

**GOVERNMENT OF TAMILNADU
DIRECTORATE OF TECHNICAL EDUCATION
CHENNAI – 600 025**

STATE PROJECT COORDINATION UNIT

Diploma in Computer Engineering

Course Code: 1052

M – Scheme

e-TEXTBOOK

on

**Computer Networks and Security for
IV Semester Computer Engineering**

Convener for Computer Engineering Discipline:

Mrs. Ghousia Jabeen. B.E(EEE), M.E(C.S.E),
Principal, T.P.E.V.R Govt. Polytechnic College,
Vellore.

Team Members for Industrial Instrumentation:

Mrs.P.Bhavani,M.E.,
Lecturer and HOD(i/c)/Dept. Computer Engg.,
Govt. Polytechnic College, Purasawalkam, Chennai -12.

Mrs. Nalini,M.E.,
Lecturer (Sr. Gr)/ Dept Computer Engg.,
Nachimuthu Polytechnic College, Pollachi.

Mrs.K.R.Kavitha M.E.,MISTE.,
Lecturer/ Dept Computer Engg., Karpagam Polytechnic College,
Pollachi Main Road, Eachanari post, Coimbatore.

Validated by

Syeda Zahara Jabeen,B.E.,M.S.,
Lecturer (Sel. Gr)/Dept. Electronics and Comm. Engg.,
Central Polytechnic College,Taramani, Chennai

CONTENTS

CHAPTER NO	CHAPTER NAME	PAGE NO
I	DATA COMMUNICATIONS	03 - 46
	1.1 Data Communications	
	1.2 Types of Networks	
	1.3 Transmission media	
	1.4 Network Devices	
II	OSI MODEL AND LAN PROTOCOLS	47 - 76
	2.1 To understand the different layers of OSI and Their functions.	
	2.2 To discuss the different LAN protocols.	
	2.3 To study FDDI concepts and frame format.	
	2.4 To understand the basic concepts of Switching.	
	2.5 To know the ISDN and BISDN.	
III	TCP/IP SUIT	77 - 108
	3.1. Overview of TCP / IP:	
	3.2. Network Layers Protocol:	
	3.3. IP Addressing	
	3.4 Application Layer Protocols	
IV	NETWORKS AND SECURITY	109 - 147
	4.1 Introduction to Network Security	
	4.2 CRYPTOGRAPHY	
	4.3 Network Security Application	
	4.4 Internet Security	
V	APPLICATIONS OF NETWORK SECURITY	148 - 183
	5.1 Introduction to network security	
	5.2 Hackers Techniques	
	5.3 Security Mechanism	
	5.4 Intrusion detection (ID)	
	5.5 Wireless Security Issues	
	Reference	184

UNIT I

DATA COMMUNICATIONS

Objective:

- To understand data communication basics.
- To understand components of data communication, mode of data transfer, topology, types of network.
- To learn the types of transmission media.

Introduction :

In this modern world the communication between computers and devices are most necessary. Without network the real time systems cannot exist.

1.1 Data Communications

1.1.1 Components of a data communication

The five components are :

1. Message - It is the information to be communicated. Popular forms of information include text, pictures, audio, video etc.
2. Sender - It is the device which sends the data messages. It can be a computer, workstation, telephone handset etc.
3. Receiver - It is the device which receives the data messages. It can be a computer, workstation, telephone handset etc.
4. Transmission Medium - It is the physical path by which a message travels from sender to receiver. Some examples include twisted-pair wire, coaxial cable, radio waves etc.
5. Protocol - It is a set of rules that governs the data communications. It represents an

agreement between the communicating devices. Without a protocol, two devices may be connected but cannot communicate.

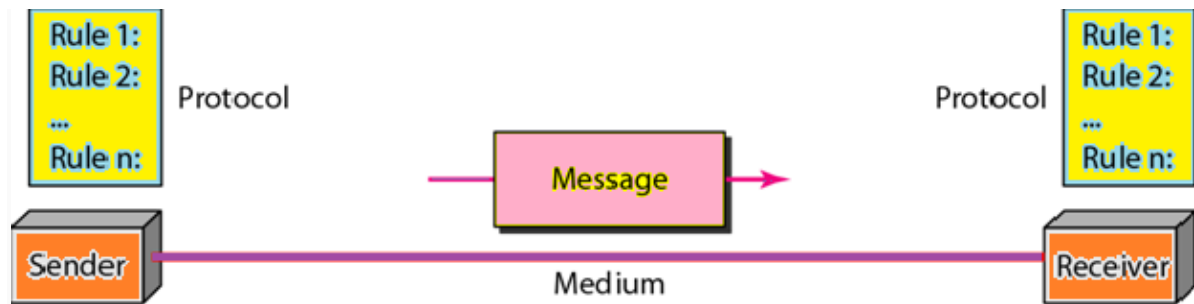


Fig 1.1

1.1.2 Data Flow:

The classification of data transmission is based on which of the communicating devices can send data and how the transmission can take place.

There are basically three ways :

- Simplex
- Half-duplex
- Full-duplex

Simplex:

In the simplex communication the direction of signal of data flow is in only one direction i.e unidirectional only. Eg. Radio station broadcasting the programs and the receiver receives the signal and listen to the program.

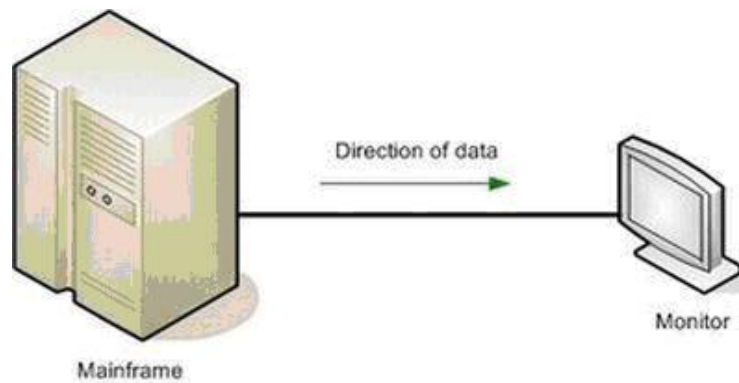


FIG 1.2

Half-Duplex:

In half-duplex mode, each station can transmit and receive, but not at same time. When one device is sending, the other can only receive. Eg. Walkie-Talkie

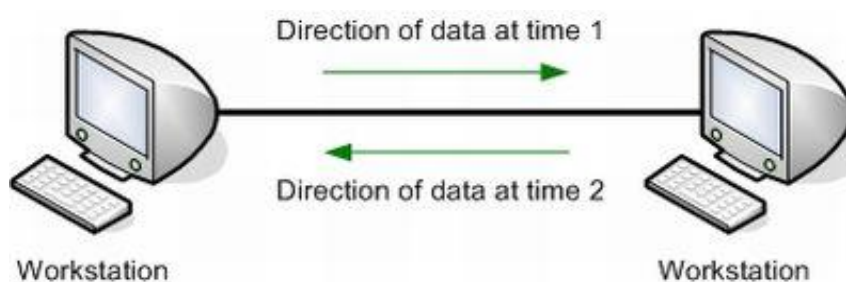


FIG 1.3

Full-Duplex:

In full-duplex mode(also called duplex), both stations can transmit and receive simultaneously. Full duplex is like a two way communication. Eg. Telephone Communication.

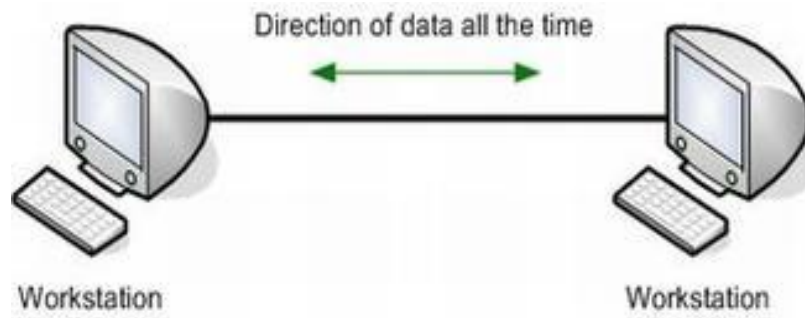


FIG 1.4

1.1.3 Network criteria

Network Selection Criteria

A network is selected on the basis of network criteria. During the network selection, it is important to consider these criteria for improving network functionality.

These factors are:

- **Network Performance**
- **Network Reliability**
- **Network Security**

Network Performance

Network performance can be measured by analyzing the request and response time.

Request time includes the time that a message can take to travel from one computer to another computer within a network.

Response time is the elapsed time between a request and the response.

The performance of the network depends on the following factors:

Number of Users - Performance of the network may degrade when the number of users connected to the network increases.

Transmission medium - It connects elements in the network and is used to transmit data over the network. The data transmission speed varies with the type of transmission medium. The bandwidth requirement and the type of transmission media can be decided depending on the size and the application of the network.

Hardware - Different types of hardware can be used in a network. It affects both the speed and capacity of the system in a network.

Software - The software is a program or set of instructions which controls the operation of a networking device. It is used to process data at the sender, receiver and intermediate nodes in a network.

Network Reliability

Network reliability plays a major role in developing network functionality.

The network monitoring systems and network devices are necessary for making the network reliable.

The network monitoring systems detects and identifies the network problems.

The network devices ensure that the data reaches the appropriate destination.

The reliability of the network is measured by following factors:

Frequency of failure - Determines how frequently the network fails.

Recovery time - It is the time taken by a device or network to recover from the failure.

Catastrophe - Network must be protected from the disasters such as fire, earthquake and fire.

Network Security

Security of the network is considered as the important aspect for improving the network performance.

The network security may be affected due to viruses and unauthorized access of other users.

To provide network security:

- Avoid opening unknown e-mail attachments which may contain virus.
- Use anti-virus software for securing the systems from virus.
- Firewalls can be implemented for detecting and preventing unauthorized access of other users in the network.
- Use backup tools to store the important data on removable media like CD. This helps to secure your data.
- Turn off the system and remove the network cable when not in use, to avoid unauthorized interference in the systems.

1.1.4 Types of Connections:

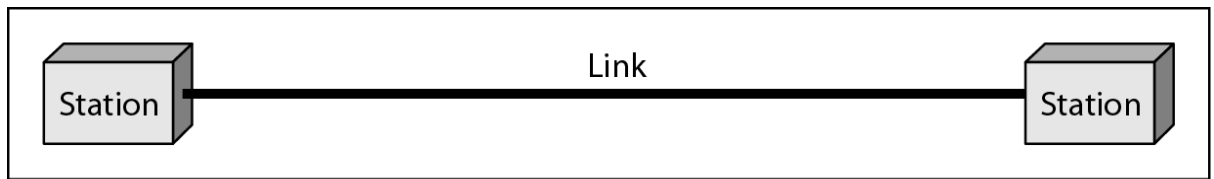
A network is two or more devices connected through links, A link is a communications pathway that transfers data from one device to another. There are two types of connections: point-to-point and multipoint.

A. Point –to-point

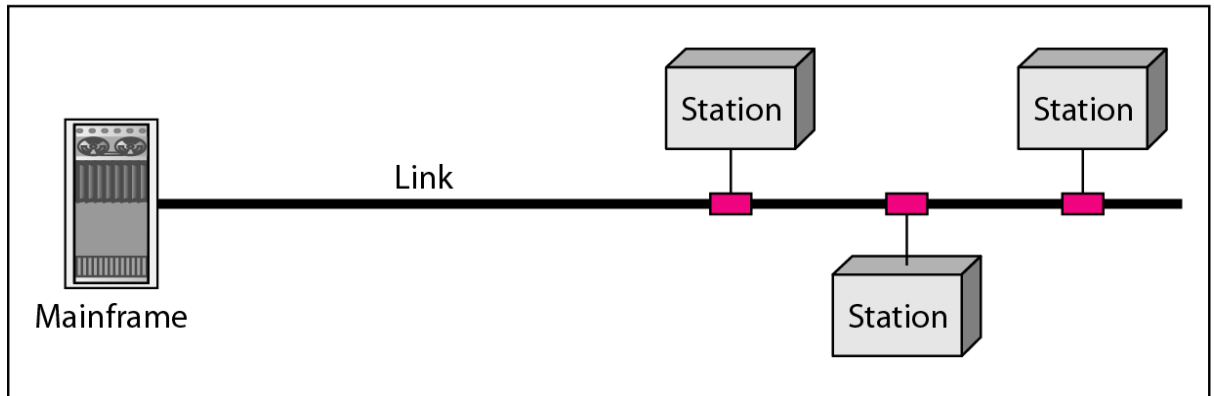
This type of connection provides a dedicated link between two devices. The entire capacity of the link is used only for transmission between those device connected point-to-point. Eg. TV controlled by remote control hence point-to-point connection established between the two devices.

B. Mutipoint

A mutipoint connection is one in which more than two specific devices share a single link. In this type of connections the link is shared by the devices either spatially i.e if the devices connected can use the link simultaneously or time shared connection. If a user make turns, it is a time-shared connection.



a. Point-to-point



b. Multipoint

FIG 1.5

Topology

Topology is defined as the way a network is laid out physically. Two or more devices connect to a link; two or more links form a topology.

There are four basic types of topologies, they are:

Star

Mesh

Bus

Ring

Star:

In a star topology the devices are connected point-to-point to the centralised hub. This hub is controller which acts as the exchange: If one device wants to send data to another, it sends to the hub which then relays the data to the destination device connected to the other side of the hub.

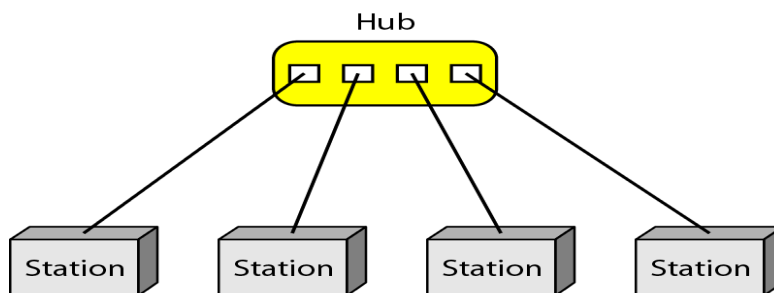


FIG 1.6

Advantages:

- Easy to install
- Less cables as only one link from the node to hub.
- Maintain: easy to add, move and delete a node from the topology without disturbing the other devices.
- Robustness- If one link fails, only that link is affected remaining links are active.
- Easy to identify the fault.

Disadvantages;

- Hub is too important
- The hub represents a single source of failure

Bus:

A bus topology is multipoint. One long cable act as the back bone to link all the devices in a network. Nodes are connected to this backbone by drop lines and taps. A drop line is the connection between the node and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to touch the metallic core of the main cable.

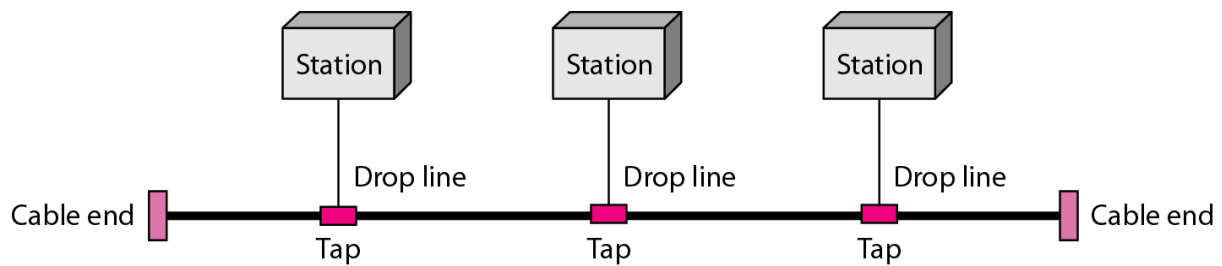


FIG 1.6

Advantages:

- Easy to install
- Less cables

Disadvantages:

- Hard to detect fault isolation.
- Bus cable is too important

Ring:

In a ring topology, each device has dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reached its destination.

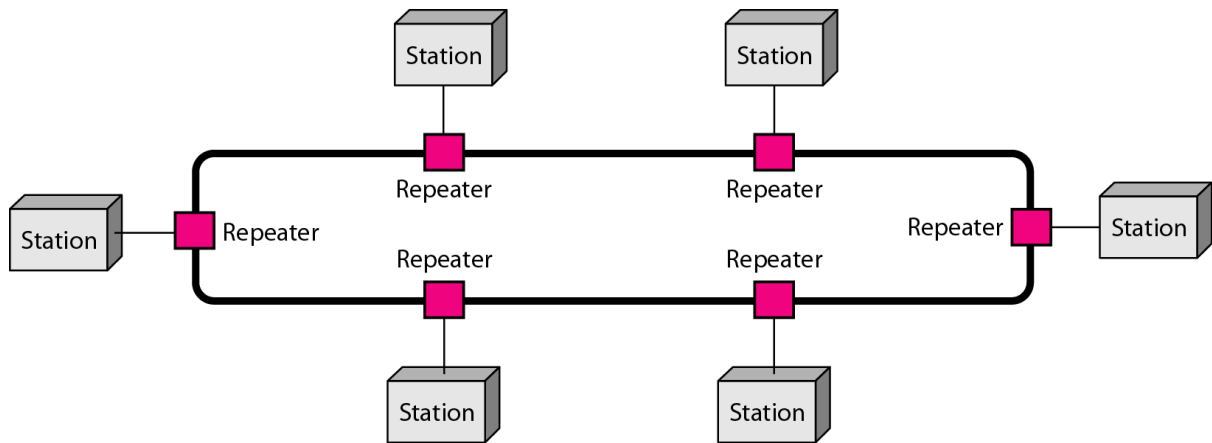


FIG 1.7

Point to point with 2 devices on both sides

Advantages:

- Easy to install
- Maintain: add move delete
- Fault isolation

Disadvantages:

Unidirectional traffic

A break in the ring the entire network is disabled.

Mesh:

Every device have point-to-point connection between every other device. Each device is directly connected therefore no traffic congestion. The number of physical links increases with number of devices connected in the network.

No need of centralised hub as in star topology. The number of duplex physical links can be calculated by $n(n-1)/2$. Also each device should have $n-1$ input/output ports.

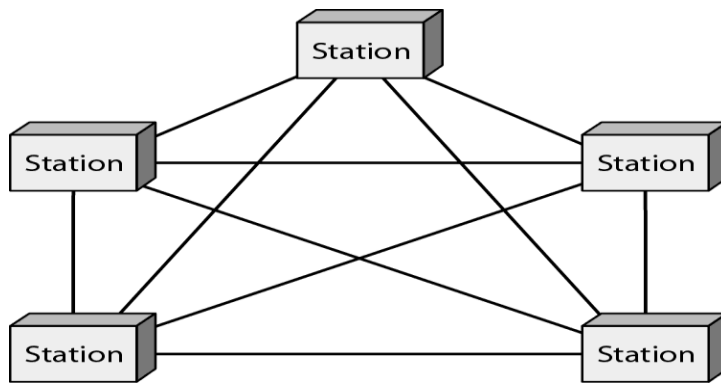


FIG 1.8

Advantages:

- no traffic problems
- Robust. No link failure no effect on others.
- Privacy security
- Easy to detect the abnormal situation.

Disadvantages:

- Amount of cables, i/o ports
- Efficiency and effectiveness
- Space
- Cost

Hybrid:

Combination one or more topologies is called hybrid topology. In the below diagram the main topology is star and the remaining part is bus topology.

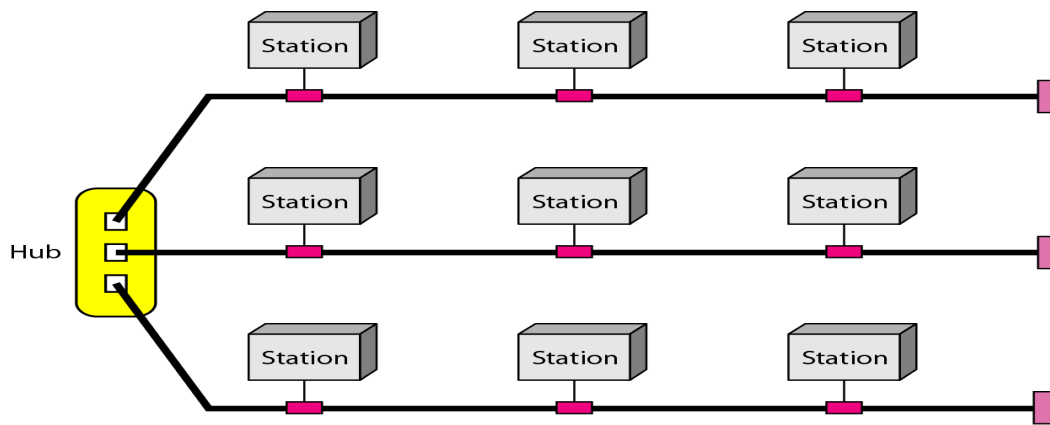


FIG 1.9

1.2 Types of Networks:

1.2.1 Need for Computer Networks:

Local Area Network (LAN) is generally a privately owned network within a single office, building or campus, covering a distance of a few kilometres.

The main reason for designing a LAN is to share resources such as disks, printers, programs and data.

Depending on the needs the LAN can be limited two PC's and a printer.

LAN size is limited to a few kilometres. They are designed to allow resources to be shared between personal computers or workstations.

The resources include both hardware like printer or software like application program or data.

Here one computer may be provided with higher capacity hard disk which can act as the server and remaining as clients or workstations.

Topology mostly adopted in use are bus, ring, star.



Fig 1.10

MAN

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).

It is for the customers who have their end points across the city or town .Eg. A organisation computers connected across the city having branches.

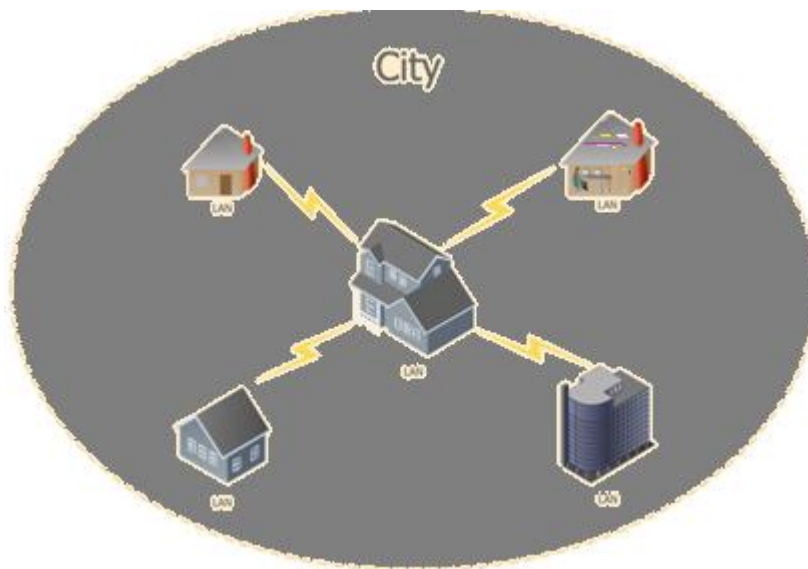


Fig 1.11

WAN

A Wide area network (WAN) is a telecommunication network that is used for connecting computers and covers a wide geographical area. WANs often contain a few smaller networks (LANs, MANs, etc.). A WAN spans across city, state, country or even continent boundaries.

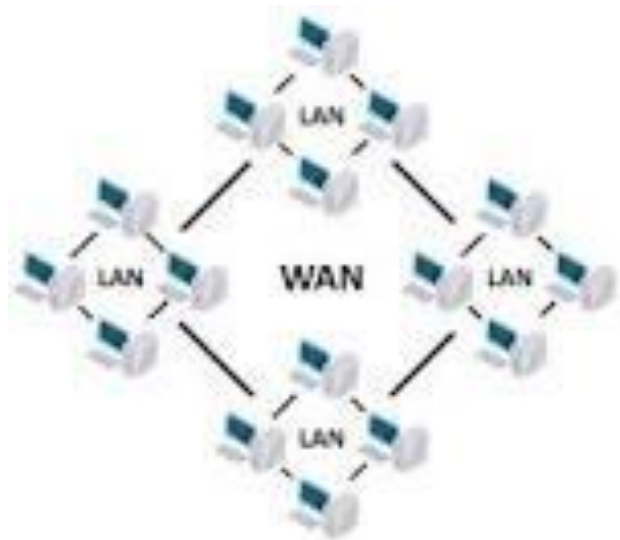


Fig 1.12

CAN

A campus area network (CAN) is a network of multiple interconnected local area networks (LAN) in a limited geographical area. A CAN is smaller than a wide area network (WAN) or metropolitan area network (MAN).

A CAN is also known as a corporate area network (CAN).

Local networks are common in the education field. Most schools and other educational institutions have computers connected to a local network.

At the same time, modern technologies allow to connect even the computers that are on different continents, and not only in the same room or building. Numerous educational institutions have branches in different countries, with computer connected via local network. Moreover, local area networks can connect computers from different colleges or universities.

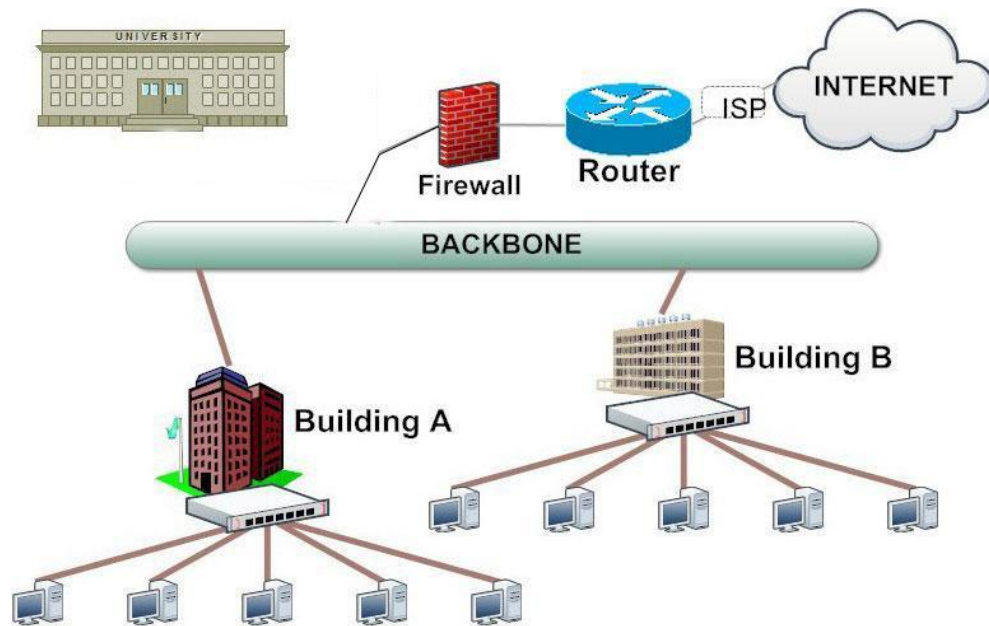


Fig 1.13

HAN

A **Home Area Networks (HAN)** is a type of local area network that is used in an individual home. The home computers can be connected together by twisted pair or by a wireless network. HAN facilitates the communication and interoperability among digital devices at the home, allows to easier access to the entertainments and increase the productivity, organize the home security.

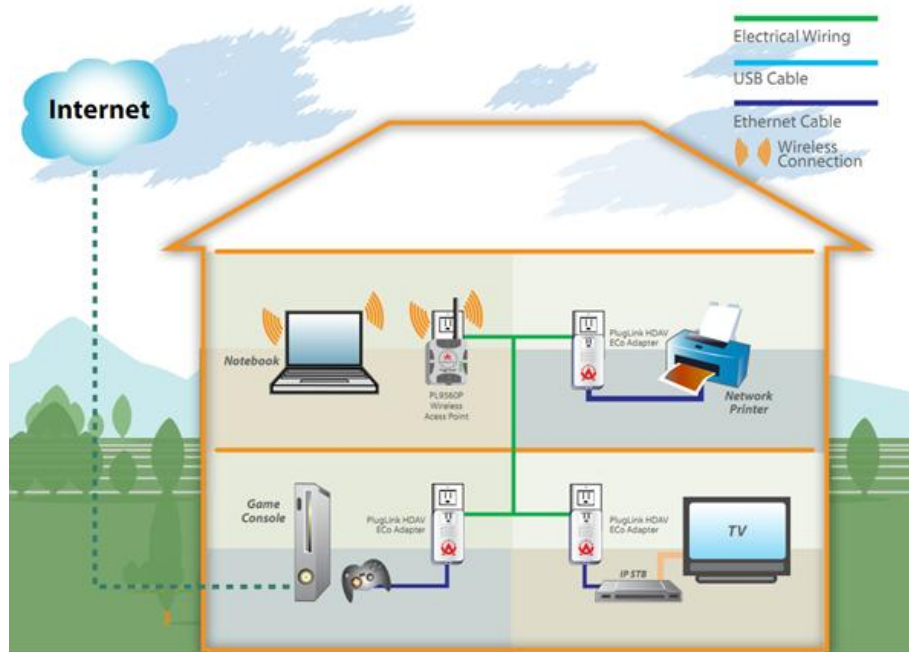


Fig 1.14

Internet

It is a worldwide system which has the following characteristics:

- Internet is a world-wide / global system of interconnected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP)
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer's location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.

- For example, a DNS server will resolve a name **http://www.google.com** to a particular IP address to uniquely identify the computer on which this website is hosted.
- Internet is accessible to every user all over the world by using various devices both by wired and wireless.



Fig 1.15

Intranet

- Intranet is system in which multiple PCs are connected to each other.
- PCs in intranet are not available to the world outside the intranet.
- Usually each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet.
- Each computer in Intranet is also identified by an IP Address which is unique among the computers in that Intranet.



Fig 1.16

Similarities in Internet and Intranet

- Intranet uses the internet protocols such as TCP/IP and FTP.
- Intranet sites are accessible via web browser in similar way as websites in internet. But only members of Intranet network can access intranet hosted sites.

Differences in Internet and Intranet

- Internet is general to PCs all over the world whereas Intranet is specific to few PCs.
- Internet has wider access and provides a better access to websites to large population whereas Intranet is restricted.
- Internet is not as safe as Intranet as Intranet can be safely privatized as per the need.

Internet vs. Intranet

Apart from similarities there are some differences between the two. Following are the differences between Internet and Intranet:

Table 1.1

Intranet	Internet
Localized Network.	Worldwide Network
Doesn't have access to Intranet	Have access to Internet.
More Expensive	Less Expensive
More Safe	Less Safe
More Reliability	Less Reliability

Extranet

Extranet

Extranet refers to network within an organization, using internet to connect to the outsiders in controlled manner. It helps to connect businesses with their customers and suppliers and therefore allows working in a collaborative manner.

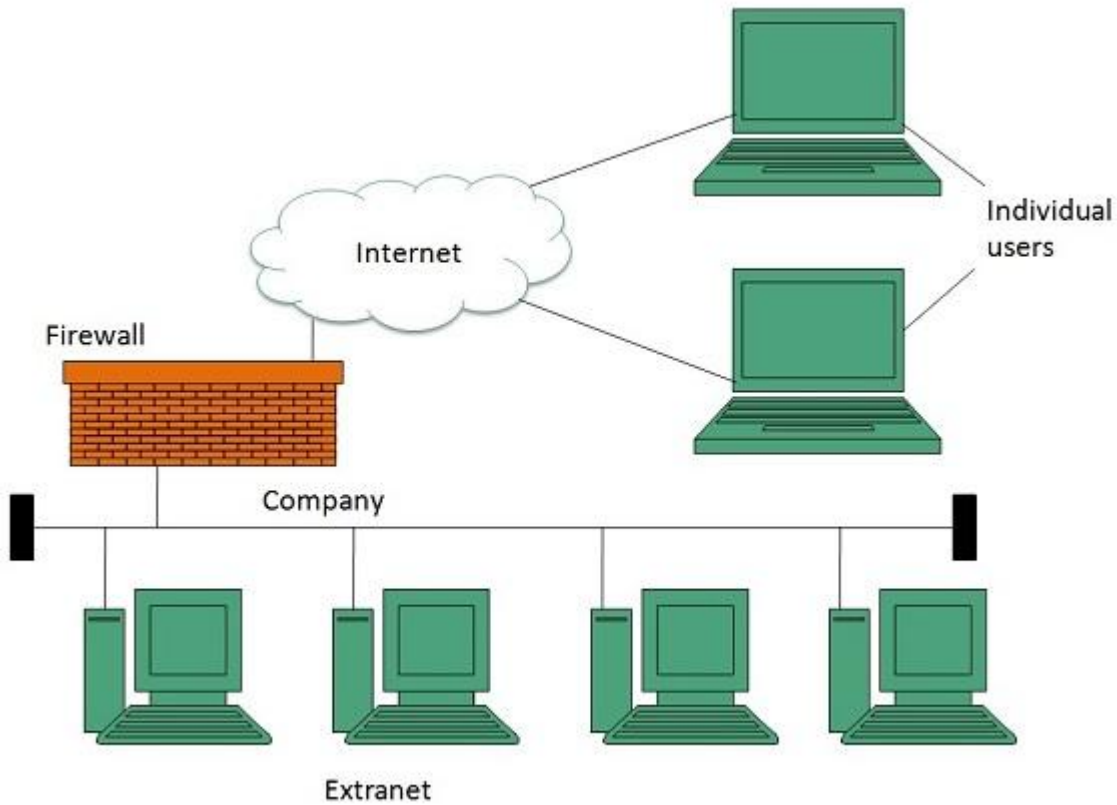


Fig 1.17

Extranet vs. Intranet

The following table shows differences between Extranet and Intranet:

Table 1.2

Extranet	Intranet
Internal network that can be accessed externally.	Internal network that can not be accessed externally.
Extranet is extension of company's Intranet.	Only limited users of a company.
For limited external communication between customers, suppliers and business partners.	Only for communication within a company.

1.2.2 Client-server

A computer network in which one centralized, powerful computer (called the server) is a hub to which many less powerful personal computers called clients are connected.

The clients run programs and access data that are stored on the server.

The clients send request to the server and the server responds to the clients request.

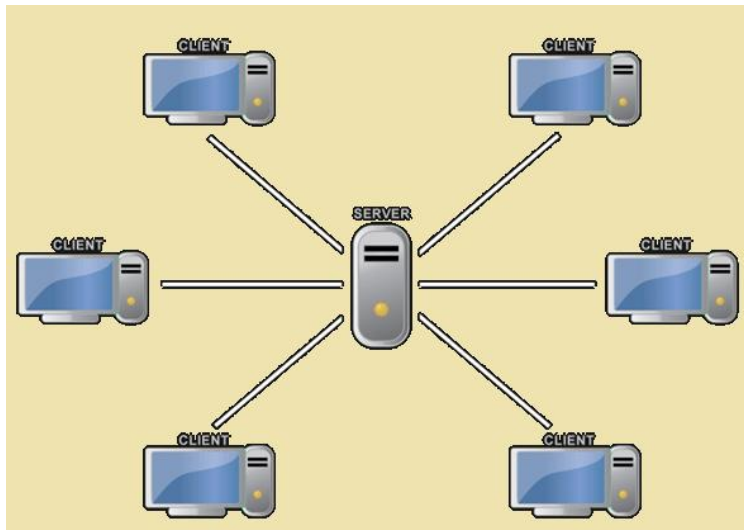


Fig 1.18

1.2.3 Peer-to-peer Networks (P2P network)

A peer to peer network group of computers capable of sharing files among the computers connected. No server in this type of network. Any peer can communicate with the another peer directly.

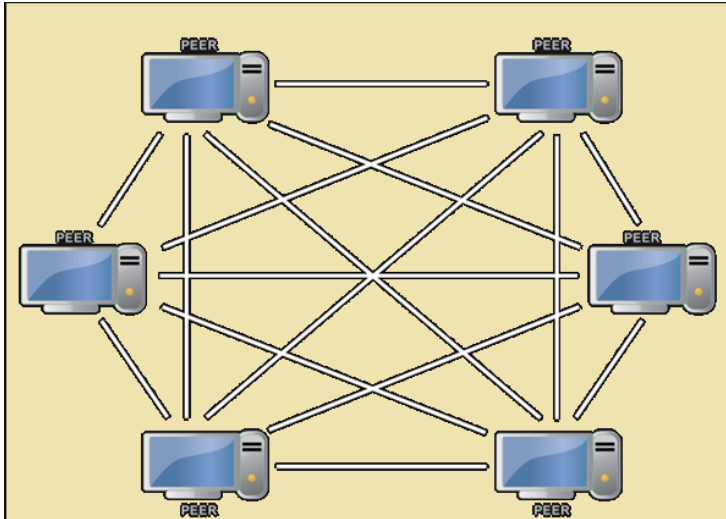


Fig 1.19

1.3 Transmission media

1.3.1 Transmission media:

A transmission medium can be broadly defined as anything that can carry information from a source to destination. In data communication the definition of information and the transmission medium is more specific.

The transmission medium is usually free space, metallic cable or fiber-optic cable.

Transmission media can be divided into two broad categories:

Guided(wired-metallic medium)

Unguided(wireless)

1.3.2 Classification of Transmission medium

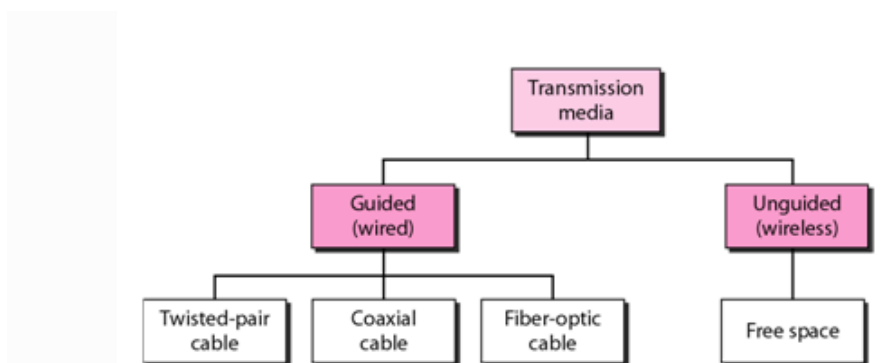


Fig 1.20

1.3.2 Guided media:

There are many types of guided media:

1. Twisted pair
2. Coaxial
3. Fiber optics

Twisted pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.

Fiber optics is a cable that accepts and transports signals in the form of light.

1.3.2.1 Twisted pair :

A twisted pair consists of two conductors usually copper with its own plastic insulation, twisted together as shown in the Fig 1.20

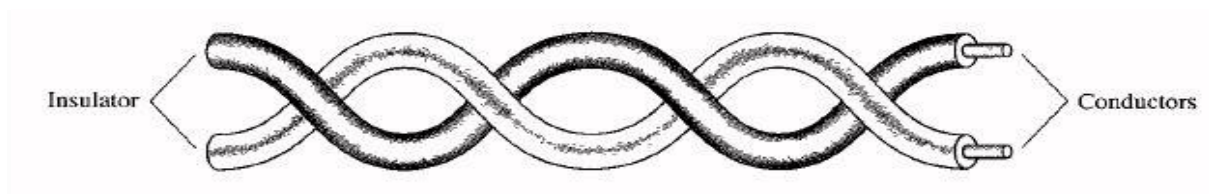


Fig 1.20

One of the wire is used to carry the signal and another for ground reference. The receiver uses the difference between the two.

Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between *pairs* of wires, two insulated copper wires are *twisted* around each other.

There are two types of twisted pair :

UTP – Unshielded Twisted Pair

STP – Shielded Twisted Pair

UTP

Unshielded twisted pair comes without any type of shielding at all but is still very capable of handling imbalances that interfere with data transmission.

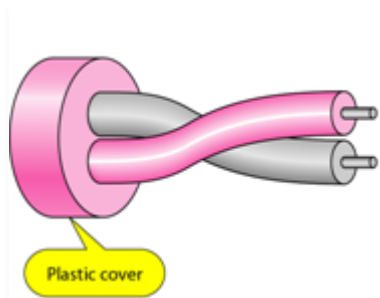


Fig 1.21

UTP categories

Table 1.3

Category 1	Voice only (Telephone)
Category 2	Data to 4 Mbps (Localtalk)
Category 3	Data to 10Mbps (Ethernet)
Category 4	Data to 20Mbps (Token ring)
Category 5	Data to 100Mbps (Fast Ethernet)
Category 5e	Data to 1000Mbps (Gigabit Ethernet)
Category 6	Data to 2500Mbps (Gigabit Ethernet)

STP

Shielded twisted pair cabling, or STP, has a metallic foil that encases the twisted wire pairs inside a cable. This protects against electromagnetic interference and allows for a faster transmission of data.

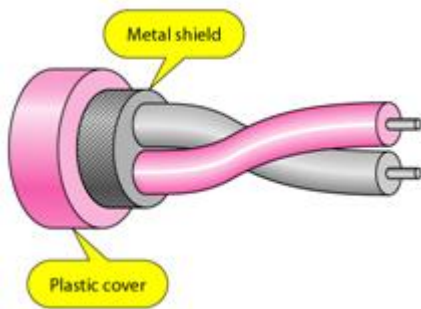


Fig 1.22

1.3.2.2 Coaxial

A type of wire that consists of a center wire surrounded by insulation and then a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference.

Coaxial cabling is the primary type of cabling used by the cable television industry and is also widely used for computer networks, such as Ethernet. Although more expensive than standard telephone wire, it is much less susceptible to interference and can carry much more data.

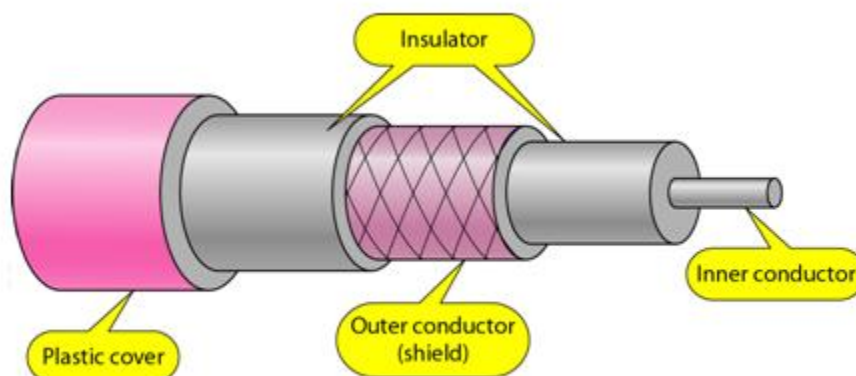


Fig 1.23

Categories of coaxial cable

Coaxial cables are categorized by their radio government (RG) ratings.

Table 1.4

<i>Category</i>	<i>Impedance</i>	<i>Use</i>
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

1.3.2.3 Fiber-optic Cable

A technology that uses glass (or plastic) threads (fibers) to transmit data. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves.

A fiber-optic cable is made up of incredibly thin strands of glass or plastic known as optical fibers; one cable can have as few as two strands or as many as several hundred. Each strand is less than a tenth as thick as a human hair and can carry something like 25,000 telephone calls, so an entire fiber-optic cable can easily carry several million calls.



Fig 1.24

Types of fiber-optic cables

Optical fibers carry light signals down them in what are called **modes**. That sounds technical but it just means different ways of traveling: a mode is simply the path that a light beam

follows down the fiber. One mode is to go straight down the middle of the fiber. Another is to bounce down the fiber at a shallow angle. Other modes involve bouncing down the fiber at other angles, more or less steep.

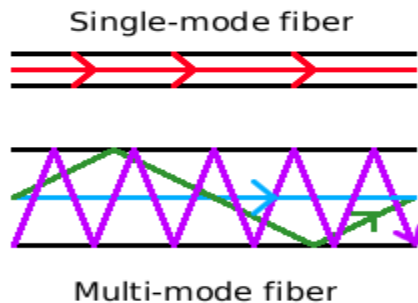


Fig 1.25

The simplest type of optical fiber is called **single-mode**. It has a very thin core about 5-10 microns (millionths of a meter) in diameter. In a single-mode fiber, all signals travel straight down the middle without bouncing off the edges (red line in diagram). Cable TV, Internet, and telephone signals are generally carried by single-mode fibers, wrapped together into a huge bundle. Cables like this can send information over 100 km (60 miles).

Another type of fiber-optic cable is called **multi-mode**. Each optical fiber in a multi-mode cable is about 10 times bigger than one in a single-mode cable. This means light beams can travel through the core by following a variety of different paths (purple, green, and blue lines)—in other words, in multiple different modes. Multi-mode cables can send information only over relatively short distances and are used (among other things) to link computer networks together.

Fiber optics has several advantages over traditional metal communications lines:

- Fiber optic cables have a much greater bandwidth than metal cables. This means that they can carry more data.
- Fiber optic cables are less susceptible than metal cables to interference.
- Fiber optic cables are much thinner and lighter than metal wires.
- Data can be transmitted digitally (the natural form for computer data) rather than analogically.

1.3.3 Unguided media

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

Radio Waves

Microwaves

Infrared

Electromagnetic spectrum for wireless communication

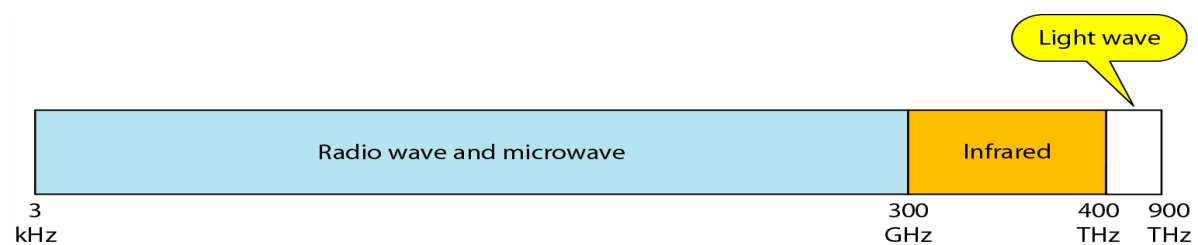


Fig 1.26

1.3.3.1 Radio waves

Electromagnetic radiation having a wavelength between about .5 centimeters and 30,000 meters; used for the broadcasting of radio and television signals.

Radio waves are used for multicast communications, such as radio and television, and paging systems. They can penetrate through walls.

Highly regulated. Use omni directional antennas.

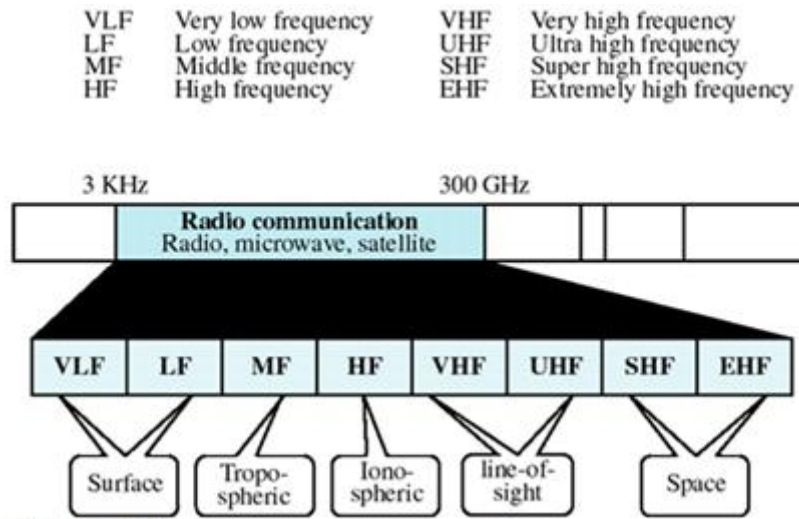


Fig 1.27

Radio propagation categories

There are a number of categories into which different types of radio propagation can be placed. These relate to the effects of the media through which the signals propagate.

- **Free space propagation:** Here the radio signals travel in free space, or away from other objects which influence the way in which they travel.
- It is only the distance from the source which affects the way in which the field strength reduces.
- This type of radio propagation is encountered with signals travelling to and from satellites.
- **Ground wave propagation:** When signals travel via the ground wave they are modified by the ground or terrain over which they travel.
- They also tend to follow the earth's curvature. Signals heard on the medium wave band during the day use this form of propagation.
- **Ionospheric propagation:** Here the radio signals are modified and influenced by the action of the free electrons in the upper reaches of the earth's atmosphere called the ionosphere.

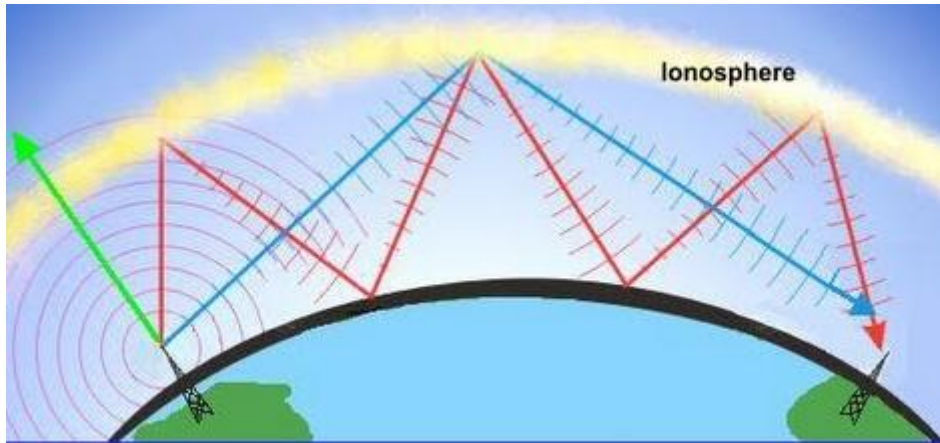


Fig 1.28.1

- This form of radio propagation is used by stations on the short wave bands for their signals to be heard around the globe.
- **Tropospheric propagation:** Here the signals are influenced by the variations of refractive index in the troposphere just above the earth's surface. Tropospheric radio propagation is often the means by which signals at VHF and above are heard over extended distances.

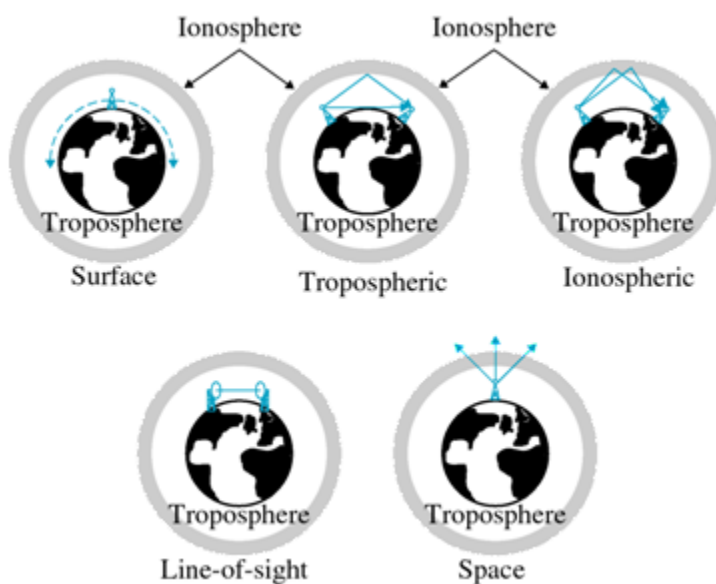


FIG 1.28 ,2 Propagation methods

1.3.3.2 Infrared signals

IR data transmission is also employed in short-range communication among computer peripherals and personal digital assistants.

These devices usually conform to standards published by IrDA, the Infrared Data Association.

Remote controls and IrDA devices use infrared light-emitting diodes (LEDs) to emit infrared radiation which is focused by a plastic lens into a narrow beam.

The beam is modulated, i.e. switched on and off, to encode the data.

The receiver uses a silicon photodiode to convert the infrared radiation to an electric current. It responds only to the rapidly pulsing signal created by the transmitter, and filters out slowly changing infrared radiation from ambient light. (ex. Signals from TV remote control to TV)

Infrared communications are useful for indoor use in areas of high population density.

IR does not penetrate walls and so does not interfere with other devices in adjoining rooms.

Infrared is the most common way for remote controls to command appliances.

Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation

1.3.3.3 Low Orbit Satellite (LOS)

Satellites are launched into orbit, which is to say that they are shot up into the sky on rockets to get them up above the atmosphere where there is no friction.

The idea is to get them flying so fast, that when they fall back to earth, they fall towards earth at the same rate as the earth's surface falls away from them.

When an object's path around the earth, when it's "trajectory" matches the earth's curvature, the object is said to be "in orbit".

Satellite Characteristics

- Key component: **transponder**
 - **Accepts** signal from earth
 - **Shifts** signal to another frequency
 - **Amplifies** signal and...
 - **Rebroadcasts** signal to earth
- Distance has impact on system:
 - Requires significant power
 - Amount of **delay** is measurable and significant factor
- Uplink always at a higher frequency than downlink

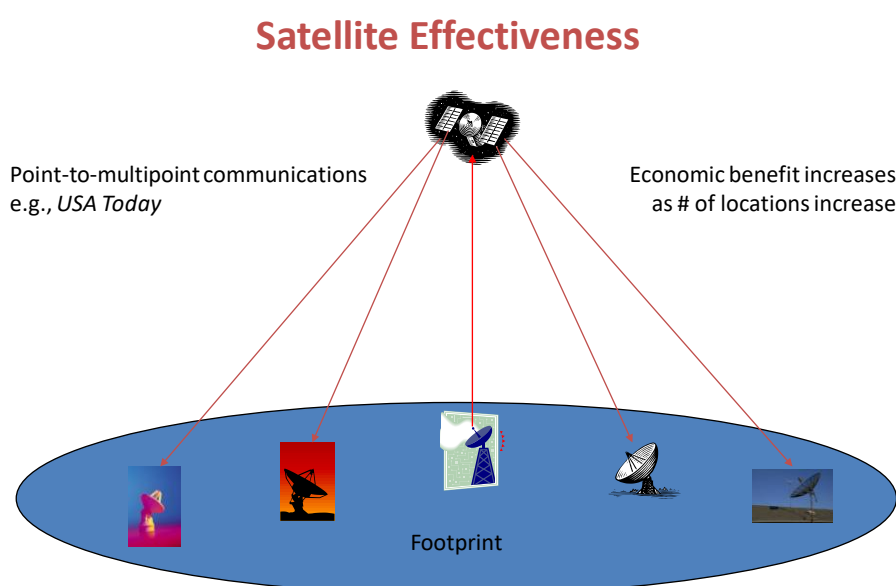


Fig 1.29

Any satellite can archive orbit at any distance from the earth if its velocity is sufficient to keep it from falling to earth and it is free of friction from earth's atmosphere. The farther the satellite is from the earth, the longer it takes for a radio or microwave frequency transmission to reach the satellite.

There are three main classes of satellites

LEO

MEO

GEO

Classes of Satellites

Three main classes of satellites:

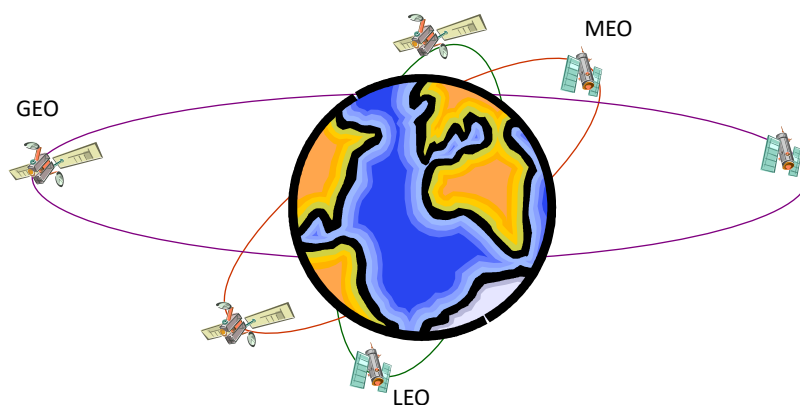


Fig 1.30

GEO Satellites

- **Geosynchronous** earth orbit
- **22,300 miles** above earth
- Requires the **most power**
- Adds **greatest delay**: 0.25 sec/leg
- Position is **constant** relative to earth – same rotational speed as the earth
- Provides **largest footprint** of all satellites
- **Three** satellites can cover earth
- Applications: One way broadcasts, international TV

MEO Satellites

- **Middle** earth orbit
- Orbit **6,200 – 9,400 miles** above earth
- **Delay reduced** to 0.05 per leg
- **Smaller** footprint; requires **10-15** to cover earth
- Applications: regional use due to footprint and speed, such as mobile voice, low-speed data
- Most rapidly growing application: GPS

LEO Satellites

- **Low earth orbit**
- **Closest to earth: 400 – 1,000 miles above earth**
- **Least amount of delay: 0.025 seconds/leg**
- **Least amount of power required; can be directed into user's handheld device**
- **Smallest footprint: requires approximately 60 to cover earth**
- **Functionality is new due to speed and small footprint – switching capability was needed and the system is very complex**
- **Jitter is a significant issue**
- **Applications: mobile voice, low-speed data, high-speed data**

Very Small Aperture Terminal (VSAT),

How the VSAT Equipment function

The Very Small Aperture Terminal (VSAT) is a satellite communications device that allows reliable data transmission via satellite using small antennas of 0.9 to 1.9 meters which is about 3.7 feet. VSAT is a plug and play device.

VSAT has got terminals arranged in a star configuration into the central hub station that is connected to the host computer. Communication between the terminals has to pass through the network central hub processor. The VSAT technology does not send signal to each other or there is no direct communication between VSAT devices without a hub

The hub consist of three elements namely Radio Frequency Terminal (RTF), VSAT hub base-band equipment and the user interface

VSAT is the most fastest technology compare to point to point connection, or dial up connection due to the fact that VSAT deploy the use of procedure to make connection which other communication system either don't have or are not reliable.

Cabling and standards

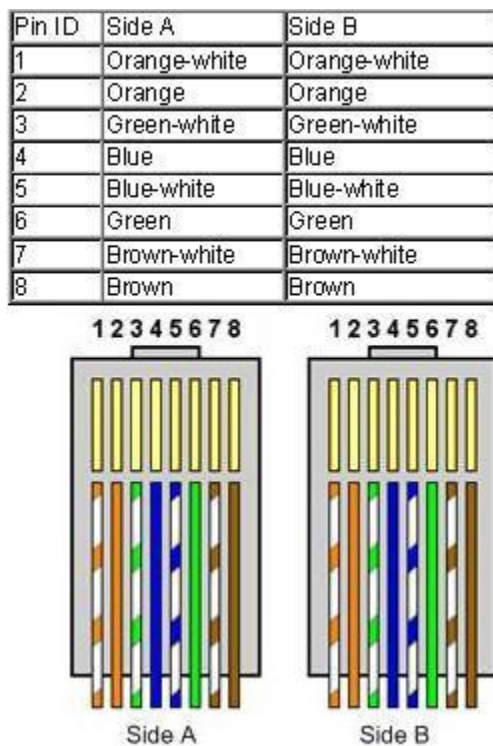
Straight Cable

You usually use straight cable to connect different type of devices. This type of cable will be used most of the time and can be used to:

- 1) Connect a computer to a switch/hub's normal port.
- 2) Connect a computer to a cable/DSL modem's LAN port.
- 3) Connect a router's WAN port to a cable/DSL modem's LAN port.
- 4) Connect a router's LAN port to a switch/hub's uplink port. (normally used for expanding network)
- 5) Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.

Both side (side A and side B) of cable have wire arrangement with same color.

Fig 1.31



Crossover Cable

Sometimes you will use crossover cable, it's usually used to connect same type of devices. A crossover cable can be used to:

- 1) Connect 2 computers directly.
- 2) Connect a router's LAN port to a switch/hub's normal port. (normally used for expanding network)
- 3) Connect 2 switches/hubs by using normal port in both switches/hubs.

In you need to check how crossover cable looks like, both side (side A and side B) of cable have wire arrangement with following different color .

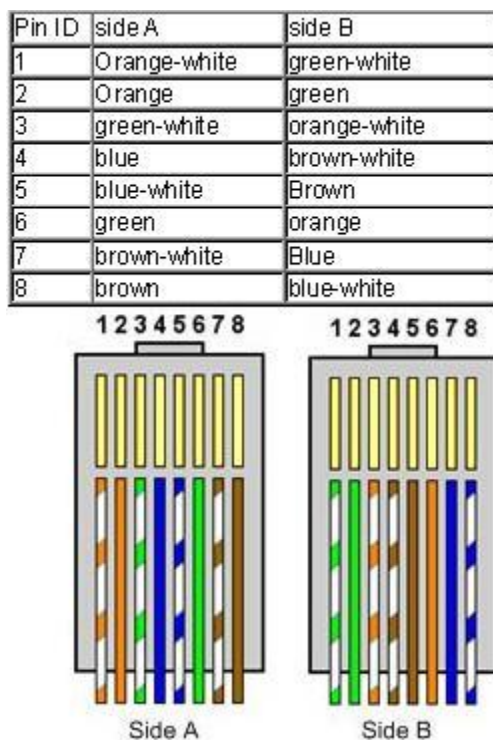


Fig 1.32

Making connections – Tools

- Cat5e cable
- RJ45 connectors

- Cable stripper
- Scissors
- Crimping tool

RJ45 connector

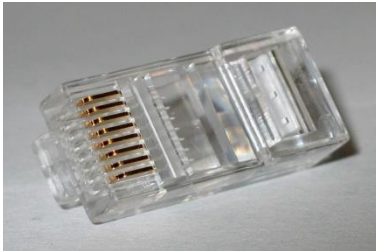


Fig 1.33

Making connections - Steps

1. Strip cable end
2. Untwist wire ends
3. Arrange wires
4. Trim wires to size
5. Attach connector
6. Check
7. Crimp
8. Test

Step 1 – Strip cable end

- Strip 1 – 1½” of insulating sheath
- Avoid cutting into conductor insulation

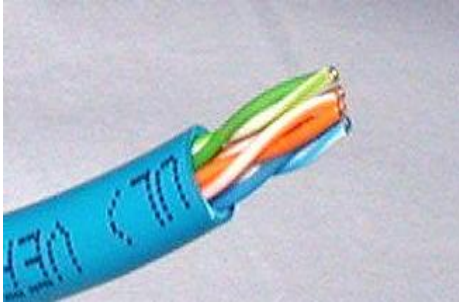


Fig 1.34

Step 2 – Untwist wire ends

- Sort wires by insulation colors

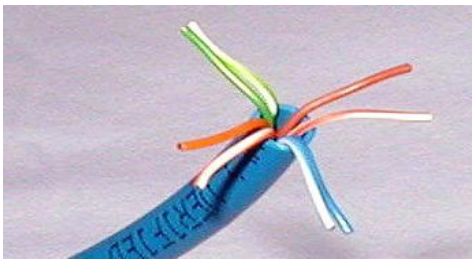


Fig 1.35

Step 3 – Arrange wires

- TIA/EIA 568A: GW-G OW-BI BIW-O BrW-Br
- TIA/EIA 568B: OW-O GW-BI BIW-G BrW-Br



Fig 1.36

Step 4 – Trim wires to size

- Trim all wires evenly
- Leave about ½” of wires exposed

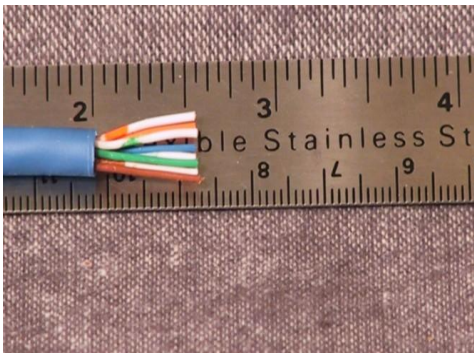


Fig 1.37

Step 5 – Attach connector

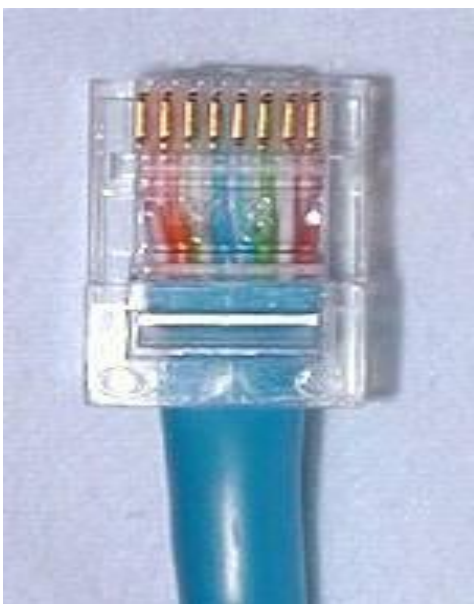


Fig 1.38

- **Maintain wire order, left-to-right, with RJ45 tab facing downward**

Step 6 – Check

- **Do all wires extend to end?**
- **Is sheath well inside connector?**

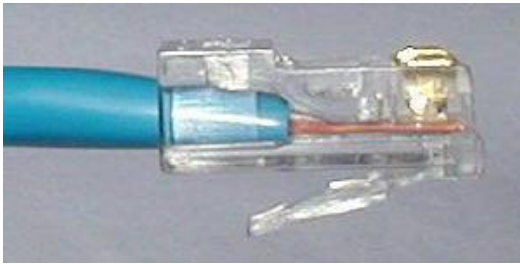


Fig 1.39

Step 7 – Crimp

- **Squeeze firmly to crimp connector onto cable end (8P)**

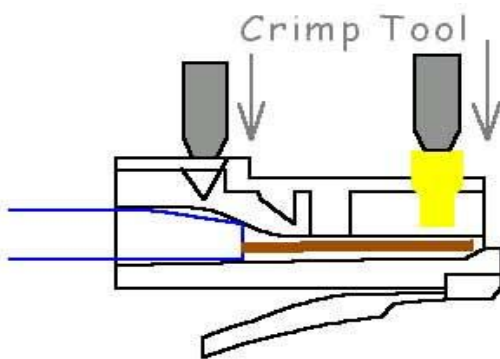


Fig 1.40

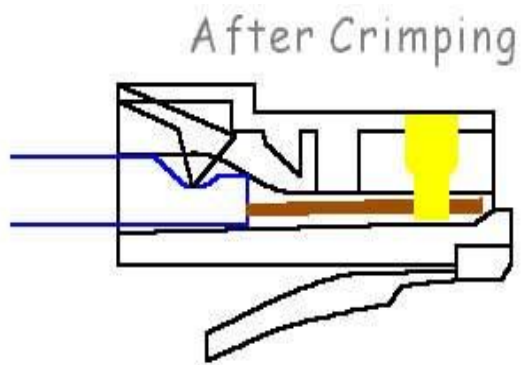


Fig 1.41

1.4 Network Devices

Computer networking devices:

To connect the computer and other devices to form a network depending upon the type and security features to be applied to the network the various networking devices are used.

Hub, bridges, switches and routers.

To build a network based on the type of network many networking components and software are required.

In this section we are going to learn about the various networking components like :

Switches , Routers and Gateways.

1.4.1 Switches

Switch is one of the devices used to group the nodes together to form a network.

Instead of broadcasting the frames to all the ports, a switch actually checks for the destination MAC address (physical address) and forward it to the relevant port to reach that computer only.

This way, switches reduce traffic and divide the collision domain into segments, this is very sufficient for busy LANs and it also protects frames from being sniffed by other computers sharing the same segment.

They build a table of which MAC address belongs to which segment. If a destination MAC address is not in the table it forwards to all segments except the source segment. If the destination is same as the source, frame is discarded.

Switches have built-in hardware chips solely designed to perform switching capabilities, therefore they are fast and come with many ports.

Sometimes they are referred to as intelligent bridges or multiport bridges. Different speed levels are supported. They can be 10 Mb/s, 100 Mb/s, 1 Gb/s or more.

Most common switching methods are:

1. Cut-through: Directly forward what the switch gets.
2. Store and forward: receive the full frame before retransmitting it.

1.4.2 Routers

Routers are used to connect different LANs or a LAN with a WAN (e.g. the internet). If the packet's destination is on a different network, a router is used to pass it the right way, so without routers the internet could not functions.

Routers use NAT (Network Address Translation) in conjunction with IP hidden to provide the internet to multiple nodes in the LAN under a single IP address.

For a network router to know where to send packets of data it receives, it uses a **routing table**.

A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination.

When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network.

1.4.3 Gateways

A node on a network that serves as an entrance to another network..They are very intelligent devices or else can be a computer running the appropriate software to connect and translate data between networks with different protocols or architecture, so their work is much more complex than a normal router.

In a workplace, the gateway is the computer that routes traffic from a workstation to the outside network that is serving up the Web pages. For basic Internet connections at home, the gateway is the Internet Service Provider that gives you access to the entire Internet.

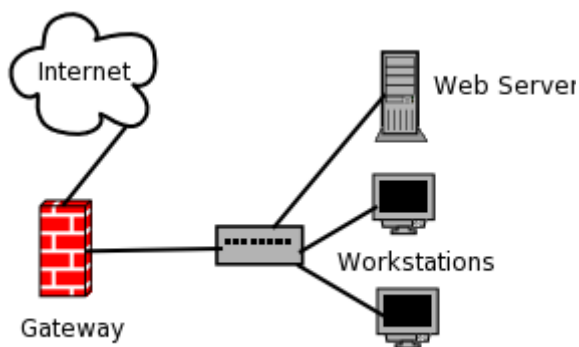


Fig 1.42

When a computer-server acts as a gateway, it also operates as a firewall and a proxy server.

A firewall keeps out unwanted traffic and outsiders off a private network.

A proxy server is software that "sits" between programs on your computer that you use (such as a Web browser) and a computer server—the computer that serves your network.

The proxy server's task is to make sure the real server can handle your online data requests.

UNIT II

OSI MODEL AND LAN PROTOCOLS

2.1 NETWORK MODELS

A network 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 to another. The software consists of instruction sets that make possible the services that expect from a network.

2.1.1 PROTOCOLS

A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- **Syntax** It is the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
- **Semantics** The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
- **Timing** The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

2.1.2 STANDARDS

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability

of data and telecommunications technology and processes. 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.

Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") **and de jure** (meaning "by law" or "by regulation").

- **De facto** 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 manufacturers who seek to define the functionality of a new product or technology.
- **De jure** Those standards that have been legislated by an officially recognized body are de jure standards.

2.1.3 THE OSI MODEL

An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. ISO is the organization. OSI is the model – Open System Interconnection model.

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.

An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

LAYERED ARCHITECTURE

The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), and presentation (layer 6), and application (layer 7).

Please Do Not Touch Steve's Pet Alligator

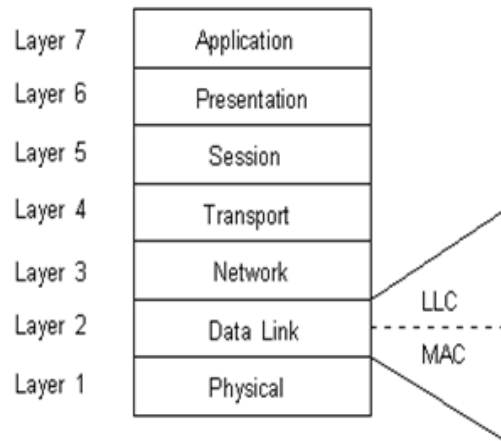


Fig 2.1: OSI Model

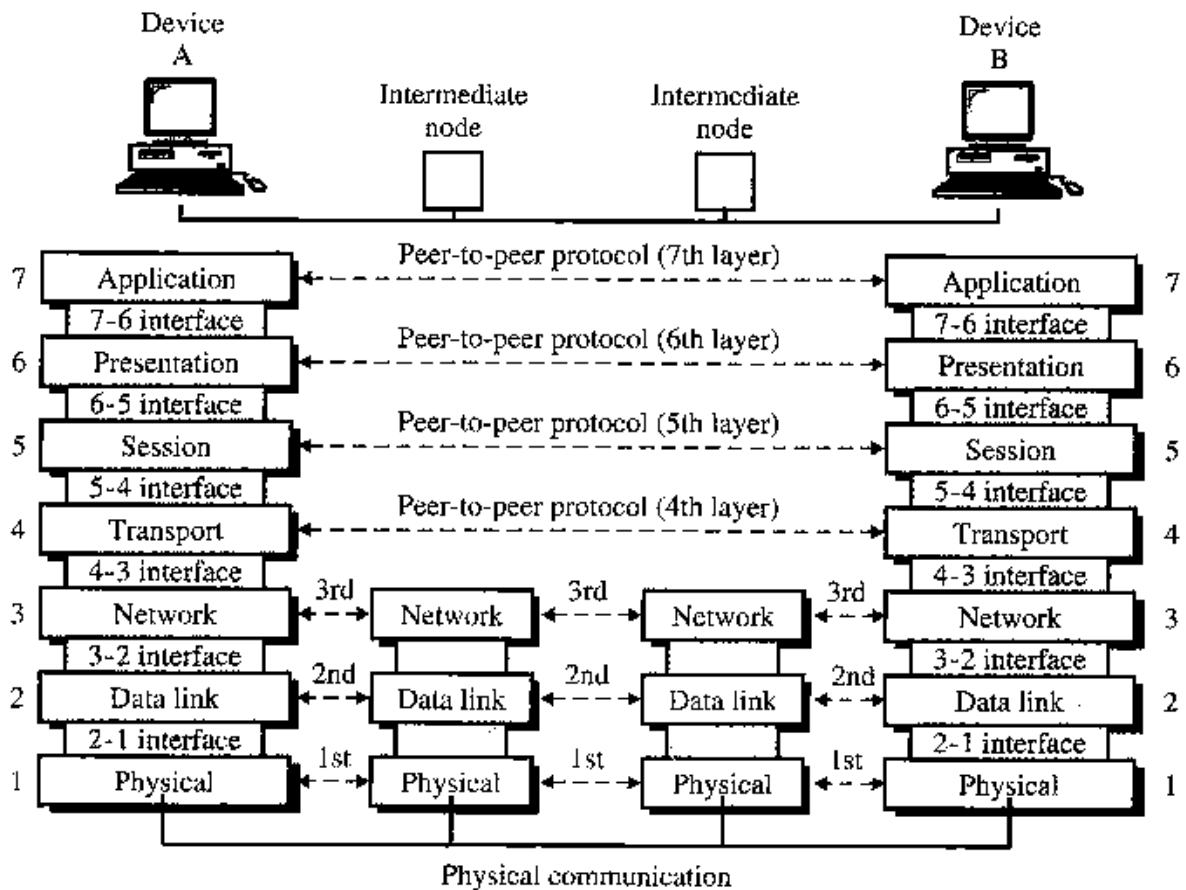


Fig.2.2 : Layered Architecture

LAYERS IN THE OSI MODEL

PHYSICAL LAYER

The physical layer coordinates the functions required to carry a bit stream over a physical medium.

It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.

The responsibilities/ functions of physical layer is follows:

Physical characteristics of interfaces and medium. The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

- **Representation of bits.** The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals).
- **Data rate.** The transmission rate--the number of bits sent each second--is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
- **Synchronization of bits.** The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.
- **Line configuration.** The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
- **Physical topology.** The physical topology defines how devices are connected to make a network.

DATA LINK LAYER

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). The data link layer is responsible for moving frames from one hop (node) to the next.

Other responsibilities of the data link layer include the following:

- ❖ **Framing.** The data link layer divides the stream of bits received from the network layer into data units called frames.
- ❖ **Physical addressing.** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.
- ❖ **D Flow control.** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- ❖ **Error control.** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
- ❖ **Access control.** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

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), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.

Other responsibilities of the network layer include the following:

- ❖ **Logical addressing.** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- ❖ **Routing.** When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices called routers or switches route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

TRANSPORT LAYER

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does.

Other responsibilities of the transport layer include the following:

- **Service-point addressing.** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
- ❖ **Segmentation and reassembly.** A message is divided into transmittable segments, with 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 transmission.

- ❖ **Connection control.** The transport layer can be either connectionless or connection oriented.

A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

- ❖ **Flow control.** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

- ❖ **Error control.** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

SESSION LAYER

The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems. The session layer is responsible for dialog control and synchronization.

Specific responsibilities of the session layer include the following:

- ❖ **Dialog control.** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- ❖ **Synchronization.** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file

of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

PRESENTATION LAYER

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems

Specific responsibilities of the presentation layer include the following:

- ❖ **Translation.** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- ❖ **Encryption.** Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- ❖ **Compression.** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

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 electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Specific services provided by the application layer include the following:

- ❖ **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa.
- ❖ **File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- ❖ **Mail services.** This application provides the basis for e-mail forwarding and storage.
- ❖ **Directory services.** This application provides distributed database sources and access for global information about various objects and services.

2.2 802.X PROTOCOLS

802 is the standard for LAN network formulated by IEEE. It deals with local area networks and metropolitan area networks. The service as and protocols specified in IEEE 802 maps to the lower two layers of seven layer OSI, networking reference model. In IEEE 802 divides the Data link layer into two sub layers logical link control and media access control. Some 802 standards are 802.3-CSMA/CD-bus (Ethernet), 802.4-Token bus, 802.5-Token Ring, 802.11- Wireless LAN

Medium Access protocols (MAC) are defined as, many of which are used with network. The most commonly used MAC protocols are 802.5 Token-Ring, 802.3 Ethernet

versions 2.0. These MAC Protocols are concerned with the transportation of packets from one node to another on a single network segment.

2.2.1 CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION (CSMA/CD)

Ethernet uses *carrier sense multiple access with collision detection* (CSMA/CD) as the method of medium access, and has been standardized by the IEEE as IEEE 802.3. Standard Ethernet has a data rate of 10 Mbps and allows frame sizes of between 64 and 1518 bytes. The frame format can be seen below.

The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting to detect a collision. When there is no collision, the station receives one signal: its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station.

FRAME FORMAT

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium. Acknowledgments must be implemented at the higher layers. The format of the MAC frame is shown in Figure 2.3

7 byte 1 byte 6 byte 6 byte 2 byte 46 to 1500 byte 4 byte

Preamble	Start frame Delimiter	Destination Address	Source Address	Length	Data	Frame Check Sequence
-----------------	--------------------------------------	--------------------------------	---------------------------	---------------	-------------	-------------------------------------

Fig 2.3 : Frame Format

- **Preamble.** The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0s and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.
- **Start frame delimiter (SFD).** The second field (1 byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits are 11 and alerts the receiver that the next field is the destination address.
- **Destination address (DA).** The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.
- **Source address (SA).** The SA field is also 6 bytes and contains the physical address of the sender of the packet.
- **Length or type.** This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field.
- **Data.** This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
- **Frame check sequence (FCS)** - Is filled by the source station with a calculated cyclic redundancy check value dependent on frame contents (as with Token Ring and Ethernet). The destination address recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded. The last field contains error detection information CRC.

2.2.2 TOKEN BUS (802.4)

Token bus is a network implementing the token ring protocol over a "virtual ring" on a coaxial cable. A token is passed around the network nodes and only the node possessing the token may transmit. If a node doesn't have anything to send, the token is passed on to the next node on the virtual ring. Each node must know the address of its neighbor in the ring, so a special protocol is needed to notify the other nodes of connections to, and disconnections from, the ring.

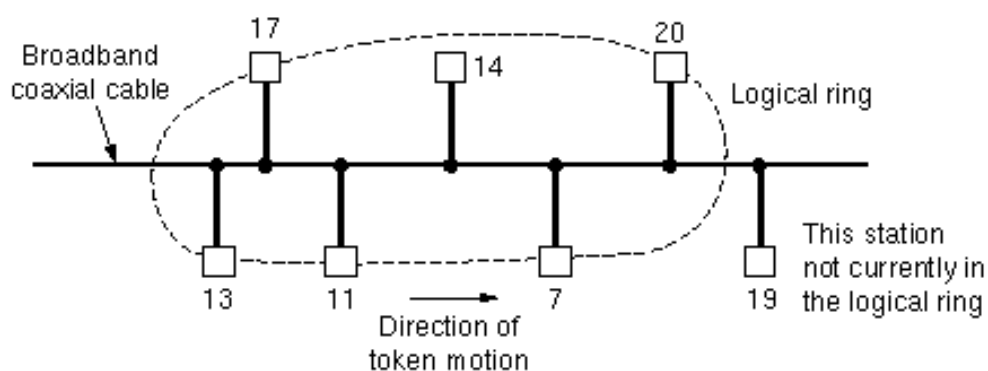


Fig 2.4 : Token Bus (802.4)

Token bus was standardized by IEEE standard 802.4. It is mainly used for industrial applications. Token bus was used by Motors for their Manufacturing Automation Protocol (MAP) standardization effort. This is an application of the concepts used in ring networks. The main difference is that the endpoints of the bus do not meet to form a physical ring.

Due to difficulties handling device failures and adding new stations to a network, token ring gained a reputation for being unreliable and difficult to upgrade. Bus networks, such as Ethernet, had a more flexible and reliable physical architecture, but Ethernet's access protocol could not absolutely guarantee a maximum time any station would have to wait to access the network, so was thought to be unsuitable for manufacturing automation applications. The Token bus protocol was created to combine the benefits of a physical bus network with the deterministic access protocol of a token ring network.

In order to guarantee the packet delay and transmission in Token bus protocol, a modified Token bus was proposed in Manufacturing Automation Systems and flexible manufacturing system (FMS). A means for carrying Internet Protocol over token bus was developed.

2.2.3 TOKEN RING (802.5)

Token ring local area network (LAN) technology is a communications protocol for local area networks. It uses a special three-byte frame called a "token" that travels around a logical "ring" of workstations or servers. This token passing is a channel access method providing fair access for all stations, and eliminating the collisions of contention-based access methods.

Introduced by IBM in 1984, it was then standardized with protocol IEEE 802.5 and was fairly successful, particularly in corporate environments, but gradually eclipsed by the later versions of Ethernet.

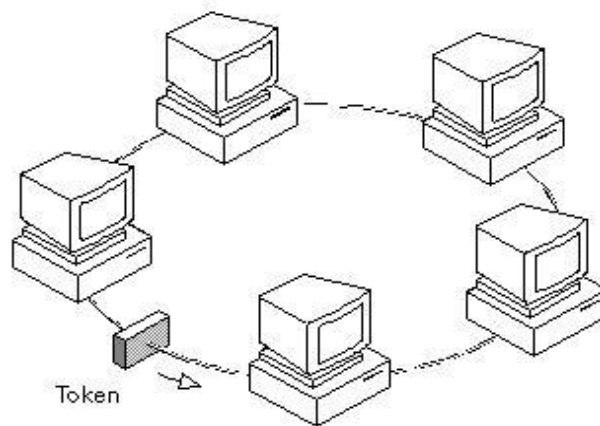


Fig.2.5 : Token Ring (802.5)

A wide range of different local area network technologies were developed in the early 1970s, of which one, the Cambridge Ring had demonstrated the potential of a token passing ring topology, and many teams worldwide began working on their own implementations.

2.2.4 ETHERNET

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations: Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and Ten-Gigabit Ethernet (10 Gbps),

10BASE5: THICK ETHERNET

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. The maximum length of the coaxial cable must not exceed 500 m.

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.

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. Note that two pairs of twisted cable create two paths (one for sending and one for receiving) 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

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.

2.2.4.1 FAST ETHERNET

Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled). IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps.

The goals of Fast Ethernet can be summarized as follows:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths.

2.2.4.2 GIGABIT ETHERNET

The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the Standard 802.3.

The goals of the 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 auto negotiation as defined in Fast Ethernet.

TEN-GIGABIT ETHERNET

The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3.

The goals of the Ten-Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 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.

2.2.5 COMPARISON OF 802.3,802.4 AND 802.5:

Standard specification	802.3	802.4	802.5
Structure	Size of the frame format is 1572 bytes	Size of the frame format is 8202 bytes	Variable size
Data field	Size of the field is 0 to 1500 bytes	Size of the data field is 0 to 8182 bytes	No limit
Priority	No priorities	Supports priorities	Priorities possible
Frame Requirement	Minimum frame short required is 64 bytes	It can handle short minimum frames	it support frames
Efficiency and throughput	Efficiency decrease and collision affects the throughput	It can handle short minimum frames	It support frames.

Modem	Modems are not required	Modems are required	Modems are required
Protocol	Protocol is simple complex	Protocol is extremely complex	Protocol is moderately complex

2.3 Fiber Distributed Data Interface

The Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps token-passing, dual-ring LAN using fiber-optic cable. FDDI is frequently used as high-speed backbone technology because of its support for high bandwidth and greater distances than copper.

As its name implies it runs on fiber optic cabling. It combines high speed performance with the advantages of a token passing ring topology. FDDI runs at 100 Mbps. FDDI are often used for MANs or larger LANs to connect several buildings in an office complex. It makes use of a token passing strategy, but its implementation and topology differ from a Token Ring.

2.3.1 FDDI Specifications

FDDI specifies the physical and media-access portions of the OSI reference model. FDDI is not actually a single specification, but it is a collection of four separate specifications, each with a specific function. Combined, these specifications have the capability to provide high-speed connectivity between upper-layer protocols such as TCP/IP and IPX, and media such as fiber-optic cabling.

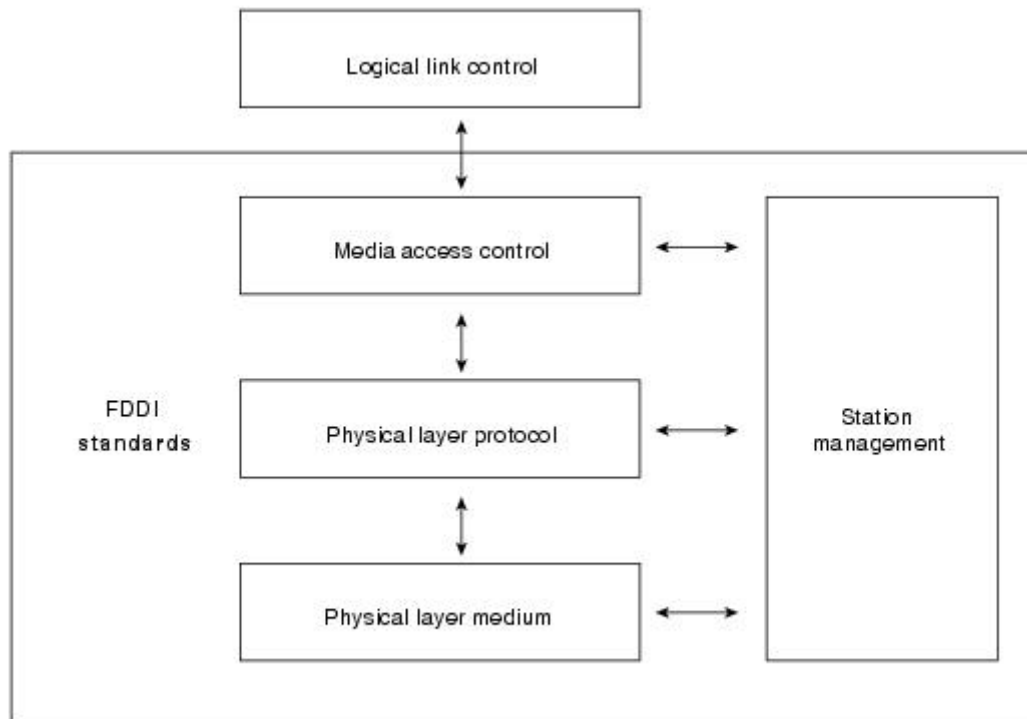


Fig.2.6 : FDDI Specifications

FDDI's four specifications are the Media Access Control (MAC), Physical Layer Protocol (PHY), Physical-Medium Dependent (PMD), and Station Management (SMT) specifications.

- The MAC specification defines how the medium is accessed, including frame format, token handling, addressing, algorithms for calculating cyclic redundancy check (CRC) value, and error-recovery mechanisms.
- The PHY specification defines data encoding/decoding procedures, clocking requirements, and framing, among other functions.
- The PMD specification defines the characteristics of the transmission medium, including fiber-optic links, power levels, bit-error rates, optical components, and connectors.
- The SMT specification defines FDDI station configuration, ring configuration, and ring control features, including station insertion and removal, initialization, fault isolation and recovery, scheduling, and statistics collection.

2.3.2 FDDI Frame Format

The FDDI frame format is similar to the format of a Token Ring frame. This is one of the areas in which FDDI borrows heavily from earlier LAN technologies, such as Token Ring. FDDI frames can be as large as 4,500 bytes.

Figure: The FDDI Frame Is Similar to That of a Token Ring Frame shows the frame format of an FDDI data frame and token.

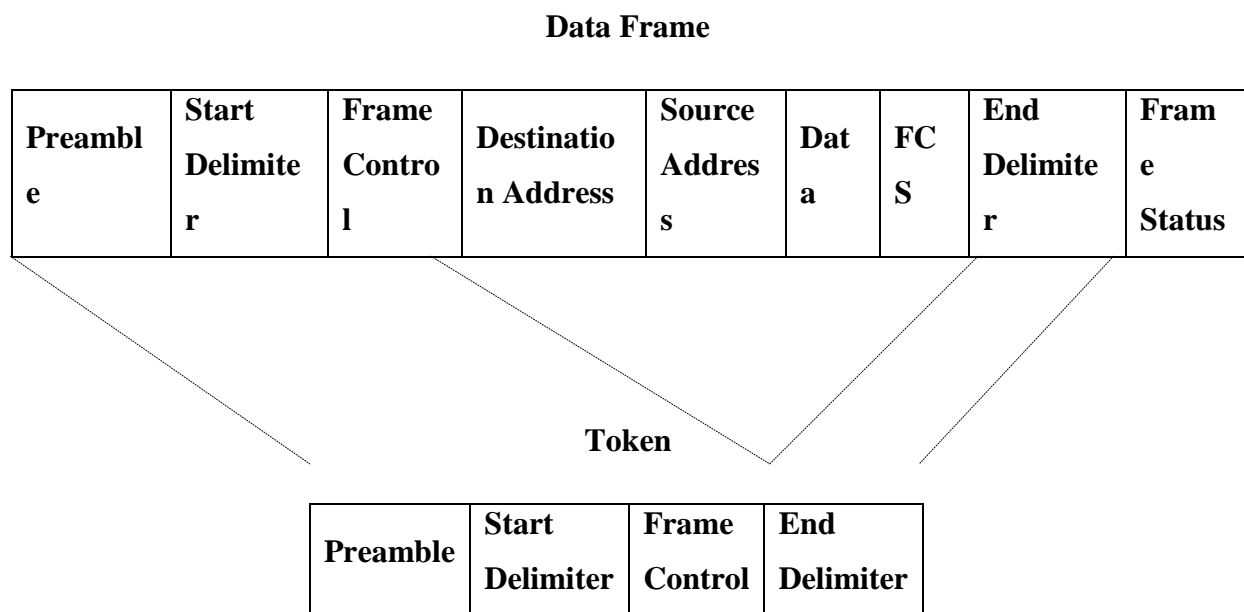


Fig.2.7 : FDDI Frame Format

FDDI Frame Fields

The following descriptions summarize the FDDI data frame and token fields illustrated in the above figure.

- **Preamble** - Gives a unique sequence that prepares each station for an upcoming frame.
- **Start delimiter** - Indicates the beginning of a frame by employing a signaling pattern that differentiates it from the rest of the frame.
- **Frame control** - Indicates the size of the address fields and whether the frame contains asynchronous or synchronous data, among other control information.

- **Destination address** - Contains a unicast (singular), multicast (group), or broadcast (every station) address. As with Ethernet and Token Ring addresses, FDDI destination addresses are 6 bytes long.
- **Source address** - Identifies the single station that sent the frame. As with Ethernet and Token Ring addresses, FDDI source addresses are 6 bytes long.
- **Data** - Contains either information destined for an upper-layer protocol or control information.
- **Frame check sequence (FCS)** - Is filed by the source station with a calculated cyclic redundancy check value dependent on frame contents (as with Token Ring and Ethernet). The destination address recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- **End delimiter** - Contains unique symbols; cannot be data symbols that indicate the end of the frame.
- **FRAME STATUS** Allows the source station to determine whether an error occurred; identifies whether the frame was recognized and copied by a receiving station.

2.3.3 MAJOR ADVANTAGES OF FDDI

- Token passing topology
- High speed fiber optic transmission
- Dual rings offer improved fault tolerance over other options
- Fiber optic cabling is less susceptible to EMI and noise
- Fiber optic cabling is more secure than copper wire
- It can send data for larger distances than Token Ring or Ethernet
- FDDI supports real-time allocation of network bandwidth.
- This allows you to use a wide array of different types of traffic.
- FDDI has a dual ring that is fault-tolerant. The benefit here is that if a station on the ring fails or if the cable becomes damaged, the dual ring is automatically doubled back onto itself into a single ring.
- The FDDI compensates for wiring failures. The stations wrap within themselves when the wiring fails.
- Optical bypass switches are used that can help prevent ring segmentation. The failed stations are eliminated from the ring.

2.3.4 MAJOR DISADVANTAGES OF FDDI

- Cost
- Distance limitations improve over other LANs, too limiting for WANs
- There's a potential for multiple ring failures.
 - This has kept many companies from deploying FDDI in a widespread manner. Instead, they have been using copper wire and the similar method of CDDI.
 - As the network grows, this possibility grows larger and larger.
 - The uses of fiber optic cables are expensive.

2.4 SWITCHING

A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central device and every other device (a star topology). These methods, however, are impractical and wasteful when applied to very large networks. The number and length of the links require too much infrastructure to be cost-efficient.

A better solution is switching. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing.

Traditionally, three methods of switching have been important: circuit switching, packet switching, and message switching. The first two are commonly used today. The third has been phased out in general communications but still has networking applications.

2.4.1 CIRCUIT-SWITCHED NETWORKS

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link.

A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels.

Figure shows a trivial circuit-switched network with four switches and four links. Each link is divided into n (n is 3 in the figure) channels by using FDM or TDM.

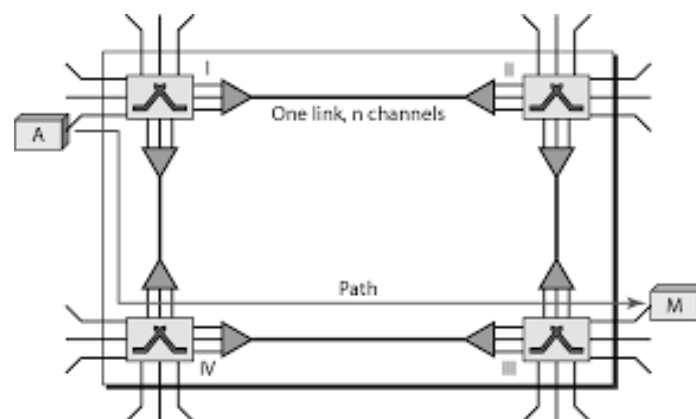


Fig.2.8 : Circuit-Switched Networks

The end systems, such as computers or telephones, are directly connected to a switch. We have shown only two end systems for simplicity. When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the setup phase; a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path. After the dedicated path made of connected circuits (channels) is established, data transfer can take place. After all data have been transferred, the circuits are torn down.

We need to emphasize several points here:

- Circuit switching takes place at the physical layer.
- Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase
- Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.
- There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM).

2.4.2 PACKET-SWITCHED NETWORKS

In data communications, we need to send messages from one end system to another. If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol.

In packet switching, there is no resource allocation for a packet. This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet. Resources are allocated on demand. The allocation is done on a firstcome, first-served basis. When a switch receives a packet, no matter what is the source or destination, the packet must wait if there are other packets being processed. As with other systems in our daily life, this lack of reservation may create delay. For example, if we do not have a reservation at a restaurant, we might have to wait.

In a packet-switched network, there is no resource reservation; resources are allocated on demand.

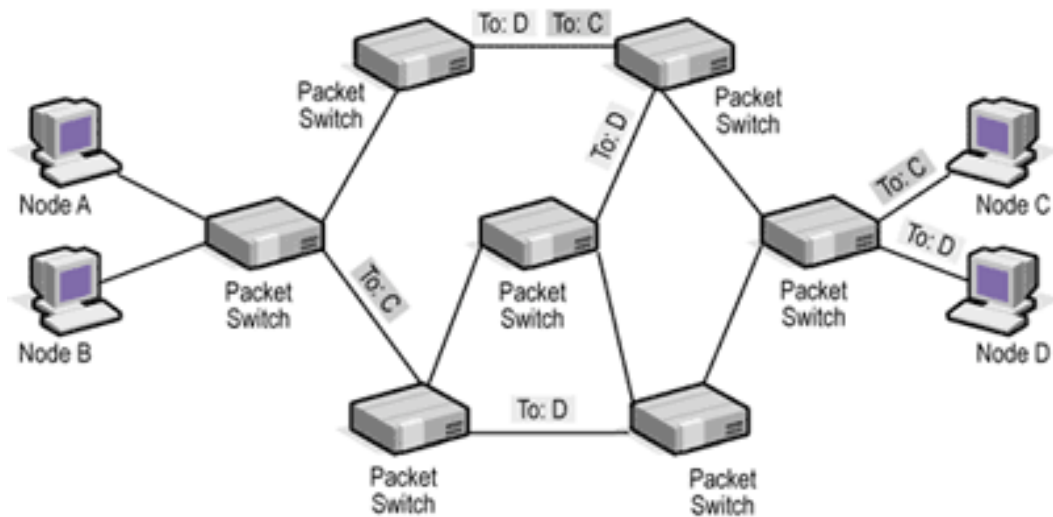


Fig 2.9 : Packet-Switched Networks

In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagram. Datagram switching is normally done at the network layer.

In this example, all four packets (or datagram) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.

The datagram networks are sometimes referred to as connectionless networks. The term connectionless here means that the switch (packet switch) does not keep information about the connection state.

2.4.3 MESSAGE SWITCHING

In telecommunications, message switching was the precursor of packet switching, where messages were routed in their entirety, one hop at a time. It was first built by Collins

Radio Company, Newport Beach, California, during the period 1959–1963 for sale to large airlines, banks and railroads. Message switching systems are nowadays mostly implemented over packet-switched or circuit-switched data networks.

Each message is treated as a separate entity. Each message contains addressing information, and at each switch this information is read and the transfer path to the next switch is decided. Depending on network conditions, a conversation of several messages may not be transferred over the same path.

Each message is stored (usually on hard drive due to RAM limitations) before being transmitted to the next switch. Because of this it is also known as a 'store-and-forward' network. Email is a common application for message switching. A delay in delivering email is allowed, unlike real-time data transfer between two computers.

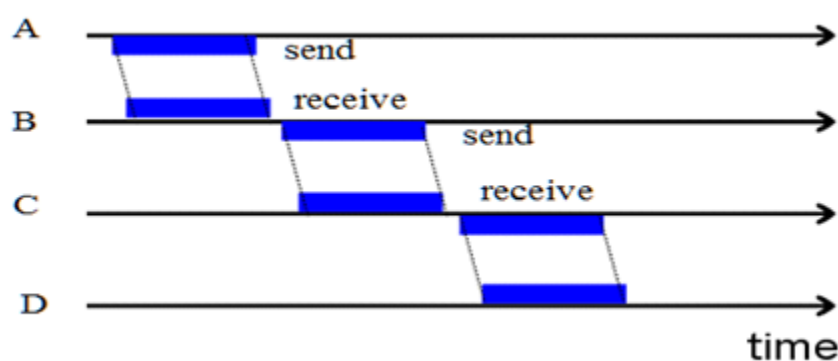


Fig 2.10 : Store and Forward

STORE AND FORWARD DELAYS

Since message switching stores each message at intermediate nodes, in its entirety before forwarding, messages experience an end to end delay which is dependent on the message length, and the number of intermediate nodes. Each additional intermediate node introduces a delay which is at minimum the value of the minimum transmission delay into or out of the node. Note that nodes could have different transmission delays for incoming messages and outgoing messages due to different technology used on the links. The transmission delays are in addition to any propagation delays which will be experienced along the message path.

In a message-switching centre an incoming message is not lost when the required outgoing route is busy. It is stored in a queue with any other messages for the same route and retransmitted when the required circuit becomes free. Message switching is thus an example of a delay system or a queuing system. Message switching is still used for telegraph traffic and a modified form of it, known as packet switching, is used extensively for data communications.

ADVANTAGES

The advantages to message switching are:

- Data channels are shared among communication devices, improving the use of bandwidth.
- Messages can be stored temporarily at message switches, when network congestion becomes a problem.
- Priorities may be used to manage network traffic.
- Broadcast addressing uses bandwidth more efficiently because messages are delivered to multiple destinations.

2.5 INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.

The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system.

The ISDN standards define several kinds of access interfaces, such as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).

ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s. In some countries,

ISDN found major market application for Internet access, in which ISDN typically provides a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. Channel bonding can achieve a greater data rate; typically the ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

In a videoconference, ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group (room) videoconferencing systems.

2.5.1 ISDN INTERFACES

Integrated services refers to ISDN's ability to deliver at minimum two simultaneous connections, in any combination of data, voice, video, and fax, over a single line. Multiple devices can be attached to the line, and used as needed. That means an ISDN line can take care of most people's complete communications needs (apart from broadband Internet access and entertainment television) at a much higher transmission rate, without forcing the purchase of multiple analog phone lines. It also refers to integrated switching and transmission in that telephone switching and carrier wave transmission are integrated rather than separate as in earlier technology.

BASIC RATE INTERFACE

The entry level interface to ISDN is the Basic Rate Interface (BRI), a 128 kbit/s service delivered over a pair of standard telephone copper wires. The 144 kbit/s payload rate is broken down into two 64 kbit/s bearer channels ('B' channels) and one 16 kbit/s signaling channel ('D' channel or data channel).

PRIMARY RATE INTERFACE

The other ISDN access available is the Primary Rate Interface (PRI), which is carried over an E1 (2048 kbit/s) in most parts of the world. An E1 is 30 'B' channels of 64 kbit/s, one 'D' channel of 64 kbit/s and a timing and alarm channel of 64 kbit/s.

2.5.2 BROADBAND INTEGRATED SERVICES DIGITAL NETWORK

In the 1980s the telecommunications industry expected that digital services would follow much the same pattern as voice services did on the public switched telephone network,

and conceived an end-to-end circuit switched services, known as Broadband Integrated Services Digital Network (B-ISDN).

Before B-ISDN, the original ISDN attempted to substitute the analog telephone system with a digital system which was appropriate for both voice and non-voice traffic. Obtaining worldwide agreement on the basic rate interface standard was expected to lead to a large user demand for ISDN equipment, hence leading to mass production and inexpensive ISDN chips. However, the standardization process took years while computer network technology moved rapidly. Once the ISDN standard was finally agreed upon and products were available, it was already obsolete. For home use the largest demand for new services was video and voice transfer, but the ISDN basic rate lacks the necessary channel.

This led to introduction of B-ISDN, by adding the word broadband. The designated technology for B-ISDN was Asynchronous Transfer Mode (ATM), which was intended to carry both synchronous voice and asynchronous data services on the same transport. The B-ISDN vision has been overtaken by other disruptive technologies used in the Internet.

PROTOCOL STRUCTURE OF B-ISDN

Broadband ISDN protocol reference model is based on the ATM reference model. ATM adaption layer is responsible for mapping the service offered by ATM to the service expected by higher layers.

ATM layer is independent of the physical medium over which transmission is to take place.

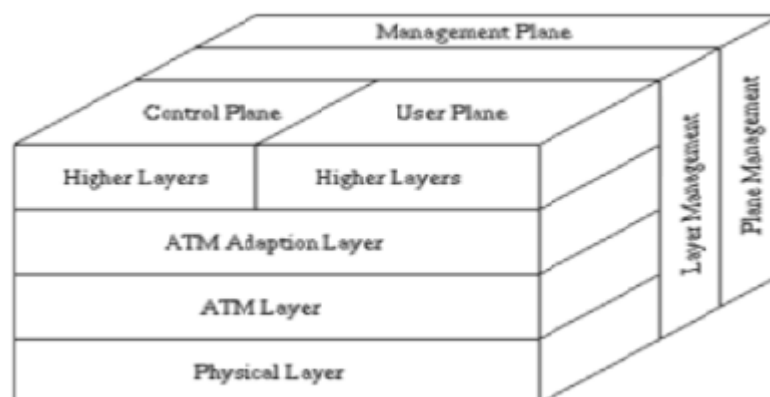


Fig 2.11 : B- ISDN protocol reference model

Physical layer consists of two sub layers Transport convergence and physical medium.

The control plane is responsible for the supervision of connections including call set up, call release and maintenance.

The User plane provides for the Transfer of user information. It also includes mechanisms to perform error recovery and flow control.

UNIT – III

TCP/IP SUIT

Objective:

- To learn the TCP/IP protocol protocol suite.
- To learn the functions of the various layer protocols – Application Layer Protocol, Transport Layer Protocol, Network Layer Protocol.
- To learn about the IP addressing, Subnetting, Supernetting and VLSM.

3.1. Overview of TCP / IP:

TCP/IP (transmission control **protocol**/Internet **protocol**) is the **suite** of communications **protocols** that is used to connect hosts on the Internet and on most other computer networks as well.

The Fig 3.1 shows the TCP / IP protocol suite with reference to the OSI seven layer model.

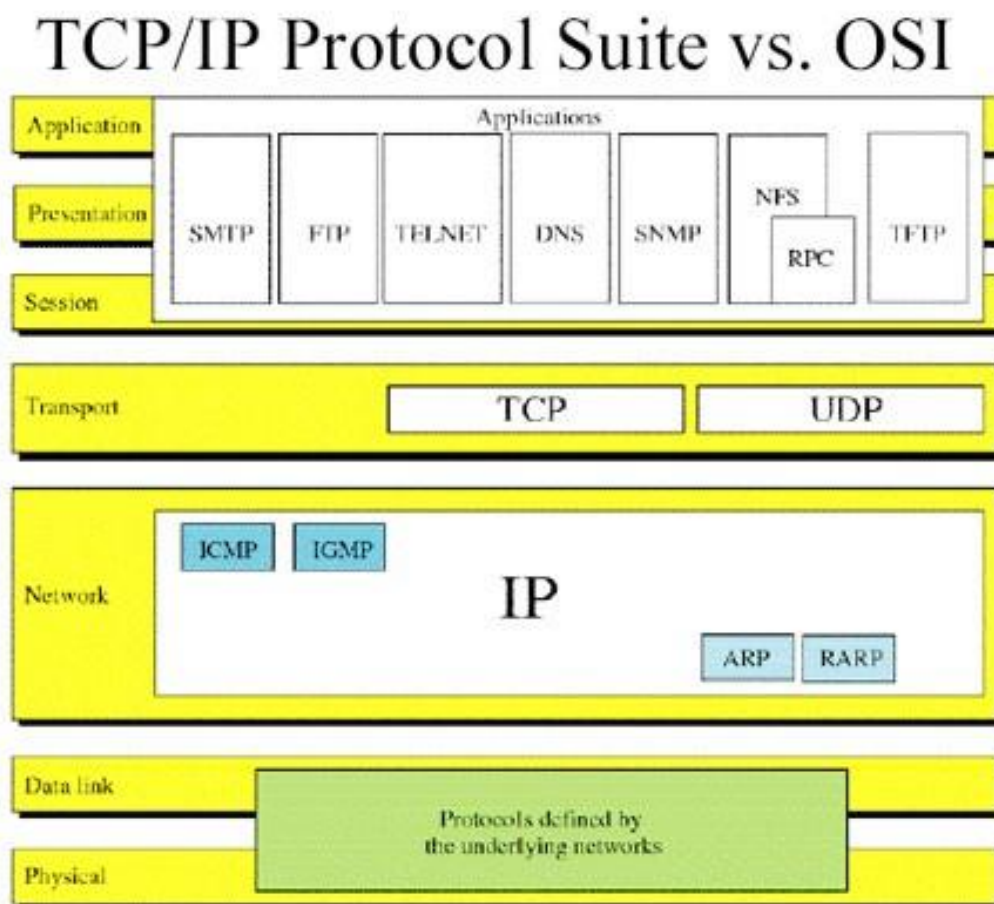


FIG 3.1

The two main protocols in the Transport layer of TCP/IP protocol suite are Transport Control Protocol (TCP) and User Datagram Protocol (UDP).

The TCP ensures that the communication between the sender and the receiver is reliable, error – free and in sequence.

The IP layer sends the individual datagrams through various routers, choosing a path for each datagram each time. The datagrams, may reach the destination via different routes and may reach out of sequence, the datagrams may not reach the destination correctly, the IP does not check the CRC of the data in datagram.

The TCP is responsible for checking any errors, reporting them and acknowledging the correct delivery of datagrams.

Whereas the UDP does not offer reliability, therefore faster.

3.1.2 Connection Oriented and Connectionless Services

In connection oriented service we have to establish a connection before starting the communication.

The following steps are performed in connection oriented service

1. Connection is established.
2. Send the message or the information
3. Release the connection.

Connection oriented service is more reliable than connectionless service. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination.

The order of message sent can be different from the order received.

In connectionless service the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

Table 3.1

Connection oriented service	Connectionless service
Authentication is required	No need for authentication
Makes a connection and checks whether message is received or not, if not it resends the message again.	It does not guarantees the delivery
More reliable	Unreliable
Stream based	Message based

3.1.3 Sockets

Applications running on different computers or devices communicate with the help of TCP with the concept called PORT. For example the various protocols in application layer uses the respective ports.:

FTP: 20 and 21

SMTP: 25

HTTP: 80

A port identifies a single application on a single computer. The term socket address or simply socket is used to identify the IP address and the port number concatenated together.

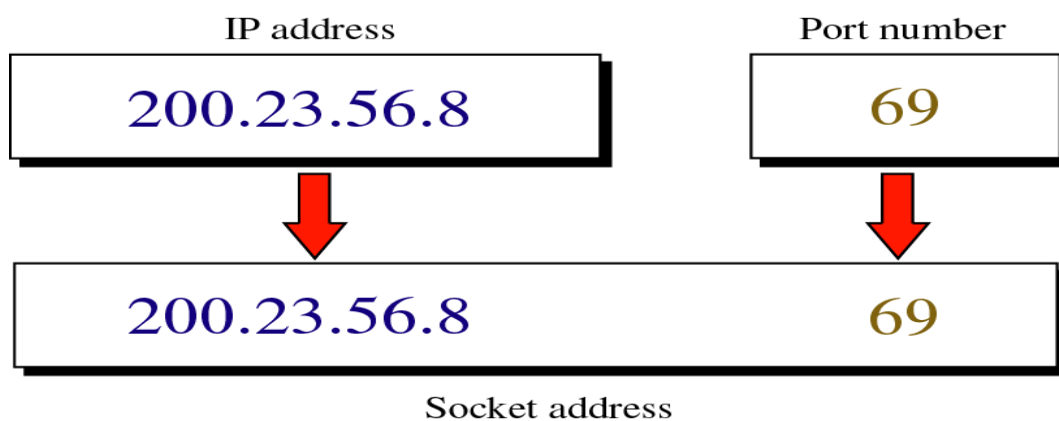


FIG 3.2

IP address + Port number = Socket

For eg:

IP address		Port number	Socket address
200.23.56.8	+	69	200.23.56.8:69

Transport Layer Protocol

- In the TCP/IP protocol suite, there are two major transport protocols: transmission control protocol (TCP) and user datagram protocol (UDP).

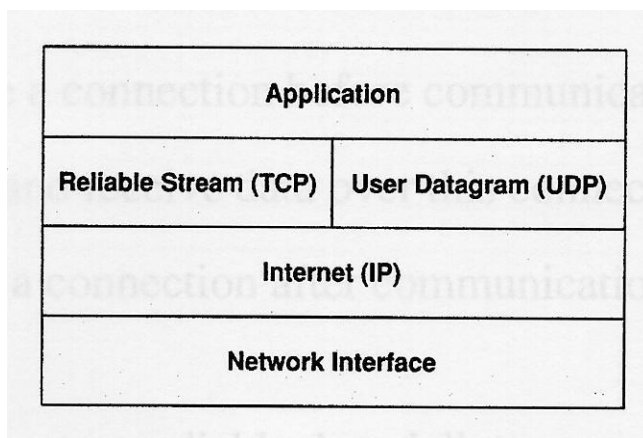


FIG 3.3

Role of TCP and UDP in the TCP/IP reference model:

3.1.4 Transmission Control Protocol (TCP)

- Basic Features
 - TCP provides connection-oriented communication (virtual circuit connection, like telephone communication). It manages a point-to-point and full-duplex connection for an application between two computers:
 - creates a connection before communication;
 - sends and receives data over this connection;
 - closes a connection after communication.
 - TCP guarantees reliable data delivery.

- The TCP recipient will receive data in a correct order without data loss or error.

Format of a TCP segment:

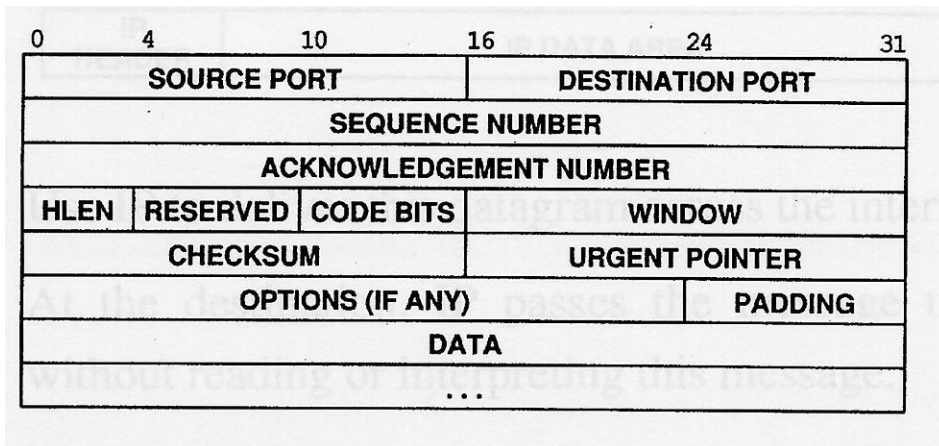


FIG 3.4

3.1.5 User Datagram Protocol (UDP)

- UDP is another popular transport protocol.
- Basic Properties of UDP
 - UDP is a connectionless transport protocol.
 - A UDP application sends messages without establishing and then closing a connection.
 - UDP has a smaller overhead than TCP, especially when the total size of the messages is small.
 - UDP does not guarantee reliable data delivery.
 - UDP messages can be lost or duplicated, or they may arrive out of order; and they can arrive faster than the receiver can process them.
 - The application programmers using UDP have to consider and tackle these issues themselves.
 - UDP has no mechanism for flow control.
 - Difference between UDP and IP

- UDP distinguishes among applications within a given host via the destination port number; an IP datagram only identifies a destination host via the IP address.

Format of a UDP segment:

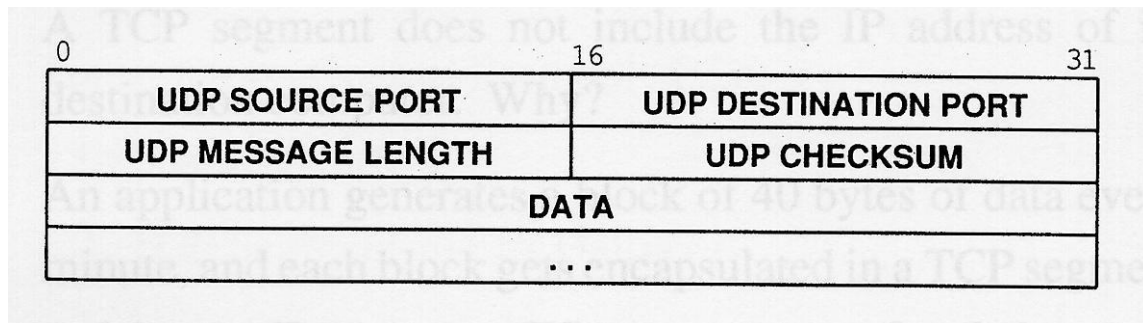


FIG 3.5

3.2. Network Layers Protocol:

The various protocols at network layer of TCP/IP protocol suite are

IGMP

ICMP

ARP

RARP

3.2.1 IGMP

The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers.

Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content.

Multicasting can be used for such applications as updating the address books of mobile computer users in the field, sending out company newsletters to a distribution list, and "broadcasting" high-bandwidth programs of streaming media to an audience that has "tuned in" by setting up a multicast group membership.

- IGMP is a protocol that manages group membership. The IGMP protocol gives the multicast routers information about the membership status of hosts (routers) connected to the network. .



FIG 3.6

- Internet Group Management Protocol (IGMP) is one of the necessary, but not sufficient, protocol for multicasting.
- IGMP is a companion to the IP protocol
- IGMP is a group management protocol. It helps a multicast router create and update a list of loyal members related to each router interface

IGMP has three types of messages: the query, the membership report, and the leave report.

There are two types of query messages, general and special.

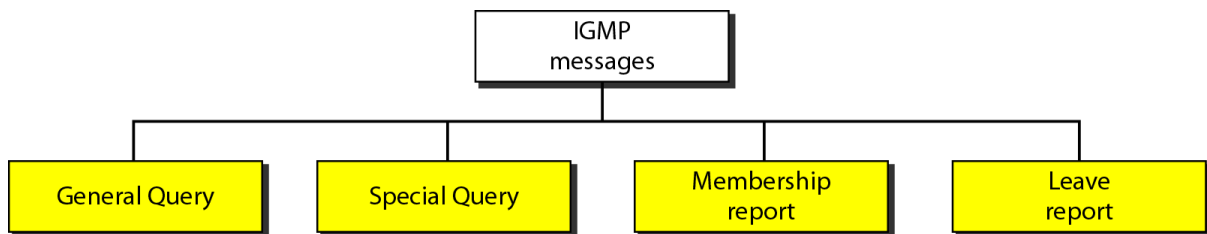


FIG 3.7

IGMP messages are used by multicast routers to track group memberships on each of its networks. It uses these rules:

1. The first time a process on a host joins a multicast group, the host will send an IGMP report. This means that every time the host needs to receive messages from a new group to support its processes, it will send a report.
2. Multicast routers will send IGMP queries regularly to determine whether any hosts are running processes that belong to any groups. The group address of the query is set

to 0, the TTL field is set to 1, and the destination IP address is 224.0.0.1 which is the all hosts group address which address all the multicast capable routers and hosts on a network.

3. A host sends one IGMP response for each group that contains one or more processes. The router expects one response from each host for each group that one or more of its processes require access to.
4. A host does not send a report when its last process leaves a group (when the group access is no longer required by a process). The multicast router relies on query responses to update this information.

IGMP message formats are encapsulated in an IP datagram which contain a time to live (TTL) field. The default is to set the TTL field to 1 which means the datagram will not leave its subnetwork. an application can increase its TTL field in a message to locate a server distance in terms of hops.

Addresses from 224.0.0.0 to 224.0.0.255 are not forwarded by multicast routers since these addresses are intended for applications that do not need to communicate with other networks. Therefore these addresses can be used for group multicasting on private networks with no concern for addresses being used for multicasting on other networks.

3.2.2 ICMP

The Internet Control Message Protocol (**ICMP**) is one of the main protocols of the Internet Protocol Suite.

The IP protocol delivers the datagram from source to destination. The IP Protocol has no error reporting or error correcting mechanism , it is an unreliable protocol.

If any error occurs in reaching the destination that error situation is handled by ICMP. So it is called the companion to IP protocol.

It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.

ICMP messages are divided into two broad categories: error-reporting messages and query messages.

The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.

The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.

Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages.

- ✓ Message Format
- ✓ Error Reporting Messages
- ✓ Query Messages
- ✓ Checksum

Error reporting –ICMP only reports the error, but do not correct the error. The error correction is handled by higher level protocols.

Five type of error are handled:



FIG 3.8

1. Destination unreachable – When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination unreachable message.

2. Source quench – This means the source host does not know the about the traffic whether routers between the source and destination host is overwhelmed with more datagrams. The source quench message in ICMP was designed to add a kind of flow control to the IP.

3. Time exceeded – this type error reporting messages are generated in two cases. Routers use routing tables to find the next hop, if any packet enter into a loop or a cycle, going from one router to another endlessly. The Time to live field handles this situation, whenever the packet hops to the next router the value is decremented by 1 and if time to live reaches 0 before reaching the destination then the Time exceeded message is reported.

4. Parameter Problem – If any router or destination host discovers any missing parameters in datagram, it discards the datagram and sends a parameter-problem message back to the source.

5. Redirection – Redirecting the datagrams to the destination hghost with the help of static routing.

Query

Apart from error reporting, ICMP can diagnose network problems. This is accomplished by the query messages.

3.2.3 ARP

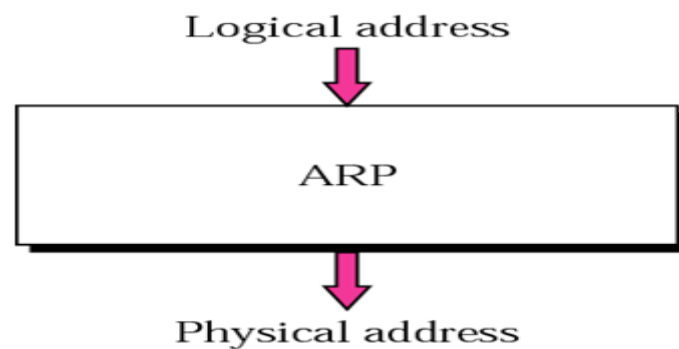
Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address.

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address.

The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine.

If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it.

A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address



that replied.

- ARP associates an IP address with its MAC addresses
- An ARP request is broadcast; an ARP reply is unicast.

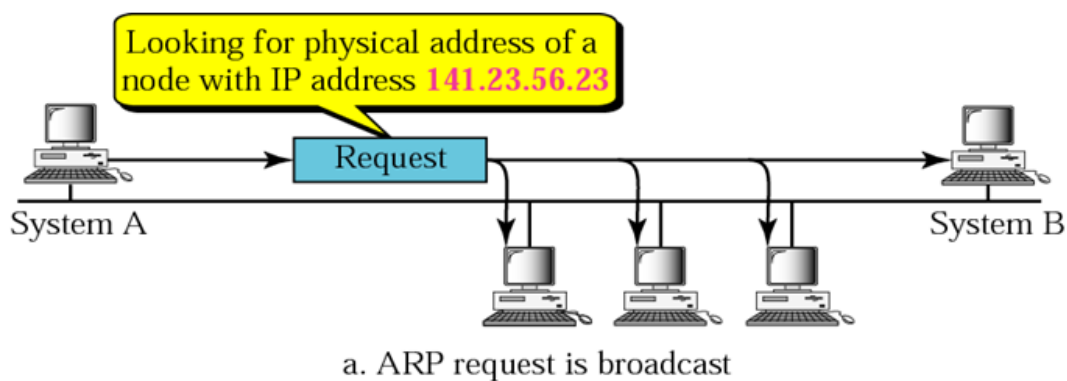


FIG 3.9

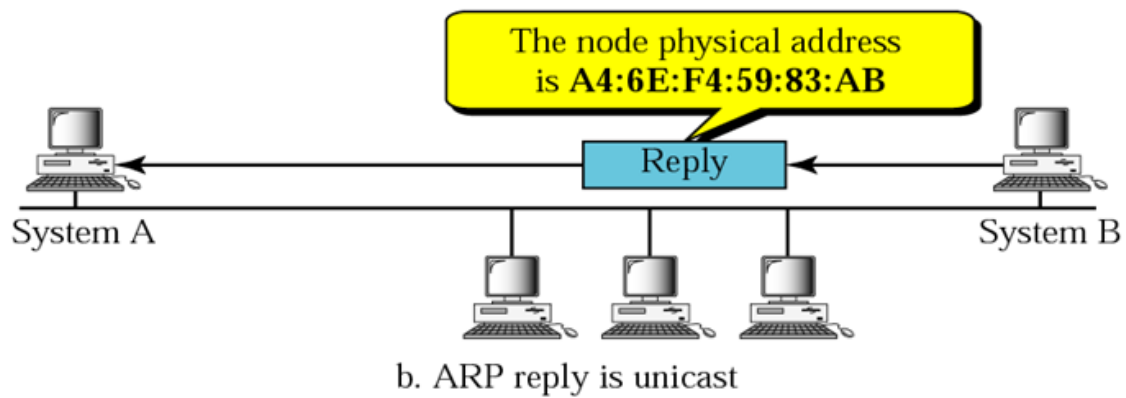


FIG 3.10

3.2.4 RARP

The Reverse Address Resolution Protocol (RARP) is an network layer protocol used by a client computer to request its Internet Protocol(IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address.

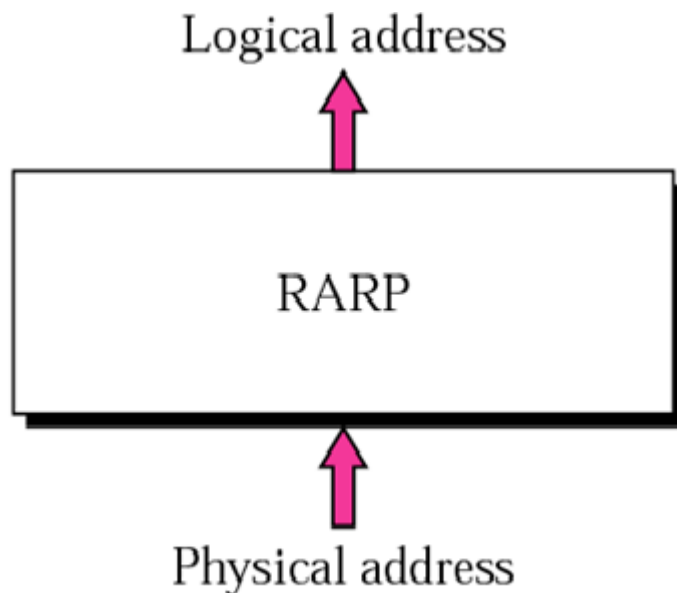


FIG 3.11

- RARP (replaced by DHCP): mapping a MAC address to an IP address

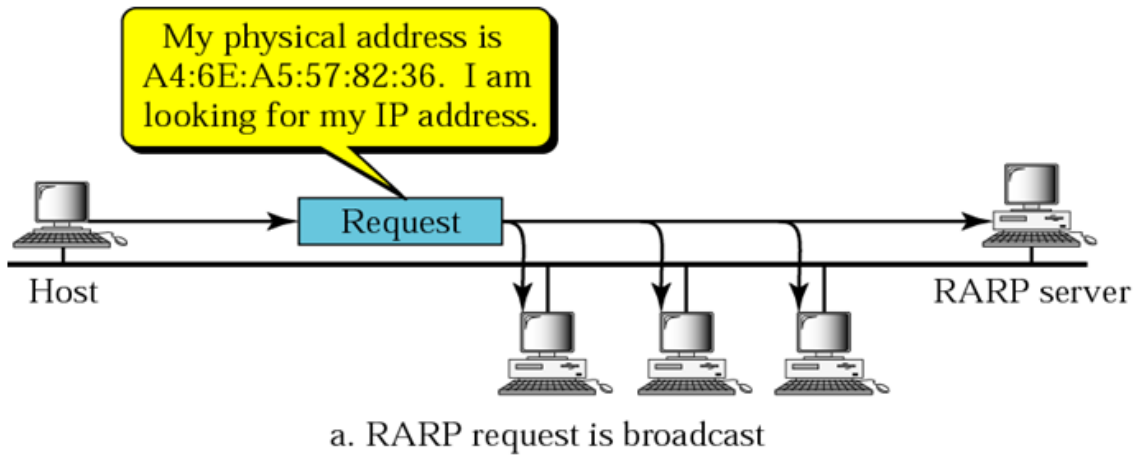


FIG 3.12

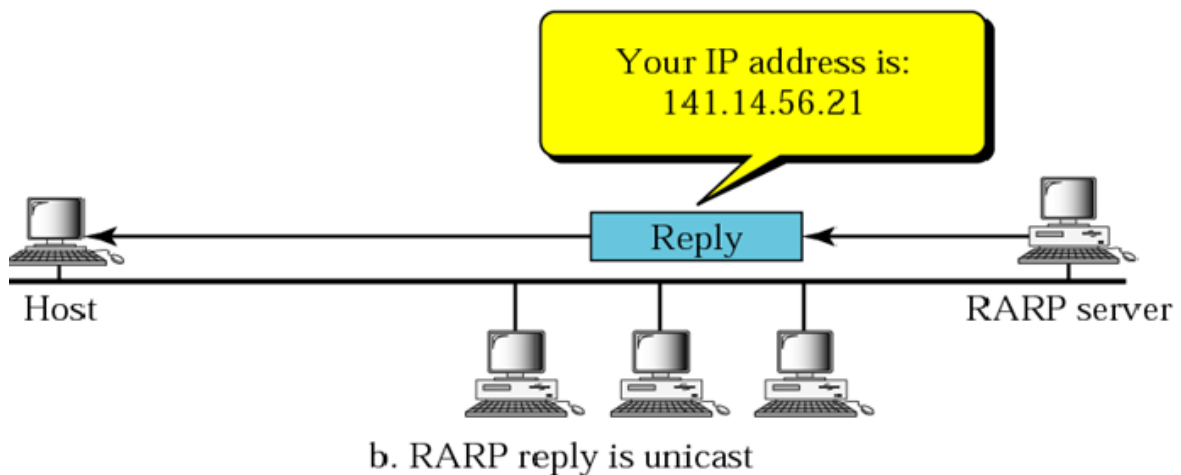


FIG 3.13

3.3. IP Addressing

Addressing of computers are categorized into two:

1. Physical address or MAC address.
2. Logical address or IP address.

3.3.1 IP addressing

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

The two most common versions of IP in use today are Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). Both IPv4 and IPv6 addresses come from finite pools of numbers. For IPv4, this pool is **32-bits** (2^{32}) in size and contains 4,294,967,296 IPv4 addresses.

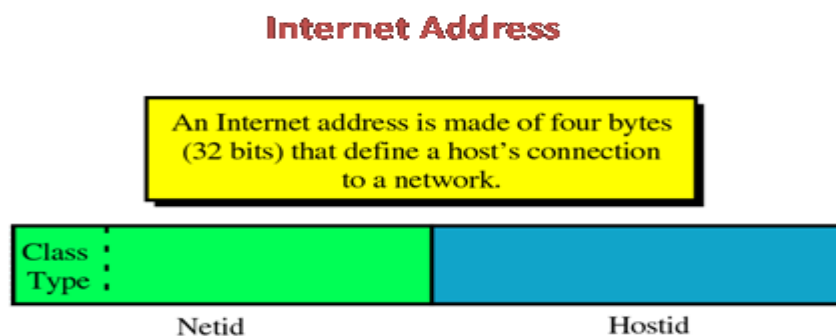


FIG 3.14

3.3.2 Dot-decimal notation

Dot-decimal notation is a presentation format for numerical data. It consists of a string of decimal numbers, each pair separated by a full stop (dot).

Example:

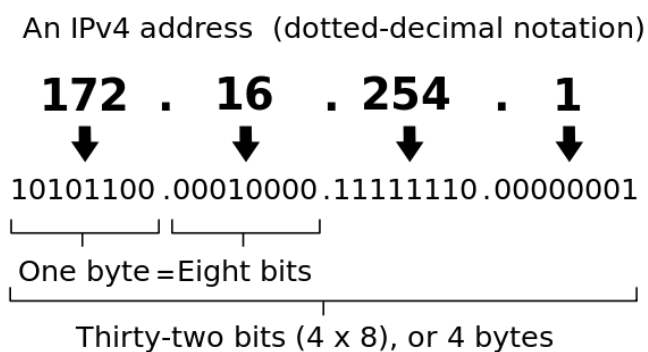


FIG 3.15

Classes of IP address:

- divided into 5 classes
 - class A: start with 0, then 7-bit code
 - $2^{24} = 16,777,216$ hosts in subnetwork
 - class B: start with 10, then 14-bit code
 - $2^{16} = 65,536$ hosts in subnetwork
 - class C: start with 110, then 21-bit code
 - $2^8 = 256$ hosts in subnetwork
 - class D: start with 1110
 - used for multicasting
 - class E: start with 11110
 - reserved for future use
 - IPv6 extends address size to 128 bits
 - extensions support authentication, data integrity, confidentiality

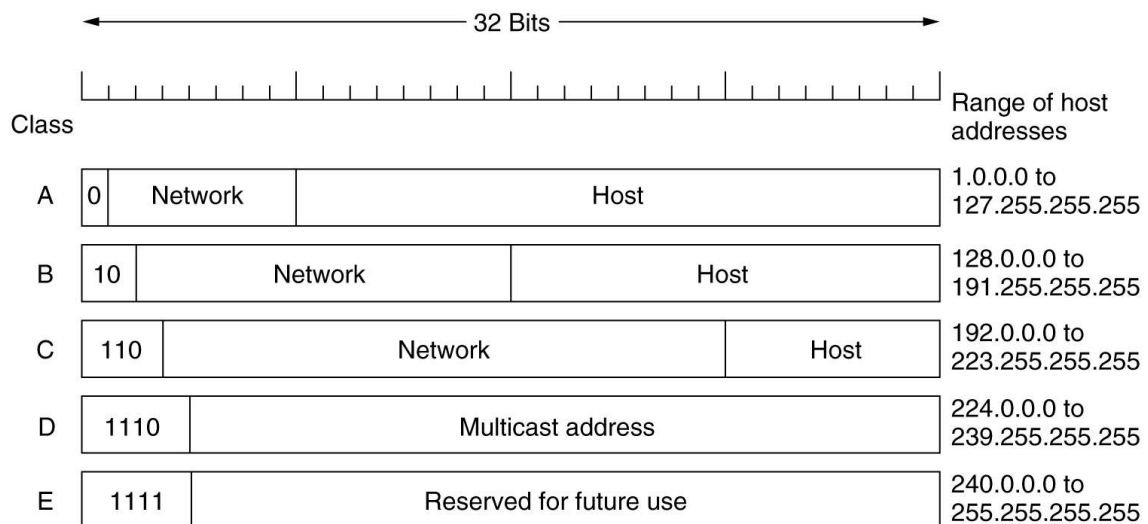


FIG 3.16 Classes of IP address

3.3.2 Subnetting

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.

In general the IP address is a two-level hierarchy with Network id and Host id. When subnetting the larger network the IP address consists of Network id, Subnet id and Host id thus forming the three-level hierarchy.

Subnet mask: Subnet mask is a 32 bits long address used to distinguish between network address and host address in IP address. Subnet mask is always used with IP address. Subnet mask has only one purpose, to identify which part of an IP address is network address and which part is host address.

For example how will we figure out network partition and host partition from IP address 192.168.1.10 ? Here we need subnet mask to get details about network address and host address.

In decimal notation subnet mask value is from 1 to 255 represent network address and value 0 represent host address.

In binary notation subnet mask ON bit 1 represent network address while OFF bit[0] represent host address.

In decimal notation

IP address	192.168.1.10
Subnet mask	255.255.255.0

Network address is **192.168.1** and host address is **10**.

In binary notation

IP address	11000000.10101000.00000001.00001010
Subnet mask	11111111.11111111.11111111.00000000

Network address is 11000000.10101000.00000001 and host address is 00001010

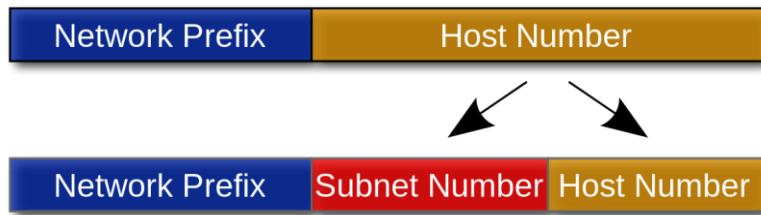


FIG 3.17

- Split the host number portion of an IP address into a **subnet number** and a (smaller) **host number**.
- Result is a 3-layer hierarchy
- Then:
 - Subnets can be freely assigned within the organization
 - Internally, subnets are treated as separate networks
 - Subnet structure is not visible outside the organization.

A Network with Two Levels of Hierarchy

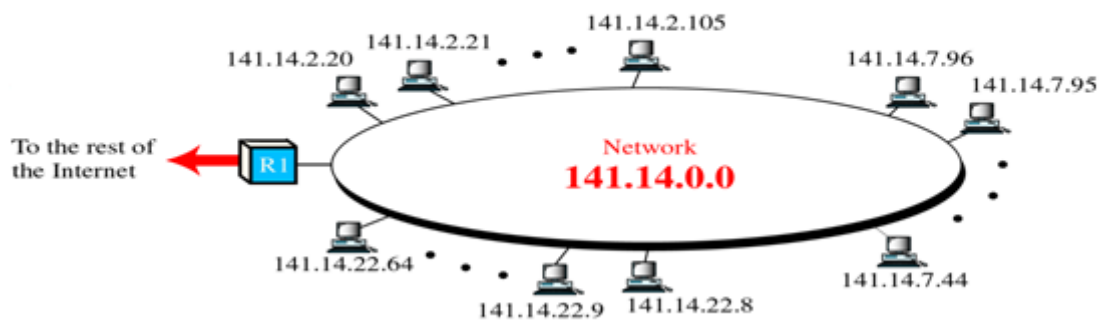


FIG 3.18

After dividing (subnetting) the larger network is divided into subnets three level of hierarchy is formed.

A Network with Three Levels of Hierarchy

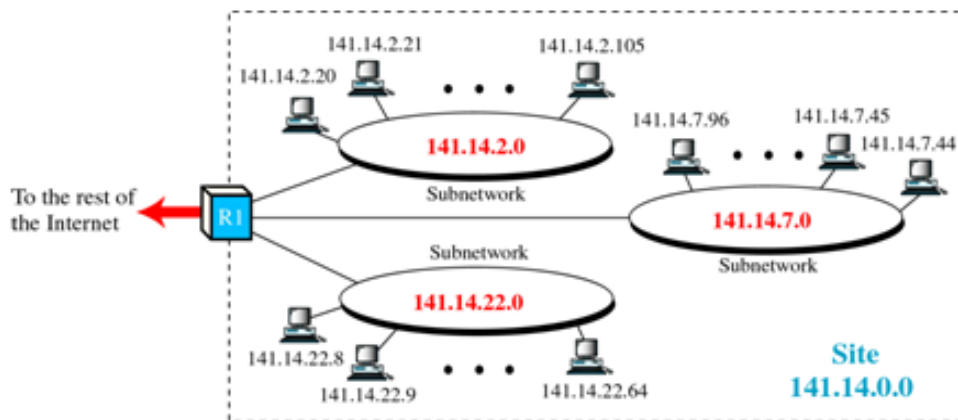


FIG 3.19

3.3.3 Supernetting

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

The new routing prefix for the combined network represents the constituent networks in a single route table entry.

Supernetting is used in route aggregation to reduce the size of routing tables and routing table updates.

As the Internet has grown, it has become more difficult for organizations to obtain Class A or Class B addresses for their networks. Most Class A or B network addresses have already been assigned. The problem is compounded by the fact that Class C networks are limited to a maximum of 254 hosts.

One solution to this problem is supernetting. To create a supernetwork, or supernet, an organization uses a block of IP addresses assigned to several Class C networks to create one large network.

3.3.4 VLSM technique

Variable Length Subnet Mask (VLSM) extends classic Subnetting. VLSM is a process of breaking down subnets into the smaller subnets, according to the need of individual networks.

VLSM allows us to divide an IP address space into a hierarchy of subnets of different sizes, making it possible to create subnets with very different host counts without wasting large numbers of addresses.

3.3.5 IPV6

In order to communicate over the Internet, computers and other devices must have sender and receiver addresses. These numeric addresses are known as Internet Protocol addresses.

IPv6 is the Internet's next-generation protocol, designed to replace the current Internet Protocol, IP Version 4.

Internet Protocol **version 6 (IPv6)** is the most recent **version** of the Internet Protocol (**IP**), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

Compared to IPv4, the most obvious advantage of IPv6 is its larger address space. The most obvious improvement in **IPv6** over IPv4 is that IP addresses are lengthened from 32 bits to 128 bits.

3.4 Application Layer Protocols

The various protocols in application layer are :

FTP

Telnet

SMTP

HTTP

DNS

POP.

3.4.1 FTP

The **File Transfer Protocol (FTP)** is a standard network **protocol** used to **transfer** computer files between a client and server on a computer network.

FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.

Command processing



FIG 3.20

It is a standard mechanism provided by TCP/IP for copying file from one host to another. FTP uses the services of TCP. It needs two TCP connections. The well-known port 21 is used for the control connection and the well-known port 20 for the data connection.

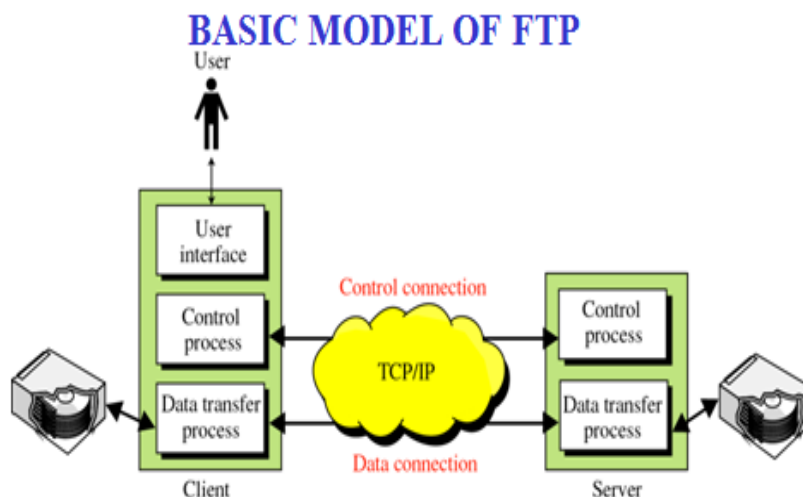


FIG 3.21

FTP presents the user with a prompt and allows entering various commands for accessing and downloading files that physically exist on a remote computer.

After invoking an FTP application,

The user identifies a remote computer and instructs FTP to establish a connection with it.

FTP contacts the remote computer using the TCP/IP software.

Once the connection is established, the user can choose to download a file from the computer or the user can send a file from his computer to be stored on the remote computer.

File transfer



FIG 3.22

The following figure depicts the communication between the client and server.

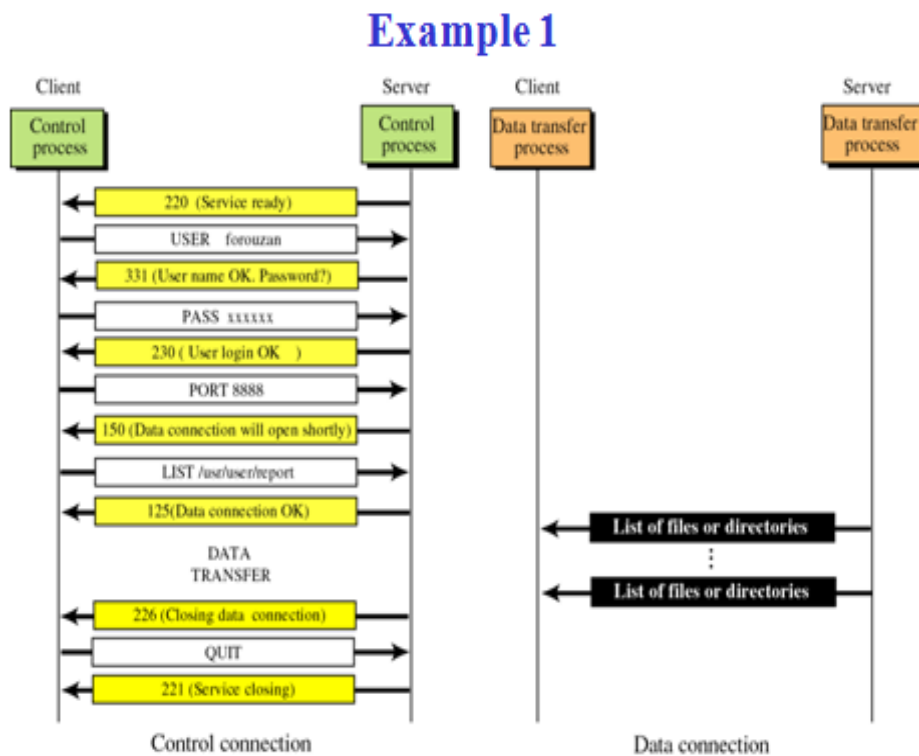


FIG 3.23

3.4.2 Telnet

TELNET is a general-purpose client-server application program. TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.

TELNET has two parts, the client and server.

The client portion of TELNET software resides on an end user's machine, and the server portion resides on a remote server machine. This server is the TELNET server, which provides an interactive terminal session to execute commands on the remote host.

In timesharing systems, all users log into the centralized server and uses its resources. This is called local login.

A user's terminal sends the commands entered by the user from the **terminal** is carried to the **terminal driver** which is running on the server and it is the part of the **server** machine operating system.

The terminal driver then sends the requests to the appropriate module of the server operating system.

The operating system then processes this commands and invokes the appropriate application program, which executes on the server machine and the result is send back to the terminal.

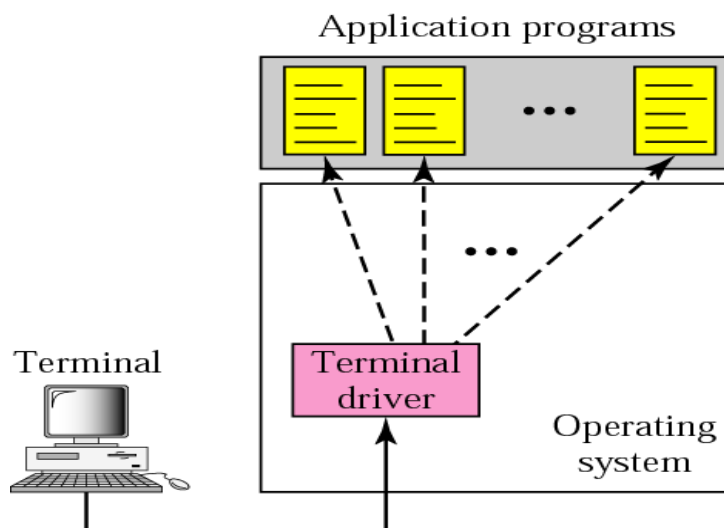


FIG 3.24

Remote Login and TELNET

Sometimes if a user wants to access an application program located on a remote computer. The user has to log on to remote computer in a process called remote login.

Via a universal interface called the Network Virtual Terminal (NVT) character set,

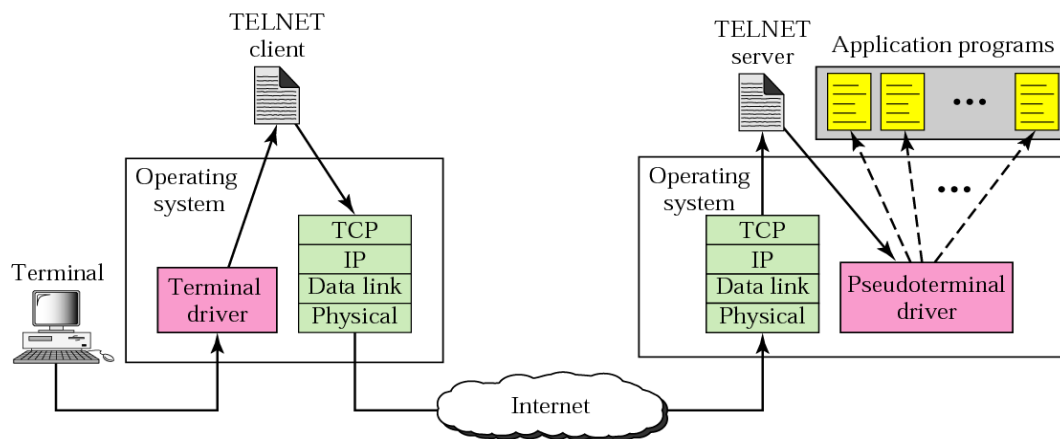


FIG 3.25

The commands from the terminal is sent to the operating system of common server computer as that in local login the commands are not interpreted but sent to the TELNET client translates characters (data or commands) that come from the local terminal into NVT form and delivers them to the network. The TELNET server translates data and commands from NVT form into the form acceptable by the remote computer.

The pseudo-terminal driver is a software program which handles the commands from the terminal via TELNET Server which invokes the appropriate application on the remote server.

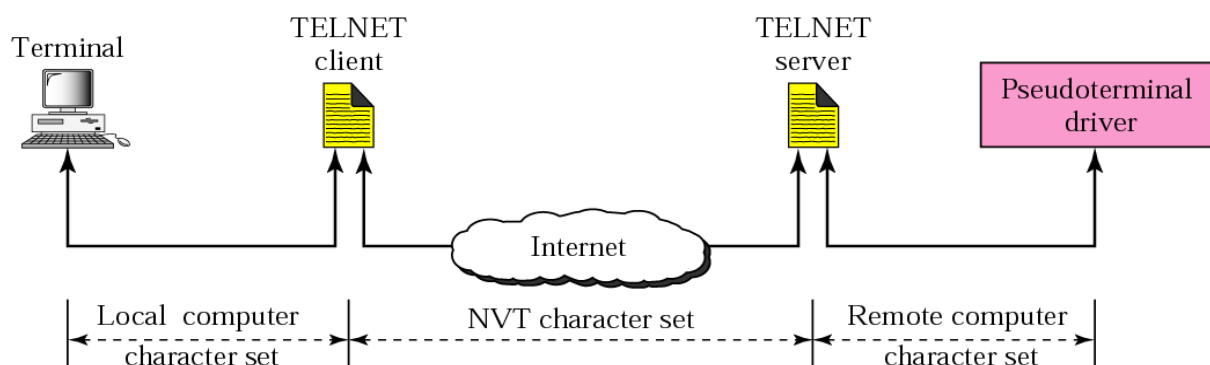


FIG 3.26

3.4.3 SMTP

Simple Mail Transfer Protocol (SMTP) is used to send mail across the internet.

SMTP concept

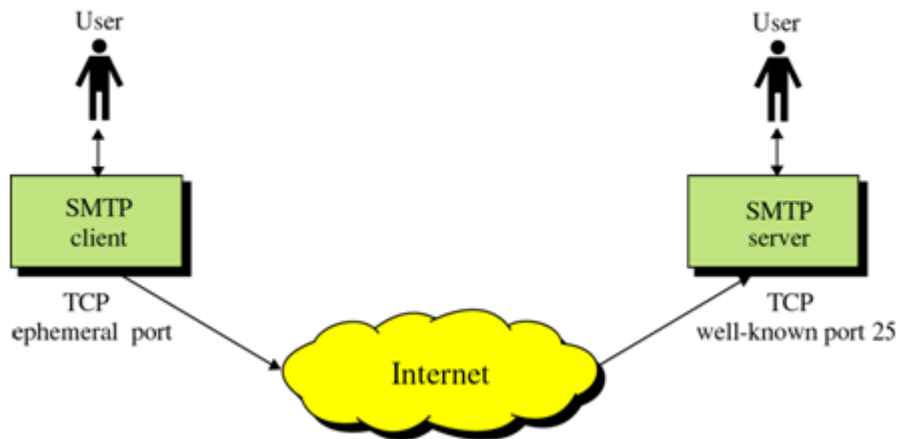


FIG 3.27

The TCP/IP protocol that supports electronic mail on the internet is called SMTP. It is the system for sending messages to other computer users based on e-mail addresses. SMTP provides for mail exchange between users on the same or different computers and supports:

1. sending single message to one or more recipients.
2. sending messages that include text, voice, video or graphics.
3. sending messages to users on networks outside the internet.

UA - users agent. This is the program a user will use to type e-mail. It usually incorporates an editor for support. The user types the mail and it is passed to the sending MTA.

MTA - Message transfer agent is used to pass mail from the sending machine to the receiving machine. There is a MTA program running on both the sending and receiving machine.

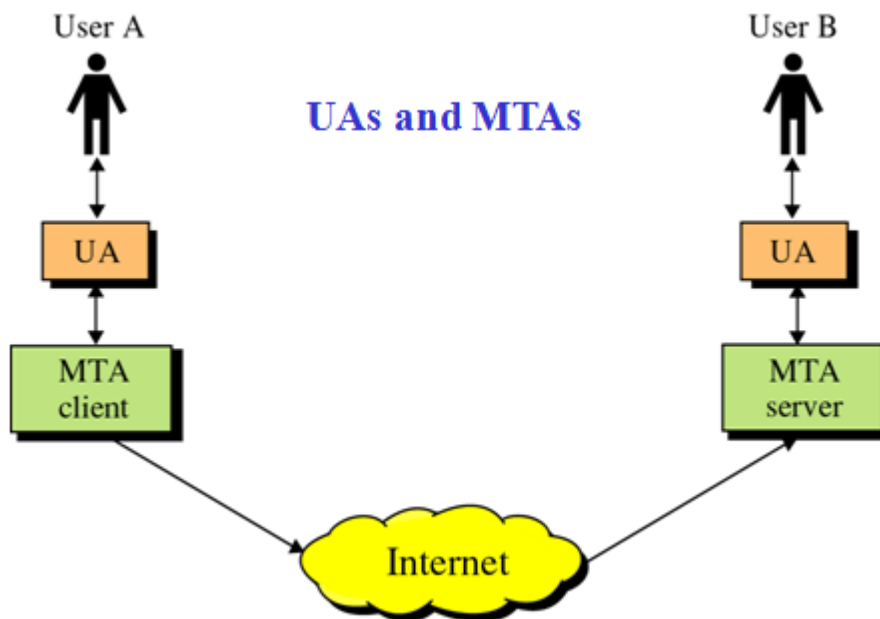


FIG 3.28

The MTA on both machines use the network SMTP (simple mail transfer protocol) to pass mail between them, usually on port 25.

SMTP protocol allows a more complex system with relaying.

Relaying system allows sites that do not use the TCP/IP protocol suite to send e-mail to users on other sites that may or may not use the TCP/IP protocol suite.

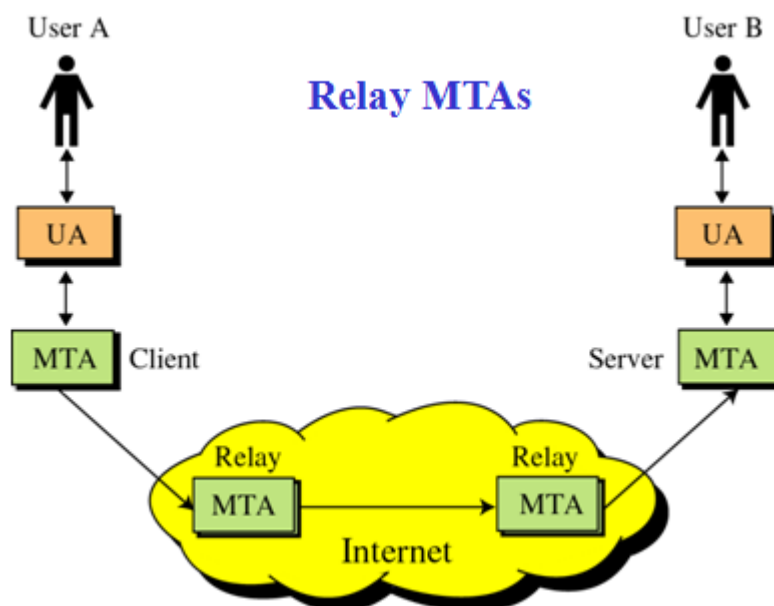


FIG 3.28(a)

This is accomplished by using mail gateway. Mail gateway is a relay MTA that can receive mail prepared by a protocol other than SMTP and transform it to SMTP format before sending it.

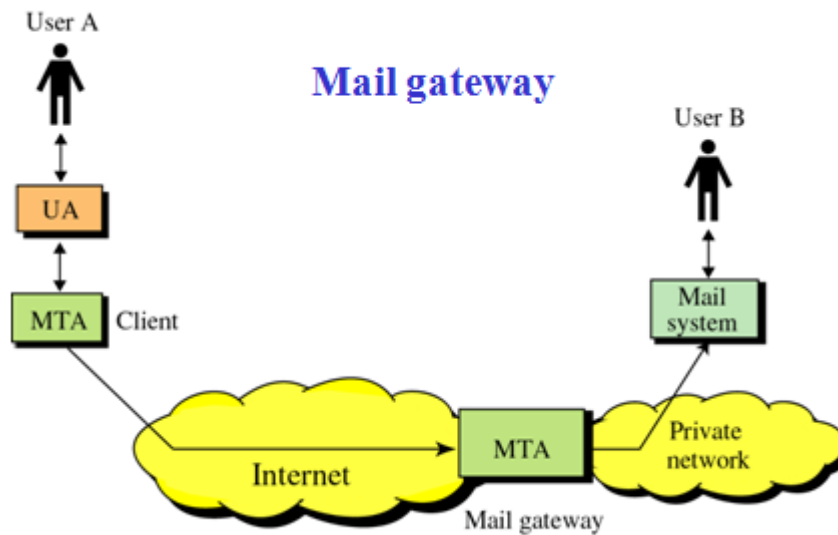


FIG 3.29

The address format used for sending mail in general which is called email id to communicate.

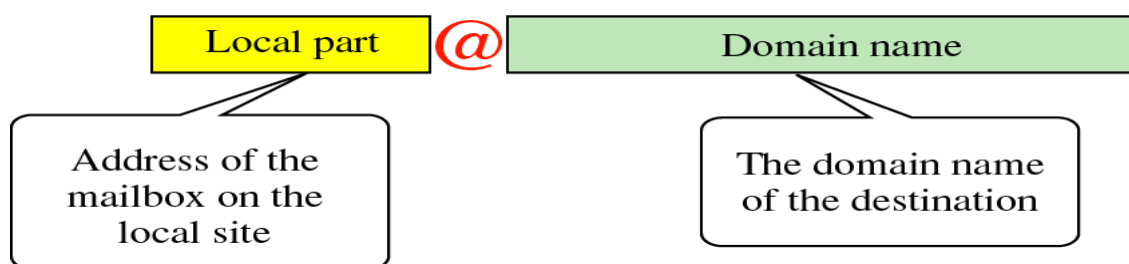


FIG 3.30

The overall protocols and components involved in mail communication is represented in figure below:

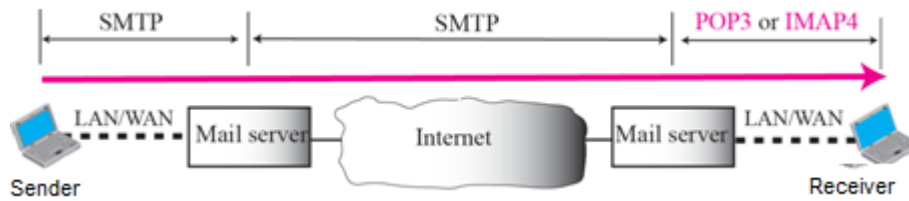


FIG 3.31

Other components of mail service include:

- Directory services - A list of users on a system. Microsoft provides a Global Address List and a Personal Address Book.
- Post Office - This is where the messages are stored.

3.4.4 HTTP

One of the application layer protocol is HTTP. Hyper Text Transfer Protocol.

HTTP is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

For example, when a URL is entered from a client browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

Some of the HTTP commands are: GET, HEAD, PUT, POST, DELETE, LINK

Request line



FIG 3.32

The client submits an HTTP request message to the server.

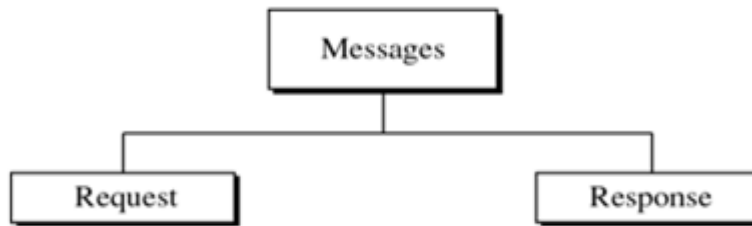


FIG 3.33

The server, which provides resources such as HTML files (web pages) and other content, or performs other functions on behalf of the client, returns a response message to the client.

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

HTTP transaction

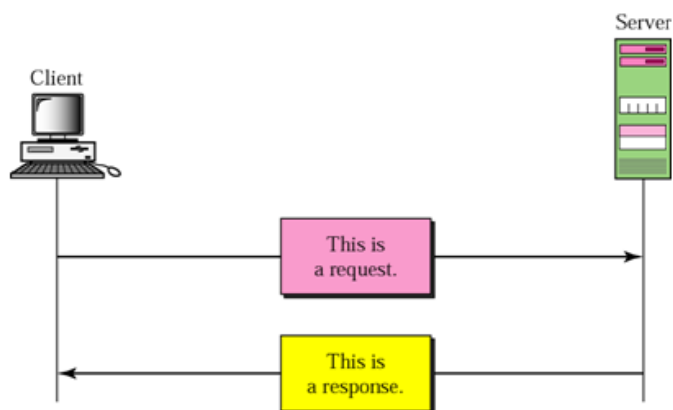


FIG 3.34

3.4.5 DNS - Domain Name System

A simple idea in identifying computer networks and computers on those networks by some name is the basis for domain names.

Domain name is a name given to a group of computers that are called by single name is called Domain.

These Domain names are to be translated to its respective IP addresses because this IP address is handled by the TCP/IP or the internet understands while sending and receiving any messages. This translation is handled by DNS.

The Domain Name System (DNS) is basically a large database which resides on various computers and it contains the names and IP addresses of various hosts on the internet and various domains.

The Domain Name System is used to provide information to the Domain Name Service to use when queries are made.

The service is the act of querying the database, and the system is the data structure and data itself.

The humans use domain names when referring to computers in network whereas computers use IP addresses.

Domain names are used in URLs to identify particular Webpages. For example, in the URL <http://www.tndte.gov> the domain name is tndte.gov.

The DNS is distributed, means the database containing the mapping between the domain names and IP addresses is scattered across the different computers.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

The domain name system database is divided into sections called **zones**.

The name servers in their respective zones are responsible for answering queries for their zones.

A zone is a subtree of DNS and is administered separately. There are multiple name servers for a zone. There is usually one primary nameserver and one or more secondary name servers. A name server may be authoritative for more than one zone.

Every domain name has a suffix that indicates which top level domain (TLD) it belongs to. There are only a limited number of such domains. For example:

- **gov** - Government agencies
- **edu** - Educational institutions
- **org** - Organizations (nonprofit)
- **mil** - Military
- **com** - commercial business
- **net** - Network organizations
- **ca** - Canada
- **in** – India

Because the Internet is based on IP addresses, not domain names, every Web server requires a Domain Name System (DNS) server to translate domain names into IP addresses.

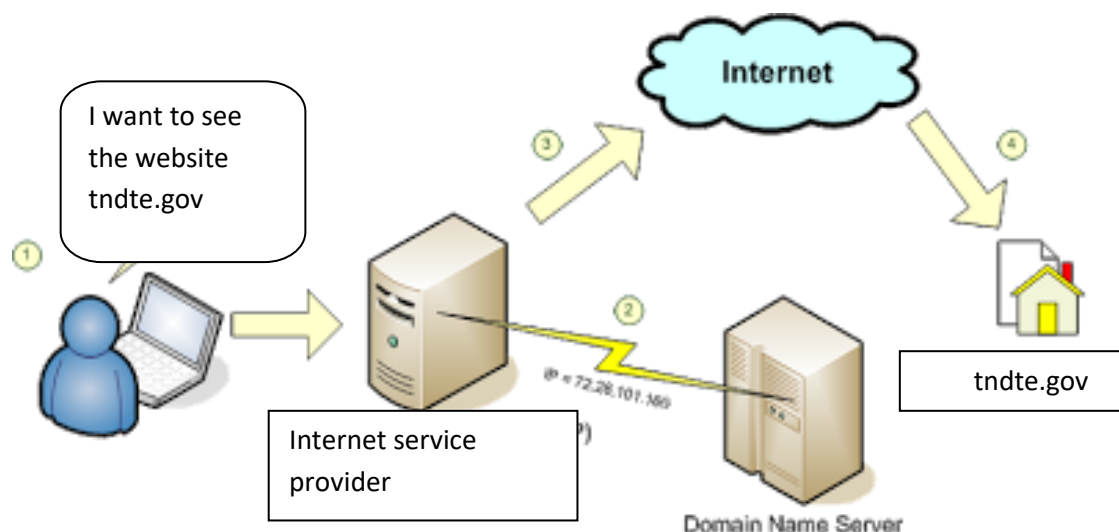


FIG 3.35

3.4.6 POP – Post Office Protocol

The Post Office Protocol (POP3) is an Internet standard protocol used by local email software clients to retrieve emails from a remote mail server over a TCP/IP connection.

Email servers hosted by Internet service providers also use POP3 to receive and hold emails intended for their subscribers.

Periodically, these subscribers will use email client software to check their mailbox on the remote server and download any emails addressed to them.

Once the email client has downloaded the emails, they are usually deleted from the server, although some email clients allow users to specify that mails be copied or saved on the server for a period of time.

Email clients generally use the well-known TCP port 110 to connect to a POP3 server.

The following picture depicts the sequence of actions be, while retrieving mail from the mail server by the user computer

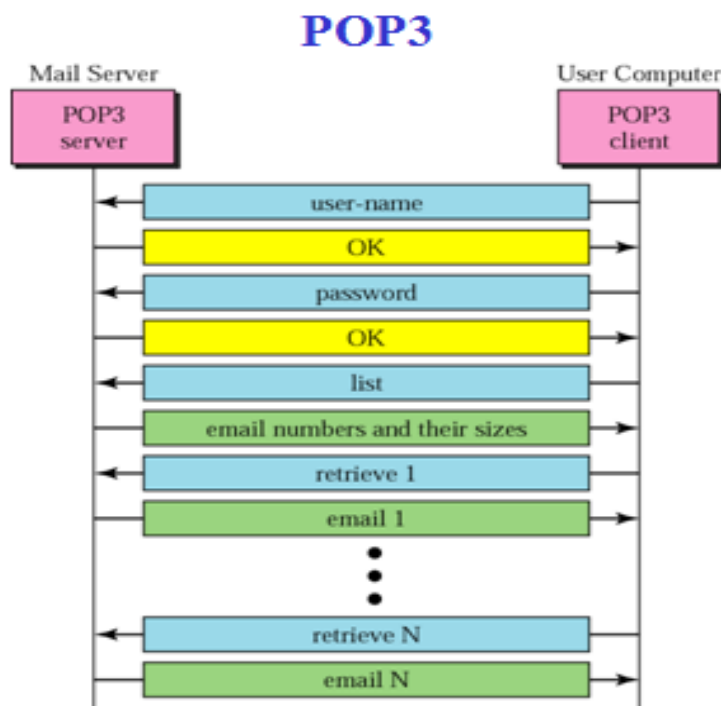


FIG 3.36

UNIT IV

NETWORKS AND SECURITY

OBJECTIVES

- To understand the basic concepts of network security and identify the attacks
- To study about cryptography and cryptography algorithms.
- To discuss about network security applications
- To know the internet security and its applications.

4.1 Introduction to Network Security

4.1.1 Definition

Network security means to protect your computer system from unwanted damages caused due to network. One of the major reason for such damages are the viruses and spywares that can wipe off all the information from your hard disk or sometimes they may be enough destructive and may cause hardware problems too. Certainly the network must be protected from such type of damaging software. The people who intentionally put such software on the network are called Hackers.

So the network needs security against attackers and hackers. Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers. Here network security not only means security in a single network rather in any network or network of networks.

4.1.2 Need for security

- To protect the secret information users on the net only. No other person should see or access it.
- To protect the information from unwanted editing, accidentally or intentionally by unauthorized users.
- To protect the information from loss and make it to be delivered to its destination properly.
- To manage for acknowledgement of message received by any node in order to protect from denial by sender in specific situations. For example let a customer orders to purchase a few shares XYZ to the broker and denies for the order after two days as the rates go down.
- To restrict a user to send some message to another user with name of a third one. For example a user X for his own interest makes a message containing some favorable instructions and sends it to user Y in such a manner that Y accepts the message as coming from Z, the manager of the organization.

- To protect the message from unwanted delay in the transmission lines/route in order to deliver it to required destination in time, in case of urgency.
- To protect the data from wandering the data packets or information packets in the network for infinitely long time and thus increasing congestion in the line in case destination machine fails to capture it because of some internal faults.

4.1.3 Principles of security

1. Encryption

In a simplest form, encryption is to convert the data in some unreadable form. This helps in protecting the privacy while sending the data from sender to receiver. On the receiver side, the data can be decrypted and can be brought back to its original form. The reverse of encryption is called as decryption. The concept of encryption and decryption requires some extra information for encrypting and decrypting the data. This information is known as key. There may be cases when same key can be used for both encryption and decryption while in certain cases, encryption and decryption may require different keys.

2. Authentication

This is another important principle of cryptography. In a layman's term, authentication ensures that the message was originated from the originator claimed in the message. Now, one may think how to make it possible? Suppose, A sends a message to B and now B wants proof that the message has been indeed sent by A. This can be made possible if A performs some action on message that B knows only A can do. Well, this forms the basic fundamental of Authentication.

3. Integrity

Now, one problem that a communication system can face is the loss of integrity of messages being sent from sender to receiver. This means that Cryptography should ensure that the messages that are received by the receiver are not altered anywhere on the communication path. This can be achieved by using the concept of cryptographic hash.

4. Non Repudiation

What happens if A sends a message to B but denies that she has actually sent the message? Cases like these may happen and cryptography should prevent the originator or sender to act this way. One popular way to achieve this is through the use of digital signatures.

4.1.4 Attacks

An attack is an act that is an intentional or unintentional attempt to cause damage to system or information

Passive attack

In this attack an adversary deploys a sniffer tool and waits for sensitive information to be captured. This information can be used for other types of attacks. It includes packet sniffer tools, traffic analysis software, filtering clear text passwords from unencrypted traffic and seeking authentication information from unprotected communication. Once an adversary found any sensitive or authentication information, he will use that without the knowledge of the user.

Active Attack

In this attack an adversary does not wait for any sensitive or authentication information. He actively tries to break or bypass the secured systems. It includes viruses, worms, trojan horses, stealing login information, inserting malicious code and penetrating network backbone. Active attacks are the most dangerous in nature. It results in disclosing sensitive information, modification of data or complete data loss.

Hijack attack

This attack usually takes place between running sessions. Hacker joins a running session and silently disconnects the other party. Then he starts communicating with active parties by using the identity of the disconnected party. The active party thinks that he is talking with the original party and may send sensitive information to the adversary.

Spoof attack

In this kind of attack an adversary changes the source address of a packet so the receiver assumes that the packet comes from someone else. This technique is typically used to bypass the firewall rules.

Criminal attacks

The attacker's main aim is to gain the maximum finance by attacking computer systems.

Legal attack

The attacked party takes the attacker to the court and takes legal action against the attacker.

4.1.5 Security Services

Network security can provide five services. Four of these services are related to the message exchanged using the network: message confidentiality, integrity, authentication, and nonrepudiation. The fifth service provides entity authentication or identification.

1. Message Confidentiality

Message confidentiality or privacy means that the sender and the receiver expect confidentiality.

The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage. When a customer communicates with her bank, she expects that the communication is totally confidential.

2. Message Integrity

Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously. As more and more monetary exchanges occur over the Internet, integrity is crucial.

3. Message Authentication

Message authentication is a service beyond message integrity. In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

4.Message Nonrepudiation

Message non repudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send. The burden of proof falls on the receiver. For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

5.Entity Authentication

In entity authentication (or user identification) the entity or user is verified prior to access to the system resources. For example, a student who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student.

4.1.6 Security Mechanisms

This section is used to implement the above security services.

1. Physical Security

Physical security refers to limiting access to key network resources by keeping the resources behind a locked door and protected from natural and human-made disasters. Physical security can protect a network from inadvertent misuses of network equipment by untrained employees and contractors. It can also protect the network from hackers, competitors, and terrorists walking in off the street and changing equipment configurations.

2. Authentication

Authentication identifies who is requesting network services. The term *authentication* usually refers to authenticating users but can also refer to authenticating devices or software processes. For example, some routing protocols support *route authentication*, whereby a router must pass some criteria before another router accepts its routing updates.

Most security policies state that to access a network and its services, a user must enter a login ID and password that are authenticated by a security server. To maximize security, one-time (dynamic) passwords can be used. With one-time password systems, a user's password always changes. This is often accomplished with a security card, also called a *Smartcard*. A *security card* is a physical device about the size of a credit card. The user types a personal identification number (PIN) into the card. The *PIN* is an initial level of security that simply gives the user permission to use the card. The card provides a one-time password that is used to access the corporate network for a limited time. The password is synchronized with a central security card server that resides on the network. Security cards are commonly used by telecommuters and mobile users. They are not usually used for LAN access.

3.Authorization

Whereas authentication controls who can access network resources, *authorization* says what they can do after they have accessed the resources. Authorization grants privileges to processes and users. Authorization lets a security administrator control parts of a network (for example, directories and files on servers).

Authorization varies from user to user, partly depending on a user's department or job function. For example, a policy might state that only Human Resources employees should see salary records for people they don't manage.

4.Accounting (Auditing)

To effectively analyze the security of a network and to respond to security incidents, procedures should be established for collecting network activity data. Collecting data is called *accounting* or *auditing*.

For networks with strict security policies, audit data should include all attempts to achieve authentication and authorization by any person. It is especially important to log "anonymous" or "guest" access to public servers. The data should also log all attempts by users to change their access rights.

The collected data should include user- and hostnames for login and logout attempts, and previous and new access rights for a change of access rights. Each entry in the audit log should be timestamped.

The audit process should not collect passwords. Collecting passwords creates a potential for a security breach if the audit records are improperly accessed. Neither correct nor incorrect passwords should be collected. An incorrect password often differs from the valid password by only a single character or transposition of characters.

4.2 CRYPTOGRAPHY

4.2.1 Definition

Cryptography, a word with Greek origins, means "secret writing. The term to refer to the science and art of transforming messages to make them secure and immune to attacks.

Two Categories

We can divide all the cryptography algorithms (ciphers) into two groups: symmetrickey (also called secret-key) cryptography algorithms and asymmetric (also called public-key) cryptography algorithms.

Symmetric-Key Cryptography

In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Asymmetric-Key Cryptography

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public. imagine A wants to send a message to B. A uses the public key to encrypt the message. When the message is received by B, the private key is used to decrypt the message.

In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption. The public key is available to the public;' the private key is available only to an individual.

Three Types of Keys

Three types of keys in cryptography: the secret key, the public key, and the private key. The first, the secret key, is the shared key used in symmetric-key cryptography. The second and the third are the public and private keys used in asymmetric-key cryptography.

Encryption can be thought of as electronic locking; decryption as electronic unlocking. The sender puts the message in a box and locks the box by using a key; the receiver unlocks the box with a key and takes out the message. The difference lies in the mechanism of the locking and unlocking and the type of keys used.

In symmetric-key cryptography, the same key locks and unlocks the box. In asymmetric-key cryptography, one key locks the box, but another key is needed to unlock it.

4.2.2 Symmetric Encryption Principles

Symmetric Encryption Principles consists of five components, namely

1. Plain text
2. Encryption algorithm
3. Secret key
4. Cipher text
5. Decryption algorithm



In cryptography the original message (before being transformed) is known as Plaintext. After the message is transformed, it is known as Ciphertext. An encryption algorithm transforms the plaintext into cipher text; a decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

4.2.3 Symmetric Block Encryption Algorithm

Symmetric-key encryption can use either stream ciphers or block ciphers. Stream ciphers encrypt the digits (typically bytes) of a message one at a time. Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits were commonly used.

Modern Round Ciphers

The ciphers of today are called **round ciphers** because they involve multiple **rounds**, where each round is a complex cipher made up of the simple ciphers. The key used in each round is a subset or variation of the general key called the round key. If the cipher has N rounds, a key generator produces N keys, K_1, K_2, \dots, K_N , where K_1 is used in round 1, K_2 in round 2, and so on.

In this section, we introduce two modern symmetric-key ciphers: DES and AES. These ciphers are referred to as block ciphers because they divide the plaintext into blocks and use the same key to encrypt and decrypt the blocks.

4.2.4 Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration –

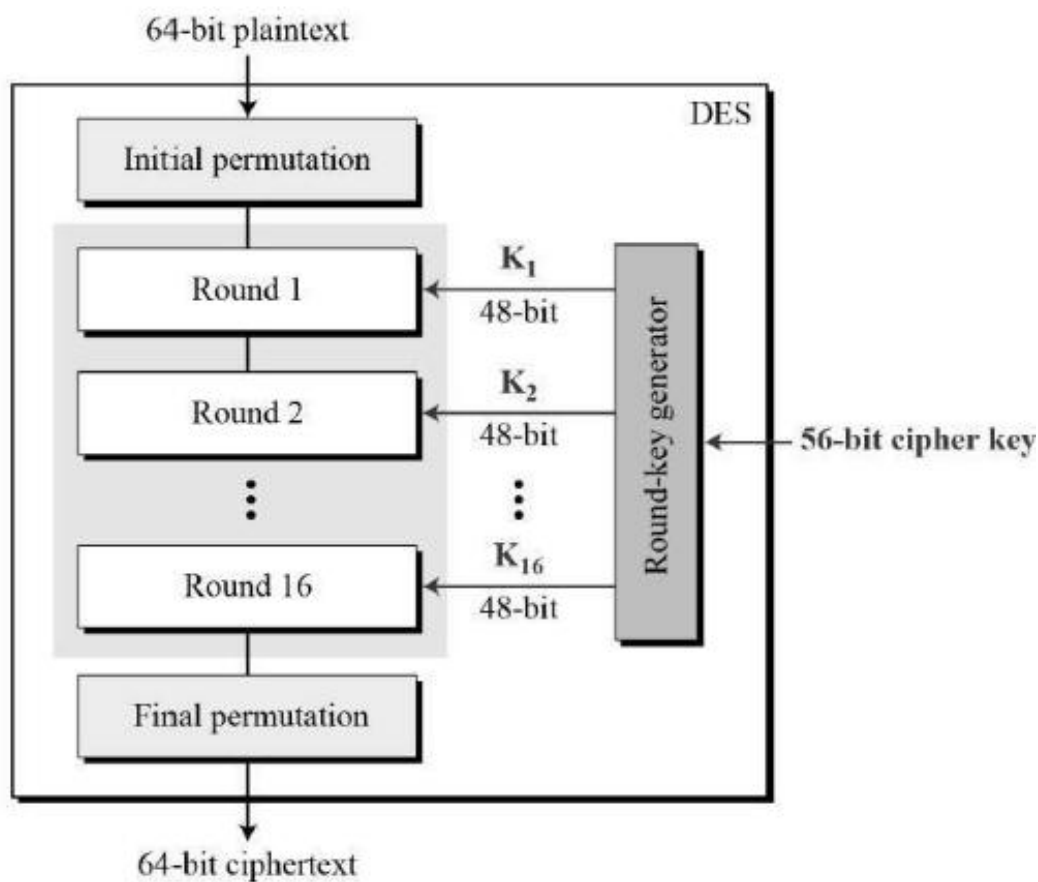


Fig 4.1 : DES Structure

Since DES is based on the Feistel Cipher, all that is required to specify DES is –

- Round function
- Key schedule
- Any additional processing – Initial and final permutation

INITIAL AND FINAL PERMUTATION

- The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows –

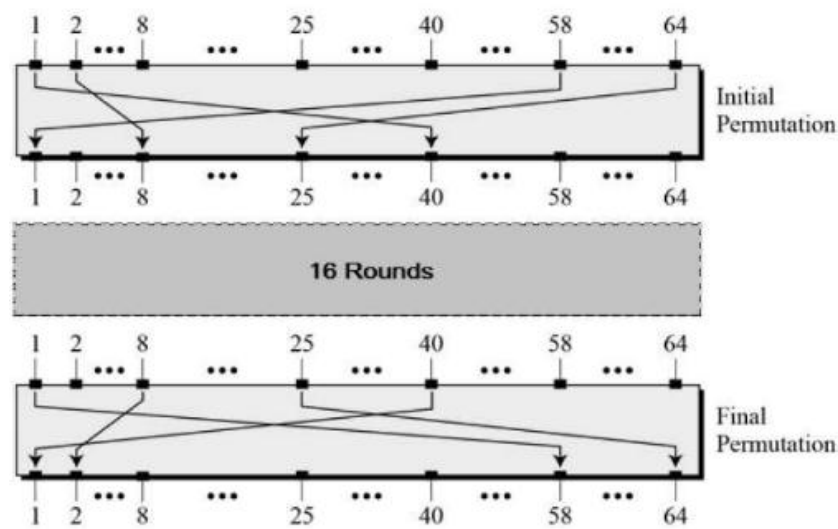


Fig 4.2 : INITIAL AND FINAL PERMUTATION

ROUND FUNCTION

The heart of this cipher is the DES function, f . The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

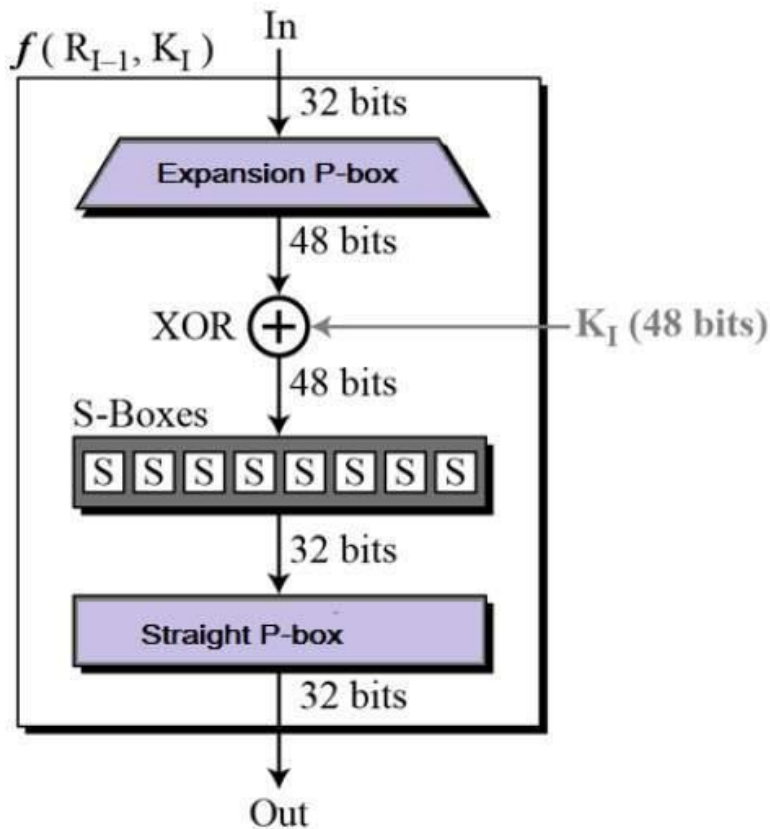


Fig 4.3 : ROUND FUNCTION

Expansion Permutation Box – Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration –

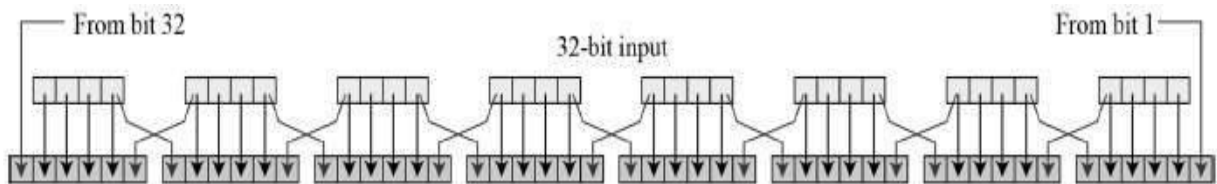


Fig 4.4 : Expansion Permutation Box

XOR (Whitener). – After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

Substitution Boxes. – The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration –

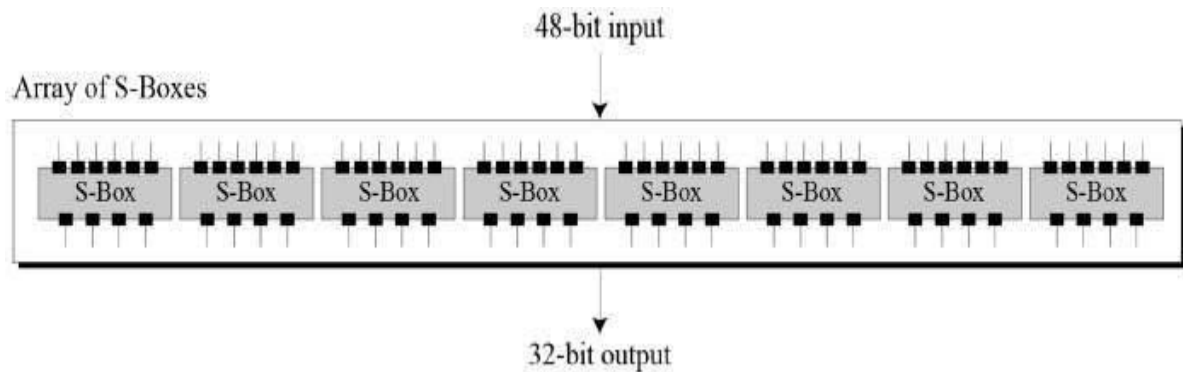
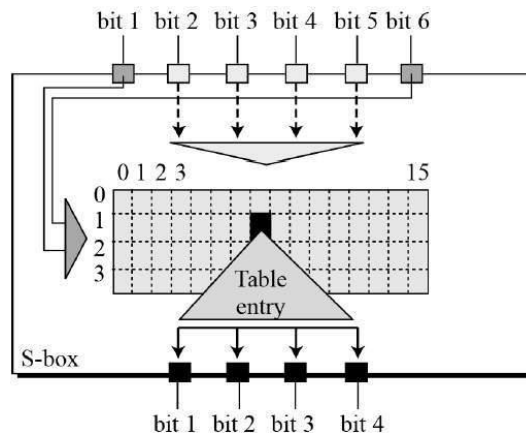


Fig 4.5 : Substitution Boxes

- The S-box rule is illustrated below –



- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- **Avalanche effect** – A small change in plaintext results in the very grate change in the ciphertext.
- **Completeness** – Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided. DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

4.2.5 Advanced Encryption Standard (AES)

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

OPERATION OF AES

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix –

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration –

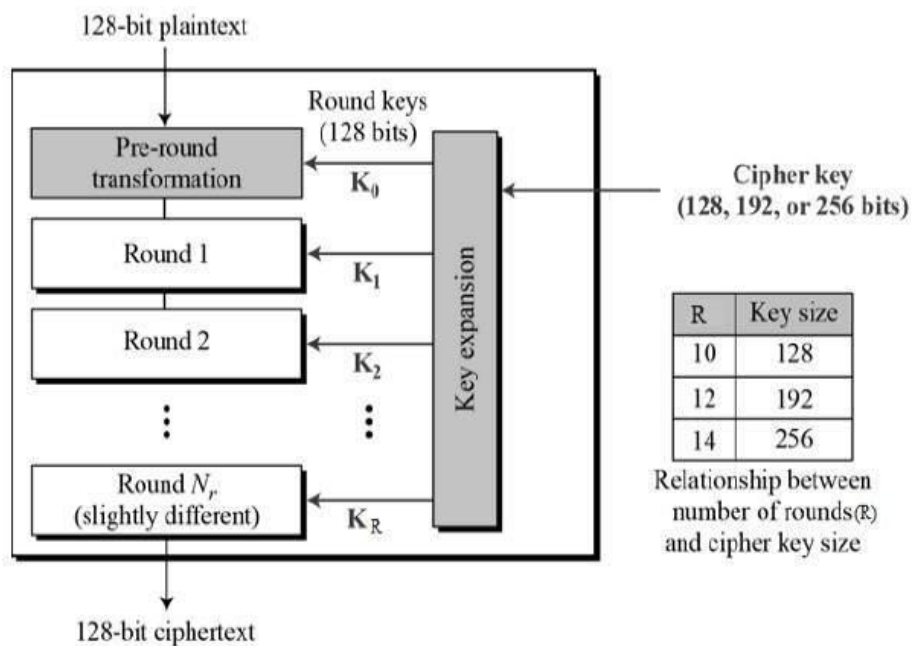


Fig 4.6 : AES Structure

ENCRYPTION PROCESS

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below –

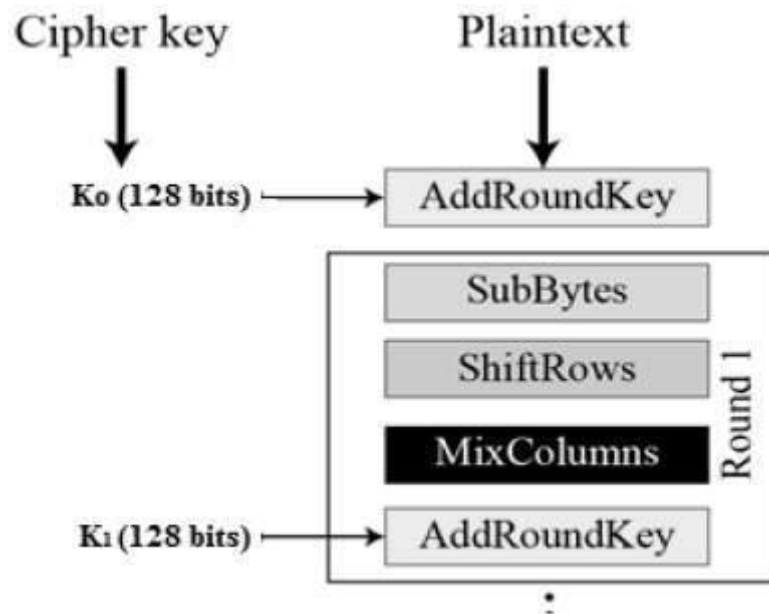


Fig 4.7 : Encryption Process

Byte Substitution (Sub Bytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shift rows

Each of the four rows of the matrix is shifted to the left. Any entries that ‘fall off’ are re-inserted on the right side of row. Shift is carried out as follows –

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Add round key

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

DECRYPTION PROCESS

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order –

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms need to be separately implemented, although they are very closely related.

AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of ‘future-proofing’ against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

4.2.6 Stream Cipher

A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream

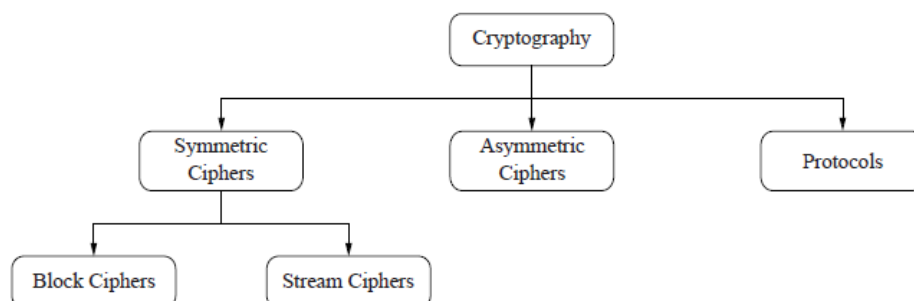


Fig 4.8 : Stream Cipher

Stream Ciphers vs. Block Ciphers

Symmetric cryptography is split into block ciphers and stream ciphers, which are easy to distinguish. Figure 2.2 depicts the operational differences between stream (Fig. 2.2a) and block (Fig. 2.2b) ciphers when we want to encrypt b bits at a time, where b is the width of the block cipher.

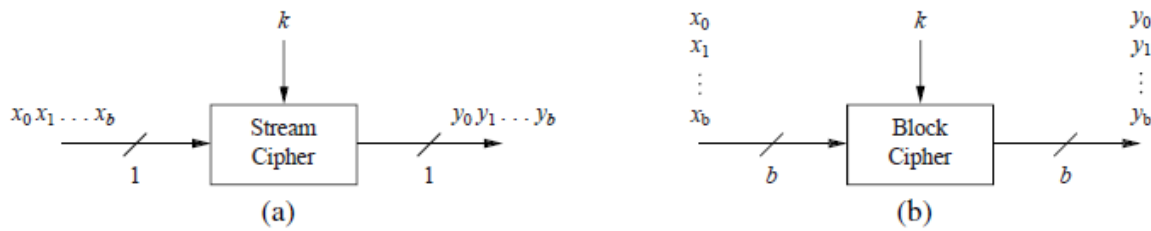


Fig 4.9 : Principles of Encrypting b bits with a stream (a) and a block (b) cipher

Stream ciphers encrypt bits individually. This is achieved by adding a bit from a *key stream* to a plaintext bit. There are synchronous stream ciphers where the key stream depends only on the key, and asynchronous ones where the key stream also depends on the cipher text. If the dotted line in Fig. 2.3 is present, the stream cipher is an asynchronous one.

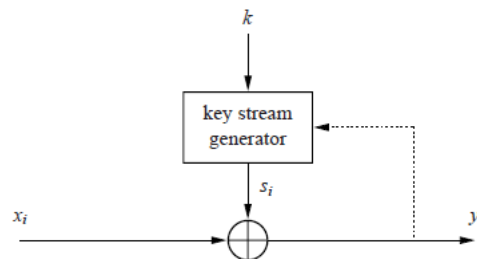


Fig 4.10 : Synchronous and asynchronous stream ciphers

Block ciphers encrypt an entire block of plaintext bits at a time with the same key. This means that the encryption of any plaintext bit in a given block depends on every other plaintext bit in the same block. In practice, the vast majority of block ciphers either have a block length of 128 bits (16 bytes) such as the advanced encryption standard (AES), or a block length of 64 bits (8 bytes) such as the data encryption standard (DES) or triple DES (3DES) algorithm.

4.2.7 RC4 Algorithm

In the RC4 encryption algorithm, the key stream is completely independent of the plaintext used. An $8 * 8$ S-Box (S_0 S_{255}), where each of the entries is a permutation of the numbers 0 to 255, and the permutation is a function of the variable length key. There are two counters i , and j , both initialized to 0 used in the algorithm.

The algorithm uses a variable length key from 1 to 256 bytes to initialize a 256-byte state table. The state table is used for subsequent generation of pseudo-random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to give the ciphertext. Each element in the state table is swapped at least once.

The key is often limited to 40 bits, because of export restrictions but it is sometimes used as a 128 bit key. It has the capability of using keys between 1 and 2048 bits. RC4 is used in many commercial software packages such as Lotus Notes and Oracle Secure SQL.

4.2.8 Digest Functions

Message digest functions also called *hash functions*, are used to produce digital summaries of information called message digests. Message digests (also called *hashes*) are commonly 128 bits to 160 bits in length and provide a digital identifier for each digital file or document. Message digest functions are mathematical functions that process information to produce a different message digest for each unique document. Identical documents have the same message digest; but if even one of the bits for the document changes, the message digest changes. Figure 4.11 shows the basic message digest process.

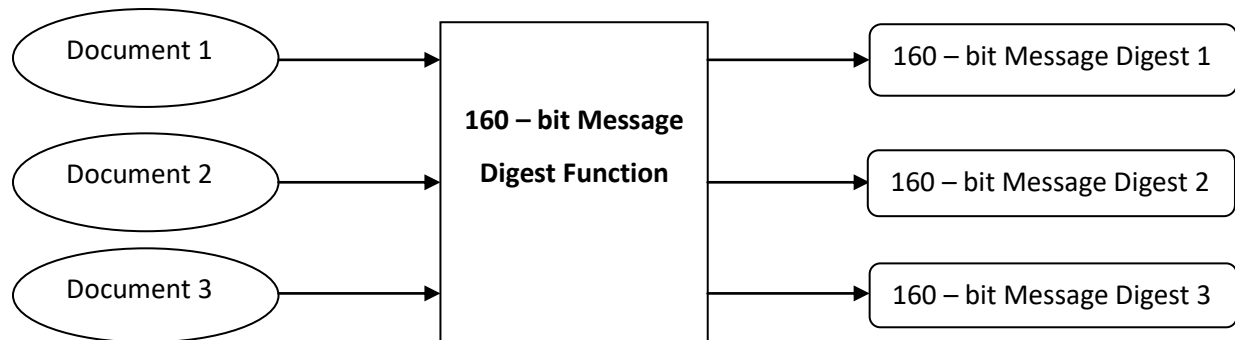


Fig 4.11 : Example of Digest Process

4.2.9 Public key Cryptography Principles

In the previous sections, we discussed symmetric-key cryptography. In this section we introduce asymmetric-key (public key cryptography). An asymmetric-key (or public-key) cipher uses two keys: one private and one public. Two algorithms: RSA and Diffie-Hellman are used in asymmetric-key.

4.2.10 The RSA Algorithm

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (e,n) , the algorithm is as follows:

1. Represent the message as an integer between 0 and $(n-1)$. Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the e th power modulo n . The result is a ciphertext message C .
3. To decrypt ciphertext message C , raise it to another power d modulo n

The encryption key (e,n) is made public. The decryption key (d,n) is kept private by the user.

How to Determine Appropriate Values for e , d , and n

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as p and q .
2. Set n equal to $p * q$.
3. Choose any large integer, d , such that $\text{GCD}(d, ((p-1) * (q-1))) = 1$
4. Find e such that $e * d = 1 \pmod{((p-1) * (q-1))}$

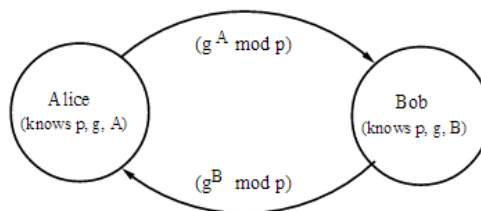
Rivest, Shamir, and Adleman provide efficient algorithms for each required operation[4].

How secure is a communication using RSA?

Cryptographic methods cannot be proven secure. Instead, the only test is to see if someone can figure out how to decipher a message without having direct knowledge of the decryption key. The RSA method's security rests on the fact that it is extremely difficult to factor very large numbers. If 100 digit numbers are used for p and q , the resulting n will be approximately 200 digits. The fastest known factoring algorithm would take far too long for an attacker to ever break the code. Other methods for determining d without factoring n are equally as difficult. Any cryptographic technique which can resist a concerted attack is regarded as secure. At this point in time, the RSA algorithm is considered secure.

4.2.11 Diffie-Hellman Algorithm

The Diffie-Hellman algorithm was developed by Whitfield Diffie and Martin Hellman in 1976. This algorithm was devised not to encrypt the data but to generate same private cryptographic key at both ends so that there is no need to transfer this key from one communication end to another. Though this algorithm is a bit slow but it is the sheer power of this algorithm that makes it so popular in encryption key generation.



Steps in the algorithm:

- Alice and Bob agree on a prime number p and a base g .
- Alice chooses a secret number a , and sends Bob $(g^a \text{ mod } p)$
- Bob chooses a secret number b , and sends Alice $(g^b \text{ mod } p)$
- Alice computes $((g^b \text{ mod } p)^a \text{ mod } p)$
- Bob computes $((g^a \text{ mod } p)^b \text{ mod } p)$.

Both Alice and Bob can use this number as their key. Notice that p and g need not be protected.

Diffie-Hellman Example:

- Alice and Bob agree on $p = 23$ and $g = 5$.
- Alice chooses $a = 6$ and sends $5^6 \text{ mod } 23 = 8$.
- Bob chooses $b = 15$ and sends $5^{15} \text{ mod } 23 = 19$.
- Alice computes $19^6 \text{ mod } 23 = 2$
- Bob computes $8^{15} \text{ mod } 23 = 2$.

Then 2 is the shared secret.

4.2.12 Digital Signatures

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

4.3 Network Security Application

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer **network** and **network-accessible** resources. ... It does as its title explains: It secures the **network**, as well as protecting and overseeing operations being done.

The following are some of the network security applications

1. Authentication applications (Kerberos)
2. Web security standards (SSL / TLS)
3. Email security
4. IP security

Authentication applications

4.3.1 KERBEROS

Kerberos is a key distribution and user authentication service developed at MIT. The problem that Kerberos addresses is this: Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment, a workstation cannot be trusted to identify its users correctly to network services. In particular, the following three threats exist:

1. A user may gain access to a particular workstation and pretend to be another user operating from that workstation.
2. A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation.
3. A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.

In any of these cases, an unauthorized user may be able to gain access to services and data that he or she is not authorized to access. Rather than building elaborate authentication protocols at each server, Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. Kerberos relies exclusively on symmetric encryption, making no use of public-key encryption. Two versions of Kerberos are in use. Version 4 implementations still exist, although this version is being phased out. Version 5 corrects some of the security deficiencies of version 4 and has been issued as a proposed Internet Standard (RFC 4120). Version 4 enables us to see the essence of the Kerberos strategy without considering some of the details required to handle subtle security threats.

4.3.2 Overview of Kerberos

Kerberos is a trusted third-party authentication protocol designed for TCP/IP networks (developed at MIT). A Kerberos service on the network acts as a trusted arbitrator. Kerberos allows clients to access different entities (clients/servers) on the network.

The Kerberos Model

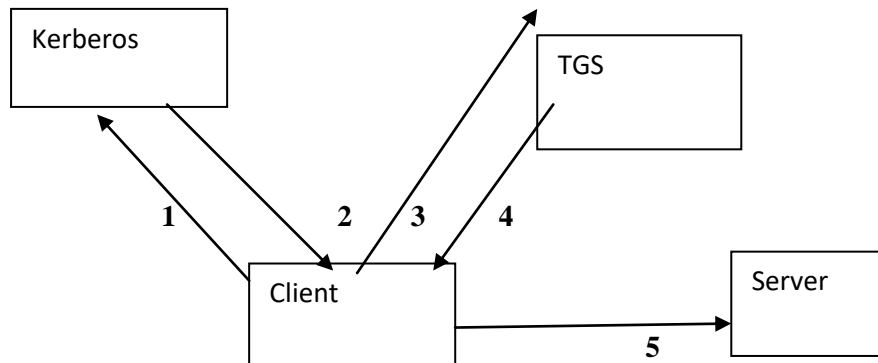
Kerberos keeps a database of clients and their secret keys. Services requiring authentication, as well as their clients, register their secret keys with Kerberos. Kerberos creates a shared session key and gives it to client and server (or two clients) to encrypt messages. Kerberos uses DES for encryption. Kerberos Version 4 provided a weak nonstandard mode for authentication. Kerberos Version 5 uses CBC mode.

How Kerberos Works

1. A client requests a ticket for a TGS (Ticket-Granting Service) from Kerberos.
2. Kerberos sends the ticket to the client, encrypted in client's secret key.
3. To use a particular service, client requests a ticket from TGS.
4. TGS issues and sends a ticket to the client, encrypted with server's secret key. The ticket is used by server to ensure that it is the same client to whom the ticket was issued - Client can use the ticket multiple times to access the server until the ticket expires.
5. Client presents ticket to server with an authenticator (the authenticator contains client's name and a timestamp, encrypted with the shared session key). Unlike a ticket, an

authenticator can only be used once - The client can generate authenticators as needed using the shared secret key .

6. If client credentials (ticket + authenticator) are correct, server provides access to service.



4.3.3 Motivation

If a set of users is provided with dedicated personal computers that have no network connections , then a user's resources and files can be protected by physically securing each personal computer .When these users instead are served by a centralized time-sharing system ,the time-sharing operating system must provide the security.The operating system can enforce access control policies based on user identity and use the logon procedure to identify users.

Today , neither of these scenarios is typical. More common is a distributed architecture consisting of dedicated user workstations (clients) and distributed or centralized servers.In this environment , three approaches to security can be envisioned.

1. Rely on each individual client workstation to assure the identity of its user or users and rely on each server to enforce a security policy based on user identification (ID).
2. Require that client systems authenticate themselves to servers , but trust the client system concerning the identity of its user.
3. Require the user to prove identity for each service invoked. Also require that servers prove their identity to clients.

In a small , closed environment , in which all systems are owned and operated by a single organization , the first or perhaps the second strategy may suffice. But in a more open environment , in which network connections to other machines are supported , the third approach is needed to protect user information and resources housed at the server. This third approach is supported by Kerberos. Kerberos assumes a distributed client/server architecture and employs one or more Kerberos servers to provide an authentication service. The first published report on Kerberos listed the following requirements for Kerberos.

- a. Secure
- b. Reliable

- c. Transparent
- d. Scalable

4.3.4 Encryption techniques

A SIMPLE AUTHENTICATION DIALOGUE

In an unprotected network environment, any client can apply to any server for service. The obvious security risk is that of impersonation. An opponent can pretend to be another client and obtain unauthorized privileges on server machines. To counter this threat, servers must be able to confirm the identities of clients who request service. Each server can be required to undertake this task for each client/server interaction, but in an open environment, this places a substantial burden on each server. An alternative is to use an authentication server (AS) that knows the passwords of all users and stores these in a centralized database. In addition, the AS shares a unique secret key with each server. These keys have been distributed physically or in some other secure manner. Consider the following hypothetical dialogue:

- (1) C \rightarrow AS: IDC || PC || IDV
- (2) AS \rightarrow C: Ticket
- (3) C \rightarrow V: IDC || Ticket

$$\text{Ticket} = E(K_v, [\text{IDC} || \text{ADC} || \text{IDV}])$$

Where

C	Client
AS	Authentication server
V	Server
IDC	Identifier of user on C
IDV	Identifier of V
PC	Password of user on C
ADC	Network address of c
Kv	Secret encryption key shared by AS and V

In this scenario, the user logs on to a workstation and requests access to server V. The client module C in the user's workstation requests the user's password and then sends a message to the AS that includes the user's ID, the server's ID, and the user's password. The AS checks its database to see if the user has supplied the proper password for this user ID and whether this user is permitted access to server V. If both tests are passed, the AS accepts the user as authentic and must now convince the server that this user is authentic. To do so, the AS creates a ticket that contains the user's ID and network address and the server's ID. This ticket is encrypted using the secret key shared by the AS and this server. This ticket is then sent back to C.

Because the ticket is encrypted, it cannot be altered by C or by an opponent. With this ticket, C can now apply to V for service. C sends a message to V containing C's ID and the ticket. V decrypts the ticket and verifies that the user ID in the ticket is the same as the unencrypted user ID in the message. If these two match, the server considers the user authenticated and grants the requested service.

Each of the ingredients of message (3) is significant. The ticket is encrypted to prevent alteration or forgery. The server's ID (IDV) is included in the ticket so that the server can verify that it has decrypted the ticket properly. IDC is included in the ticket to indicate that this ticket has been issued on behalf of C. Finally, ADC serves to counter the following threat. An opponent could capture the ticket transmitted in message (2), then use the name IDC, and transmit a message of form (3) from another workstation. The server would receive a valid ticket that matches the user ID and grant access to the user on that other workstation. To prevent this attack, the AS includes in the ticket the network address from which the original request came. Now the ticket is valid only if it is transmitted from the same workstation that initially requested the ticket.

Security of Kerberos

- a. It may be possible to cache and replay old authenticators. Although timestamps are supposed to prevent this, replays can be done during the lifetime of the ticket
- b. Authenticators assume all clocks in the network are synchronized. If a host is fooled about the correct time, an old authenticator can be replayed.
- c. Password-guessing attacks: an intruder can collect tickets and then try to decrypt them. The average user doesn't usually choose good passwords.
- d. Malicious software: Kerberos rely on that its software is trustworthy. It is possible to replace all client Kerberos software with a version that records passwords.
- e. New enhancements to Kerberos include an implementation of public-key cryptography and a smart-card interface for key management.

4.4 Internet Security

Email security

Email security refers to the collective measures used to *secure* the access and content of an *email* account or service. It allows an individual or organization to protect the overall access to one or more *email* addresses/accounts. Email security is a priority for all businesses, with the growing threat of hackers, viruses spam, phishing and identity theft, as well as the need to secure business information.

In virtually all distributed environments, electronic mail is the most heavily used network-based application. Users expect to be able to, and do, send e-mail to others who are connected directly or indirectly to the Internet, regardless of host operating system or communications suite. With the explosively growing reliance on e-mail, there grows a demand for authentication and confidentiality services. Two schemes stand out as approaches that enjoy widespread use: Pretty Good Privacy (PGP) and S/MIME.

4.4.1 PGP (Pretty Good Privacy)

PGP is a remarkable phenomenon. Largely the effort of a single person, Phil Zimmermann, PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

PGP has grown explosively and is now widely used. A number of reasons can be cited for this growth.

1.It is available free worldwide in versions that run on a variety of platforms, including Windows, UNIX, Macintosh, and many more. In addition, the commercial version satisfies users who want a product that comes with vendor support.

2.It is based on algorithms that have survived extensive public review and are considered extremely secure. Specifically, the package includes RSA, DSS, and Diffie-Hellman for public-key encryption; CAST-128, IDEA, and 3DES for symmetric encryption; and SHA-1 for hash coding.

3.It has a wide range of applicability, from corporations that wish to select and enforce a standardized scheme for encrypting files and messages to individuals who wish to communicate securely with others worldwide over the Internet and other networks.

4.It was not developed by, nor is it controlled by, any governmental or standards organization. For those with an instinctive distrust of “the establishment,” this makes PGP attractive.

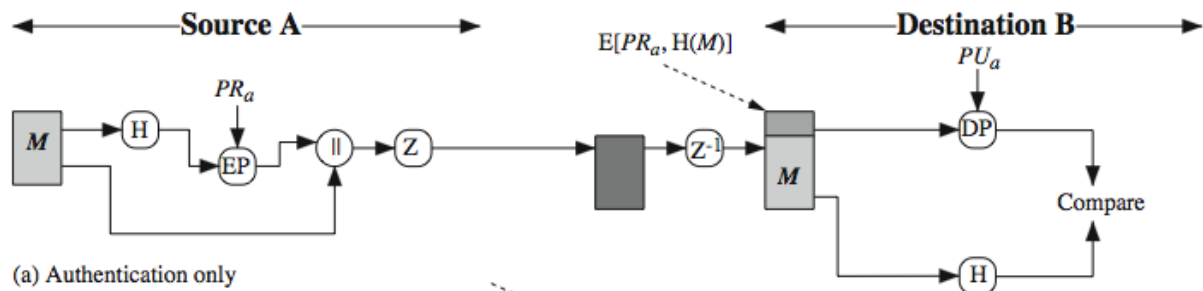
5.PGP is now on an Internet standards track. Nevertheless, PGP still has an aura of an antiestablishment endeavor.

Operational Description

The actual operation of PGP, consists of four services: authentication, confidentiality, compression, and e-mail compatibility.

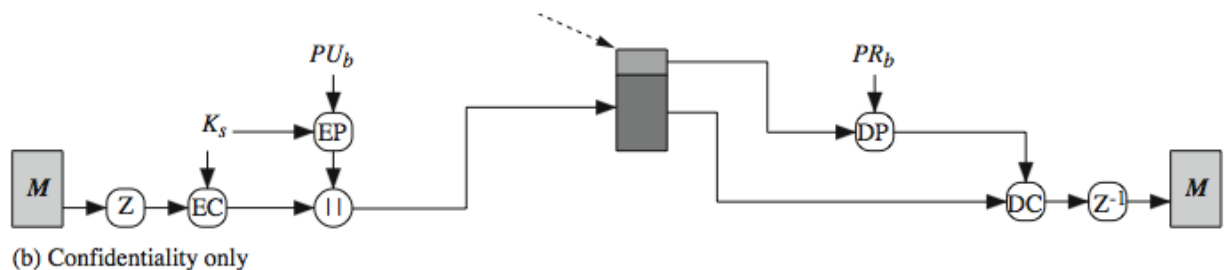
Authentication

1. Sender creates message
2. Make SHA-1160-bit hash of message
3. Attached RSA signed hash to message
4. Receiver decrypts & recovers hash code
5. Receiver verifies received message hash



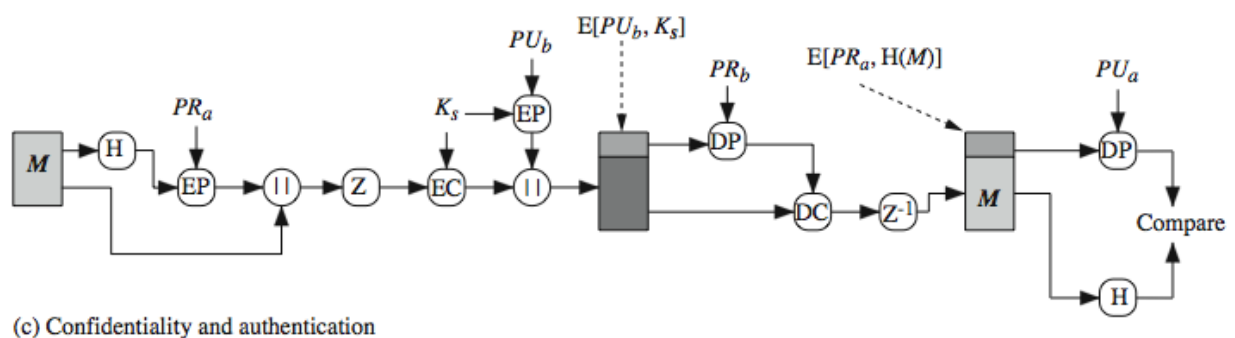
Confidentiality

1. Sender forms 128-bit random session key
2. Encrypts message with session key
3. Attaches session key encrypted with RSA
4. Receiver decrypts & recovers session key
5. Session key is used to decrypt message



Confidentiality & Authentication

1. can use both services on same message
 - Create signature & attach to message
 - Encrypt both message & signature
 - Attach RSA/ElGamal encrypted session key



Compression

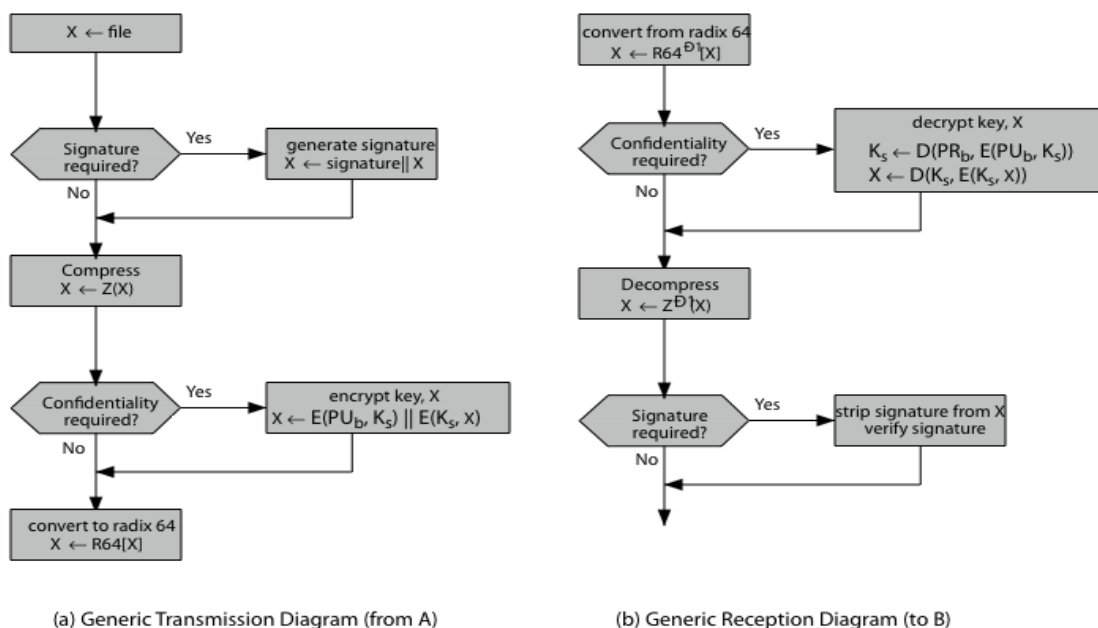
1. By default PGP compresses message after signing but before encrypting
 - so can store uncompressed message & signature for later verification and because compression is non deterministic
2. Uses ZIP compression algorithm

Email Compatibility

1. When using PGP will have binary data to send (encrypted message etc)
2. However email was designed only for text
3. Hence PGP must encode raw binary data into printable ASCII characters
4. Uses radix-64 algorithm
 - maps 3 bytes to 4 printable chars
 - also appends a CRC
5. PGP also segments messages if too big

PGP Operation – Summary

PGP makes use of four types of keys: **one-time session symmetric keys, public keys, private keys, and passphrase-based symmetric keys**. Each session key is associated with a single message and is used only for the purpose of encrypting and decrypting that message, using a symmetric encryption algorithm, such as CAST-128 and IDEA with 128-bit keys; or 3DES with a 168-bit key. Random numbers are generated using the ANSI X12.17 generator, with inputs based on keystroke input from the user, where both the keystroke timing and the actual keys struck are used to generate a randomized stream of numbers.



4.4.2 S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, which in turn provided support for varying content types and multi-part messages over the text only support in the original Internet RFC822 (now RFC5322) email standard. See text for discussion of these extensions. MIME is specified in RFCs 2045 through 2049. MIME allows encoding of binary data to textual form

for transport over traditional RFC822 email systems. S/MIME support is now included in many modern mail agents.

S/MIME Functionality

In term of general functionality , S/MIME is very similar to PGP. Both offer the ability to sign and/or encrypt messages. S/MIME provides the following functions.

- Enveloped data – (encrypted content and associated keys)
- Signed data – (encoded message + signed digest)
- Clear signed data – (cleartext message + encoded signed digest)
- Signed and enveloped data – (nesting of signed and encrypted entities)

S/MIME incorporates three public-key algorithms.

1. Digital signatures: DSS & RSA
2. Hash functions: SHA-1 & MD5
3. Session key encryption: ElGamal & RSA
4. Message encryption: AES, Triple-DES, RC2/40 and others
5. MAC: HMAC with SHA-1

S/MIME secures a MIME entity with a signature, encryption, or both. A MIME entity may be an entire message or one or more of the subparts of the message. The MIME entity plus some security related data, such as algorithm identifiers and certificates, are processed by S/MIME to produce a PKCS, which refers to a set of public-key cryptography specifications issued by RSA Laboratories. A PKCS object is then treated as message content and wrapped in MIME. A range of S/MIME content-types are used (multipart ,application etc).

S/MIME uses public-key certificates that conform to version 3 of X.509. The key-management scheme used by S/MIME is in some ways a hybrid between a strict X.509 certification hierarchy and PGP's web of trust. S/MIME managers and/or users must configure each client with a list of trusted keys and with certificate revocation lists, needed to verify incoming signatures and to encrypt outgoing messages. But certificates are signed by trusted certification authorities.

Three enhanced security services have been proposed in an Internet draft, and may change or be extended. The three services are:

- **Signed receipts:** may be requested in a SignedData object to provide proof of delivery to the originator of a message and allows the originator to demonstrate to a third party that the recipient received the message.
- **Security labels:** may be included in the authenticated attributes of a SignedData object, and is a set of security information regarding the sensitivity of the content that is protected by S/MIME encapsulation. They may be used for access control, indicating which users are permitted access to an object

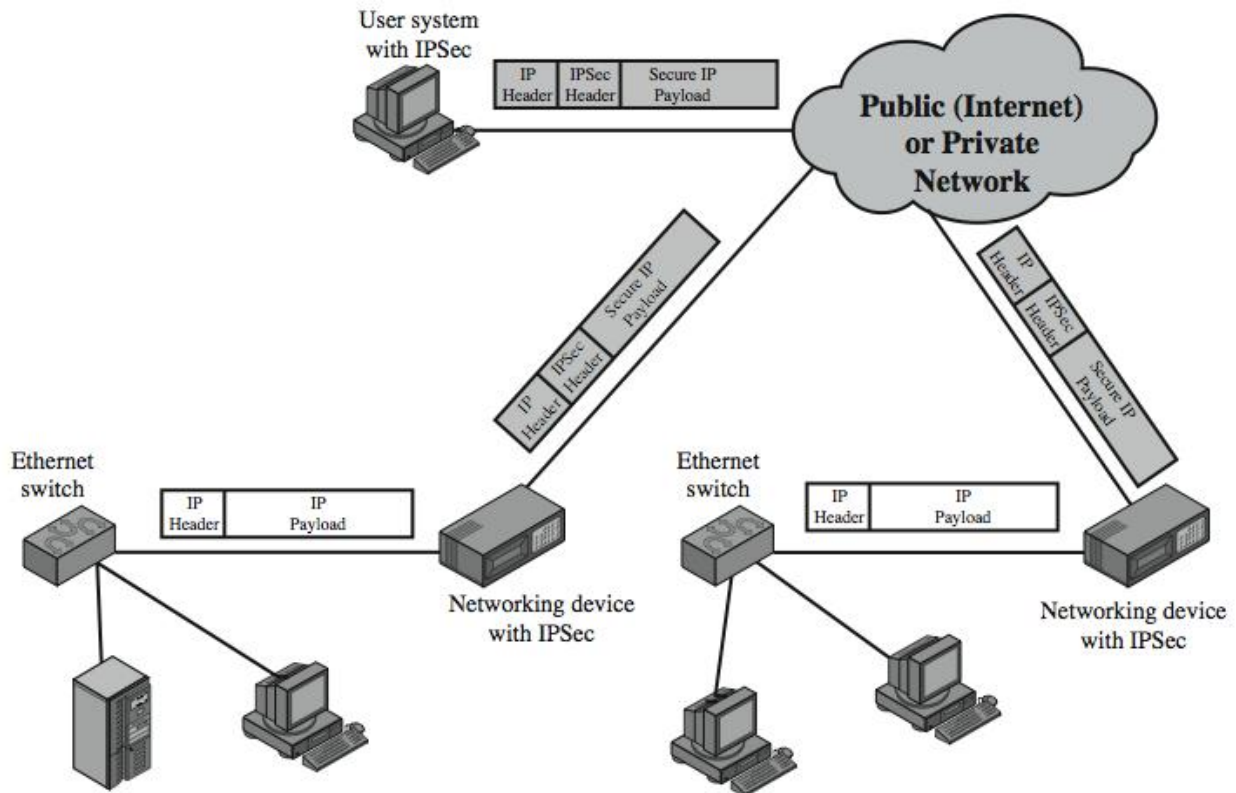
- **Secure mailing lists:** When a user sends a message to multiple recipients, a certain amount of per-recipient processing is required, including the use of each recipient's public key. The user can be relieved of this work by employing the services of an S/MIME Mail List Agent (MLA). An MLA can take a single incoming message, perform recipient-specific encryption for each recipient, and forward the message. The originator of a message need only send the message to the MLA, with encryption performed using the MLA's public key.

4.4.3 IP Security

The Internet community has developed application-specific security mechanisms in a number of application areas, including electronic mail (S/MIME, PGP), client/server (Kerberos), Web access (Secure Sockets Layer), and others. However users have some security concerns that cut across protocol layers. By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security-ignorant applications.

IP-level security encompasses three functional areas: authentication, confidentiality, and key management. The authentication mechanism assures that a received packet was transmitted by the party identified as the source in the packet header, and that the packet has not been altered in transit. The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties. The key management facility is concerned with the secure exchange of keys. IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.

In 1994, the Internet Architecture Board (IAB) issued a report titled "Security in the Internet Architecture" (RFC 1636). The report stated the general consensus that the Internet needs more and better security and identified key areas for security mechanisms. To provide security, the IAB included authentication and encryption as necessary security features in the next-generation IP, which has been issued as IPv6. Fortunately, these security capabilities were designed to be usable both with the current IPv4 and the future IPv6.



The above figure illustrates a typical IP Security scenario. An organization maintains LANs at dispersed locations. Nonsecure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPSec protocols are used. These protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world. The IPSec networking device will typically encrypt and compress all traffic going into the WAN, and decrypt and decompress traffic coming from the WAN; these operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial into the WAN. Such user workstations must implement the IPSec protocols to provide security.

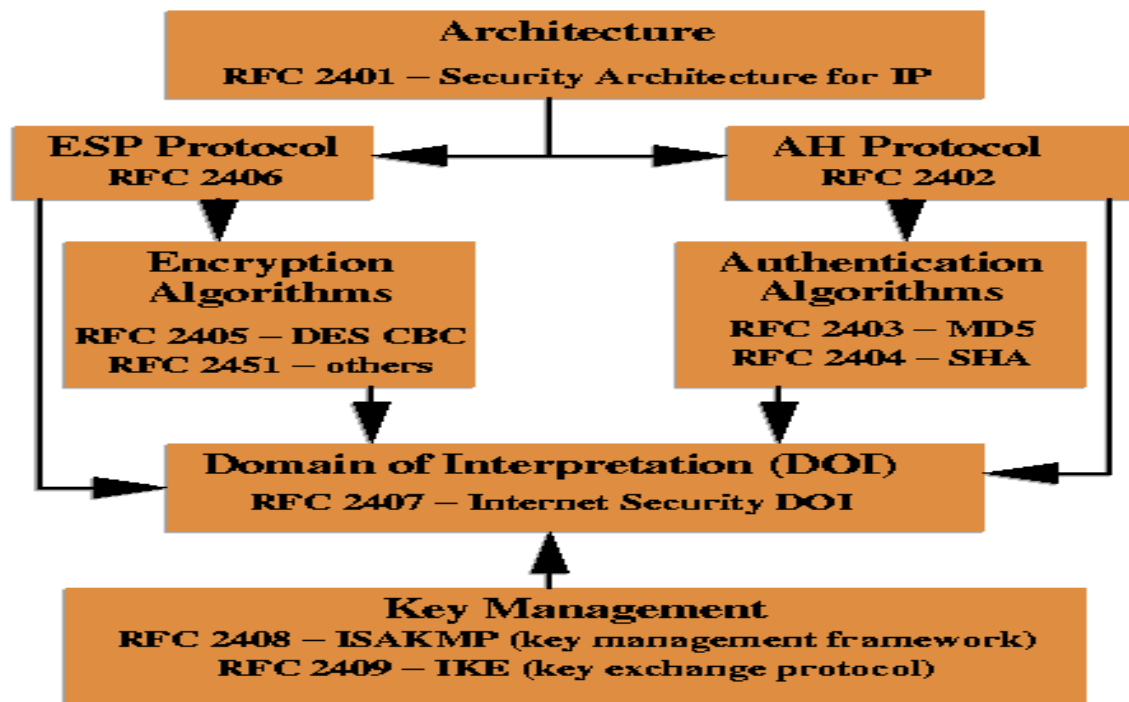
Some of the **benefits of IPSec** include:

- When implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.
- in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
- is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router. Even if IPSec is implemented in end systems, upper-layer software, including applications, is not affected.

- can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

It also plays a vital role in the routing architecture required for internetworking.

IP Security Architecture



The IPsec specification has become quite complex key management. The totality of the IPsec specification is scattered across dozens of RFCs and draft IETF documents, making this the most complex and difficult to grasp of all IETF specifications. The best way to keep track of and get a handle on this body of work is to consult the latest version of the IPsec document roadmap. The documents can be categorized into the following groups:

- **Architecture:** Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology.
- **Authentication Header (AH):** AH is an extension header for message authentication, now deprecated.
- **Encapsulating Security Payload (ESP):** ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication.

- **Internet Key Exchange (IKE):** a collection of documents describing the key management schemes for use with IPsec.
- **Cryptographic algorithms:** a large set of documents that define and describe cryptographic algorithms for encryption, message authentication, pseudorandom functions (PRFs), and cryptographic key exchange.
- **Other:** There are a variety of other IPsec-related RFCs, including those dealing with security policy and management information base (MIB) content.

Both AH and ESP support **two modes of use**:

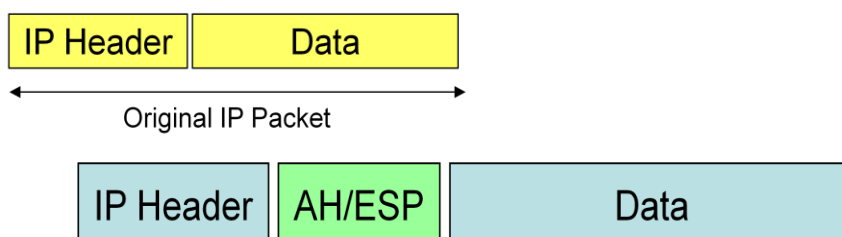
- Transport mode
- Tunnel mode.

Transport mode provides protection primarily for upper-layer protocols. Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP. Typically, transport mode is used for end-to-end communication between two hosts (e.g., a client and a server, or two workstations). When a host runs AH or ESP over IPv4, the payload is the data that normally follow the IP header. For IPv6, the payload is the data that normally follow both the IP header and any IPv6 extensions headers that are present. Transport mode operation provides confidentiality for any application that uses it, thus avoiding the need to implement confidentiality in every individual application.



Transport mode

Tunnel mode ESP is used to encrypt an entire IP packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new "outer" IP packet with a new outer IP header. The entire original, or inner, packet travels through a "tunnel" from one point of an IP network to another; no routers along the way are able to examine the inner IP header. Tunnel mode is useful in a configuration that includes a firewall or other sort of security gateway that protects a trusted network from external networks. In this latter case, encryption occurs only between an external host and the security gateway or between two security gateways. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec.



Tunnel mode

Services provided by IPSec

- a. Access control
- b. Connectionless integrity
- c. Data origin authentication
- d. Rejection of replayed packets
- e. Confidentiality (encryption)
- f. Limited traffic flow confidentiality

IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. Two protocols are used to provide security: an authentication protocol designated by the header of the protocol, Authentication Header (AH); and a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP).

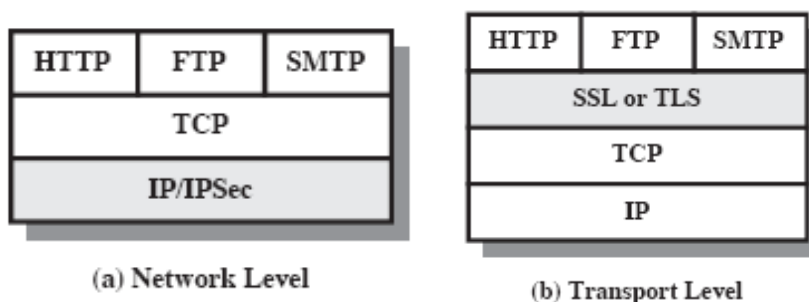
Web Security

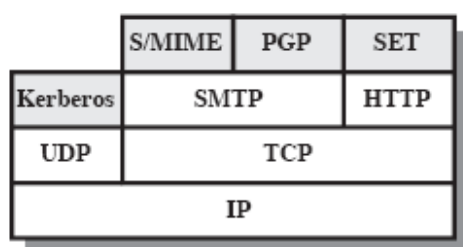
The World Wide Web is widely used by businesses, government agencies, and many individuals. But the Internet and the Web are extremely vulnerable to compromises of various sorts, with a range of threats as shown. These can be described as passive attacks including eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted, and active attacks including impersonating another user, altering messages in transit between client and server, and altering information on a Web site. The web needs added security mechanisms to address these threats.

The threats faced by web are

1. Integrity
2. Confidentiality
3. Denial of service
4. Authentication

Relative location of security facilities in the TCP/IP Protocol stack

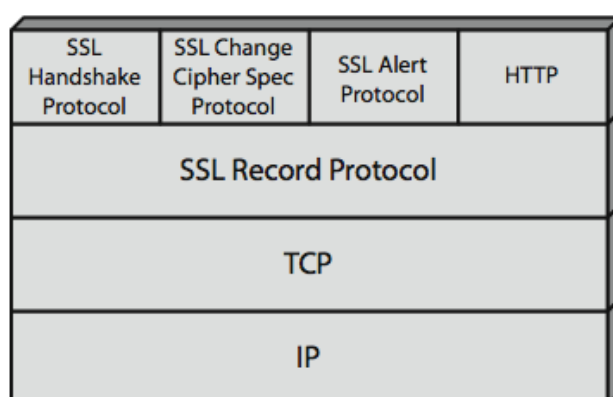




(c) Application Level

4.4.4 SSL (Secured socket layer)

SSL probably most widely used Web security mechanism. Its implemented at the Transport layer. SSL is designed to make use of TCP to provide a reliable end-to-end secure service. Netscape originated SSL. Version 3 of the protocol was designed with public review and input from industry and was published as an Internet draft document. Subsequently, the IETF TLS working group was formed to develop a common standard. SSL is not a single protocol but rather two layers of protocols.



The above figure shows the SSL Protocol stack. The SSL Record Protocol provides basic security services to various higher-layer protocols. In particular, the Hypertext Transfer Protocol (HTTP), which provides the transfer service for Web client/server interaction, can operate on top of SSL. Three higher-layer protocols are also defined as part of SSL: the Handshake Protocol, Change Cipher Spec Protocol, and Alert Protocol. These SSL-specific protocols are used in the management of SSL exchanges.

SSL Architecture

Two important SSL concepts are the SSL connection and the SSL session.

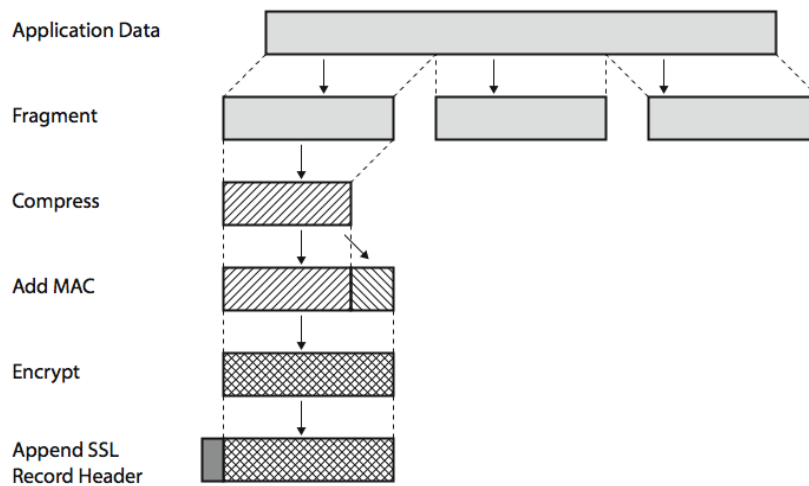
- **Connection:** A connection is a network transport that provides a suitable type of service, such connections are transient, peer-to-peer relationships, associated with one session.
- **Session:** An SSL session is an association between a client and a server, created by the Handshake Protocol. Sessions define a set of cryptographic security parameters,

which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

SSL Record Protocol defines two services for SSL connections.

- **Message Integrity:** The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC), which is similar to HMAC.
- **Confidentiality:** The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads. The message is compressed before being concatenated with the MAC and encrypted, with a range of ciphers being supported. .

SSL Record protocol operation



The above figure shows the overall operation of the SSL Record Protocol. The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment. Received data are decrypted, verified, decompressed, and reassembled and then delivered to higher-layer applications.

SSL Change Cipher Spec Protocol

The Change Cipher Spec Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol, and it is the simplest, consisting of a single message. Its purpose is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.

SSL Alert Protocol

The Alert Protocol is used to convey SSL-related alerts to the peer entity. As with other applications that use SSL, alert messages are compressed and encrypted, as specified by the current state. Each message in this protocol consists of two bytes, the first takes the value warning(1) or fatal(2) to convey the severity of the message. The second byte contains a code that indicates the specific alert. The first group shown are the fatal alerts, the others are warnings.

SSL handshake Protocol

The most complex part of SSL is the Handshake Protocol. This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record. The Handshake Protocol is used before any application data is transmitted. The Handshake Protocol consists of a series of messages exchanged by client and server, which can be viewed in 4 phases:

- Phase 1. Establish Security Capabilities - this phase is used by the client to initiate a logical connection and to establish the security capabilities that will be associated with it
- Phase 2. Server Authentication and Key Exchange - the server begins this phase by sending its certificate if it needs to be authenticated.
- Phase 3. Client Authentication and Key Exchange - the client should verify that the server provided a valid certificate if required and check that the server_hello parameters are acceptable
- Phase 4. Finish - this phase completes the setting up of a secure connection. The client sends a change_cipher_spec message and copies the pending CipherSpec into the current CipherSpec .

4.4.5 TLS (Transport layer Security)

TLS is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL. TLS is defined as a Proposed Internet Standard in RFC 2246. RFC 2246 is very similar to SSLv3 but with a number of minor differences as follows

- In record format version number
- Uses HMAC for MAC
- A pseudo-random function expands secrets
- Has additional alert codes
- Some changes in supported ciphers
- Changes in certificate types & negotiations
- Changes in crypto computations & padding

TLS was developed by IETF to replace SSL version 3.

- Based on SSL version 3, with some changes:
 - Replaced FORTEZZA key exchange option with DSS.

- Include the hash method HMAC used by IPSec for authentication in IP headers.
- More differentiation between sub-protocols.
- TLS has mechanisms for backwards compatibility with SSL.

TLS has about 30 possible cipher 'suites', combinations of key exchange, encryption method, and hashing method.

- Key exchange includes: RSA, DSS, Kerberos
- Encryption includes: IDEA(CBC), RC2, RC4, DES, 3DES, and AES
- Hashing: SHA and MD5

4.4.6 SET (Secure Electronic Transaction)

SET is an open encryption and security specification designed to protect credit card transactions on the Internet. SETv1 emerged from a call for security standards by MasterCard and Visa in 1996. Beginning in 1996, there have been numerous tests of the concept, and by 1998 the first wave of SET-compliant products was available. SET is not itself a payment system, rather it is a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network, such as the Internet, in a secure fashion, by providing:

- a secure communications channel among all parties involved in a transaction
- trust through the use of X.509v3 digital certificates
- privacy because the information is only available to parties in a transaction when and where necessary.

SET Requirements

- Provide confidentiality of payment and ordering information.
- Ensure the integrity of all transmitted data.
- Provide authentication that a cardholder is a legitimate user of a credit card account.
- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institute.
- Ensure the use of best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
- Create a protocol that neither depends on transport security mechanisms nor prevents their use.
- Facilitate and encourage interoperability among software and network providers.

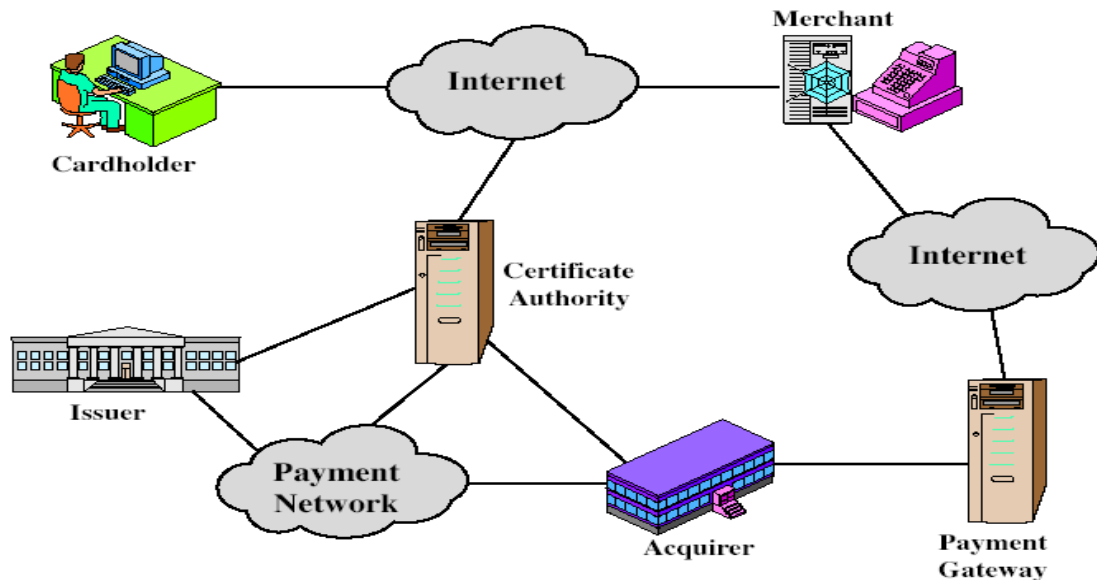
Key features of SET

SET incorporates the following features.

- Confidentiality of information

- b. Integrity of data
- c. Cardholder account authentication
- d. Merchant authentication

SET Participants



The above figure indicates the participants in the SET system

- **Cardholder:** purchasers interact with merchants from personal computers over the Internet
- **Merchant:** a person or organization that has goods or services to sell to the cardholder
- **Issuer:** a financial institution, such as a bank, that provides the cardholder with the payment card.
- **Acquirer:** a financial institution that establishes an account with a merchant and processes payment card authorizations and payments
- **Payment gateway:** a function operated by the acquirer or a designated third party that processes merchant payment messages
- **Certification authority (CA):** an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways

SET Transactions

1. Customer opens account
2. Customer receives a certificate
3. Merchants have their own certificates
4. Customer places an order
5. Merchant is verified

6. Order and payment are sent
7. Merchant requests payment authorization
8. Merchant confirms order
9. Merchant provides goods or service
10. Merchant requests payment

Dual Signature

The purpose of the SET dual signature is to link two messages that are intended for two different recipients, the order information (OI) for the merchant and the payment information (PI) for the bank. The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order, however the two items must be linked in a way that can be used to resolve disputes if necessary. The customer takes the hash (using SHA-1) of the PI and the hash of the OI, concatenates them, and hashes the result. Finally, the customer encrypts the final hash with his or her private signature key, creating the dual signature. This can be summarized as: $DS = E(PR_c, [H(H(PI)||H(OI))])$

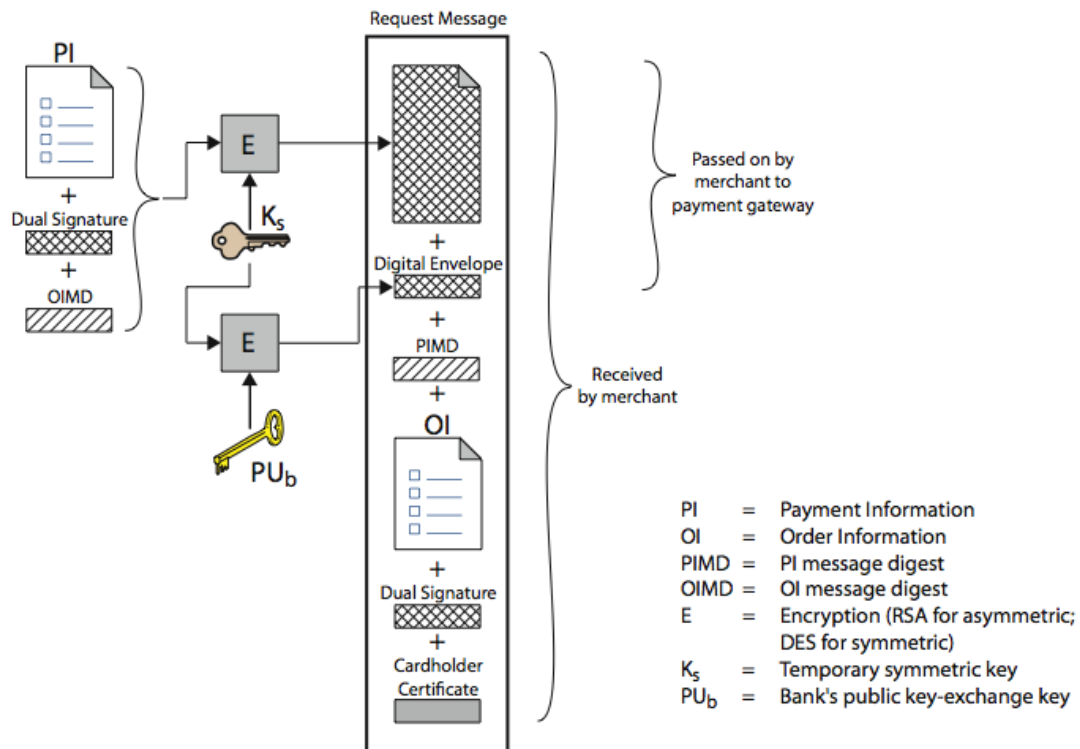
SET Purchase Request

The purchase request exchange consists of four messages: Initiate Request, Initiate Response, Purchase Request, and Purchase Response. In order to send SET messages to the merchant, the cardholder must have a copy of the certificates of the merchant and the payment gateway. The customer requests the certificates in the Initiate Request message, sent to the merchant. The merchant generates a response and signs it with its private signature key. The cardholder verifies the merchant and gateway certificates by means of their respective CA signatures and then creates the OI and PI. Next, the cardholder prepares the Purchase Request message with Purchase-related information & Order-related information. The Purchase Response message includes a response block that acknowledges the order and references the corresponding transaction number.

SET purchase request exchange consists of four messages

1. Initiate Request - get certificates
2. Initiate Response - signed response
3. Purchase Request - of OI & PI
4. Purchase Response - ack order

Purchase request Customer



Purchase request - Customer

The above figure shows the details of the contents of the Purchase Request message generated by the customer.

The message includes the following:

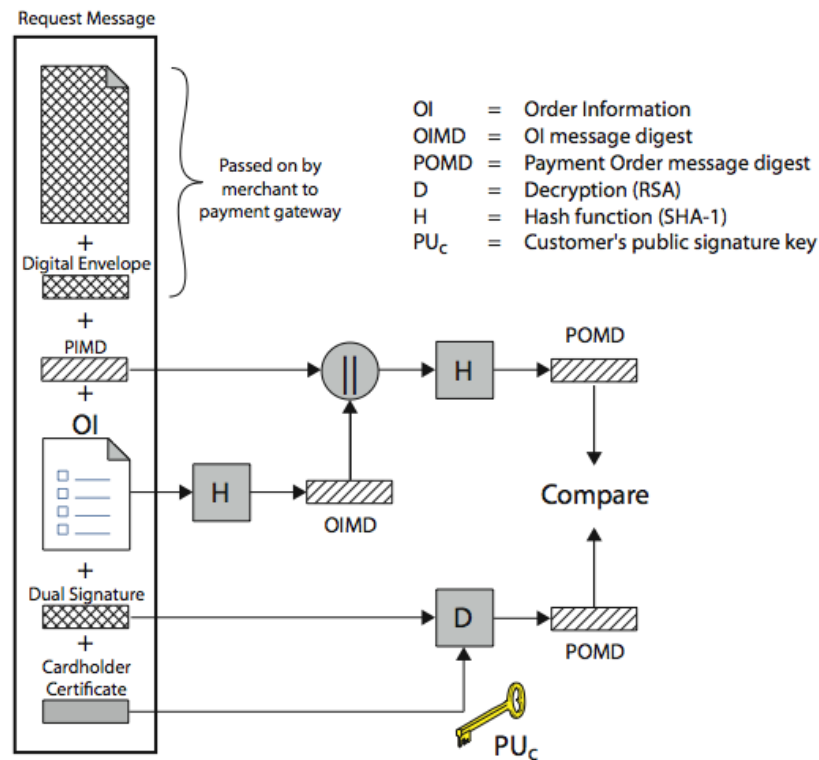
1. Purchase-related information, which will be forwarded to the payment gateway by the merchant and consists of: PI, dual signature, & OI message digest (OIMD).
2. Order-related information, needed by the merchant and consists of: OI, dual signature, PI message digest (PIMD).
3. Cardholder certificate. This contains the cardholder's public signature key.

Purchase request - Merchant

When the merchant receives the Purchase Request message, the actions listed are performed. The Purchase Response message includes a response block that acknowledges the order and references the corresponding transaction number. This block is signed by the merchant using its private signature key. The block and its signature are sent to the customer, along with the merchant's signature certificate.

1. Verifies cardholder certificates using CA signs
2. Verifies dual signature using customer's public signature key to ensure order has not been tampered with in transit & that it was signed using cardholder's private signature key
3. Processes order and forwards the payment information to the payment gateway for authorization (described later)

4. Sends a purchase response to cardholder



Purchase request – Merchant

Payment authorization

During the processing of an order from a cardholder, the merchant authorizes the transaction with the payment gateway.

1. Purchase-related information
 - PI+Dual Signature+OIMD+Digital Envelop
2. Authorization-related information
 - Authorization block (Transaction **ID**, **PR_m**)
 - Digital Envelop, **$E(PU_G(Ks))$**
3. Certificates
 - Cardholder's CA, Merchant's CA, and Merchant's Key-Exchange CA

Payment gateway authorization

During the processing of an order from a cardholder, the merchant authorizes the transaction with the payment gateway.

1. verifies all certificates
2. decrypts digital envelope of authorization block to obtain symmetric key & then decrypts authorization block
3. verifies merchant's signature on authorization block

4. decrypts digital envelope of payment block to obtain symmetric key & then decrypts payment block
5. verifies dual signature on payment block
6. verifies that transaction ID received from merchant matches that in PI received (indirectly) from customer
7. requests & receives an authorization from issuer
8. sends authorization response back to merchant

Payment Capture

To obtain payment, the merchant sends a capture request message to the payment gateway, for which the merchant generates, signs, and encrypts a capture request block, including payment amount and transaction ID.

The payment gateway receives the capture request message, decrypts and verifies the capture request block and decrypts and verifies the capture token block. It then checks for consistency between the capture request and capture token. It then creates a clearing request sent to the issuer over the private payment network, which causes funds to be transferred to the merchant's account. The gateway then notifies the merchant of payment in a Capture Response message, which includes a capture response block that the gateway signs and encrypts, plus the gateway's signature key certificate. The merchant software stores the capture response to be used for reconciliation with payment received from the acquirer.

1. merchant sends payment gateway a payment capture request
2. gateway checks request
3. then causes funds to be transferred to merchants account
4. notifies merchant using capture response

UNIT V

APPLICATIONS OF NETWORK SECURITY

5.1 Introduction to network security

Network security:

Network security consists of the policies and practices adopted 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 access to 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 businesses, 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. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network Security concepts

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' also used (e.g., a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like Wireshark traffic and may be logged for audit purposes and for later high-level analysis.

Communication between two hosts using a network may be encrypted to maintain privacy.

Honeypots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots.

Security management

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

Types of Attacks

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

Types of attacks include:

- Passive
 - Network
 - Wiretapping
 - Port scanner
 - Idle scan
- Active
 - Denial-of-service attack

- DNS spoofing
- Man in the middle
- ARP poisoning
- VLAN hopping
- Smurf attack
- Buffer overflow
- Heap overflow
- Format string attack
- SQL injection
- Phishing
- Cross-site scripting
- CSRF
- Cyber-attack

Basic concept of RAID

RAID (originally redundant **array** of inexpensive disks, now commonly redundant **array** of independent disks) is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both.

Raid contains groups or sets or Arrays. A combine of drivers make a group of disks to form a RAID Array or RAID set. It can be a minimum of 2 number of disk connected to a raid controller and make a logical volume or more drives can be in a group. Only one Raid level can be applied in a group of disks. Raid are used when we need excellent performance. According to our selected raid level, performance will differ. Saving our data by fault tolerance & high availability.

Featured Concepts of RAID

1. **Parity** method in raid regenerate the lost content from parity saved information's.
RAID 5, RAID 6 Based on Parity.

2. **Stripe** is sharing data randomly to multiple disk. This won't have full data in a single disk. If we use 3 disks half of our data will be in each disks.
3. **Mirroring** is used in RAID 1 and RAID 10. Mirroring is making a copy of same data. In RAID 1 it will save the same content to the other disk too.
4. **Hot spare** is just a spare drive in our server which can automatically replace the failed drives. If any one of the drive failed in our array this hot spare drive will be used and rebuild automatically.
5. **Chunks** are just a size of data which can be minimum from 4KB and more. By defining chunk size we can increase the I/O performance.

RAID's are in various Levels. The following levels are used mostly in real environment.

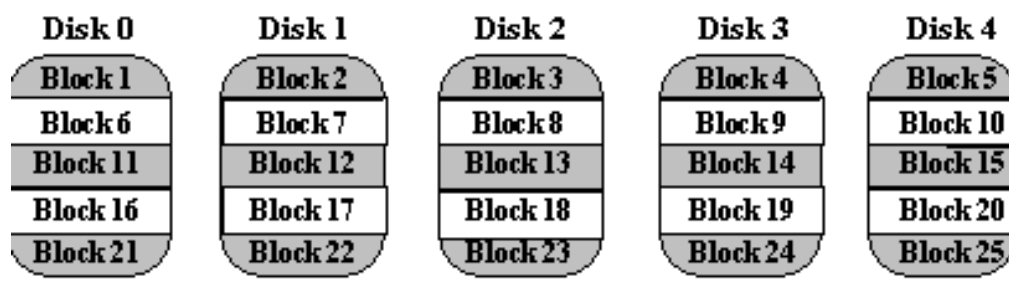
1. **RAID0** = Striping
2. **RAID1** = Mirroring
3. **RAID5** = Single Disk Distributed Parity
4. **RAID6** = Double Disk Distributed Parity
5. **RAID10** = Combine of Mirror & Stripe. (Nested RAID)

There are many types of RAID and some of the important ones are introduced below:

Non-Redundant (RAID Level 0)

A non-redundant disk array, or RAID level 0, has the lowest cost of any RAID organization because it does not employ redundancy at all. This scheme offers the best performance since it never needs to update redundant information. Surprisingly, it does not have the best performance. Redundancy schemes that duplicate data, such as mirroring, can perform better on reads by selectively scheduling requests on the disk with the shortest expected seek and rotational delays. Without, redundancy, any single disk failure will result in data-loss. Non-redundant disk arrays are widely used in super-computing environments where performance and capacity, rather than reliability, are the primary concerns.

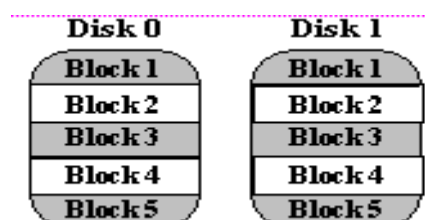
Sequential blocks of data are written across multiple disks in stripes, as follows:



The size of a data block, which is known as the "stripe width", varies with the implementation, but is always at least as large as a disk's sector size. When it comes time to read back this sequential data, all disks can be read in parallel. In a multi-tasking operating system, there is a high probability that even non-sequential disk accesses will keep all of the disks working in parallel.

Mirrored (RAID Level 1)

The traditional solution, called mirroring or shadowing, uses twice as many disks as a non-redundant disk array. whenever data is written to a disk the same data is also written to a redundant disk, so that there are always two copies of the information. When data is read, it can be retrieved from the disk with the shorter queuing, seek and rotational delays. If a disk fails, the other copy is used to service requests. Mirroring is frequently used in database applications where availability and transaction time are more important than storage efficiency.



Memory-Style(RAID Level 2)

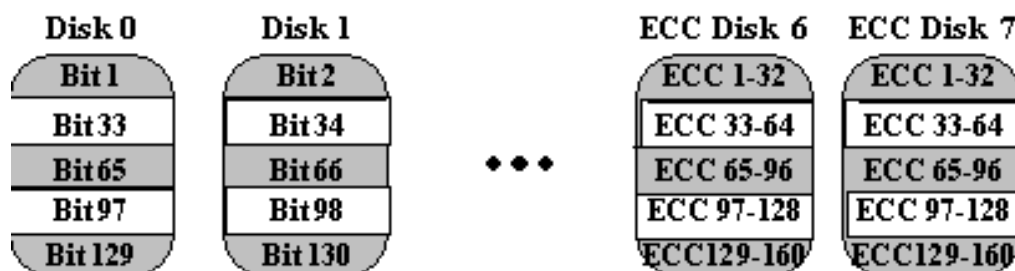
Memory systems have provided recovery from failed components with much less cost than mirroring by using Hamming codes. Hamming codes contain parity for distinct overlapping subsets of components. In one version of this scheme, four disks require three redundant disks, one less than mirroring. Since the number of redundant disks is proportional to the log of the total number of the disks on the system, storage efficiency increases as the number of data disks increases.

If a single component fails, several of the parity components will have inconsistent values, and the failed component is the one held in common by each incorrect subset. The lost information is recovered by reading the other components in a subset, including the parity component, and setting the missing bit to 0 or 1 to create proper parity value for that subset. Thus, multiple redundant disks are needed to identify the failed disk, but only one is needed to recover the lost information.

In you are unaware of parity, you can think of the redundant disk as having the sum of all data in the other disks. When a disk fails, you can subtract all the data on the good disks from the parity disk; the remaining information must be the missing information. Parity is simply this sum modulo 2.

A RAID 2 system would normally have as many data disks as the word size of the computer, typically 32. In addition, RAID 2 requires the use of extra disks to store an error-correcting code for redundancy. With 32 data disks, a RAID 2 system would require 7 additional disks for a Hamming-code ECC. Such an array of 39 disks was the subject of a U.S. patent granted to Unisys Corporation in 1988, but no commercial product was ever released.

For a number of reasons, including the fact that modern disk drives contain their own internal ECC, RAID 2 is not a practical disk array scheme.

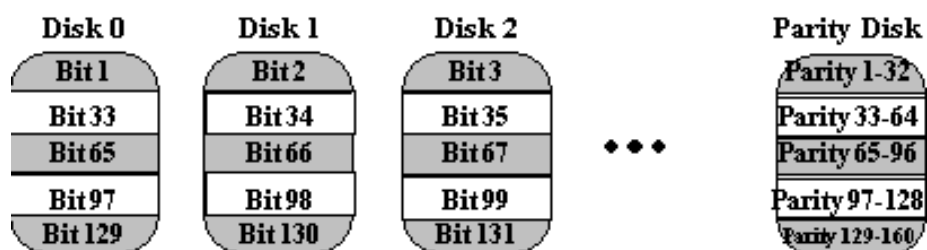


Bit-Interleaved Parity (RAID Level 3)

One can improve upon memory-style ECC disk arrays by noting that, unlike memory component failures, disk controllers can easily identify which disk has failed. Thus, one can use a single parity rather than a set of parity disks to recover lost information.

In a bit-interleaved, parity disk array, data is conceptually interleaved bit-wise over the data disks, and a single parity disk is added to tolerate any single disk failure. Each read request accesses all data disks and each write request accesses all data disks and the parity disk. Thus, only one request can be serviced at a time. Because the parity disk contains only parity and no data, the parity disk cannot participate on reads, resulting in slightly lower read performance than for redundancy schemes that distribute the parity and data over all disks. Bit-interleaved, parity disk arrays are frequently used in applications that require high bandwidth but not high I/O rates. They are also simpler to implement than RAID levels 4, 5, and 6.

Here, the parity disk is written in the same way as the parity bit in normal Random Access Memory (RAM), where it is the Exclusive Or of the 8, 16 or 32 data bits. In RAM, parity is used to detect single-bit data errors, but it cannot correct them because there is no information available to determine which bit is incorrect. With disk drives, however, we rely on the disk controller to report a data read error. Knowing which disk's data is missing, we can reconstruct it as the Exclusive Or (XOR) of all remaining data disks plus the parity disk.



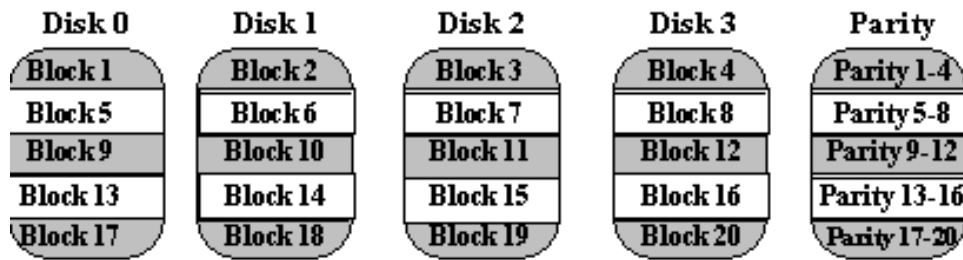
As a simple example, suppose we have 4 data disks and one parity disk. The sample bits are:

Disk 0	Disk 1	Disk 2	Disk 3	Parity
0	1	1	1	1

The parity bit is the XOR of these four data bits, which can be calculated by adding them up and writing a 0 if the sum is even and a 1 if it is odd. Here the sum of Disk 0 through Disk 3 is "3", so the parity is 1. Now if we attempt to read back this data, and find that Disk 2 gives a read error, we can reconstruct Disk 2 as the XOR of all the other disks, including the parity. In the example, the sum of Disk 0, 1, 3 and Parity is "3", so the data on Disk 2 must be 1.

Block-Interleaved Parity (RAID Level 4)

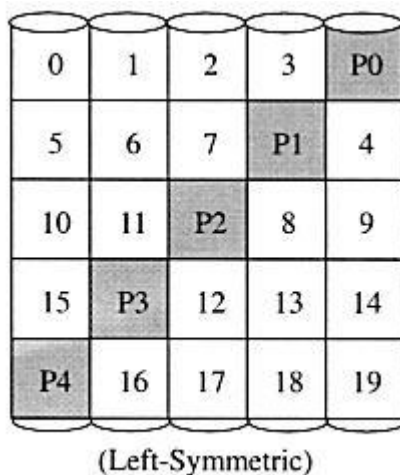
The block-interleaved, parity disk array is similar to the bit-interleaved, parity disk array except that data is interleaved across disks of arbitrary size rather than in bits. The size of these blocks is called the striping unit. Read requests smaller than the striping unit access only a single data disk. Write requests must update the requested data blocks and must also compute and update the parity block. For large writes that touch blocks on all disks, parity is easily computed by exclusive-or'ing the new data for each disk. For small write requests that update only one data disk, parity is computed by noting how the new data differs from the old data and applying those differences to the parity block. Small write requests thus require four disk I/Os: one to write the new data, two to read the old data and old parity for computing the new parity, and one to write the new parity. This is referred to as a read-modify-write procedure. Because a block-interleaved, parity disk array has only one parity disk, which must be updated on all write operations, the parity disk can easily become a bottleneck. Because of this limitation, the block-interleaved distributed parity disk array is universally preferred over the block-interleaved, parity disk array.



Block-Interleaved Distributed-Parity (RAID Level 5)

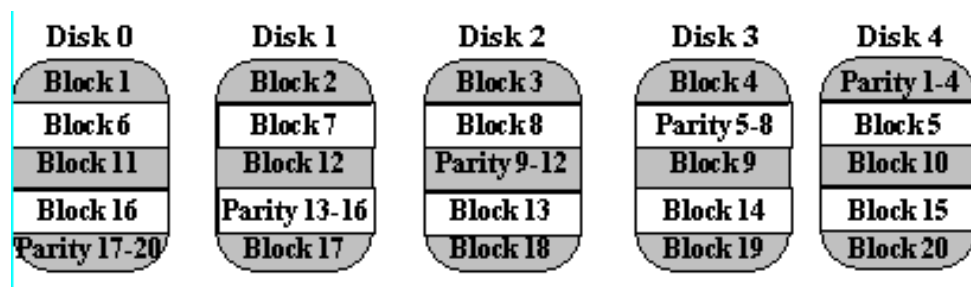
The block-interleaved distributed-parity disk array eliminates the parity disk bottleneck present in the block-interleaved parity disk array by distributing the parity uniformly over all of the disks. An additional, frequently overlooked advantage to distributing the parity is that it also distributes data over all of the disks rather than over all but one. This allows all disks to participate in servicing read operations in contrast to redundancy schemes with dedicated parity disks in which the parity disk cannot participate in servicing read requests. Block-interleaved distributed-parity disk array have the best small read, large write performance of any redundancy disk array. Small write requests are somewhat inefficient compared with redundancy schemes such as mirroring however, due to the need to perform read-modify-write operations to update parity. This is the major performance weakness of RAID level 5 disk arrays.

The exact method used to distribute parity in block-interleaved distributed-parity disk arrays can affect performance. Following figure illustrates left-symmetric parity distribution.



Each square corresponds to a stripe unit. Each column of squares corresponds to a disk. P0 computes the parity over stripe units 0, 1, 2 and 3; P1 computes parity over stripe units 4, 5, 6, and 7 etc

A useful property of the left-symmetric parity distribution is that whenever you traverse the striping units sequentially, you will access each disk once before accessing any disk device. This property reduces disk conflicts when servicing large requests.



P+Q redundancy (RAID Level 6)

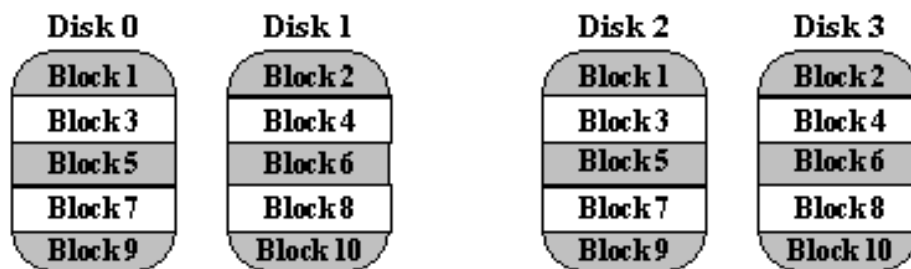
Parity is a redundancy code capable of correcting any single, self-identifying failure. As large disk arrays are considered, multiple failures are possible and stronger codes are needed. Moreover, when a disk fails in parity-protected disk array, recovering the contents of the failed disk requires successfully reading the contents of all non-failed disks. The probability of encountering an uncorrectable read error during recovery can be significant. Thus, applications with more stringent reliability requirements require stronger error correcting codes.

Once such scheme, called P+Q redundancy, uses Reed-Solomon codes to protect against up to two disk failures using the bare minimum of two redundant disk arrays. The P+Q redundant disk arrays are structurally very similar to the block-interleaved distributed-parity disk arrays and operate in much the same manner. In particular, P+Q redundant disk arrays also perform small write operations using a read-modify-write procedure, except that instead of four disk accesses per write requests, P+Q redundant disk arrays require six disk accesses due to the need to update both the 'P' and 'Q' information.

Striped Mirrors (RAID Level 10)

RAID 10 was not mentioned in the original 1988 article that defined RAID 1 through RAID 5. The term is now used to mean the combination of RAID 0 (striping) and RAID 1 (mirroring). Disks are mirrored in pairs for redundancy and improved performance, then data is striped across multiple disks for maximum performance. In the diagram below, Disks 0 & 2 and Disks 1 & 3 are mirrored pairs.

Obviously, RAID 10 uses more disk space to provide redundant data than RAID 5. However, it also provides a performance advantage by reading from all disks in parallel while eliminating the write penalty of RAID 5. In addition, RAID 10 gives better performance than RAID 5 while a failed drive remains unreplaced. Under RAID 5, each attempted read of the failed drive can be performed only by reading all of the other disks. On RAID 10, a failed disk can be recovered by a single read of its mirrored pair.



RAID Systems Need Tape Backups

It is worth remembering an important point about RAID systems. Even when you use a redundancy scheme like mirroring or RAID 5 or RAID 10, you must still do regular tape backups of your system. There are several reasons for insisting on this, among them:

- RAID does not protect you from multiple disk failures. While one disk is off line for any reason, your disk array is not fully redundant.
- Regular tape backups allow you to recover from data loss that is not related to a disk failure. This includes human errors, hardware errors, and software errors.

5.2 Hackers Techniques

The term “hacker” was originally coined for an individual who could make computers work. A hacker currently refers to an individual who breaks into computers. Studies show that hackers are most often male, between 16 and 35 years old, loners, intelligent, and technically proficient.

The most common motivation for hacking into computer systems is the challenge of doing so. The challenge motivation is usually associated with an untargeted hacker. An untargeted hacker is one who hacks just for the fun of it. The greed motivation includes desire for gain in the form of money, goods, services, or information.

Sites having something of value (software, money, information) are primary targets for hackers motivated by greed. Malicious attacks focus on particular targets. The hacker motivated by malicious intent aims at damaging, and not gaining access to the system.

The risk of a hacker being caught and convicted is low. Hence, the potential gain from hacking is high. The hackers can be classified into whitehat, blackhat and greyhat.

Whitehat Hacker

A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. The EC-Council , also known as the International Council of Electronic Commerce Consultants has developed certifications, course ware, classes, and online training covering the diverse arena of Ethical Hacking.

Blackhat Hacker

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005). Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into

secure networks to destroy data or make the network unusable for those who are authorized to use the network.

Greyhat Hacker

A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked, for example. Then they may offer to repair their system for a small fee.

Historical hacking techniques

Open sharing

When the Internet was originally created, most systems were configured to share information. The Network File System (NFS) used by UNIX allowed one computer to mount the drives of another computer across a network. Hackers used NFS to read the information by mounting remote drives. Many operating systems were shipped out with the root file system exportable to the world. Anyone could mount the system's root file and change anything they wanted if the default configuration was not changed. Hackers can get into a system with remote access, by identifying one user or administrator account on the system.

Weak passwords:

Weak passwords are the most common method used by hackers to get into systems. A two-character password is easier to guess than an eight-character one. Easy to guess passwords allow hackers a quick entry into the system.

Programming flaws and social engineering:

Hackers have used programming flaws such as back doors in a program for accessing systems that use the program. Many shopping Websites store information entered by the buyer on a URL, which can be modified before checking out. Social engineering is the use of non-technical means to gain unauthorized access to information or systems. The ability to lie and a kind voice

are the most powerful tools used by a hacker using the social engineering technique.

Buffer overflow:

Buffer overflow is an attempt to store too much information into an allocated space in a computer's memory. Buffer overflows allow hackers to run a command on the target system. A hacker can exploit a buffer overflow to overwrite the return address to point to a new instruction.

Denial-of-Service (DoS):

DoS attacks are malicious acts to deny legitimate users access to a system, network, application, or information. Most DoS attacks originate from fake addresses.

In a single-source DoS attack, a single system is used to attack another system.

The SYN flood and the Ping of Death are some of the single-source DoS attacks that have been identified.

Distributed Denial-of-Service (DDoS):

DDoS attacks originate from a large number of systems. Trinoo, Tribal Flood Network, Mstream, and Stacheldraht are some of the new DDoS attack tools.

A hacker talks to a master or server that has been placed on a compromised system. The master talks to the slave or client processes that have been placed on other compromised systems. The slaves, also called zombies, perform the actual attack against the target system.

Advanced Techniques

Vulnerability scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Note that firewalls defend computers from intruders by limiting access to ports/machines both inbound and outbound, but can still be circumvented.)

Password Cracking

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

Packet sniffer

A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

Spoofing attack (Phishing)

A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.

Rootkit

A rootkit is designed to conceal the compromise of a computer's security, and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables.

Social engineering

When a Hacker, typically a black hat, is in the second stage of the targeting process, he or she will typically use some social engineering tactics to get enough information to access the network. A common practice for hackers who use this technique, is to contact the system administrator and play the role of a user who cannot get access to his or her system.

Viruses

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Therefore, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. While some are harmless or mere hoaxes most computer viruses are considered malicious.

Worm

Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not need to attach itself to an existing program. Many people conflate the terms "virus" and "worm", using them both to describe any self-propagating program.

Trojan horses

A Trojan horse is a program which seems to be doing one thing, but is actually doing another. A trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later. (The name refers to the horse from the Trojan War, with conceptually similar function of deceiving defenders into bringing an intruder inside.)

Key loggers

A key logger is a tool designed to record ('log') every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data. Some key loggers uses virus-, trojan-, and rootkit-like methods to remain active and hidden. However, some key loggers are used in legitimate ways and sometimes to even enhance computer security. As an example, a business might have a key logger on a computer used at a point of sale and data collected by the key logger could be used for catching employee fraud.

SPAM

Email **spam**, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

In addition to wasting people's time with unwanted email, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers.

Electronic spamming is the use of electronic messaging systems to send an unsolicited message (**spam**), especially advertising, as well as sending messages repeatedly on the same site. Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, servers, infrastructures, IP ranges, and domain names, and it is difficult to hold senders accountable for their mass mailings. A person who creates electronic spam is called a *spammer*.

5.3 Security Mechanism

Introduction

The process to implement the security properties is known as security mechanism. The various type of mechanism on the basis of properties is as follows:

- Attack Prevention
- Attack Avoidance
- Attack Detection

Attack Prevention: can be defined as a series of security mechanism implemented to prevent or defend against various types of attack before they can actually reach and affect the target systems. An important mechanism is access control which is defined as the process of limiting the access to the resources of the Information System. Access can be implemented at different levels such as the operating system the network and the application layer.

A firewall is also an important access control system that is implemented at the network layer the concept behind firewall is to separate the trusted network from the entrusted network known as internet. The firewall prevents the attack from the outside world against the

machines inside the internal network by preventing connection s attempts from the unauthorized entities located outside.

Attack Avoidance: The expansion of connectivity of computers makes the need of protecting the message and message from tampering reading important. This is the technique in which the information is modified in a way that makes is unusable for the attacker. This is performed under the assumption that the attacker may have access to the subject system/information. The sender preprocess the information before it is send through the unsecured system and the same is again post processed on the receiver end systems. This encryption and decryption is perfumed by cryptography mechanism, they are further divided in the following forms:

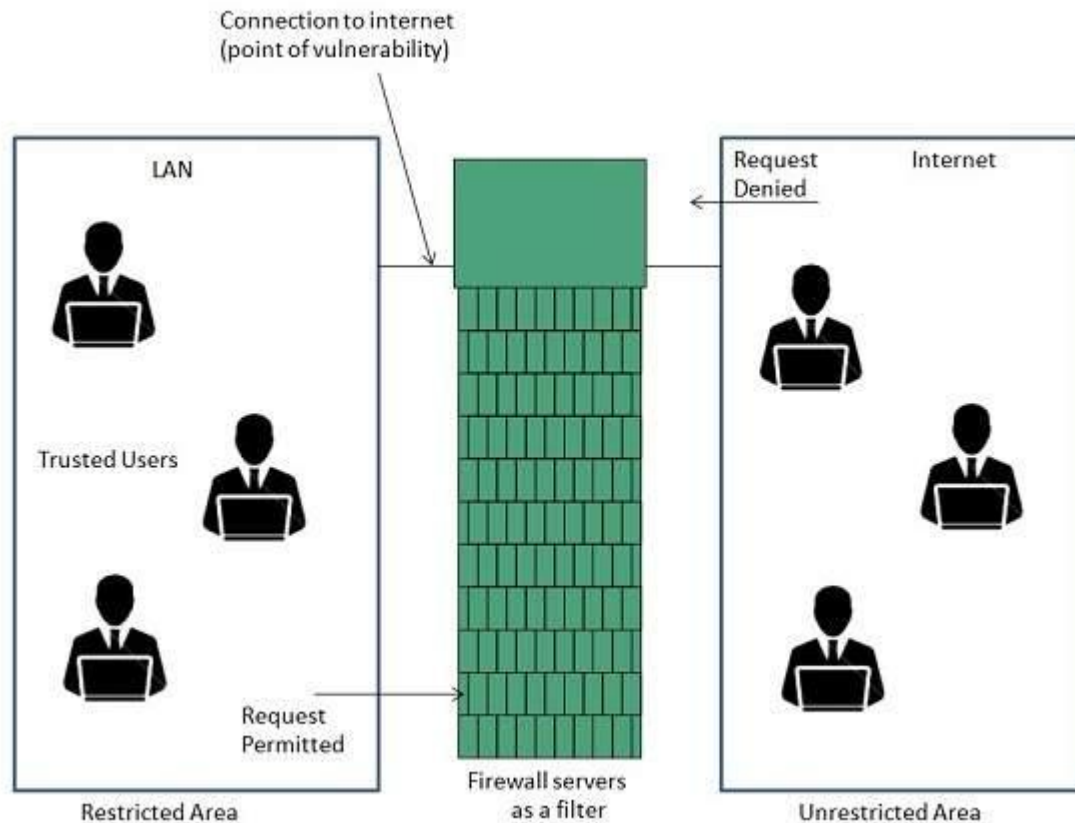
- Secret Key Cryptography
- Public Key Cryptography
- Hash Functions

Attack Detection: In this mechanism it is assumed that the attacker is able to bypass the installed security measures to access the desired target/information. When such incidents happens attack detection takes the responsibility to report someone that something went wrong somewhere in the system. Attack detection is not an applicable mechanism instead of that it's a check/measure which will make sure that if anything happened badly in the system then someone should be notified for the same.

Firewall

Firewall is a barrier between Local Area Network (LAN) and the Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions.

The following diagram depicts a sample firewall between LAN and the internet. The connection between the two is the point of vulnerability. Both hardware and the software can be used at this point to filter network traffic.



There are two types of Firewall system: One works by using filters at the network layer and the other works by using proxy servers at the user, application, or network layer.

Key Points

- Firewall management must be addressed by both system managers and the network managers.
- The amount of filtering a firewall varies. For the same firewall, the amount of filtering may be different in different directions.

Design goals of 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.
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 the use of a hardened

system with a secured operating system. Trusted computer systems are suitable for hosting a firewall and often required in government applications.

There are four general techniques that firewalls use to control access and enforce the site's security policy. Originally, firewalls focused primarily on service control, but they have since evolved to provide all four:

- 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, protocol, or 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 (IPsecurity).

- 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.

Before proceeding to the details of firewall types and configurations, it is best to summarize what one can expect from a firewall. The following capabilities are within the scope of a firewall:

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.

2.A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.

3.A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.

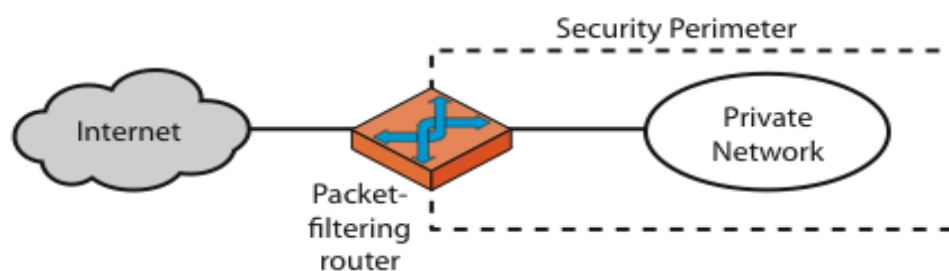
4.A firewall can serve as the platform for IPsec. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

Types of Firewall

a.Packet Filtering Firewall

A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet . The firewall 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 IP address:The IP address of the system that originated the IP packet
- Destination IP address: The IP address of the system the IP packet is trying to reach
- Source and destination transport-level address:The transport-level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET
- IP protocol field: Defines the transport protocol
- Interface: For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for.



(a) Packet-filtering router

The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken.

Two default policies are possible:

- Default = discard: That which is not expressly permitted is prohibited.
- Default = forward: That which is not expressly prohibited is permitted.

The default discard policy is more conservative. Initially, everything is blocked, and services must be added on a case-by-case basis. This policy is more visible to users, who are more likely to see the firewall as a hindrance. However, this is the policy likely to be preferred by businesses and government organizations. Further, visibility to users diminishes as rules are created. The default forward policy increases ease of use for end users but provides reduced security; the security administrator must, in essence, react to each new security threat as it becomes known. This policy may be used by generally more open organizations, such as universities.

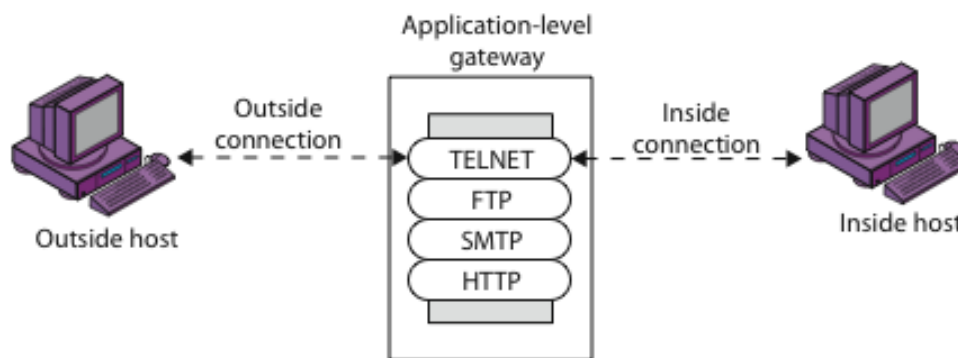
One **advantage** of a packet filtering firewall is its **simplicity**. Also, packet filters typically are transparent to users and are very fast. The following are some of the **weaknesses of packet filter firewalls**:

- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions. For example, a packet filter firewall cannot block specific application commands; if a packet filter firewall allows a given application, all functions available within that application will be permitted.
- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).

- Most packet filter firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality by the firewall.
- Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing . Many packet filter firewalls cannot detect a network packet in which the OSI Layer 3 addressing information has been altered. Spoofing attacks are generally employed by intruders to bypass the security controls implemented in a firewall platform.
- Finally, due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations. In other words, it is easy to accidentally configure a packet.

b.Application-Level Gateway

An application-level gateway, also called an application proxy, acts as a relay of application-level traffic. 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.



(b) Application-level gateway

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. In addition, it is easy to log and audit all incoming traffic at the application level. A prime disadvantage of this type of 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.

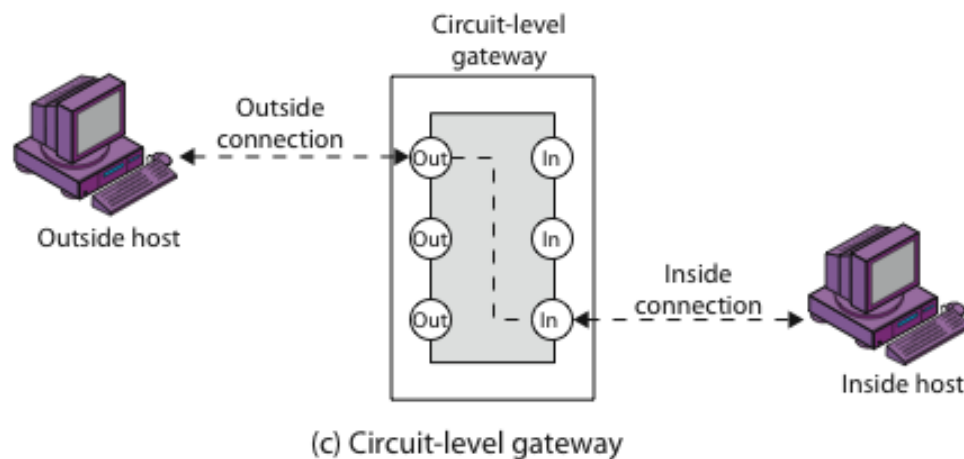
c.Circuit-Level Gateway

The circuit-level gateway or circuit-level proxy ,can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. As with

an application gateway, 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 typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections. In this

configuration, the gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data. An example of a circuit-level gateway implementation is the SOCKS package



It is common to base a firewall on a stand-alone machine running a common operating system, such as UNIX or Linux. Firewall functionality can also be implemented as a software module in a router or LAN switch.

A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Typically, the bastion host serves as a platform for an application-level or circuit-level gateway.

Limitations of Firewalls

- 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 may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.

3. An improperly secured wireless LAN may be accessed from outside the organization. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall.

4. A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally.

5.4 Intrusion detection (ID)

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as *scanning*), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

ID systems are being developed in response to the increasing number of attacks on major sites and networks, including those of the Pentagon, the White House, NATO, and the U.S. Defense Department. The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less technical ability is required for the novice attacker, because proven past methods are easily accessed through the Web.

Typically, an ID system follows a two-step process. The first procedures are host-based and are considered the *passive* component, these include: inspection of the system's configuration files to detect inadvisable settings; inspection of the password files to detect inadvisable

passwords; and inspection of other system areas to detect policy violations. The second procedures are network-based and are considered the *active* component: mechanisms are set in place to reenact known methods of attack and to record system responses.

In 1998, ICSA.net, a leading security assurance organization, formed the Intrusion Detection Systems Consortium (IDSC) as an open forum for ID product developers with the aim of disseminating information to the end user and developing industry standards.

Intruders

One of the two most publicized threats to security is the intruder (the other is viruses), generally referred to as a hacker or cracker. In an important early study of intrusion, Anderson identified three classes of intruders:

- **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
- **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
- **Clandestine user:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection .

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.

Intrusion detection systems are softwares used for identifying the intentional or unintentional use of the system resources by unauthorized users. They can be categorized into misuse detection systems and anomaly detection systems. Misuse detection systems model attacks as a specific pattern and are more useful in detecting known attack patterns. If the intrusion occurs during learning, then the anomaly detection system may learn the intruder's behavior and hence may fail.

Intrusion detection is very important aspects of protecting the cyber infrastructure from terrorist attack or from hackers. Intrusion prevention technique such as firewall, filtering

router policies fails to stop much type of attacks. Therefore, no matter how secure we try to make our system, intrusion still happens and so they must be detected. Intrusion detection systems are becoming an important part of our computer system, and security.

An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files and malware (Viruses, Trojanhorses and Worms).

An Intrusion detection system can be composed of several components: Sensors which generate security events, a Console to monitor events and alerts and control the sensors and a central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received. There are several ways to categorize an Intrusion detection system depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance. Intrusion detection can allow for the prevention of certainty, attacks severity relative to different type of attacks and vulnerability of components .Under attack the response may be to kill the connection, install filtering rules and disable user account.

Classification .There are two main classes of Intrusion such as :

(a) Misuse (abuse).

Intrusion is well-defined attacks on known weak points of system. All Intrusion which object is to misuse system resources and break it, are fall in this categories. Misuse intruder can be detected by watching for certain action being performed on certain objects and also by doing the pattern matching on audit trail information .

(b)Anomaly .

Intrusions are based on observations of deviation from normal system usage pattern. They can be detected by observing significant deviation from the normal behavior. Anomalous Intrusion is harder to detect. Anomaly or Anomalous may be symptoms of possible Intrusion. Anomaly detection has also been performed through other mechanism such as Neural

Network. System vulnerabilities involve abnormal use of system and therefore , security violation could be detected from abnormal pattern of system usage.

Intrusion Detection Systems (IDS)

For general purpose, the Intrusion Detection System (IDS) has evolved into two major architectures.

(a)Network-Based Intrusion Detection System.

Network based IDS are best suited for alert generation of intrusion from outside the perimeter of the enterprise. The network based IDS are inserted at various points on LAN and observe packets traffic on the Network information is assembled into packets and transmitted on LAN or Internet. Network based IDS are valuable if they are placed just outside the firewalls, thereby alerting personals to incoming packets that might circumvent to the firewall. Some Network -Based IDS take or allows taking input of Custom signatures taken from user security policy which permits limited detection security policy violation. This limitation is due to packets traffic information that does not work well today in switched and encrypted environments where packets analysis is weak in detecting, attacking or originating from authorized Network users. Network-Based Intrusion Detection Systems (IDS) use raw network packets as the data source. The IDS typically uses a network adapter in promiscuous mode that listens and analyses all traffic in real-time as it travels across the network.

(b)Hostbased Intrusion Detection System.

Host-based IDS places monitoring sensors also known as agents on network resources nodes to monitor audit logs which are generated by Network Operating System or application program. Audit logs contain records for events and activities taking place at individual Network resources. Because this Host -Based IDS can detect attacks that cannot be seen by Network-based IDS such as Intrusion and can be misuse by trusted insider. Host-based system utilize Signature rule base which is derived from site-specific security policy. Host-Based can overcome the problems associated with Network based IDS immediately after alarming the security personnel who can locate the source provided by site security policy. Host-based

IDS can also verify if any attack was unsuccessful, either because of immediate response to alarm or any other reason but this is not available at packet level.

Host-Based IDS can also maintain user login and user logoff action and all activity that generates audit records.

(c)The need for both types.

As we can clearly see both network and host-based IDS solutions have unique strengths and benefits over one another and that is why the next generation IDS must evolve to include a tightly integrated host and network component. There are no Silver Bullets when it comes to network security but adding these two required components will greatly enhance our resistance to attack.

Honeypots

A relatively recent innovation in intrusion detection technology is the honeypot . Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems. Honeypots are designed to

- divert an attacker from accessing critical systems.
- collect information about the attacker's activity.
- encourage the attacker to stay on the system long enough for administrators to respond.

These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access. Thus, any access to the honeypot is suspect. The system is instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activities. Because any attack against the honeypot is made to seem successful, administrators have time to mobilize and log and track the attacker without ever exposing productive systems.

Initial efforts involved a single honeypot computer with IP addresses designed to attract hackers. More recent research has focused on building entire honeypot networks that emulate an enterprise, possibly with actual or simulated traffic and data. Once hackers are within the network, administrators can observe their behavior in detail and figure out defenses.

5.5 Wireless Security Issues

Wireless security is the prevention of unauthorized access or damage to computers using **wireless** networks. The most common types of **wireless security** are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999, which was outdated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues.^[1] Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

Transmission security

Transmission security (TRANSEC) is the component of communications security (COMSEC) that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. Goals of transmission security include:

- Low probability of interception (LPI)
- Low probability of detection (LPD)
- Antijam — resistance to jamming (EPM or ECCM)

Methods used to achieve transmission security include frequency hopping and spread spectrum where the required pseudorandom sequence generation is controlled by a cryptographic algorithm and key. Such keys are known as **transmission security keys (TSK)**. Modern U.S. and NATO TRANSEC-equipped radios include SINCGARS and HAVE QUICK.

Network authentication

Network authentication is a security process required when a computer on a network tries to connect to the server in order to use its resources. If the user's identity has been stored by the server, entering a valid username and password completes the connection.

Wireless local area network (WLAN)

A **wireless local area network (WLAN)** is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network. A WLAN can also provide a connection to the wider Internet.

A **wireless intrusion detection system (WIDS)** monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Rogue devices can spoof MAC address of an authorized network device as their own. New research uses fingerprinting approach to weed out devices with spoofed MAC addresses. The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices.

Intrusion detection

A **wireless intrusion detection system (WIDS)** monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems

administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Rogue devices can spoof MAC address of an authorized network device as their own. New research uses fingerprinting approach to weed out devices with spoofed MAC addresses. The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices.

Eavesdropping

Eavesdropping is secretly listening to the private conversation of others without their consent, as defined by *Black's Law Dictionary*. The practice is commonly believed to be unethical.

Network eavesdropping is a network layer attack that focuses on capturing small packets from the network transmitted by other computers and reading the data content in search of any type of information. This type of network attack is generally one of the most effective as a lack of encryption services are used. It is also linked to the collection of metadata. Those who perform this type of attack are generally black hat hackers; however, government agencies, such as the National Security Agency, have also been connected.

Types of Attacks

Networks are subject to attacks from malicious sources. Attacks can be from two categories:

1. Active attack
2. Passive attack

1. Active attack

Active attack is the one in which an intruder initiates commands to disrupt the network's normal operation.

- Active
 - Denial-of-service attack
 - DNS spoofing
 - Man in the middle

- ARP poisoning
- VLAN hopping
- Smurf attack
- Buffer overflow
- Heap overflow
- Format string attack
- SQL injection
- Phishing
- Cross-site scripting
- CSRF
- Cyber-attack

2. Passive attack

Passive attack is the one in which a network intruder intercepts data traveling through the network

- Network
 - Wiretapping
 - Port scanner
 - Idle scan

Wired Equivalent Privacy (WEP)

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of an access point/bridge can receive the access point/bridge's radio transmissions. Because WEP is the first line of defense against intruders, Cisco recommends that you use full encryption on your wireless network.

WEP encryption scrambles the radio communication between access point/bridges to keep the communication private. Communicating access point/bridges use the same WEP key to encrypt and unencrypt radio signals. WEP keys encrypt both unicast and multicast messages. Unicast messages are addressed to just one device on the network. Multicast messages are addressed to multiple devices on the network.

Extensible Authentication Protocol (EAP) authentication provides dynamic WEP keys to wireless devices. Dynamic WEP keys are more secure than static, or unchanging, WEP keys. If an intruder passively receives enough packets encrypted by the same WEP key, the intruder can perform a calculation to learn the key and use it to join your network. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key.

Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. You must use a cipher suite to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM). Because cipher suites provide the protection of WEP while also allowing use of authenticated key management, Cisco recommends that you enable WEP by using the encryption mode cipher command in the CLI or by using the cipher drop-down menu in the web-browser interface. Cipher suites that contain TKIP provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

These security **features** protect the data traffic on your wireless LAN:

- WEP (Wired Equivalent Privacy)—WEP is an 802.11 standard encryption algorithm originally designed to provide your wireless LAN with the same level of privacy available on a wired LAN. However, the basic WEP construction is flawed, and an attacker can compromise the privacy with reasonable effort.
- TKIP (Temporal Key Integrity Protocol)—TKIP is a suite of algorithms surrounding WEP that is designed to achieve the best possible security on legacy hardware built to run WEP. TKIP adds four enhancements to WEP:
 - A per-packet key mixing function to defeat weak-key attacks
 - A new IV sequencing discipline to detect replay attacks
 - A cryptographic message integrity Check (MIC), called Michael, to detect forgeries such as bit flipping and altering packet source and destination
 - An extension of IV space, to virtually eliminate the need for re-keying

- CKIP (Cisco Key Integrity Protocol)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
- CMIC (Cisco Message Integrity Check)—Like TKIP's Michael, Cisco's message integrity check mechanism is designed to detect forgery attacks.

Reference:

- 1.Data Communications and Networking – Behrouz A Forouzan-4th edition
- 2.Data Communications and Networks.-Atul Kahate,Godbole-2nd edition
- 3.Computer Networks – Andrews S. Tannenbaum,4th Edition