With Solution to Questions of Previous Exams

Insights on COMPUTER NETWORKS

Er. Smriti Nakarmi
Er. Lila Rana
Er. Samit Kumar Singh
Er. Biplab Poudel

CONTENTS

CHAPTER – 5

TRANSPORT LAYER

CHAPTER – 6

APPLICATION LAYER

CHAPTER – 7

INTRODUCTION TO IPV6

CHAPTER – 8

NETWORK SECURITY

CHAPTER – 1

INTRODUCTION TO COMPUTER NETWORK

1.1 Computer Network

A *computer network* is the infrastructure that allows computers and networking devices to exchange data. It is a collection of computers and other devices (nodes) that use a common network protocol to share information and resources with each other over a network medium. The network medium may be copper wire, fiber optics, microwave, infrared or even communication satellites.

The uses of computer networks are:

1. Business Application

The computer networks are useful to the organization in the following ways:

a. Resource Sharing

Computer networks can have a large number of computers, which can share software, database and other resources without regarding the geographical location. With resource sharing, a device in a network can be accessed by different computers which is connected to the common devices like printer, fax, scanner, etc. Different information and data like files, videos can be exchanged between various organizations, people and technologies using the computer networks.

b. High Reliability

Computer networks provide high reliability by having alternative sources of supply. For example, all files could be replicated on two or more machines so that if one of them is unavailable, the other copies could be used.

c. Saving Money

Organizations can use separate personal computer one per user instead of using mainframe computers which

are expensive. The organizations can use the work-group model (peer to peer) in which all the PCs are networked together and each one can have the access to the other for communicating or sharing purposes.

Using computer networks, companies can do business electronically, they can place orders electronically as needed which reduces the need for large investments.

d. Scalability

Requirement of software, hardware, database etc. increases gradually with the increase in networks. In a centralized computing system, if one computer is not able to serve the purpose, it can be replaced by a new one. Replacement of new devices may require lots of investment and effort, which can be avoided in computer network systems. If there is a need for more, one can buy another powerful computer, add it to the computer network and use it.

2. Home Application

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

a. E-commerce

E-commerce supports many types of business transactions where users can pay bills, transfer cash, and do online shopping. Users can browse the website and choose from the list of items and do payment online.

b. Access to Remote Information

Computer networks facilitate users to access information that is distant away by staying at home remotely.

c. Person-to-Person Communication

With network availability, one can easily communicate with other people via voice, text or video staying at one place. The cost of this type of communication is much cheaper than a normal phone call and definitely faster.

d. Interactive entertainment

Computer networks are used in multiplayer gaming where people participate in real time simulation games. Another application is video on demand where the network user can request for a particular movie, music or video clip anytime. Users can even access social networking sites like Facebook, Twitter, etc. to connect with people.

e. Online education

With network connections, students at any location around the world can participate in an online classroom, download notebooks, and submit assignments.

3. Mobile users

With the help of networking, anyone can connect remotely through mobile computers such as mobile cell phones, laptops, notebook computers, and control their devices. Mobile users use their portable electronic equipment to send and receive telephone calls, faxes and electronic mail, surf the web, access remote files and log on to remote machines.

1.2 Networking Model, Active Network

1.2.1 Types of Networking Model

Networking model is categorized into two types:

1. Client-Server Model

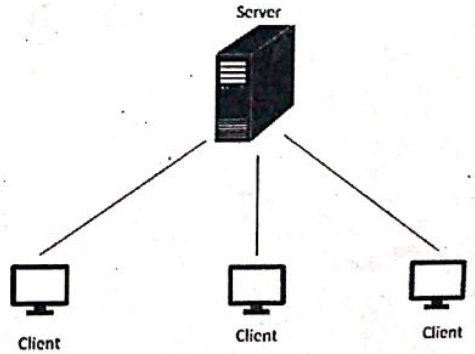


Figure 1.1: Client-server model

Client-server architecture (client/server) is a network architecture in which each computer or process on the network is either a client or a server. In this model, two processes are involved, one on the client machine and another on the server machine.

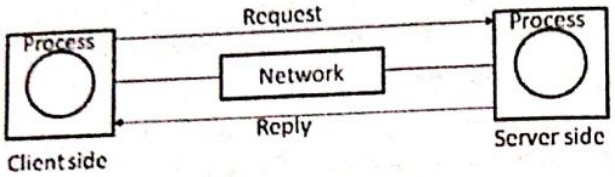


Figure 1.2: Request and reply model

Communication starts by sending a request message from client process to server process. The client process then waits for a reply message. When the server process gets the request, it performs the required processes and sends back a reply message. For example, when a person at home accesses a page on the World Wide Web, the same model is employed, with the remote web server being the server and the user's personal computer being the client.

2. Peer-to-Peer Model

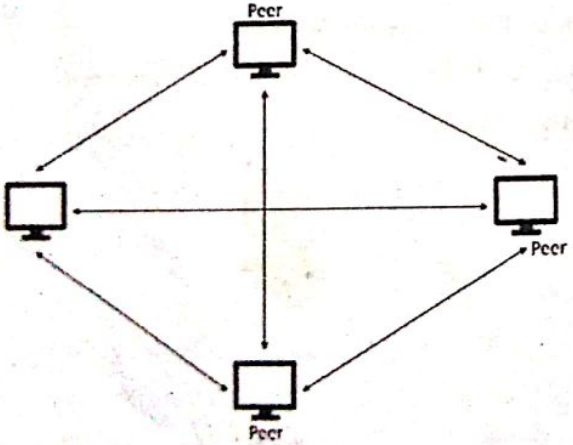


Figure 1.3: Peer-to-peer model

A peer-to-peer (P2P) network is created when two or more PCs or devices are connected and share their resources without communicating with a separate server computer. In peer-to-peer networking architecture, each computer (workstation) has equivalent capabilities & responsibilities. Each PC acts as an independent workstation that stores data on its own hard drive but which can share it with all other PCs on the network. Computers connecting with each other in a workgroup can share files, printers, and internet access.

1.2.2 Active Network

Active network is a network which not just carries the bits from one end system to another but also performs computations on the data flowing through them. Active network can be at least as secure as the legacy network. Data and algorithms in an active network are mutable and fluid. It enables a more flexible network. It has faster hardware. Devices become network-aware. It also enables faster development of new service.

1.3 Network Topology

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

Networks have both a physical and logical topology

- **Physical topology:** The layout of the devices and media
- **Logical topology:** The paths that signals travel from one point on the network to another.

Categories of Network Topology:

- Bus topology
- Tree topology
- Mesh topology
- Star topology
- Ring topology
- Hybrid topology

1.4 Protocol and Standard

A *protocol* is an agreement between two machines as to how communication links should be established, maintained and released. It defines the format, timing, sequencing, and error control mechanisms in data communication.

Protocol controls the way in which data is communicated. Protocol explains:

- How the physical network is built
- How computers connect to the network
- How the data is formatted for transmission
- How the data is sent over the network
- How to deal with errors

Standards

Standards are guidelines that are followed when a new design is to be introduced. Standards enable equipment from different vendors and with different operating characteristics to become components of the same network. Standards are developed by national and international organizations established for this exact purpose. Some of the important standards developed by various organizations are listed below;

- **ISO (International Standards Organization):** It is a voluntary organization with representatives from national standards organizations of member countries. ISO is active in many areas of science and technology, including information technology.
- **CCITT (The Consultative committee for International Telegraph and Telephone):** It is a standards organization devoted to data and telecommunication with representatives from governments, major vendors, telecommunication carriers and the scientific community.
- **IEEE (Institute of Electrical and Electrical Engineer):** It is a US standards organization with members throughout the world. IEEE is active in many electric and electronic-related areas.
- **EIA (Electronic Industries Associations):** It is a US trade association best known for its EIA-232 standards.

1.4.1 Layered Architecture

Layered architecture simplifies the network design. As it is easy to debug network applications in a layered architecture, network applications are separated into layers. Each layer follows a different set of rules, called protocol.

Some features of layering are:

- It reduces the design complexity.
- It prevents changes in one layer from affecting other layers thus,
- It provides flexibility of upgradation and reconfiguration.
- It makes standardization easy by defining what functions occur at each layer of the model.
- It divides the network communication process into smaller and simpler components, thus making it easy for design and troubleshooting.
- Since a complex system is broken down into smaller, more understandable parts and each smaller task can be handled by a specialist team.

1.4.2 Protocol Hierarchy

As we have already discussed that networks are organized as a series of layers, the name, number of the layers, the content of each layer and the function of each layer differ from network to network.

The purpose of each layer is to offer certain services to the higher layer. Layer **n** on one machine (source) carries on a conversation with layer **n** on another machine (destination) through protocol. Figure below shows protocol hierarchy of a five layers network.

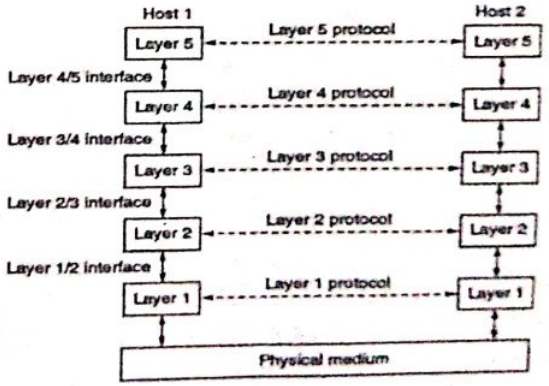


Figure 1.4: Layer, protocol and interface

The entities comprising the corresponding layers on different machines are called peers which communicate using protocols. The dotted line in the figure shows the virtual communication and the solid line represents the physical connection.

The actual transfer of data takes place from upper layer to lower layer at the source side and goes through the physical medium and from lower layer to upper layer at destination. There is an interface between each pair of adjacent layers which defines primitive operation and services the lower layer offers to the upper layer. A list of protocols used by a certain system, one protocol per layer is called a protocol stack.

Virtual Communication Between Layers:

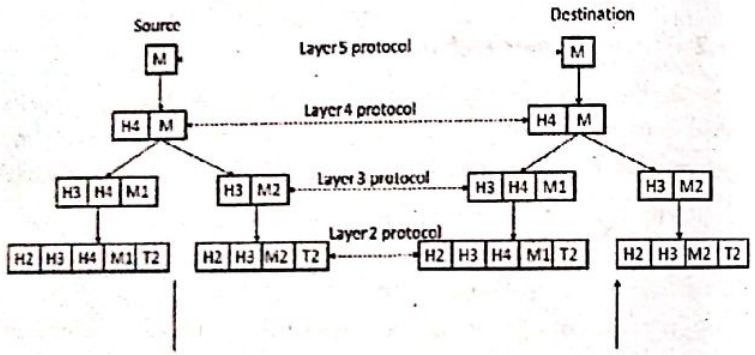


Figure 1.5: Information flow supporting virtual communication.

- **Step 1:** A message M is produced by layer 5 of the source machine and is sent to layer 4 for transmission.
- **Step 2:** Layer 4 adds a header that contains control information and is passed to layer 3.
- **Step 3:** Layer 3 breaks up the incoming message into small units, packets and appends a layer 3 header to each packet (M1 and M2).
- **Step 4:** Layer 2 adds header as well as trailer to each packet obtained from layer 2 and handover to layer 1 for physical transmission.

1.4.3 Design Issues for the layers

Some of the design issues for the layering are:

- **Addressing:** For every layer, it is necessary to have a mechanism for identifying senders and receivers. Since there are multiple possible destinations, some form of addressing is required in order to specify a specific destination.
- **Direction of transmission:** Based on whether the system communicates only in one direction of both, communication systems are classified as simplex, half duplex and full duplex systems.
- **Error Control:** Error controls and detection both are essential since physical communication circuits are not perfect. The receiver must have some ways of telling the sender which messages have been correctly received and which are not.
- **Flow Control:** All communication channels cannot preserve the order in which messages are sent on it. So, some kind of coordination must be maintained to keep a fast sender from overwhelming a slow receiver with data.
- **Multiplexing:** Multiplexing and demultiplexing is to be used to share the same channel by many sources simultaneously. It can be used for any layers. It is mostly needed in the physical layer, where all the traffic has to be sent over few physical circuits.
- **Routing:** When there are multiple paths between source and destination, a proper route should be chosen. Routing is used to find the best path in each network.

1.5 OSI Model and TCP/IP Model

1.5.1 OSI Model

International Standard Organization (ISO) has developed a referenced model for network design in 1977 commonly known as *Open Systems Interconnection*. This model is a set of guidelines that application developers can use to create and implement applications.

It proposed a seven-layer architecture which describes how the information from a software application in one computer moves through a network medium to a software application in another computer. The layers in the OSI reference model are divided into two groups. The top three layers define how the applications within the end stations will communicate with each other and with users. The bottom four layers define how data is transmitted end to end.

It is to be noted that OSI model itself is not a network architecture because it does not specify the exact services and protocols to be used in each layer. It just tells what each layer should do.

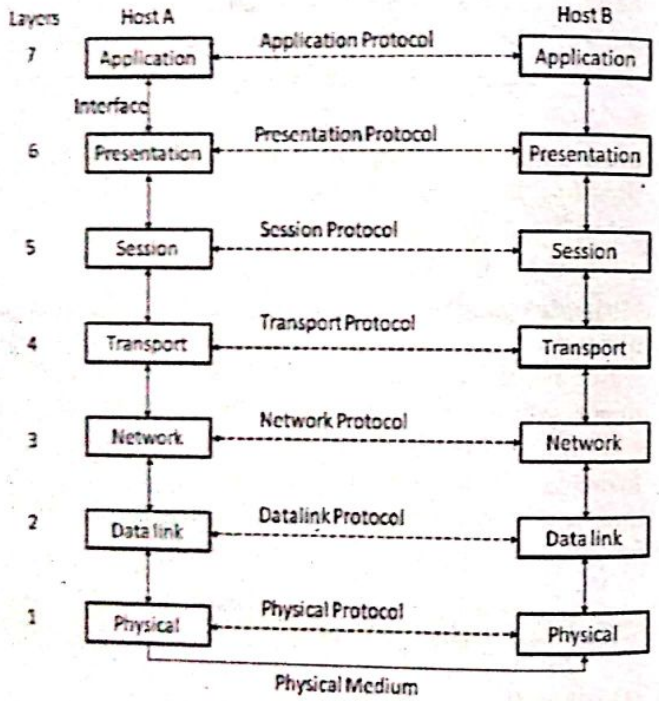


Figure 1.6: OSI model

Layer 1: Physical Layer

- *Physical layer* is concerned with the transmission of raw data bits over communication lines. The layer is implemented in the hardware of the networking device. It specifies wire and connectors for the system to connect. This layer is concerned with characteristic issues of the physical media, connectors, the type of modulation being used.

Layer 2: Data Link Layer

- *Data link layer* provides a direct link control on the network. This layer is concerned with the reliable transfer of data over the communication channel provided by the physical layer. Data link layer breaks the data into data frames, transmits the frames sequentially over the channel and checks for transmission error. It also does physical addressing and controls the flow and error.

Layer 3: Network Layer

- *Network layer* determines the best path for data transmission. It provides routing and related functions that enable multiple data links to be combined into an internetwork. Some functions of the network layer are: routing and forwarding, packet handling and maintaining routing information. It does network addressing and data transmission between the subnets.

Layer 4: Transport Layer

- *Transport layer* manages end to end connection. It accepts data from the above layer, splits it up into smaller units and passes these to lower layers isolating from each other. It manages end to end connection and data delivery between two hosts. It provides flow control, congestion control and also provides sequencing.

Layer 5: Session Layer

- *Session layer* allows users on different machines to establish sessions between them. It includes setting of various communication parameters like synchronization, dialog control. It determines the beginning, middle and end of session conversation.

Layer 6: Presentation Layer

- *Presentation layer* selects data structure, provides data transfer syntax and semantics. It maintains the format of

data and ensures the ... It involves data compression, decompression, encryption, decryption, etc.

Layer 7: Application Layer

- *Application layer* provides an interface between host communication software and any external application. It provides standards for supporting a variety of application independent services e.g., message handling system standards used for electronic mail, virtual terminal standards to allow applications to communicate with different terminals, file transfer and access between different systems.

1.5.2 TCP/IP Model

TCP/IP stands for *Transmission Control Protocol and Internet Protocol*, this model was earlier used by ARPANET (Advanced Research Project Agency) and later used by the Internet.TCP/IP defines how to use the network to transmit an IP datagram. The main goal of TCP/IP is to build an interconnection of networks referred to as an Internet that provide universal communication services over heterogeneous physical networks.

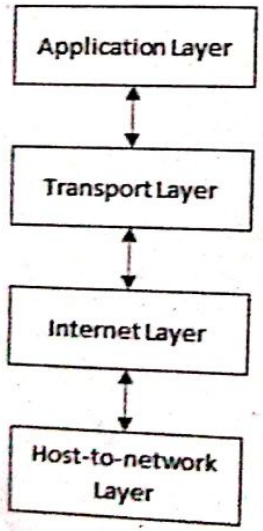


Figure 1.7: TCP/IP model

Layer 1: Host-to-Network Layer

- It is the lowest layer of TCP/IP model. This layer is also known as *network access layer*. A suitable protocol is used to connect to the host so that the packets can be sent over it.

Layer 2: Internet Layer

- This layer provides services that are roughly equivalent to the OSI network layer. The task is to allow the host to insert packets into any network and make them travel independently to the destination. This layer holds the whole architecture together. This layer defines the packet format and a protocol known as IP (Internet Protocol).

Layer 3: Transport Layer

- *Transport layer* is designed to allow devices or peers on the source and destination hosts to carry on a conversation, just as the OSI transport layer. It carries out functions such as multiplexing, segmenting or splitting into the data. It chooses a data transmission medium either parallel path or a single path. It also adds header information to the data and breaks the message into small units so that they are handled more efficiently by the network layer.

  Two protocols are defined in this layer: *TCP (Transmission Control Protocol)* and *UDP (User Datagram Protocol)*.TCP is a reliable connection oriented protocol which is used when the application wants accurate delivery. UDP is an unreliable connection protocol used for applications which do not want TCP's sequencing, flow control. UDP is used where prompt delivery is preferred rather than accurate delivery.

Layer 4: Application Layer

- This layer includes the OSI session, presentation and application layers of OSI model. The application layer uses higher-level protocol where users typically interact with the network. There are different application layer protocols in TCP/IP, including Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) used for email, Hyper Text

Transfer Protocol (HTTP) used for the World-Wide-Web and File Transfer Protocol (FTP) as they are required.

1.5.3 Comparison Between OSI Model & TCP/IP Model

Table 1.1: Comparison between OSI model and TCP/IP model

OSI Model	TCP/IP Model
1. It is seven-layered reference model.	1. It is four-layered model.
2. Internetworking is not supported.	2. TCP/IP supports internet working.
3. It clearly distinguishes between services, interfaces and protocols.	3. This model fails to distinguish between services, interfaces and protocols.
4. Network layer provides both connectionless and connection-oriented services.	4. The Internet layer provides connectionless service.
5. Transport layer provides only connection-oriented service.	5. Transport layer provides both connection-oriented and connectionless service.
6. Protocols in the OSI model are better hidden and can be replaced relatively easily.	6. Protocols in TCP/IP are not hidden and thus cannot be replaced easily.

1.5.4 Data Encapsulation

Data encapsulation is the process of adding header to wrap data. When a host transmits data across a network to another device, the data goes through encapsulation. Data is wrapped with protocol information at each layer of the OSI model. Each layer uses Protocol Data Units (PDUs) to communicate and exchange information. Each PDU is attached to the data by encapsulating it at each layer of the OSI model, and each has a specific name depending on the information provided in each header. This figure demonstrates how the upper-layer user data is converted for transmission on the network.

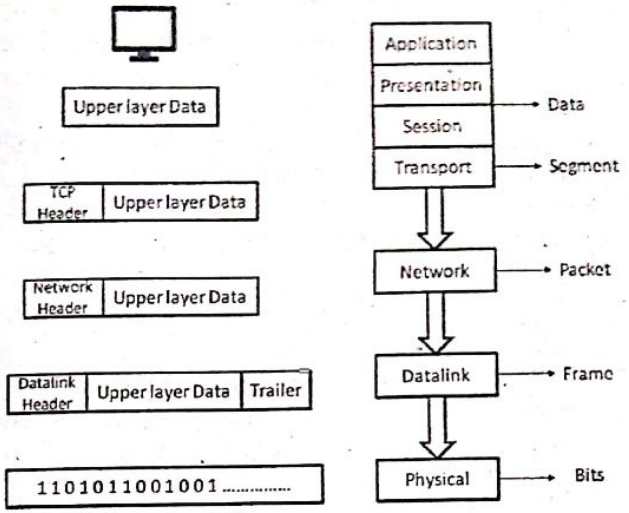


Figure 1.8: Data encapsulation

There are five steps of data encapsulation involved in the OSI reference model.

- The application, presentation and session layer create data from the user's input.
- Transport layer converts data to segments
- Network layer converts segments to packets
- Data link layer converts packets to frames.
- Physical layer converts frames to bits

1.6 Example Network: The Internet, X.25, Frame Relay, Ethernet, VoIP, NGN and MPLS, xDSL

1.6.1 The Internet

The Internet is the global system where different computer networks are connected and use the Internet protocol suite (TCP/IP) to link billions of devices worldwide. The Internet carries a wide range and variety of information resources and services. The Internet also has enabled and accelerated new forms of personal interactions through instant messaging, Internet

forums, and social networking. The Internet has no centralized governance (not exact protocol or standards) in either technological implementation or policies for access and usage; each constituent network sets its own policies. Only the overreaching definitions of the two principal name spaces on the Internet, the Internet Protocol address space and the Domain Name System (DNS), are provided by a maintainer organization, the Internet Corporation for Assigned Names and Numbers (ICANN).

1.6.2 X.25

X.25 is an ITU-T standard protocol which defines the way in which packets travel in a packet switched wide area network (WAN) communication. It was developed in the 1970s for providing an interface between public switched networks and their customers. AN X.25 is a connection-oriented service and supports virtual circuit switching.

An X.25 WAN consists of packet-switching exchange (PSE) nodes and different types of networking hardware, plain old telephone service connections or ISDN connections as physical links. X.25 network handles the combination of packets at the source device, delivery, and then dis-assembly at the destination. X.25 packet delivery technology includes error checking and retransmission logic should delivery failures occur along with the switching and network layer routing. It also supports multiple simultaneous conversations by multiplexing packets and using virtual communication channels.

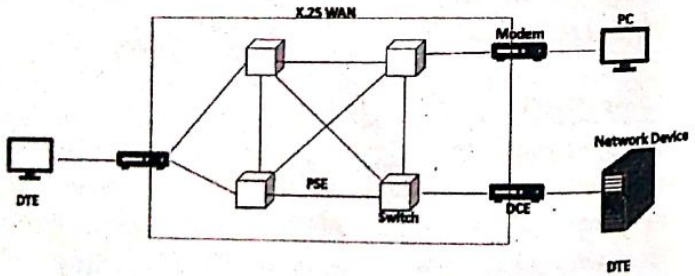


Figure 1.9: X.25 network

X.25 protocol suite maps to the lowest three layers of the OSI reference model: physical layer, frame layer, and packet layer.

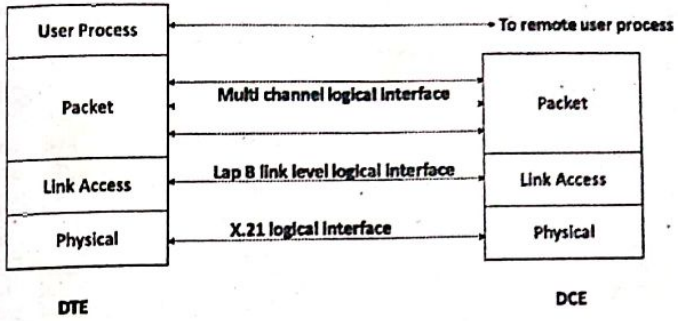


Figure 1.10: X.25 layer mapping with OSI model

- **Physical layer:** this layer takes care of the interface between a computer terminal and link which attaches it to the packet switching node.
- **Link Access layer:** In this layer, X.25 specifies the link access procedure-B which is a subset of HDLC protocol.
- **Packet layer:** This layer is responsible for end-to-end connection between two DTEs.

Advantages of X.25:

1. Frame delivery is more reliable.
2. Frames are delivered in order
3. Retransmission of frames is possible.
4. X.25 supports switched virtual circuits and permanent circuits.

Disadvantage:

1. X.25 is much slower than frame relay.

1.6.3 Frame Relay

Frame relay is a high-performance WAN protocol that provides LAN to LAN connectivity. It is connection-oriented services that operates at the physical and logical link layers. Frame relay was developed for taking advantage of the high data rates and low error rates in the modern communication system. It

operates at a high speed (1.544 Mbps to 44.376 Mbps). Frame relay can only detect error and the damaged frames detected are simply dropped.

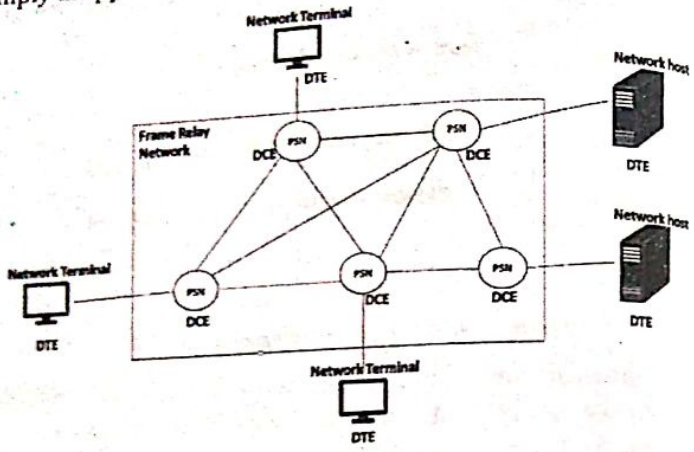


Figure 1.11: Frame relay network

Devices attached to a Frame Relay WAN fall into two categories: Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE). DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of a customer. In fact, they may be owned by the customer. Examples of DTE devices are terminals, personal computers, routers, and bridges. DCEs are carrier-owned internetworking devices. The purpose of DCE equipment is to provide clocking and switching services in a network, which are the devices that actually transmit data through the WAN. In most cases, these are packet switches.

Frame relay provides connection-oriented data link layer communication. This means that a defined communication exists between each pair of devices and that these connections are associated with a connection identifier. This service is implemented by using a Frame relay virtual circuit, which is a logical connection created between two data terminal equipment (DTE) devices across a frame relay packet-switched network (PSN). Frame relay virtual circuits are identified by data-link

connection identifiers (DLCIs). DLCI values typically are assigned by the frame relay service provider (for example, the telephone company).

Advantages :

1. Higher data rates (1.544 Mbps to 44.376 Mbps).
2. It allows transfer of bursty data
3. It has lower overheads so lower delay.
4. It reduces internetworking cost.

1.6.4 Ethernet

Ethernet is a network technology used in LANs and MANs. It is the most widely used for local area network (LAN) technology. Ethernet is a link layer protocol in the TCP/IP stack, describing how networked devices should format data for efficient transmission between other network devices on the same network segment, and how to put that data out on the network connection.

1.6.5 VoIP

Voice Over Internet Protocol (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet protocol (IP) networks, such as the Internet. Voice signals are converted to packets of data, which are transmitted on shared, public lines, hence avoiding the tolls of the traditional, public switched telephone network (PSTN). Other terms commonly associated with VoIP are IP telephony, Internet telephony, broadband telephony, and broadband phone service.

1.6.6 NGN

A *next-generation network (NGN)* is a packet-based network able to provide telecommunication services to users and able to make use of multiple broad bands, QoS-enabled transport technologies and in which service-related functions are independent of the underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

1.6.7 MPLS

Multiprotocol Label Switching (MPLS) is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows. The labels identify virtual links (*paths*) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence the "multiprotocol" reference on its name. MPLS supports a range of access technologies, including T1/E1, ATM, frame relay, and DSL.

MPLS is scalable and protocol-independent. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol.

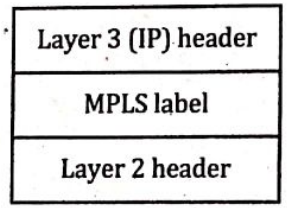


Figure 1.12: MPLS label

MPLS operates at a layer that is generally considered to lie between traditional definitions of OSI layer 2 (data link layer) and layer 3 (network layer), and thus is often referred to as a *layer 2.5* protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model.

1.6.8 xDSL

Digital subscriber line (DSL; originally digital subscriber loop) is a family of technologies that are used to transmit digital data over telephone lines. DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations. In telecommunications marketing, the term DSL is widely understood to mean asymmetric digital subscriber line (ADSL), the most commonly installed DSL technology, for Internet access. The bit rate of consumer DSL services typically ranges from 256 kbit/s to over 100 Mbit/s in the direction of the customer (downstream), depending on DSL technology, line conditions, and service-level implementation.

xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS) and both require the short runs to a central telephone office (usually less than 20,000 feet). However, xDSL offers much higher speeds - up to 32 Mbps for upstream traffic, and from 32 Kbps to over 1 Mbps for downstream traffic.

CHAPTER – 2

PHYSICAL LAYER

2.1 Introduction

Physical layer is the lowest layer of OSI model that communicates directly with the various types of actual communication media. This layer is responsible for sending and receiving bits from one device to another.

The physical layer specifies the electrical, mechanical, procedural and functional requirements for activating, and deactivating a physical link between end systems. This layer is not connected with the meaning of the bits but deals with the physical connection to the network, with transmission and reception of signals. It specifies interface characteristics such as binary voltage levels, encoding methods, data transfer rates, modes of transmission.

2.2 Network Monitoring

Network performance is an important issue in data and computer networking. Various factors are to be considered to monitor the network.

1. **Bandwidth**

   Bandwidth is the amount of data that passes through a network connection over time as measured in bits per second. It is the data rate supported by a network connection or interface. It represents the overall capacity of the connection.

2. **Latency**

   Latency is an expression of how much time it takes for a packet of data to travel from one node to another. Total latency of a network is one-way latency from source to destination plus the one-way latency from the destination back to the source.

3. **Throughput**

   Throughput is the average rate of successful messages that a communication channel can deliver over a communication period. Its measuring unit is bits/second (bps), megabits per second (Mbps) or gigabits per second (Gbps)

4. **Delay**

   The *delay* of a network specifies how long it takes for a bit of data to travel across the network from one node (host or router) or endpoint to another. When a packet travels from one node to the subsequent node along the path, it suffers from several types of delays at each and every node along the paths like Nodal processing delays /Processing Delays, delay in Queuing, Transmission delay and delay in Propagation.

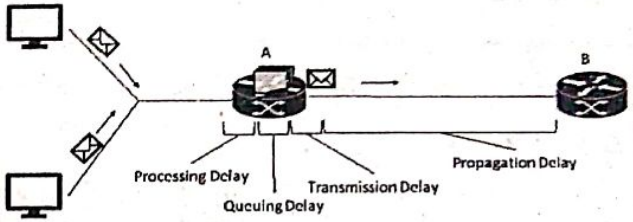


Figure 2.1: Delays in router A

- **Processing delay:** The time required to examine the packet header and determine where to direct the packet.
- **Queuing delay:** At the queue, the packets experience a queuing delay, when they wait to transmit on the links.
- **Transmission delay:** It is also called store and forward delay. The packets are transmitted on the first come first served basis. It is the time required to transmit all the packets bits into the link.
- **Propagation delay:** The time required for the packets bits to reach from the beginning of the link to the desired router is propagation delay.

2.3 Transmission Media

A *transmission medium* can be broadly defined as anything that can carry information from source to destination. It is located below the physical layer and is directly controlled by the physical layer. Transmission media can be divided into two broad categories:

i. Guided transmission media

ii. Unguided transmission media

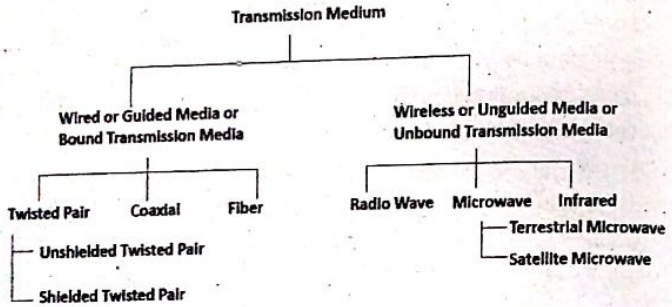


Figure 2.2: Transmission media

2.3.1 Guided Media

With guided media, the waves are guided along a solid medium, such as a fiber-optic cable, a twisted-pair copper wire or a coaxial cable. Transmission capacity (bandwidth and data rate) depends on distance and type of network. Guided media is also referred to as *wired* or *bounded transmission media*.

Features:

- High speed
- Secure
- Used for comparatively shorter distances

There are three major types of guided media:

1. Twisted Pair Cables

Twisted pair cable is the least expensive and most widely used media. Twisted pair cable is constructed of two insulated copper wires arranged in a regular spiral pattern. Number of pairs

are bundled together in a cable contained by a common jacket. Twisting of wires decreases the crosstalk between adjacent pairs in the cable and reduces the sensitivity to outside EMI.

Applications:

- Most common transmission media for digital and analog signals.
- Used in telephone networks between house and local exchange (subscriber loop)
- Used for communications within the building.

Transmission characteristics:

- Requires amplifiers every 5-6 km for analog signal
- Requires repeaters every 2-3 km for digital signals
- Susceptible to interference and noise.
- Interference can be reduced by shielding with metallic braids.
- Different twist length in adjacent pairs reduces crosstalk.

Advantages:

- Protect against cross talk & interference
- Easy to work with
- Easy to add computers to network
- Well understood technology
- Less expensive

Disadvantages:

- Susceptibility to noise
- Least secure
- Distance limitations – short range
- Low data rate
- Requires more expensive hubs

There are two types of twisted pair cables:

i. Unshielded Twisted Pair (UTP)

UTP contains no shielding and is more susceptible to external noise but is the most frequently used because of its least cost and easy installation.

Figure 2.3: Unshielded twisted pair cable

Applications:

- In ordinary telephone lines to carry voice and data channels.
- In the DSL lines
- In LANs

Advantages:

- Least expensive
- Easy to install

Disadvantages:

- Susceptible to external interference
- Lower capacity and performance
- Short distance transmission due to attenuation

ii. Shielded Twisted Pair (STP)

STP cable contains an outer conductive shield that is electrically grounded to insulate the signals from external electrical noise. STP also uses inner foil shields to protect each wire pair from noise generated by the other pairs. It is used in rapid data rate Ethernet, in voice and data channels of telephone lines.

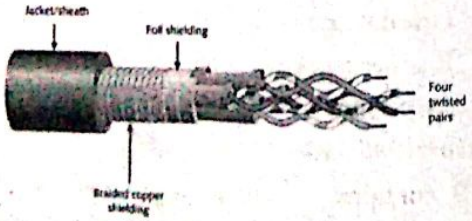


Figure 2.4: Shielded twisted pair cable

Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster

Disadvantages:

- Comparatively difficult to install and manufacture
- More expensive
- Bulky

2. Coaxial Cable

Coaxial cable consists of two conductors, but is constructed differently to permit it to operate over a wider range of frequencies. It has a central core conductor of solid enclosed in an insulating sheath, which is then encased in an outer conductor of metal foil, braid or combination of the two. The outer metallic wrapping acts as a shield against noise and as the second conductor. The outer conductor is covered with a jacket or shield.

A single coaxial cable has a diameter of from 1 to 2.5 cm. Coaxial cable can be used over longer distances and support more stations on a shared line than twisted pair.

Coaxial cable is a versatile transmission medium, used in a wide variety of applications, including:

- Television distribution - aerial to TV & CATV systems
- Long-distance telephone transmission - traditionally used for inter-exchange links, now being replaced by optical fiber/microwave/satellite
- Short-run computer system links

Figure 2.5: Coaxial cable

Applications:

- Television distribution
- Long-distance telephone transmission
- Short-run computer system links
- Local area networks

Advantages:

- Can support higher frequencies and data rates.
- Better noise Immunity
- Easy to install and expand
- Inexpensive

3. Optical Fiber Cable

Optical fiber is a thin glass or plastic cable used to guide light rays. It has a circular cross section with a diameter of only a fraction of a centimeter. A light source is placed at the end of the fiber, and light passes through it and exits at the other end of the cable.

Optical fiber consists of three parts namely core, cladding and jacket. The core is the innermost section of the fibre which may be one or more very thin strands or fibers. The cladding is a plastic or glass coating with optical properties different from core. The jacket is the outermost layer surrounding one or more claddings.

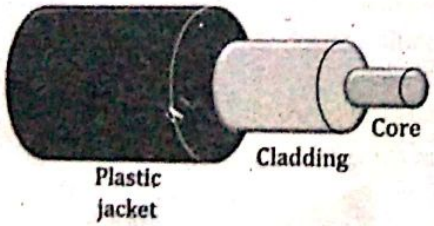


Figure 2.6: Optical fiber cable

Optical fibers use reflection to guide light through a channel. When light rays strike a reflective surface, such as a mirror, the light waves are thrown back or reflected. When light passes from denser medium to rarer medium, it bends away from the normal at the point of incidence. If the angle of incidence is greater than critical angle, the light ray will be reflected from the interface. When the light ray strikes the interface at an angle greater than the critical angle, the light ray does not pass through the interface into the glass and is reflected off the surface of the fiber cable. This action is known as Total Internal Reflection. The light ray bounces back and forth between the surfaces until it exits at the other end of the cable. This is the basic principle that allows an optical fiber cable.

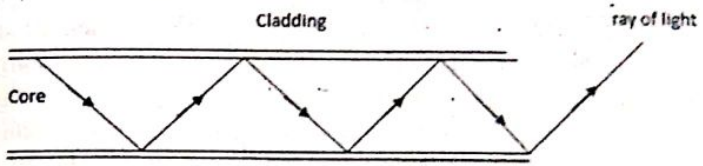


Figure 2.7: Total internal reflection in optical fiber

To transmit high-speed digital pulses, a very fast light source must be used. The two most commonly used light sources are light- emitting diode (LED) and Injection Laser Diode (ILD). LED is a PN-junction semiconductor device that emits light when forward-biased. It is cheaper and works over a greater temperature range. It has a longer operational life. ILD are capable of developing light power up to several watts. they are far more powerful than LEDs and therefore are capable of transmitting over much longer distances.

Optical Fiber Cable Types

Optical fibers are available in two varieties: single mode fiber optic cable and multimode optical fiber.

i. Single Mode Fiber

Single mode fiber has a smaller core diameter of 10 microns. It can transfer data for a longer distance without the help of a repeater and has high bandwidth. It allows a single wavelength and pathway for light to travel, which greatly decreases light reflection and lowers attenuation.

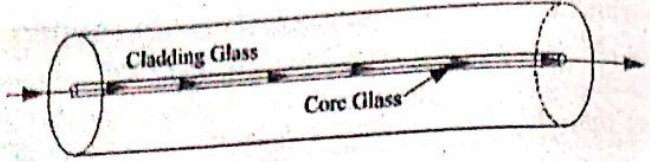


Figure 2.8: Single mode fiber

ii. Multimode Fiber

Multimode optical fiber contains a core with a larger diameter than that of single mode fiber optic cable, which allows multiple pathways and several wavelengths of light to be transmitted. Multimode optical fiber is available in two sizes, 50 microns and 62.5 microns. It is commonly used for short distances applications such as fiber to the desktop or patch panel to equipment, data and audio/video applications in LANs. Multimode fiber can be divided into two types: step index multimode and graded index fiber.

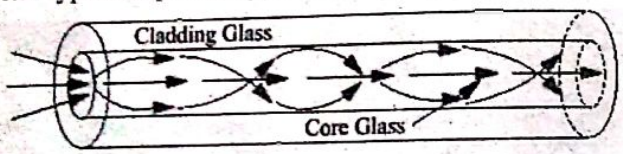


Figure 2.9: Multimode fiber

Applications:

- Used in cable TV networks.
- Used in backbone network (can transfer data rates of 1600 Gbps)
- Used in Fast Ethernet networks (can support hundreds of stations) The refractive index of the core is greater than that of the cladding.

Advantages:

- High data rate and wide bandwidth
- Immunity to electromagnetic interference and lightning damage
- Low attenuation (data loss)
- Longer distance 2 to 5 km with Multimode fiber or over 25 km with Single Mode fiber

- Small cable diameter fits anywhere
- Light weight
- No sparks if cut
- No shock hazard
- Secure communications
- Low system cost
- Longer life expectancy than copper or coaxial cable
- Cabling of the future

Disadvantages:

- Expensive- installation, testing and maintenance equipments are costly
- Difficult to install
- Fibers are not mechanically robust as copper wire
- Require two cables to transmit & receive data
- Require special connections, joining fibers can be more difficult & expensive
- Requires expert manpower

Comparison Between Twisted Pair, Co-axial and Optical Fiber cable

Table 2.1: Comparison between twisted pair, co-axial and optical fiber cable

Twisted Pair Cable	Coaxial Cable	Optical Fiber
Transmission of signals takes place in the electrical form over the metallic conducting wires.	Transmission of signals takes place in the electrical form over the inner conductor of the cable.	Signal transmission takes place in an optical form over a glass fiber.
Noise immunity is low. Therefore, more distortion.	Higher noise immunity than the twisted pair cable due to presence of shielding conductor.	Highest noise immunity as the light rays is unaffected by the electrical noise.

Twisted Pair Cable	Coaxial Cable	Optical Fiber
Affected due to an external magnetic field.	Less affected due to external magnetic fields.	Not affected by the external magnetic field.
Short circuit between the two conductors is possible.	Short circuit between the two conductors is possible.	Short circuit is not possible.
Cheapest	Moderately expensive.	Expensive than other cable.
Low bandwidth	Moderately high bandwidth.	Very high bandwidth
Power loss due to conduction and radiation.	Power loss due to conduction.	Power loss due to absorption, scattering, dispersion and bending.

2.3.2 Unguided Media

With an *unguided media*, the waves propagate in the atmosphere and in outer space. Unguided media is also referred to as wireless or unbounded transmission media which provide a means for transmitting electromagnetic waves but do not guide them.

In wireless transmission, a RF signal generated by a transmitter is sent into space and eventually picked up by a receiver. Transmission and reception are obtained by means of an antenna. Antenna is an electrical conductor used to radiate electromagnetic energy or collect EM energy.

Unguided media includes radio waves, microwave, and infrared.

1. Radio Waves

Radio waves are the electromagnetic waves but operate at radio frequency range. Area covered by a communication system that operates in radio frequency depends on the power of the transmitter. Radio waves use omnidirectional antennas that send out signals in all directions. The range in frequencies of radio waves is from 3KHz to 1 GHz. In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.

Applications of radio waves:

- Radio waves are useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

2. Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called *microwaves*. Microwaves are unidirectional and microwave propagation is a line of sight i.e., the sending and receiving antennas need to be properly aligned with each other. These waves are mainly used for mobile phone communication and television distribution.

Characteristics of Microwave:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- **Short distance:** It is inexpensive for short distances.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Microwaves links are categorized into two types:

- Terrestrial microwave link
- Satellite microwave link

a. Terrestrial Microwave Link

Terrestrial microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to

another. Terrestrial microwave communication is used extensively in situations when physical transmission media is impractical or difficult to install, for example between high buildings, across rivers, mountains and remote stations. Terrestrial Microwave systems use directional parabolic antennas to transmit and receive signals. Microwave transmission is line of sight.

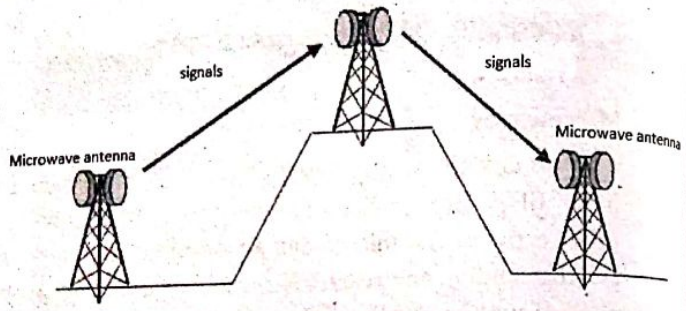


Figure 2.10: Terrestrial microwave link

Applications:

- Long haul telecom service
- Transmission between high buildings, across rivers, mountains and remote stations.

Transmission Characteristics:

- Frequencies in the range of 4-6 GHz and 21 to 23 GHz
- Higher frequency implies higher bandwidth leading to higher data rates
- Repeaters may be placed further apart compared to coaxial cable
- Attenuation is affected by antenna size, signal strength, frequency and atmospheric conditions; may increase with rainfall, especially above 10 GHz.

b. Satellite Microwave Link

Communication satellite is a microwave relay station between two or more ground stations (also called earth stations). An earth station transmits information to the

satellite. The satellite contains a receiver that picks up the transmitted signal, amplifies it and translates it on another frequency. The signal on the new frequency is then transmitted to the receiving stations on earth. The original signal being transmitted from the earth station to the satellite is called the uplink, and the transmitted signal from the satellite to the receiving stations is called the downlink. Usually the downlink frequency is lower than the uplink frequency. Satellites use different frequency bands for incoming (uplink) and outgoing (downlink) data. A single satellite can operate on a number of frequency bands, known as transponder channels or transponders.

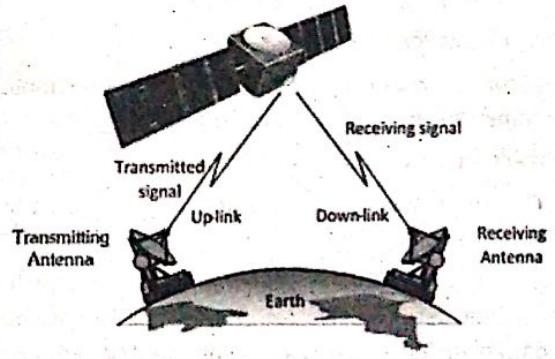


Figure 2.11: Satellite microwave link

Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems. We can communicate with any point on the globe by using satellite communication.

Applications:

- Main application is in communication.
- Communication satellites is in long-distance telephone service,
- Also used in TV, private business networks
- VSAT – Very small aperture terminals
- Used in surveillance and navigation.

Advantages of satellite microwave communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.

Disadvantages of satellite microwave communication:

- Satellite designing and development requires more time and higher cost.
- The satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

3. Infrared Waves

An infrared wave transmission is a wireless technology used for communication over short ranges.

Characteristics:

- The frequency of the infrared waves is in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.
- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.
- Limited to short distances and highly directional

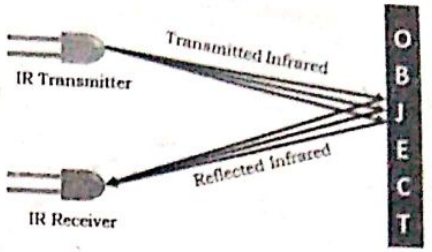


Figure 2.12: Infrared communication

Applications:

- Remote control of electronic devices at home.
- Communication between keyboards, mouse, etc.

Propagation Methods

Wireless propagation is possible in many ways:

1. Ground Wave Propagation

In *ground wave propagation*, radio waves travel through the lowest portion of the atmosphere. These are low frequency signals that radiate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal.

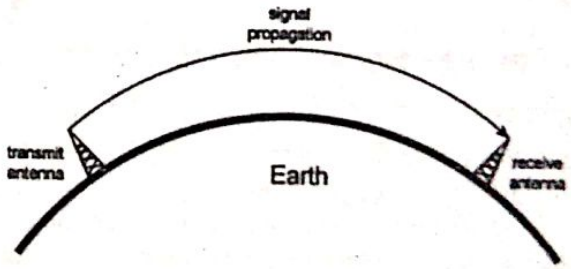


Figure 2.13: Ground wave propagation (below 2 MHz)

2. Sky Wave Propagation

In *sky wave propagation*, higher frequency radio waves radiate upward into the ionosphere where they reflect back to earth. This type of transmission allows for greater distances with lower output power.

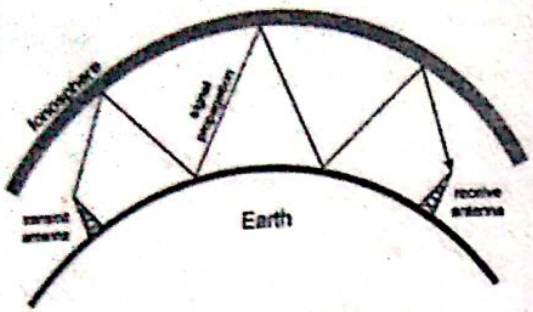


Figure 2.14: Sky wave propagation (2-30 MHz)

3. Line-of-Sight Propagation

In *line-of-sight propagation*, very high-frequency signals are transmitted in a straight line. The communicating antennas must be placed in such a way that they see each other in earth's curvature. Distance of signal propagation is limited to the curvature of the Earth.

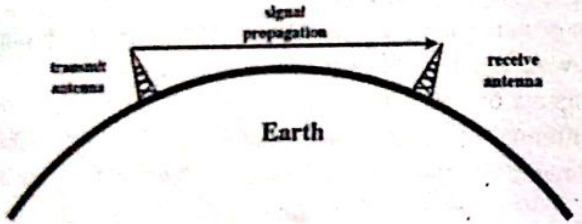


Figure 2.15: Line-of-sight propagation (above 30 MHz)

2.3.3 Satellite

A *satellite* is a physical object that revolves around the earth at a known height. It is placed in earth orbit for the purpose of communicating, weather forecast, research, military purpose, etc. The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

The transmitter-receiver combination in the satellite is known as a transponder. The basic functions of transponder are amplification and frequency translation. Transponders are wide bandwidth units so that they can receive and retransmit more than one signal. Satellites consist of transponders that gather

signals over a range of uplink frequencies and re-transmits them on a different set of downlink frequencies to receivers on Earth, often without changing the content of the received signal.

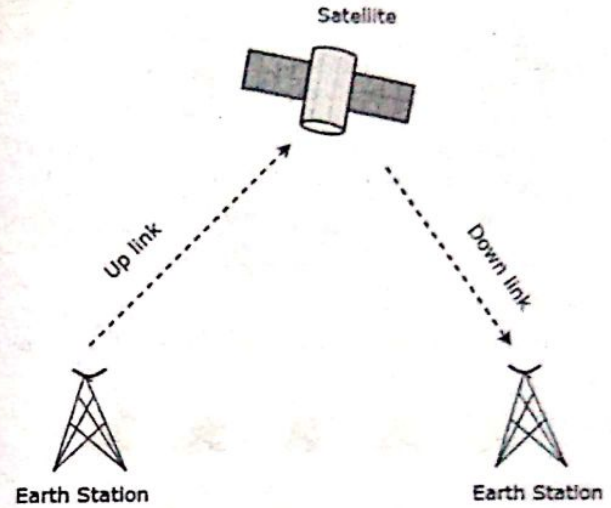


Figure 2.16: Satellite communication

Uplink frequency is the frequency at which, earth station is communicating with satellites. The satellite transponder converts this signal into another frequency and sends it down to the other earth station. This frequency is called *downlink frequency*. The process of satellite communication begins at an earth station. Here, an installation is designed to transmit and receive signals from a satellite in an orbit around the earth. Earth stations send the information to satellites in the form of high powered, high frequency (GHz range) signals.

Frequency Bands Used in Satellite Communication

Most communication satellites operate in the microwave frequency spectrum. The microwave spectrum is divided up into frequency bands that have been allocated to satellites as well as other communication services such as radar. These frequency bands are designated by letters of alphabets. Figure shows the various frequency bands used in satellite communication.

Table 2.2: Frequency bands used in satellite communication

Band	Frequency (GHz)
L Band	1-2
S Band	2-4
C Band	4-8
X Band	8-12
Ku Band	12-18
K Band	18-27
Ka Band	27-40
V Band	40-75
W Band	75-110

Types of Satellites

Satellites are classified based on the altitude of orbit as:

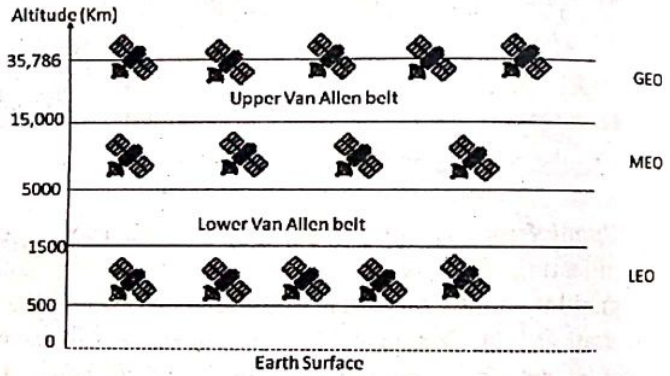


Figure 2.17: Types of satellites

1. **LEO (Low Earth Orbit) Satellites:** These satellites are kept below between 500 to 1500 Km. As the satellites are so close to the earth, the ground stations do not need much power, and the round-trip delay is only a few milliseconds. The footprint of LEO normally has a diameter of 8000Km. So, large numbers of satellites are needed for a complete system.
2. **MEO (Medium-Earth Orbit) Satellites:** MEO satellites are kept in the range of 5000 to 15000km. They take 6 to 8 hours to circle the earth depending on its orbit height above the earth surface. MEO satellites are mostly used for navigation and military services. The most common MEO satellite is a GPS satellite.
3. **GEO (Geostationary) Satellites:** GEO satellites have an almost distance of 36000 Km above the equatorial plane. They have a rotation period of 23hrs 56minutes and 4 sec. so they are stationary with respect to Earth. It takes a minimum of three satellites equidistant from each other to provide full global transmission.

Satellites may also be classified as:

- **Astronomical satellites:** These satellites are used for observation of distant planets, galaxies, and other outer space objects.
- **Biosatellites:** These satellites are designed to carry living organisms, generally for scientific experimentation.
- **Communication satellites:** These satellites are stationed in space for the purpose of telecommunications.
- **Earth observation satellites:** These satellites are intended for environmental monitoring, meteorology, map making, etc.
- **Navigational satellites:** These satellites use radio time signals transmitted to enable mobile receivers on the ground to determine their exact location.
- **Killer satellites:** These satellites are designed to destroy enemy warheads, satellites, and other space assets.

2.3.4 Switching

Switching is the process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it, is called *ingress* and when data leaves a port or goes out it is called *egress*. A communication system may include a number of switches and nodes.

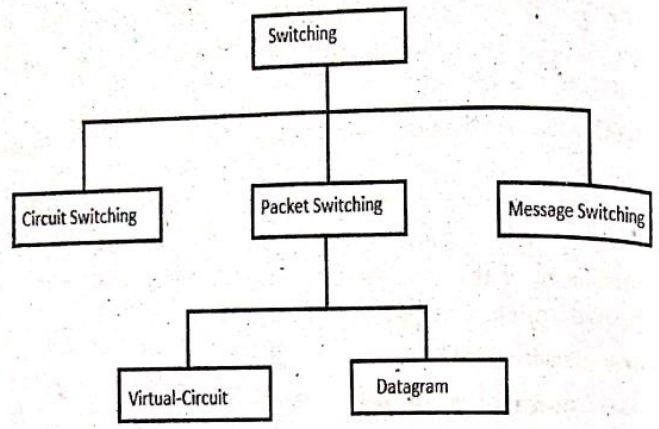


Figure 2.18: Switching Techniques

1. Circuit Switching

The most common example of circuit switching is in the Public Switched Telephone Network (PSTN). Here, a dedicated path is established between the source and the destination and then all the messages are sent over this route (Connection Oriented Switching).

In this networking method, a circuit (dedicated path) is set up between two devices which are used for the whole communication. The routing decision is made when there is set up across the network. After the link has been set up, the information is forwarded continuously over the link. The circuit switch network operated in three phases.

1. Set Up Phase
2. Data-transfer Phase
3. Terminate Phase

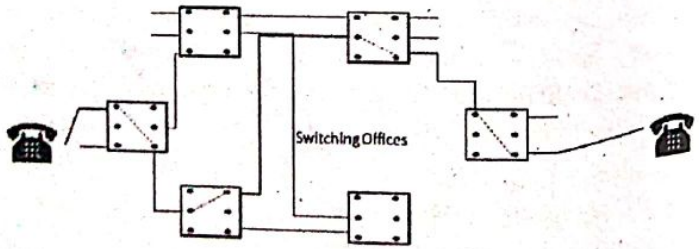


Figure 2.19: Circuit switching

2. Message Switching

Message switching is a switching technique in which a message is first received completely and is buffered until there are resources available to transfer it to the next hop. With this form of switching, no physical path is established in advance between sender and receiver. The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.

A network using this technique is called a store and forward network where each and every node stores the entire message and then forwards it . If the next hop is not having enough resource to accommodate a large size message, the message is stored and switch waits.

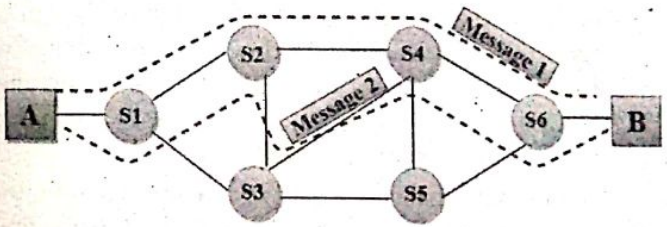


Figure 2.20: Message switching

Message switching is replaced by packet switching. Message switching has the following drawbacks:

- Every switch in the transit path needs enough storage to accommodate the entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

3. Packet switching

Packet switching is a switching technique where the message is divided and grouped into a number of units

called packets that are individually routed from the source to the destination. There is no resource allocation for a packet, resources are allocated on demand.

Two approaches:

a. Datagram Switching

In *datagram switching*, each packet is treated independently. Each packet in a packet switching technique has two parts: a header and a payload. The header contains the addressing information of the packet and is used by the intermediate routers to direct it towards its destination. The payload carries the actual data.

A packet is transmitted as soon as it is available in a node, based upon its header information. The packets of a message are not routed via the same path. So, the packets in the message arrive at the destination out of order. It is the responsibility of the destination to reorder the packets in order to retrieve the original message. The datagram networks are sometimes referred to as connectionless networks.

The process is diagrammatically represented in the following figure. Here the message comprises four packets, A, B, C and D, which may follow different routes from the sender to the receiver.

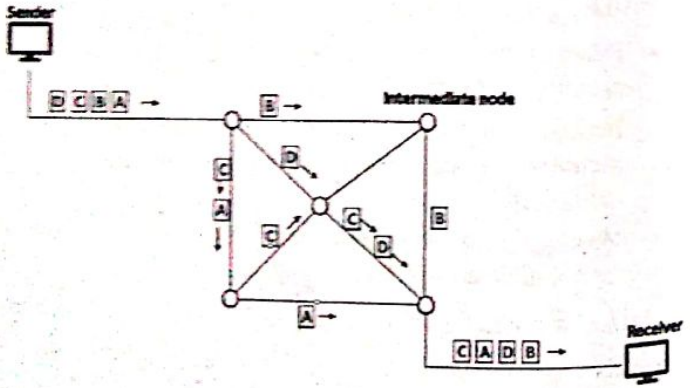


Figure 2.21: Datagram switching

b. Virtual Circuit Switching

A *virtual-circuit* network is a cross between circuit-switched network and a datagram network. A preplanned route is established before any packets are sent. Once the route is established, all the packets between a pair of communication parties follow the same path established during the connection. The route is same through the network. Because the route is fixed for the duration of the logical connection, it is somewhat similar to a circuit in a circuit switching network so referred as virtual circuit. It has some characteristics of both. As in a circuit-switched network, there are setup, data transfer and teardown phases. Resources can be allocated during the setup phase. As in a datagram network, data is packetized and each packet carries an address in the header.

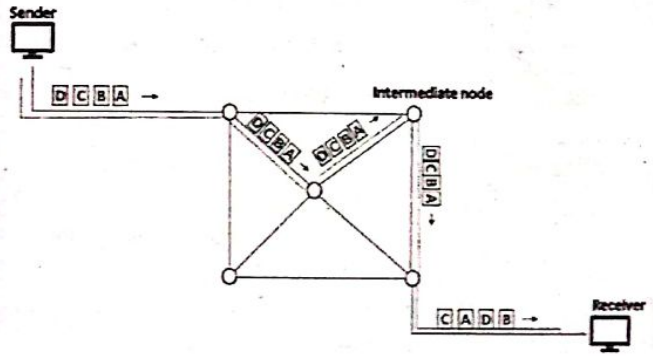


Figure 2.22: Virtual circuit establishment

An initial setup phase is used to set up a route between the intermediate nodes for all the packets passed during the session between the two end nodes. In each intermediate node, an entry is registered in a table to indicate the route for the connection that has been set up. Thus, packets passed through this route can have short headers containing only a virtual circuit identifier (VCI). A VCI is a small number used by a frame between two switches of nodes for data transfer between them. Each switch can use its own set of VCIs.

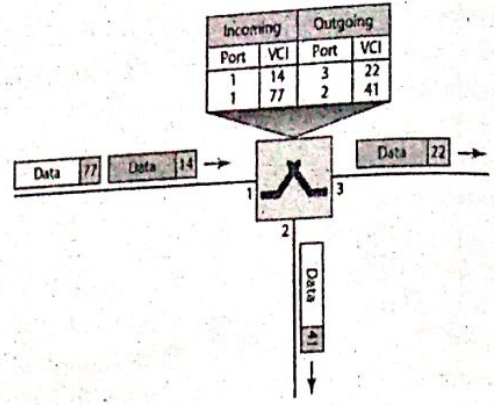


Figure 2.23: Data transfer using VCI through a switch

Types of Virtual Circuit

1. Permanent Virtual Circuit
2. Switched Virtual Circuit

Comparison Between Virtual Circuit and Datagram Approach

Table 2.3: Comparison between virtual circuit and datagram approach

Issue	Datagram Approach	Virtual-Circuit Approach
Circuit Setup	Not needed	Needed
Addressing	Each packet contains a full source and destination address.	Each packet contains a virtual circuit number.
Routing	Each packet is routed independently	Route is chosen when VC is set up and all packets follow it.
Effect of router failure	None, except for a packet lost during the crash.	All VCs that pass through failure routers are terminated.
Sate Information	Routers do not hold state information about connection.	Each VCs requires router table space per connection.
Quality of Service	Difficult to maintain.	Easy if enough resources are allocated.
Congestion control	Difficult to control	Easy if enough resources are allocated.

2.3.5 Telecommunication Switching System

Telecommunication switching system consists of a collection of switching elements arranged and controlled in such a way as to set up a common path between any two distant points electronic components. Figure below shows the classification of the switching system.

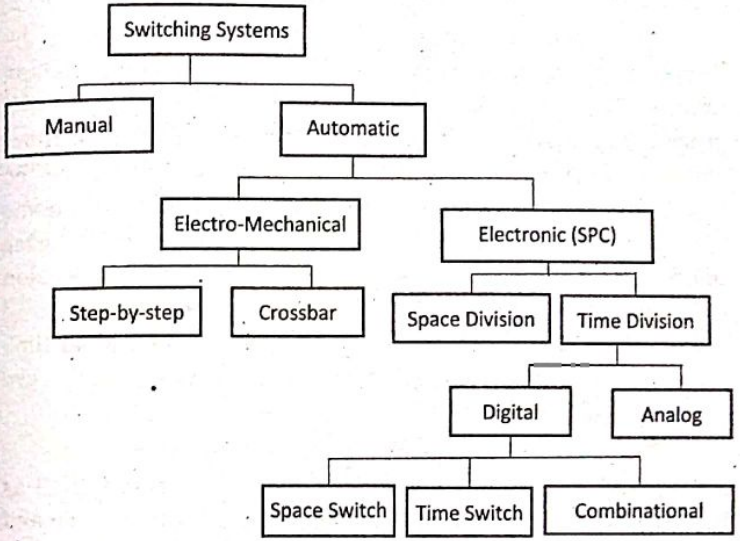


Figure 2.24: Telecommunication switching system

The switching system in the early stages were manual and were operated manually. The interconnection function was done by jacks by operators. Due to its limitation of operator dependence, manual switching was quickly replaced by an automatic switching system.

Automatic switching systems can be classified as electromechanical switching systems and electronic switching systems.

The Electromechanical switching systems are a combination of mechanical and electrical switching types. The electrical circuits and the mechanical relays are deployed in them. The Electromechanical switching systems are further classified step- by-step and crossbar switching systems. The Step-by-step

switching system is also called the Strowger switching system after its inventor A B Strowger. The control functions in a Strowger system are performed by circuits associated with the switching elements in the system. The Crossbar switching systems have hard-wired control subsystems which use relays and latches. These subsystems have limited capability and it is virtually impossible to modify them to provide additional functionalities.

The Electronic Switching systems are operated with the help of a processor or a computer which control the switching timings. The instructions are programmed and stored on a processor or computer that controls the operations. This method of storing the programs on a processor or computer is called the Stored Program Control (SPC) technology. The switching scheme used by the electronic switching systems may be either Space Division Switching or Time Division Switching. In space division switching, a dedicated path is established between the calling and the called subscribers for the entire duration of the call. In time division switching, sampled values of speech signals are transferred at fixed intervals.

The time division switching may be analog or digital. In analog switching, the sampled voltage levels are transmitted as they are. However, in binary switching, they are binary coded and transmitted. If the coded values are transferred during the same time interval from input to output, the technique is called Space Switching. If the values are stored and transferred to the output at a time interval, the technique is called Time Switching. A time division digital switch may also be designed by using a combination of space and time switching techniques.

2.3.6 Multiplexing

Multiplexing is a method where multiple message signals from different devices are combined into one single signal and transmitted over a shared medium. The multiplexing divides the transmission capacity of the single high-level communication channel into several low-level logical channels, one for transmission of each message signal or data stream. To extract the original signal on the receiver side a process called demultiplexing is done.

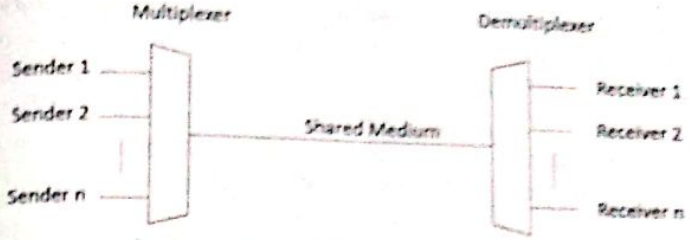


Figure 2.25: Multiplexing

There are different types of multiplexing:

1. **Frequency Division Multiplexing (FDM)**

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

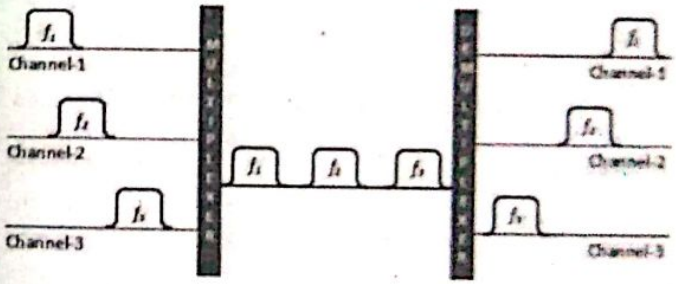


Figure 2.26: Frequency Division Multiplexing.

Applications:

- Used in AM radio broadcasting (530 to 1700 KHz band)
- Used in FM radio broadcasting (88 to 108 MHz band)
- Used in TV broadcasting
- Used in Cellular communication

2. **Time Division Multiplexing (TDM)**

   In *Time Division Multiplexing*, all the signals to be transmitted are not transmitted simultaneously. Instead,

Higher levels of multiplexing are used to generate further levels of the T-carrier hierarchy, such as DS3. Multiple DS_1s are bundled together to form DS2, and DSs are tied together into DS3. Figure below shows the standardized data rates in the T-carrier system.

Table 2.4: T1 Hierarchy

Service	Line	Rate (Mbps)	Voice Channels
DS-1	T-1	1.544	24
DS-2	T-2	6.312	96
DS-3	T-3	44.736	672
DS-4	T-4	274.176	4032

2. E1 Carrier System

E1 link is a digital communication link that enables the transmission of voice, data, and video signals at the rate of 2.048 Mbps. E1 is primarily deployed in Europe and Asia. T1 and E1 lines are conceptually identical but their capacities and number of voice channels which they carry are different.

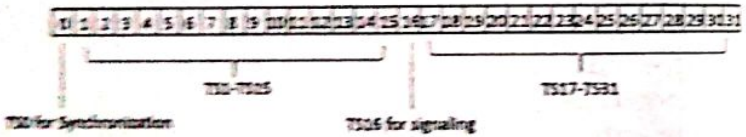


Figure 2.30: E1 frame structure

E1 frame consists of 32 time slots, each time slot contains 8 bits and are numbered from 0 to 31. The E1 frame Time Slots are nominated TS0 to TS31 and they are allocated to different purposes:

TS0: This E1 frame time slot is used for synchronization, alarms and messages. It is reserved for framing purposes and alternately transmits a fixed pattern.

TS1-TS15: These time slots are used for user data

TS16: E1 signaling data is carried on TS16. This includes control, call setup and teardown

TS17 - TS31: These E1 frame times slots are used for carrying user data

The higher rate of E carrier links are:

Table 2.5: E1 Hierarchy

E Carrier link	Data rates
E0	64kbps
E1	2.048 Mbps
E2	8.448Mbps
E3	34.368Mbps
E4	139.264Mbps

2.3.8 ISDN (Integrated Service Digital Network)

The traditional PSTN used an analog connection for communicating between the customer premises and the local exchange, also known as the local loop. The analog circuits cause the limitations on the bandwidth in the local loop. So, ISDN was developed with the intention of creating a totally digital network. ISDN technology allows digital signals to be sent over existing telephone lines. It can transfer many types of network traffics like voice, data, video, graphic, etc.

Traditional Telephone networks are used for only voice communication. ISDN is a circuit switched telephone network system which also provides access to a packet switch network designed to allow digital transmission of voice and data over ordinary telephone copper wires.

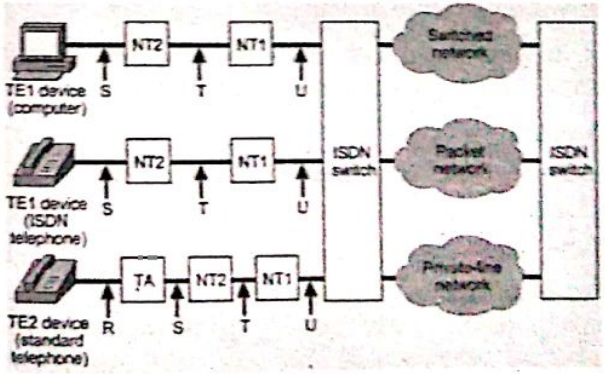


Figure 2.31: ISDN architecture

ISDN Components

- **TE1 –** (Terminal Equipment) Device compatible with ISDN network, connects to NT2
- **TE2 -** Device not compatible with ISDN requires TA
- **TA -** (Terminal Adapter) Converts signals so, non-ISDN devices can use ISDN
- **NT1 –** (Network Terminal) Connects 4-wire ISDN to 2-wire local loop
- **NT2 -** Directs traffic to and from different subscriber devices and NT1
- **ISDN Switch –** Provides multiple ISDN interfaces on an ISDN line

ISDN Reference Points

- **R:** References the connection between a non-ISDN compatible device Terminal Equipment type 2 (TE2) and a Terminal Adapter (TA), for example, an RS-232 serial interface.
- **S:** References the points that connect into the customer switching device Network Termination type 2 (NT2) and enables calls between the various types of customer premises equipment.
- **T:** Electrically identical to the S interface, it references the outbound connection from the NT2 to the ISDN network or Network Termination type 1 (NT1).
- **U:** References the connection between the NT1 and the ISDN network owned by the telephone company.

ISDN Channels

- **B-Channel (Bearer Channel):** It is used for carrying data. It has a 64 Kbps voice channel of 8 bits sampled at 8 KHz.
- **D-Channel (Bearer Channel):** It is used for carrying signaling information to the circuit switch calls associated with B-Channel. D channel might be 16 Kbps or 64 Kbps.

ISDN Interface

a. **BRI:** The ISDN Basic Rate Interface (BRI) service offers two B channels and one D channel (2B+D). Each BRI B channel operates at 64 kbps and is meant to carry user data. The BRI D channel operates at 16 kbps and is meant to carry control and signaling information, although it can support user data transmission under certain circumstances. Synchronizing and framing bits (Overhead) at 48 Kbps. Hence, total data rate is 192 Kbps

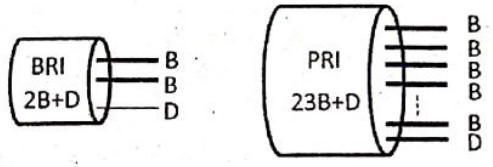


Figure 2.32: BRI and PRI

b. **PRI:** PRI stands for Primary Rate Interface.

- **Type-1 (23B+D):** The bandwidth is divided into 24 64KB channels. The ISDN PRI services used 23 B channel accesses and used the 24th D channel for signaling purposes. Total data rate is 1.544 Mbps (T1- Hierarchy).
- **Type-2 (30B+D):** The bandwidth is divided into 32 64KB channels. The ISDN PRI services used 30 B channel, One D channel and one synchronizing and framing bits with data rates 64 Kbps each. Total data rate is 2048 Kbps (E1- Hierarchy).

CHAPTER – 3

DATA LINK LAYER

The *data link layer* is the second layer in the OSI Model. It plays an important role in achieving reliable, efficient communication between two adjacent machines. It deals with formation of frames, transmission errors, regulates the flow of data, and provides a well-defined interface to the network layer.

3.1 Functions of Data Link Layer

Below are some of the important functions of data Link Layer:

- It provides a well-defined services interface to the network layer.
- It synchronizes frame for recognizing the start and end of frame
- It deals with transmission errors
- It regulates the flow of data. It provides a flow control mechanism to avoid a fast transmitter from running a slow receiver.
- It also has protocols to determine which of the devices has control over the link.

3.2 Services provided by data link layer

Data link layer can be designed to provide efficient types of services.

- **Unacknowledged connectionless services**

  In this scheme, the destination machine does not send back any acknowledgement of the receiving frame. If the frame is lost, no attempt is made to recover it. It is suitable for real time traffic.

- **Acknowledged connectionless services**

  It improves reliability since in spite of being connectionless acknowledgement is sent from receiver to transmit if the frame is not received within specified time. It is suitable for communication over unreliable channels.

- **Acknowledged connection-oriented services**

  The source and destination machines establish a connection before transferring the data. A specific number is given to each frame being sent and a data link layer guarantees that each transmitted frame is received. There are three phases to be followed for data transfer: connection established, frame transfer and connection release.

3.3 Framing

A *frame* is made by breaking down a stream of bits into smaller, digestible chunks. The frame typically includes frame synchronization features consisting of a sequence of bits or symbols arrangement such that it indicates to the receiver the beginning and end of the payload data within the stream of symbols or bits it receives.

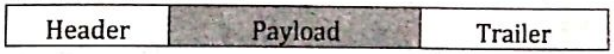


Figure 3.1: Frame

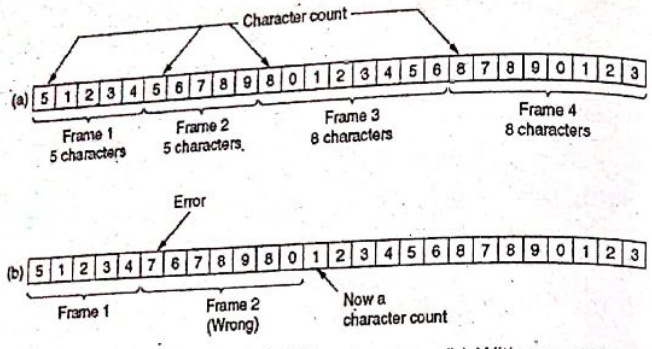
A frame has following parts:

- **Headers:** It contains the source and the destination addresses of the frame.
- **Payload Field:** It contains the message to be delivered.
- **Trailer:** It contains the error detection and error correction bits.

Framing Methods:

a. **Character Count:**

This method uses a field in the header to specify the number of characters in the frame. At destination, by seeing the character count, it knows how many characters follow and where the end of the frame is. But the problem can occur if the count is garbled in transit due to which the receiver will not know where to pick up and the sender will not know how much to resend. This method is rarely used.



A character stream. (a) Without errors. (b) With one error.

Figure 3.2: Character count

b. Flag Bytes with Byte Stuffing:

Flag	Header	Payload field	Trailer	Flag

Figure 3.3: Byte stuffing format

In this method, frames begin and end with special bytes. Flags are used as the start/end bytes which are often the same. During data transmission, if the receiver gets lost, it just looks for the pair of flag bytes to denote the end of one frame and the start of the next.

A serious problem occurs with this method when flag byte's bit pattern occurs in the data. This is solved by inserting a special escape byte (ESC) just before each flag byte in the data. This technique is called byte stuffing or character stuffing.

The main drawback of this framing method is that we have to use 8 bits character and ASCII code.

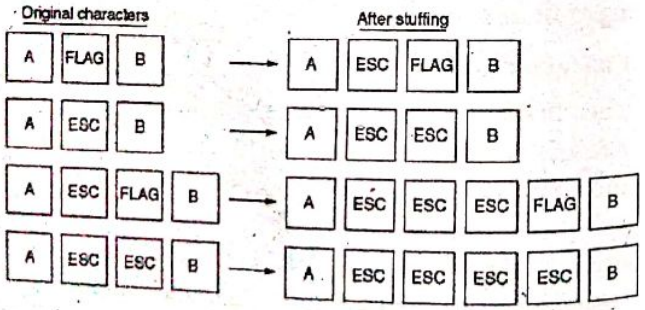


Figure 3.4: Flag byte stuffing method

c. Starting and Ending Flags with Bit Stuffing:

This new technique adds an arbitrary number of bits in data frames and character codes with an arbitrary number of bits per character. E.g., Each frame begins and ends with a special bit pattern, 01111110 (in fact, a flag byte). Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream. This process is called *Bit stuffing.*

Example: original data 01001111110111110

Data stream after framing and bit stuffing:

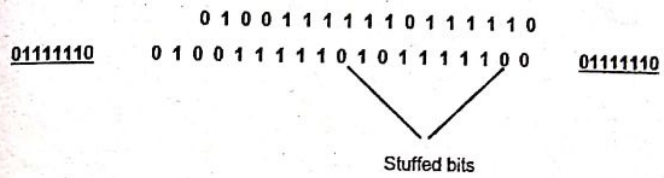


Figure 3.5: Bit stuffing

d. Physical Layer Coding Violations:

This method is only applicable to networks in which the encoding on the physical medium contains some redundancy. When data is a series of 0, it appears as the open circuit and when data is a series of 1, it appears as a short circuit. To avoid this, it is put in transit (when 0 the signal voltage is -5 to +5 and when 1 the signal voltage is +5 to -5). The combinations of low-low and high-high which are not used for data may be used for marking frame boundaries.

3.4 Error Control

Error control makes sure that all frames are eventually delivered to the network layer at the destination in proper order. Generally, feedback is sent by the receiving station to inform that a frame has been successfully received or not.

Error control in the data link layer is based upon the principle of request for automatic retransmission (ARQ) of the missing, lost or damaged frame.

ARQ system has three types

a. Stop and Wait ARQ

In this method, the sender sends one frame, stops until it receives confirmation from the receiver and then sends the next frame. For retransmission, it keeps a copy of the lost frame that was sent. The identification of data frame and ACK frame is 0 and 1 respectively. The sending device is equipped with a timer.

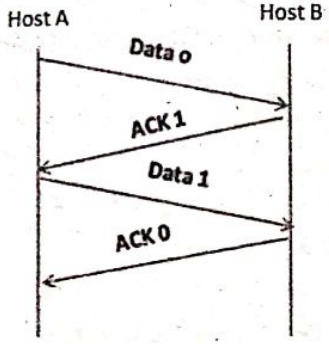


Figure 3.6: Stop and wait normal ARQ

It handles three cases of error:

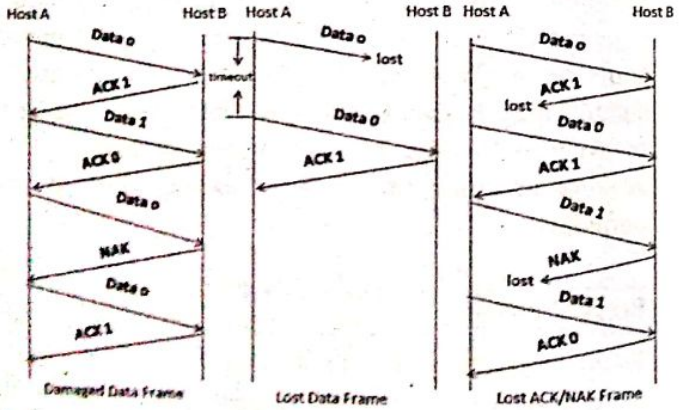


Figure 3.7: ARQ for damaged and lost data and lost ACK/NAK frame

b. Go Back N ARQ

This form of error control is based on sliding window flow control. A station may send a series of frames sequentially numbered with some maximum value. In this method acknowledgement (ACK) and negative acknowledgement (NACK) must be numbered. ACK carry the next frame to be expected and NAK carry current damaged frame. In this method, if one frame is lost or damaged, all frames sent from the last frame acknowledgement are retransmitted.

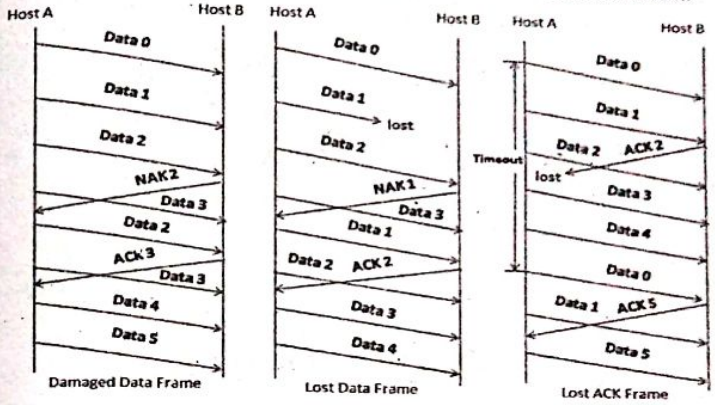


Figure 3.8: Go Back N ARQ

c. Selective Repeat ARQ

As in Go Back N ARQ, a station may send a series of frames sequentially numbered with some maximum value. But in this method, only the specified damaged or lost frame is retransmitted. It is more efficient than Go back N ARQ because it minimizes the amount of retransmission.

A selective repeat system differs from the Go back N method in the following ways.

- The receiver must contain sorting logic to reorder frames
- It must be able to store frames received after a NAK is sent until the damaged frame is replaced.
- Sender must contain a searching mechanism to find only the requested frame for retransmission.
- Buffer in the receiver must be large enough to keep all previously received frame on hold until all retransmission has been stored.

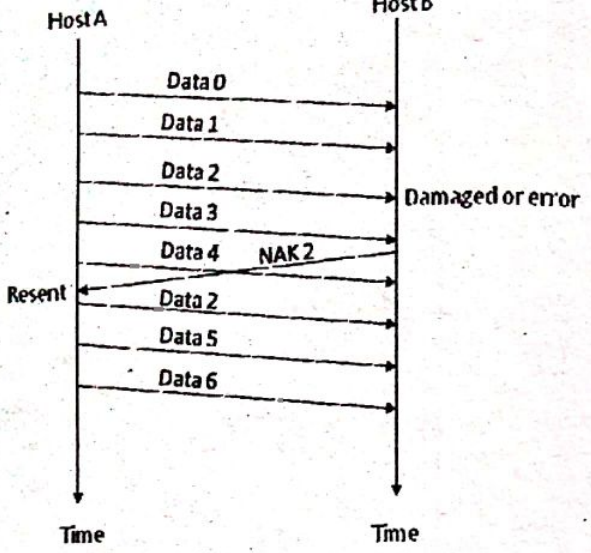


Figure 3.9: Selective repeat ARQ

3.4.1 Error Detection and Corrections

Different types of errors like bit altering, packet loss, data block missing, etc. can occur during the transmission of data in a network. These errors occur due to the fault in hardware or some other network limitations. So, various methods should be applied for detection and correction of these errors to establish a perfect communication.

Types of error

- **Content error:** It is the error in the content of a message
- **Flow integrity error:** When the message is delivered to the wrong destination, it is called flow integrity error.

Error can be further classified depending upon the number of bit error:

- **Single bit error:** if there is only one bit, anywhere though, which is corrupted.

- **Multiple bits error:** Frame is received with more than one bits in corrupted state.

- **Burst error:** Frame contains more than 1 consecutive bits are corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

1. Error Detection

For a given frame, an error-detecting code (check bits) is calculated from data bits and it is appended to the data to send to a receiver. In the receiver side, the incoming frame is separated into data bits and check bits and calculates check bits from received data bits. Then the calculated check bits are compared against received check bits and error is detected. Different techniques can be applied for error detection.

a. Parity Checking:

It is the simplest technique for detecting the error. A parity bit is added in the data bit. Then at the receiver side, the parity of data is compared with the parity bit for detection of error.

The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and the number of 1s is even then one bit with value 0 is added. This way the number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.

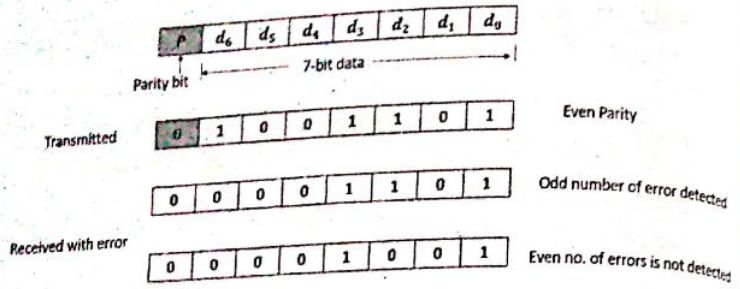


Figure 3.10: Parity checking

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But if double or even a number of errors occurred then it will not change the parity so error is unnoticed. So, parity checks cannot correct errors but can detect odd numbers of errors.

b. Checksum:

Checksum is used by the higher-layer protocol for error detection. In this technique, all the bytes in a message are added to generate a checksum which is then sent after all the messages. Then, when the receiver receives the message it separately calculates the checksum and compares it with the one sent by the sender and detects error if no match occurs.

- In a checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

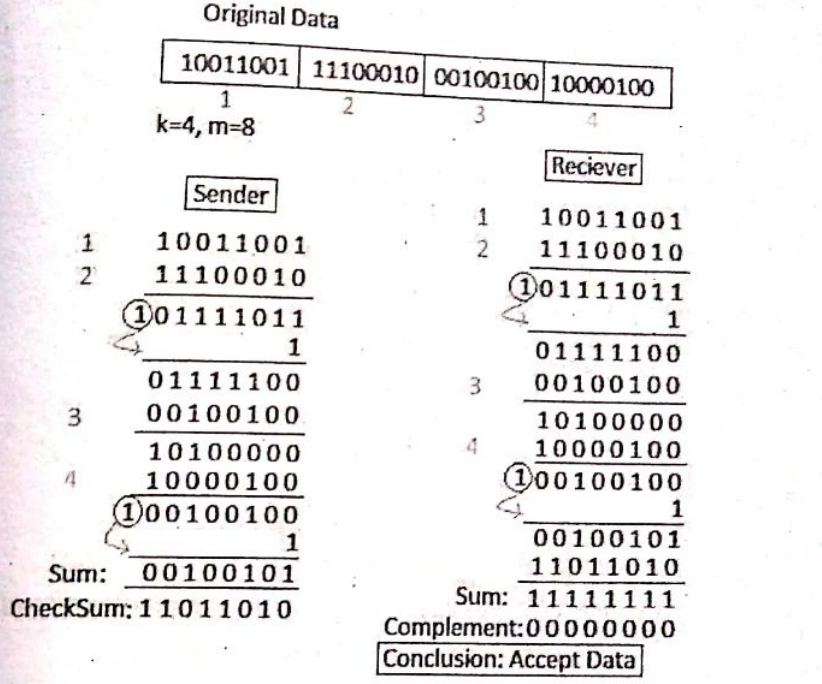


Figure 3.11: Checksum

c. Cyclic Redundancy Check (CRC):

It is more powerful than Parity and checksum. It is based on division. A sequence of redundant bits called CRC is generated by dividing the data with some specific byte and is appended at the end of data which is used at the receiver side for error detection.

- Unlike the checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder,

the data unit is assumed to be correct and is therefore accepted.

- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

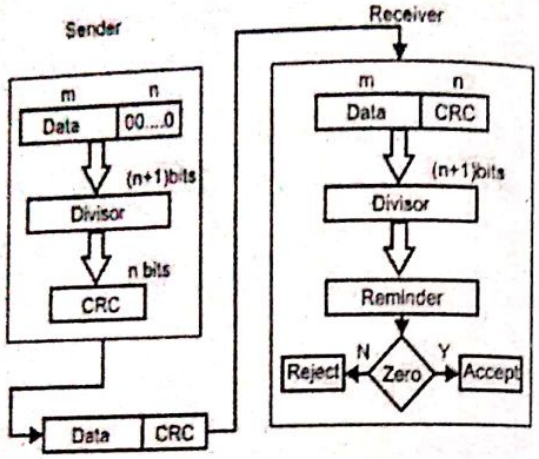


Figure 3.12: CRC

CRC can be defined in three procedural ways:

- Module 2 arithmetic,
- Polynomials, and
- Digital logic.

2. Error Correction

Error correction is the process of regeneration of actual data from a noisy or faulty data. However, over copper wire retransmission is faster than error correction but in the case of very noisy networks, without error-correction, it will be hard to get anything through. Error-correcting codes are widely used on wireless links, which are very noisy and error prone when compared to copper wire or optical fibers. Hamming code is one of the techniques used for error correction.

In the digital world, error correction can be done in two ways:

- **Backward Error Correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
- **Forward Error Correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

To correct the error in the data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection.

In error correction techniques, codes are generated at the transmitter by adding a group of check bits. The source generates the data in the form of a binary symbol. The encoder accepts these bits and adds the check bits to them to produce the code words which are transmitted towards the receiver. The check bits are used by the decoder to detect and correct the errors. There are many different error-correcting codes that we can use. These codes can be classified as block codes and convolutional codes. Sometimes they can even be classified as Linear code and non-linear code according to their distinguishable properties.

Hamming codes

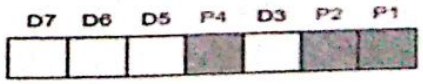
Hamming codes are linear block codes, which is an error-detection and error-correction technique, was proposed by R.W. Hamming.

Consider a message having four data bits which is to be transmitted as a 7-bit codeword by adding three error control bits. This would be called a (7,4) code.

A general method for constructing error-correcting codes by using a minimum distance of three.

Every integer m there is a $(2^m - 1)$ bit hamming code which contains m parity check bits and $2^m - 1 - m$ information bits.

The 7-bits Hamming code is as:



Here,

P1 P2 P4 = Parity check bits

D3 D5 D6 D7 = Data bits or Information bits.

If we number the bit positions from 1 to $2^m - 1$, the bits in position 2^k, where $0 \le k \le m - 1$, are the parity bits, and the bits in the remaining positions are information bits. Here k is the message sequence to be transmitted.

Calculating the Hamming Code

The key to the Hamming Code is the use of extra parity bits to allow the identification of a single error. Code word is created as follows:

1. Mark all bit positions that are powers of two as parity bits (positions 1,2,4,8,16, etc.).
2. All other bit positions are for the data to be encoded (positions 3,5,6,7,9,10,11,12, etc.).
3. Each parity bit calculates the parity for some of the bits in the code word. The position of the parity bit determines the sequence of bits that it alternately checks and skips.

Position 1: Check 1 bit, Skip 1 bit, Check 1 bit, Skip 1 bit, etc.

(1,3,5,7,9,11, 13, ...)

Position 2: Check 2 bits, Skip 2 bit, Check 2 bit, Skip 2 bit, etc.

(2,3,6,7,10,11)

Position 4 : Check 4 bit, Skip 4 bit, Check 4 bit, Skip 4 bit, etc.

(4,5,6,7,12,13,14,15,20, 21, ...)

Position 8: Check 8 bit , Skip 8 bit, Check 8 bit, Skip 8 bit, etc.

(8-15, 24-31, ...)

While checking the parity, if the total number of 1's are odd then write the value of parity bit **P1**(or **P2** etc.) as **1** (which

means the error is there) and if it is even then the value of parity bit is **0** (which means no error).

Detection of error.

Example:

A seven bits Hamming code is received as 1110111. What is the correct code?

Solution: Received codeword:

D7	D6	D5	P4	D3	P2	P1
1	1	1	0	1	1	1

Step 1: For checking parity bit **P1**, use **check one and skip one** method, which means, starting from P1 and then skip P2, take D3 then skip P4 then take D5, and then skip D6 and take D7, this way we will have the following bits,

D7 D5 D3 P1 = 1111☺number of 1 is even , so we write the value of P1 as 0. This means no error.

Step 2: Check for P2 but while checking for P2, we will use **check two and skip two** method, which will give us the following data bits. But remember since we are checking for P2, so we have to start our count from P2 (P1 should not be considered).

D7 D6 D3 P2 = 1111☺number of 1 is even , so we write the value of P2 as 0. This means no error.

Step 3: Check for P4 but while checking for P4, we will use check four and skip four method, which will give us the following data bits. But remember since we are checking for P4, so we have started our count from P4(P1 & P2 should not be considered).

D7 D6 D5 P4= 1110 ☹number of 1 is odd , so we write the value of P4 as 1. This means error exists.

P4	P2	P1

Now, we write the error word (E) =

1	0	0

i.e.

The decimal equivalent of E is 4.

Hence, the 4th bit in the codeword is incorrect.

3.5 Flow Control

Flow Control deals with the issue where the sender sends data at the higher rate than the receiver can receive. Flow control can be done by using the buffer on the receiver side. But, the main problem that occurs, in this case, is that the slower receiver cannot cope with the faster sender which causes overflow and loss of data.

Flow control tells the sender how much data should be sent to the receiver so that it is not lost. This mechanism makes the sender wait for an acknowledgment before sending the next data. There are two ways to control the flow of data:

1. Stop and Wait Protocol

It is the simplest flow control method. In this method, the sender will send one frame at a time to the receiver. Then, the sender will stop and wait for the acknowledgment from the receiver. When the sender gets the acknowledgment then it will send the next data packet to the receiver and wait for the acknowledgment again and this process will continue as long as the sender has data to send.

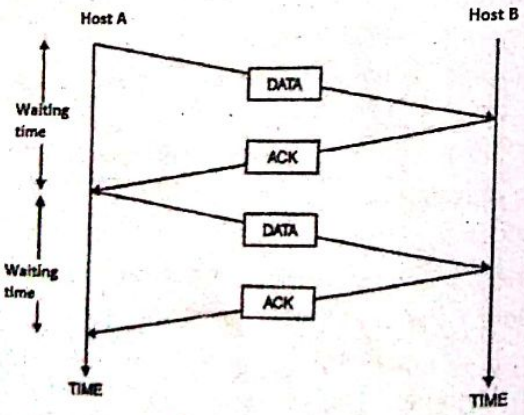


Figure 3.13: Stop and wait flow control

2. Sliding Window Protocol

In *sliding window protocol*, the sender can transmit several frames before needing an acknowledgment. Sliding window refers to imaginary boxes at both the sender and receiver side. A window is a buffer where frames are stored. Each frame in a window is numbered. If the window size is n then the frames are numbered from the number 0 to n-1. A sender can send n frames at a time. Frames may be acknowledged at any time. To keep track, it introduces identification numbers for each frame based on the size of the window. When the receiver sends an ACK, it introduces the number of next frames it expects the receiver.

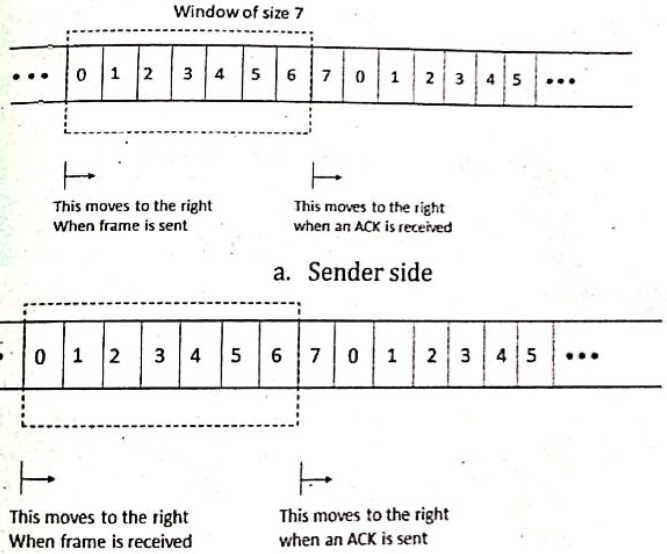


Figure 3.14: Sliding window

The sender and receiver deal with the possible range of sequence number. The range which is the concern of the sender is called the send sliding window; the range which is the concern of the receiver is called receive sliding window.

Example of sliding window protocol is shown below:

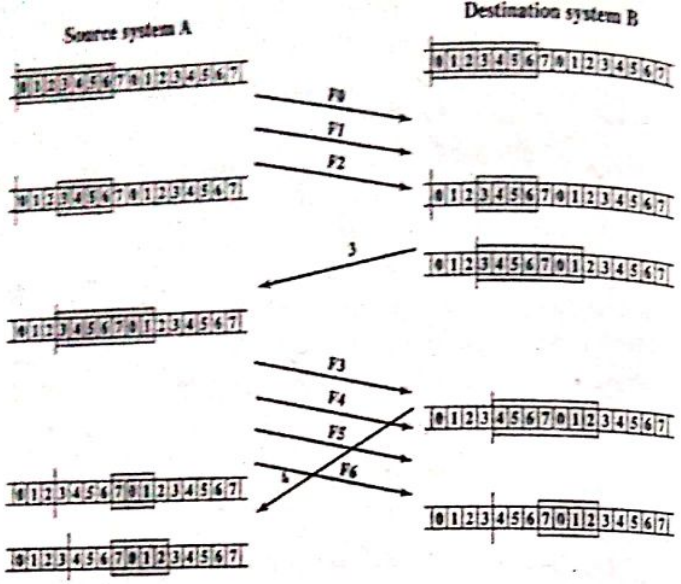


Figure 3.15: Sliding window example

3.6 Examples of Data Link Protocol, HDLC, PPP

3.6.1 HDLC (High-Level Data Link Control)

HDLC is a bit-oriented protocol, the frame and packet are interpreted as a series of bits. It specifies a packetization standard for serial links. It can provide both connection oriented and connectionless services. It is used for wide area network synchronous serial connections over leased lines.

Basic characteristics: HDLC defines three types of stations; three link configurations and three data-transfer modes of operations.

i. Stations

a. **Primary Station:** *Primary station* is the station that has the responsibility of controlling the operation of the link. Frame issued by the primary station is called commands.

b. **Secondary Station:** *Secondary station* operates under the control of the primary stations. Frame issued by the secondary are called responses.

c. **Combined Station:** *Combined station* combines the features of primary and secondary. Combined station may issue both commands and responses.

ii. Configuration

a. **Unbalanced configuration:** *Unbalanced configuration* consists of a primary station and one or more secondary stations.

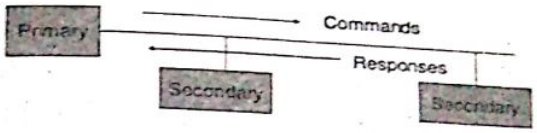


Figure 3.16: Unbalanced configuration

b. **Balanced Configuration:** *Balanced configuration* consists of two or more combined stations. Each station has equal and complimentary responsibility compared to each other.

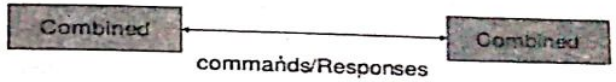


Figure 3.17: Balanced configuration

c. **Symmetric Configuration:** A *symmetric configuration* is one in which a physical station on a link consists of two logical stations; one primary and the other a secondary.

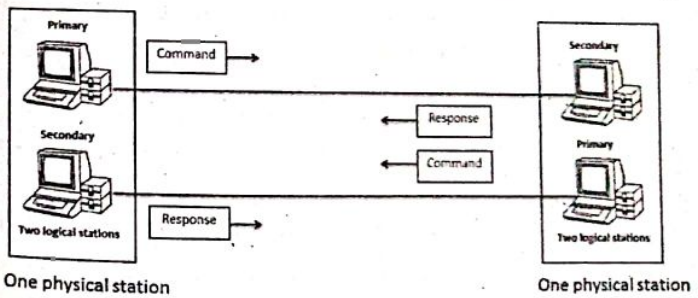


Figure 3.18: Symmetric configuration

iii. Operational Mode

A mode in HDLC is the relationship between two devices involved in an exchange mode which describes who

controls the link. HDLC offers three different modes of operation

a. **Normal Response Mode (NRM):** This mode is only used with and unbalanced configuration. The primary may initiate data transfer to a secondary, but a secondary may only transmit data in response to a command from the primary.

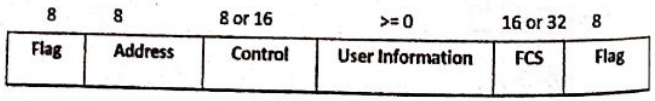
b. **Asynchronous Balanced Mode (ABM):** This mode is used with a Balanced configuration. In ABM, all stations are equal and therefore combined stations connect in point to point. There is no need for permission on the part of any station in this mode.

c. **Asynchronous Response Mode (ARM):** This mode is used with an unbalanced configuration. The secondary may initiate transmission without explicit permission of the primary. The primary still retains responsibility for the line, including initialization, error recovery and logical disconnection.

iv. HDLC Frame

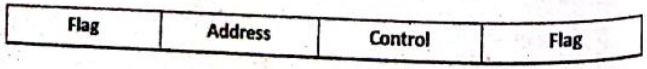
To provide the flexibility necessary to support all the options possible in the modes and configurations. HDLC defines three types of frames:

a. **Information frames (I frames):** Used for data transfer and control information



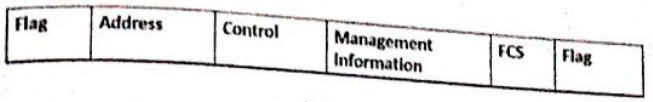
I frame

b. **Supervisory frames** (S frames): Used for control information.



S-frame

c. **Un-numbered frame** (U frames): Used for system management.



U-frame

Figure 3.19: HDLC frame structure

HDLC frame consists of following fields:

- **Flag field:** Flag field contains synchronization pattern 01111110 that identifies both the beginning and the end of a frame.
- **Address:** It contains the address of the secondary stations.

  If primary creates the frame to

  If secondary creates the frame from
- **Information field:** it contains the user's data from the network layer or management information.
- **FCS field:** The frame check sequence (FCS) is basically the HDLC error detection field. It can contain either a 2 or 4 byte.
- **Control field:** The control field is a 1- or 2-byte segment of the frame used for flow and error control. It contains different data for each of the different types of frames i.e. I frames, S frames and U frames.

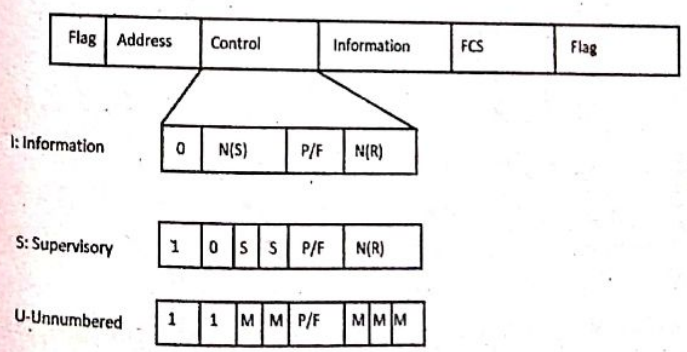


Figure 3.20: Control field of HDLC frame

Where,

N(S) defines sequence number;

P/F for Poll and Final;

N(R) defines Acknowledgement number;

SS having 2 bits. So,

0 0 = (RR) receiver is ready

0 1 = (Rej) receiver rejected

1 0 = (RNR) Receiver not ready

1 1 = Selective repeat frame

3.6.2 PPP (Point to Point Protocol)

This protocol is used for the point-to-point connection between terminals within the internet. It is often used to connect home users to the internet. Although HDLC is a general protocol that can be used in the case of both point-to-point and multipoint configurations, one of the most basic protocols for point-to-point access is the Point-to-Point Protocol (PPP).

PPP provides three features:

- An Unambiguous framing mechanism.
- A Link Control Protocol (LCP) for bringing lines up, testing them, negotiating options and bringing them down.
- One or more Network Control Protocols (NCPs): IP negotiating IP numbers for each end.

PPP Frame:

Bytes	1	1	1	1 or 2	Variable	1 or 2	1
	Flag 01111110	Address 11111111	Control 00000011	Protocol	Payload	Checksum	Flag 01111110

Figure 2.21: PPP frame

The frame format of PPP resembles HDLC frame. PPP is a character-oriented protocol. Its various fields are:

- **Flag field:** All PPP Frames begin & end with the standard HDLC Flag byte 01111110.
- **Address field:** This address is the broadcast address. Address field which is set to the binary value 11111111
- **Control field:** This field uses the format of the U-frame in HDLC. This field set to default value 00000011

- **Protocol field:** This field indicates what kind of packet is in the Payload field.
- **Payload field:** It carries user data or other information. It is variable length payload. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used.
- **Checksum field:** It is used for error detection.

PPP Link Establishment:

PPP first uses LCP to establish and test a link, and to agree on a configuration. The LCP may require authentication from its peer at the other end. PPP then uses NCP packets to select and configure the network layer protocols being used. Once the protocol information has been established, communication can begin and PPP can begin transferring packets between the two ends.

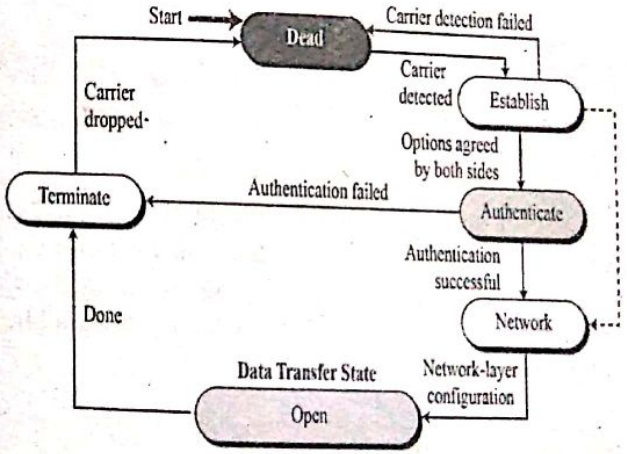


Figure 3.22: PPP link establishment

3.6.3 SLIP (Serial Line in Protocol)

SLIP is a very simple protocol that is used solely for encapsulating and framing IP packets that are being transmitted over a serial line for example, via modem. It uses point-point protocol and is used widely by users wishing to connect to the Internet from home through an Internet Access Provider).

Because it lacks error-connection capabilities and because serial connections can sometimes be quite noisy, SLIP has largely been replaced by PPP.

3.7 Medium Access Sub Layer

Network links can be divided into two categories: point to point connection and broadcast channel. *Medium Access Sub Layer* deals with broadcast networks and their protocols. In any broadcast network, the key issue is how to determine who gets to use the channel when there is competition for it. So, a controlling unit should be defined which permits only one request to access the single channel, this is done by sub layer of the data link layer called the MAC (Medium Access Control) sub-layer.

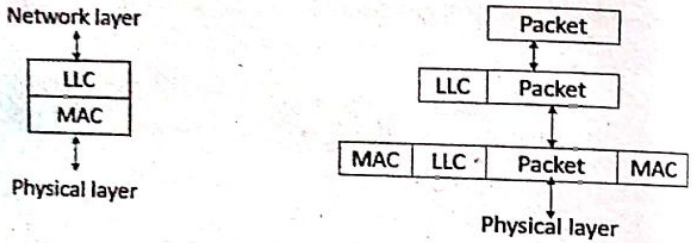


Figure 3.23: Medium access sublayer

Data Link layer functionality is split into two sub-layers: LLC (logical Link control) and MAC (Media Access Control). LLC is responsible for error and flow control. LLC also interacts with the network layer. MAC is responsible for framing, MAC addressing, multiple access control.

3.8 Channel Allocation Problem

If two transmitters transmit at the same time, their signal may interfere or collide, a method is needed to share the broadcast link among the various transmitters and avoid such collision. The *channel allocation problem* is "How to allocate a single broadcast channel among competing users". There are a variety of solutions to the problem of allocating multi-access channels among multiple competing users. They are broadly classified as: Static Channel Allocation and Dynamic Channel Allocation

- **Static Channel Allocation:** The channel's capacity is essentially divided into fixed portions; each user is then allocated a portion for all time.

  Example: FDM and TDM (Frequency/Time Division Multiplexing). FDM is used in Radio or TV broadcasting whereas TDM is POTS (Plain Old Telephone System). These channel allocation techniques waste bandwidth as they cannot cope with the dynamic environment.

- **Dynamic Channel Allocation:** With a dynamic approach the allocation of the channel based on the traffic generated by the users. It tries to get better utilization of the channel when traffic is unpredictable.

  Example: Pure/Slotted ALOHA Protocol or Carrier Sense Multiple Access (CSMA) Protocols, etc.

3.9 Multiple Access Protocol

Multiple access protocol is used to control/coordinate access to the link or link in a shared connection. Nodes can regulate their transmission within the shared broadcast channel by using Multiple Access Protocol. All the nodes can transmit a frame at the same time. This may arise to the collision, so to overcome this Multiple Access protocol is implemented.

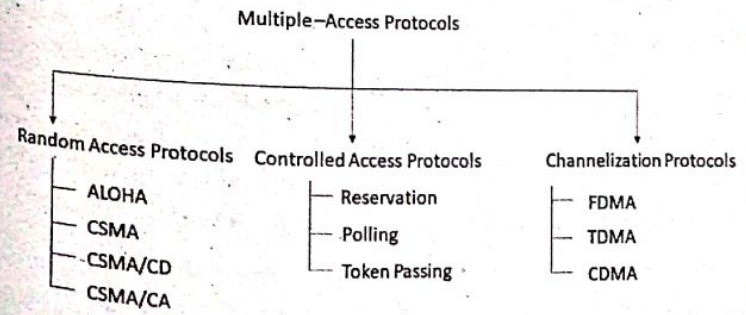


Figure 3.24: Types of multiple access protocol

3.9.1 Random Access Protocol

In this method, no station is superior to another station and none is assigned the control over another. Each station has the right to the medium without being controlled by any other station. Any station can send data depending on the medium's state (idle or busy). It has two features; no fixed time for sending data (Random Access) and no fixed sequence of stations sending data (Contention Method)

The random access protocols are further subdivided as:

1. **ALOHA:** It is the earliest random access method, developed in the early 1970s. It was designed for radio LAN but is also applicable for shared medium. In this method, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

   a. **Pure ALOHA:**

   It is an original ALOHA protocol, where the stations transmit frames whenever they have data to send. When two or more stations transmit simultaneously, there is collision and the frames are destroyed. Whenever any station transmits a frame, it expects the acknowledgement from the receiver. If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed. If the frame is destroyed because of a collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise the same frames will collide again and again. Therefore, Pure ALOHA dictates that when the time-out period passes, each station must wait for a random amount of time before re-sending its frame. This randomness will help avoid more collisions.

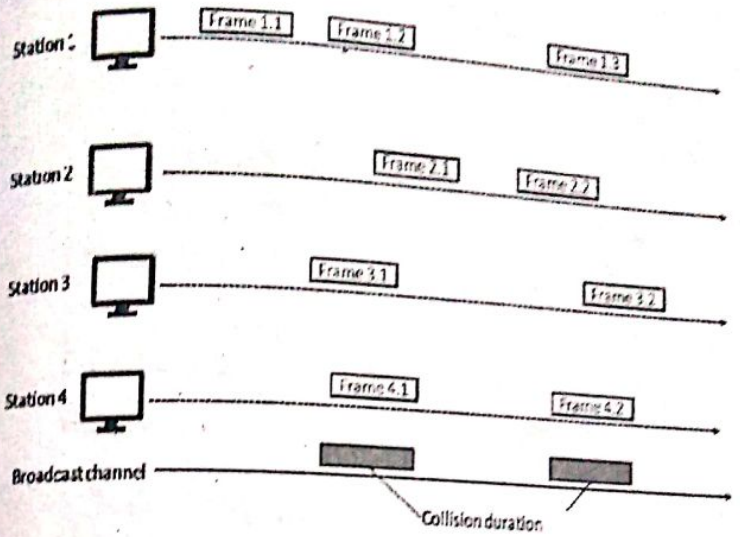


Figure 2.25: Overview of pure ALOHA

In figure, there are four stations that contend with one another for access to shared channels. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only one frame, frame 1.1 survive and all other frames are destroyed.

Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

b. **Slotted ALOHA**

Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high. In this method, the time of the shared channel is divided into discrete intervals called slots. The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.

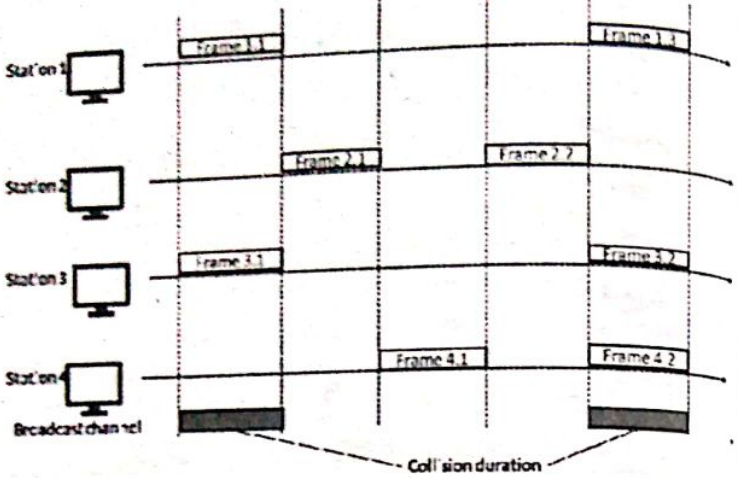


Figure 2.26: Slotted ALOHA

If any station is not able to place the frame onto the channel at the beginning of the slot *i.e.*, it misses the time slot then the station has to wait until the beginning of the next time slot. There is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.

Comparison Between Pure ALOHA and Slotted ALOHA

Table 3.1: Comparison between pure ALOHA and slotted ALOHA

Key	Pure ALOHA	Slotted ALOHA
Frame Transmission	Station can transmit data frames whenever it has data to send.	Station can transmit data only at the beginning of any time slot.
Time	In Pure Aloha, time is continuous.	In Slotted Aloha, time is discrete.
Time synchronization	The time is not globally synchronized.	The time is globally synchronized.
Successful Transmission	Probability of successful transmission of data packet = $G \times e^{-2G}$	Probability of successful transmission of data packet = $G \times e^{-G}$

Key	Pure ALOHA	Slotted ALOHA
Throughput	The maximum throughput occurs at G=½ which is 18.4%	The maximum throughput occurs at G=1 which is 36.8%

2. CSMA (Carrier Sense Multiple Access)

ALOHA and slotted ALOHA can easily be implemented, but unfortunately, they can only be used in networks that are very lightly loaded. Designing a network for a very low utilization is possible, but it clearly increases the cost of the network. To overcome the problems of ALOHA, many Medium Access Control mechanisms have been proposed which improve channel utilization. Carrier Sense Multiple Access (CSMA) is a significant improvement compared to ALOHA.

CSMA operates on the principle of carrier sensing before transmitting. Station listens to see the presence of transmission on the cable and decides to act accordingly. Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However, there is still a chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA Access Modes:

a. **Non-Persistent:** In a non-persistent method, a station that has a frame to send senses the line. If the line is idle, it sends the data immediately, otherwise it checks the medium after a random amount of time and transmits when found idle.

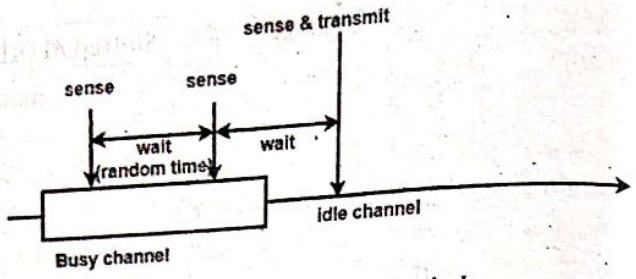


Figure 3.27: Non-persistent method

b. 1-persistent: The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally (with 1 probability) as soon as the channel gets idle.

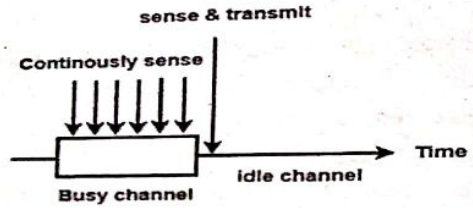


Figure 3.28: 1-persistent method

c. P-persistent: The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it sends with p probability. This repeat continues until the frame is sent.

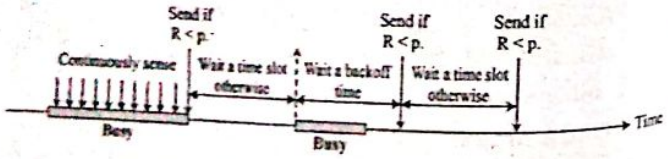


Figure 3.29: P-persistent

3. CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

CSMA/CD is a widely used MAC protocol standardized by IEEE 802.3. In this method, a station monitors the medium

after it sends a frame to see if the transmission was successful. If so, the transmission is finished. If, however, there is a collision, the following steps are done:

- Abort transmission.
- Transmit a jam signal to notify other stations of collision so that they will discard the transmitted frame.
- After sending the jam signal, back off random amount of time then,
- If again the collision takes place the back off time is increased progressively.

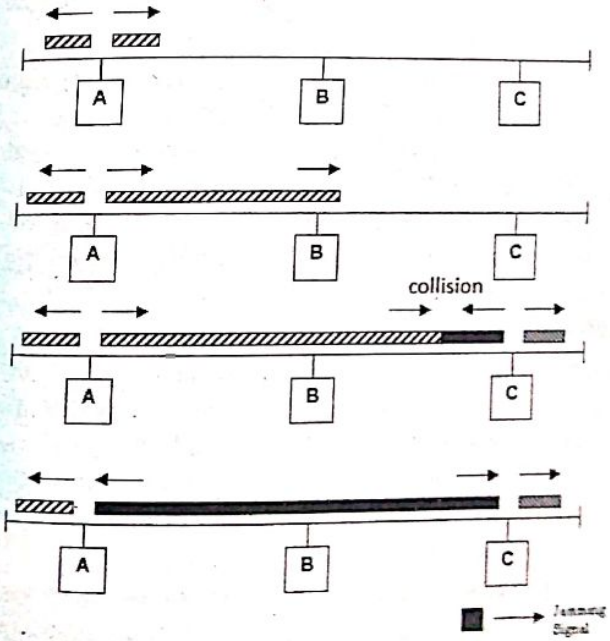


Figure 3.30: CSMA/CD

4. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

CSMA/CA is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by transmitting only when the channel is sensed to be idle. Prior to transmitting, a node first listens to the

medium to determine whether another node is transmitting or not. If another node is transmitting, it waits for a period of time for the node to stop transmitting before listening again for a free communications channel.

CSMA/CD is not suitable for wireless LANs due to various reasons:

- It is difficult to detect collision
- Control of radio environment is difficult
- Hidden station problem,

Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space, the contention window and acknowledgment.

- **Interframe space** – Station waits for the medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time, it again checks the medium for being idle. The IFS duration depends on the priority of the station.
- **Contention Window** – It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time the medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
- **Acknowledgement** – The sender re-transmits the data if acknowledgement is not received before time-out.

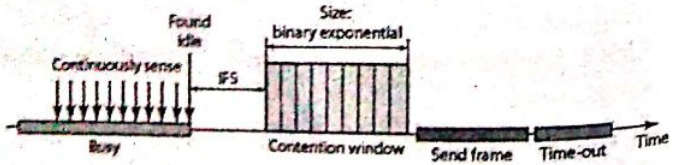


Figure 3.31: Timing in CSMA/CA

3.9.2 Controlled Access Method

In controlled access, the stations consult one another to find which station has the right to send.

1. **Reservation:** A station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame proceeds the data frames sent in that interval.
2. **Polling:** *Polling* works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device. The method uses poll and select functions to prevent collisions.
3. **Token Passing:** In *token-passing* method, the stations in a network are organized in a logical ring. A special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor. It seizes the token and sends its data.

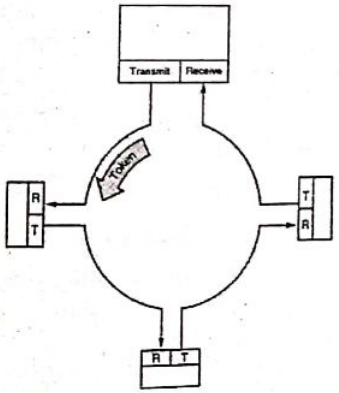


Figure 3.32: Token Passing

3.10 IEEE Standard

Institute of Electrical and Electronics Engineers is an American professional organization that defines standards related to networking and other areas.

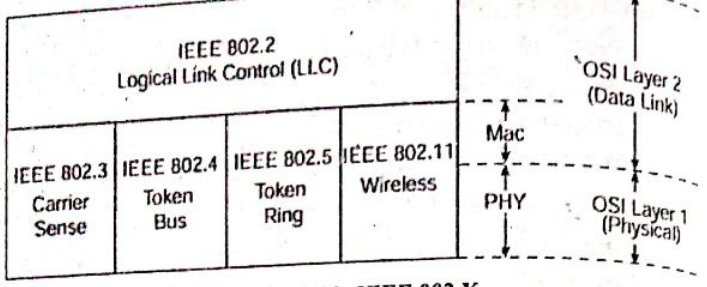


Figure 3.33: IEEE 802.X

- *IEEE 802.1* standards for network management at the higher level.
- *IEEE 802.2* defines the operation of the LLC sublayer. LLC provides an interface between media access methods and the network layer. The functions provided by the LLC, which include framing, addressing and error control.
- *IEEE 802.3* describes the physical layer and the MAC sublayer for baseband networks that uses a bus topology and CSMA/CD as their scheme for accessing the network.
- *IEEE 802.4* describes the physical layer and the MAC sublayer for baseband or broadband networks that uses a bus topology, token passing to access the network.
- *IEEE 802.5* describes the physical layer and the MAC sublayer for networks that use a ring topology and token passing to access the network.

A. Ethernet (IEEE 802.3)

The *Ethernet* LAN was developed in the 1970s by xerox corporation to operate with a data rate of 3Mbps using a CSMA/CD protocol. Ethernet is the most widely used for local area network (LAN) technology. Ethernet is a link layer protocol in the TCP/IP stack, describing how networked devices should format data for efficient transmission between other network devices on the same network segment, and how to put that data out on the network connection.

Ethernet has gone through four generations; Standard Ethernet (10Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps) and 10 Gigabit Ethernet (10Gbps).

Standard Ethernet

The original Ethernet technology with the data rate of 10Mbps as the *Standard Ethernet*.

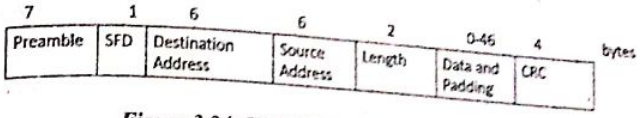


Figure 3.34: IEEE 802.3 header format

- **Preamble (Pre):** 7 Bytes bit pattern 10101010... used for synchronization
- **Start-of-frame delimiter (SFD):** 10101011 indicates Start of Frame
- **DA:** 6 bytes field that contains the physical address of the destination station.
- **SA:** It is also 6 bytes that contains the physical address of the source station.
- **Length:** It defines the upper-layer protocol whose packet is encapsulated in the frame.
- **Data:** It carries data encapsulated from the upper layer protocols.
- **CRC:** It contains error detection information.

B. IEEE 802.4/ Token Bus

Token Bus is a network architecture defined in the IEEE 802.4 specification. Token Bus is a Token Bus is a physical bus that operates as a logical ring using tokens.

Operation:

- Access to the network is determined by the token, a special frame that is passed from node to node in a well-defined sequence.
- To regulate the sequence in which the token is passed the node involved in the token passing form a logical ring.
- Each node passes the token to the node with the next lower ring address.

- To complete the ring, the node with the lowest address passes to the node with highest.

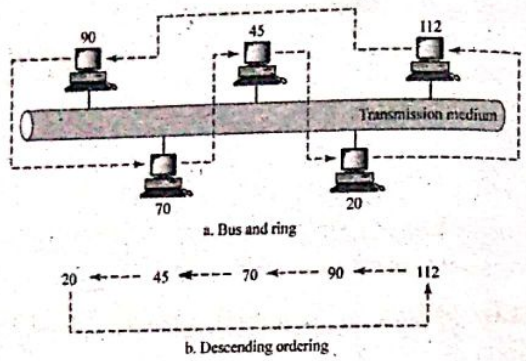


Figure 3.35: Token bus

Frame Format:

1 byte	1 byte	1 byte	2-6 byte	2-6 byte	0- 8182	4 byte	1 byte
Preamble	SD	FC	DA	SA	Data	FCS	ED

Figure 3.36: IEEE 802.4 Header Format

- **Preamble:** clock synchronization
- **Start Delimiter (SD):** marks the beginning of frame.
- **Frame Control:** used to claim token, Token lost, station with token dead, etc.
- **Destination Address (DA):** It specifies destination address.
- **Source Address (SA):** It specifies bytes source address.
- **FCS:** to detect transmission errors.
- **End Delimiter (ED):** marks the end of frame.

C. IEEE 802.5 (Token Ring)

IEEE 802.5 uses a token ring technique where a small frame called token is passed around the network. The node which passes the token can transmit data. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.

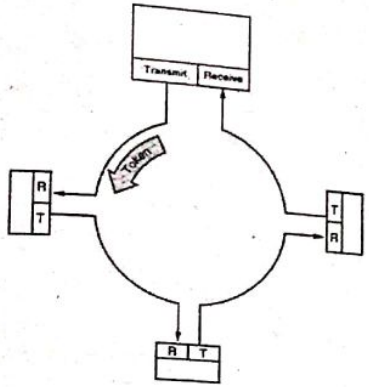


Figure 3.37: Token ring

Header Format:

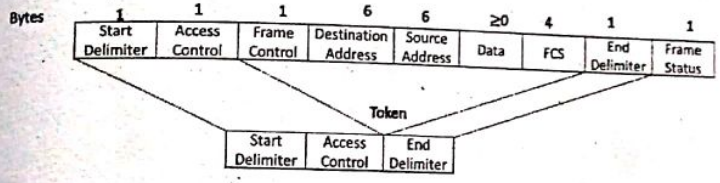


Figure 3.38: IEEE 802.5 header format

- **Start delimiter:** Alerts each station of the arrival of a token (or data/command frame).
- **Access-control byte:** Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits),
- **End delimiter:** Signals the end of the token or data/command frame.
- **Destination and source addresses:** Consists of two 6-byte address fields that identify the destination and source station addresses.
- **Data:** Indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station can hold the token.
- **Frame-check sequence (FCS):** For error detection.
- **Frame Status:** Is a 1-byte field terminating a command/ data frame. The Frame Status field includes the address recognized indicator and frame-copied indicator.

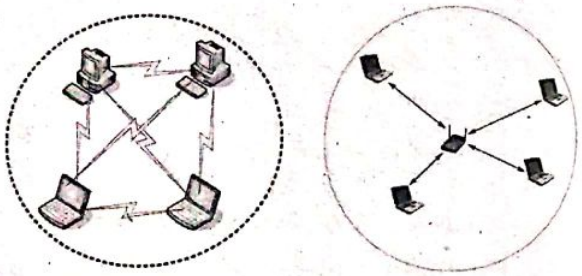
D. IEEE 802.11 / Wireless LAN

802.11 is the collection of standards set up for wirele networking. 802.11 lives in the physical layer and data lin layer in the OSI. There are three popular standard 802.11a, 802.11b, 802.11g and the latest one is 802.11n Each standard uses a frequency to connect to the networ and has a defined upper limit for data transfer speeds.

The standard defines two types of services:

1. Basic Service Set (BSS)

- IEEE 802.11 defines the BSS as the building blocks of a wireless LAN
- A *BSS* is made of stationary or mobile stations and optional centra; base station, AP.



(a) Ad-hoc BSS (b) Infrastructure BSS

Figure 3.39: BSS

2. Extended Service Set (ESS)

In *ESS*, the BSSs are connected through a distribute system, which is a wired or wireless network. Th distributed system connects the Aps in the BSS.

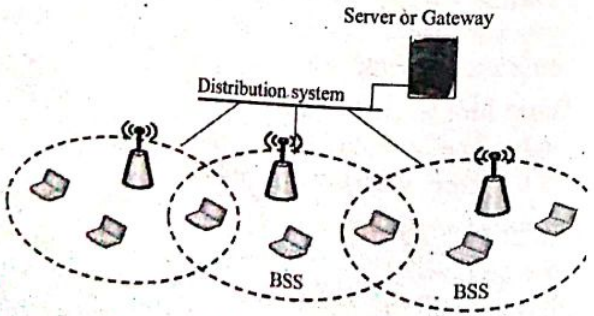


Figure 3.40: ESS

Header Format:

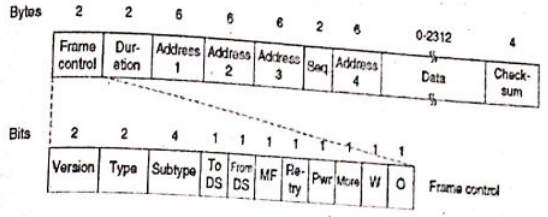


Figure 3.41: IEEE 802.11 header format

- **Frame Control:** Contains following
- **Version:** Protocol version Type: data, control or mgmt. Subtype: RTS or CTS
- **To/From DS:** Going to or Coming from inter cell distribution (eg. ethernet)
- **MF:** More fragments to follow Retry: Retransmission of earlier frame
- **Pwr:** Used by base station to sleep or wake receiver
- **More:** Sender has more frames for receiver W: WEP Encryption
- **O :** Sequence of frames must be processed in order
- **Duration:** time to occupy channel, used by other stations to manage NAV (Network Allocation Vector)
- **Addresses:** Address of sender and receiver.

E. FDDI

FDDI (Fiber Distribution Data Interface) is similar to Token ring as it shares several characteristics including token passing and a ring architecture. FDDI uses a dual-ring connection architecture. Traffic on each ring in the interface flows in opposite directions (called counter-rotating). The dual ring has a primary and a secondary ring. The primary ring is used for data transmissions during normal operation while the secondary ring remains idle. The secondary ring is only used when the primary ring fails or to send some special information. The primary purpose of the dual rings is to make the network reliable and robust.

FDDI provides multiple ways to connect devices to the ring. FDDI defines three types of devices that can be connected: single attachment station (SAS) like PCs, dual attachment station (DAS) like routers, servers, and a concentrator.

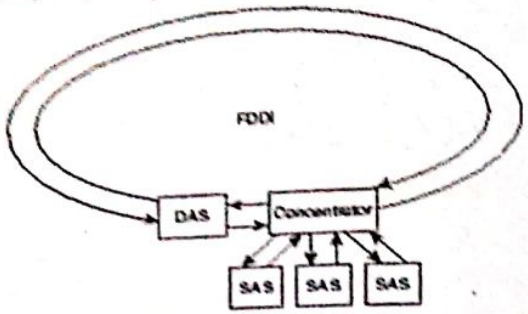


Figure 3.42: FDDI

3.11 VLAN (Virtual LAN)

A *VLAN* is a logical grouping of network users and resources connected to administratively defined ports on a switch. It can be considered as a local area network configured by software not by physical wiring. VLAN gives the ability to create smaller broadcast domains within a layer 2 switched internetwork by assigning different ports on the switch to different subnetworks.

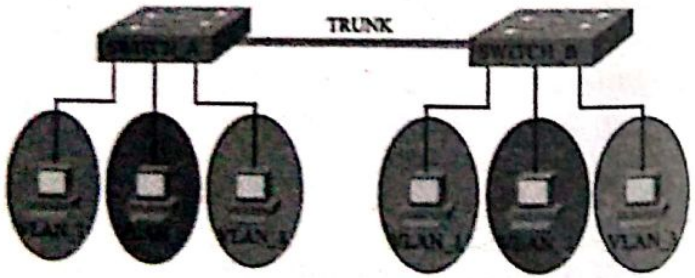


Figure 3.43: VLAN

Grouping devices with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together more easily even if they are not on the same network switch.

To set up a VLAN-based network, the network administrator decides how many VLANs there will be, which computers will be on which VLAN, and what the VLANs will be called. VLAN assigns computers to LAN segments by using software. VLANs are designed in two ways: Single-switch VLANs and Multi-switch VLANs. In Single switch VLANs, computers are assigned to VLANs using special software but physically connected together using a larger physical switch. Computer can be assigned to VLANs in different ways and they are:

- according to their VLAN switch port
- according to their data link layer address
- according to their IP address
- on the basis of the application that the computer uses

CHAPTER – 4

NETWORK LAYER

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 study the topology of the subnet and chooses appropriate path.

Functions:

- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link.
- **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

4.1 Internetworking Devices

The process of interconnecting a set of independent networks called *internetworking*. In other words, routing between two networks of the same kind or different kinds is called internetworking. An internetworking device is a widely-used term for any hardware within networks that connect different network resources.

As networks became increasingly complex, the need for internetworking devices also increased. Computer networks can be established by using various network devices such as cables, Network Interface Cards (NICs), Modems, Repeaters, Hubs, Bridges, Switches, and Gateways. As networks became increasingly complex, the need for internetworking devices also increased. Internetworking devices are active components because they do more than simply pass data across a network. They make intelligent decisions and may interpret, format and/or direct data as it passes through a network. The following are various internetwork devices that are used in building LAN/WAN.

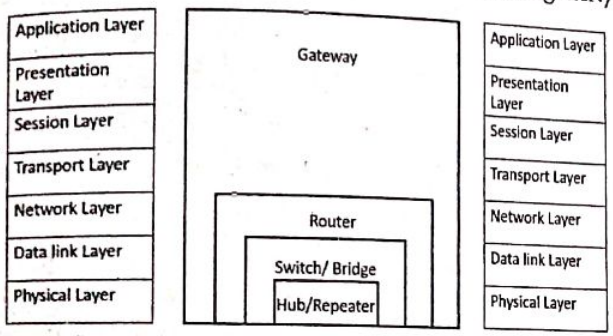


Figure 4.1: Connecting Devices and OSI model

a Repeater

A *repeater* is the physical layer devices which are used to regenerate the signal between similar networks. It extends the distance over which a signal may travel down a cable. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they operate on the Physical layer, the first layer of the OSI model. A repeater is a low-cost device and 2 Port device.

b. Hub

Hub, also called the multiport repeater is a physical layer device. It functions similar to the repeater. In a Hub, the signal received at the one port is transmitted to all the other

ports and vice-versa. The advantage of Hub is low-cost device and easy integration and it has disadvantage that it reduces the bandwidth.

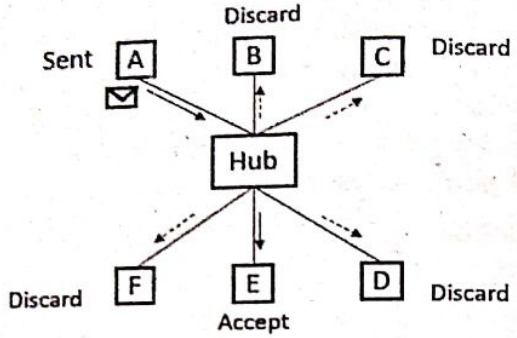


Figure 4.2: Hub operation

There are mainly two types of Hub, they are:

- **Active Hub:** An *Active hub* is also known as Concentrator. It requires a power supply and can work as a repeater. Thus, it can analyses the data packets and can amplify the transmission signals, if needed.
- **Passive Hub:** A *passive* hub does not need any power supply to operate. It only provides communication between the networking devices and does not amplify the transmission signals. In other words, it just forwards the data as it is.

c. Bridge

Bridge is a data link layer device. It functions very similar to a switch, sometimes also called the two ports switch. A bridge can divide an overloaded network into smaller, more efficient networks. It maintains a MAC table with MAC address and the port no. and decides whether to forward the frame or not. In other words, bridges filter traffic based on the destination address of the frame. Bridges divide the network into different LAN Segments.

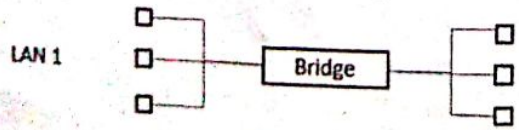


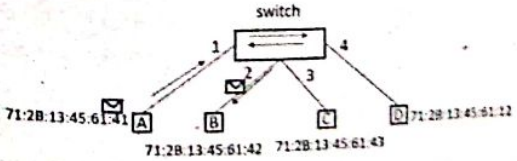
Figure 4.3: Bridge

There are mainly two types of Bridge, they are:

- **Transparent Bridge:** *Transparent bridge* simply works as a transmission medium between two devices. They are actually transparent (they are present but are not functionally visible to the devices) to the networking devices.
- **Routing Bridge:** *Routing bridges* have their unique identity; they can be easily identified by the network devices. The source station or the sender can send the data packets through specific bridges (using the unique identity of bridges).

d. Switch

A *switch* is also called the multiport bridge. It is a data link layer device. The switch is a hub with some intelligence. Switch allows each workstation to transmit information based on physical address. It doesn't distribute the signal without verifying whether the signal needs to propagate to given port. The decision is based on the internal configuration. A switch dynamically builds and maintains a MAC table, which holds all the necessary information for each port. A switch can connect the devices only in the same network. It uses the full-duplex mode of communication and saves bandwidth. The switch table keeps on updating every few seconds for better processing. A Switch has multiple collision domains, so it has less or no collisions in the transmission channel. In fact, every port of switch has a separate collision domain.



Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
71:2B:13:45:61:43	3
71:2B:13:45:61:12	4

Figure 4.4: Switch operation and switch table

When a data frame arrives at the Switch, it first checks for any kind of error in the data frame. If the frame is error-free, it will search the MAC address of the destination in the Switch table. If the address is available in the switch table, it will forward the data frame to that specific node, else switch will register the MAC address in the switch table. If the destination address is not specified, it will broadcast the data frame to each node in the network. There are mainly four types of switches on the basis of how data transmission takes place via switches, they are:

- **Store and Forward Switch:** It is the most widely and commonly used switch. It does not forward the data frames unless the frames are errorless and completely received in the switch buffer. It is reliable in nature.
- **Cut-through Switch:** Cut-through switches have no error checking. Also, it starts sending the data frame to the destination node when it starts receiving it. It is unreliable in nature.
- **Fragment-Free Switch:** It is a combination of store and forward, and cut-through switch. It checks only the starting 64 bytes (header information) of the data frame before transmitting the frame.
- **Adaptive Switch:** It is the most advanced kind of switch which automatically chooses any of the above three switches as per the need.

e. Router

A *router* is considered as a layer 3 relay that operated in the network layer. A router connects multiple networks and uses routing to forward data packets based on their IP addresses. It can be used to link two dissimilar LANs. A router receives a packet and selects the optimum path to forward the packet across the network.

It is the gateway of a network and maintains the routing table to route packets to the destination address. The information in the routing table helps to direct the packet to the next network. Because it is expensive and slower there

is a popular statement "Use switch where you can, Use router where you must".

f. Gateway

Gateway is a software or combination of software and hardware put together, works for exchanging data among networks which are using different protocols for sharing data. A Gateway is used to connect multiple networks and passes packets from one packet to the other network. It acts as a gate between two networks which may be a router, firewall, server or other device that enables traffic to flow in and out of the network. It operates at the session layer and above.

They are able to convert or translate the data format, although the data itself remains unchanged. It takes an application message, reads it and interpret it. It is the most complex devices with respect to the functionality. Gateway might be installed in some other device to add its functionality into another.

4.2 Addressing: Internet Address, Classful Address

4.2.1 Internet protocol (IP)

The network protocol in the Internet is called *internet protocol*. This is host to host network delivery protocol designed for the internet. IP is a connectionless datagram protocol with no guarantee of reliability. IP can only detect the error and discards it if it is corrupted.

1. Internet Protocol Address

An IP address is an identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to Internet. MAC address is a data link layer address also known as physical address that is recognized only in a local So, IP address is required for the globally recognized also known as logical address.

IP address is made of four bytes (32 bits)

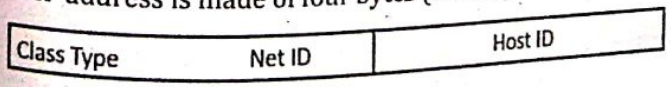


Figure 4.5 : IP address format

Notation:

Binary 10000000.00001011.00000011.00011111

Decimal 128 .11 .3 .31

IP address is generally written in dotted decimal notation.

2. **Classes of IP Address:**

There are different five classes; Class A, B, C, D, E. The class A, B, C are used for unicast, Class D is used for multicast and Class E is reserved. Each class occupies some part of the whole address space.

Nowadays, this concept has become obsolete and has been replaced with classless addressing. IP addresses, before 1993 use the classful addressing where classes have a fixed number of blocks and each block has a fixed number of hosts. In IPv4 addresses of class A, B & C, the first part of the address is considered as Network ID (Network id) and the second part of the address is called Host ID. The size of these parts varies with the classes.

- **Network ID:** The Network ID denotes the address of the network.
- **Host ID:** The Host ID denotes the address of the host attached to the corresponding network.

  In Class A, the Network ID is defined by the first byte of the address. And the rest 3 bytes define the Host ID.

  In Class B, the first two bytes of the address defines the network address and the rest two bytes defines the Host ID.

  In Class C the first three bytes define the network address and the last byte defines the Host ID.

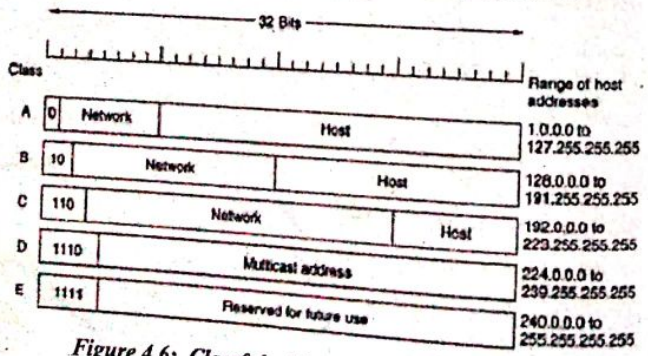


Figure 4.6: Classful address for class A, B, C, D, E

3. **Calculation of IP range**

Class A

00000000.00000000.00000000.00000000-
01111111.11111111.11111111.11111111

0.0.0.0 – 127.255.255.255

Similarly,

Class B 128.0.0.0 – 191.255.255.255

Class C 192.0.0.0 – 223.255.255.255

Class D 224.0.0.0 – 239.255.255.255

Class E 240.0.0.0 – 255.255.255.255

4. **Address Distribution Concept**

Class A net.host.host.host

network bits=7

host bits = 24

Total no. of network=2^7=128

Total no. of hosts = 2^{24} – 2 16777214

Class B net.net.host.host

network bits=14

host bits = 16

Total no. of network=2^{14}=16384

Total no. of hosts= 2^{16} – 2 = 65534

Class C net.net.net.host

network bits=21

host bits = 8

Total no. of network=2^{21}=2097152

Total no. of hosts= 2^8 – 2 = 254

Class D

- used as multicast IP
- it is a unique network that directs packets with that destination address to predefined groups for IP address.

Class E -reserved for future use

Table 4.1: Default mask for classful address

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

5. Disadvantages of Classful Addressing:

1. If we consider class A, the number of addresses in each block is more than enough for almost any organization. So, it results in wastage of addresses.
2. Same is the case with class B, probably an organization receiving blocks from class B would not require that much of addresses. So, it also results in wastage of addresses.
3. A block in class C may be too small to fulfil the addresses requirement of an organization.
4. Each address in class D defines a group of hosts. Hosts need to multicast the address. So, the addresses are wasted here too.
5. Addresses of class E are reserved for the future purpose which is also wastage of addresses.
6. In classful addressing, addresses are not assigned according to user requirements. Here, a block of a fixed size is directly assigned which has a fixed number of addresses which leads to wastage of address.

To overcome the flaws of classful addressing, subnetting and supernetting are introduced to compensate for the wastage of addresses.

6. Types of IP address

IP address is categorized into two types; Public IP and Private IP. Public IP is the number used on the Internet. Private IP: Any organization can use an address out of this set without permission from the Internet authorities. These addresses are free to use.

Address for private networks

Table 4.2: Address for private networks

Range			Total
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

7. IP (IPv4) Header Format:

An IPv4 datagram consists of a header part and a body or payload part. The header has a 20-byte fixed part and a variable-length optional part. The header format is shown above in figure. Every protocol follows a different header format for its data to be transmitted and received reliably.

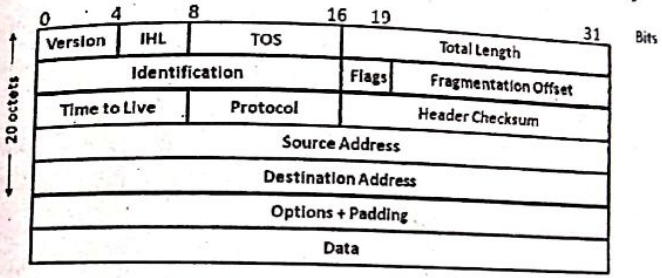


Figure 4.7: IPv4 Header

- **Version (4 Bits):** This field indicates the version number of the IP packet so that the revised version can be distinguished from the previous version. The current IP version is 4.
- **Internet Header Length (IHL) (4 Bits):** It specifies the length of the IP header in unit 32 bits. In case of no option present in the IP header, IHL will have a value of 5. So, if the value of IHL is more than 5 then the length of the option field can be easily calculated.
- **TOS (8 Bits):** This field is referred to as the Type of Service (e.g. text, audio, video etc.) and specifies the priority of the packets based on delay, throughput, reliability and cost requirements.

- **Total Length (16 Bits):** This field specifies the number of bytes of the IP packet including header and data. As 16 bits are assigned to this field, the maximum length of the packet is 65635 bytes.
- **Identification (16 Bits):** The identification field is used to identify which packet a particular fragment belongs to so that fragments for different packets don't get mixed up.
- **Flags (3 Bits):** It deals with fragmentation and reassembly of packets of data units. The flag field has three bits: Unused bit, Don't fragment (DF) bit and More fragment (MF) bit.
- **Fragment Offset (13 Bits):** The fragment offset field identifies the location of the fragment in a packet. The value measures the offset in a unit of 8 bytes, between the beginning of the packet to be fragmented and the beginning of the fragment.
- **Time to live (TTL) (8 Bits):** This field is used to indicate the amount of time in seconds a packet is allowed to remain in the network.
- **Protocol (8 Bits):** This field defines which upper layer protocol data are encapsulated in the datagram. This means that it selects the suitable protocol (e.g., connectionless or connection oriented) for next layer.
- **Header Checksum (16 Bits):** This field verifies the integrity of the header of the IP packet. The integrity of the data part is left to the upper layer protocols. The checksum is generated by the source and it is sent along with the frame header to the next router.
- **Source IP address (32 Bits) & Destination IP address (32 Bits):** These two fields contain the IP addresses of the source and destination hosts or network interfaces respectively.
- **Options + Padding (Variable):** Options fields are rarely used to include special features such as security level,

the route to be taken and time stamp at each router. Padding field is used to make the header a multiple of 32-bit words.

- **Data (Variable):** The data field must be an integer multiple of 8 bits in length. The maximum length of the datagram (data field plus header) is 65,535 Octets.

4.2.2 DHCP (Dynamic Host Configuration Protocol)

DHCP is a client- server protocol in which the client sends a request message and the server returns a response message. DHCP is used extremely in LANs and in residential internet access,

DHCP operation:

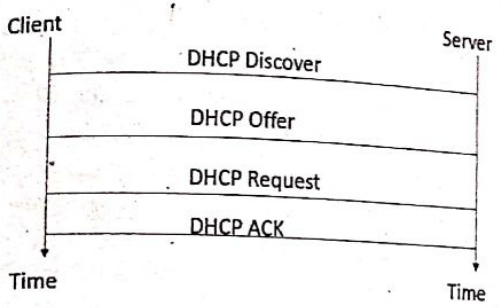


Figure 4.8: DHCP operation

The client broadcasts a DHCP DISCOVER message to identify any available DHCP servers on the network. A DHCP server replies with a DHCP OFFER message. This message offers to the client a lease that contains such information as the IP address and subnet mask to be assigned, the IP address of the DNS server, and the IP address of the default gateway. After the client receives the lease, the received information must be renewed through another DHCP REQUEST message prior to the lease expiration.

4.3 Subnetting

Subnetting is the technique of logical division of the large network into the smaller manageable sub-networks. It increases routing efficiency, enhances the security of the network and

reduces the size of the broadcast domain. Following are the advantages of subnetting.

- Subnetting breaks large networks in smaller networks and smaller networks are easier to manage.
- Subnetting reduces network traffic by removing collision and broadcast traffic, which overall improve performance.
- Subnetting allows applications to apply network security policies at the interconnection between subnets.
- Subnetting allows us to save money by reducing the requirement for IP range.

Each IP class is equipped with its own default subnet mask which binds that IP class to have a prefixed number of Networks and prefixed number of Hosts per network.

CIDR or Classless Inter Domain Routing provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

Subnet mask

A *subnet mask* is a 32-bit number that masks the IP address and divides the IP address into the network address and host address. It is used to extract the network address and subnetwork address from an IP address. For obtaining the subnet mask, assign all the network addresses as 1's and all the host address as 0's.

IP address ANDed with the subnet mask gives the network ID.

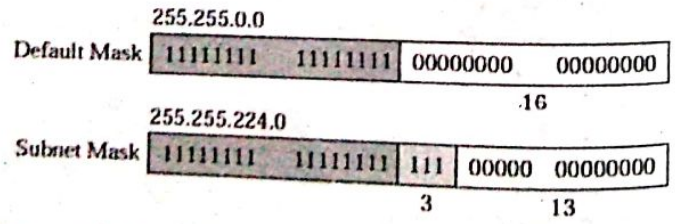


Figure 4.9: Class B network subnetted into 8 subnets

IP Subnetting Examples:

When subnetting a network, following five things should be determined:

1. Maximum number of subnets = $2^{\text{no. of subnet bits}}$
   Subnet bit is represented by '1'
2. Maximum number of hosts= $2^{\text{no. of host bits}} - 2$
   Host bit is represented by '0'
3. Valid subnets = 256-subnet mask = block size
4. Broadcast address for each subnet = the number right before the value of the next subnet.
5. Valid host = these are numbers between the subnet and broadcast address.

Example 1:

Given IP address: 130.45.32.56
Subnet Mask: 255.255.0.0
What is the subnet address?

Solution:

IP address in binary:

10000010.00101101.00100000.00111000

Subnet Mask in binary:

11111111.11111111.00000000.00000000

After binary ANDing IP with mask, we get the subnet address, which will be

10000010.00101101.00000000.00000000

i.e.,130.45.0.0 is the subnet address.

Example 2:

Given IP address 192.168.10.0/25

Solution:

25 means that the subnet mask has 25 bits 1s and 7 bits 0s. Since, the total Subnet Mask is 32 bits. So, in binary mode our Subnet Mask is:

11111111.11111111.11111111.10000000 (First 25 bits are 1s and 7 bits are 0s).

So, there is only 1 subnetting bit.

192.168.10.0 = Network Address

255.255.255.128 = Subnet mask

Maximum number of subnets $= 2^{\text{no. of subnet bits}}$

$= 2^1$

=2 subnets

Number of hosts per subnet $= 2^{\text{no. of host bits}} - 2$

$= 2^7 - 2$

= 126 hosts

Valid subnets= 256-subnet mask=256-128=128. Starting at zero and counting in block size, subnets are 0,128.

Broadcast address=the number right before the value of the next subnet. Here the broadcast address of 0 subnet is 127 i.e. 192.168.10.127 and for 128 subnet is 192.168.10.255.

Valid host is the numbers between the subnet and broadcast address. For 0 subnet valid host is 192.168.10.1-192.168.10.126 and for 128 subnet, valid host is 192.168.10.129 to 192.168.10.254

In tabular form,

Subnet Address	Valid host	Broadcast Address
192.168.10.0	192.168.10.1-192.168.10.126	192.168.10.127
192.168.10.128	192.168.10.129-192.168.10.254	192.168.10.255

Example 3:

Given IP address 192.168.5.85/24. Determine the network and host part of this address.

Solution:

IP Address: 192.168.5.85

Subnet Mask: 255.255.255.0

In binary mode,

IP Address: 11000000. 10101000. 00000101. 01010101

Subnet Mask: 11111111. 11111111. 11111111. 00000000

So, here, the first 24 bits (First 3 octets) are network bits and the last 8 bits (Last octet) are the host bits.

ANDing IP address and Subnet mask we get a network address that is 192.168.5.0.

Broadcast address is the last address i.e., 192.168.5.255

Valid host is the number between the network address and broadcast address i.e., 192.168.5.1- 192.168.5.254.

Example 4:

Given IP address 10.128.240.50/30. Determine network, broadcast and valid host address.

Solution:

IP Address: 10.128.240.50/30

/30 means that the subnet mask has 30 bits 1s and 2 bits 0s. Remember the total Subnet Mask is 32 bits. So, in binary mode our Subnet Mask is:

11111111.11111111.11111111.11111100

(First 30 bits are 1s and 2 bits are 0s)

And the decimal equal of this Subnet Mask is: 255.255.255.252

Valid subnet = 256-252=4

i.e., block size of 4. Starting from zero, it is 0, 4, 8, ..., 44 , 48, 52,....252.

ANDing IP address with Subnet mask gives network address.

IP Address: 00001010.10000000.11110000.00110010

Subnet Mask: 11111111.11111111.11111111.11111100

AND: 00001010.10000000.11110000.00110000

The result of AND operation is the Network Address.

This is 00001010.10000000.11110000.00110000 in binary. The decimal value of this is 10.128.240.48.

Here, the last two bits are host bits and the other bits are network bits. When we set all the host bits with 1s, we will find the Broadcast Address. This is 00001010.10000000.11110000.00110011 in binary. The decimal is value 10.128.240.51.

The middle addresses can be used for hosts. These addresses are 10.128.240.49 and 10.128.240.50.

Network Address: 10.128.240.48

Host Addresses: 10.128.240.49 and 10.128.240.50

Broadcast Address: 10.128.240.51

4.4 NAT (Network Address Translation)

NAT is the technology that allows a site to use a set of private addresses for internal communication and a set of global internet addresses for communication with the rest of the world.

The basic idea behind NAT is to assign each company a single IP address for Internet traffic. Within the company, every computer gets a unique IP address, which is used for routing internal traffic. However, when a packet exits the company and goes to the ISP, an address translation takes place.

In simple words, NAT translates public IP into private IP and vice versa.

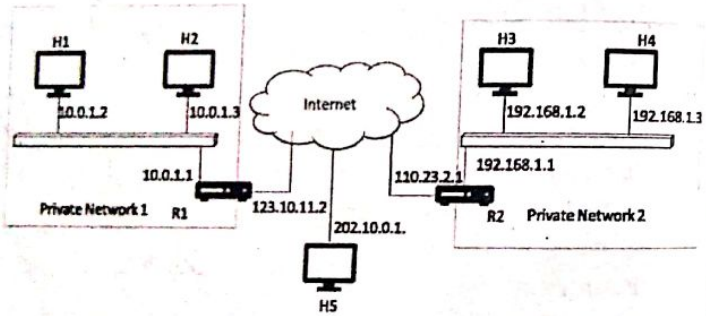


Figure 4.10: NAT operation

As in the figure, private networks use private addresses. The routers that connect the network to the global address or public address use one private address and one global address. All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address. The incoming packets also pass through the NAT router, which replaces the destination address in the packet with the appropriate private address. The private network is invisible to the rest of the Internet; rest of the Internet sees only the NAT router with the global address.

4.5 Routing

The main function of Network Layer is routing packets from the source machine to the destination machine. There are two processes inside router:

a. One of them handles each packet as it arrives, looking up the outgoing line to use for it in the routing table. This process is forwarding.

b. The other process is responsible for filling in and updating the routing tables. That is where the routing algorithm comes into play. This process is routing.

Routing is the process that a router uses to forward packets toward the destination network. The router makes the decision based upon the destination IP address of a packet. To make the correct decision, routers must learn how to reach remote networks. A routing protocol is used by routers to dynamically find all the networks in the internetwork and to ensure that all routers have the same routing table. Basically, a routing protocol determines the path of a packet through an internetwork, example RIP, OSPF etc. Once all routers know about the network, a routed protocol can be used to send user data through the established enterprise. Routed protocols are assigned to an interface and determine the methods of packet delivery, e.g., routed protocols are IP and IPv6.

The routing algorithm is the part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.

4.5.1 Criteria for Good Routing Algorithm

- **Correctness:** Choose correct route and should accurately deliver packets.
- **Robustness:** Adaptive to changes of network topology and varying traffic load.

- **Cleverness:** Ability to detour congestion links and determine the connectivity of the network.
- **Stability:** Avoiding the loops through the network when congestion.
- **Optimality and fairness:** Some performance criteria may give higher priority to the exchange of packets between nearby stations compared to an exchange between distant stations. This may maximize average throughput but will appear unfair to the station that primarily needs to communicate with distant stations.
- **Efficiency:** Rapid finding of the router and minimization of control messages.

4.5.2 Routing Techniques

There are two techniques of routing:

1. Non adaptive (Static routing)
2. Adaptive (Dynamic routing)

Regardless of whether routes are chosen independently for each packet or only when new connections are established, certain properties are desirable in a routing algorithm correctness, simplicity, robustness, stability, fairness, optimality.

1. Static Routing

In this technique, the router is configured manually. The choice of the route to use to get from I to J (for all I and is computed in advance, offline and downloaded to the router when the network is booked. The manual maintenance of the routing table for the large network could require a lot of administrative time. Sometimes a static router is used for the backup purpose.

Advantages of static routing:

- Easily implemented in a small network like LAN
- It provides more security and no advertisement send with data as in dynamic routing.
- It is very predictable, as the route to the destination is always the same.
- No complex algorithm is required
- Required no mechanism for updating
- Require no extra resources like CPU and memory etc.

Disadvantages of static routing:

- Only suitable for the small network cannot work for a large network
- Complexity automatically increases when the network grows.
- Managing static configuration in the large network becomes very complex and very time taking.
- If one link fails it affects the whole network
- In the failure of one link in static, it cannot route traffic.
- Manual intervention is required for re-routing traffic in the network.
- It cannot support complex routing algorithms.

2. Dynamic Routing

Dynamic routing makes it possible to avoid the configuration of the static routes. The router decision changes to reflect changes in the topology and usually the traffic as well. Adaptive algorithms differ in where they get their information (e.g. locally, from adjacent routers, or from all routers).

Advantages of dynamic routing:

- Suitable in all topologies where many routers are required.
- Easily used in a large network.
- Mostly independent to network size
- Failure of one link cannot affect the whole network
- In case of failure, a one link automatically re reroute without any manual intervention.
- It supports more complex routing algorithm.

Disadvantages of dynamic routing:

- More complex in implementation

- Less secure than static routing because of a multicast routing change
- An additional configuration setting is required such as a routing protocol, passive interfaces to increase security
- Required additional resources like memory CPU and link bandwidth.

Table 4.3: Comparison between static and dynamic routing

S. N.	Key	Static Routing	Dynamic Routing
1	Routing pattern	In static routing, user defined routes are used in the routing table.	In dynamic routing, routes are updated as per the changes in network.
2	Routing Algorithm	Simple routing used to figure out the shortest path.	Dynamic routing employs complex algorithms to find the shortest routes.
3	Security	Static routing provides higher security.	Dynamic routing is less secure.
4	Automation	Static routing is a manual process.	Dynamic routing is an automatic process.
5	Applicability	Static routing is used in smaller networks.	Dynamic routing is implemented in large networks.
6	Protocols	Static routing may not follow any specific protocol.	Dynamic routing follows protocols like BGP, RIP and EIGRP.

4.5.3 Routing Table for Classful Address

A *routing table* is a set of rules, often viewed in table format that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. 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. A basic routing table includes the following information:

- **Destination:** The IP address of the packet's final destination
- **Next hop:** The IP address to which the packet is forwarded
- **Interface:** The outgoing network interface the device should use when forwarding the packet to the next hop or final destination
- **Metric:** Assigns a cost to each available route so that the most cost-effective path can be chosen
- **Routes:** Includes directly-attached subnets, indirect subnets that are not attached to the device but can be accessed through one or more hops, and default routes to use for certain types of traffic or when information is lacking.

Routing tables can be maintained manually or dynamically. Tables for static network devices do not change unless a network administrator manually changes them. In dynamic routing, devices build and maintain their routing tables automatically by using routing protocols to exchange information about the surrounding network topology. Dynamic routing tables allow devices to "listen" to the network and respond to occurrences like device failures and network congestion.

4.5.4 Optimality Principle

It states that if the router J is on the optimal path form router I to router K, then the optimal path from J to K also falls along the same route. This can be elaborated as, call the part of the route from I to J as r1and rest of route as r2. If a router better than r2 existed form J to K, it could be concatenated with r1 to improve the route from I to K.

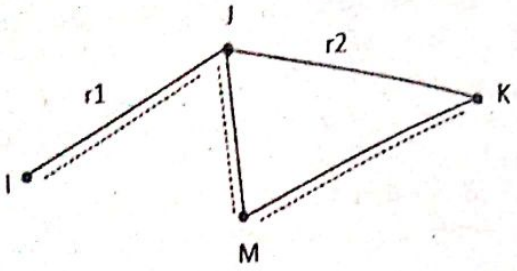


Figure 4.11: Optimality principle

4.6 Routing Algorithm

A *routing algorithm* is the part of network layer software responsible for deciding which output line and incoming packet should be transmitted on. The best path is one with minimum cost or shortest path.

4.6.1 Shortest Path Algorithm

Shortest path algorithm finds the shortest paths between routers/nodes in a graph. The widely used shortest path algorithm is Dijkstra's shortest path algorithm. It can also be used for finding the shortest paths from a single node to a single destination node by stopping the algorithm once the shortest path to the destination node has been determined.

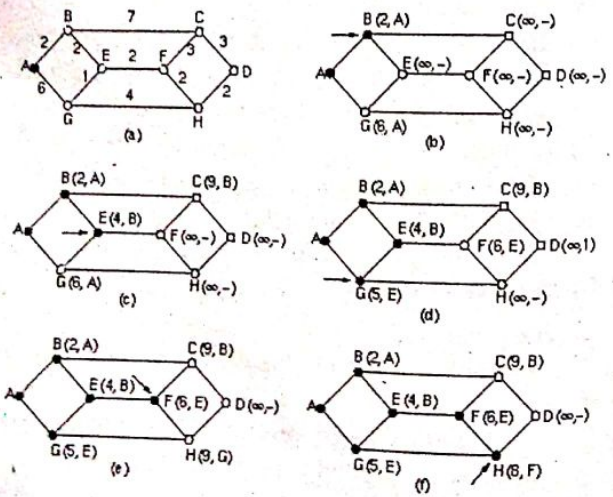


Figure 4.12: Shortest path algorithm

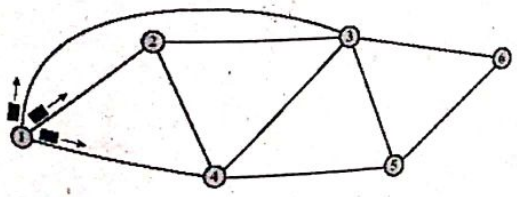
The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line or link. To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.

1. Start with the local node (router) as the root of the tree. Assign a cost of 0 to this node and make it the first permanent node.
2. Examine each neighbour of the node that was the last permanent node.
3. Assign a cumulative cost to each node and make it tentative
4. Among the list of tentative nodes a. Find the node with the smallest cost and make it Permanent b. If a node can be reached from more than one route then select the route with the shortest cumulative cost.
5. Repeat steps 2 to 4 until every node becomes permanent

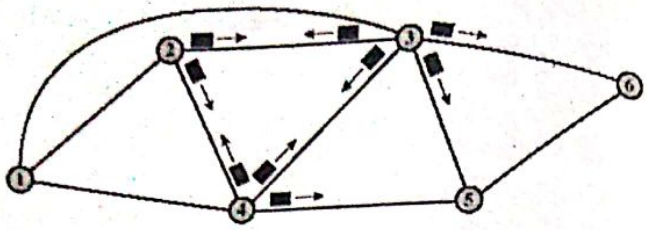
Packet is transmitting from A to D in above. Shortest path is ABEFHD

4.6.2 Flooding

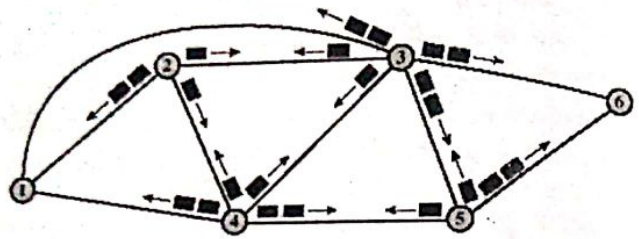
In this algorithm, every incoming packet is sent out on every outgoing line except the line of which it has arrived. One disadvantage of flooding algorithm is that it generates a large number of duplicate packets. To prevent endless copies of packets circulating indefinitely through the network a hop count may be used. Each router decrements a hop count contained in the packet header. Whenever the hop count decrements to zero, the router discards the packet. The advantage of flooding is at least one copy of the packet will arrive at the destination so the delivery is guaranteed.



(a) First hop



(b) Second hop



(c) Third hop

Figure 4.13: Flooding example (hop count = 3)

Ideally, the hop counter should be initialized to the length of the path from source to destination. A variation of flooding that is slightly more practical is selective flooding. In this algorithm the routers do not send every incoming packet out on every line, only on those lines that are going approximately in the right direction. Flooding is not practical in most applications.

4.6.3 Distance Vector Routing

Distance vector routing operates by having each router maintain a table (i.e. a vector) giving the best-known distance to each destination and which line to use to get there. In this routing algorithm, each router periodically shares its knowledge about the entire network with its neighbouring nodes.

Some of the keys to understand this algorithm are:

1. **Knowledge about the whole network**

   Each router shares its knowledge about the entire network. It sends all of its collected knowledge about the network to its neighbour.

2. **Routing only to neighbours**

   Each router periodically sends its knowledge about the entire network only to those routers to which it has direct links.

3. **Sharing information at regular intervals.**

   Each router sends its information about the whole network to its neighbour at regular intervals.

The Concept of Distance Vector Routing

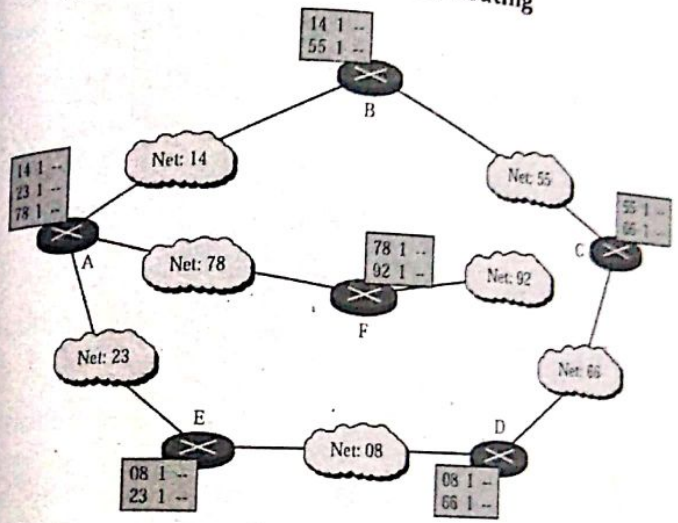


Figure 4.14: Initial routing table

The figure above shows the routing table distribution in distance vector routing. Here, clouds represent LANs and the number inside each cloud is LAN's network ID. LANs are connected by routers represented by the boxes A, B, C, D, E and F.

Upon receiving the updates for each destination in its table, it compares the metric in its local table with the metric in the neighbour's table plus the cost of reaching that neighbour. If the path via the neighbour has a lower cost, the router updates its local table to forward packets to the neighbour.

Updating routing table of router A:

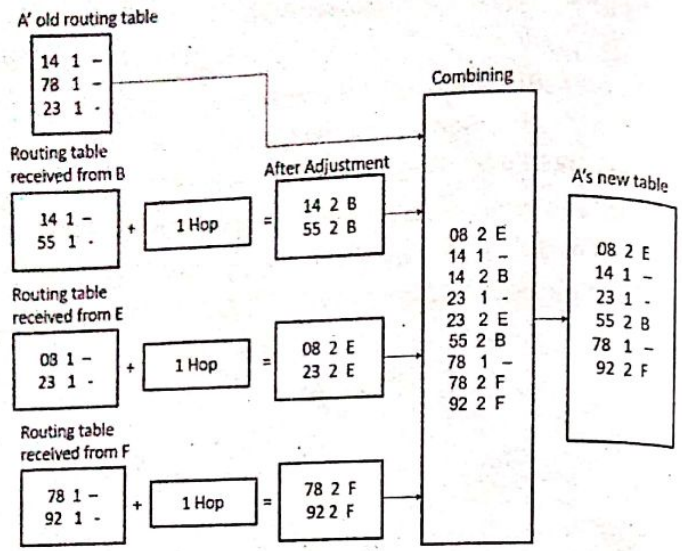


Figure 4.15: Updating routing table of router A

The final routing table for routers in the network is shown below:

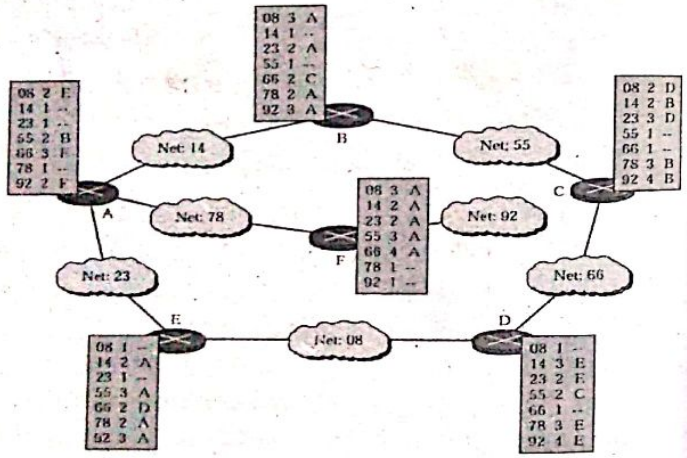


Figure 4.16: Final routing table

Drawbacks:

- The problem with distance vector routing is its slow in convergence.

- The algorithm does not take the line bandwidth into consideration when choosing route.
- May suffer from a routing loop called count-to- infinity problem.

Count to Infinity Problem

Count to infinity is just another name for a routing loop. In distance vector routing, routing loops usually occur when an interface goes down, or when two routers send updates to each other at the same time.

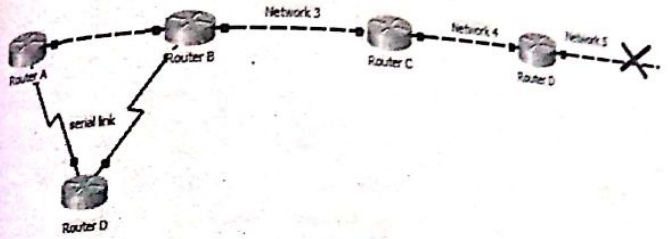


Figure 4.17: Count to infinity problem

When network 5 fails, router E tells router C. This causes router C to stop routing to network 5 through router E. But routers A, B, D don't know about network 5 yet, so they keep sending out update information. Router C will eventually send out its update and cause B to stop routing to network 5 but router A and D are still not updated. Due to this delay in information update, a routing loop occurs.

4.6.4 Link State Routing

Distance Vector Routing algorithm does not consider bandwidth. So, a new algorithm was introduced; link state routing. The idea behind link state routing is simple and can be stated as:

1. Discover its neighbours and then learn their network address
2. Measure the delay and cost to each of its neighbours.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other routers.

In link state routing, each router shares its knowledge of its neighbourhood with every other router in the internetwork.

Three keys to understand this algorithm are:

1. **Knowledge about the neighbourhood**

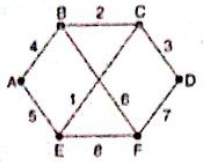
   Instead of sending its entire routing table, a router wends information about its neighbourhood only.

2. **Sharing information to all routers**

   Each router sends the information to every other router on the internetwork. It does so by a process called flooding.

3. **Information sharing when there is a change**

   Each router sends out information about the neighbours when there is a change.



Link State Packets

A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

Figure 4.18: A subnet and LSP (link state packets) for this subnet

The link-state routing algorithm maintains a complex database of topology information. The routing algorithm maintains full knowledge of distant routers and how they interconnect. Each node maintains the full graph by collecting the updates from all other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network. Router's receive topology information from their neighbour router via link state advertisements (LSA).

4.6.5 Hierarchical Routing

As a network becomes larger, the amount of information that must be propagated increases and the routing calculation becomes complex. Hierarchical Routing is an approach that hides information from far-away nodes, reducing the amount of information a given router to perform routing.

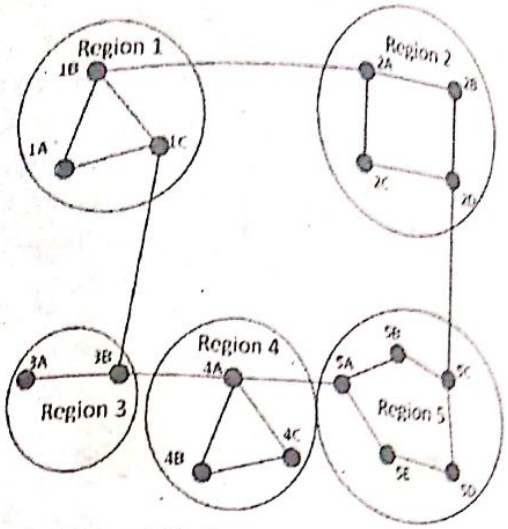


Figure 4.19: Network divided into regions

In this routing, routers are divided into regions. Routers know the routes for their own region only as shown in the figure.

Table 4.4: Full routing table and hierarchical routing table of 1A

Full table for 1A		
Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Hierarchical table for 1A		
Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

4.6.6 Unicast Routing

Simply unicast means one-to-one i.e. the transmission is done between two routers at a time. In this communication, sender sends the message to one side and the receiver receives the message to the other side. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to the next hop.

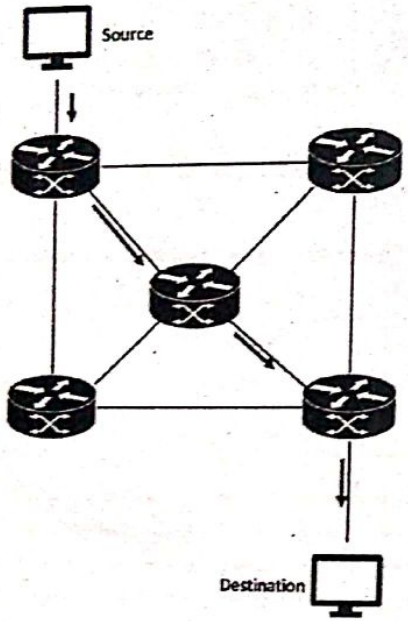


Figure 4.20: Unicast

4.6.7 Multicast Routing

Simply multicast means one-to-many i.e. the transmission is done between more than two routers at a time. In this transmission, there is one source and group of destinations. In certain applications, a process has to send a message to a well-defined group which is small compared to network size. Sending a message to such a group is multicasting and the routing algorithm used for multicasting is multicast routing.

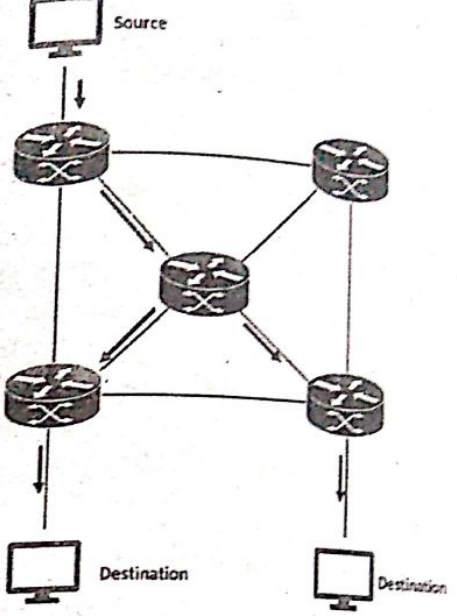


Figure 4.21: Multicast

4.7 Routing Protocols

A *routing protocol* is the implementation of a routing algorithm in software or hardware. A routing protocol uses metrics to determine which path to utilize to transmit a packet across an internetwork. It specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly.

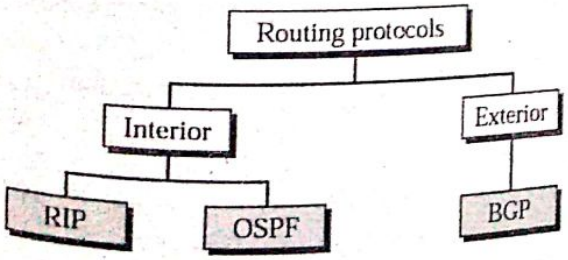


Figure 4.22: Classes of routing protocols

Before the classification of routing protocols, we need to know about the Autonomous system (AS). An Autonomous system is a group of networks and routers under the authority of a single administration.

Routing inside an autonomous system is referred to as interior routing. Routing between autonomous systems is referred to as exterior routing.

Each autonomous system can choose one or more interior routing protocols to handle routing inside the autonomous system. However, only one interior domain routing protocol handles routing between autonomous systems. RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) are popular routing protocols under the interior routing protocol. BGP (Border Gateway Protocol) is exterior routing protocol.

4.7.1 Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is an interior gateway routing protocol which is based on the distance vector routing. RIP defines how routers should share information when moving traffic among an interconnected group of local area networks (LANs). It employs the hop count as the routing metrics. Hop count is the number of a router the packet must travel till it reaches its destination. RIP uses the hop count to determine the best path between the router/location. Each router contains the RIP table and the table is updated every 30 seconds. Each router broadcasts its entire RIP table to its neighbour. Features of RIP are

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbour routers.

There are three versions of routing information protocol- RIP Version1, RIP Version2 and RIPng. RIP v1 is known as Classful Routing Protocol because it doesn't send information about subnet mask in its routing update. RIP v2 is known as Classless Routing Protocol because it sends information about subnet masks in its routing update.

The main limitations of RIP are followings:

- **Increased network traffic:** RIP checks with its neighbouring routers every 30 seconds, which increases network traffic.
- **Maximum hop count:** RIP has a maximum hop count of 15, which means that on large networks, other remote routers may not be able to be reached.
- **Closest may not be shortest:** Choosing the closest path by hop count does not necessarily mean that the fastest route was selected. RIP does not consider other factors when calculating the best path.
- RIP only updates neighbours so the updates for non-neighbouring routers are not first-hand information.

4.7.2 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is the routing algorithm that uses the link state routing algorithm. It is the shortest path algorithm to calculate the best path from the source to the destination. OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks. It falls into the group of interior routing protocols, operating within a single autonomous system (AS). OSPF doesn't need a high memory and high-speed processor.

Routers running OSPF need to establish the neighbour relationship before exchanging routing updates. Since OSPF is a link state routing protocol, neighbours don't exchange routing tables; instead, they exchange information about network topology. Each OSPF router then runs the SPF algorithm to calculate the best routes and adds those to the routing table. Since each router knows the entire topology of a network, a chance for a routing loop to occur is minimal.

For handling the routing efficiently and in a timely manner, the OSPF divides an AS into areas.

Features of OSPF:

- Consists of areas and an autonomous system.
- Minimizes routing update traffic

- Supports VLSM (Variable Length Subnet Masking)

OSPF routers stores routing and topology information in three tables:

- **Neighbour table:** stores information about OSPF neighbours.
- **Topology table:** stores the topology structure of the network.
- **Routing table:** stores the best routes.

4.7.3 Border Gateway Protocol (BGP)

Border Gateway Protocol is the Exterior Gateway Protocol which is used for communicating information among autonomous systems (AS) on the Internet. Neighbouring BGP routers i.e. BGP peers exchange detailed path information, widely used by Internet Service Providers (ISPs). It is also called the path vector routing algorithm. The protocols are more concerned with reachability than optimality.

Unlike an Interior Gateway Protocol (IGP), such as Open Shortest Path First (OSPF) and Routing Information Protocol (RIP), BGP is an Exterior Gateway Protocol (EGP) which controls route advertisement and selects optimal routes between ASs rather than discovering or calculating routes.

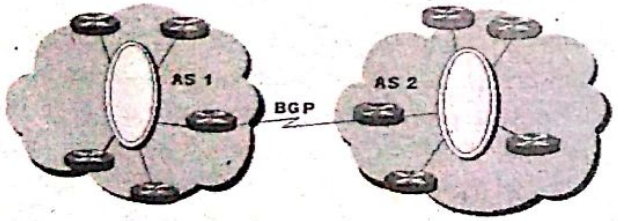


Figure 4.23: BGP communicating between two AS

BGP uses four types of messages for communication between BGP across the autonomous systems.

- **Open message:** open a BGP communication session between peer by TCP connection.
- **Update message:** used to provide routing updates to other BGP systems.

- **Keepalive message:** to inform BGP peers that a device is active.
- **Notification:** to alert an error condition or to close the session.

4.8 Internet Control Protocols

In order to transfer data, the internet has several control protocols used in the network layer. Some of them are ICMP, ARP, RARP, etc.

4.8.1 Internet Control Message Protocol (ICMP)

ICMP is a network layer protocol that helps IP to handle some errors that may occur in the network layer delivery. ICMP is used to test the Internet, which works at the Network layer.. ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute). It is management protocol and messaging service provider for IP.

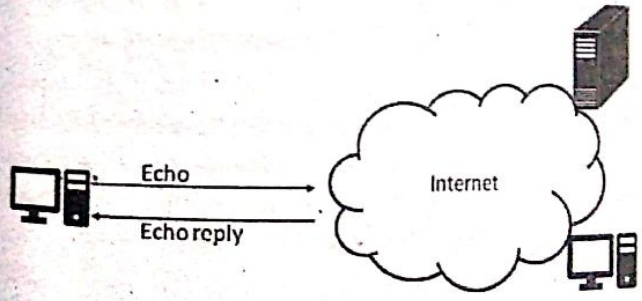


Figure 4.24: ICMP message

ICMP can provide hosts with information about network problems. They are encapsulated within IP datagram.

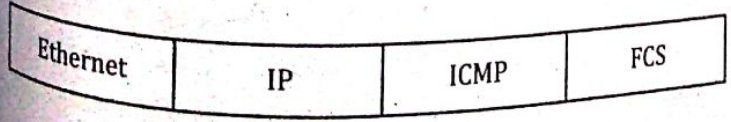


Figure 4.25: ICMP format

Some of the messages of ICMP are:

- **Destination unreachable:** When router cannot locate the destination.
- **Time exceeded:** When a packet is dropped because of time out.
- **Parameter Problem:** If a router discovers a missing value in any field of the datagram, it discards the datagram and the messages is sent to source.
- **Echo:** Used to see if a given destination is reachable alive.
- **Echo reply:** Upon receiving an echo message, the destination is expected to send an Echo Reply message back.

4.8.2 ARP (Address Resolution Protocol)

Address Resolution Protocol (ARP) is used to map the IP address to the MAC address. Sometimes it may happen that the source knows the IP address but not the Physical Address i.e. MAC address of the router. To find the destination address the router broadcast the IP address by asking what is the physical address of the router having this IP address? Then the router matching the IP address reply back to the source by sending the MAC address.

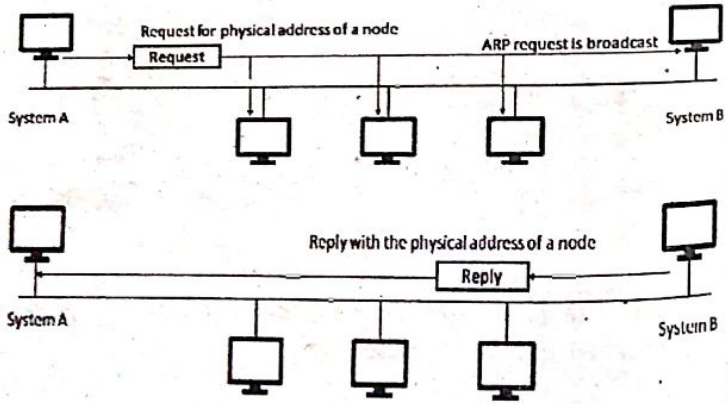


Figure 4.26: ARP protocol

To reduce the number of address resolution requests, a client normally caches resolved addresses for a (short) period of time. The ARP cache is of a finite size, and would become full of incomplete and obsolete entries for computers that are not in use if it was allowed to grow without check. The ARP cache is therefore periodically flushed of all entries. This deletes unused entries and frees space in the cache. It also removes any unsuccessful attempts to contact computers which are not currently running. If a host changes the MAC address it is using, this can be detected by other hosts when the cache entry is deleted and a fresh ARP message is sent to establish the new association. The use of gratuitous ARP (e.g. triggered when the new NIC interface is enabled with an IP address) provides a more rapid update of this information.

4.8.3 RARP (Reverse Address Resolution Protocol)

Reverse Address Resolution Protocol (RARP) is used to map the MAC address to the IP address. It is just the reverse of the ARP. To find the destination address the router broadcast the MAC address by asking what is the logical address of the router having this MAC address? Then the router matching the MAC address reply back to the source by sending the IP address.

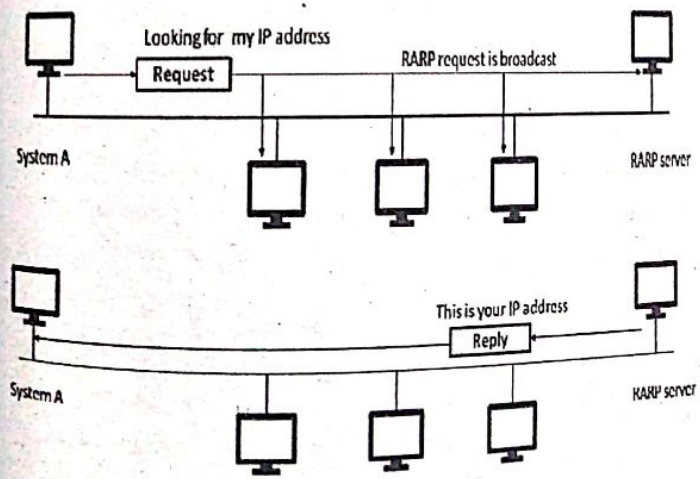


Figure 4.27: RARP protocol

SOLUTION TO IMPORTANT PROBLEMS

1. Design a network for 5 departments containing 29, 14, 15, 23, and 5 computers. Take a network example IP 202.83.54.91/25. [2075 Ashwin]

Solution:

Given IP: 202.83.54.91

Given mask:

255.255.255.128(11111111.11111111.11111111.10000000)/25

AND operation of 202.83.54.91 with 255.255.255.128 gives the network address i.e., 202.83.54.0

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 29 computers,

$29 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 5

Now, new subnet mask becomes,

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0,32, 64, ...)

Network address = 202.83.54.0

Broadcast address = 202.83.54.31

Range = difference of 32 (i.e., 0, 32, 64, ...)

Usable host range = 202.83.54.1-202.83.54.30

For 23 computers,

$23 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 5

Now, new subnet mask becomes,

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256 – 224 =32

Network address = 202.83.54.32

Broadcast address = 202.83.54.63

Usable host range = 202.83.54.33-202.83.54.62

For 15 computers,

$15 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 5

Now, new subnet mask becomes,

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256 – 224 = 32

Range = difference of 32 (i.e., 0, 32, 64, ...)

Network address = 202.83.54.64

Broadcast address = 202.83.54.95

Usable host range = 202.83.54.65-202.83.54.94

For 14 computers,

$14 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 4

Now, new subnet mask becomes,

11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256 – 240 = 16

Range = difference of 32 (i.e., 0, 16, 32, ...96, 112, ...)

Network address = 202.83.54.96

Broadcast address = 202.83.54.111

Usable host range = 202.83.54.97-202.83.54.110

For 5 computers,

$5 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 3

Now, new subnet mask becomes

11111111.11111111.11111111.11111000/29

i.e., 255.255.255.248

Subnet id = 256 – 248 = 8

Range = difference of 8 (i.e., 0, 8, 16, 32, ..., 112, 120, ...)

Network address= 202.83.54.112

Broadcast address=202.83.54.119

Usable host range= 202.83.54.113-202.83.54.118

No. of Computers	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
29	202.83.54.0	202.83.54.1-202.83.54.30	202.83.54.31	255.255.255.224
23	202.83.54.32	202.83.54.33-202.83.54.62	202.83.54.63	255.255.255.224
15	202.83.54.64	202.83.54.64-202.83.54.94	202.83.54.95	255.255.255.224
14	202.83.54.96	202.83.54.97-202.83.54.110	202.83.54.111	255.255.255.240
5	202.83.54.112	202.83.54.113-202.83.54.118	202.83.54.119	255.255.255.248

2. Banijya bank need to allocate 15 IPs in HR department; 30 in finance department, 24 in customer care unit and 25 in ATM machines. If you have one network of class C range public IP address. Describe how you will manage it. [2069 Chaitra]

Solution:

Let the network address be 200.10.10.0/24 (class C public IP). We will perform the subnetting to allocate the required number of IPs in different departments.

First, we start with the department that needs the maximum no of IPs.

In the finance department, we need 30 IPs.

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

or, $30 = 2^{\text{no. of host bits}} - 2$

∴ No. of host bits =5

Subnet mask becomes,

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 =32.

Range = 0, 32, 64, ...

Network address = 200.10.10.0

Broadcast address = 200.10.10.31

Usable host range = 200.10.10.1-200.10.10.30

In ATM machines, we need 25 IPs.

No. of host bits = 5

So, the subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = 0, 32, 64,...

Network address = 200.10.10.32

Broadcast address = 200.10.10.63

Usable host range = 200.10.10.33-200.10.10.62

In customer care, we need 24 IPs.

No. of host bits = 5

So, the subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = 0, 32, 64, 96...

Network address = 200.10.10.64

Broadcast address = 200.10.10.95

Usable host range = 200.10.10.65-200.10.10.94

Finally, the HR department needs 15 IPs.

$15 = 2^{\text{no. of host bits}} - 2$

∴no. of host bits = 5

So, the subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range=0,32,64,96,128, ..

Network address = 200.10.10.96

Broadcast address = 200.10.10.127

Usable host range = 200.10.10.97-200.10.10.126

No. of IP needed	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
30	200.10.10.0	200.10.10.1-200.10.10.30	200.10.10.31	255.255.255.224
25	200.10.10.32	200.10.10.33-200.10.10.62	200.10.10.63	255.255.255.224
24	200.10.10.64	200.10.10.65-200.10.10.94	200.10.10.95	255.255.255.224
15	200.10.10.96	200.10.10.97-200.10.10.126	200.10.10.127	255.255.255.224

3. A large number of consecutive IP addresses are available at 202.70.64.0/19. Suppose that four organizations A, B, C and D request 100, 500, 800 and 400 addresses respectively, how the subnetting can be performed so that address wastage will be minimum?

[2070 Magh, 2073 Shrawan]

Solution:

Given IP: 202.70.64.0 /19

Given mask:

255.255.224.0 (11111111.11111111.11100000.00000000)/19

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 800 addresses,

$800 = 2^{\text{no. of host bits}} - 2$

4 no. of host bits = 10

Now, new subnet mask becomes

11111111.11111111.11111100.00000000/22

i.e., 255.255.252.0

Subnet id = 256-252=4

Range = difference of 4 (i.e., 0,4, ... , 64,68,...)

Network address = 202.70.64.0

Broadcast address =202.70.67.255

Usable host range = 202.70.64.1- 202.70.67.254

For 500 hosts,

$500 = 2^{\text{no. of host bits}} - 2$

∴ No. of host bits = 9

Now, new subnet mask becomes

11111111.11111111.11111110.00000000/23

i.e., 255.255.254.0

Subnet id= 256-254=2

Range = difference of 2

Network address = 202.70.68.0

Broadcast address = 202.70.69.255

Usable host range = 202.70.68.1- 202.70.69.254

For 400 hosts,

No. of host bits = 9

Now, new subnet mask

11111111.11111111.11111110.00000000/23

i.e., 255.255.254.0

Subnet id = 256 – 254 = 2

Range = difference of 2

Network address = 202.70.70.0

Broadcast address = 202.70.71.255

Usable host range = 202.70.70.1- 202.70.71.254

For 100 hosts,

$100 = 2^{\text{no. of host bits}} - 2$

∴ No. of host bits = 7

Now, new subnet mask becomes

11111111.11111111.11111111.10000000/25

i.e., 255.255.255.128

Subnet id = 256 – 128 = 128

Range = 0,128

Network address = 202.70.72.0

Broadcast address = 202.70.72.127

Usable host range = 202.70.72.1- 202.70.72.127

Organization	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
C (800)	202.70.64.0	202.70.64.1-202.70.67.254	202.70.67.255	255.255.252.0
B (500)	202.70.68.0	202.70.68.1-202.70.69.254	202.70.69.255	255.255.254.0
D (400)	202.70.70.0	202.70.70.1-202.70.71.254	202.70.71.255	255.255.254.0
A (100)	202.70.72.0	202.70.72.1-202.70.72.126	202.70.72.127	255.255.255.128

4. A large number of consecutive IP addresses are available starting at 192.122.2.1. Suppose that four organizations Pulchowk, Thapathali, WRC, and ERC request 6000, 2000, 4000, and 2500 addresses respectively. Design the network and find the first valid IP address, last IP address and mask in x.y.z/s notation for each organization. [2070 Bhadra]

Solution:

Given IP: 192.122.2.1 (starting address)

We have,

Maximum number of host = $2^{\text{no. of host bits}} - 2$

For 6000 addresses,

$6000 = 2^{\text{no. of host bits}} - 2$

$\therefore$ No. of host bits = 13

Now, new subnet mask becomes

11111111.11111111.11100000.00000000/19

i.e., 255.255.224.0

Subnet id= 256-224=32

Range = difference of 32 (i.e., 0, 32, 64, ...)

Since the available starting IP is 192.122.2.1, we need to calculate the network address of the given IP.

ANDing 192.122.2.1 with 255.255.224.0 we get network address as 192.122.0.0.

Network address = 192.122.0.0

Broadcast address = 192.122.31.255

Usable host range = 192.122.2.1-192.122.31.254

For 4000 addresses,

$4000 = 2^{\text{no. of host bits}} - 2$

$\therefore$No. of host bits = 12

Now, new subnet mask

= 11111111.11111111.11110000.00000000/20

i.e., 255.255.240.0

Subnet id = 256 – 240 = 16

Range = 0,16,32,48,64 ,...

Network address= 192.221.32.0

Broadcast address=192.221.47.255

Usable host range= 192.221.32.1-192.221.47.254

For 2500 addresses,

No. of host bits = 12

Now, new subnet mask becomes

11111111.11111111.11110000.00000000/20

i.e., 255.255.240.0

Subnet id = 256 – 240 = 16

Range = difference of 16

Network address = 192.221.48.0

Broadcast address = 192.221.63.255

Usable host range = 192.221.49.1-192.221.63.254

For 2000 addresses,

$2000 = 2^{\text{no. of host bits}} - 2$

∴ No. of host bits = 11

Now, new subnet mask becomes

11111111.11111111.11111000.00000000/21

i.e., 255.255.248.0

Subnet id = 256 – 248 = 8

Range = difference of 8

Network address = 192.221.64.0

Broadcast address = 192.221.71.255

Usable host range = 192.221.64.1-192.221.71.254

Organization	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
Pulchowk (6000)	192.221.0.0	192.221.2.1-192.221.31.254	192.221.31.255	255.255.224.0/19
WRC (4000)	192.221.32.0	192.221.32.1-192.221.47.254	192.221.47.255	255.255.240.0/20
ERC (2500)	192.221.48.0	192.221.48.1-192.221.63.254	192.221.63.255	255.255.240.0/20
Thapathali (2000)	192.221.64.0	192.221.64.1-192.221.71.254	192.221.71.255	255.255.248.0/21

5. How can you dedicate 10,12,8,14 public IP addresses to department A, B, C, and D respectively from the pool of class C with minimum losses of IP? Explain.

[2070 Chaitra]

Solution:

Suppose the IP be 190.16.0.0/24

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 14 addresses,

$14 = 2^{\text{no. of host bits}} - 2$

∴No. of host bits = 4

Now, new subnet mask

= 11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256 – 240 = 16

Range = difference of 4 (i.e., 0,16, 32,...)

Network address = 190.16.0.0

Broadcast address = 190.16.0.15

Usable host range = 190.16.0.1-190.16.0.14

For 12 addresses,

$12 = 2^{\text{no. of host bits}} - 2$

∴No. of host bits = 4

Now, new subnet mask becomes

11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256 – 240 = 16

Range = difference of 4 (i.e., 0,16, 32, ...)

Network address = 190.16.0.16

Broadcast address = 190.16.0.31

Usable host range = 190.16.0.17-190.16.0.30

For 10 addresses,

No. of host bits = 4

Now, new subnet mask becomes

11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256 – 240 = 16

Range = difference of 4 (i.e., 0,16, 32, 48,...)

Network address = 190.16.0.32

Broadcast address = 190.16.0.47

Usable host range = 190.16.0.33-190.16.0.46

For 8 addresses,

No. of host bits = 4

Now, new subnet mask

11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256 – 240=16

Range = difference of 4 (i.e., 0,16,32,48,64, ...)

Network address = 190.16.0.48

Broadcast address = 190.16.0.63

Usable host range = 190.16.0.49-190.16.0.62

Departme-nt	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
D (14)	190.16.0.0	190.16.0.1-190.16.0.14	190.16.0.15	255.255.255.24
B (12)	190.16.0.16	190.16.0.17-190.16.0.30	190.16.0.31	255.255.255.24
C (10)	190.16.0.32	190.16.33-190.16.0.46	190.16.0.47	255.255.255.24
D (8)	190.16.0.48	190.16.0.49-190.16.0.62	190.16.0.63	255.255.255.24

6. What is subnet masking? If there are 5 departments which require 27, 28, 7, 12, 8 hosts respectively. Design the subnet with minimum loss of IPs and write the starting and ending address of each subnet.

[2071 Magh]

Solution:

Subnet masking extracts the network address from an IP address when subnetting is not used. It extracts the subnetwork address from an IP address when subnetting is used.

For example, a packet addressed to 130.45.34.56 with subnet mask 255.255.0.0, we will extract the subnetwork address by binary AND operation given IP address and subnet mask.

IP : 10000010.00101101.00100010.00111000

Mask : 11111111.11111111.00000000.00000000

ANDing

10000010.00101101.00000000.00000000

130.45.0.0 is the subnet address.

Numerical solution:

Suppose IP be 192.168.0.0 /24

Given mask:

255.255.224.0 (11111111.11111111.11111111.00000000)/19

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 28 addresses,

$28 = 2^{\text{no. of host bits}} - 2$

∴ No. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256 – 224 = 32

Range = difference of 32 (i.e., 0, 32, 64,...)

Network address = 192.168.0.0

Broadcast address = 192.168.0.31

Usable host range = 192.168.0.1-192.168.0.30

For 27 hosts,

No. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

255.255.255.224

Subnet id = 256 –224 = 32

Range = difference of 32 (i.e., 0, 32, 64, ...)

Network address = 192.168.0.32

Broadcast address = 192.168.0.63

Usable host range = 192.168.0.33-192.168.0.62

For 12 hosts,

No. of host bits = 4

Now, new subnet mask

= 11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256 – 240 = 16

Range = difference of 16 (0,16, 32, 48, 64, 80, ...)

Network address = 192.168.0.64

Broadcast address=192.168.0.79

Usable host range = 192.168.0.65-192.168.0.78

For 8 hosts,

$8 = 2^{\text{no. of host bits}} - 2$

∴ No. of host bits = 4

Now, new subnet mask becomes

11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256 – 240 = 16

Range = difference of 16 (0, 16, 32, 48, 64, 80, ...)

Network address = 192.168.0.80

Broadcast address = 192.168.0.95

Usable host range = 192.168.0.81-192.168.0.94

For 7 hosts,

$8 = 2^{\text{no. of host bits}} - 2$

∴ No. of host bits = 4

Now, new subnet mask becomes

11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256 –240 = 16

Range = difference of 16 (0, 16, 32, 48, 64, 80, ...)

Network address = 192.168.0.96

Broadcast address = 192.168.0.111

Usable host range = 192.168.0.97-192.168.0.110

Organization	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
28	192.168.0.0	192.168.0.1-192.168.0.30	192.168.31	255.255.255.224
27	192.168.0.32	192.168.0.33-192.168.0.62	192.168.63	255.255.255.224
12	192.168.0.64	192.168.0.65-192.168.0.78	192.168.79	255.255.255.240
8	192.168.0.80	192.168.0.81-192.168.0.94	192.168.95	255.255.255.240
7	192.168.0.96	192.168.0.97-192.168.0.110	192.168.0.111	255.255.255.240

7. You are given the following address space 10.10.10.0/24. You have to assign addresses to 4 departments with the following hosts 5, 16, 23 and 27 respectively. Perform the subnetting in such a way that the IP address wastage in each department is minimum. Also find out the subnet mask, network address, broadcast address, and unassigned range in each department. [2071 Chaitra]

Solution:

Given IP: 10.10.10.0/24

Given mask:

255.255.255.0 (11111111.11111111.11111111.00000000)/24

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 27 addresses,

$27 = 2^{\text{no. of host bits}} - 2$

∴ No. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256 – 224 = 32

Range = difference of 32 (i.e., 0, 32, 64, ...)

Network address = 10.10.10.0

Broadcast address = 10.10.10.31

Usable host range = 10.10.10.1-10.10.10.30

For 23 hosts,

No. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256 – 224 = 32

Range = difference of 32 (i.e., 0, 32, 64, ...)

Network address = 10.10.10.32

Broadcast address = 10.10.10.63

Usable host range = 10.10.10.33- 10.10.10.62

For 16 hosts,

No. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256 – 224 = 32

Range = difference of 32 (i.e., 0,32,64,96...)

Network address = 10.10.10.64

Broadcast address = 10.10.10.95

Usable host range = 10.10.10.65- 10.10.10.94

For 5 hosts,

$5 = 2^{\text{no. of host bits}} - 2$

∴ No. of host bits = 3

Now, new subnet mask becomes

11111111.11111111.11111111.11111000/29

i.e., 255.255.255.248

Subnet id = 256 – 248 = 8

Range = difference of 8

Network address = 10.10.10.96

Broadcast address = 10.10.10.103

Usable host range = 10.10.10.97-10.10.10.102

Department	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
27	10.10.10.0	10.10.10.1-10.10.10.30	10.10.10.31	255.255.255.224
23	10.10.10.32	10.10.10.33-10.10.10.62	10.10.10.63	255.255.255.224
16	10.10.10.64	10.10.10.65-10.10.10.94	10.10.10.95	255.255.255.224
5	10.10.10.96	10.10.10.97-10.10.10.102	10.10.10.103	255.255.255.248

8. Design IPv4 sub network for an organization having 16, 48, 61, 32, and 24 computers in each department. Use 192.168.5.0/24 to distribute the network. [2072 Magh]

Solution:

Given IP: 192.168.5.0

Given mask:

255.255.255.0 (11111111.11111111.11111111.00000000)/24

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 61 computers,

$61 = 2^{\text{no. of host bits}} - 2$

∴No. of host bits = 6

Now, new subnet mask becomes

11111111.11111111.11111111.11000000/26

i.e., 255.255.255.192

Subnet id = 256 – 192 = 64

Range = difference of 64 (i.e., 0, 64, 128, ...)
Network address = 192.168.5.0
Broadcast address = 192.168.5.63
Usable host range = 192.168.5.1-192.168.5.62
For 48 computers,
No. of host bits = 6
Now, new subnet mask becomes
11111111.11111111.11111111.11000000/26
i.e., 255.255.255.192
Subnet id = 256 −192 = 64
Range = difference of 64 (i.e., 0, 64, 128, ...)
Network address = 192.168.5.64
Broadcast address = 192.168.5.127
Usable host range = 192.168.5.65-192.168.5.126
For 32 computers,
No. of host bits = 6
Now, new subnet mask becomes
11111111.11111111.11111111.11000000/26
i.e., 255.255.255.192
Subnet id = 256 − 192 = 64
Range = difference of 64 (i.e., 0, 64, 128, ...)
Network address = 192.168.5.128
Broadcast address = 192.168.5.191
Usable host range = 192.168.5.129-192.168.5.190
For 24 computers,
No. of host bits = 5
Now, new subnet mask becomes
11111111.11111111.11111111.11100000/27
i.e., 255.255.255.224
Subnet id = 256 − 224 = 32
Range = difference of 32 (i.e., 0, 32, 64, ...)

Network address = 192.168.5.192
Broadcast address = 192.168.5.223
Usable host range = 192.168.5.193-192.168.5.222
For 16 computers,
No. of host bits = 5
Now, new subnet mask becomes
11111111.11111111.11111111.11100000/27
i.e., 255.255.255.224
Subnet id = 256 −224 = 32
Range = difference of 32 (i.e., 0, 32, 64, ...)
Network address = 192.168.5.224
Broadcast address = 192.168.5.255
Usable host range = 192.168.5.225-192.168.5.254

Organization	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
61	192.168.5.0	192.168.5.1-192.168.5.63	192.168.5.63	255.255.255.192
48	192.168.5.64	192.168.5.65-192.168.5.126	192.168.5.127	255.255.255.192
32	192.168.5.128	192.168.5.129-192.168.5.190	192.168.5.191	255.255.255.192
24	192.168.5.192	192.168.5.193-192.168.5.222	192.168.5.223	255.255.255.224
16	192.168.5.224	192.168.5.225-192.168.5.254	192.168.5.255	255.255.255.224

9. **Design a network for the Institute of Engineering Central Campus, Pulchowk having 5 departments having 45, 35, 40, 23, and 30 computers in their respective network by allocating public IP to each computer with minimum losses. Assume IP by yourself.** [2072 Ashwin]

Solution:

Suppose public IP be 200.10.10.0/24
We have,

Maximum number of host = $2^{\text{no. of host bits}} - 2$

For 45 computers,

$45 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 6

Now, new subnet mask becomes

11111111.11111111.11111111.11000000/26

i.e., 255.255.255.192

Subnet id = 256-192 = 64

Range = difference of 64 (i.e., 0, 64,128,...)

Network address = 200.10.10.0

Broadcast address = 200.10.10.63

Usable host range = 200.10.10.1-200.10.10.62

For 40 hosts,

no. of host bits = 6

Now, new subnet mask becomes

11111111.11111111.11111111.11000000/26

i.e., 255.255.255.192

Subnet id = 256-192 = 64

Range = difference of 64 (i.e., 0, 64,128, ...)

Network address = 200.10.10.64

Broadcast address = 200.10.10.127

Usable host range = 200.10.10.65-200.10.10.126

For 35 hosts,

no. of host bits = 6

Now, new subnet mask becomes

11111111.11111111.11111111.11000000/26

i.e., 255.255.255.192

Subnet id = 256-192 = 64

Range = difference of 64 (i.e., 0, 64,128, ...)

Network address = 200.10.10.128

Broadcast address = 200.10.10.191

Usable host range = 200.10.10.129-200.10.10.190

For 30 hosts,

no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = 0, 32, ...192,224,

Network address = 200.10.10.192

Broadcast address = 200.10.10.223

Usable host range = 200.10.10.193-200.10.10.222

For 23 hosts,

no. of host bits = 5

Now, new subnet mask

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = 0, 32, ...192,224,

Network address = 200.10.10.224

Broadcast address = 200.10.10.255

Usable host range = 200.10.10.225-200.10.10.254

Organization	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
45	200.10.10.0	200.10.10.1-200.10.10.62	200.10.10.63	255.255.255.192
40	200.10.10.64	200.10.10.65-200.10.10.126	200.10.10.127	255.255.255.192
35	200.10.10.128	200.10.10.129-200.10.10.190	200.10.10.191	255.255.255.192
30	200.10.10.192	200.10.10.193-200.10.10.222	200.10.10.223	255.255.255.224
23	200.10.10.224	200.10.10.225-200.10.10.254	200.10.10.255	255.255.255.224

10. Explain how you can allocate 30,24,25 and 20 IP addresses to the four different departments of ABC company with minimum wastage. Specify the range of IP addresses, Broadcast Address, Network Address and Subnet mask for each department form the given address pool 202.77.19.0/24. [2072 Chaitra]

Solution:

Given IP: 202.77.19.0

Given mask:

255.255.255.0 (11111111.11111111.11111111.00000000)/24

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 30 addresses,

$30 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0, 32, 64, ...)

Network address = 202.77.19.0

Broadcast address = 202.77.19.31

Usable host range = 202.77.19.1-202.77.19.30

For 25 hosts,

$25 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id= 256-224=32

Range = difference of 32 (i.e., 0, 32, 64, ...)

Network address = 202.77.19.32

Broadcast address = 202.77.19.63

Usable host range = 202.77.19.33-202.77.19.62

For 24 hosts,

no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0, 32, 64, ...)

Network address = 202.77.19.64

Broadcast address = 202.77.19.95

Usable host range = 202.77.19.65-202.77.19.94

For 20 hosts,

no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0, 32, 64, ...)

Network address = 202.77.19.96

Broadcast address =202.77.19.127

Usable host range = 202.77.19.97-202.77.19.126

Organization	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
30	202.77.19.0	202.77.19.1-202.77.19.30	202.77.19.31	255.255.255.224
25	202.77.19.32	202.77.19.33-202.77.19.62	202.77.19.63	255.255.255.224
24	202.77.19.64	202.77.19.65-202.77.19.94	202.77.19.95	255.255.255.224
20	202.77.19.96	202.77.19.97-202.77.19.126	202.77.19.127	255.255.255.224

11. You are given the IP address block 201.40.58.0/24. Design the subnet for 49, 27, 11, and 45 hosts group so that IP address wastage is minimum. Find subnet mask, network ID, broadcast ID, assigned IP and unassigned IP range in each department. [2073 Magh]

Solution:

Given IP: 201.40.58.0

Given mask:

255.255.255.0 (11111111.11111111.11111111.00000000)/24

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 49 addresses,

$49 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 6

Now, new subnet mask becomes

11111111.11111111.11111111.11000000/26

i.e., 255.255.255.192

Subnet id = 256-192 = 64

Range = difference of 64 (i.e., 0, 64, 128, ...)

Network address = 201.40.58.0

Broadcast address = 201.40.58.63

Usable host range = 201.40.58.1-201.40.58.62

For 45 hosts,

no. of host bits = 6

Now, new subnet mask becomes

11111111.11111111.11111111.11000000/26

i.e., 255.255.255.192

Subnet id= 256-192=64

Range = difference of 64 (i.e., 0, 64, 128, ...)

Network address = 201.40.58.64

Broadcast address = 201.40.58.127

Usable host range = 201.40.58.65-201.40.58.126

For 27 hosts,

$27 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0, 32, 64, ...)

Network address = 201.40.58.128

Broadcast address = 201.40.58.159

Usable host range = 201.40.58.129-201.40.58.158

For 11 hosts,

no. of host bits = 4

Now, new subnet mask becomes

11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256-240 = 16

Range = 0, 16, ...128,144,160,176

Network address = 201.40.58.160

Broadcast address =201.40.58.175

Usable host range = 201.40.58.161-201.40.58.174

Organization	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
49	201.40.58.0	201.40.58.1-201.40.58.62	201.40.58.63	255.255.255.192
45	201.40.58.64	201.40.58.65-201.40.58.126	201.40.58.127	255.255.255.192
27	201.40.58.128	201.40.58.129-201.40.58.158	201.40.58.159	255.255.255.224
11	201.40.58.160	201.40.58.161-201.40.58.174	201.40.58.175	255.255.255.240

12. Suppose we have 4 departments A, B, C and D having 25 hosts, 16 hosts, 29 hosts and 11 hosts respectively. You are given a network 202.70.91.0/24. Perform the subnetting in such a way that the IP address wastage in

each department is minimum and find out the subnet mask, network address, broadcast address, and usable host range in each department. [2073 Chaitra]

Solution:

Given IP: 202.70.91.0 /24

Given mask: 255.255.255.0

11111111.11111111.11111111.00000000/24

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 29 hosts,

$29 = 2^{\text{no. of host bits}} - 2$

∴no. of host bits =5

Now, new subnet mask becomes

= 11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = 0, 32, 64, ...

Network address = 202.70.91.0

Broadcast address = 202.70.91.31

Usable host range = 202.70.91.1- 202.70.91.30

For 25 hosts,

no. of host bits =5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = 0, 32, 64, ...

Network address = 202.70.91.32

Broadcast address = 202.70.91.63

Usable host range = 202.70.91.33- 202.70.91.62

For 16 hosts,

no. of host bits =5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224=32

Range = 0, 32, 64,96 ....

Network address = 202.70.91.64

Broadcast address = 202.70.91.95

Usable host range = 202.70.91.65- 202.70.91.94

For 11 hosts,

no. of host bits = 4

Now, new subnet mask becomes

11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256-240 = 16

Range = 0, 16,32,64,96,112, ...

Network address = 202.70.91.96

Broadcast address = 202.70.91.111

Usable host range = 202.70.91.97- 202.70.91.110

No. of Hosts	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
29	202.70.91.0	202.70.91.1- 202.70.91.30	202.70.91.31	255.255.255.224
25	202.70.91.32	202.70.91.33- 202.70.91.62	202.70.91.94.63	255.255.255.224
16	202.70.91.64	202.70.91.65- 202.70.91.94	202.70.91.95	255.255.255.224
11	202.70.91.96	202.70.91.97- 202.70.91.110	202.70.91.111	255.255.255.240

13. Design a network for 5 departments containing 29, 14, 15, 23, and 5 computers. Take a network example IP 202.83.54.91/25. [2075 Ashwin]

Solution:

Given IP: 202.83.54.91

Given mask:

255.255.255.128(11111111.11111111.11111111.10000000)/25

AND operation of 202.83.54.91 with 255.255.255.128 gives the network address i.e., 202.83.54.0

We have,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 29 computers,

$29 = 2^{\text{no. of host bits}} - 2$

∴no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0,32, 64, ...)

Network address = 202.83.54.0

Broadcast address = 202.83.54.31

Usable host range = 202.83.54.1-202.83.54.30

For 23 computers,

no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0,32, 64, ...)

Network address = 202.83.54.32

Broadcast address = 202.83.54.63

Usable host range = 202.83.54.33-202.83.54.62

For 15 computers,

$15 = 2^{\text{no. of host bits}} - 2$

∴no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0,32, 64,.....)

Network address = 202.83.54.64

Broadcast address = 202.83.54.95

Usable host range = 202.83.54.65-202.83.54.94

For 14 computers,

$14 = 2^{\text{no. of host bits}} - 2$

∴no. of host bits = 4

Now, new subnet mask becomes

11111111.11111111.11111111.11110000/28

255.255.255.240

Subnet id = 256-240 = 16

Range = difference of 32 (i.e., 0,16,32,...96,112,.....)

Network address = 202.83.54.96

Broadcast address = 202.83.54.111

Usable host range = 202.83.54.97-202.83.54.110

For 5 computers,

$5 = 2^{\text{no. of host bits}} - 2$

∴no. of host bits = 3

Now, new subnet mask becomes

11111111.11111111.11111111.11111000/29

i.e., 255.255.255.248

Subnet id = 256-248 = 8

Range = difference of 8 (i.e., 0,8, 16, 32, ...112, 120, ...)

Network address = 202.83.54.112

Broadcast address = 202.83.54.119

Usable host range = 202.83.54.113-202.83.54.118

No. of Computers	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
29	202.83.54.0	202.83.54.1-202.83.54.30	202.83.54.31	255.255.255.192
23	202.83.54.32	202.83.54.33-202.83.54.62	202.83.54.63	255.255.255.192
15	202.83.54.64	202.83.54.64-202.83.54.94	202.83.54.95	255.255.255.192
14	202.83.54.96	202.83.54.97-202.83.54.110	202.83.54.111	255.255.255.224
5	202.83.54.112	202.83.54.113-202.83.54.118	202.83.54.119	255.255.255.224

14. A company has four departments having 20, 32, 60, and 24 computers in their respective departments. Assume an IPv4 class C public network address and design IP address blocks for each department from the assumed IP network using VLSM. Include network address, broadcast address, usable IP range, and subnet mask for each of the subnet. [2076 Bhadra]

Solution:

Let's suppose class C public network address be 200.10.10.0/24

We have,

Maximum number of hosts= $2^{\text{no. of host bits}} - 2$

For 60 computers,

$60 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 6

Now, new subnet mask becomes

11111111.11111111.11111111.11000000/26

i.e., 255.255.255.192

Subnet id = 256-192 = 64

Range = difference of 64 (i.e., 0, 64, 128, ...)

Network address = 202.10.10.0

Broadcast address = 202.10.10.63

Usable host range = 202.10.10.1-202.10.10.62

For 32 computers,

$32 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 6

Now, new subnet mask becomes

11111111.11111111.11111111.11000000/26

i.e., 255.255.255.192

Subnet id = 256-192 = 64

Range = difference of 64 (i.e., 0, 64, 128, ...)

Network address = 202.10.10.64

Broadcast address = 202.10.10.127

Usable host range = 202.10.10.65-202.10.10.126

For 24 computers,

$24 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0,32,64,96,128,160 .....)

Network address = 202.10.10.128

Broadcast address = 202.10.10.159

Usable host range = 202.10.10.129-202.10.10.158

For 20 computers,

$20 = 2^{\text{no. of host bits}} - 2$

$\therefore$ no. of host bits = 5

Now, new subnet mask becomes

11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0,32,64,96,128,160 .....)

Network address = 202.10.10.160

Broadcast address = 202.10.10.191

Usable host range = 202.10.10.161-202.10.10.190

No. of Computers	Network Address	Usable Host Range	Broadcast Address	Subnet Mask
60	202.10.10.0	202.10.10.1-202.10.10.62	202.10.10.63	255.255.255.192
32	202.10.10.64	202.10.10.65-202.10.10.126	202.10.10.127	255.255.255.192
24	202.10.10.128	202.10.10.129-202.10.10.158	202.10.10.159	255.255.255.224
20	202.10.10.160	202.10.10.161-202.10.10.190	202.10.10.191	255.255.255.224

15. Suppose your company has leased the IP address of 222.70.94.0/24 from your ISP. Divide it for five different departments containing 50, 30, 25, 12, 10 no of hosts. There are also two point to point links for interconnection between routers. List out the network

address, broadcast address, usable IP address range and subnet mask for each subnet. Also mention the unused range of IP addresses. [2076 Chaitra]

We have the given IP address of 222.70.94.0 and given mask is /25.

We know,

Maximum number of hosts = $2^{\text{no. of host bits}} - 2$

For 50 computers,

$50 = 2^{\text{no. of host bits}} - 2$

∴no. of host bits = 6

Now, new subnet mask becomes,

11111111.11111111.11111111.11000000/26

i.e., 255.255.255.192

Subnet id = 256-192 = 64

Range = difference of 64 (i.e., 0, 64, 128, ...)

Network address =222.70.94.0

Broadcast address = 222.70.94.63

Usable host range = 222.70.94.1-222.70.94.50

Unused range= 222.70.94.51-222.70.94.62

For 30 computers,

$32 = 2^{\text{no. of host bits}} - 2$

∴no. of host bits = 5

Now, new subnet mask becomes

= 11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 =32

Range = difference of 32 (i.e., 0, 32, 64, 96, 128, ...)

Network address = 222.70.94.64

Broadcast address = 222.70.94.95

Usable host range = 202.10.10.65-202.10.10.94

For 25 computers,

$25 = 2^{\text{no. of host bits}} - 2$

∴ no. of host bits = 5

Now, new subnet mask becomes

= 11111111.11111111.11111111.11100000/27

i.e., 255.255.255.224

Subnet id = 256-224 = 32

Range = difference of 32 (i.e., 0,32,64,96,128,160 .....)

Network address = 222.70.94.96

Broadcast address = 222.70.94.127

Usable host range = 222.70.94.97-222.70.94.121

Unused range=222.70.94.122-222.70.94.126

For 12 computers,

$12 = 2^{\text{no. of host bits}} - 2$

∴ no. of host bits = 4

Now, new subnet mask

= 11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256-240 = 16

Range = difference of 16

Network address = 222.70.94.128

Broadcast address = 222.70.94.143

Usable host range = 222.70.94.129-222.70.94.140

Unused IP range= 222.70.94.141-222.70.94.142

For 10 computers,

$10 = 2^{\text{no. of host bits}} - 2$

∴no. of host bits = 4

Now, new subnet mask becomes

11111111.11111111.11111111.11110000/28

i.e., 255.255.255.240

Subnet id = 256-240 = 16

Range = difference of 16

Network address = 222.70.94.144

Broadcast address = 222.70.94.159

Usable host range = 222.70.94.145-222.70.94.154

Unused IP range= 222.70.94.155-222.70.94.158

For point-to-point connection,

$2 = 2^{\text{no. of host bits}} - 2$

∴ no. of host bits = 2

Now, new subnet mask becomes

11111111.11111111.11111111.11111100/30

i.e., 255.255.255.252

Subnet id = 256-252 = 4

Range = difference of 4

Network address = 222.70.94.160

Broadcast address = 222.70.94.163

Usable host range = 222.70.94.161-222.70.94.162

No. of Computers	Network Address	Usable Host Range	Unused Range	Broadcast Address	Subnet Mask
50	222.70.94.0	222.70.94.1-222.70.94.50	222.70.94.51-222.70.94.62	222.70.94.63	255.255.255.192
30	222.70.94.64	222.70.94.65-222.70.94.94	-	222.70.94.95	255.255.255.224
25	222.70.94.96	222.70.94.97-222.70.94.121	222.70.94.122-222.70.94.126	222.70.94.127	255.255.255.224
12	222.70.94.128	222.70.94.129-222.70.94.141	222.70.94.142,222.70.94,143	222.70.94.143	255.255.255.240
10	222.70.94.144	222.70.94.145-222.70.94.154	222.70.94.155-222.70.94.158	222.70.94.159	255.255.255.240
2	222.70.94.160	222.70.94.161-222.70.94.162	-	222.70.94.163	255.255.255.252
2	222.70.94.164	222.70.94.165-222.70.94.166	-	222.70.94.167	255.255.255.252

CHAPTER – 5

TRANSPORT LAYER

The *transport layer* is located between the application layer and the network layer. It provides a process-to-process communication between two application layers, one at local host and other at remote host. Communication is provided using a logical connection which may be located in different parts of the globe, assuming imaginary direct connection through which they can send and receive messages

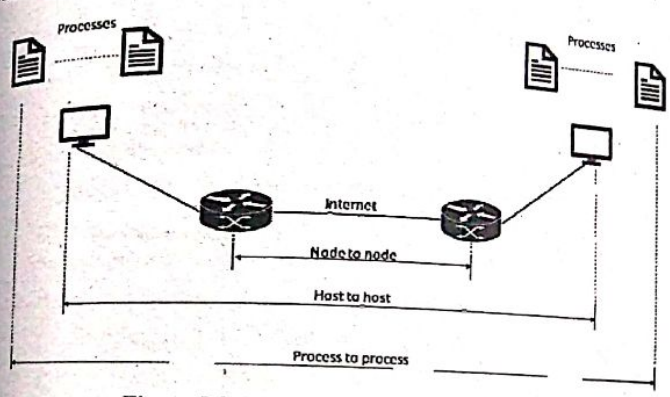


Figure 5.1: Process to process communication

A process is an application layer entity that uses the services of the transport layer. The data link layer is basically responsible for the delivery of frames between two neighbouring nodes over a link, node-to-node delivery. The network layer is responsible for communication at the computer level. A network layer can deliver the message only to the destination computer. The transport layer protocol is responsible for delivery of the message to the appropriate process. Communication normally takes place between two processes (application programs). We need process-to-process delivery.

5.1 Transport Layer Service

Transport layer provides logical communication between application processes running on different hosts. Sender breaks

application messages into segments, and passes to the network layer. Receiver reassembles segments into messages, passes to application layer. This layer ensures that data must be received in the same sequence in which it was seen. It provides end-to-end delivery of data between hosts.

Some of the main services are:

- Process to process communication
- Addressing
- Flow control and buffering
- Multiplexing and demultiplexing
- Congestion control

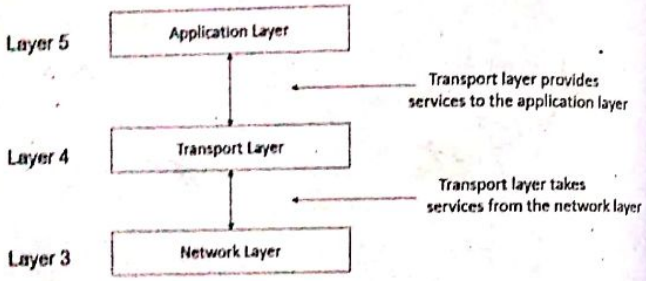


Figure 5.2: Transport layer

Services Provided to the Upper Layer

The transport layer is responsible for providing services to the application layer. The transport layer resides between the application layer and the network layer. The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine with a desired level of reliability that is independent of the physical networks currently in use. It provides the communication services to the application directly and provides the abstractions that applications need to use the network.

There are basically two types of services provided by the transport layer:

a. **Connection Oriented Services**

In *connection-oriented services*, a session connection is required before any data can be sent. The establishment of connection may take place on the physical level or logical level and needs some kind of signaling i.e., handshaking is done to setup the end-to-end connection. It works only in the bidirectional environment. This type of connection establishment needs some form of resource reservation (such as bandwidth). After the connection establishment, the actual data transfer will take place. After the exchange of data, the connection is cleared or broken (terminated). Due to connection establishment this type of services becomes more reliable and services are slower than connectionless services.

Example: TCP (Transmission Control Protocol)

b. **Connectionless Services**

In *connectionless services* session connection is not required before any data sent. It doesn't require the connection termination. Instead, information is transferred by using independent data units. Each data unit contains the complete destination address. This is analogous to the postal mailing service. This connectionless service can exchange data without setting an explicit communication path or connection. The packets are not numbered. They can get delayed, lost, or can arrive out of sequence. There is no acknowledgement, UDP is a connectionless protocol. This type of service is not reliable but faster than the connection-oriented services.

Example: UDP (User Datagram Protocol)

5.2 Transport Protocols: UDP, TCP

5.2.1 UDP (User Datagram Protocol)

UDP is a connectionless, unreliable transport level service protocol. In this protocol, there is no flow control, it does not provide packet sequencing. It is used by applications that do not need a reliable transport service. The main advantage of UDP is speed and is usually used for real time traffics like video streaming video or video chatting etc.

The header size of the UDP protocol is smaller than the header of TCP.

Source Port	Destination Port
Length	Checksum
Application data (message)	

Figure 5.3: UDP header format

- **Source Port:** This field is an optional field. When meaningful, it indicates the port of the sending process and assumed to be the port to which a reply should be addressed. If the field is not used, a value of zero is inserted. It is 2 Byte long field.
- **Destination Port:** This field identifies the destination port and is required. It is a 2-byte long field.
- **Length:** This is the size in bytes of the UDP packet including the header and data. The minimum length is 8 bytes, the length of the header zone.
- **Checksum:** The 2-byte long checksum field is used for error checking of the header and data.

5.2.2 TCP (Transmission Control Protocol)

TCP is a reliable, connection-oriented byte-stream protocol. In TCP, there is flow control (with seq. and ACK with sliding window). TCP provides ordered and error-checked delivery of a stream. TCP offers efficient control, which means when sending acknowledgement back to the source, the receiving TCP process indicates about the internal buffer to avoid overflow. It is usually used for file transfers. It doesn't support multicasting because it is connection-oriented. The data in the TCP is called segment. These segments are obtained after breaking the big file into small pieces.

The header size of the TCP protocol is larger than the header of UDP.

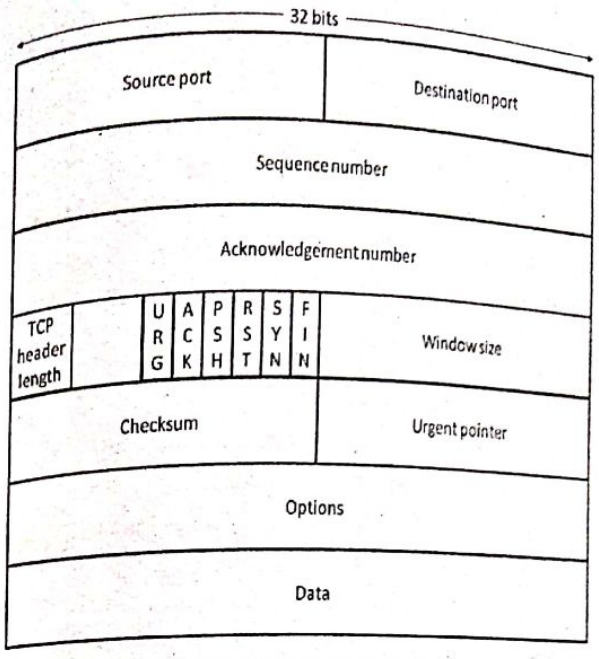


Figure 5.4: TCP header format

The header of a TCP segment can range from 20-60 bytes. 40 bytes are for options. If there are no options, header is of 20 bytes else it can be of utmost 60 bytes.

Header Fields

- **Source port:** This is a 16-bit field that holds the port address of the application that is sending the data segment.
- **Destination port address:** This is a 16-bit field that holds the port address of the application in the host that is receiving the data segment.
- **Sequence number:** This is a 32-bit field that holds the sequence number i.e., the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end if the segments are received out of order.
- **Acknowledgement number:** This is a 32-bit field that holds the acknowledgement number i.e., the byte number that the receiver expects to receive next. It is an acknowledgment for the previous bytes being received successfully.

- **Header length (HLEN):** This is a 4-bit field that indicates the length of the TCP header by number of 4-byte words in the header, i.e., if the header is of 20 bytes (min length of TCP header), then this field will hold 5 (because 5×4 = 20) and the maximum length: 60 bytes, then it'll hold the value 15(because 15×4 = 60). Hence, the value of this field is always between 5 and 15.
- **Control flags:** These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc. Their function is:
  - **URG:** Urgent pointer is valid, the receiving TCP should interpret the urgent pointer field.
  - **ACK:** Acknowledgement number is valid (used in case of cumulative acknowledgement)
  - **PSH:** Request for push
  - **RST:** Reset the connection
  - **SYN:** Synchronize sequence numbers
  - **FIN:** Terminate the connection (Finish)
- **Window size:** This field tells the window size of the sending TCP in bytes.
- **Checksum:** This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.
- **Urgent pointer:** This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.
- **Options:** This field provides additional functionality, like congestion control.

TCP divides the byte stream into appropriately sized segments (maximum transmission unit is less than or equal to size of data link layer) to which the computer is attached. TCP then passes the resulting packets to the internet protocol for delivery through a network to the TCP module of the entity at the other end. Then, it checks to makes sure that no packets are lost by giving each packet a sequence number, which is also used to make sure that the data is delivered to the entity at the other end in the correct order. The TCP module at the far end sends back an acknowledgement for packets which have been successfully received, a timer at the sending TCP will cause a time-out if an acknowledgement is not received within a responsible round-trip time (RTT) and the lost data will be re-transmitted. It checks that no bytes are corrupted by using a checksum, one is computed at the sender for each blocks of data before it is sent and checked at the receiver.

5.2.3 Difference Between TCP and UDP

The major differences between the TCP and UDP protocol are as follows:

Table 5.1: Difference between TCP and UDP

Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
1. It is a connection-oriented protocol and reliable delivery of messages.	1. It is connectionless oriented protocol and considered as unreliable.
2. The data is sent in the form of byte-stream.	2. The data is sent in the form of a packet.
3. The connection must be established before application-level protocol exchanges the information.	3. Immediately exchange the information by application-level protocol.
4. Guaranteed delivery due to error correction (or flow control) mechanism.	4. No flow control mechanism so unsecured communication.
5. Used to send the important data such as web pages, database information etc.	5. It has high speed to deliver the data so used for real time audio, video exchange.

Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
6. Only concerns with accuracy so the speed is automatically slow.	6. Only concerned with speed but not accuracy.
7. Well known applications are FTP, Telnet, HTTP.	7. Well known applications are DNS, DHCP, SNMP.

5.3 Addresses

On the Internet, four levels of addresses are used employing the TCP/IP protocols: physical (link) address, logical (IP) address, port address, and application-specific address. Each address is related to a one layer in the TCP/IP architecture, as shown in the following Figure.

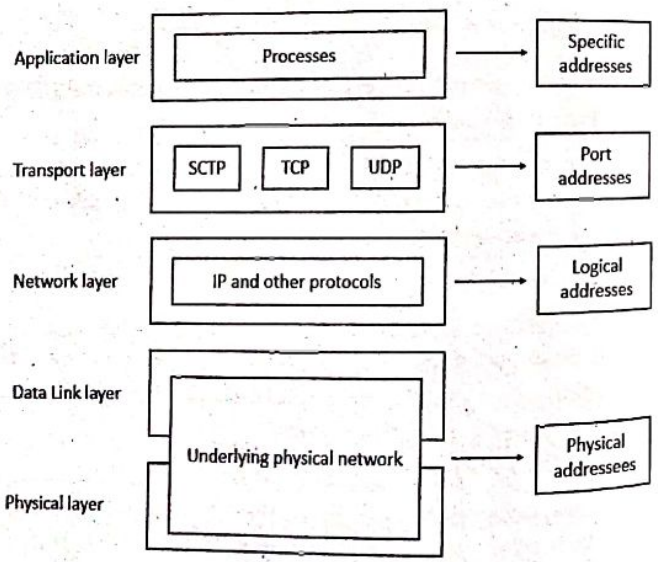


Figure 5.5: Addresses in TCP/IP

- **Physical Addresses:**

The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address. The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC). Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as 07:01:02:01:2C:4B; A 6-byte (12 hexadecimal digits) physical address.

- **Logical Addresses:**

Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32- bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address. The physical addresses will change from hop to hop but the logical addresses remain the same.

- **Port Addresses:**

The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. Computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we

need a method to label the different processes. In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.

- **Application-Specific Addresses:**

  Some applications have user-friendly addresses that are designed for that specific application. Examples include the e-mail address and the Universal Resource Locator (URL). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.

5.3.1 Port Address and Socket Address

Ports are essentially ways to address multiple entities in the same location. For example, the first line of a postal address is a kind of port, and distinguishes between different occupants of the same house. Computer applications will each listen for information on their own ports, which is why we can use more than one-network based application at the same time. TCP and UDP must use port numbers to communicate with the upper layer.

IANA Ranges

The IANA (Internet Assigned Number Authority) has divided the port numbers into three ranges: well-known, registered, and dynamic or private ports

- **Well-known ports:**

  The ports ranging from 0 to 1,023 are assigned and controlled by IANA.

- **Registered ports:**

  The ports ranging from 1,024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.

- **Dynamic ports:**

  The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers.

Some of the examples are:

Table 5.2: Protocols with port numbers

Protocol	UDP/TCP	Port No.
Internet Control Message Protocol (ICMP)		1
IP	UDP/TCP	17/6
File Transfer Protocol (FTP)-Data	TCP	20
File Transfer Protocol (FTP)-Control	TCP	21
Terminal Network (TELNET)	TCP	23
Internet Protocol Version 6 (IPv6)		41
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP/TCP	53
Hyper Text Transfer Protocol (HTTP)	TCP	80
Open Shortest Path First (OSPF)		89
Border Gateway Protocol (BGP)	TCP	179
Routing Information Protocol (RIP)	UDP	520

The client program defines itself with a port number which is chosen randomly. This number is called an ephemeral port number (temporary port number). The server process should also define itself with a port number but this port number cannot be chosen randomly. The internet uses universal port numbers for servers and these numbers are called well-known port numbers.

The process sends messages into, and receives messages from, the network through its socket. A socket is the interface between the application layer and the transport layer within a host. It is also called API (Application Programming Interface) as the socket is the programming interface with which network applications are built in the internet. The application developer has control of everything on the application-layer of the socket but has little control of transport layer side of the socket. The only control that the application developer has on the transport side is the choice of transport protocol and the ability to fix a few transport-layer parameters such as maximum buffer and maximum segment size.

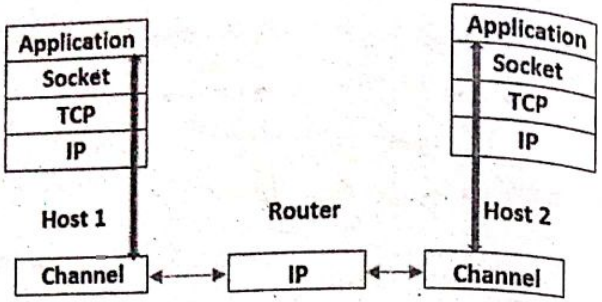


Figure 5.6: Flow of message using socket

In order for a process on one host to send a message to a process on another host, the sending process must identify the receiving process. For identification, two things are to be specified,

1. The name or address of the host (IP address)
2. An identifier that specifies the receiving process in the destination host (destination port)

Socket = IP Address: Port Number

= 200.23.56.8 : 96

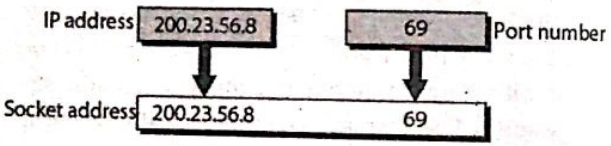


Figure 5.7: Socket address

For identifying the host, IP address is used. For identification of the receiving process, a destination port number is used.

5.4 Connection Establishment and Termination

Connection is established when one transport entity sends a Connection Request TPDU to the destination and wait for a Connection Accepted reply. This is done by using 3-way handshaking method. The 3-way handshaking help to solve the problem of delayed duplicate request.

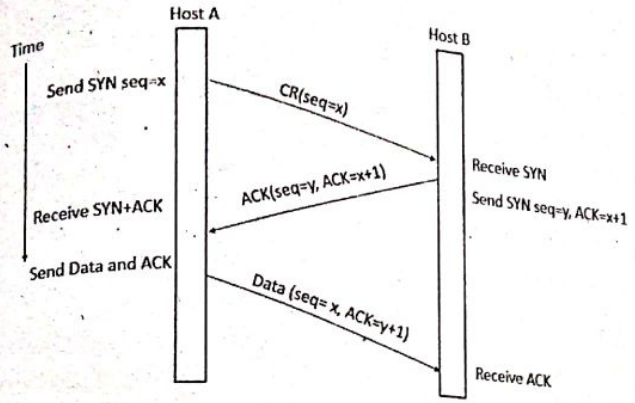


Figure 5.8: TCP connection established using 3-way handshaking

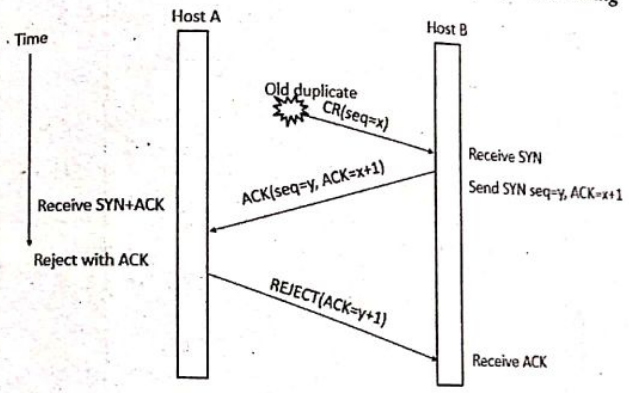


Figure 5.9: Old duplicate connection request appearing from nowhere

To establish a connection between Host A and Host B, first Host A send a TCP segment for connection request towards Host B. At that time SYN field get set. Consider initial sequence number (ISN) is 'x' in the sequence number field Host B sends SYN and ACK to Host A when Host B receive a SYN from Host A. The response given by Host B has its own ISN. During the response from Host B to Host A SYN field gets set and ACK field is set to value x+1, indicating next expected byte starting with sequence number from Host A.

After delivery of Host B ACK and ISN at Host A, Host A tries to end connection establishment by responding final acknowledgement. This time ACK field is set to value y+1. This

ACK field indicates, Host A expects from Host B next sequence byte starting with number y+1.

In the second figure when delayed duplicate connection request appear, host B sends the ACK with its sequence number in response. But when host A receives an ACK of the request it has not send, it simply rejects the request.

Closing a Connection (Connection Termination)

Four segments are required in order to terminate the connection in TCP. This is necessary because TCP transmit the data on both directions simultaneously. Following figure shows different phase of connection termination.

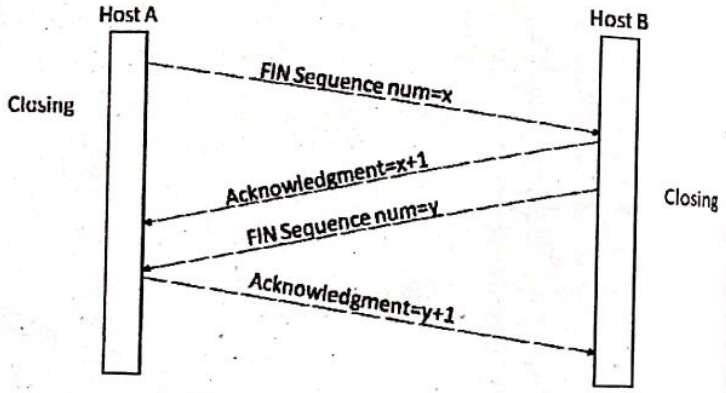


Figure 5.10: Connection termination

In this case, SYN field is replaced with FIN control field to terminate the connection.

To close an established connection, Host A need to send a closing signal over TCP. Hence Host A produced a FIN signal and sends it to Host B. Host B generates acknowledgment signal and send towards host A to notify the termination request of destination. When Host B decided to terminate the connection, it generate FIN signal and send it towards Host A which will processed by Host A. Again, Host A gives a response with ACK.

TCP Synchronization or 3-Way Handshaking

The connection establishment in TCP is called three-way handshaking. TCP is connection-oriented protocol. Communicating hosts go through a synchronization process to establish a virtual connection. This synchronization process ensures that both sides are ready for data transmission and allows the devices to determine the initial sequence numbers.

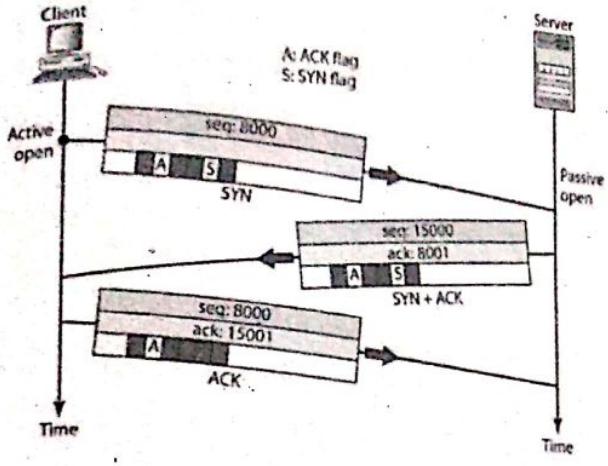


Figure 5.11: Connection establishment using three-way handshaking

5.5 Flow Control and Buffering

For flow control, a sliding window is required on each connection to keep a fast transmitter from overwhelming slow receiver; same as in data link layer. Since a host may have numerous connections, it is impractical to implement the same data link buffering strategy (use of dedicated buffers for each line). A suitable size value is negotiated during connection establishment. The value can be dynamically adjusted subsequently by the receiver.

- **Chained fixed size buffer:** If most of the TPDUs are nearly the same size, it is natural to organize the buffers as a pool of identically-sized buffers, with one TPDU per buffer.
- **Chained variable-sized buffer:** If there is wide variation in TPDU size, from a few characters typed to thousands of characters, then variables-sized buffer can be used but must have high price.

- **One large circular buffer per connection:** The optimum trade-off between source buffering, and destination buffering depends on the type of traffic carried by the connection.

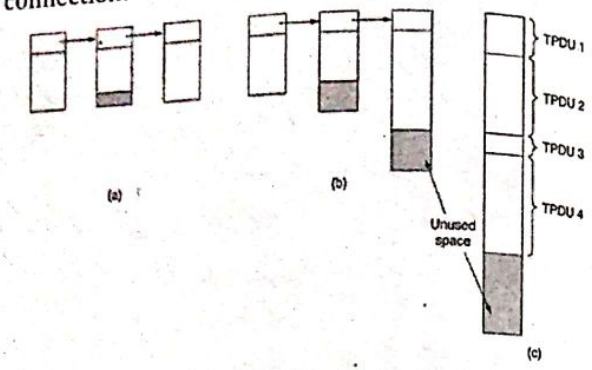


Figure 5.12: (a) Chained fixed-size buffers (b) Chained variable-sized buffers (c) One large circular buffer per connection.

Type of traffic carried by a connection also influences buffering strategy.

5.6 Multiplexing and Demultiplexing

Generally, *multiplexing* means sending the different channel data through a common channel by switching the channel using a different technique. Multiplexing here means multiplexing multiple transport connections on a single network layer connection, which is generally required if the available bandwidth is more than or equal to the integration of individual requirements of each connection, thus making an effective utilization of the available bandwidth.

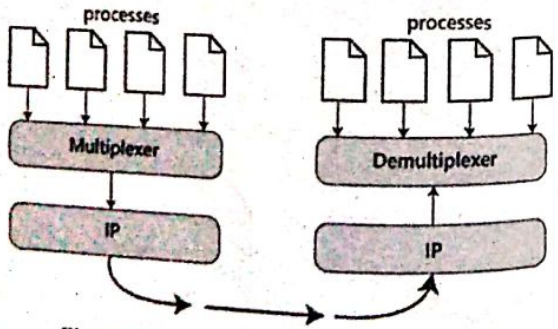


Figure 5.13: Multiplexing and demultiplexing

Consider how a receiving host directs the incoming transport layer segment to the appropriate socket. Each transport layer segment has a set of fields for this purpose. At the receiving end, the transport layer examines these fields to identify the receiving socket and then it directs the segment to that socket. This job of delivering the data in the transport layer segment to the correct socket is called *demultiplexing*.

The job of gathering data chunks at the source host from the different sockets, encapsulating each data chunk with the header information to create segments and passing the segments to the network layer is called multiplexing. At the destination host, the transport layer receives segments from the network layer just below. The transport layer has the responsibility to deliver the data in these segments to the appropriate application process running in the host.

5.7 Congestion Control Algorithm: Leaky Bucket Algorithm, the Token Bucket Algorithm

When too many packets are present in (a part of) the subnet, performance degrades. *Congestion* occurs when the number of packets sent to the network is greater than the capacity of the network. Congestion will lead to a large queue length which results in buffer overflow and loss of packets. Therefore, congestion control is necessary in the network.

Factors causing congestion:

- Packet arrival rate exceeds the outgoing link capacity.
- Insufficient memory to store arriving packets
- Burst traffic
- Slow processor

Congestion cannot be eliminated but can be controlled. The two approaches of Congestion Control are:

- **Open loop control:** It is a prevention approach. Open loop solutions try to solve the problems by excellent design to prevent the congestion from happening. It uses techniques like deciding when to accept the new packets, when to

discard the packets, which packets are to be discarded and making scheduling decisions at various points.

- **Closed-loop control:** The closed loop congestion control uses some kind of feedback. A closed loop control is based on the following three steps.
  - After congestion occurred, detect the congestion and locate it by monitoring the system.
  - Transfer the congestion information to places where action can be taken
  - Adjust the system operations to correct the congestion.

5.7.1 Traffic Shaping

Traffic shaping is a process of altering a traffic flow to avoid burst. Traffic shaping manages the congestion by forcing the packet transmission rate to be more predictable. It regulates the average rate of data transmission. Monitoring a traffic flow is called traffic policing.

Two traffic shaping techniques are used to control the congestion. These are:

1. Leaky Bucket Algorithm

It is an algorithm used to control congestion in network traffic. It uses a similar technique to a leaky bucket. Every host in the network is having a buffer with finite queue length. Packets which are put in the buffer when the buffer is full are thrown away.

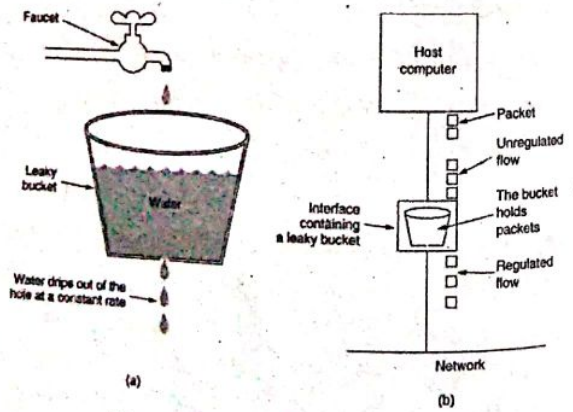


Figure 5.14: Leaky bucket algorithm

Imagine a bucket with a small hole in the bottom. No matter the rate at which water enters the bucket, the outflow is at a constant rate, when there is any water in the bucket and zero when the bucket is empty. Also,, once the bucket is full, any additional water entering it spills over the sides and is lost. The same idea can be applied to packets, as shown in Fig. (b).

Conceptually, each host is connected to the network by an interface containing a leaky bucket, that is, a finite internal queue. If a packet arrives at the queue when it is full, the packet is discarded. In other words, if one or more processes within the host try to send a packet when the maximum number is already queued, the new packet is unceremoniously discarded.

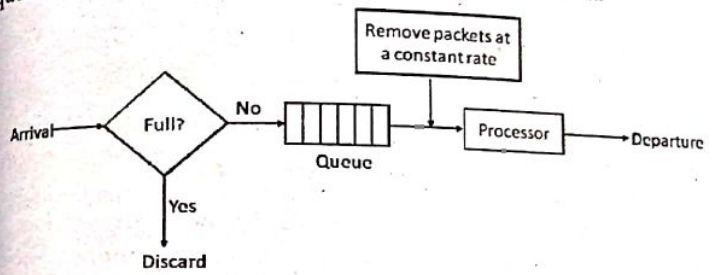


Figure 4.15: Leaky bucket algorithm implementation

The following is an algorithm for variable-length packets:

1. Initialize a counter to n at the tick of the clock.
2. If n is greater than the size of the packet, send the packet and decrement the counter by the packet size.
3. Repeat this step until n is smaller than the packet size.
4. Reset the counter and go to step 1.

2. The Token Bucket Algorithm

The leaky bucket algorithm is based on a constant rate output pattern at the average rate at the average rate no matter how bursty the traffic is. In leaky bucket algorithms, there are chances of loss of packet as the packet is filled in the bucket and overflow if the bucket is full. To minimize such limitation of packets, Token Bucket Algorithm is introduced. Here, the bucket holds a token not a packet. Tokens are generated by clocks at the rate of one token per ΔT second.

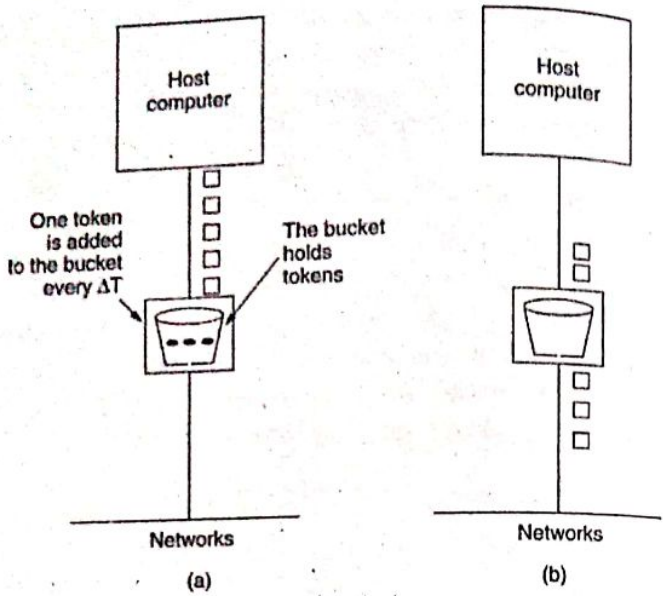


Figure 5.16: Token bucket algorithm

For many applications, it is better to allow the output to speed up somewhat when large bursts arrive, so a more flexible algorithm is needed, preferably one that never loses data. One such algorithm is the token bucket algorithm. Tokens arrive at the constant rate in the token bucket. If the bucket is full, tokens are discarded. A packet from the buffer can be taken out only if a token in the token bucket can be drawn.

The token bucket algorithm provides a different kind of traffic shaping than that of the leaky bucket algorithm. The leaky bucket algorithm does not allow idle hosts to save up permission to send large bursts later. The token bucket algorithm does allow saving, up to the maximum size of the bucket, n. This property means that bursts of up to n packets can be sent at once, allowing some burstiness in the output stream and giving the faster response to sudden bursts of input.

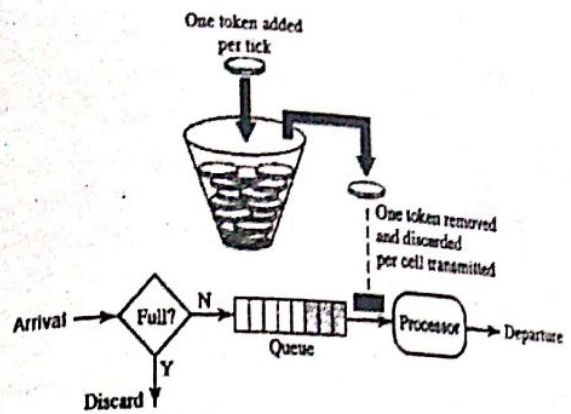


Figure 5.17: Token bucket algorithm implementation

The token bucket algorithm throws away a token when the bucket fills up but never discards packets. The implementation of the basic token bucket algorithm is just a variable count tokens. The counter is incremented by one at every ΔT sec and decremented by one whenever one packet is sent. When the counter hits zero, no packet can be sent.

CHAPTER – 6

APPLICATION LAYER

Application layer is the top most layer of the internet model. This layer is for applications which are involved in communication system. The application layer provides services to the users and the users can be human or software and receives services from the transport layer. For the real applications in the application layer to function, there is a requirement of support protocols. The three areas or protocols required for such support may be Network security, Domain Name Service (DNS),or Network Management.

Some of the important applications of this layer are:

- WWW
- Electronic Mail
- Remote file transfer and access
- Multimedia, etc.

6.1 Web: HTTP and HTTPS

Web is one of the major communication technologies that has changed the way people live and work. The WWW today is a distributed client-server service, in which a client using a browser can access a service using a server. The service provided is distributed over many locations called sites. The web today is a repository of information in which the documents, called web pages, are linked together.

6.1.1 Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP), the web's application-layer protocol, is at the heart of the web: HTTP is a simple request-response protocol that normally runs over TCP. It is implemented in two programs: client program and server program. The client program and server programs, executing on different end systems, talk to each other by exchanging HTTP messages

HTTP (Hypertext Transfer Protocol) is the most popular application protocol used in the Internet (or the WEB). It defines how web clients (i.e., browser) request web pages from the server (i.e., web server) and how servers transfer web pages to clients. When a user requests a web page, the browser sends HTTP request messages for the objects in the page to the server. The server receives the requests and responds with HTTP response messages that contain the objects. HTTP uses TCP as their underlying transport protocol. HTTP client first initiates a TCP connection with the server. Once the connection is established, the browser and the server processes access TCP through their socket interface. The default port of HTTP is TCP 80.

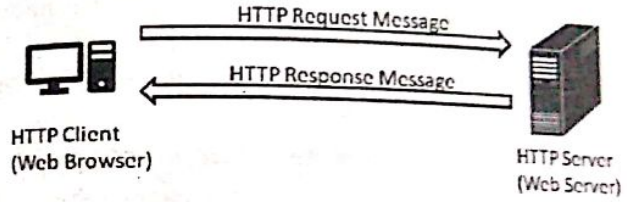


Figure 6.1: Hypertext transfer protocol (HTTP)

HTTP is a pull protocol, the client pulls information from the server, here the client accesses the authorized data and pulls it from the server (the server doesn't pushes the information to the client instead the client pulls the information from the server).

6.1.2 Hypertext Transfer Protocol Secure (HTTPS)

HTTPS is a communication protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not protocol in and of itself, rather, it is the result of simply layering the HTTP on top of SSL/TLS (secure socket layer/ Transport layer security) protocol.

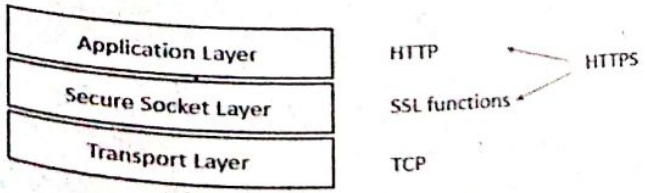


Figure 6.2: HTTPS

Enterprises are utilizing HTTPS for everything from e-commerce to mission-critical applications. It is underlying protocol for all secure web-based applications for communicating internally with employees, and externally with partners and customers. In its popular deployment on the internet, HTTPS provides authentication of the website and associated web server that one is communicating with; which protects against man in the middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with the contents of the communication. The port address of HTTPS is 443.

HTTPS is use of HTTP with an encryption on Secure Socket Layer (SSL) or Transport Layer Security (TLS) connection to provide encryption and secure identification of the server.

SSL builds a secure connection between two sockets, including:

- Parameter negotiation between client and server.
- Authentication of the server by the client.
- Secret communication.
- Data integrity protection.

To operate webserver to accept HTTPS connection, the administrator must create a public key certification for the webserver. We need to request the SSL certificate from the Trusted Certificate Authority to deploy HTTPS. This Encryption/Decryption Mechanism is used between client and server for transferring data

6.1.3 HTTP vs HTTPS

The differences between HTTP and HTTPS are:

HTTP	HTTPS
It is hypertext transfer protocol.	It is hypertext transfer protocol with secure.
It is less secure as the data can be vulnerable to hackers. It uses port 80 by default.	It is designed to prevent hackers from accessing critical information. It is secure against such attacks. It uses port 443 by default

HTTP	HTTPS
HTTP URLs begin with http://	HTTPs URLs begin with https://
It's a good fit for websites designed for information consumption like blogs.	If the website needs to collect the private information such as credit card number, then it is a more secure protocol.
HTTP does not scramble the data to be transmitted. That's why there is a higher chance that transmitted information is available to hackers.	HTTPS scrambles the data before transmission. At the receiver end, it descrambles to recover the original data. Therefore, the transmitted information is secure which can't be hacked.
It operates at TCP/IP level.	HTTPS does not have any separate protocol. It operates using HTTP but, uses encrypted TLS/SSL connection.
HTTP website do not need SSL and doesn't use encryption.	HTTPS requires SSL certificate and use encryption.
HTTP does not improve search rankings.	HTTPS helps to improve search ranking.
It is fast and vulnerable to hacker.	It is slower than HTTP and highly secure as the data is encrypted before it is seen across a network.

6.2 File Transfer: FTP, PuTTY, WinSCP

File transfer is a generic term for the act of transmitting files over a computer network like the Internet. There are numerous ways and protocols to transfer files over a network. Computer which provides a file transfer service are called *file server.*

6.2.1 File Transfer Protocol (FTP)

FTP is the standard mechanism provided by TCP/IP for copying a file from one host to another. It is like HTTP, runs on top

of TCP. However, unlike HTTP, FTP uses two parallel TCP connections to transfer a file, a control connection (port #21) and a data connection (port #20). The control connection is used for sending control information like password, identification, commands to "put" and "get" files, etc. and the data connection is used to actually send a file.

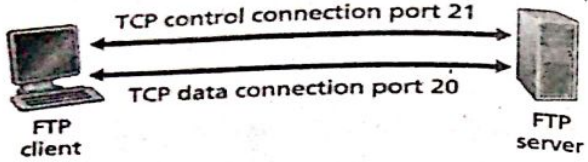


Figure 6.3: Control and data connection

FTP (File Transfer Protocol) establishes the two different connections between the client and server. One is for data transfer and the other is for the control information. In FTP, the control connection used between client and server uses the simple rules of communication. Only one line of command at a time or a line of response is transferred at a time. But the more complex rule is used by the data connection due to the variety of data types being transferred. FTP uses port 21 for control connection which is used for information control (command and responses) and port 20 for the data connection which is used for data/file transfer. The Control of the control connection is maintained during the entire FTP session and the data connection is first opened and the file are being transferred and connection is closed. This is done for transferring each file.

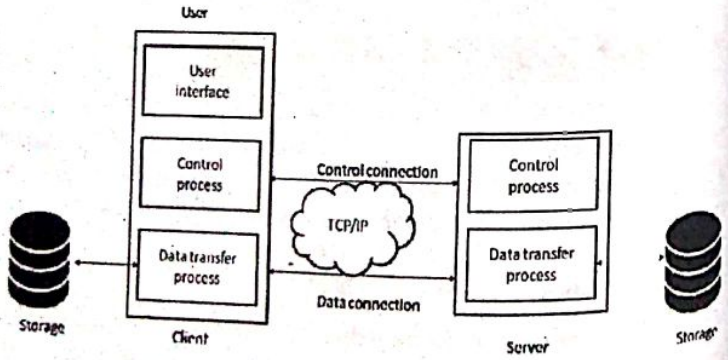


Figure 6.4: Basic model of FTP

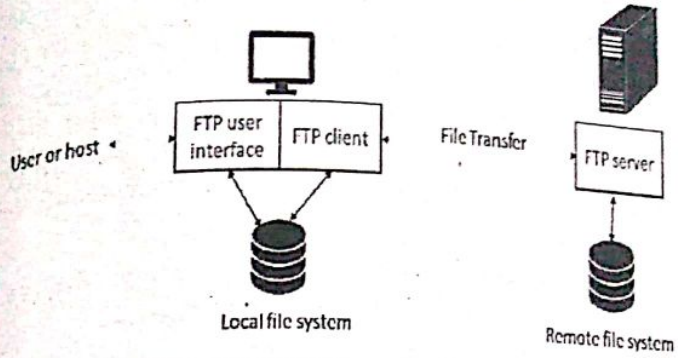


Figure 6.5: FTP moves files between local and remote file systems

In a typical FTP session, the user is sitting in front of one host (local host) and wants to transfer files to or from a remote host. In order to access the remote account, the user must provide a user identification and password. After providing the authorization, the user can transfer files from the local file system to the remote file system and vice-versa. As shown in the figure, the user interacts with FTP through an FTP user agent. The user first provides the hostname of the remote host, which causes the FTP client process in the local host to establish a TCP connection with the FTP server process in the remote host. The user then provides the user identification and password, which get sent over the TCP connection as part of FTP commands. Once the server authorizes the user, the user copies one or more files stored in the local file system into the remote file system.

6.2.2 Trivial File Transfer Protocol (TFTP)

TFTP is minimal protocol for transferring files without authentication. There are no separate ports for control information and data as in FTP. TFTP is frequently used by devices without permanent storage for copying an initial memory image from a remote server when the devices are powered on. TFTP uses an unreliable transport protocol UDP for data transfer.

6.2.3 WinSCP (Windows Secure Copy)

WinSCP is a small, free, open-source file transfer client for windows that uses secure shell technology to enable the safe copying of files between a local and a remote PC using the File Transfer Protocol (FTP), SSH FTP (SFTP) or SCP (secure copy) protocol as well as offering some basic file management features for proper operation of the information.

For secure transfers, WinSCP uses the Secure Shell (SSH) and supports the SCP protocol which is in an addition to SFTP. WinSCP protocol application is based on the implementation of the SSH protocol from PuTTY and FTP protocol from FileZilla for secure transfer of files and information.

6.2.4 PuTTY

PuTTY is one of the free and open-source terminal emulator application which can act as a client program and communicate the server for the SSH, Telnet, rlogin, and raw TCP computing protocols where client claiming the secure transfer of the data. PuTTY the open-source application was originally written for Microsoft Windows by its developers, but it has been ported to various other operating systems. The Official ports from Microsoft Windows are available for some Unix-like platforms, and they work-in- the progress ports to uplift the Mac OS X and Classic Mac OS, and the unofficial ports defined by the source are being contributed on platforms like Symbian, Windows Mobile and Windows Phone.

6.3 Electronic Mail: SMTP, POP3, IMAP

Along with the web, *electronic mail* is one of the most popular Internet applications.. Email is asynchronous means people send and read messages when it is convenient for them, without needing to coordinate with other people's schedules.

Components of Email System

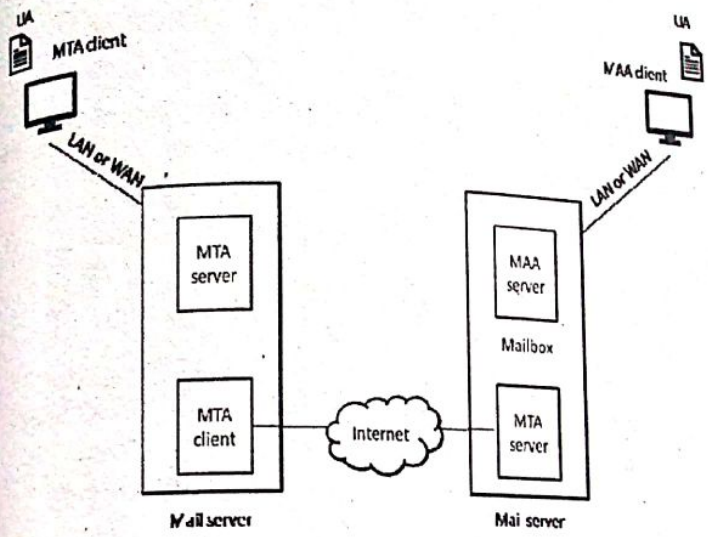


Figure 6.6: Components of E-mail system

- **User Agent:** The first component of an electronic mail system is the user agent (UA). The user agent provides the services to the user to make the process of sending and receiving a message easier and efficient manner. It is software package that composes, reads, replies to, and forwards messages.
- **Message Transfer Agent:** The actual mail transfer is done through message transfer agents (MTAs). A system must possess the MTA client to send mail and server to receive the mail. The MTA client and server on the Internet is called Simple Mail Transfer Protocol that defines the formal protocol for it.
- **Message Access Agent:** SMTP can't be used to obtain the message: obtaining a message is a Pull operation whereas SMTP is a Push protocol. It pushes the message from the client to the server. A Pull protocol is needed to access the mail as client must pull messages from the server. Hence, message access agent is used to access the mail.

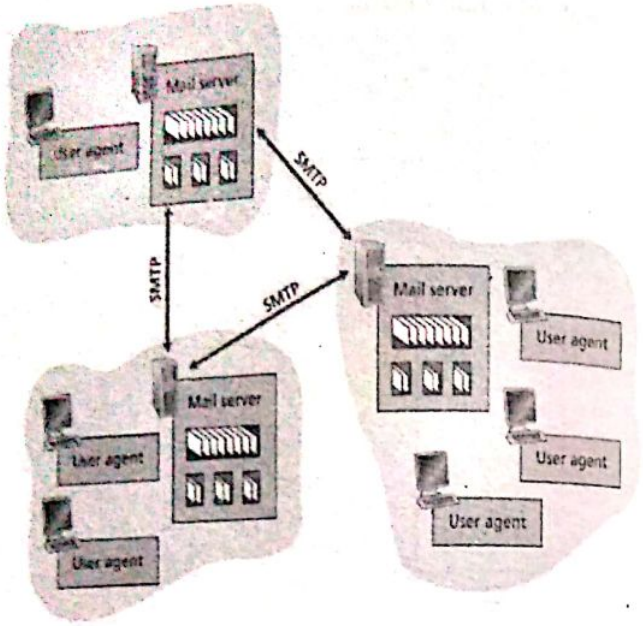


Figure 6.7: A high-level view of the Internet E-mail system

When the sender finishes composing his/her message, the corresponding user agent sends the message to the mail server's outgoing message queue. When the receiver wants to read a message, the receiver's user agent obtains the message from the receiver mailbox in the mail server.

6.3.1 SMTP

SMTP is the protocol that defines the MTA client and server on the Internet. It uses a reliable data transfer service of TCP to transfer mail from the sender's mail server to the recipient's mail server.

SMTP has two sides: a *client side* which executes on the sender's mail server, and a *server side* which executes on the recipient's mail server. Both the client and server sides of SMTP run on every mail server. When the mail server sends mail, it acts as an SMTP client. When a mail server receives mail, it acts as an SMTP server.

Working of SMTP:

- First, the client SMTP has TCP connection on port 25 to the server SMTP.
- If the server is down, the client tries again later.
- Once the connection is established, the server and client perform some application layer handshaking.
- During the handshaking phase, the SMTP client indicates the email address of the sender and the email address of the recipient,
- Once the SMTP client and server have introduced themselves to each other, the client sends the messages.

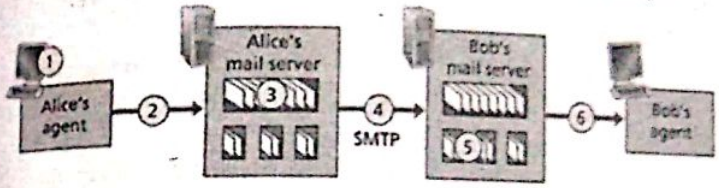


Figure 6.8: Alice sends E-mail to BOB

Steps:

1. Alice uses UA to compose the message to send to: bob@someschool.edu
2. Alice's UA sends message to her mail server and the message placed in message queue for sending
3. The Client side of SMTP opens the TCP connection with Bob's mail server
4. SMTP client sends Alice's message over the TCP connection of bob
5. Bob's mail server places the message in the mailbox Bob
6. Bob invokes his user agent to read message that he received from Alice

6.3.2 Mail Access Protocols (Pull Protocols)

The two protocols, which transfer messages from receiver's mail server to the local PC are POP3 (Post Office Protocol Version 3) and IMAP (Internet Mail Access Protocol).

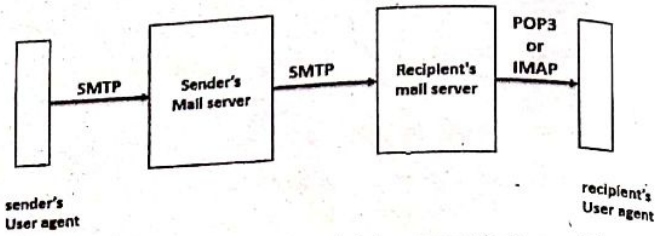


Figure 6.9: E-mail protocols and their communicating entities.

1. Post Office Protocol (POP3)

POP3 is a simple mail access protocol but with limited in functionality. POP3 consists of client POP3 software and server POP3 software. The client POP3 software is installed on the recipient computer whereas the server POP3 software is installed on the mail server.

When the user wants to download e-mail from the mailbox on the email server, following events take place in sequence.

- The client opens a connection with the server on TCP port 110
- It sends its username and password to access the mailbox.
- The user can then list and retrieve the mail messages, one by one.

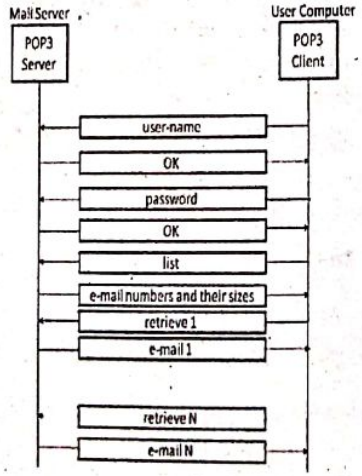


Figure 6.10: POP3 example

POP3 progresses through three phases:

- **Authorization:** user agent sends username and password
- **Transaction:** user agent retrieve message
- **Update:** occurs after the client quit command.

POP3 has two modes: delete mode and the keep mode.

- **Delete mode:** the mail is deleted from the mailbox after each retrieval. This mode is used when the user is working at his permanent computer.
- **Keep mode:** the mail remains in the mailbox after retrieval. This mode is used when the user accesses mail away from the primary computer.

Disadvantages of POP3:

- The user cannot have different folders on the server.
- The user cannot partially check the contents of email before downloading.
- For nomadic user who would prefer to maintain a folder hierarchy on a remote server that can be accessed from any computer. This is not possible with POP3.

2. IMAP (Internet Mail Access Protocol)

IMAP is similar to POP3, but has more features along with more complexity. Since, POP3 has some demerits like it does not allow the user to organize her mail on the server; the user cannot have different folders on the server. In addition, POP3 does not allow the user to partially check the contents of the mail before downloading. User prefer to maintain a folder hierarchy on the remote server that can be accessed from any computer. This is not possible with POP3 however IMAP protocol is defined to solve these issues. When the message first arrives, it is associated with the recipient's INBOX folder. The recipient can then move the message from one folder to another. Unlike POP3, IMAP maintains state information across IMAP session, - for example, names of folders and which messages are

associated with which folders. IMAP enable to obtain components of messages

IMAP provides following extra functions:

- A user can check the e-mail header prior to downloading.
- A user can search the contents of the e-mail for a specific string prior to downloading,
- A user can create, delete or rename mailboxes on the mail server.

Difference between POP3 and IMAP:

Post Office Protocol (POP3)	Internet Message Access Protocol (IMAP)
1. When anyone opens the mail box, new mail is moved or downloaded permanently from the host server and saves on the computer. Hence, if he/she wants to see the previous mail. He/she has to go back to the previous.	1. The mail is permanently stored in the server until you delete this. Thus, you can access them from various locations at various times.
2. With POP, only one folder will be in the mail server i.e., index folder.	2. Mail stays on the server in multiple folders, some of which you have created.
3. Users cannot access his multimedia email if he has limited bandwidth.	3. If limited bandwidth is available then users can partially download e-mail content.
4. POP has only two modes i.e., keep mode and delete mode for message.	4. A user can create, delete or rename mailboxes on the mail server.
5. Reading your e-mail from multiple computers results in the message scattering.	5. Multiple computers can access the same e-mail at the same time
6. Message storage is limited only by the capacity of your computer but if your computer fails; you may lose all your messages.	6. The message storage capacity is limited to 2 GB and there is no any effect if your computer fails.
7. Port used is 110	7. The TCP port used is 143.
8. Connection time required is small.	8. Connection time required is large.
9. User backs up mail boxes	9. ISP backs up mail boxes.

6.4 DNS (Domain Name System)

For communication to take place successfully, the sender and receiver both should have addresses and they should be known to each other. The addressing in application program is different from that in other layers. Each program will have its own address format. There is an alias name for the address of remote host. It is easier to remember an IP address. The application program uses an alias name instead of IP address. TCP/IP protocols use the IP address to identify the connection of a host to the Internet. However, people prefer to use names instead of numeric addresses. Therefore, the Internet needs to have a directory system that can map a name to an address, called DNS. DNS provides translation between the host name and IP address. It uses UDP port no. 53. The user generally enters a host name. the application takes the hostname and forward it to DNS for translation to an IP address.

6.4.1 Working of DNS

DNS servers do two things:

- Accept requests from programs for converting domain names into IP addresses.
- Accept requests from other DNS servers to convert domain names into IP addresses.

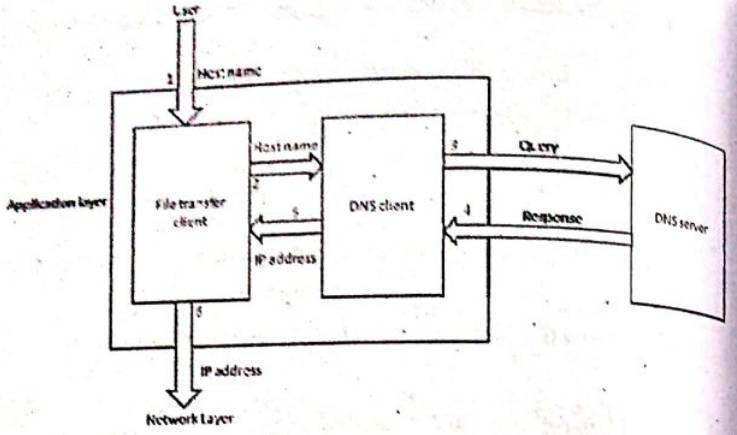


Figure 6.11: Working of DNS

The following six steps map the host name to an IP address:

1. The user passes the host name to the file transfer client.
2. The file transfer client passes the host name to the DNS client
3. Each computer, after being booted, knows the address of one DNS server. The DNS client sends the message to DNS server with the query that gives the file transfer server name using the known IP address of the DNS server.
4. The DNS server response with the IP address of the desired file transfer server.
5. The DNS server passes the IP address to the file transfer client.
6. The file transfer client now uses the received IP addresses to access the file transfer server.

6.4.2 Domain Name Space

Domain Name Space was designed to have a hierarchical name space. In this design the names are defined in an inverted-tree structure with the root at the top. Each node in the tree has a label. The root label is a null string. DNS requires that the children of the node have different labels.

Each node in the tree has a domain name. A full domain name is a sequence or label separated by dots (.). The domain names are always read from the node up to the root. The last label is the label of the root (null).

If the label is terminated by a null string, it is called a fully qualified domain name (FQDN). If the label is not terminated by a null string, it is called partially qualified domain name (PQDN).

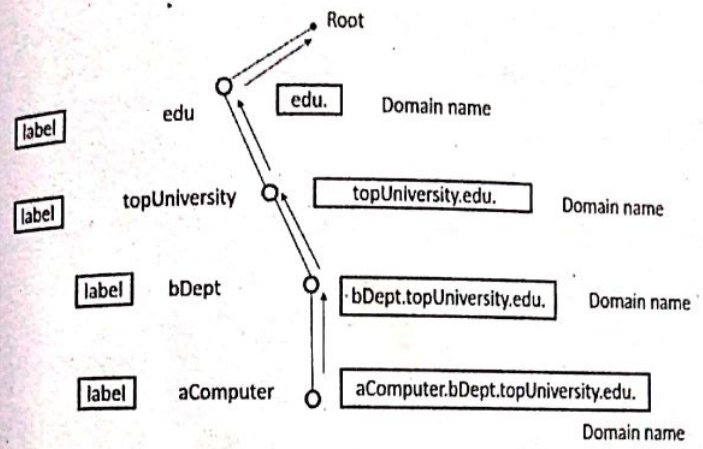


Figure 6.12: Domain name and labels

Root Domains

The root domain is at the top of the hierarchy and is represented as a period (.). Organizations, including Network Solutions, Inc. manage the internet root domain.

Top-Level Domains

There are two- or three-character name codes in Top-level domains. Top-level domains are presumed to be grouped in categories like organization type or geographic location.

Second Level Domains

This is the domain that is directly below the Top Level Domains (TLD). This is the main part of the domain name. It can vary according to the buyer. There are no limits here as the TLDs. Once the domain is available anyone can purchase it.

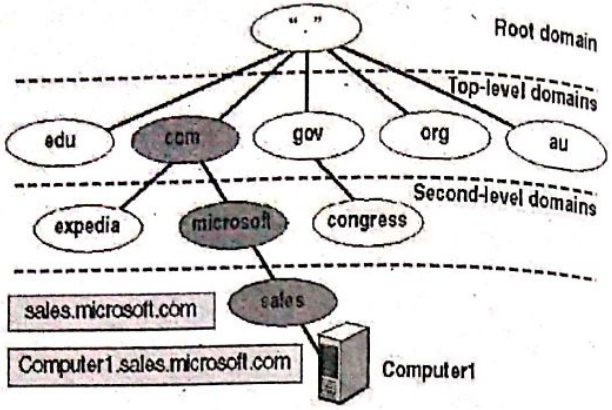


Figure 6.13: Hierarchical structure of Domain Name

6.4.3 Hierarchy of Name Servers

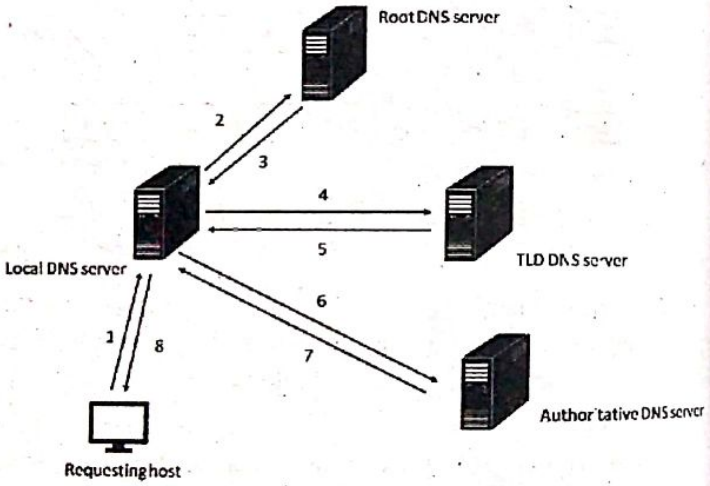


Figure 6.14: Types of name servers

- **Top-level domain (TLD) servers:** TLD is the one responsible for com, org, net, edu, etc, and all top-level country domains np, uk, jp. The Network solutions of the system maintain servers for com TLD. Educational institutions use for edu TLD
- **Authoritative DNS servers:** IP mappings for organization's servers (e.g., Web and mail) from hostname, id is provided by the DNS servers as the organization's DNS servers Can be maintained by organization or service provider
- **Local DNS servers:** It does not strictly belong to hierarchy. Each ISP (residential ISP, company, university) has one. A query is sent to its local DNS server, whenever a host makes a DNS query. Here, local DNS is also widely recognized as the "default name server", which acts as a proxy, forwards query into the hierarchy.

6.4.4 DNS components

The DNS service has four components:

1. **DNS Cache**

   DNS cache can be the list of names and IP addresses that already have been queried and have been resolved and are cached. The second meaning regards a DNS server that simply performs recursive queries and caching without actually being an authoritative server itself.

2. **Resolvers**

   Resolvers are any hosts on the Internet that need to look up domain information, such as the computer you are using to read this website.

3. **Name Servers**

   These are servers that contain the database of names and IP addresses and server DNS requests for clients.

4. **Name Space**

   Name space is the database of IP addresses and their associated names.

6.5 Peer to Peer Applications (P2P)

P2P is a Peer-to-Peer networking where a P2P program is installed on a user's computer which creates a community of P2P application users and a virtual network between these users. A P2P application runs on ones' machine allowing it to connect directly to other user's machines and giving other users the ability to connect to machines in order to transfer files back and forth between the machines.

There are various applications which help to share information between the systems. Peer-to-peer is a method or application of structuring distributed applications in a network such that the individual nodes have symmetrical roles. Instead of dividing the system into client and server in P2P applications a node may act as both a client and a server. An example of pure P2P application is Gnutella- an open source, P2P File Sharing Application. Due to decentralized nature, P2P applications are very difficult to manage. Many Applications like Napster, bit torrent, µTorrent, etc. are hybrid of server-client and P2P architecture.

Peer-to-peer (P2P) computing or networking is a distributed application architecture that divides the available tasks or workloads between peers present in the system. Peers are equally privileged, an equivalent role of participants in the application. They are said to form a peer-to-peer network of nodes.

Some key characteristics defining P2P applications are:

- The ability to discover other peers
- The ability to query other peers
- The ability to share content with other peers.

Peer to peer is more efficient because when a user wishes to download a file from a website, P2P protocol creates TCP connections with multiple hosts and makes small data requests to each. The P2P client then combines the chunks to recreate the file. A single file host will usually have limited upload capacity but connecting to many servers simultaneously allows for higher file transfer.

Disadvantages:

- Consume a huge amount of bandwidth without production
- P2P application is very famous for distributing pirated software
- File downloading from a remote user in P2P environment cannot be trusted because the files may contain malwares.

6.6 Socket Programming

A network socket is presented as the endpoint of an inter-process communication flow across a computer network. Today, most communication systems carried out between computers is based on the Internet Protocols. So, most network sockets that we use are Internet sockets. A *socket address* is the combination of IP address plus corresponding TCP/UDP port numbers. A socket is supposed to behave like a terminal which is created and used by the application program. Communication between a client process and a server process is communication between two sockets created at two ends. When a client program and server program are executed, a client and server process are created. These two processes communicate with each other by reading from and writing to sockets. Hence socket can be considered as a door between the application process and TCP.

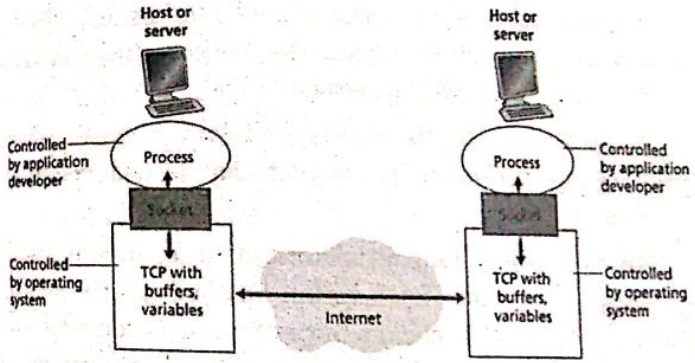


Figure 6.15: Process communicating through TCP sockets

The client process can initiate a TCP connection to the server. This is done in the client program by creating a socket object. When the client creates its socket object, it specifies the address of the server process (IP address of the server and the port number of the process). Upon creation of the socket object TCP in the client initiates a three way handshaking and establish a TCP connection with the server.

In JAVA language java.net. Socket provides a socket and java.net. ServerSocket provides the mechanism on how the server

program listens to the clients where it establishes the best communication between them.

Steps that occur when establishing connection using sockets between two computers:

1. The server instantiates a Server Socket object, which represents the port no. denoting which specific communication to occur on.
2. The server invokes the accept() method of the ServerSocket class. This method waits for a client until it connects to the server on the given port.
3. After the server is waiting, a client instantiates a Socket object, specifying which server name and the port number to connect to.
4. The specified server and the specific port number is used to connect the client by the constructor of the socket class. If communication is successfully established then the connected client possesses the Socket object capable of communicating with the server.
5. In the server side, the accept() method returns a reference to a new socket on the server that is connected to the client's socket.

After the connections are established, communication can occur using I/O streams. Each socket has both an OutputStream and an InputStream. The client's OutputStream is connected to the server's InputStream, and the client's InputStream is connected to the server's OutputStream.

Types of Socket

There are three different types of sockets:

i. **Stream Socket (SOCK_STREAM):** Stream sockets corresponds to TCP protocol in TCP/IP. A stream of bytes is sent after a logical connection is established with each other. It provides reliable, connection-oriented communication. Some examples of an application that uses stream socket is FTP, telnet, SSH, HTTP, etc.

ii. **Datagram Socket (SOCK_DGRAM):** Datagram socket corresponds to the UDP protocol in TCP/IP suite. Discrete message called datagrams are sent directly with having logical connection with each other. The delivery of data is unreliable. Network File System is an application that uses datagram sockets.

iii. **Raw Socket (SOCK-RAW):** Provide direct access to the lower-layer protocols for example: IP and ICMP.

Example: ping command.

An Internet socket is characterized by a unique combination of the following:

- **Local socket address:** Is resembles Local IP address and port number
- **Remote socket address:** Only for established TCP sockets. As discussed in the client-server section, this is necessary since a TCP server may serve several clients concurrently. The server creates one socket for each client, and these sockets share the same local socket address.
- **Protocol:** A transport protocol (e.g., TCP, UDP, raw IP, or others). TCP port 53 and UDP port 53 are consequently different, distinct sockets.

Table 6.2: Socket programming primitives

Primitive	Meaning
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections: give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

6.7 Application Server Concept: Proxy Caching (Web Caching)

6.7.1 Proxy Server (Web Caching)

In computer networks, a *proxy server* can be a program running on the same machine working as a browser or can be a computer system. Proxy server is also called a *web cache* which is a network entity that satisfies HTTP requests on the behalf of a client. The Web cache has its own disk storage, and keeps in this storage copies of recently requested objects.

When a user configures his browsers, the browser establishes a TCP connection to the proxy server. The proxy server sees if it has a copy of the page stored locally. If the page is there then it will see for updates. If the page is up to date, it passes the page to the user otherwise a new copy of the page is fetched with it.

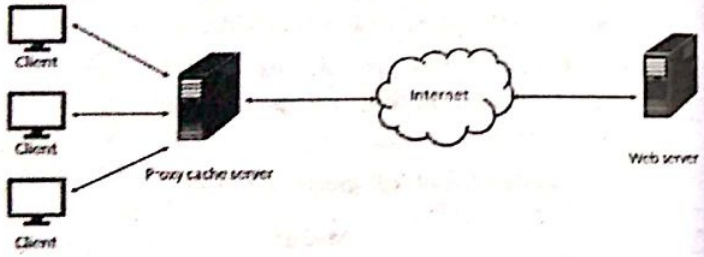


Figure 6.16: Proxy server

If the Web cache does not have the object, the Web cache opens a TCP connection to the origin server. The Web cache then sends an HTTP request for the object into the TCP connection. After receiving this request, the origin server sends the object within an HTTP response to the Web cache. When the Web cache receives the object, it stores a copy in its local storage and forwards a copy, within an HTTP response message, to the client browser (over the existing TCP connection between the client browser and the Web cache).

Types of Proxy

i. **Transparent Proxy:** Transparent Proxy makes the original IP address available through the http headers. Since, transparent proxies have their own right and power to cache the websites and does not provide any anonymity to the user.

ii. **Anonymous Proxy:** It does not make the original IP address available to the users and also it is detectable and identifies itself as a proxy server but provides reasonable anonymity for most users.

iii. **Distorting Proxy:** It makes an incorrect original IP address available through the http headers but identifies itself as a proxy server.

iv. **High Anonymity Proxy:** It does not make available the original IP address and does not identify itself as a proxy server.

Main Uses of Proxy Server are:

i. **Caching:** When a user accesses a web page, that page is temporarily stored in the proxy cache. Then, when a subsequent user requests for the same web page which is stored in the proxy cache, they access the copy in the proxy cache, rather than having the web page.

ii. **Filtering:** Allows to block specific sites

iii. **Maintain Privacy:** Proxy server can hide actual IP address of Client from the outside world thus maintaining privacy.

6.8 Concept of Traffic Analyser: MRTG, PRTG, SNMP, Packet tracer, Wireshark

6.8.1 MRTG (Multi Router Traffic Grapher)

It is a tool to generate HTML pages and monitor the traffic load on network links. *MRTG* works on most UNIX platforms and Windows NT. MRTG is written in Perl and comes with full source. It uses a highly portable SNMP (Simple Network Management Protocol) implementation written entirely in Perl. The traffic

loads on network links are monitored and measured allowing the user to see traffic load on a network over time in graphical form.

6.8.2 PRTG (Paessler Router Traffic Grapher)

PRTG Network Monitor runs on a Windows machine within the network. It also collects the various statistics from the machines, software, and devices. It can also auto-discover them, and also retains the data so that the historical performance can be analyzed. PRTG can collect data and for this it supports multiple protocols. The network analyzer tool uses SNMP, packet sniffing, and Net Flow to track network traffic. PRTG Network Monitor can be used for server room monitoring and for monitoring windows 2003 terminal server. PRTG can also be used as database monitor and for VMware SNMP monitoring.

6.8.3 SNMP (Simple Network Management Protocol)

SNMP is a framework for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet. It uses the concept of manager and agent where manager controls and monitors a set of agents. SNMP is an application-level protocol so that it can monitor devices made by different manufactures and installed on different physical networks. SNMP uses two management tasks: Structure of Management Information (SMI) and Management Information Base (MIB). SMI defines the general rules for naming objects, defining objects types and showing how to encode objects and values. MIP creates a collection of named objects, their types and their relationships to each other in an entity to be managed.

It is a popular protocol network management and is widely used for collecting information and configuring network devices, the devices can be servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. The devices that typically support SNMP are devices like routers, switches, servers, workstations, printers, modem racks. MRTG uses the Simple Network Management Protocol (SNMP) to send requests with object identifiers (OIDs) to a device. It will have a management information base (MIB) to look up the OIDs specified. After complete collection of the information, it will send back the raw data encapsulated in an SNMP protocol. The software then creates an HTML document from the logs, containing a list of graphs detailing traffic for the selected device.

6.8.4 Packet Tracer

It is a powerful network simulation program which helps to simulate the real-world network components like the router, hub, switches, server, etc. It allows users to experiment with network behaviour. The simulation, visualization, authoring, assessment and collaboration can easily learn with complex technology concept using Cisco-Packet Tracer.

6.8.5 Wireshark

It is a free and open-source packet analyzer which troubleshoots, analysis, software and communication protocol development and education of network system. It was Originally named Ethereal. Wireshark is cross-platform. Wireshark uses the GTK+ widget toolkit to implement the user interface, and using cap to capture packets; It runs on various Unix-like operating systems such as Linux, Mac OS X, BSD, and Solaris, and on Microsoft Windows as well. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

CHAPTER – 7

INTRODUCTION TO IPV6

The huge growth in Internet use has not only led to increased demand for better, faster technology but has also increased the demand for addresses from which to send and receive information. This is especially true for developing countries where people are only really starting to use the Internet. IPv6 deployment can solve the problem.

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. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.

IPv6 Address Space

IPv6 uses a 128-bit address that is very large space compared to IPV4. IPv6 uses a special notation called hexadecimal colon notation. Here 128 bits are divided into 8 sections, each one is 2 bytes long.

Example: FE80:0000:0000:0001:0800:23e7:f5db

Limitation of IPv4

The network layer protocol in the TCP/IP protocol suite is currently IPv4 (Internetworking Protocol, version 4). IPv4 provides the host-to-host communication between systems in the Internet. Although IPv4 is well designed, data communication has evolved since the inception of IPv4 in the 1970s. IPv4 has some deficiencies (listed below) that make it unsuitable for the fast-growing Internet.

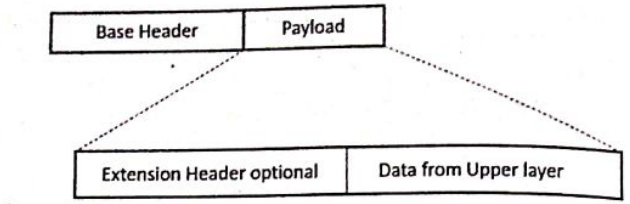
- Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.
- The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.
- The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.

7.1 Advantages of IPv6

1. **Larger address space**
   The address space of IPv6 contains 2^{128} addresses. This address space is very large in compared to the IPv4 address.
2. **Better header format**
   IPv6 uses a new header format in which options are separated from the base header and inserted, when needed. This reduces processing delay due to fixed header size and there is no header checksum.
3. **Possibility of extension**
   IPv6 has been designed in such a way that there is possibility of extension of protocol if required.
4. **Reduction in routing table**
   Globally unique and hierarchical addressing, based on prefixes rather than address classes to keep routing tables small and backbone routing efficient.
5. **Support for more security**
   The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.
6. **Support for resource allocation**
   In IPv6, the type-of-service field has been removed, but a mechanism has been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.
7. **It aids multicasting by allowing scopes to be specified.**

7.2 IPV6 Header Format

IPv6 packet is composed of a mandatory base header followed by payload. The payload consists of two parts: optional extension header and data from the upper layer.



The overall packet format is:

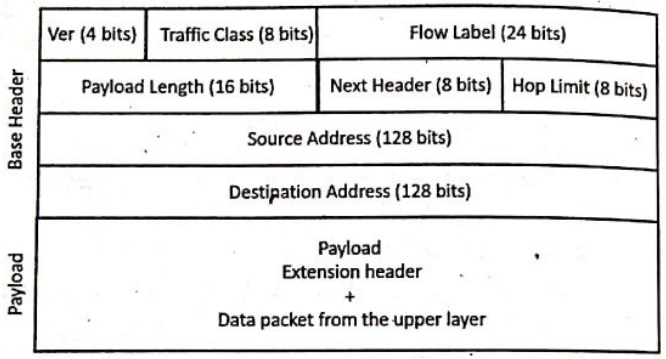


Figure 7.1: IPv6 basic packet format

- **Version (4 bits):** 4 bits are used to indicate the version of IP and is set to 6
- **Traffic Class (8 bits):** Same function as the Type of Service field in the IPv4, distinguish different real-time delivery requirement
- **Flow Label (24 bits):** Identifies a flow and it is intended to enable the router to identify packets that should be treated in a similar way without the need for deep lookups within those packets. Set by the source and should not be changed by routers along the path to the destination.
- **Payload Length (16 bits):** Only the length of the payload (Header length is fixed to 40 bytes)
- **Next Header (8 bits):** Indicates either the first extension header (if present) or the protocol in the upper layer PDU (such as TCP, UDP, or ICMPv6).

- **Hop Limit (8 bits):** IPv4 TTL was appropriately renamed Hop Limit because it is a variable that is decremented at each hop, and it does not have a temporal dimension.
- **Source Address (128 bits):** Stores the IPv6 address of the originating host.
- **Destination Address (128 bits):** Stores the IPv6 address of the current destination host.

Header comparison of IPv4 and IPv6

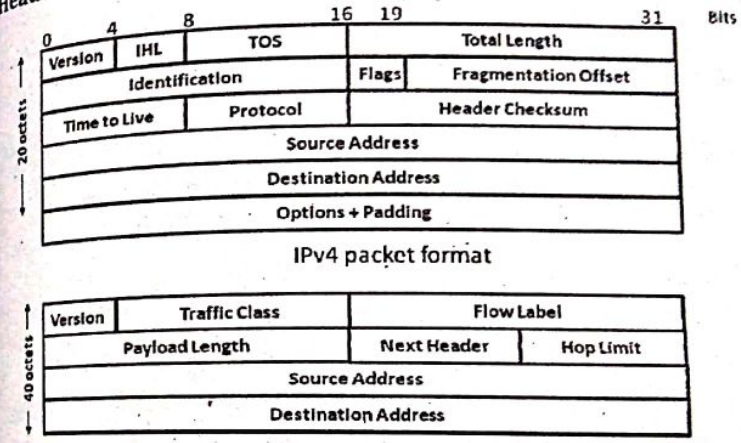


Figure 7.2: Header comparison of IPV4 and IPV6

Few fields have been removed:

- Identification, flags, fragmentation offset
- TOS, header length
- Header checksum

Some of the name of fields have been changed:

- Total length→ Payload length
- Protocol→ Next header
- Time to live→ Hop limit

Some of the added fields in IPv6 header are:

- Traffic class
- Flow label

Major Improvements

- No option field: replaced by extension header. Result in a fixed length, 40-byte IP header
- No header checksum: result in fast processing
- No fragmentation at intermediate nodes: result in fast IP forwarding

7.3 Difference Between IPv4 and IPv6

The difference between IPv4 and IPv6 is shown below:

IPV4	IPV6
IPv4 has 32-bit address length.	IPv6 has 128-bit address length.
It Supports Manual and DHCP address configuration.	It does not require Manual and DHCP address configuration It supports Auto and renumbering address configuration.
In IPv4, end to end connection integrity is unachievable.	In IPv6, end to end connection integrity is achievable.
Security features are dependent on application.	IPSec is an inbuilt security feature in the IPv6 protocol.
Address representation of IPv4 is in decimal.	Address Representation of IPv6 is in hexadecimal.
Fragmentation performed by Sender and forwarding routers.	In IPv6 fragmentation performed only by sender.
In IPv4 Packet, flow identification is not available.	In IPv6 packet, flow identification is available and uses flow label field in the header.
In IPv4, checksum field is available.	In IPv6, checksum field is not available.
It has broadcast Message Transmission Scheme.	In IPv6 multicast and any cast message transmission scheme is available.
In IPv4, encryption and authentication facility not provided	In IPv6, encryption and authentication are provided
IPv4 has header of 20 bytes.	IPv6 has header of 40 bytes fixed

7.4 Optimization of Writing of IPV6 Address

The IPv6 address can be abbreviated if there are many zero digits in it. In such a case, the leading zeros of a section can be omitted.

FE80:0000:0000:0001:0800:23E7:F5DB

dropped

FE8.0:0:0:1:0800:23E7:F5DB

Substitute by double colon

The address can be further abbreviated if there are a group of all zeros. A string of repeated zeros is replaced with a pair of colons

FE80::1:0800:23E7:F5DB

In IPv6 address, double colon can only be used once. For example, we have address

0000:0000:1212:2341:0000:0000:1212:251E

which can be written as either

::1212:2341:0000:0000:1212:251E

Or

0000:0000:1212:2341::1212:251E

7.5 Extension Headers

The paradigm of a fixed base header followed by a set of optional extension headers was chosen as a compromise between generality and efficiency. IPV6 needs to include mechanisms to support functions such as fragmentation, source routing, and

authentication. However, choosing to allocate fixed fields in datagram header for all mechanisms is inefficient because most datagrams don't use all mechanisms; the large IPV6 address size exacerbates the inefficiency.

The IPV6 extension header paradigm works similar to IPV4 options a sender can choose which extension headers to include in a given datagram and which to omit. Thus, extension headers provide maximum flexibility.

The length of the base header is 40 bytes. However, in IPv6 header can be followed by up to 6 extension headers. This is to give more functionality to IP datagram. Extension headers of variable size contain a Header Extension Length field and must use padding as needed to ensure that their size is a multiple of 8 bytes. Next Header field in the IPv6 header and zero or more extension headers form a chain of pointers. Each pointer indicates the type of header that comes after the immediate header until the upper layer protocol is ultimately identified. Extension headers must be processed strictly in the order they appear in the packet.

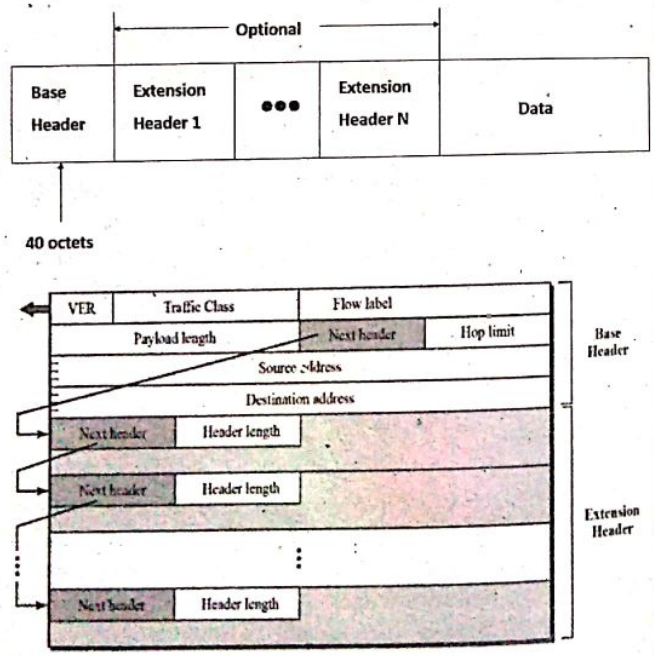


Figure 7.3: IPV6 extension headers

Types of Extension Headers:

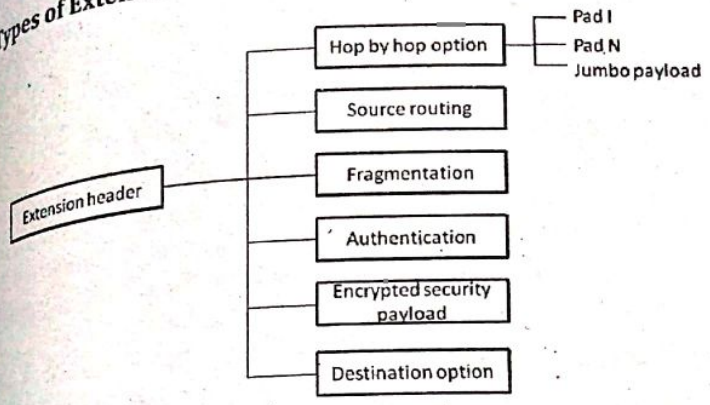


Figure 7.4: Extension header types

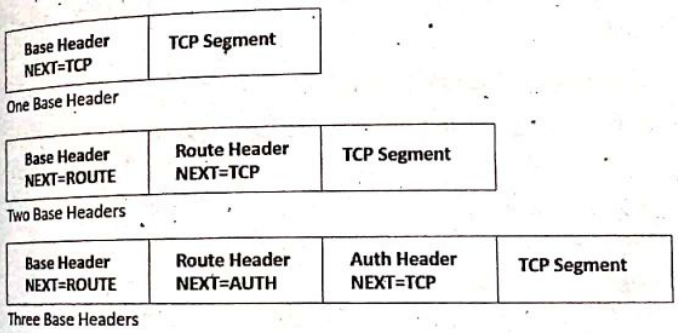


Figure 7.5: Example of header chain

1. **Hop-by-Hop Options Header**

The *hop-by-hop* option is used when the source needs to pass information to all routers visited by the datagram. So far, only three options have been defined: Padl, PadN, and jumbo payload. The Padl option is 1 byte long and is designed for alignment purposes. PadN is similar in concept to Padi. The difference is that PadN is used when 2 or more bytes are needed for alignment. The jumbo payload option is used to define a payload longer than 65,535 bytes.

2. **Source Routing**

The *source routing* extension header combines the concepts of the strict source route and the loose source route options of IPv4.

3. Fragmentation

The concept of fragmentation is the same as that in IPv4. However, the place where fragmentation occurs differs. In IPv4, the source or a router is required to fragment if the size of the datagram is larger than the MTU of the network over which the datagram travels. In IPv6, only the original source can fragment. A source must use a path MTU discovery technique to find the smallest MTU supported by any network on the path. The source then fragments using this knowledge.

4. Authentication

The authentication extension header has a dual purpose: it validates the message sender and ensures the integrity of data.

5. Encrypted Security Payload

The encrypted security payload (ESP) is an extension that provides confidentiality and guards against eavesdropping.

6. Destination Option

The destination option is used when the source needs to pass information to the destination only. Intermediate routers are not permitted access to this information.

Table 7.1: Next Header Code used in IPV6

Code	Next Header	Code	Next Header
0	Hop-by-hop option	44	Fragmentation
2	ICMP	50	Encrypted Security Payload
6	TCP	51	Authentication
17	UDP	59	Null (No Next Header)
43	Source Routing	60	Destination option

7.6 Transition from IPV4 to IPV6

Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly. The problem when transitioning to IPv6 is that while new IPv6

capable systems can be made
send route and receive IPv4 datagram but already IPv4 capable
systems are not capable of handling IPv6 datagrams. It takes a
considerable amount of time before every system in the Internet
can move from IPv4 to IPv6. The transition must be smooth to
prevent any problems between IPv4 and IPv6 systems. Three
strategies have been devised to help the transition.

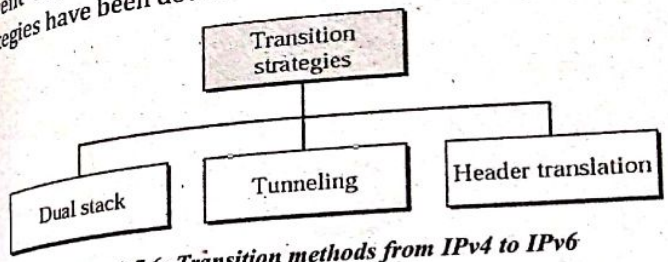


Figure 7.6: Transition methods from IPv4 to IPv6

7.6.1 Dual Stack Operation

Here a node has both IPv4 and IPv6 implementation, referred to as IPv6 / IPv4 node which has ability to send and receive both IPv4 and IPv6 datagram.

When interoperating with an IPv4 node, an IPv6/IPv4 node can use IPv4 datagrams and when interoperating with an IPv6 node, it can speak IPv6. In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.

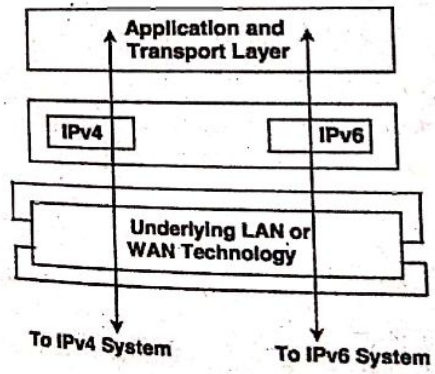


Figure 7.7: Dual stack

To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS

returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

7.6.2 Tunneling

Tunneling provides a way to use an existing IPv4 routing infrastructure to carry IPv6 traffic. The key to a successful IPv6 transition is compatibility with the existing installed base of IPv4 hosts and routers. While the IPv6 infrastructure is being deployed, the existing IPv4 routing infrastructure can remain functional, and can be used to carry IPv6 traffic.

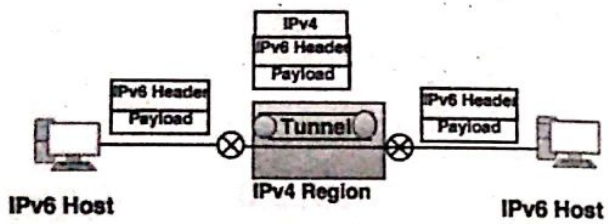


Figure 7.8: Tunneling

Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. With tunneling, the IPv6 node on the sending side of the tunnel takes the entire IPv6 packet and put it in the data fields of an IPv4 packet which is then addressed to the IPv6 node on the receiving side of the tunnel. The intermediate IPv4 routers in the tunnel route this IPv4 among themselves without concerning about the content. It seems as if the IPv6 packet goes through a tunnel at one end and emerges at the other end.

7.6.3 Header Translation

Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6. Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver. In this case, the header format must be totally changed through

header translation. The header of the IPv6 packet is converted to an IPv4 header. Header translation uses the mapped address to translate an IPv6 address to an IPv4 address.

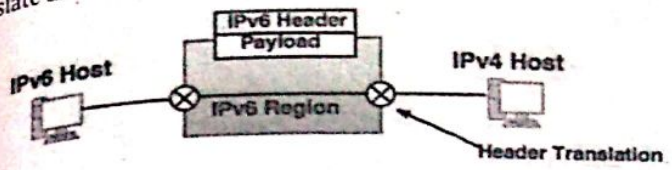


Figure 7.9: Header translation

Header Translation Procedure:

- Change the IPv6 mapped address to an IPv4 address by extracting the rightmost 32 bits.
- Discard the value of IPv6 priority field.
- Set the type of service field in IPv4 to be zero.
- Calculate the checksum for IPv4 and insert in the corresponding field.
- Ignore the Ipv6 flow label.
- Convert the compatible extension headers to options and insert them in the IPv4 header.
- Calculate the length of IPV4 header and insert it into the corresponding field.
- Eventually, compute the total length of the IPv4 packet and insert it into the corresponding field.

7.7 IPV6 Addressing

1. **Unicast:**

   The destination address specifies a single computer (host or router); the datagram should be routed to the destination along the shortest path. A relation between source and destination is one-to-one. Types of unicast addresses are global, link local and site local unicast.

2. **Anycast:**

   The destination is a set of computers, possibly at different locations, that all share a single address; the datagram

should be routed along the shortest path and delivered to exactly one member of the group (i.e. the closest member).

3. **Multicast:**

The destination is a set of computers, possibly at multiple locations. One copy of the datagram will be delivered to each member of the group using hardware multicast or broadcast if viable. The relation between source and destination is one-to-many.

7.8 IPv6 Multicasting

In IPv6, multicast traffic operates in the same way that does in IPv4. Arbitrarily located IPv6 nodes can listen for multicast traffic on an arbitrary IPv6 multicast address. Nodes can join or leave a multicast group at any time. IPv6 multicast addresses have the first 8 bits set to 1111 1111. Therefore, an IPv6 multicast address always begins with FF.

IP multicast address has a prefix FF00:/8. The second octet defines the lifetime and scope of the multicast address. Multicast addresses cannot be used as source address or as intermediate destination in a Routing Extension Header. Some examples of IPv6 Multicast address are for different purposes are; RIPng, OSPFv3, EIGRP.

CHAPTER – 8

NETWORK SECURITY

Computer Networks are a shared resource used by many applications for many different purposes. Network security continues to be an increasingly important topic, particularly with the increase in network interconnectivity. The basic objective of network security is to communicate securely over an insecure medium. Users sometimes want to encrypt the messages they send with the goal of keeping anyone who is eavesdropping on the channel from being able to read the contents of the message. Network security has become a very important issue with the ability to contact anybody form anywhere and more and more people joining the internet with diverse application. Some possible threats that can be encountered in networking environment are: viruses, worms, etc.

Attacks:

The internet has helped to open the door to vandals all over the world, masking any system connected to it vulnerable to attack. Some of the possible attacks are:

- **Interruption:** It is an attack on the availability of information by cutting wires, jamming wireless signals or dropping of packets
- **Interception:** When a message is communicated through network, eavesdroppers can listen in use it for his/her own benefit and try to tamper it.
- **Modification:** Eavesdropper can intercept it and send a modified message in place of the original one.
- **Fabrication:** A message may be sent by a stranger by posing as a friend.
- **Denial of service attacks:** It makes a service unusable, usually by overloading the server or network

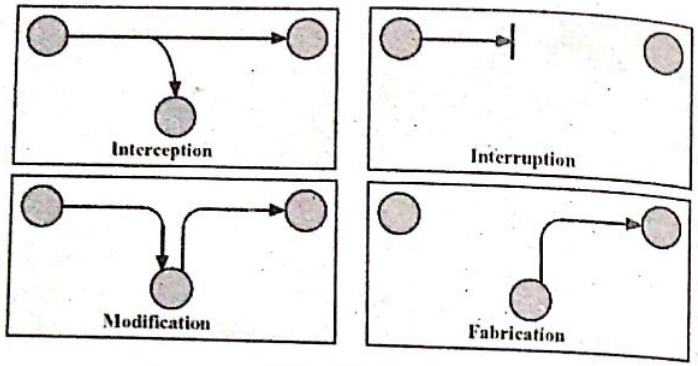


Figure 8.1: Attacks

8.1 Properties of Secure Communication

When two people want to communicate securely over the computer network, certainly sender wants only the receiver to be able to understand a message that sender has sent even though they are communicating over an insecure medium where an intruder may intercept, read and perform computation on whatever is transmitted from sender to receiver. A receiver also wants to be sure that the message he/she receives from a sender indeed sends by a real sender and sender also wants to sure that person to whom he/she communicating is indeed the actual receiver. Sender and receiver also want to make sure that the content of their message has not been altered in transit. Considering these requirements, we can identify the following desirable properties for secure communication, as essential task of Network Security.

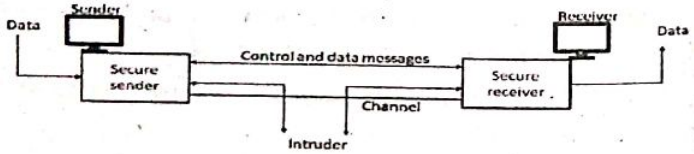


Figure 8.2: Sender, receiver and intruder

1. **Confidentially**

   Only the sender and intended receiver should be able to understand the content of the transmitted message.

Because intruder may tap the message, it is necessary that the message somehow encrypted so that data can't be understood by other than the receiver.

2. **Authentication**

   Both the sender and receiver should able to confirm the identity of the other party involved in the communication to confirm that the other party is indeed who or what he/she claim to be.

3. **Non-repudiation**

   It is the ability to prove that the sender actually sent the data.

4. **Message Integrity and Non-reliability**

   Even if the sender and receiver are able to authenticate each other, they also want to ensure that the content of their communications is not altered, either maliciously or by the accident, in transmission. Checksum techniques, Digital Signature message digest is some ways to provide such message integrity and non-repudiation.

5. **Access control and availability**

   Some user may be legitimate to access resources while others are not. This leads to the notion of access control; ensuring the entities seeking to gain access to resources are allowed to do so only if they have the appropriate access rights, and perform their access in a well-defined manner. Access controls can be implemented by firewalls on application-level, on packet-filtering etc.

8.2 Cryptography

Cryptography refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. Cryptography plays a vital role for private communication through public network. Some important terminologies used in cryptography are:

- **Plaintext /clear text:** The original message produced by the sender is called as plaintext. It is data before transmission.
- **Cipher (code) text:** The plain text is transformed into ciphertext. The encryption program converts the plain the plaintext into ciphertext. It is encrypted or disguised data
- **Key:** It is a secret information to encrypt or decrypt data which is a value or a number. The cipher as an algorithm operates on the key.
- **Ciphers:** The encryption and decryption algorithms together are referred to as ciphers. This term is also used to refer to different categories of algorithms in cryptography.

Cryptography software and/or hardware devices use mathematical formulas (algorithms) to change text from one form to another. It is the technique in protecting integrity or secrecy of electronic messages by converting them into unreadable (cipher text) form. The encryption and decryption algorithms are public and anyone can use them but the encryption and decryption keys are secret.

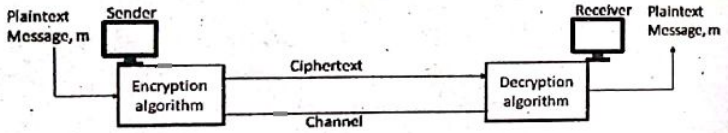


Figure 8.3: Components of cryptography

8.2.1 Traditional Cipher

Encryption methods have historically been divided into two categories: Substitution ciphers and transposition ciphers.

1. Substitution Cipher

In a *substitution cipher* each letter or group of letters is replaced by another letter or group of letters to disguise it. Substitution cipher can be of following types:

a. Caesar cipher

For English text, substitution of the letter in plaintext message is done by a letter that is k position behind that letter. If k=2, then "I am a student" would be "k co c UV FG PV" in cipher text. While the ciphertext looks like nonsense, it wouldn't take long to break the code if you knew that the Caesar cipher was being Used, as there are only 25 possible key values. It is easier to break if you know that cipher text is used to disguise data.

b. Monoalphabetic Cipher

In *monoalphabetic cipher*, substitution of one letter in plaintext message is done by another letter, but not following the regular pattern as Caesar cipher, as long as each letter has a unique substitution.

Plaintext: abcdefghijklmnopqrstuvwxyz

Ciphertext: mnbvcxzasdfghjkipoiuytrewq

For example, Plaintext: attack would be transformed into the cipher text QZZQEA

c. Polyalphabetic Encryption: The idea behind *polyalphabetic encryption* is to use multiple monoalphabetic or Caesar ciphers, with specific cipher to encode a letter in a specific position in plaintext message.

For example, if two different Caesar cipher (with k=2 and k=5), as shown below, one might choose to use these ciphers C1 and C2, in the repeating pattern of C1, C2, C1 i.e., first letter of plaintext is to be encoded using C1, the second using C2, and third using C1 and fourth using again C1 by repeating pattern.

Plaintext	i	a	m	.a	s	t	u	d	e	n	t
C1(K=2)	k	c	o	c	u	v	w	f	g	p	v
C2(K=5)	n	f	r	f	x	y	z	i	j	s	y

Then plaintext message "I am a Student "is encrypted as "k fo c xvwigpy" using C1C2C1 pattern. Here encryption and decryption keys are knowledge of two Caesar keys k=2 and k=5 as well as pattern C1C2C1.

2. Transposition Ciphers

Substitution ciphers preserve the order of the plaintext symbols but disguise them. *Transposition ciphers* reorder the letters but do not disguise them. A transposition-based cipher is different from a substitution-based cipher in that the order of the plaintext is not preserved. Rearranging the order of the plaintext characters makes common patterns unclear and the code much more difficult to break.

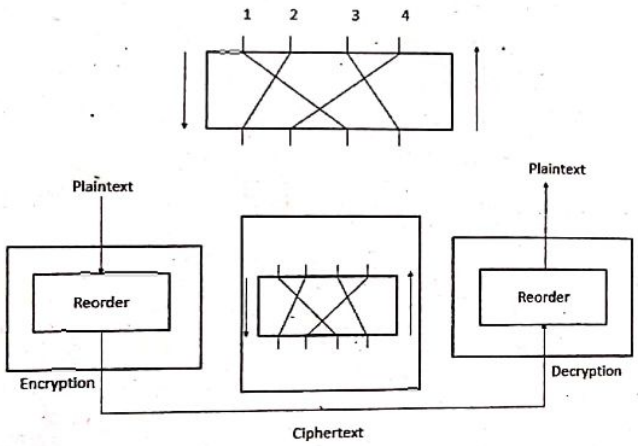


Figure 8.4: Transposition cipher

8.2.2 Types of Cryptography Algorithm

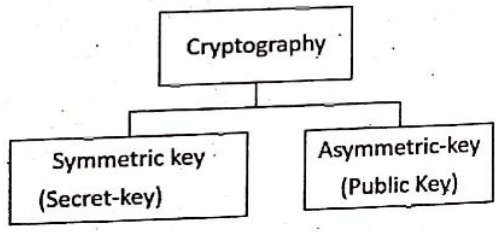


Figure 8.5: Cryptography

1. Symmetric Key Cryptography

In *Symmetric key cryptography*, both sender and receiver share a single secret key for encryption and decryption. The

cipher text has almost the same size as the original message and built on a secret or some random unpredictable data. The strength mostly depends on the key length and encryption of large files is faster and efficient.

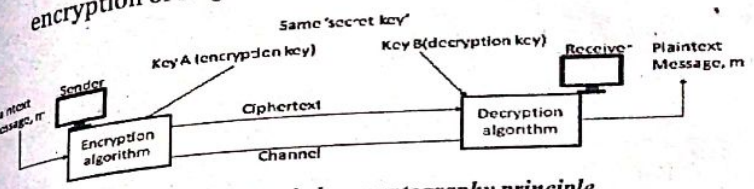


Figure 8.6: Symmetric key cryptography principle

Advantages:

- It takes less time to encrypt a message using the symmetric key algorithm. This is because this key is of smaller size (length).
- It is effective to use for long messages.

Disadvantages:

- The sender and receiver both should have a unique symmetric key. Therefore, a large numbers of user increases.
- The distribution of keys between two users can be difficult.

2. Asymmetric Key Cryptography (Public Key)

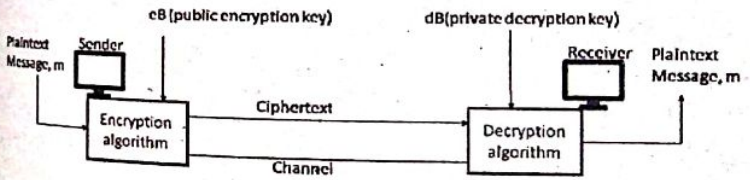


Figure 8.7: Asymmetric key cryptography principle

The *asymmetric key cryptography* is also called public key cryptography. This cryptography principle uses two keys:

i. **Public encryption key (e):** It is announced to the public. The sender uses the public key to encrypt the message to be sent.

ii. **Private decryption key (d):** It is kept by the receiver. The message is decrypted with the help of this key.

In Asymmetric Key Cryptography principle whenever the value 'e' is known encryption easy and any messages can easily encrypt. Likewise, decryption very hard, complex when d is not known (this is regarded as a key of decryption). Decryption easy when d is known. The most famous Asymmetric Key Cryptography algorithm is RSA.

Advantages:

- There is no compulsion of using (sharing) the symmetric key by the sender and receiver.
- The number of keys required reduces tremendously.

Drawbacks:

- The algorithms used are highly complex.
- It takes a long time to calculate ciphertext from plain text.
- It is necessary to verify the association between a sender and public key.

Difference between Symmetric and Asymmetric key system:

Symmetric Key System (Secret Key)	Asymmetric Key System (Public Key)
Sender and receiver both users share a pair key.	The sender uses the public key of receiver to encrypt and receiver decrypt the message using private key.
It is more efficient.	It is less efficient.
It is useful for encryption and decryption of long message.	It is used for encryption and decryption of short messages.
A large number of keys are required.	The number of keys is less.

Block Cipher

Block ciphers use a block of bits as the unit of encryption and decryption. Block ciphers process messages in blocks, each of

which is then encrypted or decrypted, like a substitution on very big characters. Block cipher is made of a combination of transposition units (also called P-boxes), substitution units (also called S-box) and exclusive-OR (XOR) operation. *Permutation box* parallels the traditional transposition cipher for characters. There are three types of P-boxes in modern block ciphers: Straight P-boxes, Expansion P-boxes and Compression P-boxes.

8.3 Data Encryption Standard (DES)

DES is a symmetric-key block cipher which is an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bit string of the same length. DES was designed by IBM and adopted by the U.S. government as the standard encryption method for non-military and non-classified use.

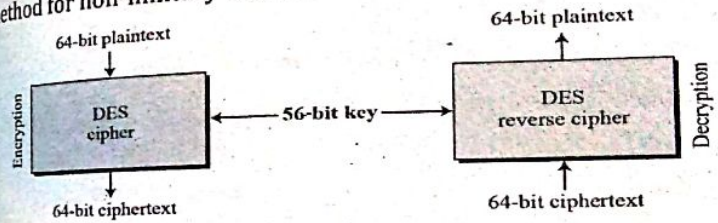


Figure 8.8: Encryption and decryption in DES

Operation

- It encrypts data in 64-bit blocks. A 64-bit block of plaintext goes in one end of the algorithm and a 6-bit block of ciphertext comes out the other end. The same algorithm and key are used for both encryption and decryption.
- The encryption process is made of two permutations which is called initial and final permutations, and 16 round iterations.
- The key is also 64 bits long, of which in fact only 56 bits are used. The remaining 8 bits are used for parity checks.
- The DES algorithm essentially consists of a series of permutations and substitutions. A block which is to be enciphered is first subjected to an initial permutation IP,

then to a complex series of key-dependent operations and finally to a permutations IP^{-1}, which is the inverse of the initial permutation.

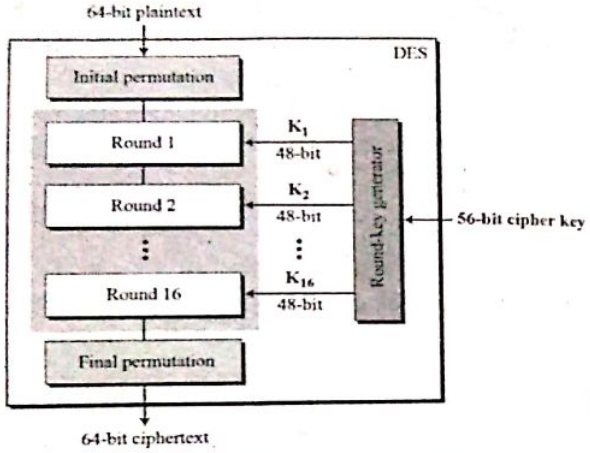


Figure 8.9: General structure of DES

DES uses 16 rounds and each round is a Feistel cipher. The overall processing at each iteration is shown below:

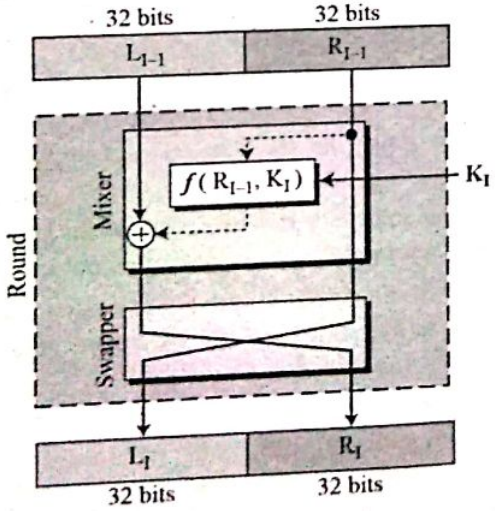


Fig (a) round operation

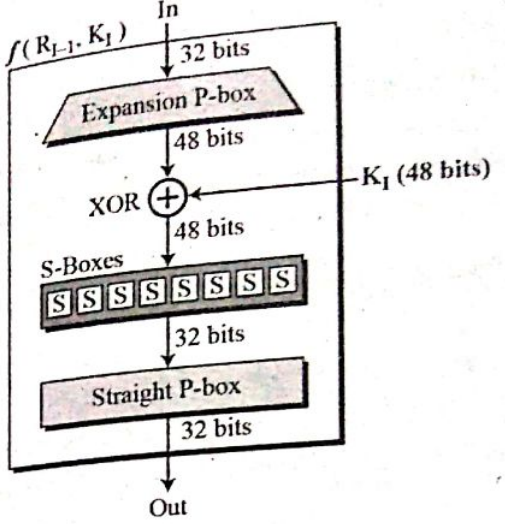


Fig (b) function operation

Figure 8.10: Overall processing

8.4 RSA Algorithm (Rivest, Shamir, Adleman)

RSA algorithm is the most common public key encryption algorithm used in Network Security. It uses two numbers 'e' and 'd' as public and private which have a special relationship to each other. These two keys help to encrypt and decrypt the information. It is based upon a fact that it is easy to multiply two prime numbers but it is very difficult to factor that product and get them back.

Algorithm:

- Choose two large prime numbers: p and q such that p is not equal to q.
- Compute $n=p \times q$,
  $z = (p-1)(q-1)$
- Choose the public key 'e' (with $e<n$) that has no common factors with z (e and z are relatively prime).
- Choose the private key 'd' such that ed-1 is exactly divisible by z
  i.e. $(e \times d) \bmod z = 1$

- A public key is (n, e) and a Private key is (n, d).
- **Encryption:** Cipher text, $C = m^e \bmod (n)$
- **Decryption:** message text, $m = C^d \bmod (n)$

RSA provides a very good security since it uses very large prime numbers. Their product is so large that an attempt to break the code using even the fastest computer shall require a few years.

Example 1: Encrypt a plaintext 'E' using RSA algorithm.

Solution:

Let p=7 and q=11

Then, $n = p \times q = 77$ and $z = (p-1)(q-1) = 6 \times 10 = 60$

Lets find e which is a number that is prime to z and must be $1<e<z$.

We choose e=13 which satisfies the given condition.

So, public key is (e,n) i.e. (13, 77)

Then our ciphertext becomes,

Given plaintext is 'E' so m=5.

Ciphertext (c) = $m^e \bmod (n)$

$= 5^{13} \bmod (77)$

$= 26$

For decryption, d must be such that $(e \times d) \bmod z = 1$ i.e., (ed-1) is divisible by 60

If d=37, then (ed-1) =480 which is exactly divisible by 60.

So , $m = C^d \bmod (n)$

$= 26^{37} \bmod (77)$

Example 2: Encrypt "SUZANNE" using RSA algorithm.

Solution:

Let, p=3 and q=11 are the two prime numbers.

Thus, $n = p \times q = 33$ and $z = (3-1)(11-1) = 20$.

1,2,4,5 and 10 ($e<n$) are factors of 20. So, e can be any value other than these factors.

Let, e=3 such that e and z are relatively

To compute d, condition is $(d \times e) \bmod z = 1$

We do it by using $d = \frac{1 + z \times i}{e}$

For i=1, $d = \frac{1 + 20 \times 1}{3} = \frac{21}{3} = 7$

Thus, d=7 which satisfies the condition $(d \times e) \bmod z = 1$ i.e., $21 \bmod 20 = 1$ (Remainder)

Letters	m	m^e	$C = m^e \bmod (n)$ {Encryption}	C^d	$m = C^d \bmod (n)$ {Decryption}
S	19	6859	28	28^7	19(S)
U	21	9261	21	21^7	21(U)
Z	26	17576	20	20^7	26(Z)
A	1	1	1	1^7	1(A)
N	14	2744	5	5^7	14(N)
N	14	2744	5	5^7	14(N)
E	5	125	26	26^7	5(E)

8.5 Deffi Helman Algorithm

This is a key exchange algorithm used for securely establishing a shared secret over an insecure channel. The communicating parties exchange public information from which they derive a key. An eavesdropper cannot reconstruct the key from the information that went through the insecure channel. More precisely, the reconstruction is computationally infeasible. After the shared secret has been established, it can then be used to derive keys for use with symmetric key algorithms.

The following steps outline the algorithm:

Before establishing a symmetric key, the two parties need to choose two numbers N and G. The first number N, is a large prime number with the restriction that (N-1)/2 must also be a prime number. The second number G is also a prime number.

These two numbers need not be confidential; they can be sent through the Internet and can be public.

The steps are as follows:

1. A chooses a large random number x and calculates $R_1 = G^x \bmod N$
2. A sends R_1 to B. Note that A does not send the value of x; A only send R_1
3. B chooses another large number y and calculate $R_2 = G^y \bmod N$
4. B sends R_2 to A. Again, note that B does not send the value of y but only send R_2
5. A calculate $K = (R_2)^x \bmod N$. B also calculates $K = (R_1)^y \bmod N$. And K is the symmetric key for the session

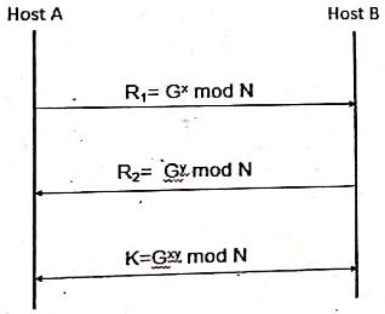


Figure 8.11: Deffi helman

Note: the symmetric key in Diffie-Hellman protocol is $K = G^{xy} \bmod N$.

Example:

Suppose G = 7 and N = 23

A chooses x = 3 and calculate $R_1 = G^x \bmod N = 7^3 \bmod 23 = 21$

B chooses y = 6 and calculate $R_2 = G^y \bmod N = 7^6 \bmod 23 = 4$

Now,

A sends the number 21 to B

B sends the number 4 to A

A calculates the symmetric key as

$K = (R_2)^x \bmod N$

$= (4)^3 \bmod 23$

$= 18$

B calculate the symmetric key as

$K = (R_1)^y \bmod N$

$= (21)^6 \bmod 23$

$= 18$

Hence both keys are calculated separately and they shared same key.

8.6 Digital Signatures

Digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as signature. The signature guarantees the source and integrity of the message.

Why digital signature?

When participating in financial or legal transactions, people often identify themselves through a handwritten signature or by entering a PIN, but when a person want to sign an electronic document so that later he will be able to prove that it is his document and no one else, he need to create a digital signature.

A digital signature is a security procedure that uses public key cryptography to assign to a document a code for which user alone have the key.

Digital signatures should be done in such a way that, they are:

a. **Verifiable:** It must be possible to prove that a document signed by an individual was indeed signed by that individual. The signature must be verifiable.

b. **Non forgeable and Non repudiable:** The signature cannot be forged and a signer cannot later repudiate or deny having signed the document. Individual can only sign the document.

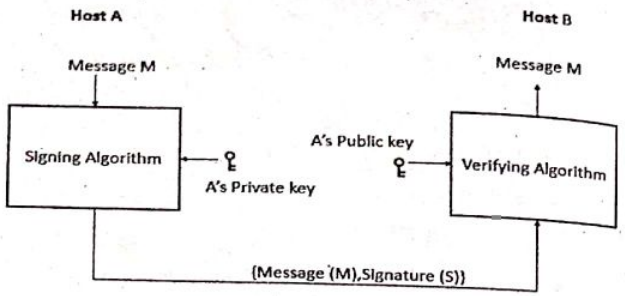


Figure 8.12: Digital signature process

A digital signature may be formed by encrypting the entire with the sender's private key or by encrypting a hash code of the message with the sender's private key. This encoded hash becomes the digital signature or transmitted with the document.

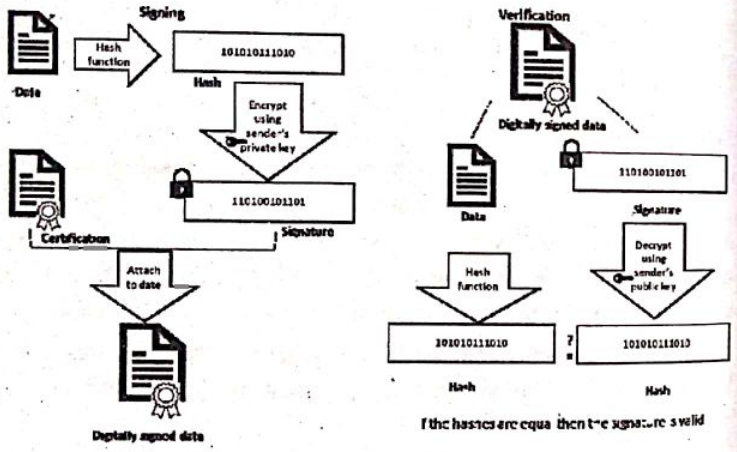


Figure 8.13: Signing and verification of digitally data

When a user digitally signs a document, a hash is generated from the document through a complex mathematical computation that generates a large prime number. This encoded hash becomes the digital signature and is either stored with the document or transmitted with the document. Later if someone wants to verify that this document belongs to this use, a new hash is created form the document. The original hash which has been encrypted with the owner's private key is decrypted with the owner's public key,

and the two hashes are compared. If the two hashes agree, the data was not tampered with, and the user's digital signature is valid.

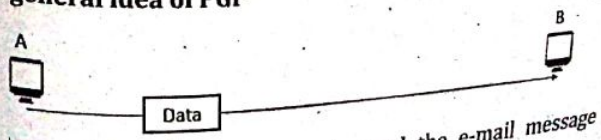
8.7 Securing E-mail (PGP)

PGP is developed by Phil Zimmerman in 1995. Pretty Good Privacy (PGP) is an e-mail encryption scheme (technique) that has become a de-facto standard that is being used widely, by thousands of users all over the globe. Depending on the version, the PGP software was supposed to use MD5 or SHA for calculating the message digest such as CAST, Triple-DES or IDEA.

PGP is high-quality encryption software that has become quite popular for creating secure e-mail message and encrypting other types of data files. In addition, PGP provides data compression. PGP employs some of the latest techniques of encryption including public key cryptography & digital signature.

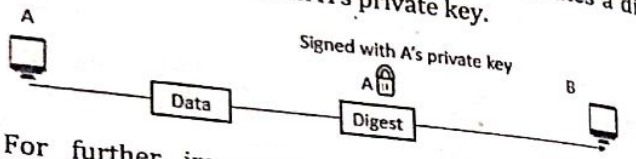
When PGP is installed, the software creates a public key pair for the user. The public key can be posted on the user's Web site or placed on a public key server. The private key is protected by the use of a password. To maintain the security of the system, the password has to be entered every time the user accesses the private key. PGP gives the user the option of digitally sign the (sent/received) messages, encryption of those messages, or both digitally signing and encrypting. It is assumed that all users are using the public key cryptography and they have generated a private/public key pair. All users also use a symmetric key system such as triple DES. PGP encrypts data using block cipher called IDEA (International Data Encryption Algorithm) which uses 128-bit keys.

The general idea of PGP

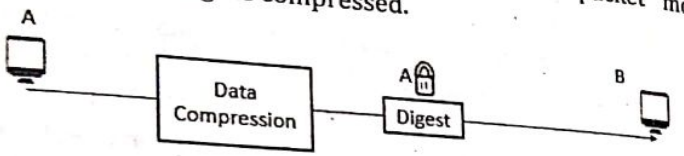


The simplest scenario is to send the e-mail message in plaintext.

For authentication, A signs the message. A creates a digest of the message and signs it with A's private key.



For further improvement, to make the packet more compact, the message is compressed.



Confidentiality in an e-mail system can be achieved using conventional encryption with one-time session key as shown below:

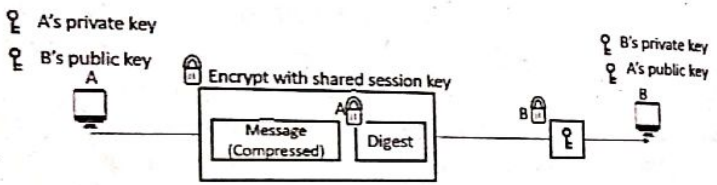


Figure 8.14: PGP process

A's can create a session key, use the session key to encrypt the message and the digest and send the key itself with the message. However, to protect the session key, A encrypt it with B's public key.

When B receives the packet, he first decrypts the session key, using his private key. Then uses the session key to decrypt the rest of the message. After decompressing the rest of the message, B creates a digest of the message and checks to see if it is equal to the digest sent by A. If it is, then the message is authentic.

Services offered by PGP:

- Authentication
- Confidentiality
- Compression
- Email compatibility

8.8 S/MIME (Secure/ Multipurpose Internet Mail Extension)

Multipurpose Internet Main Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail. MIME transforms non-ASCII data at the sender site to NVT (Network Virtual Terminal) ASCII data and delivers it to the client MTA to be sent through the Internet. The message at the receiving site is transformed back to the original data. E-mail can send messages only in NVT 7-bit ASCII format. Also, it cannot be used to send binary files or video or audio data.

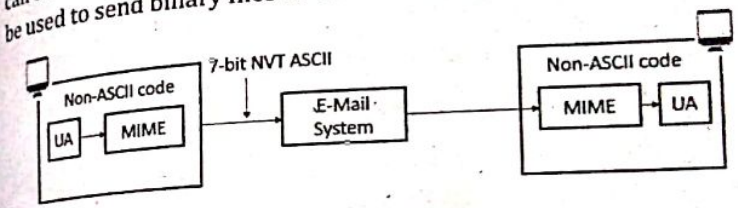


Figure 8.15: MIME

8.9 Securing TCP connections: Secure Socket Layer (SSL)

SSL is designed to provide security and compression services to data generated from the application layer. SSL can receive data from application layer protocol, the received data is compressed, signed and encrypted. The data is then passed to a reliable transport-layer protocol.

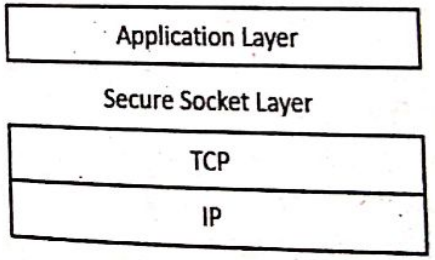


Figure 8.16: SSL Layer

Secure sockets layer (SSL), originally developed by Netscape, is a protocol designed to provide data encryption and authentication between a Web client and a Web server. Whenever

a web surfer visits a secure site that uses SSL technology, it creates an encrypted link between their browser session and the web server. The protocol begins with a handshake phase that negotiates an encryption algorithm and keys, and authenticates the server to the client. Optionally, the client can also be authenticated to the server. Once the handshake is complete and the transmission of application data begins, and all data is encrypted using session keys negotiated during the handshake phase. SSL is widely used in Internet commerce, being implemented in almost all popular browsers and Web servers.

SSL provides several services on data received from the application layer;

- **Fragmentation:** SSL divides the data into blocks.
- **Compression:** Each fragment of data is compressed using one of lossless compression method between the client and server.
- **Message Integrity:** SSL uses a keyed-hash function to create a Message Authentication Code (MAC).
- **Confidentiality:** To provide confidentiality, symmetric key cryptography is used,
- **Framing:** A header is added to the encrypted payload.

The exchange of messages facilitates the following actions:

- Authenticate the server to the client;
- Allows the client and server to select a cipher that they both support;
- Optionally authenticate the client to the server;
- Use public-key encryption techniques to generate share secrets;
- Establish an encrypted SSL connection

Advantages:

- To secure online credit card transactions.

- To secure system logins and any sensitive information exchanged online and webmail and applications like Outlook Web Access, Exchange and Office Communications Server.
- To secure workflow and virtualization applications like Citrix Delivery Platforms or cloud-based computing platforms and the connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.
- To secure the transfer of files over https and FTP(s) services such as website owners updating new pages to their websites or transferring large files.
- To secure hosting control panel logins and activity.
- To secure intranet based traffics such as internal networks, file sharing, extranets, and database connections.
- To secure network logins and other network traffic with SSL VPNs such as VPN Access Servers or applications like the Citrix Access Gateway.

8.10 Network Layer Security (IPsec, VPN)

8.10.1 IPsec (IP security)

The IETF has devised a set of protocols that provide secure internet communication, called *IPsec* (IP security). At the network layer, security is applied between two hosts, two routers, or host and a router. The purpose of IPsec is to protect those applications that used the service of the network layer directly such as routing protocols. The protocol offers authentication and privacy services at the IP layer, and can be used with both IPV4 and IPV6. It enhances flexibility and extensibility of the system.

1. **IPsec Modes**

IPsec operates in one of two modes.

Transport Mode

In *transport mode*, IPsec protects what is delivered form the transport layer to the network layer. In other words, transport mode protects the payload to be encapsulated in the network layer. The transport mode does not protect the IP header. It only protects the packet from the transport layer.

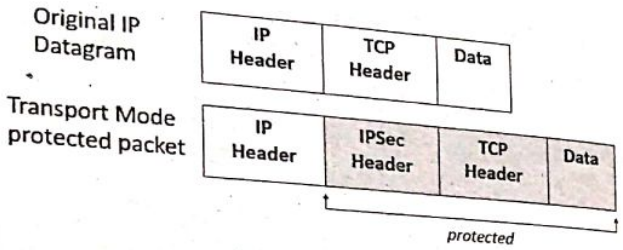


Figure 8.17: IPsec in transport mode

b. Tunnel Mode

In *tunnel mode*, IPsec protects the entire IP packet. It takes an IP packet including the header, applies IPsec security methods to the entire packet and then adds a new IP header.

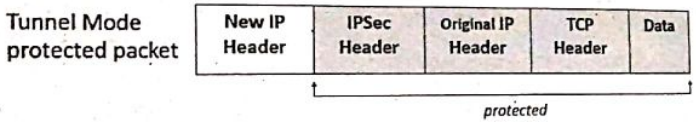


Figure 8.18: IPsec in tunnel mode

2. Two security protocols

IPsec defines two protocols: Authentication Header (AH) protocol and Encapsulating Security Payload (ESP) protocol.

a. Authentication Header (AH) protocol

Authentication Header (AH) is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet. AH is placed in the appropriate location, based on the mode (transport or tunnel). AH provides source authentication and data integrity but not privacy.

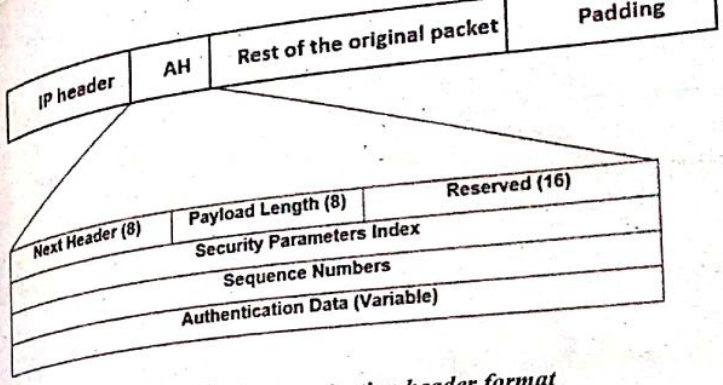


Figure 8.19: Authentication header format

- **Nest Header:** defines the type of payload carried by the IP datagram.
- **Payload Length:** It defines the length of the authentication header.
- **Security parameter index:** It plays the role of a virtual circuit identifier and is same for all packets sent during a connection.
- **Sequence number:** It provides ordering information for a sequence of datagram.
- **Authentication Data:** It is the result of applying a hash function to the entire IP datagram.

b. Encapsulating Security Payload

Authentication Header protocol does not provide confidentiality, only provides source authentication and data integrity. *ESP*'s authentication data are added at the end of the payload which makes its calculation easier. ESP adds a header and trailer.

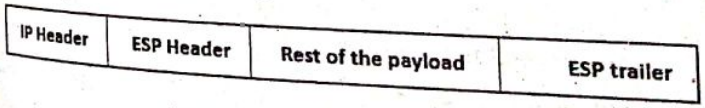


Figure 8.20: IPsec ESP format

8.10.2 VPN (Virtual Private Network)

One of the applications of IPsec is in virtual private network. A *virtual private network (VPN)* is a private network that

interconnects remote networks through primarily used public communication infrastructures for example, Internet. A computer is enabled to send and receive data across the shared or public networks as if it is directly connected to the private network by the VPN. The VPN are created by implementing a virtual (point to point) connections through the use of either dedicated connection or through the virtual tunneling protocols. And also, through the means of traffic encryptions.

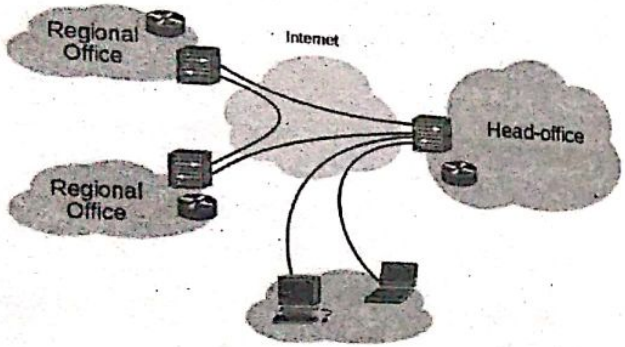


Figure 8.21: Remote roaming users VPN

a. Remote Access VPN

It allows an individual user to connect to a private business network from a remote location. And that can be easily done through the use of multiple computers (i.e. desktop or laptop) to the Internet. It allows all its user to have the most secure connection over a remote computer network.

Remote Access VPN Working:

- **Two connections:** It comprises of two connections in which one is connected to the internet and the second is connected to the VPN.
- **Datagrams:** In the case of diagrams it comprises the data, destination and source information.
- **Firewalls:** VPNs allows authorized users to pass through the firewalls.
- **Protocols:** In the case of protocols, it is used to create the VPN tunnels.

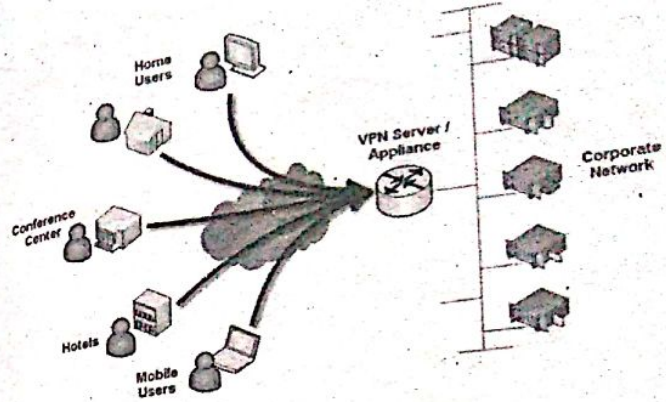


Figure 8.22: Host to gateway/remote-access VPNs

Some functions of Remote Access VPN are:

i. **Authentication:** It helps to validate those data which were sent from the sender.

ii. **Access control:** It limit unauthorized users from accessing the network of the system.

b. Site to Site VPN

If an organization or any sorts of the company comprises multiple numbers of fixed location to develop secure communication over a network (can be used by public) such as the Internet then they can implement *Site to site VPN*. It extends the company's network, i e. it allows making computer resources available to its employee at the different location. An example: Growing corporation with the bunch of branch offices around the world needs Site to Site VPN.

Types of site-to-site VPNs:

- **Intranet-based:** *Intranet based VPN* network communication is best for those types of organization in which the organization or company has one or more remote locations that they want to join in a single private secure network.

- **Extranet-based:** This type of communication is best for those type of organization in which the company or organization has close good relation with other organizations or the company like the partner, suppliers or even the customers. In such scenario, the company can establish or implement extranet VPN that connects those all prerequisites of the company. Such an extranet based connection can easily allow the companies to cooperate and work together in a secure networking environment without fear of the intruders.

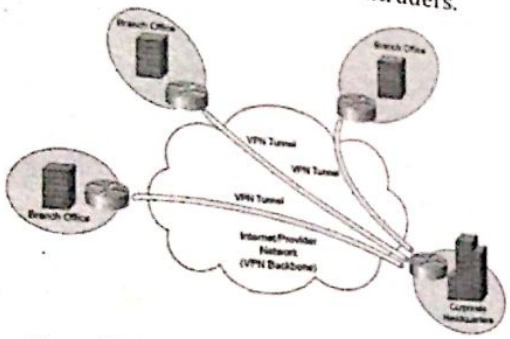


Figure 8.23: Gateway to gateway/Site to Site VPN

8.11 Securing Wireless LANs

8.11.1 WEP (Wired Equivalent Privacy) Protocol

Wired Equivalent Privacy Protocol (WEP) is a data link level security protocol prescribed by 802.11 standards. It is first and widely used security choice offered in routers for users. It is secured as wired network but less in comparison to WPA2 (Wi-Fi Protected Access 2). It is recognized with 10 or 26 hexadecimal digits.

The 802.11 standard prescribes a data link level security protocol called WEP (Wired Equivalent Privacy), which is designed to make the security of a wireless LAN as good as that of a wired LAN. When 802.11 security is enabled, each station has a secret key shared with the base station. How the keys are distributed is not specified by the standard.

WEP features:

- Protect wireless communication from eavesdropping (secretly listening to the private conversation of others without their consent)
- Prevent unauthorized access to wireless network
- Goals of WEP are access control, data integrity, confidentiality. WEP relies on a secret key which is shared between the sender and the receiver. Sender may be a mobile station (e.g.: Laptop) and receiver is access point (e.g., base station). The Secret Key encrypts packets before they are transmitted. Integrity check is used to ensure packet are not modified in transit. WEP encryption uses a stream cipher based on the Ron's Code 4 (RC4) algorithm which was designed by Ronald Rivest. In WEP, RC4 generates a key stream that is XORed with the plaintext to form the cipher text.

WEP Encryption

Encryption details:

- Uses RC4 algorithm for confidentiality and CRC-32 checksum for integrity.
- Standard 64-bit WEP uses a 40-bit key which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key.
- The key size was limited before but now it is extended as 128-bit WEP using 104-bit key size.

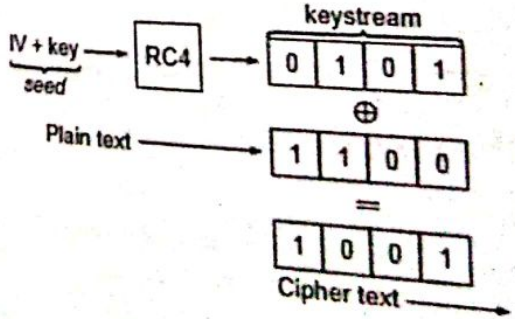


Figure 8.24: WEP encryption

Decryption Details:

- At the receiver side, cipher text is XORed with keystream to obtain the plain text.
- 64-bit WEP key is usually entered as a string 10 hexadecimal character.
- Each character represents four bits, 10 digits of four bits each gives 40 bits & adding 24 bits IV gives 64 bits WEP key.
- A 128-bit WEP key is usually entered as a string of 26 hexadecimal characters.
- 26 digits of four bits each give 104 bits and adding the 24-bit IV produces the complete key.

8.11.2 WPA (Wi-Fi Protected Access)

WPA is a wireless security protocol designed to address and fix known security issues in WEP. WPA provides users with a higher level of assurance that their data will remain protected by using Temporary Key Integrity Protocol (TKIP) for data encryption.

8.11.3 WPA2

Wi-Fi protected Access 2 based on IEEE 802.11i, is a wireless security protocol in which only authorized users can access a wireless device, with features supporting stronger cryptography example, AES (Advanced Encryption Standard), stronger authentication protocol example, Extension Authentication Protocol (EAP), key management, replay attack protection and data integrity.

8.12 Firewalls: Application Gateway and Packet Filtering, and IDS

8.12.1 Firewall

A *firewall* is a system (or group of systems) that enforces a security policy between a secure internal network and an untrusted network such as the Internet. Firewall is a security system intended to protect an organization's network against external threats such as hackers coming from another network.

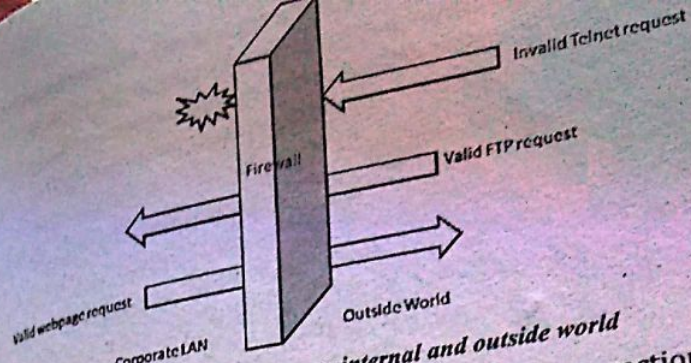


Figure 8.25: Firewall between internal and outside world

An organization places a firewall at its connection to external networks. A firewall partitions the internet into two regions referred to informally as the inside and outside. Thus, firewall isolates organization's internal net from the larger internet, allowing some packets to pass, blocking others. A firewall is a combination of hardware and software that isolates an organization's internal network from the Internet allowing specific connections to pass and blocking others.

Organizations employ firewalls for the following reasons:

- To prevent intruders from interfering with the daily operation of the internal network, denial of service attack, SYN FIN Attack
- To prevent intruders from deleting or modifying information stored within the internal network.
- To prevent intruders from obtaining secret information.
- Allow only authorized access to inside network
- Prevent illegal modification/access of internal data: e.g., attacker replaces official homepage with something else

Types of Firewalls:

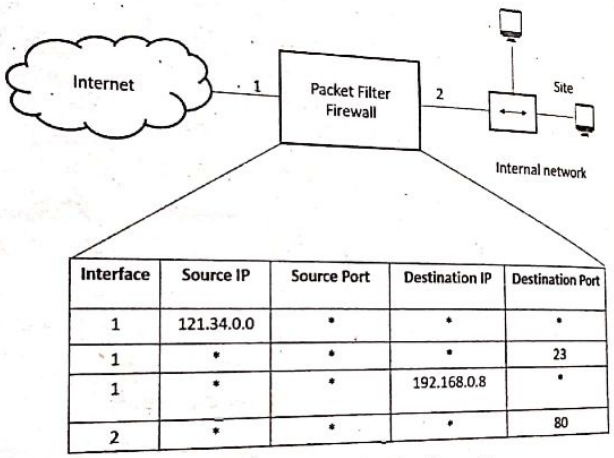
A firewall is usually classified as a packet-filter firewall and a proxy-based firewall/ application-level gateway firewall.

a. **Packet- Filter Firewall**

Packet filter is the first, generation firewall which is essentially a router that has been programmed to filter out

certain IP addresses or TCP port numbers. These types of routers perform a static examination of the IP addresses and TCP port numbers, then either deny a transaction or allow it to pass on the basis of information stored in their tables. These types of routers are relatively simple in design. Also, they act very quickly, but they are a little too simple to provide a high level of security.

In Packet Filtering, internal network is connected to the internet via router firewall. It works at the network layer. Router filters packet-by-packet and compares to a set of criteria before it is forwarded. Router uses a filtering table to decide which packet must be forwarded/dropped based on: The Source and destination IP addresses, TCP/UDP source and destination port numbers, ICMP message type, etc.



Interface	Source IP	Source Port	Destination IP	Destination Port
1	121.34.0.0	*	*	*
1	*	*	*	23
1	*	*	192.168.0.8	*
2	*	*	*	80

Figure 2.26: Table in packet filter firewall

Description:

1. Incoming packets from the network 121.34.0.0 are blocked.
2. Incoming packets destined for any internal TELNET server (port 23) are blocked.
3. Incoming packets destined for internal host 192.168.0.8 are blocked.
4. Outgoing packets destined for an HTTP server (port ... are blocked. The organization does not want its employees to browse the Internet.

Advantages:

- Simplicity
- Transparency to users
- High speed

Disadvantages:

- Difficulty of setting up packet filter rules
- Lack of Authentication

b. **Application-Level Gateway:**

It is not possible to control the data with packet filters because they are not capable of understanding the contents of a particular service. For this purpose, an application-level control is required.

An *application-level gateway* is often referred to as a proxy. An application-level gateway provides higher-level control on the traffic between two networks in that the contents of a particular service can be monitored and filtered according to the network security policy. Therefore, for any desired application, the corresponding proxy code must be installed on the gateway in order to manage that specific service passing through the gateway.

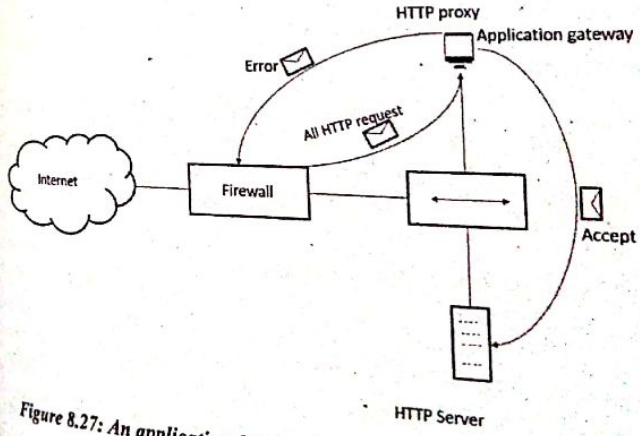


Figure 8.27: An application-level gateway implementation for HTTP

When the user client process sends a message, the application gateway runs a server process to receive the request. The server opens the packets in the application level and finds out if the request is reasonable. If it is, the server acts as a client process and sends the message to real server. If it is not, the message is dropped and error message is sent to external user. An application gateway is an application-specific server through which all application inbound and outbound data must pass. Application with multiple application gateways can run on the same host, but in such case each gateway is a separate server having its own processes.

Advantages:

- Higher security than packet filters
- Only need to scrutinize a few allowable applications
- Easy to log and audit all incoming traffic

Disadvantages:

- Additional processing overhead on each connection

8.12.2 Intrusion Detection System (IDS)

An *intrusion detection system (IDS)* is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

There is a wide spectrum of IDS, varying from antivirus software to hierarchical systems that monitor the traffic of an entire backbone network. The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A system that monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on

machine learning). Some IDS have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system.

Types of IDS

a. **Network Intrusion Detection Systems**

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of the NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulation network intrusion detection systems. NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS. When we classify the design of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS. On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not. Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

b. **Host intrusion detection systems**

Host intrusion detection systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

BIBLIOGRAPHY

- Andrew S. Tanenbaum, "Computer Networks", 4th Edition, Pearson Prentice Hall, 2011.
- Behrouz A. Forouzan," Data Communications and Networking", 5th Edition, McGraw Hill Education (India), 2013
- William Stalling, "Data and Computer Communication", 8th Edition, Pearson Prentice Hall, 2007.
- James F. Kurose and Keith W. Ross," Computer Networking: A top-down approach featuring the Internet", 2nd Edition, Pearson Education,2003.
- Todd Lammle, "Cisco Certified Network Associate, study guide", 7th Edition, Wiley India Pvt. Ltd, 2009.