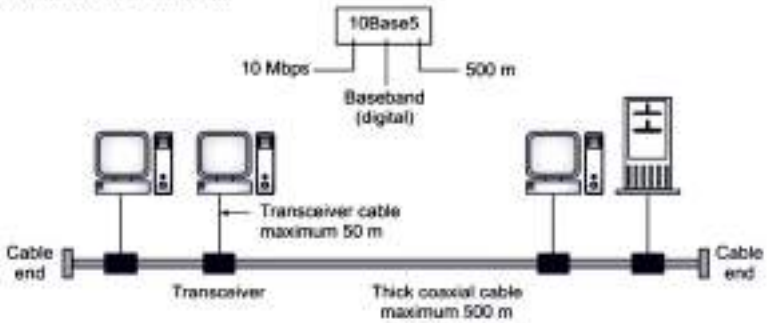


Fig. 4.14: 10Base5 implementation

- The first implementation is called 10Base5, thick Ethernet, or Thicknet. The nickname derives from the size of the cable, which is roughly the size of a garden hose and too stiff to bend with your hands. 10Base5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable

b. 10Base2: Thin Ethernet

- The second implementation is called 10Base2, thin Ethernet, or Cheapernet. 10Base2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

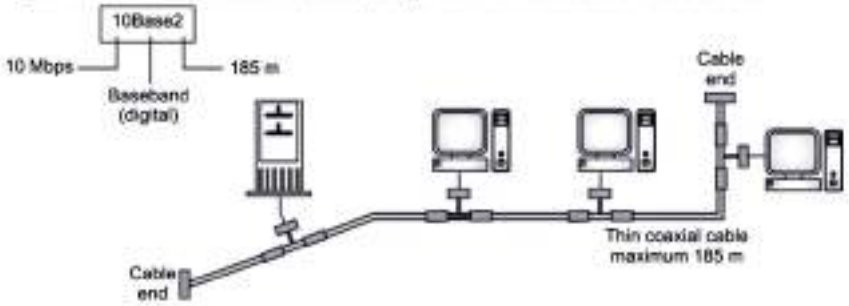


Fig. 4.15: 10Base2-T implementation

c. 10Base-T: Twisted-Pair Ethernet

- The third implementation is called 10Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable.

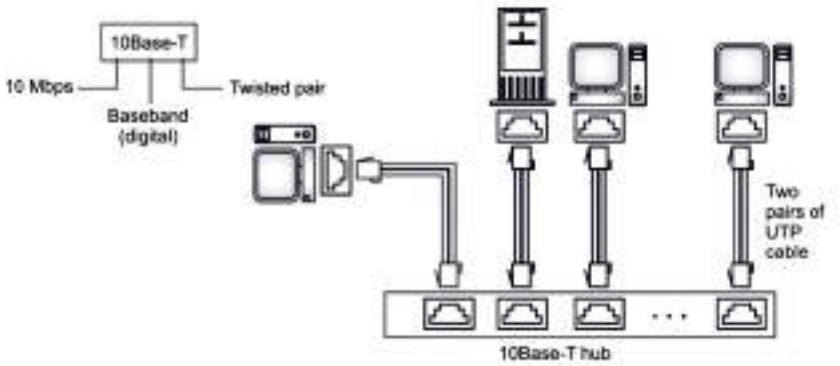


Fig. 4.16: 10Base-T implementation

- Note that two pairs of twisted cable create two paths between the station and the hub. Any collision here happens in the hub. Compared to 10Base5 or 10Base2, we can see that the hub actually replaces the coaxial cable as far as a collision is concerned. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.

d. 10Base-F: Fiber Ethernet

- Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-F. 10Base-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables

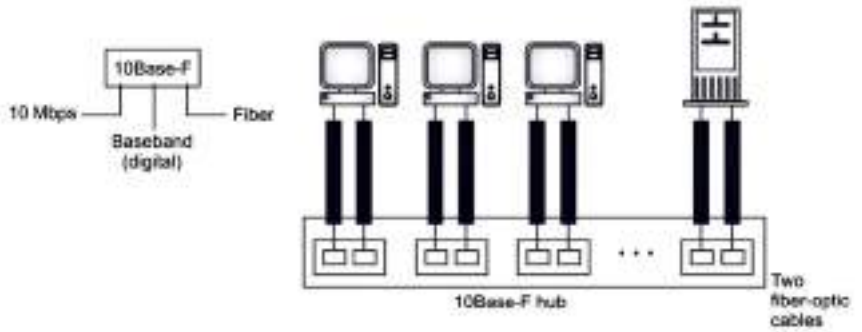


Fig. 4.17: 10Base-F: Fiber Ethernet

4.3 FAST ETHERNET (S-18)

Goals:

- The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

Topology

- Fast Ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center.

Implementations:

- There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

- Network managers who want to incorporate Fast Ethernet into an existing configuration are required to make many decisions. The number of users in each site on the network that need the higher throughput must be determined; which segments of the backbone need to be reconfigured specifically for 100BASE-T; plus what hardware is necessary in order to connect the 100BASE-T segments with existing 10BASE-T segments. Gigabit Ethernet is a future technology that promises a migration path beyond Fast Ethernet so the next generation of networks.
- Increasing the Ethernet transmission rate by a factor of ten over 10Base-T was not a simple task and the effort resulted in the development of three separate physical layer standards for 100 Mbps over UTP cable: 100Base-TX and 100Base-T4 in 1995 and 100Base-T2 in 1997. Each was defined with different encoding requirements and a different set of media-dependent sublayers, even though there is some overlap in the link cabling. Table compares the physical layer characteristics of 10Base-T to the various 100Base versions.

Table 4.1: Summary of 100Base-T Physical Layer Characteristics

Ethernet Version	Transmit Symbol Rate*	Encoding	Cabling	Full-Duplex Operation
10Base-T	10 MBd	Manchester	Two pairs of UTP Category -3 or better	Supported
100Base-TX	125 MBd	4B/5B	Two pairs of UTP Category -5 or Type 1 STP	Supported
100Base-T4	33 MBd	8B/6T	Four pairs of UTP Category -3 or better	Not supported
100Base-T2	25 MBd	PAM5x5	Two pairs of UTP Category -3 or better	Supported

[* One baud = One transmitted symbol per second, where the transmitted symbol may contain the equivalent value of 1 or more binary bits.]

- Although not all three 100-Mbps versions were successful in the marketplace, all three have been discussed in the literature and all three did impact future designs. As such, all three are important to consider here.

1. 100Base-X:

- 100Base-X was designed to support transmission over either two pairs of Category 5 UTP copper wire or two strands of optical fiber. Although the encoding, decoding and clock recovery procedures are the same for both media, the signal transmission is different—electrical pulses in copper and light pulses in optical fiber.

- The 100Base-X encoding procedure is based on the earlier FDDI optical fiber physical media-dependent and FDDI/CDDI copper twisted-pair physical media-dependent signaling standards developed by ISO and ANSI. The 100Base-TX physical media-dependent sublayer (TP-PMD) was implemented with CDDI semiconductor transceivers and RJ-45 connectors; the fiber PMD was implemented with FDDI optical transceivers and the Low Cost Fiber Interface Connector (commonly called the duplex SC connector).
- The 4B/5B encoding procedure is the same as the encoding procedure used by FDDI, with only minor adaptations to accommodate Ethernet frame control. Each 4-bit data nibble (representing half of a data byte) is mapped into a 5-bit binary code-group that is transmitted bit-serial over the link.

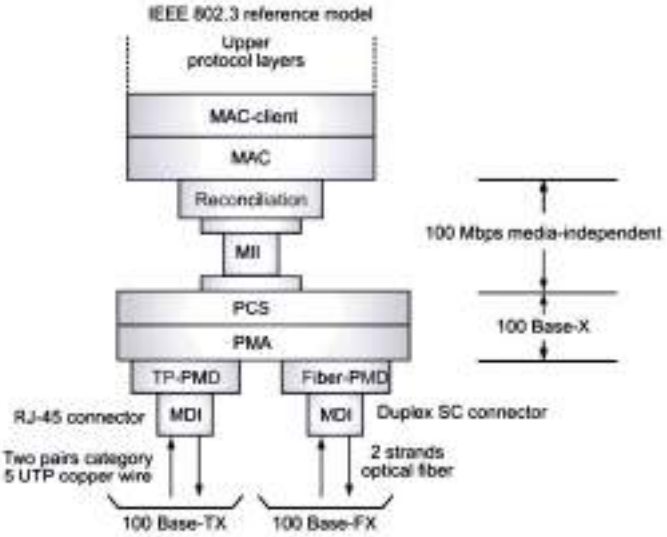


Fig. 4.18: The 100Base-X Logical Model

- The expanded code space provided by the 32 5-bit code-groups allow separate assignment for the following:
- The 16 possible values in a 4-bit data nibble (16 code-groups).
- Four control code-groups that are transmitted as code-group pairs to indicate the Start-of-Stream Delimiter (SSD) and the End-of-Stream Delimiter (ESD). Each MAC frame is "encapsulated" to mark both the beginning and end of the frame. The first

byte of preamble is replaced with SSD code-group pair that precisely identifies the frame's code-group boundaries. The ESD code-group pair is appended after the frame's FCS field.

- A special IDLE code-group that is continuously sent during interframe gaps to maintain continuous synchronization between the NICs at each end of the link. The receipt of IDLE is interpreted to mean that the link is quiet.
- Eleven invalid code-groups that are not intentionally transmitted by a NIC (although one is used by a repeater to propagate receive errors). Receipt of any invalid code-group will cause the incoming frame to be treated as an invalid frame.

MAC Sublayer:

- Fig. 4. 19 show how a MAC frame is encapsulated before being transmitted as a 100Base-X code-group stream.
- 100Base-TX transmits and receives on the same link pairs and uses the same pin assignments on the MDI as 10Base-T. 100Base-TX and 100Base-FX both support half-duplex and full-duplex transmission.

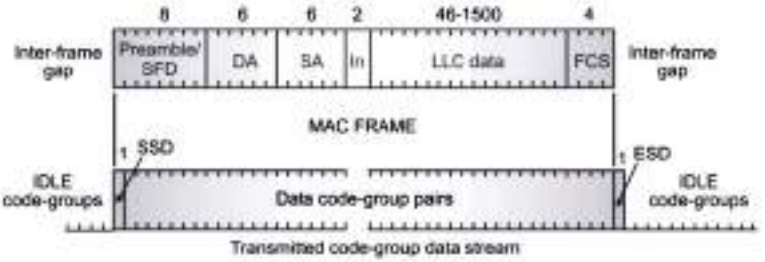


Fig. 4.19: The 100Base-X Code-Group Stream with Frame Encapsulation

2. 100Base-T4:

- 100Base-T4 was developed to allow 10BaseT networks to be upgraded to 100-Mbps operation without requiring existing four-pair Category 3 UTP cables to be replaced with the newer Category 5 cables. Two of the four pairs are configured for half-duplex operation and can support transmission in either direction, but only in one direction at a time. The other two pairs are configured as simplex pairs dedicated to transmission in one direction only. Frame transmission uses both half-duplex pairs, plus the simplex pair that is appropriate for the transmission direction, as shown in Fig. 4.20. The simplex pair for the opposite direction provides carrier sense and collision detection. Full-duplex operation cannot be supported on 100Base-T4.

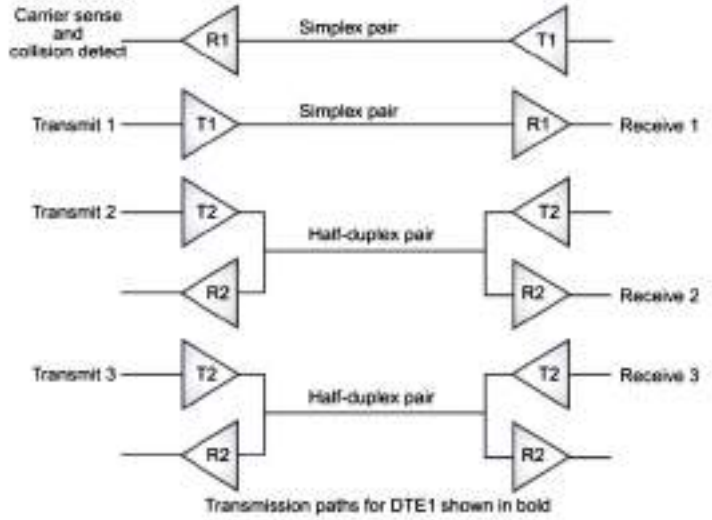


Fig. 4.20: The 100Base-T4 Wire-Pair Usage during Frame Transmission

- 100Base-T4 uses an 8B6T encoding scheme in which each 8-bit binary byte is mapped into a pattern of six ternary (three-levels: +1, 0, –1) symbols known as 6T code-groups. Separate 6T code-groups are used for IDLE and for the control code-groups that are necessary for frame transmission. IDLE received on the dedicated receive pair indicates that the link is quiet.

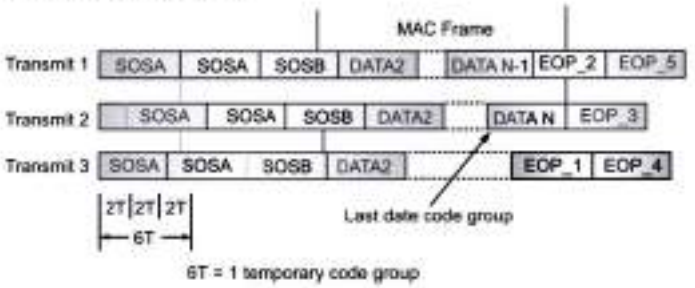


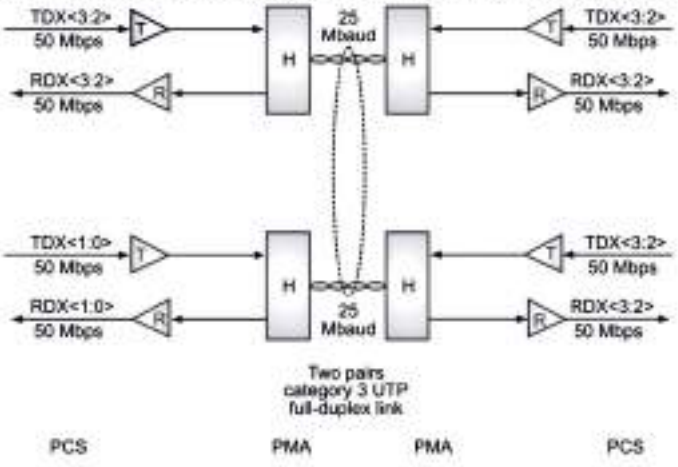
Fig. 4.21: The 100Base-T4 Frame Transmission Sequence

- During frame transmission, 6T data code-groups are transmitted in a delayed round-robin sequence over the three transmit wire-pairs, as shown in Fig. 4.22.
- Each frame is encapsulated with start-of-stream and end-of-packet 6T code-groups that mark both the beginning and end of the frame and the beginning and end of the

6T code-group stream on each wire pair. Receipt of a non-IDLE code-group over the dedicated receive-pair any time before the collision window expires indicates that a collision has occurred.

3. 100Base-T2:

- The 100Base-T2 specification was developed as a better alternative for upgrading networks with installed Category 3 cabling than was being provided by 100Base-T4. Two important new goals were defined:
  - To provide communication over two pairs of Category 3 or better cable.
  - To support both half-duplex and full-duplex operation.
- 100Base-T2 uses a different signal transmission procedure than any previous twisted-pair Ethernet implementations. Instead of using two simplex links to form one full-duplex link, the 100Base-T2 dual-duplex baseband transmission method sends encoded symbols simultaneously in both directions on both wire pairs. The term "TDX<3:2>" indicates the 2 most significant bits in the nibble before encoding and transmission. "RDX<3:2>" indicates the same 2 bits after receipt and decoding.



H = Hybrid canceller transceiver
T = Transmit encoder
R = Receive decoder
Two PAM5 code symbols = one nibble

Fig. 4.22: The 100Base-T2 Link Topology

- Dual-duplex baseband transmission requires the NIC's at each end of the link to be operated in a master/slave loop-timing mode. Which NIC will be master and which will be slave is determined by auto negotiation during link initiation. When the link is

operational, synchronization is based on the master NIC's internal transmit clock. The slave NIC uses the recovered clock for both transmit and receive operations, as shown in Fig. 4.22. Each transmitted frame is encapsulated, and link synchronization is maintained with a continuous stream of IDLE symbols during interframe gaps.

- The 100Base-T2 encoding process first scrambles the data frame nibbles to randomize the bit sequence. It then maps the two upper bits and the two lower bits of each nibble into two five-level (+2, +1, 0, −1, −2) pulse amplitude-modulated (PAM5) symbols that are simultaneously transmitted over the two wire pairs (PAM5x5). Different scrambling procedures for master and slave transmissions ensure that the data streams travelling in opposite directions on the same wire pair are uncoordinated.
- Signal reception is essentially the reverse of signal transmission. Because the signal on each wire pair at the MDI is the sum of the transmitted signal and the received signal, each receiver subtracts the transmitted symbols from the signal received at the MDI to recover the symbols in the incoming data stream. The incoming symbol pair is then decoded, unscrambled and reconstituted as a data nibble for transfer to the MAC.

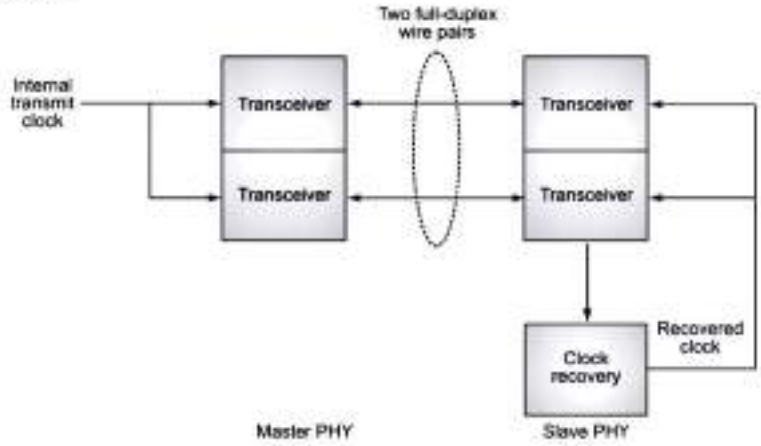


Fig. 4.23: The 100Base-T2 Link Topology

4.4 GIGABIT ETHERNET

- Since, its inception at Xerox Corporation in the early 1970's, Ethernet has been the dominant networking protocol. Of all current networking protocols, Ethernet has, by far, the highest number of installed ports and provides the greatest cost performance relative to Token Ring, Fiber Distributed Data Interface (FDDI) and Asynchronous Transfer Mode (ATM) for desktop connectivity. Fast Ethernet, which increased

Ethernet speed from 10 to 100 megabits per second (Mbps), provided a simple, cost-effective option for backbone and server connectivity.

- Gigabit Ethernet builds on top of the Ethernet protocol, but increases speed tenfold over Fast Ethernet to 1000 Mbps or 1 gigabit per second (Gbps). This protocol, which was standardized in June 1998, promises to be a dominant player in high-speed local area network backbones and server connectivity. Since, Gigabit Ethernet significantly leverages on Ethernet, customers will be able to leverage their existing knowledge base to manage and maintain gigabit networks.
- Gigabit Ethernet design can be summarized as follows:
  1. Upgrade the data rate to 1 Gbps.
  2. Make it compatible with Standard or Fast Ethernet.
  3. Use the same 48-bit address.
  4. Use the same frame format.
  5. Keep the same minimum and maximum frame lengths.
  6. To support autonegotiation as defined as Fast Ethernet.

4.4.1 Gigabit Ethernet Protocol Architecture

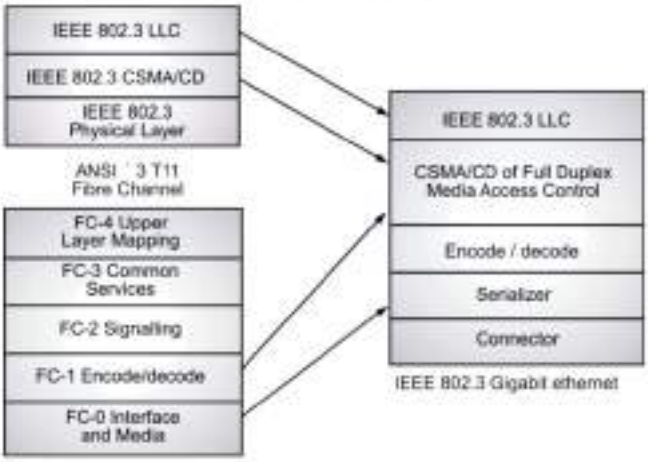


Fig. 4.24: Gigabit Ethernet Protocol Stack

- In order to accelerate speeds from 100 Mbps Fast Ethernet up to 1 Gbps, several changes need to be made to the physical interface. It has been decided that Gigabit Ethernet will look identical to Ethernet from the data link layer upward. The challenges involved in accelerating to 1 Gbps have been resolved by merging two technologies together: IEEE 802.3 Ethernet and ANSI X3T11 Fiber Channel. Fig. 4.25

shows how key components from each technology have been leveraged to form Gigabit Ethernet.

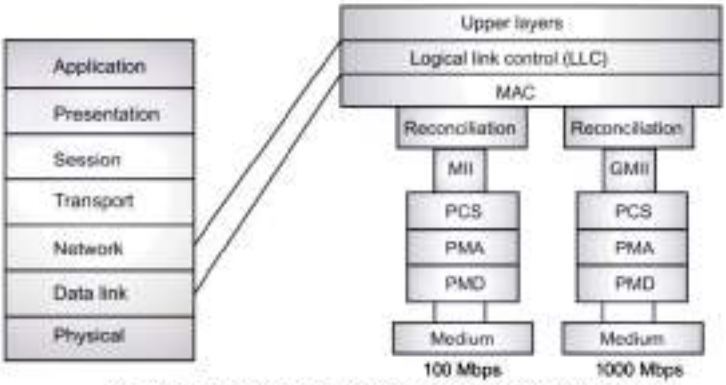


Fig. 4.25: Architectural Model of IEEE 802.3z Gigabit Ethernet

- Leveraging these two technologies means that the standard can take advantage of the existing high-speed physical interface technology of Fiber Channel while maintaining the IEEE 802.3 Ethernet frame format, backward compatibility for installed media and use of full- or half-duplex Carrier Sense Multiple Access with Collision Detect (CSMA/CD). This scenario helps minimize the technology complexity, resulting in a stable technology that can be quickly developed.

4.4.2 Topology

- Gigabit Ethernet is designed to connect two or more stations. If there are only two stations, they can be connected point to point. Three or more stations need to be connected in a star topology with a hub or a switch at the center. Another possible configuration is to connect several star topologies or let a star topology be part of another as shown in Fig. 4.26.

4.4.3 Implementation

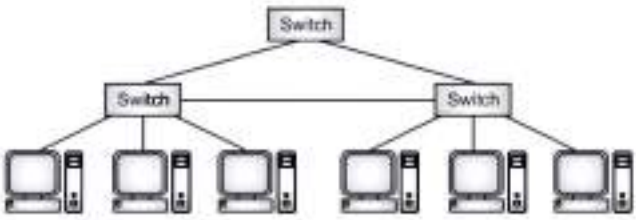


Fig.4.26: Hierarchy of stars

- Gigabit Ethernet can be classified as either a two-wire or a four-wire implementation. The two-wire implementation use fiber-optic cable (1000Base-SX, short-wave, or 1000Base-LX, long-wave), or STP (1000Base-CX). The four-wire version uses category 5 twisted-pair cable (1000Base-T).
- Fig. 4.27 shows the physical implementation.

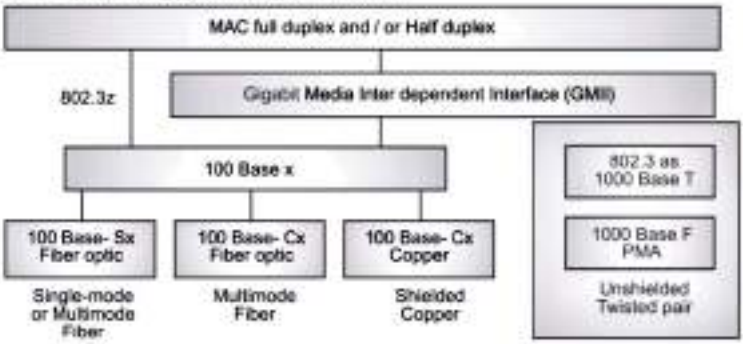


Fig. 4.27: 802.3z and 802.3ab Physical Layouts

1. Gigabit Ethernet Interface Carrier:

- The Gigabit interface converter (GBIC) allows network managers to configure each gigabit port on a port-by-port basis for short-wave (SX), long-wave (LX), long-haul (LH) and copper physical interfaces (CX).
- LH GBICs extended the single-mode fiber distance from the standard 5 km to 10 km. Cisco views LH as a value add, although it's not part of the 802.3z standard, allowing switch vendors to build a single physical switch or switch module that the customer can configure for the required laser/fiber topology.
- As stated earlier, Gigabit Ethernet initially supports three key media: short-wave laser, long-wave laser, and short copper. In addition, fiber- optic cable comes in three types: Multimode (62.5 μm), multimode (50 μm), and Single mode. A diagram for the GBIC is shown in Fig. 4.28.
- The Fiber Channel Physical Medium Dependent (PMD) specification currently allows for 1.062-gigabaud signaling in full duplex. Gigabit Ethernet will increase this signaling rate to 1.25 Gbps. The 8B/10B encoding (to be discussed later) allows a data transmission rate of 1000 Mbps. The current connector type for Fiber Channel and therefore for Gigabit Ethernet, is the SC connector for both single-mode and multimode fiber.
- The Gigabit Ethernet specification calls for media support for multimode fiber-optic cable, single-mode fiber-optic cable and a special balanced shielded 150-ohm copper cable.

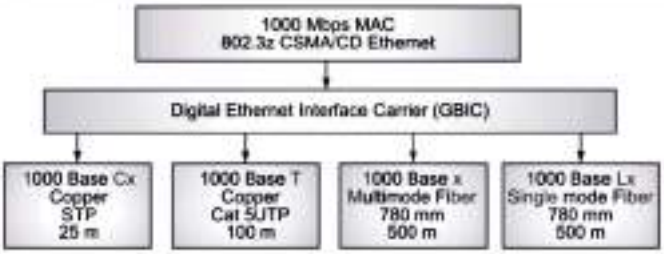


Fig. 4.28: Function of the GBIC Interface

- In contrast, Gigabit Ethernet switches without GBICs either cannot support other lasers or need to be ordered customized to the laser types required.

2. Long-Wave and Short-Wave Lasers over Fiber-Optic Media:

- Two laser standards will be supported over fiber: 1000BaseSX (short-wave laser) and 1000BaseLX (long-wave laser). Short- and long-wave lasers will be supported over multimode fiber.
- Two types of multimode fiber are available: 62.5 and 50 micron-diameter fibers. Long-wave lasers will be used for single-mode fiber, because this fiber is optimized for long-wave laser transmission. There is no support for short-wave laser over single-mode fiber.
- The key differences between the use of long and short-wave laser technologies are cost and distance.
- Lasers over fiber-optic cable take advantage of variations in attenuation in a cable. At different wavelengths, "dips" in attenuation are found over the cable. Short and long-wave lasers take advantage of those dips and illuminate the cable at different wavelengths.
- Short-wave lasers are readily available because variations of these lasers are used in compact-disc technology. Long-wave lasers take advantage of attenuation dips at longer wavelengths in the cable. The net result is that although short-wave lasers will cost less, they transverse a shorter distance. In contrast, long-wave lasers are more expensive but these transverse longer distances.
- Single-mode fiber has been traditionally used in the networking cable plants to achieve long distance. In Ethernet, for example, single-mode cable ranges reach up to 10 km. Single-mode fiber, using a 9-micron core and 1300-nanometer laser, demonstrate the highest-distance technology. The small core and lower-energy laser elongate the wavelength of the laser and allow it to transverse greater distances. This setup enables single-mode fiber to reach the greatest distances of all media with the least reduction in noise.

- Gigabit Ethernet will be supported over two types of multimode fiber: 62.5 and 50 micron-diameter fibers.
- The 62.5-micron fiber is typically seen in vertical campus and building cable plants and has been used for Ethernet, Fast Ethernet and FDDI backbone traffic. This type of fiber, however, has a lower modal bandwidth (the ability of the cable to transmit light), especially with short-wave lasers. In other words, short-wave lasers over 62.5-micron fiber will be able to transverse shorter distances than long-wave lasers.
- Relative to 62.5-micron fiber, the 50-micron fiber has significantly better model bandwidth characteristics and will be able to transverse longer distances with short-wave lasers.

3. 150-Ohm Balanced Shielded Copper Cable (1000BaseCX):

- For shorter cable runs (of 25 meters or less), Gigabit Ethernet will allow transmission over a special balanced 150-ohm cable. This is a new type of shielded cable; it is not unshielded twisted-pair (UTP) or IBM Type I or II.
- In order to minimize safety and interference concerns caused by voltage differences, both transmitters and receivers will share a common ground. The return loss for each connector is limited to 20 dB to minimize transmission distortions. The connector type for 1000BaseCX will be a DB-9 connector. A new connector is being developed by AMP called the HSSDC.

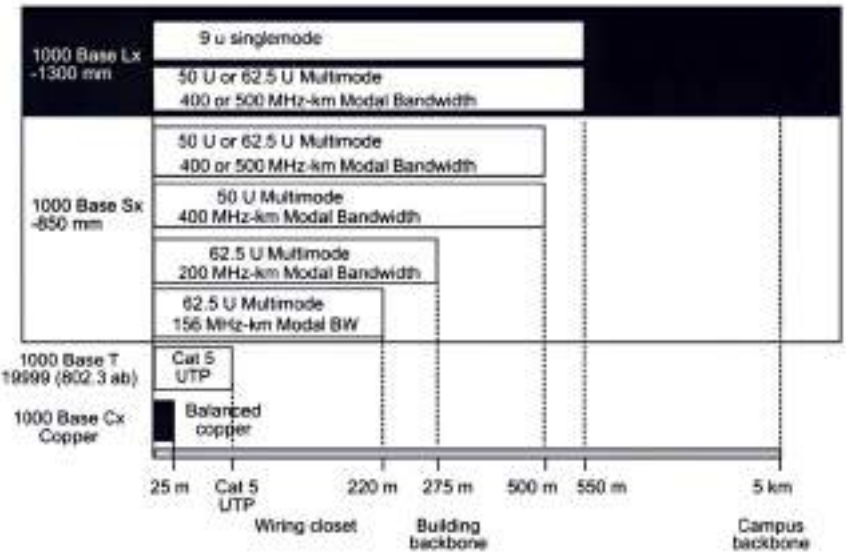


Fig. 4.29: 802.3z and 802.3ab Distance Chart

- The application for this type of cabling will be short-haul data-center interconnections and inter- or intra-rack connections. Because of the distance limitation of 25 meters, this cable will not work for interconnecting data centers to riser closets.
- The distances for the media supported under the IEEE 802.3z standard are shown in Fig. 4.29.

Serializer/Deserializer :

- The Physical Media Attachment (PMA) sublayer for Gigabit Ethernet is identical to the PMA for Fiber Channel. The Serializer/deserializer is responsible for supporting multiple encoding schemes and allowing presentation of those encoding schemes to the upper layers. Data entering the physical sublayer (PHY) will enter through the PMD and will need to support the encoding scheme appropriate to that media. The encoding scheme for Fiber Channel is 8B/10B, designed specifically for fiber-optic cable transmission. Gigabit Ethernet uses a similar encoding scheme.
- The difference between Fiber Channel and Gigabit Ethernet, however, is that Fiber Channel utilizes 1.062-gigabaud signaling whereas Gigabit Ethernet utilizes 1.25-gigabaud signaling. A different encoding scheme will be required for transmission over UTP. This encoding will be performed by the UTP or 1000BaseT PHY.

8B/10B Encoding :

- The Fiber Channel FC-1 layer describes the synchronization and the 8B/10B encoding scheme. FC-1 defines the transmission protocol, including serial encoding and decoding to and from the physical layer, special characters, and error control.
- Gigabit Ethernet utilizes the same encoding/decoding as specified in the FC-1 layer of Fiber Channel. The scheme utilized is the 8B/10B encoding. This scheme is similar to the 4B/5B encoding used in FDDI; however, 4B/5B encoding was rejected for Fiber Channel because of its lack of DC balance. The lack of DC balance can potentially result in data-dependent heating of lasers because a transmitter sends more 1's than 0's, resulting in higher error rates.
- Encoding data transmitted at high speeds provides some advantages:
  - Encoding limits the effective transmission characteristics, such as ratio of 1's to 0's, on the error rate.
  - Bit-level clock recovery of the receiver can be greatly improved by using data encoding.
  - Encoding increases the possibility that the receiving station can detect and correct transmission or reception errors
  - Encoding can help distinguish data bits from control bits
- All these features have been incorporated into the Fiber channel FC-1 specification.
- In Gigabit Ethernet, the FC-1 layer takes decoded data from the FC-2 layer 8 bits at a time from the reconciliation sublayer (RS), which "bridges" the Fiber Channel physical

interface to the IEEE 802.3 Ethernet upper layers. Encoding takes place via an 8- to 10-bit character mapping. Decoded data comprises 8 bits with a control variable. This information is, in turn, encoded into a 10-bit transmission character.

- Encoding is accomplished by providing each transmission character with a name, denoted as Zxx.y. Z is the control variable that can have two values: D for Data and K for Special Character. The xx designation is the decimal value of the binary number composed of a subset of the decoded bits. The y designation is the decimal value of the binary number of remaining decoded bits. This scenario implies that there are 256 possibilities for Data (D designation) and 256 possibilities for Special Characters (K designation). However, only 12 Kxx.y values are valid transmission characters in Fiber Channel. When data is received, the transmission character is decoded into one of the 256 8-bit combinations.

4.4.4 MAC Sublayer

(S-18, W-18)

- Gigabit Ethernet has two approaches for medium access: half duplex and full-duplex.

1. **Full Duplex Mode:**

- In the full duplex mode, there is a centre switch connected to the all computer or other switches. In this mode, each switch as buffers for each input port in which data are stored until they transmitted. There is no collision in this mode, as we discussed before. This means that CSMA/CD is not used. Lack of collision implies that the maximum length of the cable is determined by the signal attenuation in the cable, not by the collision detection process.

2. **Half-Duplex Mode:**

- Gigabit Ethernet can also be used in half-duplex mode, although it is rare. In this case, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur. The half-duplex approach uses CSMA/CD. However, as we saw before, the maximum length of the network in this approach is totally dependent on the minimum frame size. Three methods have been defined: Traditional, carrier extension, and frame bursting.

4.4.5 Ethernet Frame Format

(S-18, 19)

- Gigabit Ethernet has been designed to adhere to the standard Ethernet frame format. This setup maintains compatibility with the installed base of Ethernet and Fast Ethernet products, requiring no frame translation. Fig. 4.30 describes the IEEE 802.3/Ethernet frame format.
- The original Xerox specification identified a *type* field, which was utilized for protocol identification. The IEEE 802.3 specification eliminated the *type* field, replacing it with the *length* field. The *length* field is used to identify the length in bytes of the data field. The protocol type in 802.3 frames are left to the data portion of the packet.

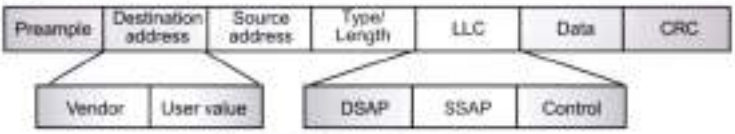


Fig. 4.30: Ethernet Frame Format

- The Logical Link Control (LLC) is responsible for providing services to the network layer regardless of media type, such as FDDI, Ethernet, Token Ring, and so on. The LLC layer makes use of LLC Protocol Data Units (PDUs) in order to communicate between the Media Access Control (MAC) layer and the upper layers of the protocol stack.
- The LLC layer uses three variables to determine access into the upper layers via the LLC-PDU. Those addresses are the destination service access point (DSAP), source service access point (SSAP), and control variable.
- The DSAP address specifies a unique identifier within the station providing protocol information for the upper layer; the SSAP provides the same information for the source address.
- The LLC defines service access for protocols that conform to the Open System Interconnection (OSI) model for network protocols. Unfortunately, many protocols do not obey the rules for those layers. Therefore, additional information must be added to the LLC in order to provide information regarding those protocols. Protocols that fall into this category include IP and IPX.
- The method used to provide this additional protocol information is called a Subnetwork Access Protocol, or SNAP frame. A SNAP encapsulation is indicated by the SSAP and DSAP addresses being set to "0 x AA". When that address is seen, we know that a SNAP header follows. The SNAP header is 5 bytes long: the first 3 bytes consist of the organization code, which is assigned by the IEEE; the second 2 bytes use the type value set from the original Ethernet specifications.

4.5 TEN-GIGATBIT ETHERNET – GOALS, MAC SUBLAYER, PHYSICAL LAYER

10 Gigabit Ethernet

- Gigabit Ethernet (10GE, 10GbE, or 10 GigE) is a group of computer networking technologies for transmitting Ethernet frames at a rate of 10 gigabits per second. It was first defined by the IEEE 802.3ae-2002 standard.
- Gigabit Ethernet is the fastest and most recent of the Ethernet standards. This Ethernet is defined only for full-duplex operation which does not use CSMA/CD.

Standards:

- IEEE 802.3ae and IEEE 802.aq: define 10Gb/s for fiber media. IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbit/s that makes it 10 times faster than Gigabit Ethernet.

- IEEE 802.3ak and IEEE 802.an: 10Gb/s over copper cables.

Goals:

1. Upgrade the data rate of 10 Gbps.
2. Make it compatible with Standard, Fast and Gigabit Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
7. Make Ethernet compatible with technologies such as Frame Relay and ATM.

MAC Sublayer

- Ten-Gigabit Ethernet operates only in full duplex mode which means there is no need for connection; CSMA/CD is not used in Ten-Gigabit Ethernet.

Physical Layer

- The physical layer in Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances. Three implementations are the most common: 10GBase-S, 10GBase-L, and 10GBase-E. Table 4.2 shows a summary of the Ten-Gigabit Ethernet implementations.

Table 4.2: Summary of Ten-Gigabit Ethernet Implementations

Characteristics	10GBase-S	10GBase-L	10GBase-E
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-nm single mode
Maximum length	300 m	10 km	40km

4.6 BACKBONE NETWORK

- Backbone is most important part of a system which provides the central support to the rest system, for example backbone of a human body that balance and hold all the body parts. Similarly in Computer Networks a **Backbone Network** is as a Network containing a high capacity connectivity infrastructure that backbone to the different part of the network.
- Actually a backbone network allows multiple LANs to get connected in a backbone network, not a single station is directly connected to the backbone but the stations are part of LAN, and backbone connects those LANs.

Backbone LANs:

- Because of increasing use of distributed applications and PCs, a new flexible strategy for LANs has been introduced. If a premises wide data communication system is to be

supported then we need a networking system which can span over the required distance and which capable of interconnecting all the equipment in a single building or in a group of buildings.

- It is possible to develop a single LAN for this purpose but practically this scheme faces the following drawbacks:

1. **Poor Reliability:**

- With a single LAN, the reliability will be poor since a service interruption even for a short duration can cause major problem to the user.

2. **Capacity:**

- There is a possibility that a single LAN may be saturated due to increase in number of devices beyond a certain number.

3. **Cost:**

- A single LAN can not give its optimum performance for the diverse requirements of communication and interconnection.
- So the alternative for using a single LAN is to use low cost low capacity LANs in each building or department and then interconnection all these LANs with high capacity LAN. Such network is called as Backbone LAN. The backbone network allows several LANs to be connected. In the backbone network, no station is directly connected with backbone, instead each station is a part of LAN, and the LANs are connected to the backbone.
- The backbone itself is a LAN, it uses a LAN protocol such as ethernet, hence each connection in the backbone is itself another LAN.

Type of Backbone Architectures:

- The two very common used architectures are: Bus backbone, Star backbone. These are explained as following below.

1. **Bus Backbone:**

- In Bus backbone the topology used for the backbone is bus topology.

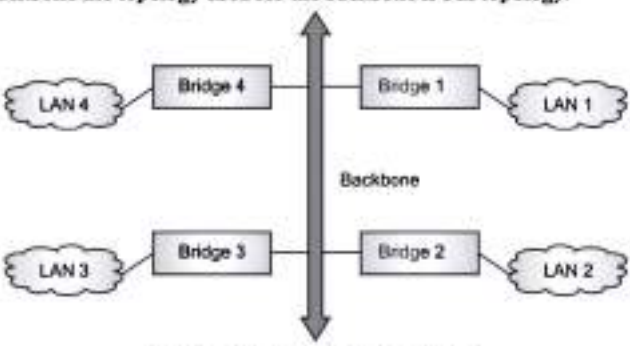


Fig. 4.31: Structure of a Bus backbone

- In above the Bus backbone structure is used as a distribution backbone for connecting different buildings in an organization. Each building may have either a single LAN or another backbone which comes in star backbone. The structure is a bridge based (bridge is the connecting device) backbone with four LANs.

Working:

- In above structure if a station in LAN 2 wants to send a frame to some other station in Same LAN then Bridge 2 will not allow the frame to pass to any other LAN, hence this frame will not reach the backbone. If a station from LAN 1 wants to send a frame to a station in LAN 4 then Bridge 1 passes this frame to the backbone. This frame is then received by Bridge 4 and delivered to the destination.

2. Star Backbone:

- The topology of this backbone is star topology.

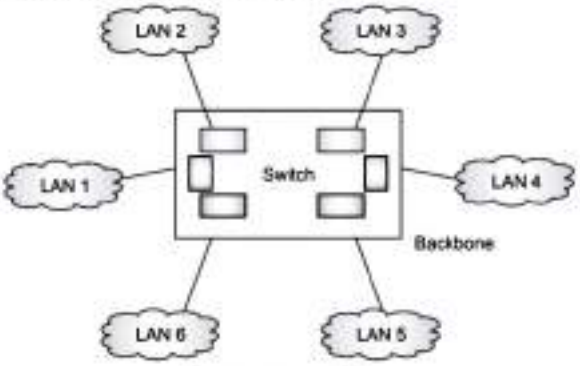


Fig. 4.32: Star Backbone

- Above figure shows the Star backbone in this configuration, the backbone is simply a switch which is used to connect various LANs. The switch does the job of backbone and connects the LANs as well. These types of backbone are basically used as distribution backbone inside a building.
- There is one more category of backbone network is Interconnecting of Remote LANs:

3. Interconnection of Remote control:

- In this type of backbone network the connection are done through the bridge called remote bridges which acts as connecting devices in connect LANs as point to point network link.
- Example of point to point networks is leased telephone lines or ADLS lines. Such a point to point network can be considered as being equivalent to a LAN without stations.

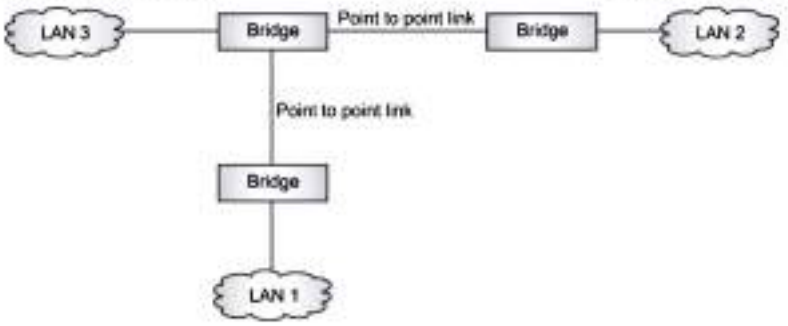
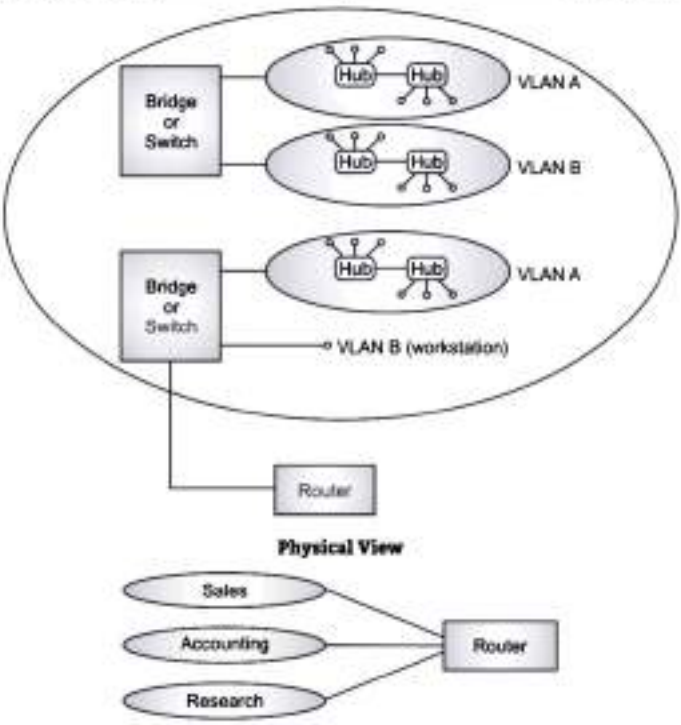


Fig. 4.33: Connecting remote LANs to each other

4.7 VIRTUAL LAN

- In a traditional LAN, workstations are connected to each other by means of a hub or a repeater. These devices propagate any incoming data throughout the network. However, if two people attempt to send information at the same time, a collision will occur and all the transmitted data will be lost. Once the collision has occurred, it will continue to be propagated throughout the network by hubs and repeaters.
- The workstations, hubs, and repeaters together form a LAN segment. A LAN segment is also known as a collision domain since collisions remain within the segment. The area within which broadcasts and multicasts are confined is called a broadcast domain or LAN. Thus a LAN can consist of one or more LAN segments. Defining broadcast and collision domains in a LAN depends on how the workstations, hubs, switches, and routers are physically connected together. This means that everyone on a LAN must be located in the same area.
- VLAN's allow a network manager to logically segment a LAN into different broadcast domains (see Figure 4.34). Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together. Users on different floors of the same building, or even in different buildings can now belong to the same LAN.
- VLAN's also allow broadcast domains to be defined without using routers. Bridging software is used instead to define which workstations are to be included in the broadcast domain. Routers would only have to be used to communicate between two VLAN's.
- Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network.



Physical View

Logical View

Fig. 4.34: Physical and logical view of a VLAN

- Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges. This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.

Features of VLANs:

- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.

- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.
- VLANs help large organizations to re-partition devices aiming improved traffic management.
- VLANs also provide better security management allowing partitioning of devices according to their security criteria and also by ensuring a higher degree of control connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections. This aids is quicker and cheaper reconfiguration of devices when the logical partitioning needs to be changed.

Types of VLANs:

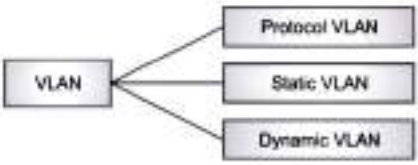


Fig. 4.35: Types of VLANs

- **Protocol VLAN** – Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames the come to it based upon the traffics protocol.
- **Port-based VLAN** – This is also called static VLAN. Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.
- **Dynamic VLAN** – Here, the network administrator simply defines network membership according to device characteristics.

Difference between LAN and VLAN:

Sr. No.	LAN	VLAN
1.	LAN stands for Local Area Network.	VLAN stands for Virtual Local Area Network.
2.	The cost of Local Area Network is high.	The cost of Virtual Local Area Network is less.
3.	The latency of Local Area Network is high.	The latency of Virtual Local Area Network is low.

Contd..

4.	The devices which are used in LAN are: Hubs, Routers and switch.	The devices which are used in VLAN are: Bridges and switch.
5.	In local area network, the Packet is advertised to each device.	In virtual local area network, packet is send to specific broadcast domain.
6.	Local area network is less efficient than virtual local area network.	Virtual local area network is greater efficient than local area network.

4.8 WIRELESS LAN

- A wireless LAN or WLAN is the linking of two or more computers or devices using spread-spectrum or OFDM modulation technology based to enable communication between devices in a limited area.
- This gives users the mobility to move around within a broad coverage area and still be connected to the network.
- For the home user, wireless has become popular due to ease of installation, and location freedom with the gaining popularity of laptops.
- Public businesses such as malls have begun to offer wireless access to their customers; some are even provided as a free service.
- Large wireless network projects are being put up in many major cities.

Need of wireless LAN:

- An increasing number of LAN users are becoming mobile. These mobile users require that they should be connected to the network regardless of where they are because they want simultaneous access to the network. This makes the use of cables, or wired LANs, impractical if not impossible.
- Wireless LANs are very easy to install. There is no requirement for wiring every workstation and every room. This ease of installation makes wireless LANs inherently flexible.
- If a workstation must be moved, it can be done easily and without additional wiring, cable drops or reconfiguration of the network.
- Another advantage is its portability. If a company moves to a new location, the wireless system is much easier to move than ripping up all of the cables that a wired system would have snaked throughout the building.
- Most of these advantages also translate into budgetary savings.

Fig. 4.36: Wireless LAN

- Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs.
- Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected.
- For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.
- Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

Objectives of Wireless LAN:

- Objectives of wireless LAN includes:
  1. **Convenience:** The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (home or office). With the increasing saturation of laptop-style computers, this is particularly relevant.
  2. **Mobility:** With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.
  3. **Productivity:** Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location. For example, a hospital or warehouse may implement Voice over WLAN applications that enable mobility and cost savings.
  4. **Deployment:** Initial setup of an infrastructure-based wireless network requires little more than a single access point. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building).
  5. **Expandability:** Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring.
  6. **Cost:** Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables.

Design goals of Wireless LAN:

- Design goals of Wireless LAN are listed below:
  1. **Global operation:** LAN equipment may be carried from one country to another and this operation should be legal, (frequency regulations national and international).
  2. **Low power:** Take into account that devices communicating via WLAN are typically running on battery power. Specially,power saving modes and power management functions.
  3. **Protection of investment:** A lot of money has been invested for Wired LANs, WLANs should be able to interoperate with existing network, (same data type and services).
  4. **Safety and Security:** Safe to operate. Encryption mechanism, do not allow roaming profiles for tracking people, (privacy).
  5. **Transparency for applications:** Existing applications should continue to work.
  6. **Simplified spontaneous co-operation:** No complicated setup routines but operate spontaneously after power.
  7. **Easy to use:** WLANs are made for simple users, they should not require complex management but rather work on a plug-and-play basis.

4.8.1 How Wireless LAN Works?

- Wireless LAN (WLAN) uses electromagnetic airwaves (radio and infrared) to communicate information from one point to another without relying on any physical connection.
- Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver.
- The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end.
- This is generally referred to as modulation of the carrier by the information being transmitted.
- Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier.

4.8.2 Advantages of Wireless LAN

- Wireless LAN offer the following productivity, service, convenience and cost advantages over traditional wired networks:

1. **Mobility improves productivity and Service:** Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
2. **Installation Speed and Simplicity:** Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
3. **Installation Flexibility:** Wireless technology allows the network to go where wire cannot go.
4. **Reduced Cost-of-Ownership:** While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, adds and changes.
5. **Scalability:** Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from independent networks suitable for a small number of users to full infrastructure networks of thousands of users that allow roaming over a broad area.
6. **Planning:** Wireless ad hoc networks allow for communication without planning. Wired networks need wiring plans.
7. **Robustness:** Wireless networks can survive disasters, if the wireless devices survive people can still communicate.

4.8.3 Disadvantages of Wireless LAN

- Wireless LAN technology, while replete with the conveniences and advantages described above, has its share of downfalls.
- For a given networking situation, wireless LANs may not be desirable for a number of reasons.
- Most of these have to do with the inherent limitations of the technology.

1. **Reliability:** Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects that are beyond the control of the network administrator. One of the most insidious problems that can affect the stability and reliability of a wireless LAN is the microwave oven. In the case of typical networks, modulation is achieved by complicated forms of Phase-Shift Keying (PSK) or Quadrature Amplitude Modulation (QAM), making interference and propagation effects all the more disturbing. As a result, important network resources such as servers are rarely connected wirelessly.

2. **Range:** The typical range of a common 802.11g network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient in a larger structure. To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly. Other technologies are in the development phase, however, which feature increased range, hoping to render this disadvantage irrelevant.
3. **Speed:** The speed on most wireless networks (typically 1-108 Mbit/s) is reasonably slow compared to the slowest common wired. There are also performance issues caused by TCP and its built-in congestion avoidance. For most users, however, this observation is irrelevant since the speed bottleneck is not in the wireless routing but rather in the outside network connectivity itself.
4. **Security:** Wireless LAN transceivers are designed to serve computers throughout a structure with uninterrupted service using radio frequencies. Because of space and cost, the antennas typically present on wireless networking cards in the end computers are generally relatively poor. In order to properly receive signals using such limited antennas throughout even a modest area, the wireless LAN transceiver utilizes a fairly considerable amount of power. What this means is that not only can the wireless packets be intercepted by a nearby adversary's poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance; perhaps hundreds of times the radius as the typical user. In fact, there are even computer users dedicated to locating and sometimes even cracking into wireless networks, known as wardrivers.

   On a wired network, any adversary would first have to overcome the physical limitation of tapping into the actual wires, but this is not an issue with wireless packets. To combat this consideration, wireless networks users usually choose to utilize various encryption technologies available such as Wi-Fi Protected Access (WPA). Some of the older encryption methods, such as WEP are known to have weaknesses that a dedicated adversary can compromise.
5. **QoS:** WLAN offer typically lower QoS. Lower bandwidth due to limitaitons in radio transmission and higher error rates due to interference.
6. **Proprietary Solutions:** Slow standardization procedures lead to many proprietary solutions only working in a homogeneous environment.

4.8.4 IEEE Standard 802.11 (WLAN)

- IEEE has defined the specifications for wireless LAN, named IEEE 802.11, which covers both physical and data link layers.

- Fig. 4.37 shows various components of WLAN which described below:

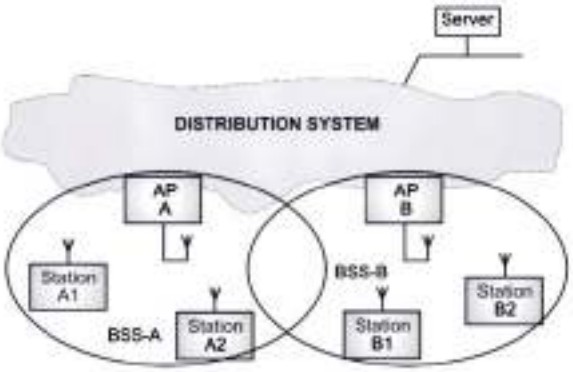


Fig. 4.37: Components of WLAN

Architecture of 802.11 (WLAN):

- Each computer, mobile which is portable or fixed, is referred to as a station in 802.11 wireless networks.
- When two or more stations come together to communicate with each other, they form a **Basic Service Set (BSS)**.
- The minimum BSS consists of two stations. 802.11 LANs use the BSS as the standard building block.
- The BSS can be either without AP (Access Point) or with AP which is as shown in Fig. 4.38.

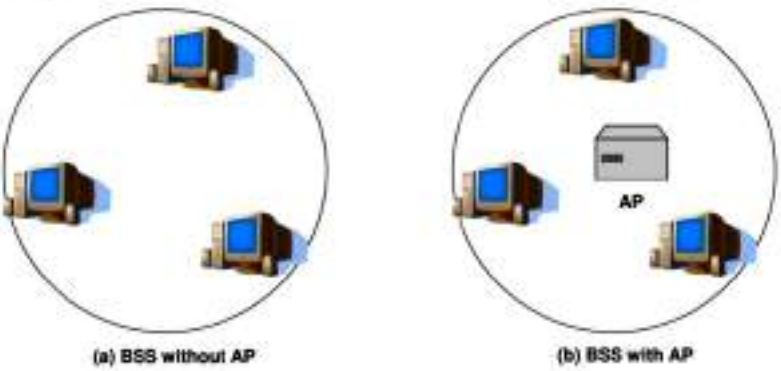


Fig. 4.38: Types of BSS

- The BSS without AP can not send data to another BSS. So it is called as standalone or ad-hoc network.
- Two or more BSSs are interconnected using a Distribution System or DS.
- This concept of DS increases network coverage, which can be either wired or wireless.
- Entry to the DS is accomplished with the use of access points.
- An access point is a station, thus addressable. So data moves between the BSS and the DS with the help of these access points.
- Creating large and complex networks using BSSs and DSs leads us to the next level of hierarchy, the Extended Service Set or ESS.
- An Extended Service set contains two or more BSS with APs. The BSSs in the system are connected to each other via a distribution system which is generally a wired LAN as shown in Fig. 4.39.

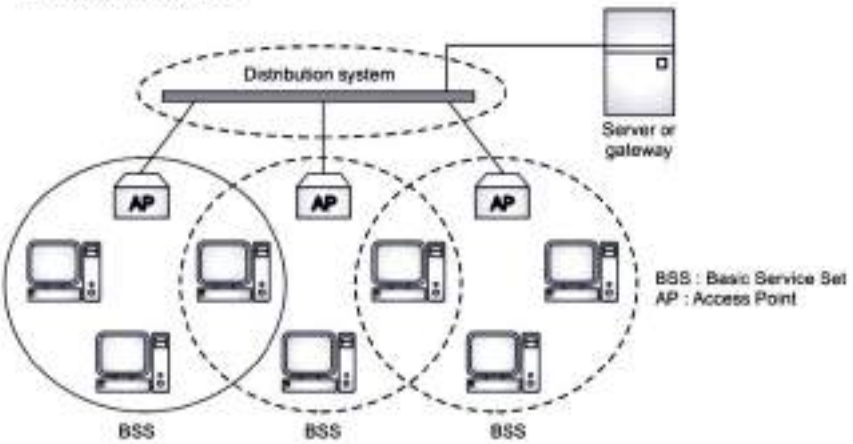


Fig. 4.39: Extended Service Set (ESS)

- The beauty of the ESS is the entire network looks like an independent basic service set.
- This means that stations within the ESS can communicate or even more between BSSs transparently.
- The implementation of the DS is not specified by 802.11. So a distribution system may be created from existing or new technologies.
- As the implementation for the DS is not specified, 802.11 specify the services, which the DS must support. Services are divided into two sections, Station Services (SS) and Distribution System Services (DSS).

Layers of 802.11 (WLAN):

1. Physical Layer:

- 802.11 provides Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and OFDM (Orthogonal Frequency Division Multiplexing), physical definitions which supports 1 and 2 Mbps data transfer rates and of DM.

(i) Frequency Hopping Spread Spectrum (FHSS):

- Frequency Hopping Spread Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver.
- Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.
- FHSS is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver.
- Fig. 4.40 shows frame format of FHSS.

<table>
<tr><td>80 bit preamble</td><td>SFD 16 bits</td><td>LENGTH 12 bits</td><td>PSF 4 bits</td><td>CRC 16 bits</td><td>CRC 16 bits</td></tr>
<tr><td colspan="2">PLCP Preamble</td><td colspan="3">PLCP Header</td><td>Payload MPDU</td></tr>
<tr><td colspan="6">PPDU</td></tr>
</table>

Fig. 4.40: FHSS Frame Format

- The 80 bit Preamble has a 0101 sync format and is used for signal detection.
- The SFD stands for Start of Frame Delimiter.
- The LENGTH field indicates the Payload length in bytes.
- The PSF stands for Payload Signaling Field and indicates the rate used and some bits for future use.
- The hopping rules say that there are 79 hopping channels and that the minimum hop should be 6 channels. The transmitter should settle on the new channel within 224 microseconds.

(ii) Direct Sequence Spread Spectrum (DSSS):

- DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code).
- The longer the chip, the greater the probability that the original data can be recovered and, of course, the more bandwidth required.
- Each bit is transmitted as 11 chips using a Barker Sequence.
- Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for

retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

- With direct sequence spread spectrum the transmission signal is spread over an allowed band.
- A random binary string is used to modulate the transmitted signal. This random string is called the spreading code.
- The data bits are mapped to a pattern of chips and mapped back into a bit at the destination.
- The number of chips that represent a bit is the spreading ratio. The higher the spreading ratio, the more the signal is resistant to interference. The lower the spreading ratio, the more bandwidth is available to the user.
- The FCC dictates that the spreading ratio must be more than 10. IEEE 802.11 standard requires a spreading ratio of 11.
- Fig. 4.41 shows frame format of DSSS.

<table>
<tr><td>128 bit preamble</td><td>SFD 16 bits</td><td>SIGNAL 8 bits</td><td>SERVICE 8 bits</td><td>LENGTH 16 bits</td><td>CRC 16 bits</td><td></td></tr>
<tr><td colspan="2">PLCP Preamble</td><td colspan="4">PLCP Header</td><td>Payload MPDU</td></tr>
<tr><td colspan="7">PPDU</td></tr>
</table>

Fig. 4.41: DSSS Frame Format

- The **128 bit preamble** is used for signal detection.
- The **SFD** stands for Start of Frame Delimiter
- The **SIGNAL** field indicates the speed used.
- The **SERVICE** field is reserved for future use and now contains 00.
- The **LENGTH** field indicates the Payload length in bytes.

(iii) Orthogonal Frequency Division Multiplexing (OFDM):

- OFDM is multicarrier spread spectrum technique.
- In OFDM, high rate serial data stream divided into numerous parallel low-rate data streams that are modulated by a set of subcarriers.
- In OFDM, subcarriers are orthogonal with overlapping spectra. It uses 5GHz ISM band for its operation.
- The basic working of OFDM is same as that of FDM but the main difference is that all the frequency sub bands are used by one source at a given time.

2. MAC Layer:

- IEEE 802.11 defines two MAC sublayers i.e. the Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF is the fundamental, required

contention-based access service for all networks. PCF is an optical contention-free service, used for non-QoS STAs.

- The Point Coordination Function (PCF) is an optional access method which is implemented in an infrastructure network and not in ad-hoc network. It is implemented on top of the DCF and is used for time sensitive transmission.
- Fig. 4.42 shows the relationship between the two MAC sublayers, the LLC sublayer and the physical layer.

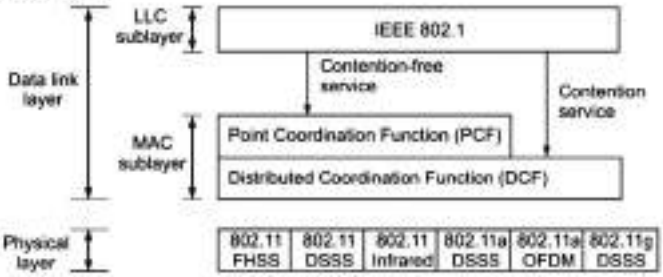


Fig. 4.42: MAC Layer

- MAC provides a reliable delivery mechanism for user data over noisy, unreliable wireless medium.
- Before transmitting frames, a station must first gain access to the medium, which is a radio channel that stations share.
- CSMA/CA is the protocol used to access method defined by IEEE at the MAC sub layer is called the distributed coordination function.
- The MAC layer consists of nine fields as shown in Fig. 4.43.

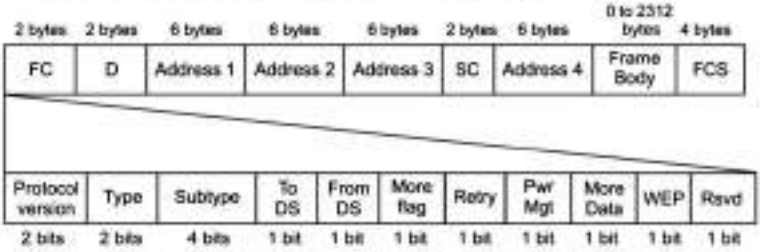


Fig. 4.43: Frame Format

- **Frame Control (FC):** The FC field is 2 bytes long and defines the type of frame and some control information.

Table 4.3: Subfields in FC fields.

Field	Explanation
Version	Current version is 0.
Type	Type of information: Management (00), Control (01), or Data (10).
Subtype	Subtype (RTS, CTS, ACK).
TO DS	Shown in Table 4.4.
From DS	Shown in Table 4.4.
More flag	When set to 1, means more fragments.
Retry	When set to 1 means retransmitted frame.
Power management	When set to 1 means station is in power management made.
More data	When set to 1, means station has more data to send.
WEP	Wired equivalence privacy.
Rsvd	Reserved.

- **D:** In all frames, this field defines the duration of the transmission that is used to set the value of NAV.
- **Addresses:** There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the TO DS and From DS subfields.

Table 4.4: Addresses

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

- **Sequence Control:** This field defines the sequence number of the frame to be used in flow control.
- **Frame Body:** This field between 0 to 2312 bytes contains information based on the type and the subtype defined in the FC field.
- **FCS:** This field is used for error detection.

4.8.5 IEEE Standard 802.11x

(S-19)

- 802.11x refers to a group of evolving wireless local area network (WLAN) standards that are under development as elements of the IEEE 802.11 family of specifications, but that have not yet been formally approved or deployed.

- As of August 2004, these incomplete standards included the following:
  1. **802.11e:** Adds Quality of Service (QoS) features to exiting 802.11 family specifications.
  2. **802.11f:** Adds Access Point Interoperability to existing 802.11 family specifications.
  3. **802.11h:** Resolves interference issues with existing 802.11 family specifications.
  4. **802.11j:** Japanese regulatory extensions to 802.11 family specifications.
  5. **80211k:** Radio resource measurement for 802.11 specifications so that a wireless network can be used more efficiently.
  6. **802.11m:** Enhanced maintenance features, improvements, and amendments to existing 802.11 family specifications.
  7. **802.11n:** Next generation of 802.11 family specifications, with throughput in excess of 100 Mbps.
- Above standards are being developed with the goal that they support all the 802.11 family specifications in current use.
- 802.11x is also sometimes used as a generic term for any existing or proposed standard of the 802.11 family.

4.9 BLUETOOTH (W-18, S-18, 19)

- Bluetooth is an open specification for short-range wireless transmission of voice and data. It provides a simple, low-cost seamless wireless connectivity between Personal Digital Assistants (PDAs), cellular phones, laptops and other portable handheld devices.
- Bluetooth can be used for bridging data networks, connecting peripherals to devices and forming ad hoc connections between groups of information appliances.
- Bluetooth is the initiative of a consortium called the Bluetooth Special Interest Group (SIG), whose original members include industry leaders Ericsson, IBM, Intel, Nokia, and Toshiba.

4.9.1 How Bluetooth Works ?

- Bluetooth supports transmission of voice and data over 2.4 GHz radio frequencies, using a frequency-hopping scheme with a maximum of 1600 hops per second, resulting in a new frequency being used to transmit each packet.
- This scheme allows for smooth operation in spite of fading due to reflecting obstacles or excessive distance, and in spite of noise due to Electro Magnetic Interference (EMI), such as that generated by microwave ovens.
- In addition, Bluetooth uses short packets and fast acknowledgements to increase reliability and employs forward error correction to reduce the effects of random noise.

- The range of transmission for Bluetooth is typically between 0.1 and 10 meters but can be as much as 100 meters using higher transmission power. The system's automatic power adaptation adjusts transmission power to the minimum needed for reliable transmission in any given situation, which reduces the chance of eavesdropping.
- Bluetooth also includes encryption and authentication mechanisms. The entire Bluetooth technology is implemented in a single 9-millimeter-by-9-millimeter chip.
- Bluetooth data transmission normally takes place over an asynchronous channel that provides 721 Kbps in the forward direction and 57.6 Kbps in the return direction, but synchronous data transmission at 432.6 Kbps in both directions is also supported.
- Time-Division Duplexing (TDD) is employed to alternate transmission between the two directions and thus provide full-duplex communication.
- Each TDD slot normally carries one packet, but packets can be spread across up to five slots. Signaling is baseband and uses a binary FM scheme.
- Channels can be routed by using a combination of circuit switching and packet switching.
- Bluetooth voice transmission can use up to three concurrent synchronous 64 Kbps voice-only channels or one channel that simultaneously supports both asynchronous data and synchronous voice transmission.
- The voice channels use the continuous variable-slope delta modulation coding scheme.
- Bluetooth supports concurrent connections among up to eight devices, forming what is called a Piconet. Each device is temporarily assigned a unique 3-bit MAC address for the duration of the connection.
- A master/slave relationship exists between one device and all other devices for the duration of the connection for the purpose of establishing clocking and the hopping sequence. In all other respects, the devices operate as peers during a connection.
- Unconnected devices are in standby mode and listen for connection attempts every 1.28 seconds on each of 32 preassigned hopping frequencies.
- Link setup and authentication is performed using the Link Manager Protocol (LMP), which uses the link controller services built into the chip.
- Connections between devices can be either point-to-point or point-to-multipoint, and piconets can be joined, with each piconet having a different hopping sequence.
- Bluetooth is both a hardware-based radio system and a software stack that specifies the linkages between layers.
- This supports flexibility in implementation across different devices and platforms. It also provides robust guidelines for maximum interoperability and compatibility.

4.9.2 Bluetooth Architectures

- Bluetooth communication occurs between a master radio and a slave radio. Bluetooth radios are symmetric in that the same device may operate as a master and also the slave. Each radio has a 48-bit unique device address (BD_ADDR) that is fixed.
- Two or more radio devices together form ad-hoc networks called piconets. All units within a piconet share the same channel.
- Each piconet has one master device and one or more slaves. There may be up to seven active slaves at a time within a piconet. Thus, each active device within a piconet is identifiable by a 3-bit active device address. Inactive slaves in unconnected modes may continue to reside within the piconet.
- A master is the only one that may initiate a Bluetooth communication link. However, once a link is established, the slave may request a master/slave switch to become the master.
- Slaves are not allowed to talk to each other directly. All communication occurs within the slave and the master. Slaves within a piconet must also synchronize their internal clocks and frequency hops with that of the master.
- Each piconet uses a different frequency hopping sequence. Radio devices used Time Division Multiplexing (TDM).
- A master device in a piconet transmits on even numbered slots and the slaves may transmit on odd numbered slots.

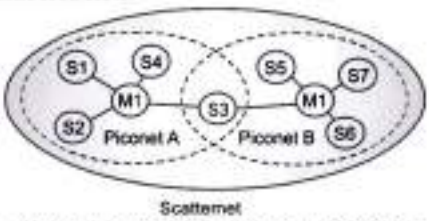


Fig. 4.44: Bluetooth Scatternets and Piconets

- Multiple piconets with overlapping coverage areas form a scatternet. Each piconet may have only one master, but slaves may participate in different piconets on a time-division multiplex basis.
- A device may be a master in one piconet and a slave in another or a slave in more than one piconet.

4.9.2.1 Piconet Architecture

- A Bluetooth network is called a *piconet* or a small net.
- A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.

- All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station.
- The communication between the primary and the secondary can be one-to-one or one-to-many. Fig. 4.45 shows a piconet architecture of bluetooth.

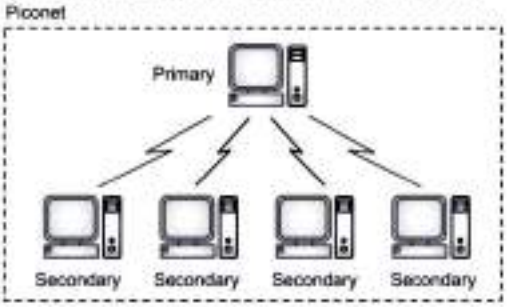


Fig. 4.45: A Piconet Architecture

- Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the *parked state*.
- A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state.
- Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

4.9.2.2 Scatternet Architecture

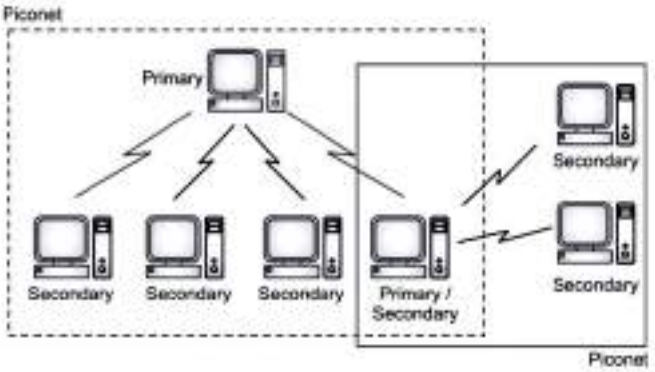


Fig. 4.46: Scatternet Architecture

- Piconets can be combined to form what is called a scatternet.

- A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets. Fig. 4.46 illustrates a scatternet architecture of bluetooth.

4.9.3 Bluetooth Protocol Stack

- The heart of the Bluetooth specification is the Bluetooth protocol stack. By providing well-defined layers of functionality, the Bluetooth specification ensures interoperability of Bluetooth devices and encourages adoption of Bluetooth technology.
- As you can see in Fig. 4.47 these layers range from the low-level radio link to the profiles.

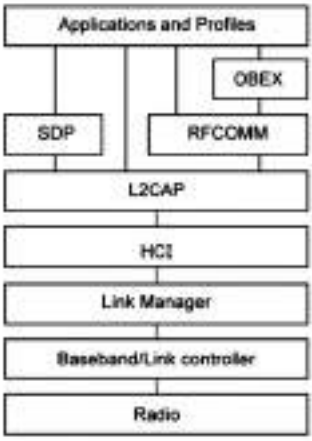


Fig. 4.47: Bluetooth Protocol Stack

4.9.3.1 Lower Layers (Radio, Baseband, Link Control Layers)

- At the base of the Bluetooth protocol stack is the **radio layer**.
- The radio module in a Bluetooth device is responsible for the modulation and demodulation of data into RF signals for transmission in the air.
- The radio layer describes the physical characteristics of the Bluetooth receiver-transmitter components.
- These include modulation characteristics, radio frequency tolerance, and sensitivity level.
- Above the radio layer is the **baseband and link controller layer**.

- The Bluetooth specification does not establish a clear distinction between the responsibilities of the baseband and those of the **link controller**.
- The best way to think about it is that the baseband portion of the layer is responsible for properly formatting data for transmission to and from the radio layer. In addition, it handles the synchronization of links.
- The link controller portion of this layer is responsible for carrying out the link manager's commands and establishing and maintaining the link stipulated by the **link manager**.
- The link manager itself translates the **Host Controller Interface** (HCI) commands it receives into baseband-level operations.
- It is responsible for establishing and configuring links and managing power-change requests, among other tasks.
- The Bluetooth specification defines two types of links between Bluetooth devices:
  1. **Synchronous, Connection-Oriented (SCO),** for isochronous and voice communication using, for example, headsets.
  2. **Asynchronous, Connectionless (ACL),** for data communication, such as the exchange of vCards.
- Each link type is associated with a specific packet type.
- A **SCO** link provides reserved channel bandwidth for communication between a master and a slave, and supports regular, periodic exchange of data with no retransmission of SCO packets.
- An ACL link exists between a master and a slave the moment a connection is established.
- The data packets Bluetooth uses for **ACL** links all have 142 bits of encoding information in addition to a payload that can be as large as 2712 bits.
- The extra amount of data encoding heightens transmission security. It also helps to maintain a robust communication link in an environment filled with other devices and common noise.
- The HCI **(Host Controller Interface)** layer acts as a boundary between the lower layers of the Bluetooth protocol stack and the upper layers.
- The Bluetooth specification defines a standard **HCI** to support Bluetooth systems that are implemented across two separate processors.
- For example, a Bluetooth system on a computer might use a Bluetooth module's processor to implement the lower layers of the stack (radio, baseband, link controller, and link manager). It might then use its own processor to implement the upper layers (**L2CAP, RFCOMM, OBEX**, and Selected profiles).
- In this scheme, the lower portion is known as the Bluetooth module and the upper portion as the Bluetooth host.

- Of course, it is not required to partition the Bluetooth stack in this way. Bluetooth headsets, for example, combine the module and host portions of the stack on one processor because they need to be small and self-contained.
- In such devices, the HCI may not be implemented at all unless device testing is required.
- Because the Bluetooth HCI is well defined, you can write drivers that handle different Bluetooth modules from different manufacturers. Apple provides an HCI controller object that supports a USB implementation of the HCI layer.

4.9.1.2 Upper Layers

L2CAP Layer:

- Above the HCI layer are the upper layers of the protocol stack. The first of these is the **L2CAP (Logical link control and Adaptation protocol)** layer.
- The L2CAP is primarily responsible for:
  1. Establishing connections across existing ACL links or requesting an ACL link if one does not already exist.
  2. Multiplexing between different higher layer protocols, such as RFCOMM and SDP, to allow many different applications to use a single ACL link.
  3. Repackaging the data packets it receives from the higher layers into the form expected by the lower layers.
- The **L2CAP** employs the concept of channels to keep track of where data packets come from and where they should go.
- You can think of a channel as a logical representation of the data flow between the L2CAP layers in remote devices.
- Because it plays such a central role in the communication between the upper and lower layers of the Bluetooth protocol stack, the L2CAP layer is a required part of every Bluetooth system.
- Above the L2CAP layer, the remaining layers of the Bluetooth protocol stack are not quite so linearly ordered.
- However, it makes sense to discuss the service discovery protocol next, because it exists independently of other higher-level protocol layers. In addition, it is common to every Bluetooth device.

Service Discovery Protocol (SDP):

- The **SDP (Service Discovery Protocol)** defines actions for both servers and clients of Bluetooth services. The specification defines a service as any feature that is usable by another (remote) Bluetooth device. A single Bluetooth device can be both a server and a client of services.
- An **SDP** client communicates with an SDP server using a reserved channel on an L2CAP link to find out what services are available. When the client finds the desired

service, it requests a separate connection to use the service. The reserved channel is dedicated to SDP communication so that a device always knows how to connect to the SDP service on any other device. An SDP server maintains its own SDP database, which is a set of service records that describe the services the server offers. Along with information describing how a client can connect to the service, the service record contains the service's UUID, or Universally Unique Identifier.

Radio Frequency Communication (RFCOMM):

- Above the L2CAP layer is the **RFCOMM layer**. This is the most important layer in the Bluetooth architecture. The RFCOMM protocol emulates the serial cable line settings and status of an RS-232 serial port. RFCOMM connects to the lower layers of the Bluetooth protocol stack through the L2CAP layer.
- It connects the serial ports of all the devices according to the requirement. It also supports the OBEX protocol.

OBEX (Object Exchange):

- OBEX (Object Exchange) is a transfer protocol that defines data objects and a communication protocol two devices can use to easily exchange those objects. Bluetooth adopted OBEX from the IrDA IrOBEX specification because the lower layers of the IrOBEX protocol are very similar to the lower layers of the Bluetooth protocol stack.
- In addition, the IrOBEX protocol is already widely accepted and therefore a good choice for the Bluetooth SIG, which strives to promote adoption by using existing technologies.
- A Bluetooth device wanting to set up an OBEX communication session with another device is considered to be the client device.
  1. The client first sends SDP requests to make sure the other device can act as a server of OBEX services.
  2. If the server device can provide OBEX services, it responds with its OBEX service record. This record contains the RFCOMM channel number the client should use to establish an RFCOMM channel.
  3. Further communication between the two devices is conveyed in packets, which contain requests, responses, and data. The format of the packet is defined by the OBEX session protocol.

4.9.4 Bluetooth Frame Structure

- There are several frame formats of the Bluetooth the most and important common of which is shown in Fig. 4.39.
- Bluetooth frame begins with an access code that usually identifies the master so that slaves within radio range of two masters can tell which traffic is for them.
- Next comes a 54-bit header containing typical MAC sublayer fields. Then comes the data field, of up to 2744 bits.

Header field:

- Let us take a quick look at the header of Bluetooth frame.
  - **The Address field:** Identifies which of the eight active devices the frame is intended for.
  - **Type field:** Identifies the frame type, the type of error correction used in the data field, and how many slots long the frame is.
  - **Flow bit:** Flow bit is asserted by a slave when its buffer is full and cannot receive any more data.
  - **Acknowledgement bit:** It is used to piggyback an ACK onto a frame.
  - **Sequence bit:** It is used to number the frames to detect retransmission; the protocol is stop-and-wait, so 1 bit is enough.
  - **Checksum:** Then comes the 8-bit header Checksum.
- The entire 18-bit header is repeated three times to form the 54-bit header shown in Fig. 4.48.
- On the receiving side, a simple circuit examines all three copies of each bit. If all three are the same, the bit is accepted. If not, the majority opinion wins. Thus, 54 bits of transmission capacity are used to send 10 bits of header.

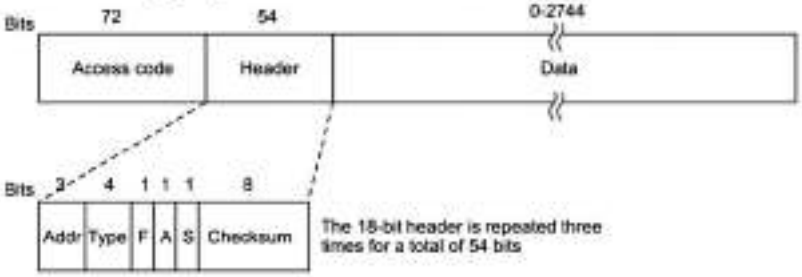


Fig. 4.48: A Typical Bluetooth Data Frame

4.10 BLUETOOTH APPLICATIONS

Important application of Bluetooth are given below:

- It allows a transfer of images (or) word documents (or) applications (or) audio and video files between devices without the help of cables.
- It can be used for remote sales technology allowing wireless access to vending machines and other commercial enterprises.
- It provides inter accessibility of PDAs, palmtops and desktops for file and data exchanges.
- It can be used to setup a personal area network (PAN) or a wireless personal area network (WPAN).

- It is used in the short-range transmission of data from sensors devices to sensor nodes like mobile phones.
- It is used by modern healthcare devices to send signals to monitors.

Summary

- A WLAN, or wireless LAN, is a network that allows devices to connect and communicate wirelessly. Unlike a traditional wired LAN, in which devices communicate over Ethernet cables, devices on a WLAN communicate via Wi-Fi.
- IEEE 802 is a collection of networking standards that cover the physical and data-link layer specifications for technologies such as Ethernet and wireless.
- IEEE 802 specifications also split the data link layer into two different layers: an LLC layer and a MAC layer.
- IEEE Standards are: 802 - LAN/MAN, 802.1 - Media access control (MAC), 802.2 - Logical Link Control (LLC), 802.3 - Carrier Sense Multiple Access with Collision Detection (CSMA/CD),802.11 - Wireless Networking "WiFi".
- A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and LocalTalk.
- In computer networks, Fast Ethernet is a variation of Ethernet standards that carry data traffic at 100 Mbps (Mega bits per second) in local area networks (LAN).
- Gigabit Ethernet, a transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs), provides a data rate of 1 billion bits per second (one gigabit).
- 10 gigabit Ethernet is a telecommunication technology that offers data speeds up to 10 billion bits per second.
- A backbone or core network is a part of a computer network which interconnects pieces of various networks, providing a path for the exchange of information between different LANs or subnetworks.
- Backbone network contains a Distributed (Bus backbone) and collapsed backbone (Star backbone).
- A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs).
- Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (Local Area Network). Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.

- Bluetooth wireless technology is a worldwide specification for a small-form factor, low-cost radio solution that provides links between mobile computers, mobile phones, other portable handheld devices, and connectivity to the Internet.

Check Your Understanding

1. Ethernet frame consists of _____.
   (a) MAC address (b) IP address
   (c) Default mask (d) Network address
2. MAC address is of _____.
   (a) 24 bits (b) 36 bits
   (c) 42 bits (d) 48 bits
3. In a backbone, the _____ backbone is a just switch.
   (a) bus (b) ring
   (c) star (d) mesh
4. An interconnected collection of Piconet is called _____.
   (a) Scatternet (b) Micronet
   (c) Mininet (d) Multinet
5. Bluetooth is the wireless technology for _____.
   (a) Local area network
   (b) Personal area network
   (c) Metropolitan area network
   (d) Wide area network

ANSWERS

(1) a	(2) d	(3) c	(4) a	(5) b		

Practice Questions

Q.I Answer the following questions in short.

1. What is IEEE standards?
2. Describe Fast Ethernet.
3. What is network interface card?
4. What is Wireless LAN?
5. What is Bluetooth in WLAN?

Q.II Answer the following questions.

1. Write a short note on IEEE standards 802.11.
2. How Bluetooth works?
3. With suitable diagram describe Bluetooth architecture.
4. Write short notes on:

i) Scartternet architecture.
ii) Piconet architecture.

5. What is VLAN? What are types of VLAN?
6. What is Backbone network?
7. What is Ethernet? What are its types? Explain any one.
8. What are the different categories of Fast Ethernet?
9. Explain BSS and ESS in detail.

Q.III Define the Terms:

1. Ethernet
2. Star backbone
3. Bus backbone
4. VLAN
5. CSMA/CD

Previous Exams Questions

Summer 2018

1. Describe the frame format and physical layer of Ethernet. 5M

Ans. Please refer to section 4.4.5 and 4.5.

2. Explain Bluetooth in detail. 5M

Ans. Please refer to section 4.9.

3. Write short note on: MAC sublayer with its frame format. 5M

Ans. Please refer to section 4.4.4.

Winter 2018

1. Explain Bluetooth in detail. 5M

Ans. Please refer to section 4.9.

2. Write short note on: MAC sublayer with its frame format. 5M

Ans. Please refer to section 4.4.4.

Summer 2019

1. Explain IEEE 802.11 in detail. 5M

Ans. Please refer to section 4.8.5.

2. Describe the frame format and physical layer of Ethernet. 5M

Ans. Please refer to sections 4.4.5 and 4.5.

3. Write short note on: Bluetooth. 5M

Ans. Please refer to section 4.9.

❖❖❖

5... Network Connectivity Devices

Objectives...

- To learn about categories of network connectivity devices.
- To study about Hubs, Repeaters, Bridges, Switches, Routers and Gateways.

5.1 NETWORK CONNECTIVITY DEVICES

- Networking Connecting Devices include all computers, peripherals, interface cards and other equipments needed to perform data-processing and communications within the network.
- **Examples:** Network Interface Card (NIC), Hub, Switch, Bridge, Router, Gateway.

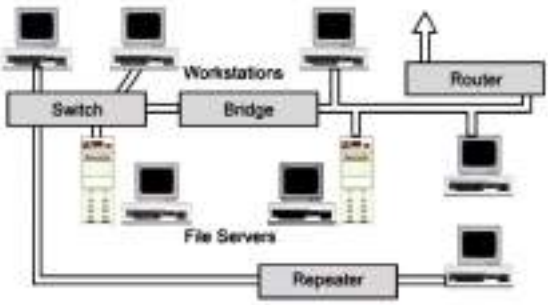


Fig. 5.1: Networking Hardware with Network connectivity devices

- A file server stands at the heart of most networks. It is a very fast computer with a large amount of RAM and storage space, along with a fast network interface card.
- The network operating system software resides on this computer, along with any software applications and data files that need to be shared.

- All user computers connected to a network is called workstations.
- A typical workstation is a computer that is configured with a network interface card, networking software and the appropriate cables. Workstations do not necessarily need floppy disk drives because files can be saved on the file server.
- Almost any computer can serve as a network workstation.

5.2 ACTIVE AND PASSIVE HUBS (S-18,19)

5.2.1 What is Hub?

- As the name suggests, the meaning of hub is a center of activities. A hub is a medium used to collect signals from the input line(s) and redistribute them in various available wirings around a topology (Topologies such as: Arcnet, 10base-T, 10base-F etc.).
- Hubs operate at the Physical layer of the Open Systems Interconnection (OSI) model.

Physical Structure:

- A hub is a small rectangular box, often constructed mainly of plastic that receives its power from an ordinary wall outlet. A hub joins multiple computers or other network devices together to form a single network segment.
- On this network segment, all computers can communicate directly with each other. Ethernet hubs are by far the most common type, but hubs for other types of networks (such as USB) also exist.
- Hubs come in a variety of shapes and sizes.
- A hub includes a series of ports that each accepts a network cable. Small hubs network four computers. They contain four or sometimes five ports (the fifth port being reserved for "uplink" connections to another hub or similar device). Larger hubs contain 8, 12, 16, and even 24 ports.
- Even the most basic hubs can provide satisfactory file sharing and Internet connection sharing for a LAN.
- They will work with traditional dial-up, cable modem, and DSL service. For high-performance networking such as online gaming, net workers will want a more expensive 10/100 Fast Ethernet-capable hub.
- Future high-speed Internet services like VDSL will almost certainly require Fast Ethernet performance as well.
- Hubs differ in the features they support as well as in performance, making direct comparisons difficult.
- Hubs are used in Ethernet (IEEE 802.3) networks. The electronics in hubs need to be more sophisticated however, because a signal received at any port must be "instantly" retransmitted on all other ports for the CSMA/CD access method to work.

- Network segments that employ hubs are often described as having a Star-Bus network topology, in which the hub forms the wiring centre of the "star".

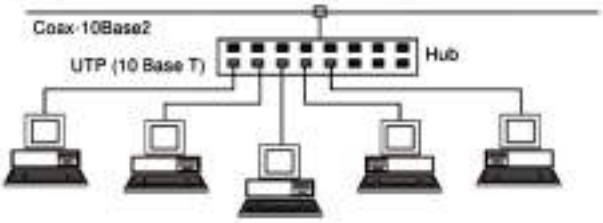


Fig. 5.2: Typical hub is used to connect the Different Nodes

Advantages:

- Hubs offer a convenient, affordable way to build a home or small business network.
- It provides a degree of fault tolerance, because each node has its own connection to the hub, and if the connection fails, only that node is affected.
- It also simplifies the task of expanding the network, as many additional nodes can be added to the network using a single hub, which is normally connected to the network backbone.

Disadvantages:

- In early computer networks, nodes were connected together in daisy-chain fashion. Once, all the nodes were connected, each end of the cable would be closed with a terminator.
- The main problem with this design was that a break anywhere in the cable meant that the network would not function, and one of the major overheads was the time spent in locating the problem.

Need of Hub:

- Generally, when we build a network using two or more computers, we need a hub. However, it is possible to connect two computers to each other directly without the need of hub but when we add a third computer in the network, we need a hub to allow a proper data communication within the network.
- There are many types of hubs with various features/specifications, which provide the type of functionality you need in building network.

Types of Hubs:

- Hubs can be either active or passive.
- Small hubs with five or eight connection ports are commonly referred to as workgroup hubs. Others can accommodate larger numbers of devices (normally up to 32).
- These are referred to as high-density devices. Because hubs do not perform any processing, they do little except enable communication between connected devices.

5.2.2 Active Hub (S-18,19)

- Active hub is a type of hub that takes active participation in data communication within the network/LAN.
- An active hub is basically a multiport repeater of the Class II type, although it is still a physical layer device - it buffers incoming frames and regenerates them, sending the regenerated signal out on all of its ports.
- In order to do this, active hubs require their own power supply. Because the signal is regenerated at the hub, each output port can take full advantage of the maximum cable length. Since the medium used is Unshielded Twisted Pair (UTP), maximum length will be 100 meters.

Features:

- Active hubs come with various features, such as,
  - Receiving the signal (data) from the input port and storing it for some time before forwarding it. This feature allows the hub to monitor the data that is forwarding.
  - Some hubs come with a feature that helps in transmitting data that has high priority before the data that has lower priority (this feature is very important for some applications and some type of networks).
  - Some hubs help in synchronizing data communication (by retransmitting the packets, which are not properly received at the receiving computer or by adjusting re-transmission of the data packets to compensate timing).
  - Some active hubs come with a feature that rectifies the data/signal before forwarding it in the network/LAN.
  - Active hubs also help in troubleshooting at certain level. If there is a bottleneck within the network/LAN, active hubs can be used to find out the problem at certain extent.
- Active hubs have some benefits over the use of passive hubs; however, active hubs are more expensive than passive hubs as they provide additional features.

5.2.3 Passive Hub (S-18,19)

- As its name suggests, passive hubs which does not provide any additional feature except for working just as an interface between the topology.
- A passive hub simply receives signal(s) on input port(s) and broadcasts it (them) on the output port(s) without even rectifying it (them).
- Managed hubs offer some control over the nodes connected to them.
- For example, each port can be individually enabled or disabled by the network administrator and some intelligent hubs can track network activities such as the number of packets transferred and the occurrence of errors within those packets.
- A hub does not perform any processing on the data that it forwards, nor does it perform any error checking.

5.3 REPEATERS (S-18,19)

- A repeater is primarily a non-intelligent network device that receives a signal on one of its connections and passes that signal on to all of its other connections after regenerating it.

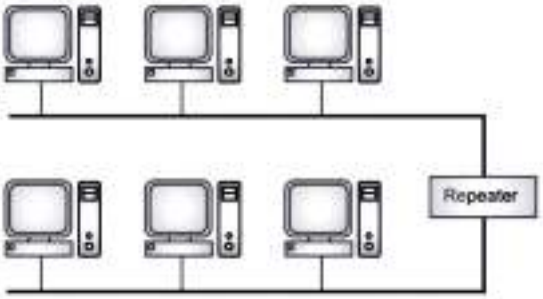


Fig. 5.3: Repeaters can be used to extend the Length of a Network

- Repeaters work at the physical layer and can be used to extend the length of a network, but not the capacity.
- As signals travel along a network cable (or any other medium of transmission), they degrade and become distorted in a process that is called attenuation.
- If a cable is long enough, the attenuation will finally make a signal unrecognizable by the receiver.
- A Repeater enables signals to travel longer distances over a network. A repeater regenerates the received signals and then retransmits the regenerated (or conditioned) signals on other segments.
- Amplifier cannot discriminate between the intended signal and noise i.e. it amplifies equally everything fed into it.
- A repeater does not amplify the signal, it regenerates the signal. When repeater receives a weakened or corrupted signal, it creates a copy, bit for bit, at the original strength.
- Hub is basically a multiport repeater.

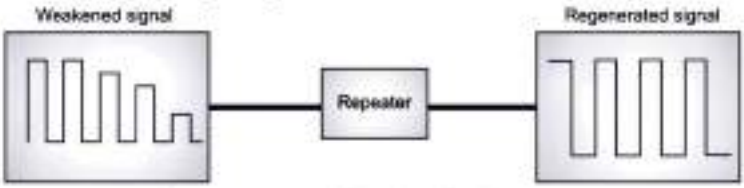


Fig. 5.4: Regenerated signal using the Repeater

- To pass data through the repeater in a usable fashion from one segment to the next, the packets and the Logical Link Control (LLC) protocols must be the same on the each segment.
- This means that a repeater will not enable communication, for example, between an 802.3 segment (Ethernet) and an 802.5 segment (Token Ring).
- That is, they cannot translate an Ethernet packet into a Token Ring packet. In other words, repeaters do not translate anything. As signals travel along a transmission medium, there will be a loss or attenuation, of signal strength.

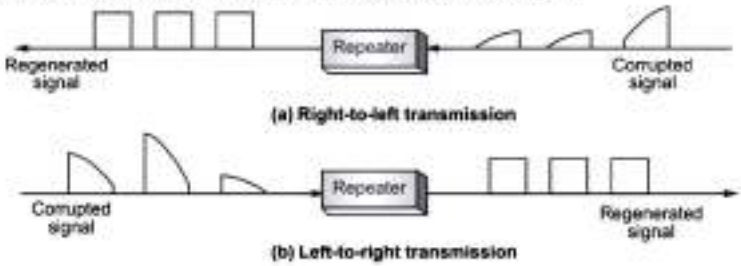


Fig. 5.5: Function of a Repeater

- Repeaters are defined into 2 classes:
  1. Class I (or Type I): These are not stackable, and cannot be daisy- chained.
  2. Class II (or Type II): These are stackable, and can be daisy-chained.
- Some multiport repeaters act as multiport hubs and connect different types of media.

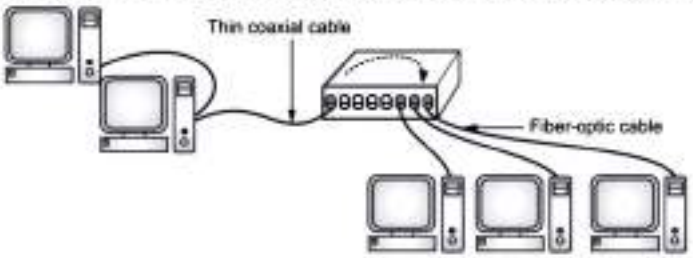


Fig. 5.6: Repeaters can connect different types of Media

- Repeaters cannot be used to enlarge a network beyond the capabilities of its underlying architecture, nor they can be used to connect network segments that rely on different access methods.
- They can, however, be used to move transmissions between different media types, such as coaxial and fiber optic cables.

5.4 BRIDGES (W-18, S-18,19)

- Like a repeater, a bridge can join segments or workgroup LANs. However, a bridge can also divide a network to isolate traffic or problems.
- For example, if the volume of traffic from one or two computers or a single department is flooding the network with data and slowing down entire operation, a bridge can isolate those computers or that department.

Fig. 5.7 (a): Bridge

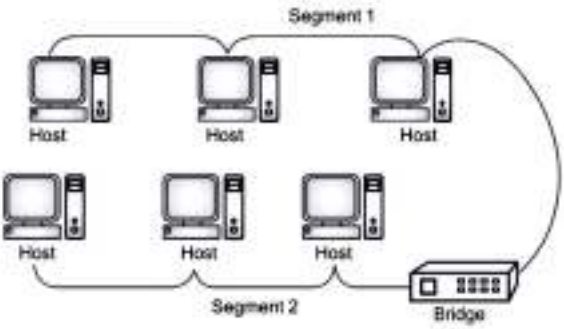


Fig. 5.7 (b): Use of Bridge

- In Fig. 5.7(b), a bridge is used to connect two segments, Segment 1 and Segment 2.
- Bridges operate at the Data Link Layer of the OSI Reference Model. A bridge both filters and passes packets between network segments.
- While true bridges connect only LANs that have an identical network architecture (i.e. 802.3 - 802.3, 802.5 - 802.5), certain types of bridge (bridge-routers or brouters) can also join LANs based on different network architectures.
- For example, they can join an Ethernet segment to a Token Ring segment and transfer packets between the two despite the difference in protocols used.
- Thus bridges can both extend the length of a network and increase its capacity.

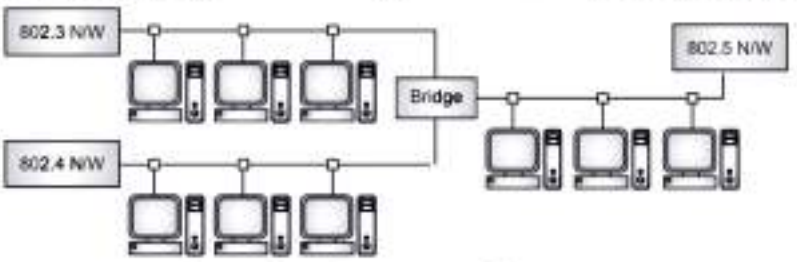


Fig. 5.8: Bridge used to connect Multiple Segments

- Unless the sender and the recipient are on different network segments, there is no need for the bridge to transfer the packet to another network segment. If the sender and the recipient are on different segments, the bridge needs to be able to determine where the recipient is.
- Bridges can be used to:
  - Expand the distance of a segment.
  - Provide for an increased number of computers on the network.
- Network bridges can be used to connect LAN segments or to isolate heavily trafficked segments from the rest of the network.

Working principle:

- A bridge works on the principle that each network node has its own address.
- A bridge forwards the packets based on the address of the particular destination node. As traffic passes through the bridge, information about the computer addresses is then stored in the bridge's RAM.
- The bridge will then use this RAM to build a routing table based on source addresses.

5.4.1 Types of Bridges

- Three types of bridges are used in networks:
  1. Transparent Bridge
  2. Source Route Bridge
  3. Spanning Tree Bridge

1. Transparent Bridge:

- A transparent bridge is a type of Network Bridge. It interconnects several computers in a network by forwarding packets to hosts.
- A transparent bridge is a bridge whose presence and operation is invisible to hosts on the network.
- A transparent bridge does nothing except block or forward data based on the MAC address.

- Physically, a transparent bridge looks like a box with two or more holes (ports) where network cables are plugged. The other extreme of each cable is usually connected to the network port of a computer, or to another network device, which is further connected to one or more computers.
- While a network bridge simply enables local networks (or segments) to communicate with each other, but forwards the traffic to all ports, a transparent bridge is capable of redirecting the packets to the proper port, hence it can isolate the networks from broadcast traffic.
- A transparent bridge directs the outgoing data traffic using a forwarding table that associates addresses to ports.
- The table can be static or built by learning the network topology from the analysis of the incoming traffic. For example, learning happens by the device inspecting the source Media Access Control (MAC) address of all incoming data frames. The device will send frames out of all its ports.
- This method uses a forwarding database to send frames across network segments.
- The forwarding database is initially empty and entries in the database are built as the bridge receives frames.
- If an address entry is not found in the forwarding database, the frame is rebroadcast to all ports of the bridge, forwarding the frame to all segments except the source address.
- By means of these broadcast frames, the destination network will respond and a route will be created. Along with recording the network segment to which a particular frame is to be sent, bridges may also record a bandwidth metric to avoid looping when multiple paths are available.
- Devices that have this transparent bridging functionality are also known as *adaptive bridges*. They are primarily found in Ethernet networks.

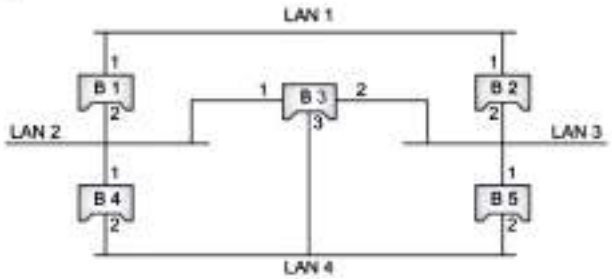
2. Source Route Bridge:

- The source route bridge derives its name from the fact that the entire path that the packet is to take through the network is embedded within the packet. Used in Token Ring networks.
- With source route bridging two frame types are used in order to find the route to the destination network segment: Single-Route (SR) frames and All-Route (AR) frames.
- Single-Route (SR) frames make up most of the network traffic and have set destinations, while All-Route (AR) frames are used to find routes.
- Bridges send AR frames by broadcasting on all network branches; each step of the followed route is registered by the bridge performing it.
- Each frame has a maximum hop count, which is determined to be greater than the diameter of the network graph, and is decremented by each bridge. Frames are dropped when this hop count reaches zero, to avoid indefinite looping of AR frames.

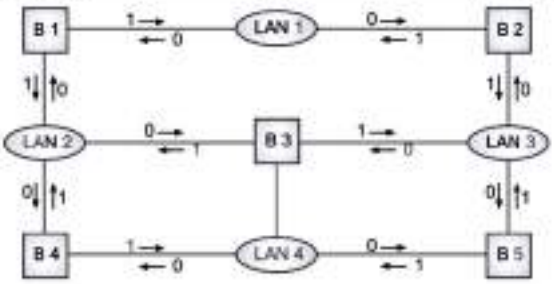
- The first AR frame which reaches its destination is considered to have followed the best route, and the route can be used for subsequent SR frames; the other AR frames are discarded. This method of locating a destination network can allow for indirect load balancing among multiple bridges connecting two networks.
- The more a bridge is loaded, the less likely it is to take part in the route finding process for a new destination as it will be slow to forward packets.
- A new AR packet will find a different route over a less busy path if one exists. This method is very different from transparent bridge usage, where redundant bridges will be inactivated; however, more overhead is introduced to find routes, and space is wasted to store them in frames.
- A switch with a faster backplane can be just as good for performance, if not for fault tolerance. They are primarily found in Token Ring networks.

3. Spanning Tree Bridge:

- A spanning tree is a graph in which there is no loop. In a bridged LAN, this means creating a topology in which each and every LAN can be reached from any other LAN through one path only i.e. no loop.
- You cannot change the physical topology of the system because of physical connections between cables and bridges, but you can create a logical topology which overlays the physical one.
- Fig. 5.9 shows a system with four LANs and five bridges. You have shown the physical system and its representation in graph theory.
- The connecting arcs show the connection of a LAN to a bridge and vice versa. To find the spanning tree, you need to assign a cost to each arc.
- The interpretation of the cost is left up to the systems administrator. It may be the path with minimum nodes, the path with minimum delay or the path with maximum bandwidth.



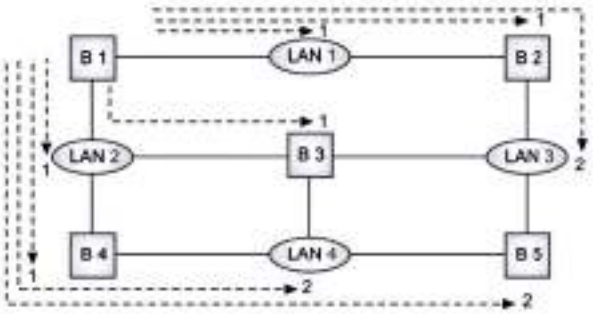
(a)



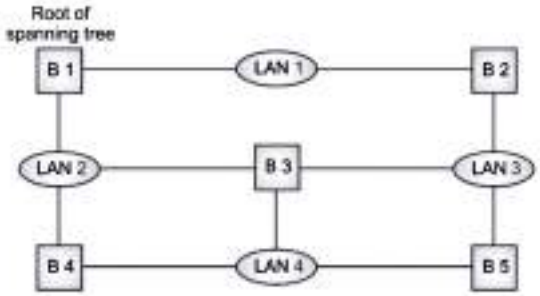
(b)

Fig. 5.9: A system of connected LANs and show its graph representation

- If two ports have the same shortest value, the systems administrator just chooses one. You have chosen the minimum nodes.
- The process to find the spanning tree involves three steps given below:
  1. Every bridge has a built-in ID. Each and every bridge broadcasts this ID so that all bridges know which one has the smallest ID. The bridge with the smallest ID is selected as the root bridge. You assume that bridge B1 has the smallest ID, for this reason B1 selected as the root bridge.
  2. The algorithm tries to find the shortest path from the root bridge to every other bridge. The shortest path can be found by examining the total cost from the root bridge to the destination. Fig. 5.10 shows the shortest paths.
  3. The combination of the shortest paths creates the shortest tree, which is also shown in Fig. 5.10.



(a) Shortest paths



(b) Spanning tree

Fig. 5.10: Determining the shortest paths and the spanning tree in a system of bridge

- Based on the spanning tree, you mark the ports that are part of the spanning tree, the forwarding ports, which forward a frame that the bridge receives. You also mark those ports that are not part of the spanning tree, the blocking ports, which block the frames received by the bridge. Fig. 5.11 illustrates the physical systems of LANs with forwarding points (solid lines) and blocking ports (broken lines).
- Note there is only one single path from any LAN to any other LAN in the spanning tree system. No loops are created. You can prove to yourself that there is only one path from LAN 1 to LAN 2, LAN 3 or LAN 4. Similarly, there is only one path from LAN 2 to LAN 1, LAN 3, and LAN 4. The same is true for LAN 3 and LAN 4.

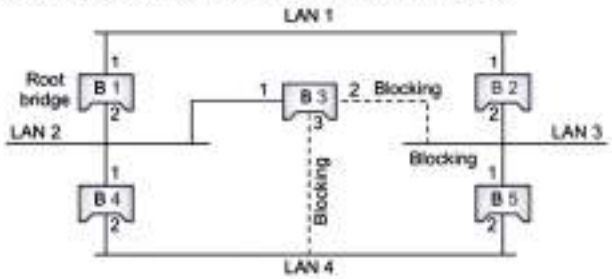


Fig. 5.11: The physical systems of LANs with forwarding points and blocking ports

5.4.2 Advantages of Bridges

- Advantages of bridges are given below:
  1. Self configuring.
  2. Primitive bridges are often inexpensive.

3. Reduce the size of collision domain by micro segmentation in non-switched networks.
4. Transparent to protocols above the MAC layer.
5. Allows the introduction of management/performance information and access control.
6. LANs interconnected are separate and physical constraints such as number of stations, repeaters and segment length do not apply.
7. Helps minimize bandwidth usage.
8. Used to interconnect two LANs.

5.4.3 Disadvantages of Bridges

- Disadvantages of bridges are given below:
  1. Does not limit the scope of broadcasts.
  2. Does not scale to extremely large networks.
  3. Buffering introduces store and forward delays; on average traffic destined for bridge will be related to the number of stations on the rest of the LAN.
  4. Bridging of different MAC protocols introduces errors.
  5. Because bridges do more than repeaters by viewing MAC addresses, the extra processing makes them slower than repeaters.

5.5 SWITCHES (S-18,19)

- A network switch is a computer networking device that connects network segments. The term commonly refers to a Network bridge that processes and routes data at the Data link layer (layer 2) of the OSI model.
- Switches that additionally process data at the Network layer (layer 3) are often referred to as Layer 3 switches or Multilayer switches.

Fig. 5.12: Switch

- The term network switch does not generally encompass unintelligent or passive network devices such as hubs and repeaters.
- The switch is a relatively new network device which is beginning to be used in Local Area Networks either in place of or in combination with Hubs.

- Unlike hubs, which broadcast messages to all ports regardless of the destination address, switches use internal address tables to route frames to only the port associated with the recipient node.
- Switches can be used to connect single network nodes or entire network segments and in this respect they superficially resemble a cross between a hub and a Bridge.
- Technically, switches work at the Data Link Layer of the OSI Reference Model, and use the MAC address (48 bit Hardware Address) within the frame to determine which node to send the frame to.

Difference between Hub and Switch:

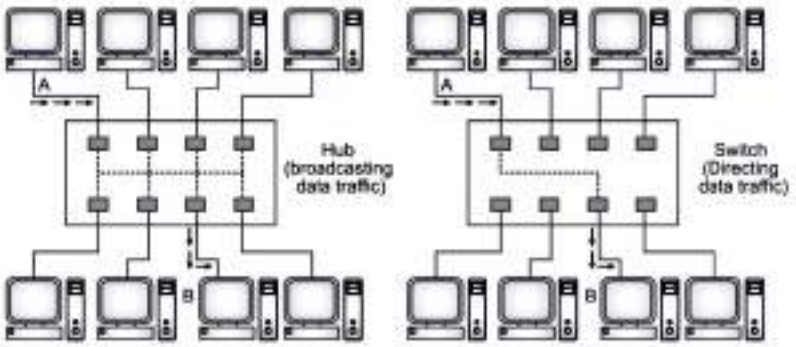


Fig. 5.13: The difference between a Hub and a Switch

- One major difference between a hub and a switch is that all the nodes connected to a hub share the available bandwidth, whereas a device connected to a switch port has the full bandwidth to itself.
- For example, if 8 nodes are connected using a hub on a 10 Mbps network, then each node may only get a portion of the 10 Mbps if other nodes on the hub want to communicate at the same time. With a switch, each node can communicate at 10 Mbps.
- The Fig. 5.13 illustrates the difference between a hub and a switch in a situation where node A transmits data to node B.
- With the hub, the data is transmitted to all nodes because the incoming frame from node A is broadcast to all ports. If other nodes are transmitting at the same time, collisions will occur.
- With the switch, the incoming frame is sent only to the port to which node B is attached via a "data pipe", avoiding possible collisions.

Types of Switches:

- There are two kinds of switches - the workgroup switch and the enterprise switch.

1. **The Workgroup Switch:**

- This is the direct replacement for the hub and works as described above, where the switch gives each port its own dedicated "data pipe" as opposed to the shared bandwidth of the traditional hub.
- This is like having a multi-port bridge with dedicated port-to-port connections, with one major difference. Hubs and bridges are connected to, and therefore rely on the backbone, whereas the workgroup switch has pre-assigned logical channels to avoid collisions.
- The transfer of data between ports uses specific channels for any possible bi-directional combinations on the device, so that for any given pair of ports there is a distinct and separate channel.

2. **The Enterprise Switch:**

- This is connected to the backbone, with no user connections directly attached to it (although this is possible).
- This allows the network management to connect the enterprise switch to hubs, bridges and Routers (the diagram below illustrates this concept).
- The bandwidth of the Enterprise Switch should be greater than the combined bandwidth of the entire network to which it is connected.

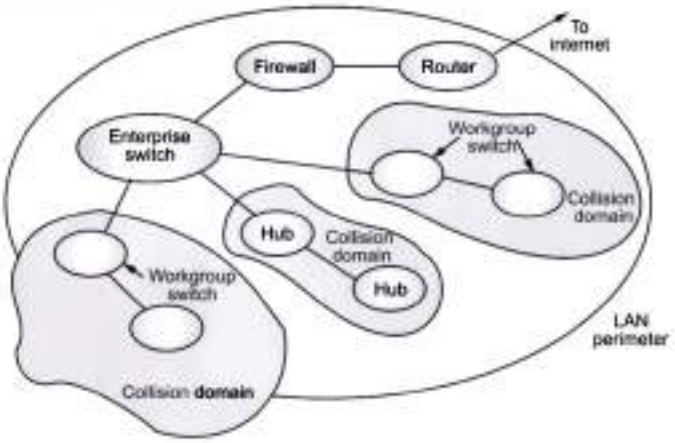


Fig. 5.14: Switch Architecture

Role of Switches in Network:

- Switches may operate at one or more OSI layers, including physical, data link, network, or transport (i.e., end-to-end).
- A device that operates simultaneously at more than one of these layers is called a Multilayer Switch, although use of the term is diminishing.

- In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including Ethernet, Fiber Channel, ATM, ITU-T G.hn and 802.11.
- This connectivity can be at any of the layers mentioned. While Layer 2 functionality is adequate for speed-shifting within one technology, interconnecting technologies such as Ethernet and token ring are easier at Layer 3.
- Interconnection of different Layer 3 networks is done by routers. If there are any features that characterize "Layer-3 switches" as opposed to general-purpose routers, it tends to be that they are optimized, in larger switches, for high-density Ethernet connectivity.
- In some service provider and other environments where there is a need for a great deal of analysis of network performance and security, switches may be connected between WAN routers as places for analytic modules.
- Some vendors provide firewall, network intrusion detection, and performance analysis modules that can plug into switch ports. Some of these functions may be on combined modules.
- In other cases, the switch is used to create a mirror image of data that can go to an external device.
- Since most switch port mirroring provides only one mirrored stream, network hubs can be useful for fanning out data to several read-only analyzers, such as intrusion detection systems and packet sniffers.

5.5.1 Layer 2 Switch

- A network bridge, operating at the Media Access Control (MAC) sublayer of the data link layer, may interconnect a small number of devices in a home or office.
- This is a trivial case of bridging, in which the bridge learns the MAC address of each connected device.
- Single bridges also can provide extremely high performance in specialized applications such as storage area networks.
- Bridges may also interconnect using a spanning tree protocol that allows the best path to be found within the constraint that it is a tree.
- In contrast to routers, bridges must have topologies with only one active path between two points.
- The older IEEE 802.1D spanning tree protocol could be quite slow, with forwarding stopping for 30–90 seconds while the spanning tree would re-converge.
- A Rapid Spanning Tree Protocol was introduced as IEEE 802.1w, but the newest edition of IEEE 802.1D-2004, adopts the 802.1w extensions as the base standard.
- While "layer-2 switch" remains more of a marketing term than a technical term, the products that were introduced as "switches" tended to use micro segmentation and Full duplex to prevent collisions among devices connected to Ethernets.

- By using an internal forwarding plane much faster than any interface, they give the impression of simultaneous paths among multiple devices.
- Once a bridge learns the topology through a spanning tree protocol, it forwards data link layer frames using a layer 2 forwarding method.
- There are four forwarding methods a bridge can use, of which the second through fourth method were performance-increasing methods when used on "switch" products with the same input and output port speeds:
  1. **Store and Forward:** The switch buffers and, typically, performs a checksum on each frame before forwarding it on.
  2. **Cut through:** The switch reads only up to the frame's hardware address before starting to forward it. There is no error checking with this method.
  3. **Fragment free:** A method that attempts to retain the benefits of both store and forward and cut through. Fragment free checks the first 64 bytes of the frame, where addressing information is stored. According to Ethernet specifications, collisions should be detected during the first 64 bytes of the frame, so frames that are in error because of a collision will not be forwarded. This way the frame will always reach its intended destination. Error checking of the actual data in the packet is left for the end device in Layer 3 or Layer 4 (OSI), typically a router.
  4. **Adaptive switching:** A method of automatically switching between the other three modes.
- Cut-through switches have to fall back to store and forward if the outgoing port is busy at the time the packet arrives.
- While there are specialized applications, such as storage area networks, where the input and output interfaces are the same speed, this is rarely the case in general LAN applications.
- In LANs, a switch used for end user access typically concentrates lower speed (e.g. 10/100 Mbit/s) into a higher speed (at least 1 Gbit/s). Alternatively, a switch that provides access to server ports usually connects to them at a much higher speed than used by end user devices.

5.5.2 Layer 3 Switch

- Within the confines of the Ethernet physical layer, a layer-3 switch can perform some or all of the functions normally performed by a router. A true router is able to forward traffic from one type of network connection (For example, T1, DSL) to another (For example, Ethernet, Wi-Fi).
- The most common layer-3 capability is awareness of IP multicast. With this awareness, a layer-3 switch can increase efficiency by delivering the traffic of a multicast group only to ports where the attached device has signaled that it wants to listen to that group.

- If a switch is not aware of multicasting and broadcasting, frames are also forwarded on all ports of each broadcast domain, but in the case of IP multicast this causes inefficient use of bandwidth. To work around this problem some switches implement IGMP snooping.
- The term "Layer 3 switch" often is used interchangeably with router, but switch is a general term without a rigorous technical definition. In marketing usage, it is generally optimized for Ethernet LAN interfaces and may not have other physical interface types.

5.6 ROUTERS

- In an environment that consists of several network segments with differing protocols and architectures, a bridge might be inadequate for ensuring fast communication among all segments.
- A network this complex needs a device that not only knows the address of each segment, but can also determine the best path for sending data and filtering broadcast traffic to the local segment. Such a device is called a "router".

Fig. 5.15: Router

- Routers are networking devices which interconnect two different networks. For an example your home router connects your internet connection with a private local network.
- Routers work at the Network Layer of the OSI reference model. This means they can switch and route packets across multiple networks. They do this by exchanging protocol-specific information between separate networks.
- Routers read complex network addressing information in the packet and because they function at a higher layer in the OSI reference model than bridges, they have access to additional information.
- Router's software and hardware are usually tailored to the tasks of routing and forwarding information. For example, on the Internet, information is directed to various paths by routers.
- Bridges work at the Data-link layer MAC sublayer, and Routers work at the Network Layer.

- Routers connect two or more logical subnets, which do not necessarily map one-to-one to the physical interfaces of the router. In comparison, a network hub does not do any routing; instead every packet it receives on one network line gets forwarded to all the other network lines.
- Routers operate in two different planes:
  1. Control Plane: In which the router learns the outgoing interface that is most appropriate for forwarding specific packets to specific destinations.
  2. Forwarding Plane: Which is responsible for the actual process of sending a packet received on a logical interface to an outbound logical interface.

Functions:

- Routers can provide the following functions of a bridge:
  - Filtering and Isolating traffic.
  - Connecting network segments.
  - Routers have access to more of the information in packets than bridges have and use this information to improve packet deliveries.
  - Routers are used in complex networks because they provide better traffic management.

Routing Table:

- Routers maintain their own routing tables, usually consisting of network addresses; host addresses can also be kept if the network architecture calls for it.
- To determine the destination address for incoming data, the routing table includes:
  1. All known network addresses.
  2. Instructions for connection to other networks.
  3. The possible paths between routers.
  4. The costs of sending data over those paths.
- Router uses its data-routing table to select the best route for the data based on costs and available paths.
- Routing tables play a very important role in the routing process. They are the means by which the router makes its decisions. For this reason, a routing table needs to do two things. It must be up-to-date and complete.

Routing Process:

- When routers receive packets destined for a remote network, they send them to the router that manages the destination network. In some ways, this is an advantage because it means routers can:
  1. Segment large networks into smaller ones.
  2. Act as safety barriers between segments.
  3. Prohibit broadcast storms, because broadcasts are not forwarded.

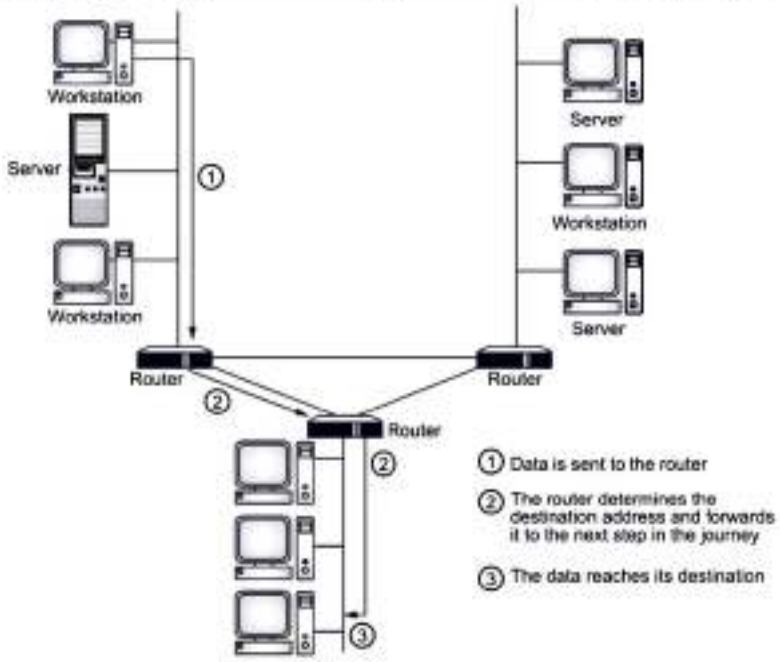


Fig. 5.16: Routing Process

- Routers do not communicate with remote hosts - it communicates only with other routers.
- **Routable Protocols:** Routing protocols determine how your data gets to its destination and helps to make that process as smooth as possible.
- All routing protocols can be classified into the following:
  - Distance Vector or Link State Protocols
  - Interior Gateway Protocols (IGP) or Exterior Gateway Protocols (EGP)
- Examples of IGP:
  - Open Shortest Path First (OSPF)
  - Routing Information Protocol (RIP)
  - Intermediate System to Intermediate System (IS-IS)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
- Examples of EGP:
  - Border Gateway Protocol (BGP)
  - Exterior Gateway Protocol (EGP)

- The ISO's InterDomain Routing Protocol (IDRP)

- Classful or Classless Protocols
  - Classful routing protocols don't send subnet mask information during routing updates but classless routing protocols do. Examples: RIPv1 and IGRP.
  - Classless routing protocols send IP subnet mask information during routing updates. Examples: RIPv2, EIGRP, OSPF, and IS-IS
- There are two ways that the router can get the information for the routing table - through Static routing or dynamic routing.
- Static routing is the process in which the system network administrator would manually configure network routers with all the information necessary for successful packet forwarding. The administrator constructs the routing table in every router by putting in the entries for every network that could be a destination.
- Dynamic routing protocols allow routers to automatically add information to their routing tables from connected routers. With these protocols, routers send out topology updates whenever the topological structure of the network changes.

Routing Components:

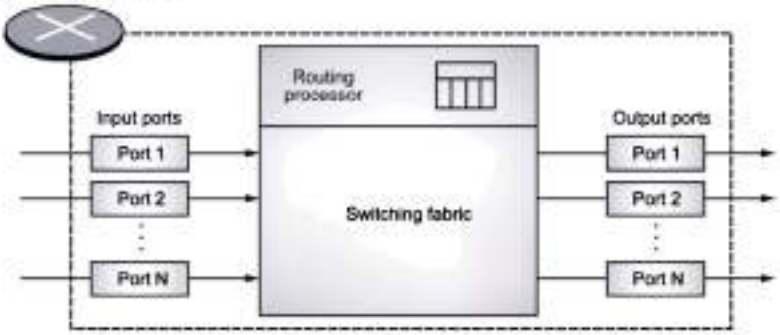


Fig. 5.17: Router Components

- Router has four components:
  1. Input ports
  2. Output ports
  3. Routing processor
  4. Switching fabric

Fig. 5.18: Input Port

- **Input port** performs the physical and data link layer functions of router. The bits are constructed from the received signal.
- **Output port** performs the same functions as the input port but in the reverse order. Packet is encapsulated in a frame and physically transmitted on the line in raw bits fashion.

Fig. 5.19: Output Port

- **Routing processor** performs the function at network layer. The destination address is used to find the address of the next hop and at the same time the output port number from which the packet is sent out.
- **Switching fabrics** is used to move the packet from the input queue to output queue.
- The switching fabric is most difficult process in router. The following switching techniques are used:
  (a) Crossbar switching
  (b) Banyan switching
  (c) Batcher-Banyan switch.

Advantages of Routers:

- Following are the advantages of Routers:
  1. It shares connection between different network architectures such as Ethernet & token ring etc.
  2. It can choose best path across the internetwork using dynamic routing techniques.
  3. It can reduce network traffic by creating collision domains and also by creating broadcast domains.
  4. It provides sophisticated routing, flow control and traffic isolation.
  5. They are configurable which allows network manager to make policy based on routing decisions.

Drawbacks or disadvantages of Routers:

- Following are the drawbacks or disadvantages of Routers:
  1. Dynamic router communications can cause additional network overhead. This results into less bandwidth for user data.
  2. They are slower as they need to analyze data from physical to network layer.
  3. They require considerable amount of initial configurations.

4. They are protocol dependent devices which must understand the protocol they are forwarding.
5. They only do operations using routable protocols.
6. They are expensive compare to other network devices.

5.7 GATEWAYS

- Gateways make communication possible between different architectures and environments. They repackage and convert data going from one environment to another so that each environment can understand the other's environment data.
- A gateway repackages information to match the requirements of the destination system.
- Gateways can change the format of a message so that it will conform to the application program at the receiving end of the transfer. A gateway links two systems that do not use the same:
  1. Communication protocols
  2. Data formatting structures
  3. Languages
  4. Architecture.
- For example, electronic mail gateways, such as X.400 gateway, receive messages in one format, and then translate it, and forward in X.400 format used by the receiver and vice versa.
- To process the data, the gateway:
  1. Decapsulates incoming data through the networks complete protocol stack.
  2. Encapsulates the outgoing data in the complete protocol stack of the other network to allow transmission.
- Also a gateway is a device that can join together networks that use different protocols, example, Novell SPX to TCP/IP. The gateway contains two complete protocol stacks - one for each system.

Levels of Gateways:

- Data is extracted from a packet arriving at one port and is retransmitted at the other port using a different protocol. Although gateways are considered to exist at the top of the OSI Reference Model, in reality they can be found at various levels of the model:
  - **Physical Layer Gateway:** Carries out translation from one speed to another or from one medium to another, i.e. 10 Mbps Ethernet to 100 Mbps Fast Ethernet or UTP to fiber optic (this term is not generally used).
  - **MAC Gateway:** Translates one MAC protocol to another, i.e. Token Ring to Ethernet or vice versa. These are more commonly referred to as translating and tunneling bridges.

- **Architecture Gateway:** Changes the packet from one protocol stack (or architecture) to another, i.e. SNA to TCP/IP, TCP/IP to IPX/SPX or TCP/IP to Appletalk. This is achieved by replacing all the headers from the network layer up to the application layer.
- **Application Gateway:** These can translate Application Layer protocols (X.500, X.400) or actual end user applications.

- Gateways can be either dedicated standalone box, a specific installed printed circuit-board or software loaded onto an existing server.
- The term Gateway is also used to refer to a network point that acts as an entrance to another network.
- In a company network, a proxy server acts as a gateway between the internal network and the Internet and may also act as a firewall server.
- The term is also used to refer to any device that passes packets from one network to another network in their trip across the Internet.
- Fig 5.20 shows the application gateway is required for communication between two different Network Architectures.

Fig. 5.20: Application Gateway

5.8 NETWORK INTERFACE CARD (NIC)

- A NIC is either an expansion card (the most popular implementation) or built in to the motherboard of the computer. In most cases, a NIC connects to the computer through expansion slots, which are special slots located on a computer's motherboard that allow peripherals to be plugged directly into it. In some notebook, NIC adapters can be connected to the printer port or through a PC card slot.
- NIC cards generally all have one or two light emitting diodes (LEDs) that help in diagnosing problems with their functionality. If there are two separate LEDs, one of them may be the Link LED, which illuminates when proper connectivity to an active network is detected. This often means that the NIC is receiving a proper signal from the hub/MAU or switch, but it could indicate connectivity to and detection of a carrier on a coax segment or connectivity with a router or other end device using a crossover

cable. The other most popular LED is the Activity LED. The Activity LED will tend to flicker, indicating the intermittent transmission or receipt of frames to or from the network.

Summary

- Networking connecting devices include all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network.
- A hub is a small rectangular box, often constructed mainly of plastic that receives its power from an ordinary wall outlet. A hub joins multiple computers or other network devices together to form a single network segment. Types are: Passive and Active Hub.
- Passive hub does not provide any additional feature except for working just as an interface between the topology.
- Active hub takes active participation in data communication within the network / LAN.
- A repeater is a network device that receives a signal on one of its connections and passes that signal on to all of its other connections after regenerating it.
- Network bridges can be used to connect LAN segments or to isolate heavily trafficked segments from the rest of the network. Three types of bridges are used in networks: Transparent Bridge, Source Route Bridge and Spanning tree bridge.
- A network switch is a computer networking device that connects network segments. The term commonly refers to a Network bridge that processes and routes data at the Data link layer (layer 2) of the OSI model. There are two kinds of switches - the workgroup switch and the enterprise switch.
- Routers can share status and routing information with one another and use this information to bypass slow or malfunctioning connections.
- Routers maintain their own routing tables, usually consisting of network addresses; host addresses can also be kept if the network architecture calls for it.
- Gateways make communication possible between different architectures and environments. They repackage and convert data going from one environment to another so that each environment can understand the other's environment data.

Check Your Understanding

1. _____ called Network layer Device.
   (a) Router (b) Gateway
   (c) Bridge (d) Switch
2. _____device is not amplified the signal.
   (a) Router (b) Gateway
   (c) Bridge (d) Switch

3. The device that provides a central connection point for cables is _____.
   (a) Router (b) Gateway
   (c) HUB (d) Switch
4. Which networking device connects one LAN to other LAN using same protocol standards?
   (a) Router (b) Gateway
   (c) HUB (d) Switch
5. _____ device is called intelligent device in networking
   (a) Router (b) Gateway
   (c) HUB (d) Switch

ANSWERS

(1) a	(2) b	(3) c	(4) d	(5) a		

Practice Questions

Q.I Answer the following questions in short.

1. What are network connectivity devices?
2. What is active and passive hub?
3. Which are types of bridges in networking?
4. Describe the term transparent bridge.
5. Which two frame types are used in order to find the route to the destination network segment in Source Route Bridging?

Q.II Answer the following questions.

1. What is Router? Explain its components..
2. Explain the various network connecting devices.
3. With a neat diagram explain repeaters.
4. Describe hub in brief.
5. Explain switches with suitable diagram.
6. What are repeaters? Define different types of repeaters.
7. Compare between:
   (i) Repeater and Hub
   (ii) Switches and Hub
   (iii) Bridges and Gateways
   (iv) Router and Hub.

Q.III Define the Terms:

1. Gateways
2. Source routing bridges

3. Router
4. Hub
5. Repeater

Previous Exams Questions

Summer 2018

1. Define the bridge. Explain the types of bridges. [5M]

Ans. Please refer to Section 5.4.

2. What is switch? How does it differ from HUB? [5M]

Ans. Please refer to Section 5.5 and 5.2.

3. Explain active and passive HUB. [5M]

Ans. Please refer to Section 5.2.2 and 5.2.3.

4. Write a short note on Repeater. [5M]

Ans. Please refer to Section 5.3.

Winter 2018

1. What is bridge? What are its types? Explain any one in details. [5M]

Ans. Please refer to Section 5.4.

Summer 2019

1. Define the Bridge. Explain types of Bridges. [5M]

Ans. Please refer to Section 5.4.

2. What is switch? How does it differ from HUB? [5M]

Ans. Please refer to Section 5.5 and 5.2

3. Explain active and passive HUB. [5M]

Ans. Please refer to Section 5.2.2 and 5.2.3

4. Write a short note on Repeater. [5M]

Ans. Please refer to Section 5.3

❖❖❖

6... Network Security

Objectives...

- To know the need for Network Security
- To learn about Security Services: Message-confidentiality, Integrity, Authentication, Non repudiation
- To study about types of Attack
- To get knowledge of Cryptography, PlainText, Cipher Text, Encryption, Decryption
- To learn Substitution Techniques, Caesar Cipher, and Transposition Cipher
- To get information about Firewalls, Steganography and Copyright

6.1 INTRODUCTION

- Network/Computer security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
- Users choose or are assigned an ID and password or other authenticating information that allows them to access the information and programs within their authority.
- Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among business, organizations government agencies and individuals.
- Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions.
- Providing network security means controlling systems to prevent any accidental and/or intentional data loss.
- The overall computer security is the protection of data and assets from unauthorized access, use, alteration or destruction.

- Mainly there are two types of security as explained below:
  1. **Physical Security:** Physical security includes protecting all hardware units of a network against any unauthorized access (here, preferably a theft minded person who want to steel the hardware units and destroy them) and against any natural disaster.
  2. **Logical Security:** The logical security deals with protecting the network data (software) from unauthorized access and of course from natural disaster.

6.2 NEED FOR SECURITY

- There are common mechanism to provide the basic security:
  1. Authenticate a user by providing a user identification and password to every user.
  2. Encode the information stored in the databases, so that it is not visible to those users who do not have right permission.
- Computer security deals with prevention and detection of unauthorized actions by users of a computer. In simple words security is defined as, "protecting information/ data from unintended/unauthorized access".

OR

- Security can be defined as, "the extent to which access the data can be restricted and hence protected against its illegal misuse and alteration."
- However, there are many examples of what could happen if there are insufficient securities built in applications developed for the Internet.
- To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability).
- With the advent of computers, information storage became electronic. Instead of being stored on physical media, it was stored in computers. The three security requirements however, did not change. The files stored in computers require confidentiality, integrity and availability.
- In the companies or business organizations, the security measures are very important to protect the data/information. These security measures include authentications, encryptions, access control, confidentiality, etc.
- The money transaction using credit card requires more security. There are many attacks reported using such transactions.

6.3 SECURITY SERVICES

- Security service is a processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. These services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

6.3.1 Messages

- Network security means to protect information. It deals with the prevention and detection of unauthorized actions by users of a computer.
- Before discussing general network security threats, we need to be familiar with the principle of security itself. The four principles of security are Confidentiality, Integrity, Authentication and Non-repudiation.

6.3.1.1 Confidentiality

- Confidentiality means maintain security and secrecy. This means only authorized people can see protected data or resources. The main issue here is to decide what is confidential and who has the right to access it.
- Confidentiality is concerned with keeping data secure from those who lack the need to know it.
- The objects are not disclosed to unauthorized subjects. If user X is sending the envelope (contains check) to user Y then user X will ensure that no one else, user Y gets the envelope.
- If another user Z gets access to this message without the permission and knowledge of X and Y then this type of attack is called interception. Interception causes loss of message confidentiality.

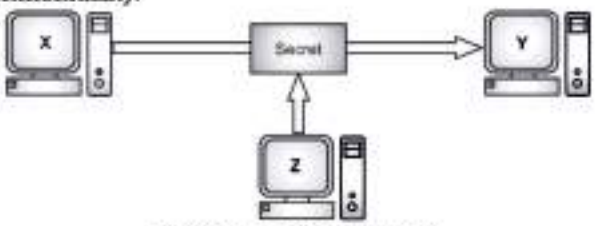


Fig. 6.1: Loss of Confidentiality

6.3.2 Integrity

- Integrity is concerned with keeping data pure and trustworthy by protecting data/information from intentional or accidental changes/modifications.
- The objects retain their veracity. The user X and user Y ensures that the contents in the envelope should not be tamper or change by other user. If content of message is change before it reaches to the intended recipient, then integrity of message is lost.
- The user X wants to send the message to user Y. The user Z change the original message contents by accessing it, and send the change message to user Y. Both X and Y are unaware of the such change. This attack is called modification. Modification causes loss of integrity.

Fig 6.2: Loss of Integrity

- In short, integrity concerned with preventing unauthorized modification/alteration of data/information.

6.3.3 Authentication

- Message authentication ensures that the message has been sent by a genuine identity and not by the fraud.
- Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying authorizations.
- If authentication principle followed, guarantees the valid and genuine message received from a trusted source through a valid transmission.
- Apart from intruders, the transfer of message between two people also faces other external problems like noise, which may alter the original message constructed by the sender. To ensure this, message authentication is needed.
- The service used to provide message authentication is a Message Authentication Code (MAC).
- MAC stands for Message Authentication Code. A MAC uses a keyed hash function that includes the symmetric key between the sender and receiver when creating the digest.

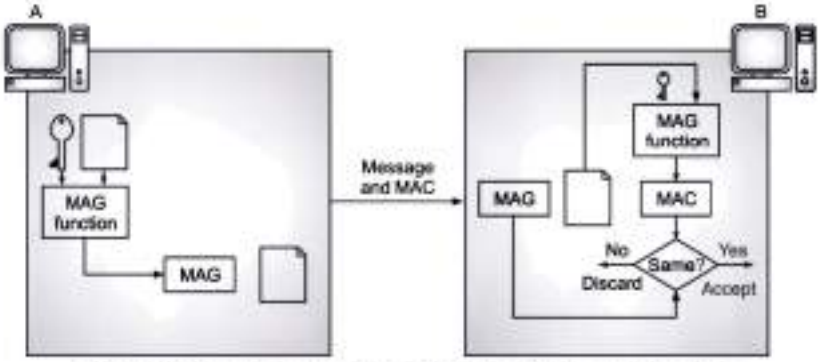


Fig. 6.3: MAC created by user A (sender) and checked by user B (Receiver)

- In MAC, sender and receiver share same key where sender generates a fixed size output called Cryptographic checksum or Message Authentication code and appends it to the original message. On receiver's side, receiver also generates the code and compares it with what he/she received thus ensuring the originality of the message.

6.3.4 Non-repudiation

- Non-repudiation refers to the fact that sender refuses sometimes for the transmission of the malicious messages. Therefore, it is important to have some methodology to verify the original sender of the message.
- In this principle, the user sends the message and later refuses (repudiates) that he/she had send the message. If Y deposits a check in the account and money get transferred from X's account to Y's account, and then X refuses having sent the check. In this fund transfer process, X's signature is required. Non-repudiation does not allow the sender of a message to refute the claim of not sending that message.

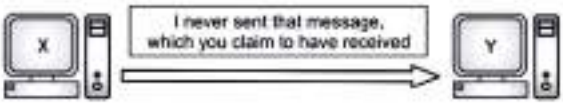


Fig. 6.4: Establishing Non-repudiation

Table 6.1: Summary of Security Principles

Sr. No.	Security Principle	Description	Compromising Attack	Security Solution
1.	Confidentiality	Only intended recipient must be able to access the message that has been sent secretly.	Interception	Symmetric key algorithms like DES, AES or IDEA and Asymmetric key algorithms like RSA.
2.	Integrity	Contents of the message must not be altered or modified by any means.	Modification	Message Digest algorithms like SHA, MD5.
3.	Authentication	The sender of the message must be properly identified.	Fabrication	Digital Signatures.
4.	Non-repudiation	One must not refuse transmission of the message.	Refusal of transmission	Digital Signatures.

6.3.5 Entity (User) - Authentication

- User authentication is performed in almost all human-to-computer interactions other than guest and automatically logged in accounts.
- One of the key aspects of cryptography and network/Internet security is authentication. Authentication helps establish trust by identifying the particular user/system. Authentication ensures that the applicant is really who he/she claims to be.
- Authentication is process of establishing the legitimacy of a node or user before allowing access to requested information.
- In most computer security contexts, user authentication is the fundamental building block and the primary line of defense. User authentication is the basis for most types of access control and for user accountability.
- RFC 2828 defines user authentication as, "the process of verifying an identity claimed by or for a system entity".
- User authentication is a method that keeps unauthorized users from accessing sensitive information. For example, User A only has access to relevant information and cannot see the sensitive information of User B.
- There are many methods to authenticate a user. Traditionally, user ids and passwords have been used. But there are many security concerns in this mechanism. Passwords can travel in clear text or can be stored in clear text on the server, both of which are dangerous propositions. Modern password-based authentication techniques use alternatives as encrypting passwords, or using something derived from the passwords in order to protect them.
- Authentication tokens add randomness to the password-based mechanism, and make it far more secure. This mechanism requires the user to possess the tokens. Authentication tokens are quite popular in applications that demand high security.
- Certificate-based authentication has emerged as a modern authentication mechanism, thanks to the emergence of the PKI technology. This is also quite strong, if implanted correctly. Smart cards can also be used in conjunction with this technology. Smart cards facilitate cryptographic operations inside the card, making the whole process a lot more secure and reliable.
- Biometrics is also getting a lot of attention these days, and is based on human biological characteristics. However, it has still not matured completely.
- In next sections, the above approaches of user authentication are explained in detail.

Types of Authentication:

- The main types of authentication available are Password based authentication, Token based authentication, Biometric based authentication and Image based authentication.

6.3.5.1 Password Based Authentication

- A password is a string of alphabets, numbers and special characters, which is supposed to be known only to the entity (usually person) that is being authenticated.
- Clear Text Password is the simplest Password based authentication mechanism. It works as follows as shown in Fig. 6. 5.
  - It prompts for user ID and Password.
  - User enters user ID and Password.
  - Validation User ID and Password.
  - Authentication Results.
  - User is informed accepted or rejected accordingly.

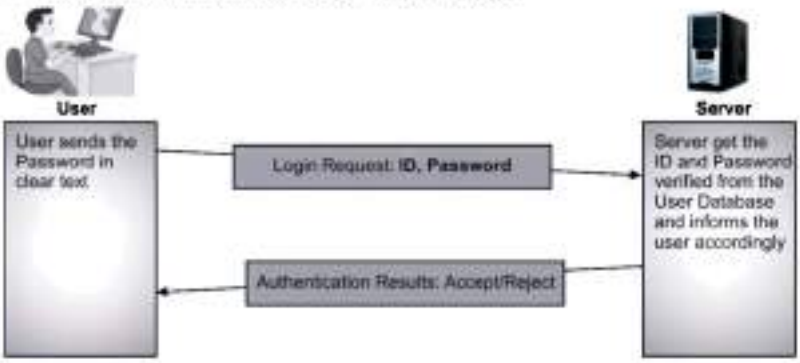


Fig. 6.5: User Authentication using Clear Text Password

- Problems with clear text passwords are as follows:
  1. Database contains passwords in clear text which is not secure. It is advised that password should not be stored in clear text in databases. Instead the passwords should be stored in encrypted form in database.
  2. Password travel in clear text from user's computer to the server. If the attacker breaks into the communication link, he can easily obtain the clear text password.

Improvements Over Basic Password Based Authentication:

- The variations from the basic password-based authentication are not to use password itself, but to use something that is derived from passwords.

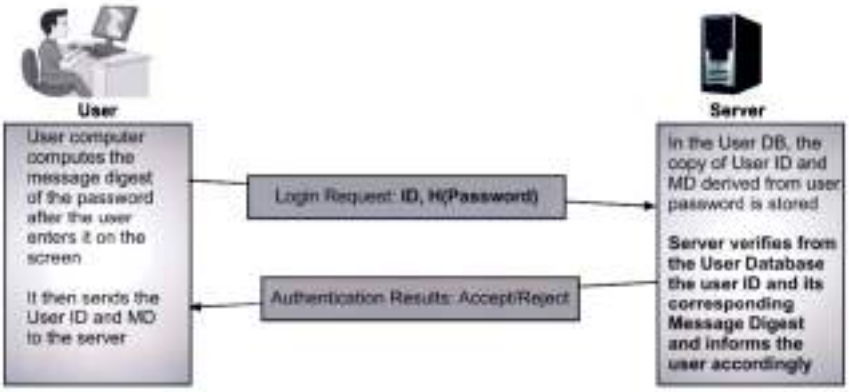
1. Storing Password in Encrypted or Derived Format:

- In this method, instead of storing password in clear text, it is stored in encrypted format. This method works as follows:
  - The user ID and password travels to the server in clear text.

- The server encrypts the password using password-encryption program and store it in database.
- When user wants to be authenticated the user enters the password, user's computer performs the same algorithm locally, and sends the derived password to server for verification.
- The server's user-authentication program now check the user-id and encrypted password against the database and inform user accepted or rejected accordingly.

2. Message Digest (MD) of Passwords:

- To solve the above problem of storing password in clear text in database, message digests as derived passwords stored in the user database. It works as follows shown in Fig. 6.16.
  - When a user needs to be authenticated, the user enters the ID and Password.
  - User's computer computes the message digest of the password
  - User's computer sends the user ID and computed Message Digest to the server for authentication.
  - Server verifies from the user databases the user ID and its corresponding Message Digest and inform user accepted or rejected accordingly.



* H(Password) = Message Digest (MD) derived from the User Password

Fig. 6.6: User Authentication using Message Digest of password

Problems with the Message Digests of the Passwords:

- An Attacker cannot compute the original password back from the message digest of the password, but he can simply copy the User ID and the corresponding Message Digest of the password, and submit them after some time to the same server as a part of the new login request.

- The server has no way of knowing that this login attempt is not from a legitimate user, but actually an attacker. This is called as **REPLAY ATTACK**, because the attacker simply replays the sequence of the actions of a normal user.

3. Adding Randomness:

- To improve the security and to detect a replay attack we need to add a bit of unpredictability or randomness to the earlier schemes. This will ensure that the replay attack is foiled:

(i) Storing Message Digests as derived passwords in the user database: User Ids and corresponding MDs are stored in user Database with the server.

(ii) User sends a login request: It contains only user ID.

(iii) Server creates a random Challenge: Server first verifies the validity of user ID. Then it sends a random challenge (a random number) to the user. Random challenge travels as plaintext from server to user computer.

(iv) User Signs the Random Challenge with the Message Digest of the Password: User Computer's computes the Message Digest (MD) of its password. User Computer's encrypts the Random Challenge by using MD of the Password. (symmetric key encryption). User Computer's sends the random challenge, which is encrypted with the message digest of the password to the server.

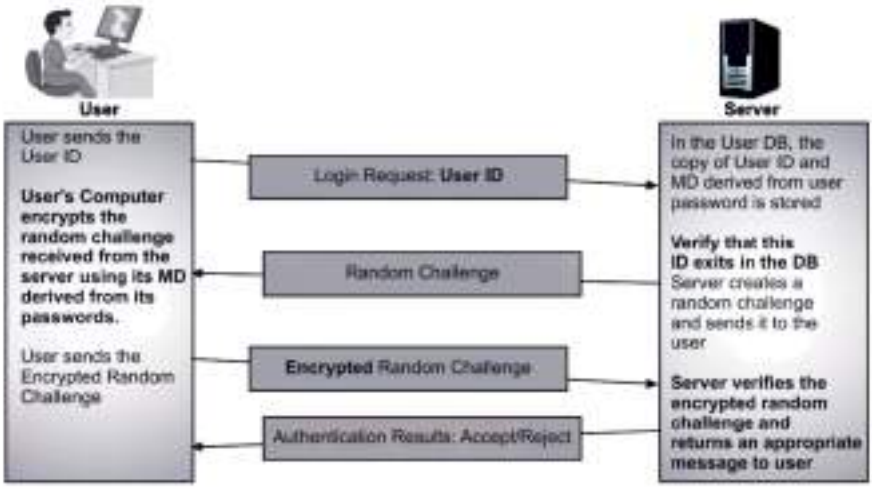


Fig. 6.7: Password Authentication using Randomness

(v) **Server Verifies the Encrypted Random Challenge from the user:** Server can do the verification in two ways either decrypting the Random Challenge or comparing the challenge values or it can encrypt the Random Challenge by the MD of the password and compare the two encrypted entities.

(vi) **Server returns an appropriate message back to the user Note:** The Random Challenge value is different every time. Therefore the random challenge encrypted with the MD of password would also be different. Therefore replay attacks can easy to detect.

Problems with the Passwords:

- Typically an organization has a number of applications, networks, shared resources and intranets. These applications may have varying needs of security measures; each resource may demand its own username and password. In that case end users/network administrators have to keep a large number of user ids and passwords to be used with different applications.
- Password maintenance is a very big concern for system administrations.
- Organizations specify password policies, which mandate the structure of passwords. For instance, an organization policy could have some of the following policies governing the passwords of its users:
  1. The password length must be at least 8 characters.
  2. It must not contain any blanks.
  3. There must be at least one lower case alphabet, one upper case alphabet, one digit and one special character in the password.
  4. The password must begin with an alphabet.
- There exit other authentication mechanisms as well besides password based authentication.

6.3.5.2 Authentication Tokens

- It is an extremely useful alternative to a password. An authentication token is a small device that generates a new random value every time it is used. This random value becomes the basis for authentication. These small devices are usually of the size of a small key chain, calculators or smart cards.
- In short, authentication token is a portable device for user authentication. Authentication tokens operate by challenge and response, time-based code sequences, or other techniques that may include paper-based lists of one-time passwords.
- Usually an authentication token has the features like processor, LCD for displaying outputs, battery, optionally a small keypad for entering information and optionally a real-time clock.

- Each authentication token is pre-programmed with a unique number called as a Random Seed or just Seed. The seed value forms the basis for ensuring the uniqueness of the output produced by the token.

Steps Involved in Authentication Token:

Step 1: Creation of a Token: It is created by the authentication servers that are designed to use with authentication tokens. A unique value i.e. a seed is automatically placed or pre-programmed inside each token by the server. Server also keeps a copy of the seed against the user ID in the user database. Seed can be conceptually considered as a user password. Difference is that the user password is known to the user, seed value remains unknown to the user.

Step 2: Use of the Token: An authentication token automatically generates pseudorandom numbers called one-time passwords. One Time Password (OTP) is generated randomly by authentication tokens using seed value.

Step 3: Validating Token: When a user wants to be authenticated by any server, the user will get a screen to enter user ID and the latest One time password. The users enter its ID and gets is latest one-time password from the authentication token. The user ID and password travels to the server as a part of the login request. Server verifies the ID, and one-time password using the stored seed value from user DB. Then Server sends an appropriate message back to the user.

6.3.5.3 Types of Authentication Tokens

- There are main two types of authentication tokens namely, Synchronous dynamic token or time-based tokens and Asynchronous dynamic token or challenge or response tokens.
- A synchronous token generates a unique password at fixed time intervals with the authentication server. An asynchronous token generates the password based on a challenge/response technique with the authentication server, with the token device providing the correct answer to the authentication server's challenge.

1. **Synchronous Dynamic Token:**

- Synchronous dynamic token use time or counters to synchronize a displayed token code with the code expected by the Authentication Server (AS).
- Time-based synchronous dynamic token display dynamic token codes that change frequently, such as every 60 seconds. The dynamic code is only good during that window.
- The AS knows the serial number of each authorized token, as well as the user with whom it is associated and the time. It can predict the dynamic code of each token using these three pieces of information.

- Counter based synchronous dynamic tokens use a simple counter, the AS expects token code 1, and the user's token displays the same code 1. Once used, the token displays the second code, and the server also expects token code 2.

2. **Asynchronous Dynamic Token:**

- Asynchronous dynamic tokens are not synchronized with a central server. The most common variety is challenge-response tokens.
- Challenge-response token authentication systems produce a challenge or input the token device.
- The user manually enters the information into the device along with their PIN, and the device produces an output, which is then sent to the system.
- The advantage of a token device is, it usually only implemented in very secure environments because of the cost of deploying the token device.
- The disadvantages of tokens are their small size and their price. If the token breaks or becomes lost, a replacement will be needed to gain access.

6.3.5.4 Multifactor Authentication

- One method for ensuring proper authentication security is the use of multifactor authentication. Multifactor authentication gets its name from the use of multiple authentication factors.
- We can think of a factor as a category of authentication. There are three authentication factors that can be used namely **'something you know'**, (would be a password, a PIN etc.), **'something you have'** (would be a token or a smart card etc.) and **'something you are'** (would be biometric identity, like a fingerprints, retina etc.).
- In order for something be considered multifactor authentication, it must make use of at least two of the three factors mentioned. For example, when a user attempts to authenticate, he or she may have to enter both their password and a one-time use token code.
- If the authentication token device gets stolen, PIN numbers are used to generate one-time passwords with the authentication token devices.
  1. **Password is a 1-factor authentication:** It is something you know.
  2. **Authentication Token are 2-factor authentication:** We must have something that is authentication token itself and PIN to protect it.

6.3.5.5 Biometric Authentication

- Biometric authentication is a type of system that relies on the unique biological characteristics of individuals to verify identity for secure access to electronic systems.
- The biometric technologies involved are based on the ways in which individuals can be uniquely identified through one or more distinguishing biological traits, such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, keystroke dynamics, DNA and signatures.

- Biometric authentication is the application of that proof of identity as part of a process validating a user for access to a system.
- Biometric technologies are used to secure a wide range of electronic communications, including enterprise security, online commerce and banking; even just logging in to a computer or smart phone.
- Biometric verification is considered a subset of biometric authentication. Di Nardo defines biometrics as, "the automated use of physiological or behavioral characteristics to determine or verify identity".

Working of Biometric Authentication System:

- The user database contains a sample of user's biometric characteristics.
- During the authentication, the user is required to provide another sample of the users' biometric characteristic.
- This is matched with the one in the database, and if the two samples are same, the user is considered to be a valid one.
- The samples produced during every authentication process can vary slightly (e.g. cuts on the finger). So an approximate match can be acceptable.
- This is also the reason why, during the user registration process, multiple samples of the user biometric data are created. They are combined and their average stored in the user database, so that the different possibilities of the user's samples during the actual authentication can roughly map to this average sample.
- The biometric authentication process consists of several stages such as measurement, signal processing, pattern matching, and decision making.
- Measurement involves sensing biometric characteristics and is necessary both for the creation of the reference model and for each authentication trial. For example, when voice verification is utilized, this stage involves recording one's voice through a microphone.
- Then the digital data are mathematically modeled. When the user wants to be authenticated, the device compares the received data to the user model and makes a decision mostly based on a pre-calculated threshold.
- Any Biometric Authentication System defines following two configurable parameters:
  1. **False Accept Ratio (FAR):** FAR is a measurement of the chance that a user who should be rejected is actually accepted by a system as good enough.
  2. **False Reject Ratio (FRR):** It is a measurement of the chance that a user who should be accepted as valid is actually rejected by a system as not good enough.
- Thus FAR and FRR are exactly opposite to each other and in general can be controlled by a confidence threshold. To increase the security of the system, the threshold can be increased, which decreases FA errors and increases FR errors.

Types of Biometric Authentication Techniques:

- Biometric techniques are generally classified into two sub-categories namely, Physiological techniques and Behavioral techniques.

1. Physiological Techniques:

- Physiological biometrics is related to human body shape and features. With the change of this body geometry, these biometrics need to be updated to avoid failure of authentication. In general, the accuracy of physiological biometrics is higher than behavioral biometrics.
- Several techniques mentioned below:
  - (i) **Retina Scans,** produce an image of the blood vessel pattern in the light-sensitive surface lining the individual's inner eye.
  - (ii) **Iris Recognition,** is used to identify individuals based on unique patterns within the ring shaped region surrounding the pupil of the eye.
  - (iii) **Finger Scanning,** the digital version of the ink-and-paper fingerprinting process, and works with details in the pattern of raised areas and branches in a human finger image.
  - (iv) **Finger Vein ID,** is based on the unique vascular pattern in an individual's finger.
  - (v) **Facial Recognition Systems,** work with numeric codes called face prints, which identify 80 nodal points on a human face.
  - (vi) **Voice Identification Systems,** rely on characteristics created by the shape of the speaker's mouth and throat, rather than more variable conditions.

2. Behavioral Techniques:

- Behavioral biometrics is related to certain kind of behavior of an individual. Hence, this authentication system can prevent a person from accessing a cyber-system, if his current behavior pattern is different from the stored behavioral pattern.
- Examples of this type of biometrics are keystroke analysis, mouse dynamics, signature, gesture, etc.

(i) Keystroke Analysis:

- Keystroke recognition is a behavioral biometric trait which captures the unique way a person types in order to correctly verifies the identity of the individual.
- Typing patterns are generally extracted from computer keyboards, phone's virtual keyboard, etc. In order to extract features for keystroke recognition, it is needed to consider the time taken to move between two keys, how hard the buttons are pressed, and how long a key is pressed before it is released.

(ii) Signature Authentication:

- Handwritten signature authentication is based on systems for signature verification and signature identification. The given signature belongs to a particular person or is

not decided through a signature identification system, whereas the signature verification system decides if a given signature belongs to a claimed person or not.

- Signature-based authentication can be either static or dynamic. In the static mode (referred to as off-line), only the digital image of the signature is available.
- In the dynamic mode, also called "on-line", signatures are acquired by means of a graphic tablet or a pen-sensitive computer display.

Advantages and Limitations of Biometric Systems:

Advantages:

1. Improved security.
2. Improved customer experience.
3. Cannot be forgotten or lost.
4. Reduced operational costs.

Limitations:

1. Biometrics can be complicated and costly to deploy. All biometric deployments require installation of their own hardware and application servers.
2. The market is still fractured. Should you buy a fingerprint reader, a voice recognition system or an iris scanner? Since each product differs greatly in its approach and installation, it is difficult to compare them during a typical company bid process.
3. Biometric data is like any other data. It sits on servers, which are bait for hackers if not properly hardened and secured. Therefore, when reviewing any biometric product, make sure it transmits data securely, meaning encrypted, from the biometric reader back to the authenticating server. And, make sure the authenticating server has been hardened, patched and protected.
4. Biometric readers are prone to errors. Fingerprints can smudge, faces and voices can be changed and all of them can be misread, blocking a legitimate user, or permitting access to an unauthorized or malicious user.
5. Difficulties with user acceptance. Properly trained employees may be willing to use biometrics devices, but customers, like those logging on to the Web site, may be more reluctant to use – or worse, forced to purchase – a device that's difficult to use or makes doing business, such as banking, on the site, a hassle instead of a convenience. And both the employees and customers may be squeamish about exposing their eyes to devices like iris scanners, even if they appear harmless.

6.3.5.6 Image-based Authentication

- Common user authentication based on passwords has the main drawback of the human difficulty in recalling them. An authentication system based on character strings as password is very vulnerable.

- An attacker can guess the user password when people use words that are easy to remember or he can use the well-known dictionary attacks methods for discovering the password.
- Images are easier to remember than passwords. An authentication method based on images can improve the security of the user authentication compared to that of textual password.
- An image based authentication system has following advantages:
  1. The user can remember images more easily than passwords ;
  2. The system will be less vulnerable to hacker attack techniques. For this reason, the use of personal/personalized images can be a means of user authentication more effective than string based (password) authentication.
  3. Moreover, modern compression and transmission techniques make image exchange between different devices (e.g. mobile phones, personal digital assistants, laptops, and workstations) in heterogeneous networks practically feasible.
- An authentication system can collect user images to be used by a challenge and response protocol for authenticating the user. Functionalities such as scalability, progressive image transmission, client/server interactivity are undoubtedly necessary in order to make the image exchange and user authentication process feasible.
- The image-based authentication identifies users by utilizing the clicked information that is inputted from the user on specific images that are displayed on the monitor as the password.
- When the clicked information is equal to the clicked information that is registered on the authentication server, the user is identified correctly. This method is mainly utilized for high-priority services such as e-commerce and Internet-baking services.

Fig. 6.8: An Example of the Image-based Authentication applied on the Internet Banking Service

6.4 TYPE OF ATTACKS

- An attack is a threat that is carried out (threat action) and if successful, leads to an undesirable violation of security. The person who carrying out the attack is referred to as attacker.
- In the next section, we will study various types of attacks.

6.4.1 Attacks (A General View)

- A network security attack refers to, an act of breaching the security provisions of a network.
- Attacks are classified into three categories as shown in Fig. 6.9.

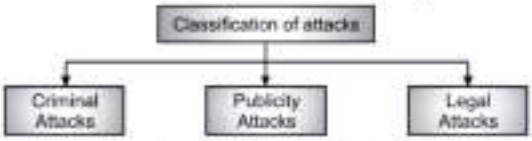


Fig. 6.9: Classification of Attacks

- The attacks in Fig. 6.9 are explained below:
  1. **Criminal Attacks:** The aim of the attacker is to maximize financial gain by attacking computer system. Fraud (credit cards, ATM, checks etc.), Scams (sale of services, auctions, business opportunities), Destructions, identity theft, intellectual property theft, Brand theft are some form of criminal attacks.
  2. **Publicity Attacks:** These types of attacks are usually not hardcore criminals. The people or students of university, or employees, uses a novel approach of attacking computer systems for publicity. For example, damage of web pages of a site by attacking it.
  3. **Legal Attacks:** The attacker attacks the computer system and the attacked party manages to take the attacker to the court. In such case, the attackers try to convince the judge that there is a weakness in the computer system and easily escape.

6.4.2 Attacks (A Technical View)

- The attacks are generally classified into four categories in terms of principle of security as follows:

1. **Interruption:** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Availability is concerned with keeping data and resources available for authorized use when they are needed.

   Examples:

   (i) Destroying some hardware (disk or cable).

(ii) Disabling file system.

(iii) Swamping a computer with jobs or communication link with packets.

2. **Interception:** An unauthorized party gains access to an asset. This is an attack on confidentiality.

   Examples:

   (i) Wiretapping to capture data in a network.

   (ii) Illicitly copying data or programs.

3. **Modification:** An unauthorized party gains access and tampers an asset. This is an attack on integrity.

   Examples:

   (i) Changing data files.

   (ii) Altering a program.

   (iii) Altering the contents of a message.

4. **Fabrication:** An unauthorized party inserts a counterfeit object into the system. This is an attack on authenticity.

   Examples:

   (i) Insertion of records in data files.

   (ii) Insertion of spurious messages in a network (message replay).

- These attacks are further grouped into active attacks and passive attacks as shown in the Fig. 6.10.

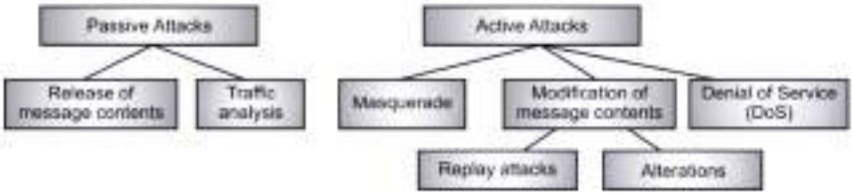


Fig. 6.10: Active and Passive Attacks

6.4.2.1 Active Attacks

- In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses.
- Active attacks include attempts to avoid or break protection features, to introduce malicious code, and to steal or modify information.
- These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave.

- Active attacks result in the disclosure or dissemination of data files or modification of data.
- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into three categories: masquerade, modification of messages, and Denial of Service (DoS).
- Modification attacks can be classified further into replay attacks and alteration of messages.
- Fabrication causes Denial of Service (DOS) attacks.

1. **Masquerade Attacks:** These attacks takes place when one entity pretends to be a different entity. The user Z might pose as user X and send the message to user Y. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

   Example: An entity captures an authentication sequence and replays it later to impersonate the original entity.

2. **Modification of Messages:** A portion of a legitimate message has been altered to produce an undesirable effect. In other words, some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver, even if we do not require confidentiality for all communications, we do not want any of our messages to be modified in transit.

   Example: If we are exchanging purchase requisitions, we do not want the items, amounts or billing information to be modified.

3. **Replay Attacks:** An attack in which a service already authorized and completed is forged by another duplicate request in an attempt to repeat authorized commands. Replay involves capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

   Example: The user X wants to send some amount to the user Z's bank account. Both X and Y have account with bank Y. User X sends an electronic message to bank Y for fund transfer. User Z could capture this message and send second copy of the same to bank Y. Bank Y would have no idea that this is an unauthorized message and treats the second message as different message. So user Z would get the benefits of the fund transfer twice.

4. **Denial of Service (DoS):** Prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target.

Examples: An entity may suppress all messages directed to a particular destination (For example, the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

5. **Alteration:** Alteration of message involves some changes/modifications in the original message.

6.4.2.2 Passive Attacks

- A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks.
- Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords.
- Passive interception of network operations enables adversaries to see upcoming actions.
- Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.
- Passive network security attacks are in the nature of eavesdropping of transmissions of many types.
- The goal of passive attack or the hacker is to gain information being transmitted in the message to gain an edge on the other party.
- There are two main types of passive attacks as explained below:

1. **Release of a Message Contents:** In this contents of a message are read and a message may be carrying sensitive or confidential data. Release of message content - is easy to grasp just from its name and what it does it easily figured out also. In this type of passive attack a mail message, phone call any transferred message pretty much of sensitive information that would be intercepted or listened to.

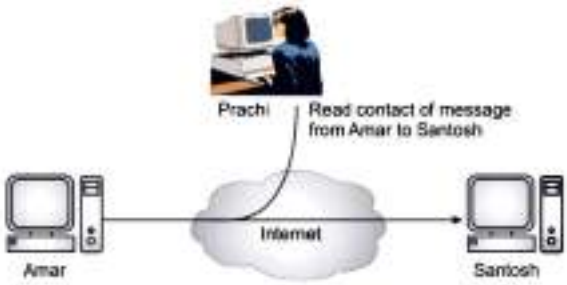


Fig. 6.11: Release of Message Contents

2. **Traffic Analysis:** In traffic analysis the intruder makes inferences by observing message patterns and can be done even if messages are encrypted. Traffic Analysis is a little more complicated. It is very subtle and hard to detect. It would be like this if we had a way to hide the information in the message and the hacker has still viewed the information this would be a traffic analysis attack.

- Passive attacks are very hard to detect because they do not damage or change the information so we cannot tell they have been attacked.
- There are many different programs out there which can help monitor against this type of network attack and against many other attacks. Again these are made for spying and for the attacker not to be noticed.

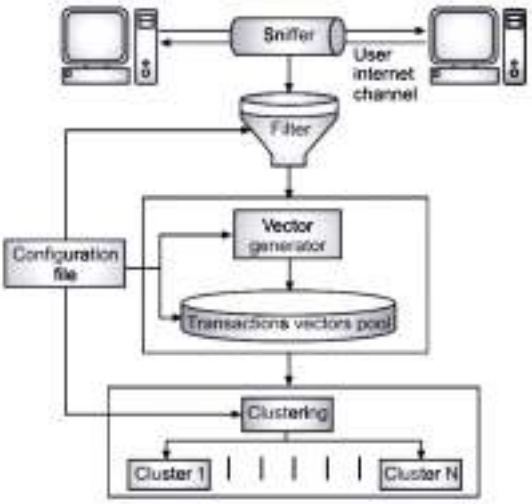


Fig. 6.12: Traffic Analysis

6.4.3 Programs that Attack

- In this section we study various programs which cause attacks:

1. **Virus:**

- A virus is a computer program that attacks itself to another legitimate program, and causes damage to the computer system or to the network.
- A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity such as some may cause only mildly annoying effects while others can damage the hardware, software or files.

- Almost all viruses are attached to an executable file, which means the virus may exist on the computer but it actually cannot infect the computer unless we run or open the malicious program.

2. **Worm:**

- A worm does not perform any destructive actions, and instead, only consumes system resources to bring it down.
- A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.
- The biggest danger with a worm is its capability to replicate itself on the system, so rather than the computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

3. **Trojan Horse:**

- A Trojan Horse allows an attacker to obtain some confidential information about a computer or a network.
- The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on the computer. Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source.
- Unlike viruses and worms, Trojans do not reproduce by infecting other files nor they do self-replicate.

6.4.4 Specific Attacks

- There are at least seven types of network attacks which explained below:

1. **Packet Spoofing (Identity Spoofing or IP Address Spoofing):**

- Any internet connected device necessarily sends IP datagrams into the network. Such internet data packets carry the sender's IP address as well as application layer data.
- If the attacker obtains control over the software running on a network device, they can then easily modify the device's protocol to place an arbitrary IP address into the data packet's source address field.
- This is known as IP spoofing, which makes any payload appear to come from any source. With a spoofed source IP address on a datagram, it is difficult to find the host that actually sent the datagram.
- The countermeasure for spoofing is ingress filtering. Routers usually perform this. Routers that perform ingress filtering check the IP address of incoming datagrams and determine whether the source addresses that are known to be reachable via that interface.
- If the source address is not in the valid range, then such packets will be discarded.

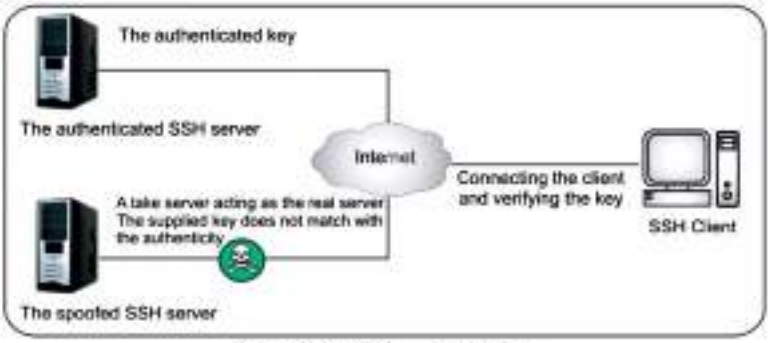


Fig. 6.13: Packet Spoofing Attack

2. Packet Sniffing:

- Packet sniffing is the interception of data packets traversing a network. A sniffer program works at the Ethernet layer in combination with Network Interface Cards (NIC) to capture all traffic traveling to and from internet host site.

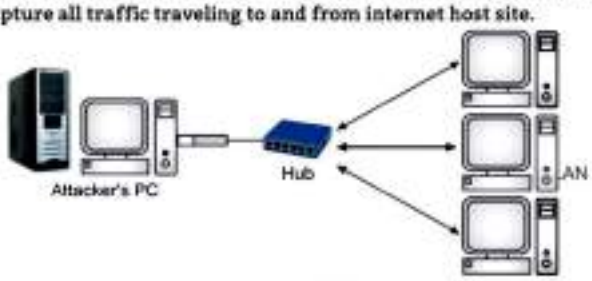


Fig. 6.14: Packet Sniffing Concept

- Further, if any of the Ethernet NIC cards are in promiscuous mode, the sniffer program will pick up all communication packets floating by anywhere near the internet host site.
- A sniffer placed on any backbone device, inter network link or network aggregation point therefore it will be able to monitor a whole lot of traffic.
- Most of packet sniffers are passive and they listen all data link layer frames passing by the device's network interface. There are dozens of freely available packet sniffer programs on the internet. The more sophisticated ones allow more active intrusion.
- The key to detecting packet sniffing is to detect network interfaces that are running in promiscuous mode. Sniffing can be detected two ways:

  (i) **Host-based:** Software commands exist that can be run on individual host machines to tell if the NIC is running in promiscuous mode.

(ii) **Network-based:** Solutions tend to check for the presence of running processes and log files, which consume a lot of sniffer programs. However, sophisticated intruders almost always hide their tracks by disguising the process and cleaning up the log files.

- The best countermeasure against sniffing is end-to-end or user-to-user encryption.

3. Mapping (Eavesdropping):

- Before attacking a network, attackers would like to know the IP address of machines on the network, the operating systems they use, and the services that they offer.
- With this information, their attacks can be more focused and are less likely to cause alarm. The process of gathering this information is known as mapping.

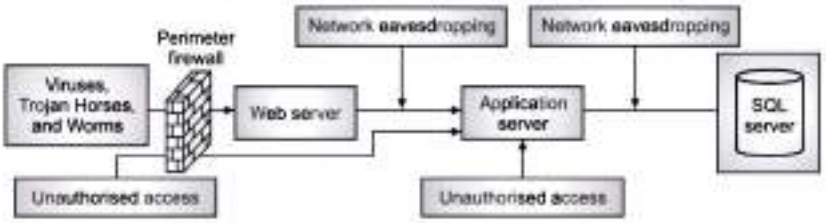


Fig. 6.15: Process of Mapping (Eavesdropping)

- In general, the majority of network communications occur in an unsecured or clear text format, which allows an attacker who has gained access to data paths in your network to listen in or interpret the traffic.
- When an attacker is eavesdropping on your communications, it is referred to as *sniffing* or *snooping*. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise.
- Counter measures are strong encryption services that are based on cryptography only. Otherwise, the data can be read by others as it traverses the network.

4. Phishing:

- Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
- Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate one and the only difference is the URL of the website in concern. Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims.

- Phishing emails may contain links to websites that are infected with malware.

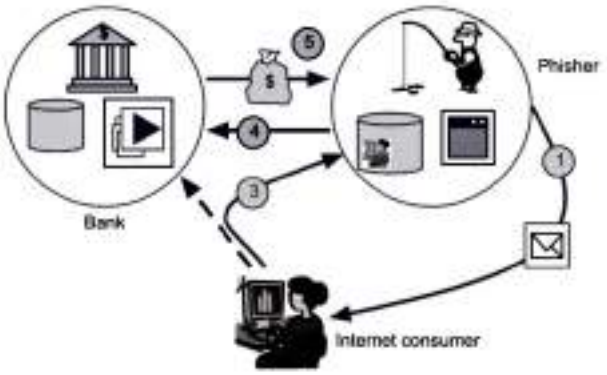


Fig. 6.16: Phishing Attack

5. Pharming (DNS Spoofing):

- DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

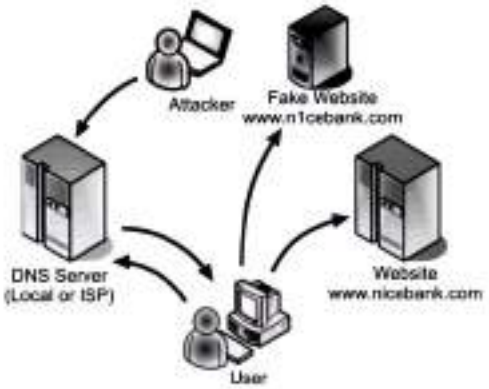


Fig. 6.17: DNS Spoofing Attack

- A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask

another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time. This means if it receives another request for the same translation, it can reply without needing to ask any other servers, until that cache expires.

- When a DNS server has received a false translation and caches it for performance optimization, it is considered poisoned, and it supplies the false data to clients. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer (often an attacker's).

6.5 CRYPTOGRAPHY

- Cryptography is the study of secret (crypto) writing (graphy).
- Cryptography is the art of achieving security by encoding messages to make them non-readable.
- It concerned with developing algorithms which may be used to:
  1. Conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or
  2. Verify the correctness of a message to the recipient (authentication). Cryptography forms the basis of many technological solutions to computer and communications security problems.
- Cryptography is the study of mathematical techniques for all aspects of information security. Cryptanalysis is the complementary science concerned with the methods to defeat these techniques.
- Cryptanalysis is the technique of decoding messages from a non-readable format back to a readable format without knowing how they were initially converted from readable format to non-readable format.
- Cryptology is a combination of Cryptography and Cryptanalysis, (See Fig. 6.18).

Fig. 6.18: Cryptographic and Cryptanalysis System

Purpose of Cryptography:

- Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription.

- In computer field cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.
- Within the context of any application-to-application communication, there are some specific security requirements, including:
  1. **Authentication:** The process of proving one's identity. (the primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak).
  2. **Privacy/Confidentiality:** Ensuring that no one can read the message except the intended receiver.
  3. **Integrity:** Assuring the receiver that the received message has not been altered in any way from the original.
  4. **Non-repudiation:** A mechanism to prove that the sender really sent this message.
- Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.
- There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below.
- In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into ciphertext, which will in turn (usually) be decrypted into usable plaintext.

Objectives of Cryptography:

- Modern cryptography concerns itself with the following four objectives or goals:
  1. **Confidentiality:** The information cannot be understood by anyone for whom it was unintended.
  2. **Integrity:** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
  3. **Non-repudiation:** The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
  4. **Authentication:** The sender and receiver can confirm each other's identity and the origin/ destination of the information.

6.5.1 Plaintext and Ciphertext

- The plaintext or clear text message can be understood by anybody, (sender, recipients) else who gets access total message.
- When a plaintext message is codified using any suitable scheme (encryption), the resulting message is called ciphertext.
- Fig. 6.19 shows an example for plaintext and ciphertext messages.

Plaintext: YOUAREACOMPUTEREXPERT

Ciphertext: BRXDUHDFRPSXWUHASHUW

Fig. 6.19: Plaintext and Ciphertext

- In short, plaintext refers to the original unencrypted message that the sender wishes to send while ciphertext refers to the encrypted message that is received by the receiver.
- Fig. 6.20 shows basic model for encryption.

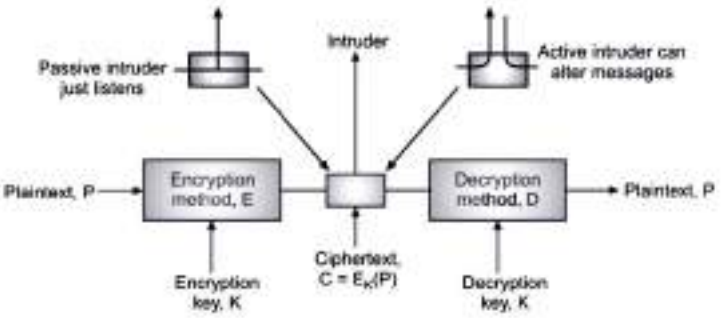


Fig. 6.20: The Basic Encryption Model

- The messages to be encrypted, known as the 'plaintext', are transformed by a function that is parameterized by a 'key'.
- The output of the encryption process, known as the 'ciphertext', is then transmitted, often by messenger or radio.
- We assume that the enemy, or 'intruder', hears and accurately copies down the complete ciphertext.
- However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the ciphertext easily.
- Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify messages before they get to the receiver (active intruder).
- The art of breaking ciphers, called cryptanalysis, and the art devising them (cryptography) is collectively known as cryptology.
- Encryption methods have historically been divided into two categories namely, substitution ciphers and transposition ciphers.

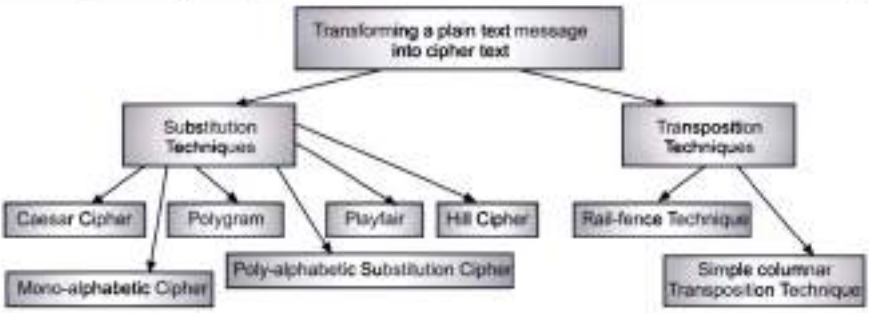


Fig. 6.21: Techniques of Transforming a Plaintext into Ciphertext

6.5.2 Encryption and Decryption

- Encryption is the process of converting the original information which is in meaningful and readable form (in cryptography we called it as plaintext) into unreadable form (in cryptography we called it is ciphertext) and requires a key for this conversion.
- The process of converting the ciphertext into plaintext is called decryption. Decryption is the reverse process of encryption and also uses a key for conversion.
- There are a number of algorithms available for encryption. Depending upon the number of key/keys used encryption is divided into two types namely, symmetric encryption and asymmetric encryption.
- A model used for encryption and decryption process is called a cryptosystem. The area of study in which one can study various techniques of encryption is known as cryptography.
- There are various techniques available to derive the plaintext or decrypt the ciphertext without much knowledge about the key and plaintext and this process is called cryptanalysis. The area of cryptography and cryptanalysis together are called cryptology.
- Fig. 6.22 (a) shows encryption and decryption process.

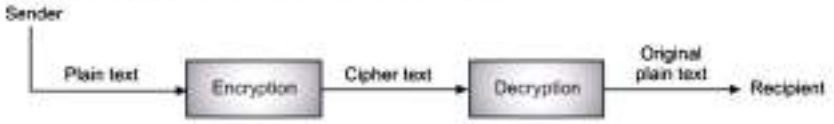


Fig. 6.22 (a): Encryption and Decryption Process

- Fig. 6.22 (b) shows an example of encryption and decryption. The process of encoding the plaintext into the ciphertext is called encryption. Decryption transforms a ciphertext message back into plaintext.

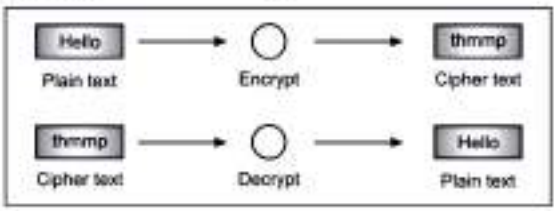


Fig. 6.22 (b): Encryption and Decryption

- Every encryption and decryption process has the algorithm and the key. The algorithm is known, but the key used for the encryption and decryption is cryptography secure.
- To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used.
- There are two cryptographic mechanisms namely, Symmetric key cryptography and Asymmetric key cryptography.
- Symmetric key cryptography involves the usage of the same key for encryption and decryption. Asymmetric key cryptography involves the usage of the one key for encryption and different key for decryption.
- The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext to ciphertext; a decryption algorithm transforms the ciphertext back to plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.
- We can divide all the cryptography algorithms in the world into two groups: symmetric-key (sometimes called secret-key) cryptography algorithms and asymmetric-key (often called public-key) cryptography algorithms.

6.5.3 Symmetric Key Cryptography

- Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way.
- This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.
- Symmetric key encryption is also known as shared-key, single-key, secret-key, private-key or one-key encryption.

- In this type of message encryption, both sender and receiver share the same key which is used to both encrypt and decrypt messages. Sender and receiver only have to specify the shared key in the beginning and then they can begin to encrypt and decrypt messages between them using that key.
- Examples include AES (Advanced Encryption Standard) and TripleDES (Data Encryption Standard).
- In symmetric cryptography (or symmetric-key encryption), the same key is used for both encryption and decryption as shown in Fig. 6.23.

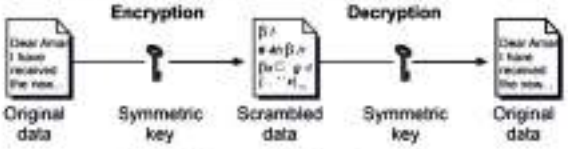


Fig. 6.23: Symmetric Key Encryption

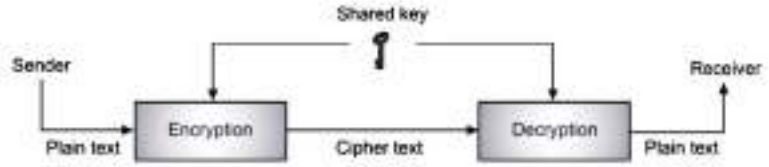


Fig. 6.24: Message Exchange Using Secret Key

- Symmetric key ciphers are valuable because:
  1. It is relatively inexpensive to produce a strong key for these ciphers.
  2. The keys tend to be much smaller for the level of protection they afford.
  3. The algorithms are relatively inexpensive to process.
- Therefore, implementing symmetric cryptography (particularly with hardware) can be highly effective because we do not experience any significant time delay as a result of the encryption and decryption.
- Symmetric cryptography also provides a degree of authentication because data encrypted with one symmetric key cannot be decrypted with any other symmetric key.
- Therefore, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.
- Typically, with a symmetric key, we can exchange the key with another trusted participant; usually we produce a unique key for each pair of participants. We can be

assured that any messages that we exchange, which are encrypted in a specific key, between the participants can only be deciphered by the other participant that has that key. In this way, the key must be kept secret to each participant.

- When user A wanted to communicate with B, then we need one lock-and-key pair (A-B). When user A wanted to communicate with B and C, then we need two lock-and-key pair (A-B, and A-C), and B wants to communicate with C then pair is (B-C). When user A, B, C and D wanted to communicate with each other, then we need lock-and-key pairs (A-B, A-C, A-D, B-C, B-D, C-D). In general, for n users, the number of lock-and-key pairs is

$$n \times (n-1)/2$$

- Consequently, these keys are also referred to as secret-key ciphers. If anyone else finds the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but can encrypt new messages and send them as if they came from one of the two parties who were originally using the key.

Advantages:

1. **Simple:** This type of encryption is easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages.
2. **Fast:** Symmetric key encryption is much faster than asymmetric key encryption.
3. **Less Computer Resources:** Single-key encryption does not require a lot of computer resources when compared to public key encryption.
4. **Prevents Widespread Message Security Compromise:** A different secret key is used for communication with every different party. If a key is compromised, only the messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.

Disadvantages:

1. **Need for Secure Channel for Secret Key Exchange:** Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures it remains secret.
2. **Too Many Keys:** A new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys.
3. **Origin and Authenticity of Message cannot be Guaranteed:** Since, both sender and receiver use the same key, messages cannot be verified to have come from a particular user. This may be a problem if there is a dispute.

6.5.4 Asymmetric Key Cryptography

- The concept of modern Asymmetric Cryptography or Public Key Cryptography ("PKC") was published in a Mathematics paper titled, "New directions in

cryptography" by a Stanford University professor Martin Hellman and a graduate student Whitfield Diffie in 1976. Diffie and Hellman can be regarded as the fathers of the asymmetric key cryptography.

- Asymmetric key cryptography is known as public key cryptography. It uses two separate keys namely one private and one public.
- The encryption process where different keys are used for encrypting and decrypting the information is known as asymmetric key encryption.
- Encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.
- A public-key encryption scheme has six parts:
  1. **Plaintext:** This is the readable message or data that is fed into the algorithm as input.
  2. **Encryption Algorithm:** The encryption algorithm performs various transformations on the plaintext.
  3. & 4. **Public and Private Keys:** This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
  5. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
  6. **Decryption Algorithm:** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Steps in Asymmetric Key Cryptography:

- The essential steps followed in Asymmetric Key Cryptography are as follows:
  - **Step 1:** Each user generates a pair of keys to be used for the encryption and decryption of messages.
  - **Step 2:** Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private.
  - **Step 3:** If Sender Rajesh wishes to send a confidential message to Amar, Rajesh encrypts the message using Amar's public key.
  - **Step 4:** When Amar receives the message, he decrypts it using his private key. No other recipient can decrypt the message because only Amar knows Amar's private key.
- With this approach, all participants have access to public keys, and private keys are generated locally by each participant and therefore need never be distributed. As long as a user's private key remains protected and secret, incoming communication is secure.

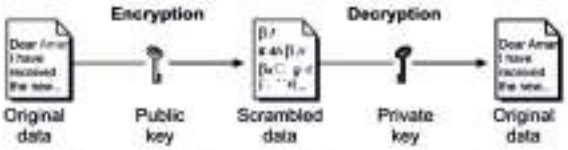


Fig. 6.25: Steps in Asymmetric Key Cryptography

- **Trapdoor Functions:** A trapdoor function is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the "trapdoor". Trapdoor functions are widely used in cryptography.

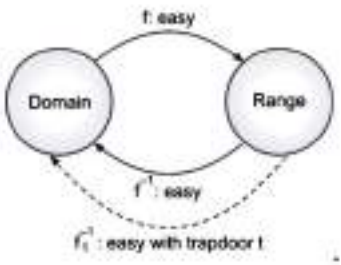


Fig. 6.26: Steps in Asymmetric Key Cryptography

Advantages:

1. **Convenience:** It solves the problem of distributing the key for encryption. Everyone publishes their public keys and private keys are kept secret.
2. **Provides for Message Authentication:** Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender.
3. **Detection of Tampering:** The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.
4. **Provide for Non-repudiation:** Digitally signing a message is similar to physically signing a document. It is an acknowledgement of the message and thus, the sender cannot deny it.

Disadvantages:

1. **Public Keys should/must be Authenticated:** No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.

2. **Slow and Time Consuming:** Public key encryption is slow compared to symmetric encryption. Calculating the ciphertext from plaintext using the long keys takes a lot of time.
3. **Uses more Computer Resources:** It requires a lot more computer supplies compared to single-key encryption.
4. **Widespread Security Compromise is Possible:** If an attacker determines a person's private key, his or her entire messages can be read.
5. **Loss of Private Key may be Irreparable:** The loss of a private key means that all received messages cannot be decrypted.

6.6 SUBSTITUTION TECHNIQUES

- In substitution cipher technique, the characters of plaintext messages are replaced by other characters, numbers or symbols.
- A substitution cipher is a one in which each character in the plaintext is substituted for another character in the ciphertext. The receiver inverts the substitution on the ciphertext to recover the plaintext.
- In this section we study various types of substitution ciphers like Caesar, Playfair, Mono-alphabetic etc.

6.6.1 Caesar Cipher

- In this technique, the characters of a plaintext message are replaced by other characters. The method is named after Julius Caesar, who used it in his private correspondence.
- A Caesar cipher, or the shift cipher, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
- In Caesar cipher each alphabet of plaintext is replaced by an alphabet obtained by shifting three (3) letters from it.
- For example, with a left shift of 3, D would be replaced by A, E would become B, and so on.

Example:

- The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by 3 places. For instance, here is a Caesar cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the key):

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

- When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.

  Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

  Ciphetext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

- Deciphering is done in reverse, with a right shift of 3.

Algorithm to break Caesar Cipher:

Step 1: Read each alphabet in the ciphertext message, and search for it in the second row of the replacement table.

Step 2: When the match is found, replace that alphabet in the ciphertext message with the corresponding alphabet in the same column but first row of the table.

Step 3: Repeat the process for all alphabets in the message.

Example:

Ciphertext	L		O	R	Y	H		B	R	X
Plaintext	I		L	O	V	E		T	E	A

Modified version of Caesar Cipher:

- Let us assume that the ciphertext alphabets corresponding to the original plaintext alphabets may not necessarily be three places down the order, instead any places down the order. For example, Letter A in plaintext would not necessary replace by D, but by any letter (i.e. B through Z).
- For each alphabet there are 25 possibilities of replacement (letter itself cannot be replace).
- The attacker attempts to use all possible permutations and combinations, is called brute –force attack.
- To break the ciphertext, under each letter of the ciphertext, the entire alphabet is written out in reverse starting at that letter. This attack can be accelerated using a set of strips prepared with the alphabet written down in reverse order. The strips are then aligned to form the ciphertext along one row, and the plaintext should appear in one of the other rows. (See the following example).
- To break this version of Caesar cipher the following Algorithm used:

  Step 1: Let K = 1

  Step 2: Read ciphertext message.

  Step 3: Replace each alphabet in the ciphertext with an alphabet that is n position down the order.

  Step 4: K=K+1.

  Step 5: If K<26, goto step 2, else stop.

- **Disadvantage:** There an easy attack that consists of trying, by "brute force", all the possible 26 keys. This is no smart analysis of the encryption algorithm: the problem is the (very) small number of keys.

Example:

- Consider ciphertext "KWUMPMZN". The output produce by the above algorithm to break the cipher message "KWUMPMZN" is shown in the table. The 18th attempt is the correct plaintext "come here".

Ciphertext	K	W	U	M		P	M	Z	M
Attempt Number (Value of k)									
1	L	X	V	N		Q	N	A	N
2	M	Y	W	O		R	O	B	O
3	N	Z	X	P		S	P	C	P
4	O	A	Y	Q		T	Q	D	Q
5	P	B	Z	R		U	R	E	R
6	Q	C	A	S		V	S	F	S
7	R	D	B	T		W	T	G	T
8	S	E	C	U		X	U	H	U
9	T	F	D	V		Y	V	I	V
10	U	G	E	W		Z	W	J	W
11	V	H	F	X		A	X	K	X
12	W	I	G	Y		B	Y	L	Y
13	X	J	H	Z		C	Z	M	Z
14	Y	K	I	A		D	A	N	A
15	Z	L	J	B		E	B	O	B
16	A	M	K	C		F	C	P	C
17	B	N	L	D		G	D	Q	D
18	C	O	M	E		H	E	R	E
19	D	P	N	F		I	F	S	F
20	E	Q	O	G		J	G	T	G
21	F	R	P	H		K	H	U	H
22	G	S	Q	I		L	I	V	I
23	H	T	R	J		M	J	W	J
24	I	U	S	K		N	K	X	K
25	J	V	T	L		O	L	Y	L

6.6.2 Transposition Cipher

- In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.
- Transposition cipher changes the location of characters in plaintext to from the ciphertext. In this cipher, there is no substitution of characters and thus, the order of characters in the plaintext is no longer preserved in the ciphertext.

1. Rail-Fence Technique:

- In the rail fence cipher, the plaintext is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we reach the bottom rail. When we reach the top rail, the message is written downwards again until the whole plaintext is written out.
- The message is then read off in rows. For example, if we have 3 "rails" and a message of 'WE ARE DISCOVERED FLEE AT ONCE', ciphertext writes out:

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

- Now read the text row by row. The ciphertext is: WECRLTEERDSOEEFEAOCAIVDEN

2. Simpler Columnar Transposition Techniques:

(i) Basic Techniques:

- The message is written out in row by row of a fixed length. Then read out the message column by column, and the columns are chosen in some scrambled order, i.e. it can be any order such as 3, 2, 4 etc. The message thus obtained is ciphertext message.

Example:

- Consider the plaintext message " Hello I am here", Now this message can be transform into cipher as follows:

Column 1	Column 2	Column 3	Column 4	Column 5
h	E	l	l	o
i	A	m	h	e
r	E			

- Let us consider 5 columns. Now, decide the order of columns (random), say, 3, 4, 2, 5, 1 and read the text in this order. We get ciphertext as **lmlheaeoehir.**

(ii) Simpler Columnar Transposition Techniques with Multiple rounds:

- A single columnar transposition could be attacked by guessing possible column lengths.

- To improve the above technique, we can have the basic technique, but to do it more than once.
- The ciphertext produce by Simpler Columnar Transposition Techniques with Multiple rounds is much more complex and hard to crack.

Procedure:

Step 1: Write the plaintext row by row. Read the message column by column in random order.

Step 2: The message obtained is the ciphertext of round one.

Step 3: Repeat the steps 1 and 2 as many times as desire.

Example:

- Let us consider same plaintext message " Hello I am here" , which generate ciphertext in round 1 as lmlheaecehir .
- Now, Repeat the same process on the cipher for further round as follows:

Column 1	Column 2	Column 3	Column 4	Column 5
l	M	l	h	e
a	E	o	e	h
i	R			

- Now, use the same order of column as 3, 4, 2, 5, 1 and read the text in this order. We get ciphertext as lohemerehlai
- Repeat this process with more number of times if desire, otherwise stop.

3. Vernam Cipher/ One-Time Pad (OTP):

- In Cryptography, the One-Time Pad (OTP) is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key the same size as, or longer than, the message being sent. In this technique, a plaintext is paired with a random secret key (also referred to as a one-time pad).
- One-time pad (OTP), also called Vernam-cipher or the perfect cipher.
- Once, an input ciphertext for transposition is used, it is never been used again for any other message.
- The length of the input ciphertext and the original plaintext should be the same.

Procedure:

Step 1: Consider each character in the plaintext as a number i.e. A=0, B=1 ..., Z=25.

Step 2: Add each number corresponding to the plaintext alphabet to the corresponding input ciphertext alphabet number.

Step 3: If the sum produced is greater than 26, subtract 26 from it.

Step 4: Translate each number of the sum back to the corresponding letter, which results the output ciphertext.

Example:

- Consider the plaintext "How are you", using one-time-pad NCBTZQARX.
- We will discuss to produce a ciphertext message as follows:

Plaintext	H	o	w	a	r	e	y	o	u	
	7	14	22	0	17	4	24	14	20	
One-time Pad	N	C	B	T	Z	Q	A	R	X	**SUM**
	13	2	1	19	25	16	0	17	23	
Initial total	20	16	23	19	42	20	24	31	43	
Subtract 26	20	16	23	19	16	20	24	5	17	
Ciphertext	U	Q	X	T	Q	U	Y	F	R	

6.7 FIREWALL (W-18)

- Firewalls can be used to protect a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.
- Firewalls exist both as software (software firewalls are installed on the computers) that run on a hardware (hardware firewalls are standalone products).

6.7.1 Need of Firewall

- For most of the organization, the Internet is the virtual backbone of their enterprise network, interconnecting an organization's corporate network and those of its business partners and customers.
- Every organization needs internet access, it enables the outside world to reach and interact with local network assets. This creates a threat to the organization.
- To protect confidential information from those who do not explicitly need to access it and its resources from malicious users & accidents that originate outside of our network.

6.7.2 What is Firewall?

- **Definition:** A firewall is defined as a single choke point that keeps unauthorized users out of trusted or protected network, prohibits potential vulnerable services from entering and leaving the network and provides protection from various kinds of IP spoofing and routing attacks.
- A firewall is inserted between premises of the network connects and the Internet. This location permits the firewall to provide authentication and other security services to remote users in order to prevent unauthorized users from logging in to the network.

- It is a network security device, either hardware or software based, which monitors all incoming and outgoing traffic and based on defined set of security rules it accept, reject or drop that specific traffic.
- Technically, Firewall is specialized version of a router.
- It provides a location for monitoring security related events and provides convenient platform for several internet functions such as NAT, internet usage audit or logs.
- A firewall can serve as platform for IPsec to implement VPN.
- Firewall must immune itself to penetration since it will be target of attack.
- The following Fig. 6.27 illustrates a firewall-controlled access to the enterprise network from the Internet.

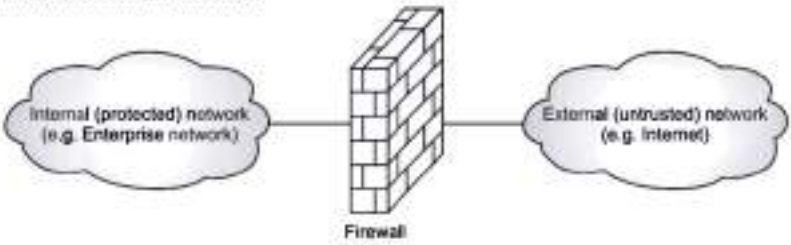


Fig. 6.27: Firewall controlled access from Internet

6.7.3 Design Goals of Firewall

- The following are the design goals of a firewall.
  1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible.
  2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.
  3. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.
- There are four essential controls exercised by a firewall:
  - **Service control:** Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.
  - **Direction control:** Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

- **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPSec.
- **Behavior control:** Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

6.7.4 Limitations of Firewall

- Firewalls have their limitations, including the following:

1. The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
2. The firewall does not protect against internal threats, such as an unhappy employee or an employee who unwittingly cooperates with an external attacker.
3. The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

6.7.5 Types of Firewall

- The following figure 6.28 shows types of firewall.

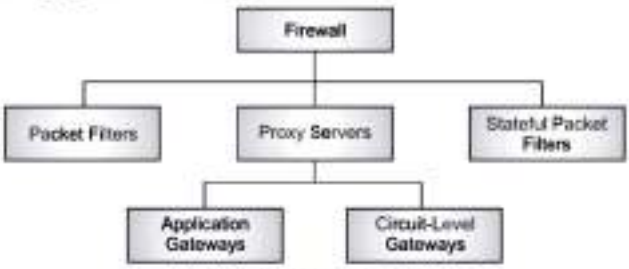


Fig. 6.28: Types of firewall

6.7.5.1 Packet Filters Firewall

- A packet-filtering router applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.

- The router is typically configured to filter packets going in both directions (from and to the internal network).
- Filtering rules are based on information contained in a network packet: Source and destination IP address protocols and ports.
- It analyses traffic at the transport protocol layer.
- Packet firewalls treats each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic.
- Only it can allow or deny the packets based on unique packet headers.
- Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded.

Advantages:

1. Packet filters are fast and can be easily implemented in existing routers.
2. Transparency to the user is the users need not know about the presence of the firewall and this is also typically high speed.

Disadvantages:

1. It may be difficult to set up the packet filter in rules.
2. Lack of authentication and less secure: cryptographic technique is not used anywhere. So that here attacks like IP spoofing can be carried out where someone can change the IP address of a network of the machine and can get some unwanted advantage or authorization which otherwise that person is not allowed to have.

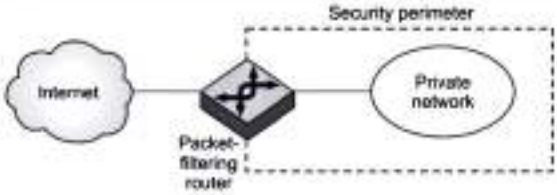


Fig. 6.29: Packet-Filtering

6.7.5.2 Stateful Inspection Firewall

- Stateful packet firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient.
- It keeps track of the state of networks connection travelling across it, such as TCP streams.
- A stateful inspection packet filter tightens up the rules for TCP traffic by creating a directory of outbound TCP connections.

- There is an entry for each currently established connection.
- The stateful packet firewall will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.
- So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

Advantages:

- The connection table greatly reduces the chance that a packet will be spoofed to appear as it were part of an existing connection.
- It has the ability to look into the data of certain packet types.

Disadvantages:

- It does not protect the internal hosts to the same degree as an application layer firewall.
- It does not act as proxy or setup a separate connection on behalf of the source.

6.7.5.3 Proxy Servers

- A proxy service is an application that redirects users' requests to the actual services based on an organization's security policy.
- All communication between a user and the actual server occurs through the proxy server.
- A proxy server acts as a communications broker between clients and the actual application servers. Because it acts as a checkpoint where requests are validated against specific applications, a proxy server is usually processing intensive and can become a bottleneck under heavy traffic conditions.
- Proxy servers can operate at either the application layer or the transport layer.
- There are two classes of proxy servers: application gateways, which operate at the application layer; and circuit-level gateways, which operate at the transport layer.

1. **Application Level Gateway:**

- An application gateway is a proxy server that provides access control at the application layer.
- It acts as an application-layer gateway between the protected network and the untrusted network. Because it operates at the application layer, it is able to examine traffic in detail and, therefore, is considered the most secure type of firewall.
- The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.
- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.

- If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall.
- Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features.
- It can also log all network activities according to applications for both accounting and security audit purposes.
- Application layer firewalls can also be used as Network Address Translator.

Advantages:

- Application level gateways tend to be more secure than packet filters.
- Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application level gateway need only scrutinize a few allowable applications.
- It is easy to log and audit all incoming traffic at the application level.

Disadvantages:

- Prime disadvantage of the application level gateway is the additional processing overhead on each connection. In effect there are two spliced connections between the end users with the gateway at the splice point and the gateway must examine and forward all traffic in both directions.

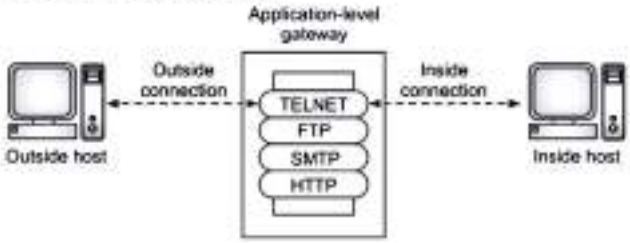


Fig. 6.30: Application-level Gateway

1. **Circuit-level Gateways:**

- A circuit-level gateway is a proxy server that validates TCP and UDP sessions before allowing a connection or circuit through the firewall. It is actively involved in the connection establishment and does not allow packets to be forwarded until the necessary access control rules have been satisfied.
- A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.

- Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.
- A circuit-level gateway is not as secure as an application gateway because it validates TCP and UDP sessions without full knowledge of the applications that use these transport services. Moreover, once a session has been established, any application can run across that connection. This behavior exposes the protected network to attacks from intruders.

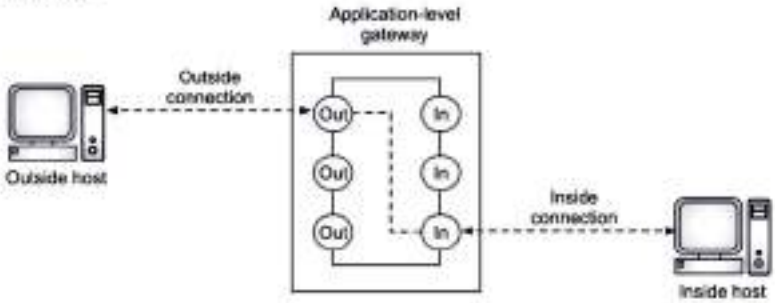


Fig. 6.31: Circuit-level Gateway

Advantages:

- Private network data hiding.
- Avoidance of filtering individual packets.
- Flexible in developing address schemes.
- Don't need a separate proxy server for each application.
- Simpler to implement.

Disadvantages:

- A circuit level gateway cannot examine the data content of the packets it relays between a trusted network and an untrusted network. The potential exists to slip harmful packets through a circuit level gateway to a server behind the firewall.
- It can only handle TCP connections – new extensions proposed for UDP.
- TCP/IP stacks are mandatorily be modified by vendor for using CL Gateways.

6.8 STEGANOGRAPHY

- Steganography is a technique that facilitates hiding of message that is to be kept secret inside other messages. It is also known as stego.
- The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.

- Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent as well as concealing the contents of the message.
- Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size.
- For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.
- In steganography, an unintended recipient or an intruder is unaware of the fact that observed data contains hidden information. In cryptography, an intruder is normally aware that data is being communicated, because they can see the coded/scrambled message.

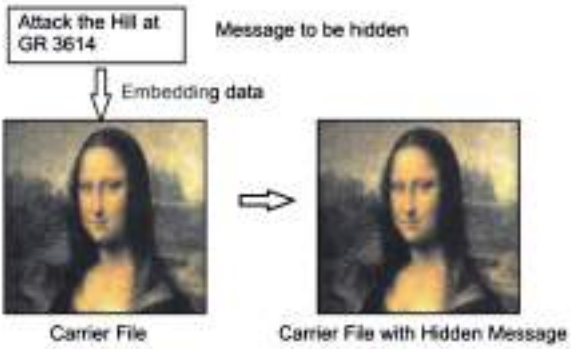


Fig. 6.32: Example of Steganography

6.9 COPYRIGHT

- Copyright refers to the legal right of the owner of intellectual property. In simpler terms, copyright is the right to copy. This means that the original creators of products and anyone they give authorization to are the only ones with the exclusive right to reproduce the work.
- With the ceaseless usage of web and other online services, it has turned out that copying, sharing, and transmitting digital media over the Internet are amazingly simple.

- Since the text is one of the main available data sources and most widely used digital media on the Internet, the significant part of websites, books, articles, daily papers, and so on is just the plaintext.
- Therefore, copyrights protection of plaintexts is still a remaining issue that must be improved in order to provide proof of ownership and obtain the desired accuracy.
- Major area of steganography is copyright marking, where the message to be inserted is used to assert copyright over a document. This can be further divided into watermarking and fingerprinting.
- Watermarking hides copyright information within a watermark by overlaying files not easily detected by the naked eye. This prevents fraudulent actions and gives copyright protected media extra protection.
- During the last decade, digital watermarking and steganography techniques have been used as alternatives to prevent tampering, distortion, and media forgery and also to protect both copyright and authentication.
- Digitally marking a file with a text or with an image is known as Digital Watermarking. It is commonly used for the purpose of authenticating a digital file and for copyright protection. By placing a watermark in a digital file, can ensure copyright protection and authenticity of the digital file.
- Fingerprinting involves hiding a unique identifier for the customer who originally acquired the file and therefore is allowed to use it. Should the file be found in the possession of somebody else, the copyright owner can use the fingerprint to identify which customer violated the license agreement by distributing a copy of the file.

Applications:

- Text watermarking techniques are applicable in many applications. The following points are the most important watermarking applications.

(i) **Digital Copyright Protection (Proof of Ownership):** Text watermarking provides passive protection tools for digital documents so that the text content cannot be illegally copied or replicated. For example, if someone copies a watermarked document/file (e.g., PDF, Docx, Latex, and RTF), then the reversibility of watermarking techniques can be used to prove the ownership of the copied documents

(ii) **Access Control (Copy Control):** Currently, the publishers and the content providers are seeking more reliable ways to control copy or access to their valuable documents, and simultaneously, they want to make the documents accessible on the Internet in order to obtain more revenue. The text watermarking is a desirable technique on the online systems that provide access control to prevent illegal copy or restrict the number of times of copying the original text.

(iii) **Tamper Proofing:** These days a huge number of text documents are available online for selling or reading for users. Therefore, these documents are prone to be exposed to a number of attacks (e.g., unauthorized access, copy, and redistribution). In this case, text watermarking can be used as a fragile tool for tamper proofing of the watermarked texts against attacks. In general, a fragile watermark is embedded into text documents, and if any type of alterations has been made, then it fails to detect the watermark.

(iv) **Text Content Authentication:** The online publishing of articles and newspapers in form of plaintext documents has brought several issues related to authenticating the integrity of these documents. Text watermarking can be applied as an authentication tool to verify the integrity of plaintext documents.

(v) **Forgery Detection (Prevention):** Plagiarism and reproduction of text documents are serious forgery activities and are rapidly increasing. Text watermarking can be used as a forgery detection tool by embedding a watermark in the original text before the online publishing. Thus, it can prove the plagiarism and reproduction of the watermarked texts.

Summary

- Network security is the security provided to a network from unauthorized access and risks. It measures are needed to protect data during their transmission and to guarantee that data transmissions are authentic.
- One of the key aspects of cryptography and network/Internet security is authentication. Authentication helps establish trust by identifying the particular user/system. Authentication ensures that the claimant is really who he/she claims to be. This is process of establishing the legitimacy of anode or user before allowing access to requested information.
- The main types of authentication available are Password based authentication, Token based authentication, Biometric based authentication and Image based authentication.
- Attacks are typically categorized based on the action performed by the attacker. Thus an attack can be passive or active.
- Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy.
- Data integrity is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently.

- The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.
- Encryption key is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- Decryption key is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it.
- Substitution and transposition ciphers are two categories of ciphers used in cryptography.
- In the substitution-cipher technique, the characters of a plain-text message are replaced by other characters, numbers or symbols.
- A transposition cipher is methods of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.
- A firewall is defined as a single choke point that keeps unauthorized users out of trusted or protected network, prohibits potential vulnerable services from entering and leaving the network and provides protection from various kinds of IP spoofing and routing attacks.
- Firewalls are classified into three common types namely packet filters, circuit level gateways and application level gateways.
- Packet filters firewalls processes network traffic on a packet-by-packet basis. A packet filter's main function is to filter traffic from a remote.
- The circuit level gateway represents a proxy server that statically defines what traffic will be forwarded. Circuit proxy's always forward packets containing a given port number if that port number is permitted by the rule set. A circuit level gateway operates at the network level of the OSI model. This gateway acts as an IP address translator between the Internet and the internal system. The main advantage of a proxy server is its ability to provide NAT.
- The application-level gateway represents a proxy server, performing at the TCP/IP application level, that is set up and torn down in response to a client request, rather than existing on a static basis. Application proxies forward packets only when a connection has been established using some known protocol.
- Steganography is a technique that facilitates hiding of message that is to be kept secret inside other messages.
- Major area of steganography is copyright marking, where the message to be inserted is used to assert copyright over a document. This can be further divided into watermarking and fingerprinting.

Check Your Understanding

1. The _____ is the original message before transformation.
   (a) ciphertext (b) plaintext
   (c) secret-text (d) none of the above
2. In an asymmetric-key cipher, the sender uses the _____ key.
   (a) private (b) public
   (c) either (a) or (b) (d) neither (a) nor (b)
3. A combination of an encryption algorithm and a decryption algorithm is called a _____
   (a) cipher (b) secret
   (c) key (d) none of the above
4. Proxy firewall filters _____.
   (a) physical layer (b) data-link layer
   (c) network layer (d) application layer
5. Technically, _____ is specialized version of a router.
   (a) Firewall (b) Bridge
   (c) Gateway (d) Modem

ANSWERS

(1) b	(2) b	(3) a	(4) d	(5) a		

Practice Questions

Q.I Answer the following questions in short.

1. What is meant by Network security?
2. What is plaintext and ciphertext?
3. What is attack? What are its types?
4. What is encryption and decryption?
5. Write names of substitution techniques?
6. What are types of Firewall?

Q.II Answer the following questions.

1. How proxy servers and firewalls help in maintaining network security? Explain.
2. Explain working of firewall.
3. Explain the devices used to maintain network security.
4. What is difference between substitution cipher and transposition cipher?
5. Distinguish between symmetric and asymmetric cryptography.

Q.III Define the Terms:

1. Firewall
2. Steganography
3. Copyright
4. Passive attack
5. Active attack

Previous Exams Questions

Winter 2018

1. Explain Firewall and its security features. 5M

Ans. Refer to section 6.7

❖❖❖

NOTES