UNIT I INTRODUCTION AND APPLICATION LAYER

Data Communication - Networks – Network Types – Protocol Layering – TCP/IP Protocol suite –OSI Model – Introduction to Sockets - Application Layer protocols: HTTP – FTP – Email protocols(SMTP - POP3 - IMAP - MIME) – DNS – SNMP

1.1 Data Communication

When we communicate, we are sharing information. This sharing can be ***local or remote***.

The term telecommunication, which includes telephony, telegraphy, and television, means communication at a distance (tele is Greek for "far").

The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.

"Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable".

For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

The effectiveness of a data communications system depends on ***four fundamental characteristics:***

I. Delivery: The system must deliver data to the correct destination. Data must be received by the intended device or user .

2. Accuracy: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

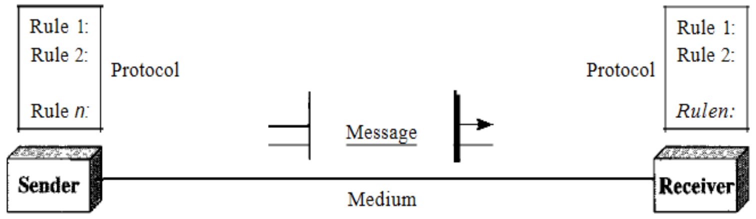
3. Timeliness: The system must deliver data in a timely manner. Data delivered late are useless.

4. Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

1.1.1 Components

A data communications system has five components

Figure 1.1 *Five components ofdata communication*



1.Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2.Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber optic cable, and radio waves.

5. Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

1.1.2 Data Representation

Information today comes in different forms such as text, numbers, images, audio, and video.

Text

In data communications, text is represented as a bit pattern, a sequence of bits (O s or 1 s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding.

Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Numbers

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

Images

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution. The size and the value of the pattern depend on the image.

For an image made of only black-and-white dots (e.g., a chessboard), a I-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale

There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of three primary colors: red, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio

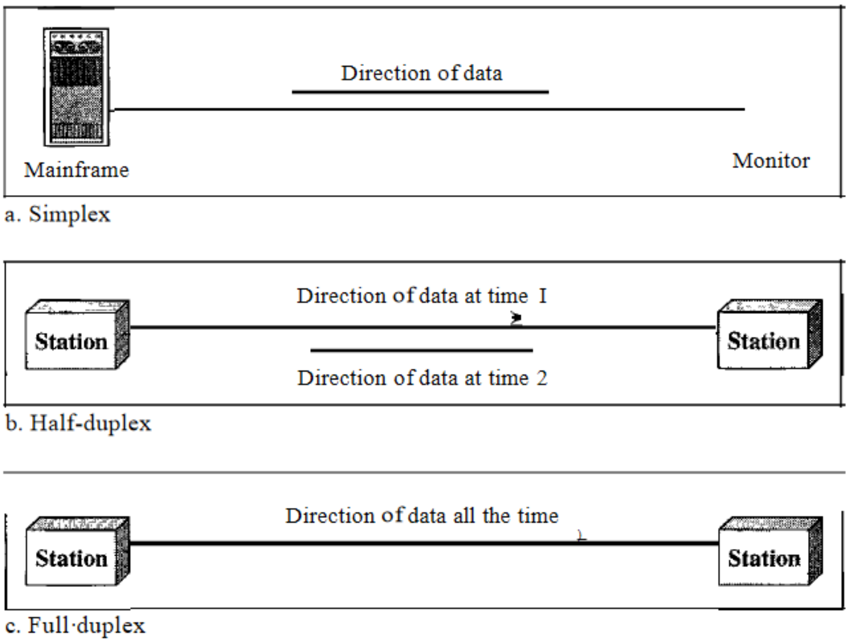
Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images.

Video
Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

1.1.3 Data Flow / transmission mode

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure 1.2.

Figure 1.2 *Dataflow (simplex, half-duplex, andfull-duplex)*


Direction of data
Mainframe
Monitor
Direction of data at time I
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

c. Full·duplex

Simplex
In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.2a). Keyboards and traditional monitors are examples of simplex devices.

Advantage of Simplex mode:

- In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

Disadvantage of Simplex mode:

- Communication is unidirectional, so it has no inter-communication between devices.

Half-Duplex
In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa (see Figure 1.2b)

Walkie-talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time.

Advantage of Half-duplex mode:

- In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

Disadvantage of Half-Duplex mode:

- In half-duplex mode, when one device is sending the data, then another has towait, this causes the delay in sending the data at the right time.

Full-Duplex

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously (see Figure 1.2c).The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time.

Advantage of Full-duplex mode:

- Both the stations can send and receive the data at the same time.

Disadvantage of Full-duplex mode:

- If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

1.2 NETWORKS

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Distributed Processing

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.

1.2.1 Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance

Performance can be measured in many ways, including transit time and response time. ***Transit time*** is the amount of time required for a message to travel from one device to another. ***Response time*** is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software. Performance is often evaluated by two networking metrics: ***throughput and delay***. Throughput is an actual measurement of how fast data can be transmitted. Latency/delay is time required for a message to completely arrive at the destination from source. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

1.2.2 Physical Structures

Type of Connection / Line configuration

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

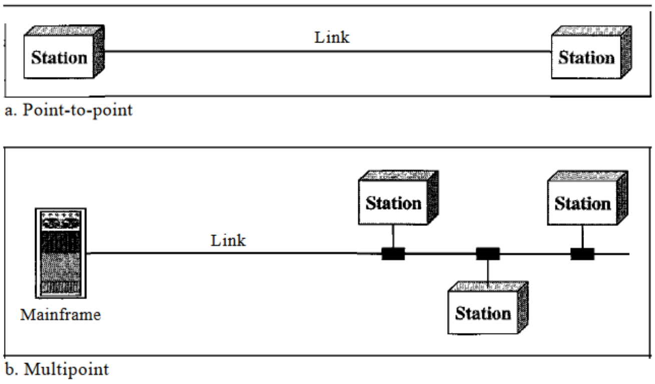
Point-to-Point

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends (see Figure 1.3a). When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.3b). In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

Figure 1.3 *Types of connections: point-to-point and multipoint*



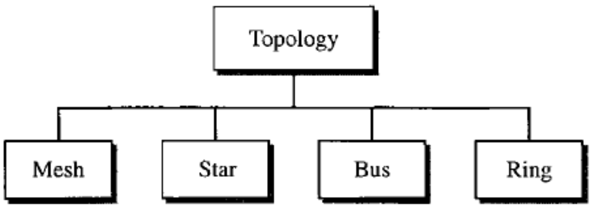
a. Point-to-point

b. Multipoint

Physical Topology

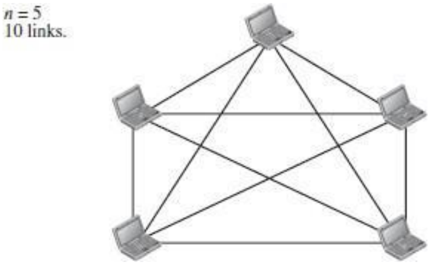
The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring (see Figure 1.4).

Figure **1.4** *Categories oftopology*



Mesh Topology

- In a mesh topology, every device has a dedicated point-to-point link to everyother device.
- The term dedicated means that the link carries traffic only between the twodevices it connects.
- The number of physical links in a fully connected mesh network with *n* nodes isgiven by *n* (*n* – 1) / 2.

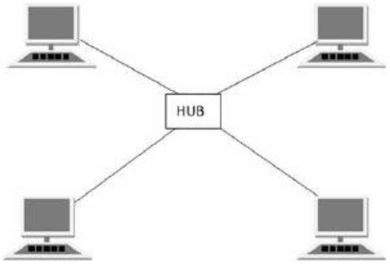


Advantages of Mesh Topology	Disadvantages of Mesh Topology
1. Each connection can carry its own data load. 2. It is robust. 3. Fault is diagnosed easily. 4. Provides security and privacy.	1. Installation and configuration is difficult. 2. Cabling cost is more. 3. Bulk wiring is required.

Star Topology

- In a star topology, each device has a dedicated point-to-point link only to acentral controller, usually called a hub.
- The devices are not directly linked to one another.

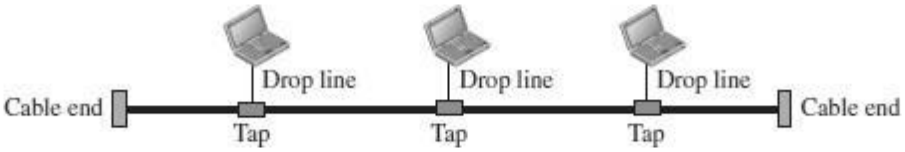
- The controller/hub acts as an exchange.
- If one device wants to send data to another, it sends the data to the controller/hub ,which then relays the data to the other connected device.



Advantages of Star Topology	***Disadvantages of Star Topology***
1. Fast performance with few nodes and low network traffic. 2. Hub can be upgraded easily. 3. Easy to troubleshoot. 4. Easy to setup and modify. 5. Only that node is affected which has failed, rest of the nodes can work smoothly	1. Cost of installation is high. 2. Expensive to use. 3. If the hub fails, then the wholenetwork is stopped. 4. Performance is based on the hub thatis it depends on its capacity

Bus Topology

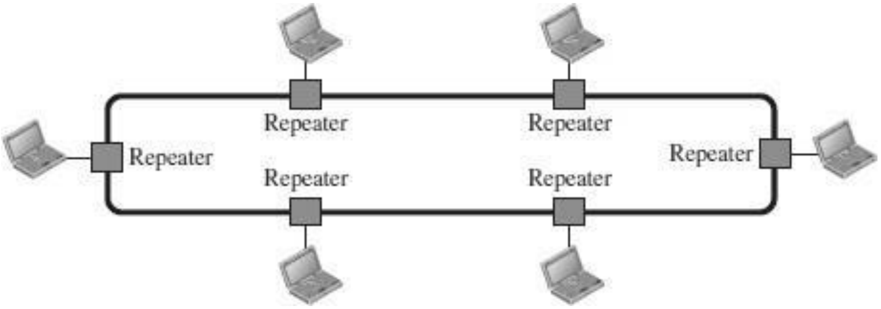
- Bus topology is a network type in which every computer and network device isconnected to single cable.
- The long single cable acts as a backbone to link all the devices in a network.
- When it has exactly two endpoints, then it is called Linear Bus topology.
- It transmits data only in one direction.



Advantages of Bus Topology	**Disadvantages of Bus Topology**
1. It is cost effective. 2. Cable required is least compared to other network topology. 3. Used in small networks. 4. It is easy to understand. 5. Easy to expand joining two cables together	1. Cables fails then whole network fails. 2. If network traffic is heavy or nodes are more, the performance of the network decreases. 3. Cable has a limited length. 4. It is slower than the ring topology.

Ring Topology

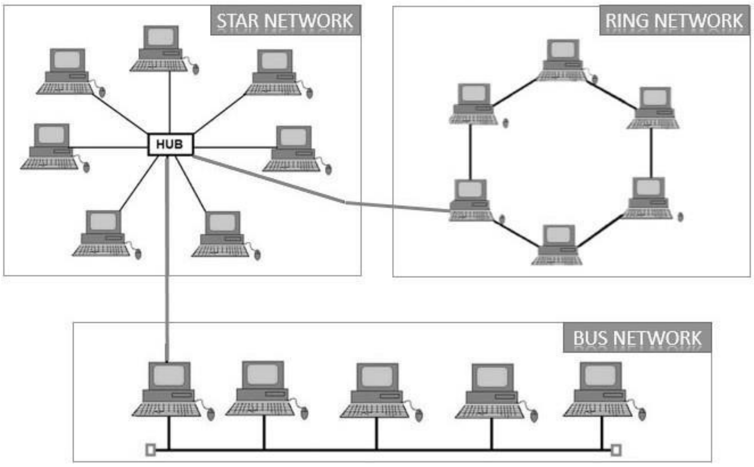
- In a ring topology, each device has a dedicated point-to-point connection withonly the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until itreaches its destination.
- Each device in the ring incorporates a repeater.
- When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages of Ring Topology	Disadvantages of Ring Topology
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data. 2. Cheap to install and expand	1. Troubleshooting is difficult in ring topology. 2. Adding or deleting the computers disturbs the network activity. 3. Failure of one computer disturbs the whole network

Hybrid Topology

- Hybrid Topology is a combination of one or more basic topologies.
- For example if one department in an office uses ring topology, the other departments uses star and bus topology, then connecting these topologies will result in Hybrid Topology.
- Hybrid Topology inherits the advantages and disadvantages of the topologies included.



Advantages of Hybrid Topology	Disadvantages of Hybrid Topology
1. Reliable as Error detecting and trouble shooting is easy. 2. Effective. 3. Scalable as size can be increased easily. 4. Flexible.	1. Complex in design. 2. Costly

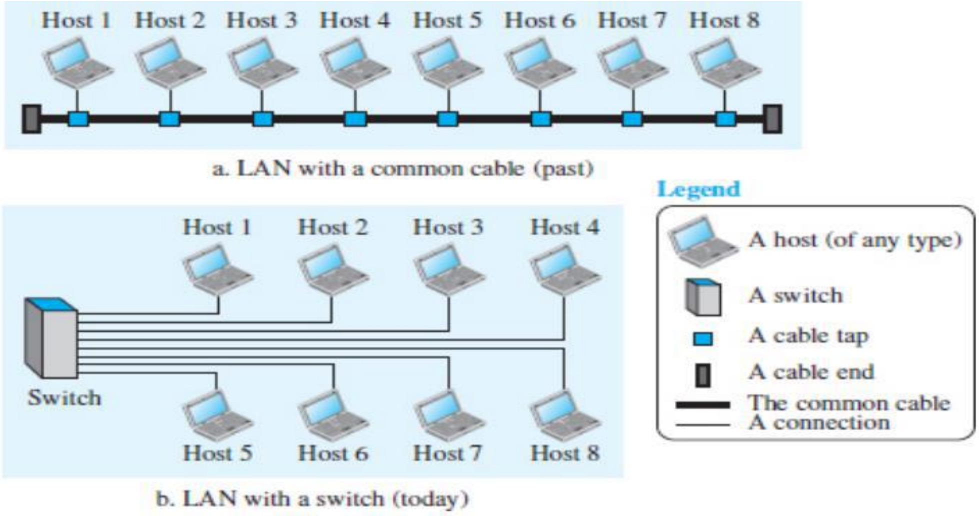
1.3 NETWORK TYPES

Different types of networks: LANs MANs and WANs.

1.3.1 Local Area Network

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, networkadapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- LAN can be connected using a common cable or a Switch

Figure 1.8 *An isolated LAN in the past and today*



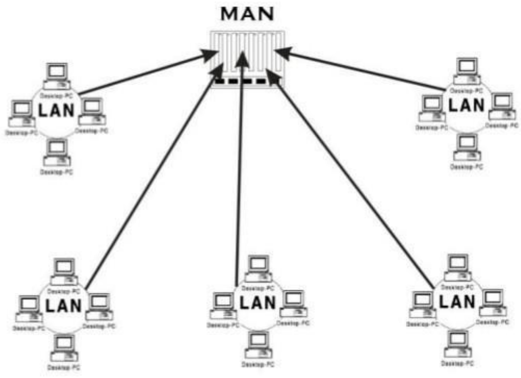
a. LAN with a common cable (past)

b. LAN with a switch (today)

Advantages of LAN	Disadvantages of LAN
• Resource Sharing • Software Applications Sharing. • Easy and Cheap Communication • Centralized Data. • Data Security • Internet Sharing	• High Setup Cost • Privacy Violations • Data Security Threat • LAN Maintenance Job • Covers Limited Area

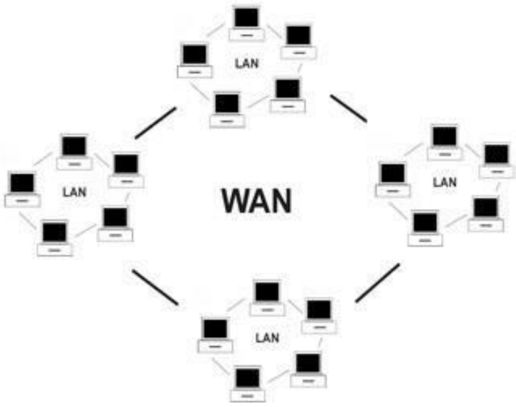
1.3.2 Metropolitan Area Network (MAN)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- It generally covers towns and cities (50 km)
- In MAN, various LANs are connected to each other through a telephone exchange line.
- Communication medium used for MAN are optical fibers, cables etc.
- It has a higher range than Local Area Network(LAN).It is adequate for distributed computing applications.



1.3.3 Wide Area Network (WAN)

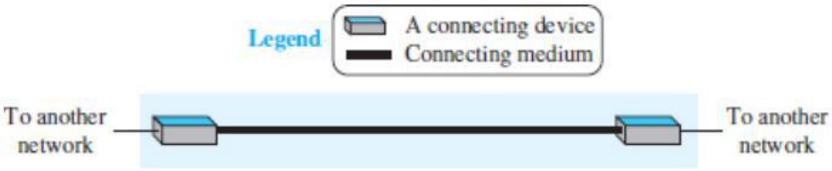
- A Wide Area Network is a network that extends over a large geographical areasuch as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a largegeographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, andeducation.
- WAN can be either a point-to-point WAN or Switched WAN.



Point-to-Point WAN

A point-to-point WAN is a network that connects two communicating devices through a transmission medium (cable or air). Figure 1.9 shows an example of a point-to-point WAN.

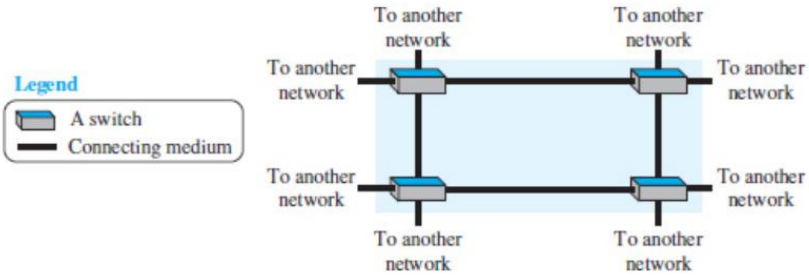
Figure 1.9 *A point-to-point WAN*



Switched WAN

A switched WAN is a network with more than two ends. It is used in the backbone of a global communications network today. Figure 1.10 shows an example of a switched WAN

Figure 1.10 *A switched WAN*



Advantages of Wide Area Network:	**Disadvantages of Wide Area Network:**
○ Large Geographical area ○ Centralized data ○ Exchange messages ○ Sharing of software and resources ○ High bandwidth	○ Security issue ○ Needs Firewall & antivirus software ○ High Setup cost ○ Troubleshooting problems

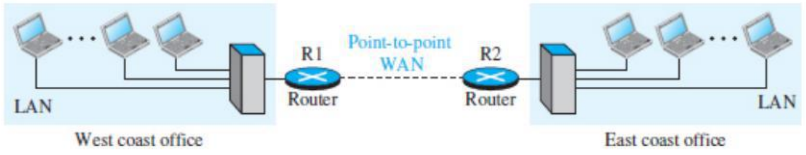
Internetwork

Today, it is very rare to see a LAN or a WAN in isolation; they are connected to one another. When two or more networks are connected, they make an internetwork, or internet. As an example, assume that an organization has two offices, one on the east coast and the other on the west coast.

Each office has a LAN that allows all employees in the office to communicate with each other. To make the communication between employees at different offices possible, the management leases a point-to-point dedicated WAN from a service provider, such as a telephone company, and connects the two LANs.

Now the company has an internetwork, or a private internet (with lowercase i). Communication between offices is now possible. Figure 1.11 shows this internet.

Figure 1.11 *An internetwork made of two LANs and one point-to-point WAN*



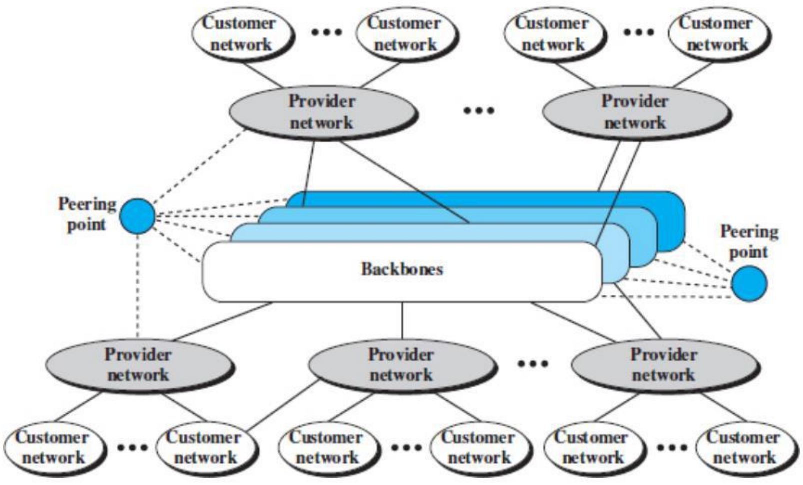
Types of Internetwork

Extranet	***Intranet***
An extranet is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can becategorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must haveone connection to the **external network**.	An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

1.3.4 The Internet

An internet (note the lowercase i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase I) and is composed of thousands of interconnected networks. Figure 1.13 shows a conceptual (not geographical) view of the Internet.

Figure 1.13 *The Internet today*



The figure shows the Internet as several backbones, provider networks, and customer networks. At the top level, the backbones are large networks owned by some communication companies. The backbone networks are connected through some complex switching systems, called peering points.

At the second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee. The provider networks are connected to backbones and sometimes to other provider networks. The customer networks are networks at the edge of the Internet that actually use the services provided by the Internet. They pay fees to provider networks for receiving services.

Backbones and provider networks are also called Internet Service Providers (ISPs). The backbones are often referred to as international ISPs; the provider networks are often referred to as national or regional ISPs.

1.3.5 Accessing the Internet

The Internet today is an internetwork that allows any user to become part of it. The user, however, needs to be physically connected to an ISP. The physical connection is normally done through a point-to-point WAN (such as a telephone network, a cable network, a wireless network, or other types of networks).

Using Telephone Networks

Today most residences and small businesses have telephone service, which means they are connected to a telephone network. Because most telephone networks have already connected themselves to the Internet, one option for residences and small businesses to connect to the Internet is to change the voice line between the residence or business and the telephone center to a point-to-point WAN. This can be done in two ways.

❑ Dial-up service. The first solution is to add a modem that converts data to voice to the telephone line. The software installed on the computer dials the ISP and imitates making a telephone connection. Unfortunately, the dial-up service is very slow, and when the line is used for an Internet connection, it cannot be used for a telephone (voice)connection. It is only useful for small residences and businesses with occasional connection to the Internet.

❑ DSL Service. Since the advent of the Internet, some telephone companies have upgraded their telephone lines to provide higher-speed Internet services to residences or small businesses. The digital subscriber line (DSL) service also allows the line to be used simultaneously for voice and data communications.

Using Cable Networks

More and more residents over the last two decades have begun using cable TV services instead of antennas to receive TV broadcasting. The cable companies have been upgrading their cable networks and connecting to the Internet. A residence or a small business can be connected to the Internet by using this service. It provides a higher-speed connection, but the speed varies depending on the number of neighbors that use the same cable.

Using Wireless Networks

Wireless connectivity has recently become increasingly popular. A household or a small business can use a combination of wireless and wired connections to access the Internet. With the growing wireless WAN access, a household or a small business can be connected to the Internet through a wireless WAN.

Direct Connection to the Internet

A large organization or a large corporation can itself become a local ISP and be connected to the Internet. This can be done if the organization or the corporation leases a high-speed WAN from a carrier provider and connects itself to a regional ISP. For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet.

1.4 PROTOCOL LAYERING

- In networking, a protocol **defines the rules** that both the sender and receiver andall intermediate devices need to follow to be able **to communicate effectively**.
- A protocol provides a communication service that the process use to exchange messages.
- When communication is simple, we may need only one simple protocol.
- When the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or **protocol layering.**
- Protocol layering is that it allows us to separate the services from the implementation.
- A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer.
- Any modification in one layer will not affect the other layers.

Basic Elements of Layered Architecture

- **Service**: It is a set of actions that a layer provides to the higher layer.
- **Protocol**: It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.

- **Interface:** It is a way through which the message is transferred from one layer to another layer.

Features of Protocol Layering

1. It decomposes the problem of building a network into more manageable components.
2. It provides a more modular design.

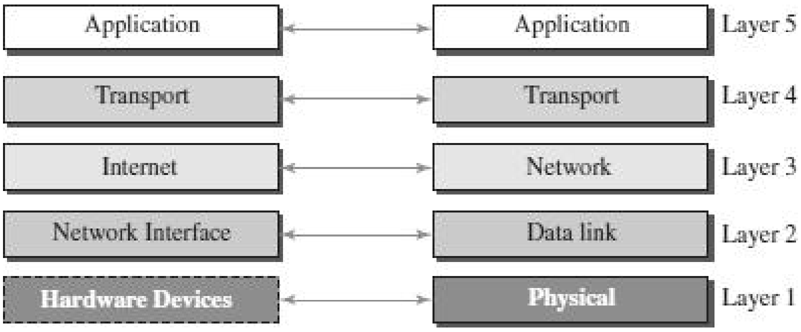
1.4.2 Principles of Protocol Layering

1. The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.
2. The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.

1.5 TCP/IP PROTOCOL SUITE (INTERNET ARCHITECTURE)

The TCP/IP architecture is also called as Internet architecture.
It is developed by the US Defense Advanced Research Project Agency (**DARPA**)for its packet switched network (**ARPANET**).
TCP/IP is a protocol suite used in the Internet today.
It is a 5-layer model. The layers of TCP/IP are

1. Application layer
2. Transport Layer (TCP/UDP)
3. Network Layer
4. Datalink Layer
5. Physical Layer

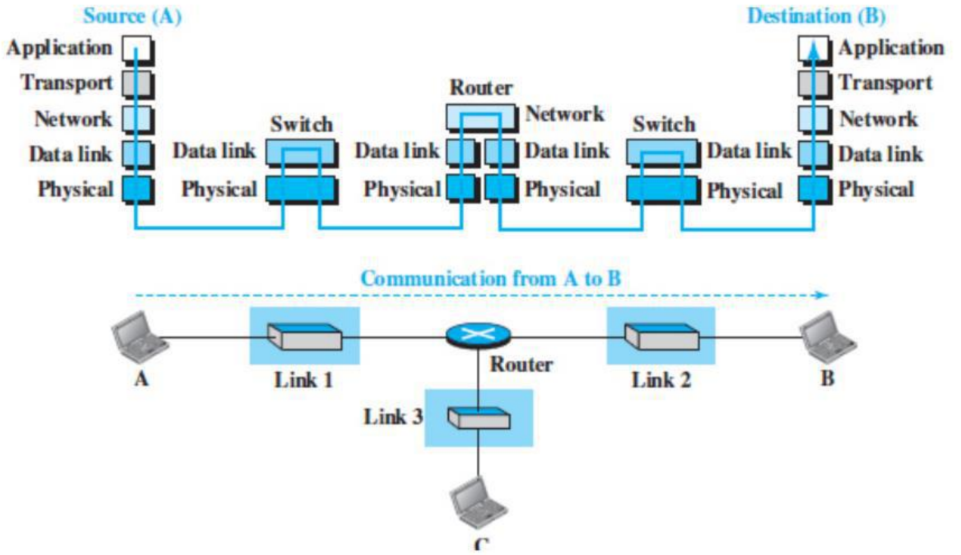


1.5.1 Layered Architecture

To show how the layers in the TCP/IP protocol suite are involved in communication between two hosts, we assume that we want to use the suite in a small internet made up of three LANs (links), each with a link-layer switch. We also assume that the links are connected by one router, as shown in Figure 1.18 (on next page). Let us assume that computer A communicates with computer B.

As Figure 1.18 shows, we have five communicating devices in this communication: source host (computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2, and the destination host (computer B). Each device is involved with a set of layers depending on the role of the device in the internet. The two hosts are involved in all five layers.

Figure 1.18 *Communication through an internet*



1.5.2 Description of Each Layer

After understanding the concept of logical communication, we are ready to briefly discuss the duty of each layer.

Application Layer

- An application layer incorporates the function of top three OSI layers. Anapplication layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- Protocols such as FTP, HTTP, SMTP, POP3, etc running in the application layer provides service to other program running on top of application layer

Transport Layer

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

- The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.
  - **UDP** – UDP provides connectionless service and end-to-end delivery of transmission. It is an unreliable protocol as it discovers the errors but not specify the error.
  - **TCP** – TCP provides a full transport layer services to applications. TCP is a reliable protocol as it detects the error and retransmits the damaged frames.

Network Layer

- The network layer is the third layer of the TCP/IP model.
- The main responsibility of the network layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- Network layer handle the transfer of information across multiple networks through router and gateway .
- IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Data Link Layer

We have seen that an internet is made up of several links (LANs and WANs) connected by routers. When the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link.

Physical Layer

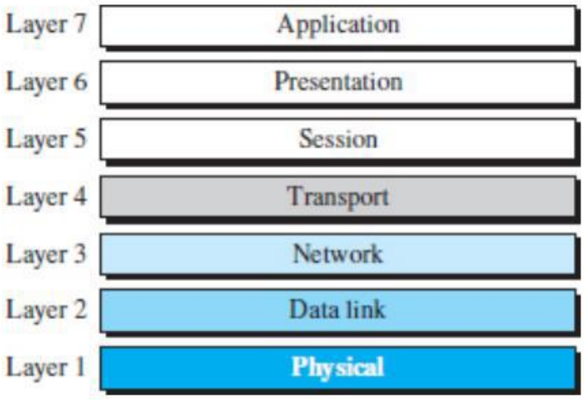
- The physical layer is responsible for carrying individual bits in a frame across the link.
- The physical layer is the lowest level in the TCP/IP protocol suite.
- The communication between two devices at the physical layer is still a logical communication because there is another hidden layer, the transmission media, under the physical layer.

1.6 THE OSI MODEL

An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

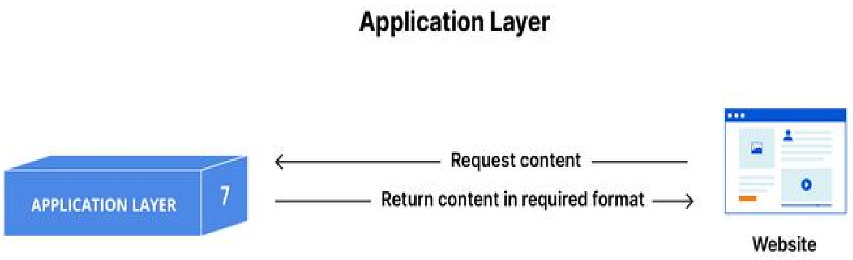
An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network (see Figure 1.21).



1.6.1 Application Layer

This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications. But it should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user. Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).



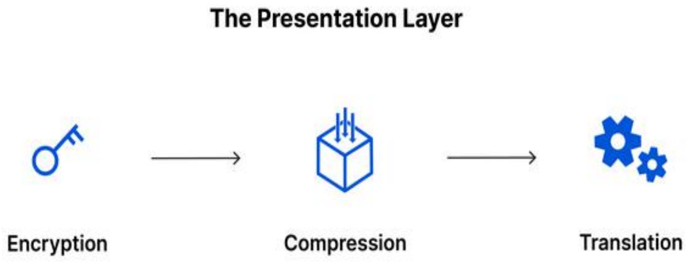
1.6.2 Presentation Layer

This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data.

Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for ***translating*** incoming data into a syntax that the application layer of the receiving device can understand.

If the devices are communicating over an ***encrypted*** connection, layer 6 is responsible for adding the encryption on the sender’s end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.

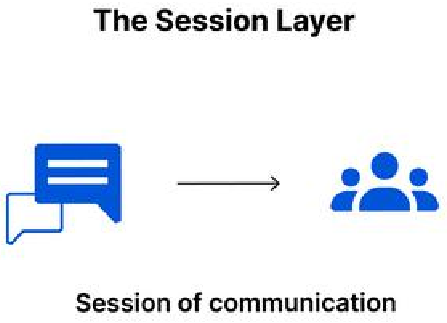
Finally the presentation layer is also responsible for ***compressing*** data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.



1.6.3 Session Layer

This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

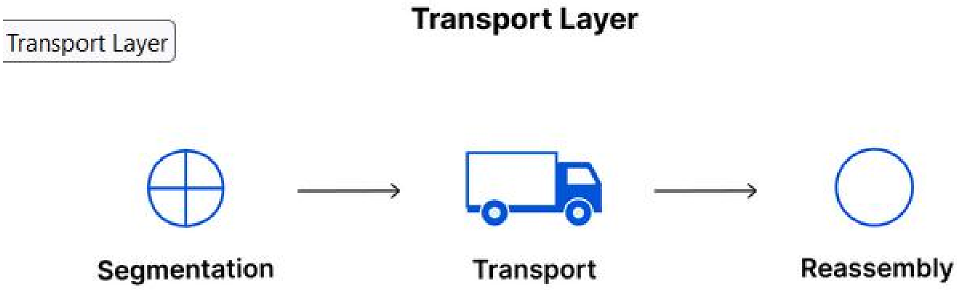
This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.



1.6.4 Transport Layer

Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called ***segments*** before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

The transport layer is also responsible for ***flow control and error control***. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection does not overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn't.



1.6.5 Network Layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of ***packet routing*** i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

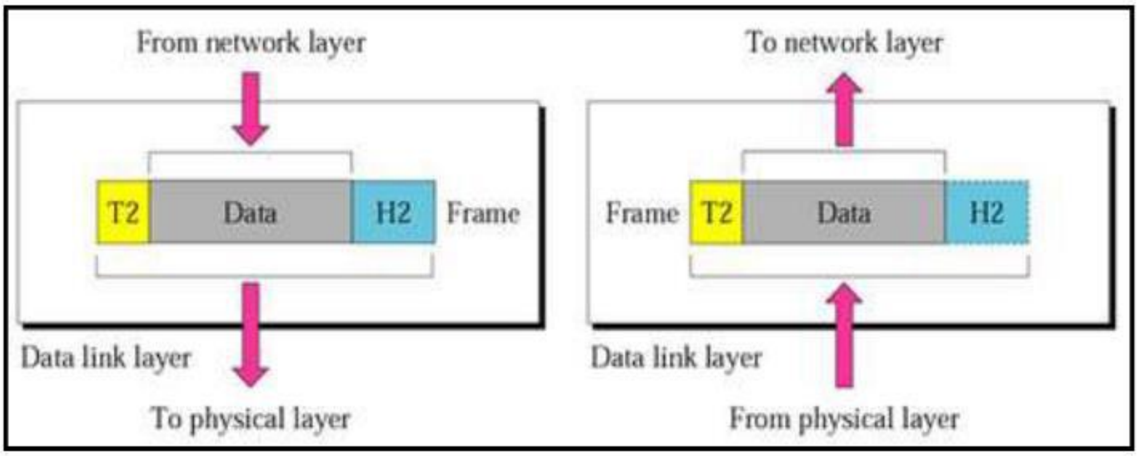
1.6.6 Data Link Layer

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
Data Link Layer is divided into two sublayers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.



1.6.7 Physical Layer

This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

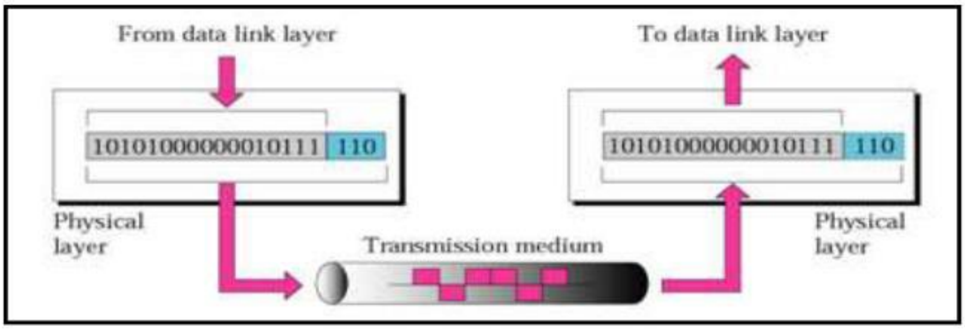
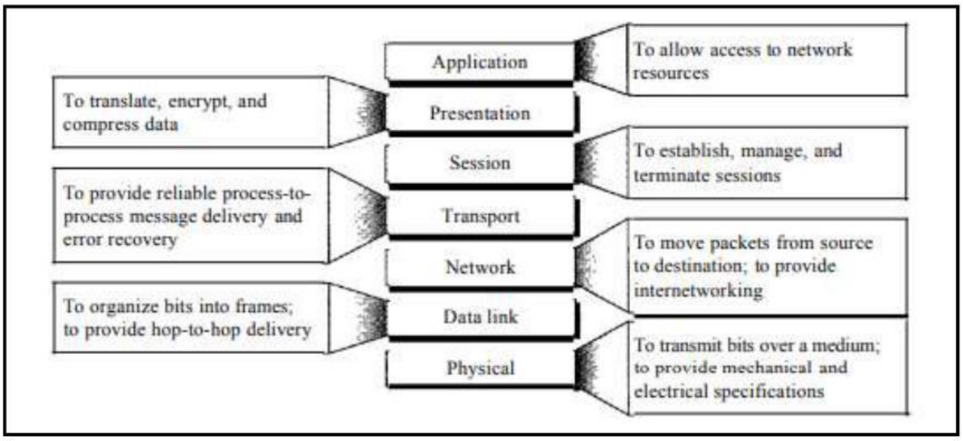
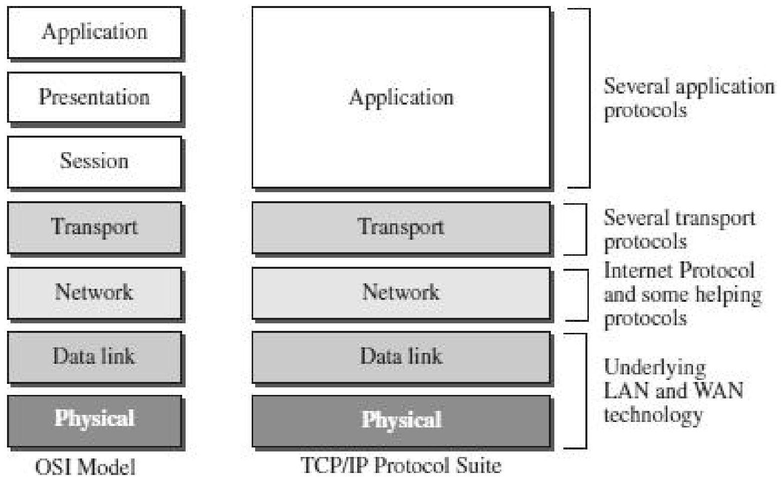


Figure 1.15 *Physical layer*

Summary of Layers


Application
Presentation
Session
Transport
Network
Data link
Physical
To allow access to network resources
To translate, encrypt, and compress data
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
To transmit bits over a medium; to provide mechanical and electrical specifications

COMPARISON - OSI MODEL AND TCP/IP MODEL



S.No	OSI MODEL	TCP/IP MODEL
1	Defined before advent of internet	Defined after the advent of Internet.
2	Service interface and protocols are clearly distinguished before	Service interface and protocols were notclearly distinguished before
3	Internetworking not supported	TCP/IP supports Internet working
4	Strict layering	Loosely layered
5	Protocol independent standard	Protocol Dependant standard
6	Less Credible	More Credible
7	All packets are reliably delivered	TCP reliably delivers packets, IP doesnot reliably deliver packets

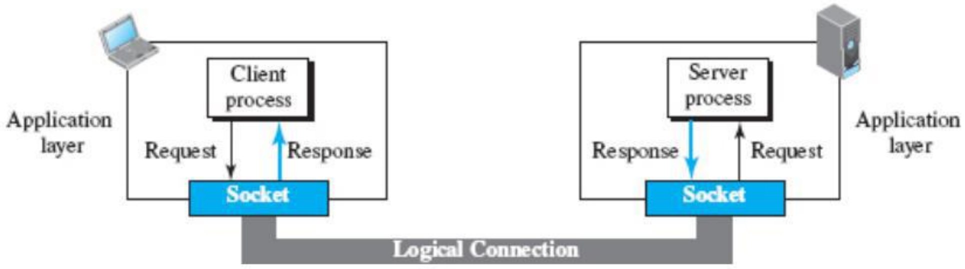
1.7 Introduction to Sockets

A **socket** is one endpoint of a **two way** communication link between two programs running on the network. The socket mechanism provides a means of inter-process communication (IPC) by establishing named contact points between which the communication take place.

Like 'Pipe' is used to create pipes and sockets is created using **'socket'** system call. The socket provides bidirectional **FIFO** Communication facility over the network. A socket connecting to the network is created at each end of the communication. Each socket has a specific address. This address is composed of an IP address and a port number.

Socket are generally employed in client server applications. The server creates a socket, attaches it to a network port addresses then waits for the client to contact it. The client creates a socket and then attempts to connect to the server socket. When the connection is established, transfer of data takes place.

Use of sockets in process-to-process communication



1.7.1 Socket Addresses

The interaction between a client and a server is two-way communication. In a two-way communication, we need a pair of addresses:

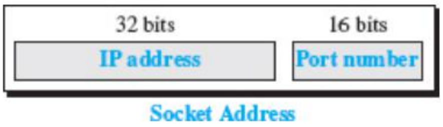
local (sender) and remote (receiver).

The local address in one direction is the remote address in the other direction, and vice versa. Because communication in the client/server paradigm is between two sockets, we need a pair of socket addresses for communication:

a local socket address and a remote socket address.

A socket address should first define the computer on which a client or a server is running. A computer in the Internet is uniquely defined by its IP address, a 32-bit integer in the current Internet version. An application program can be defined by a port number, a 16-bit integer. This means that a socket address should be a combination of an IP address and a port number as shown in Figure 10.7.

Figure 10.7 *A socket address*



Because a socket defines the end-point of the communication, we can say that a socket is identified by a pair of socket addresses, a local and a remote.

1.7.2 Finding Socket Addresses

How can a client or a server find a pair of socket addresses for communication? The situation is different for each site.

Server Site

The server needs a local (server) and a remote (client) socket address for communication.

Local Socket Address The local (server) socket address is provided by the operating system. The operating system knows the IP address of the computer on which the server process is running. The port number of a server process, however, needs to be assigned. If the server process is a standard one defined by the Internet authority, a port number is already assigned to it. When a server starts running, it knows the local socket address.

Remote Socket Address The remote socket address for a server is the socket address of the client that makes the connection. Because the server can serve many clients, it does not know beforehand the remote socket address for communication. The server can find this socket address when a client tries to connect to the server. The client socket address, which is contained in the request packet sent to the server, becomes the remote socket address that is used for responding to the client.

Client Site

The client also needs a local (client) and a remote (server) socket address for communication.

Local Socket Address The local (client) socket address is also provided by the operating system. The operating system knows the IP address of the computer on which the client is running. The port number, however, is a 16- bit temporary integer that is assigned to a client process each time the process needs to start the communication. The port number, however, needs to be assigned from a set of integers defined by the Internet authority and called the ephemeral (temporary) port numbers. The operating system, however, needs to guarantee that the new port number is not used by any other running client process.

Remote Socket Address Finding the remote (server) socket address for a client, however, needs more work. When a client process starts, it should know the socket address of the server it wants to connect to. We will have two situations in this case.

Sometimes, the user who starts the client process knows both the server port number and IP address of the computer on which the server is running. This usually occurs in situations when we have written client and server applications and we want to test them

Although each standard application has a well-known port number, most of the time, we do not know the IP address. This happens in situations such as when we need to contact a web page, send an e-mail to a friend, or copy a file from a remote site. In these situations, the server has a name, an identifier that uniquely defines the server process. Examples of these identifiers are URLs, such as www.xxx.yyy, or e-mail addresses, such as xxxx@yyyy.com. The client process should now change this identifier (name) to the corresponding server socket address.

1.8 Application Layer

- The application layer is the highest layer in the protocol suite.
- The application layer provides services to the user.
- Communication is provided using a logical connection, which means that the two application layers assume that there is an imaginary direct connection through which they can send and receive messages.
- The application layer is the only layer that provides services to the Internet user
- The application layer exchange messages with their peers on other machines
- Applications need their own protocols. These applications are part of network protocol.

Types of Application Protocols:

Standard and Nonstandard Protocols

Standard Application-Layer Protocols

o There are several application-layer protocols that have been standardized and documented by the Internet authority.

o Each standard protocol is a pair of computer programs that interact with the user and the transport layer to provide a specific service to the user.

o Two very widely-used standardized application protocols:

SMTP: Simple Mail Transfer Protocol is used to exchange electronic mail.

HTTP : Hyper Text Transport Protocol is used to communicate between Web browsers and Web servers.

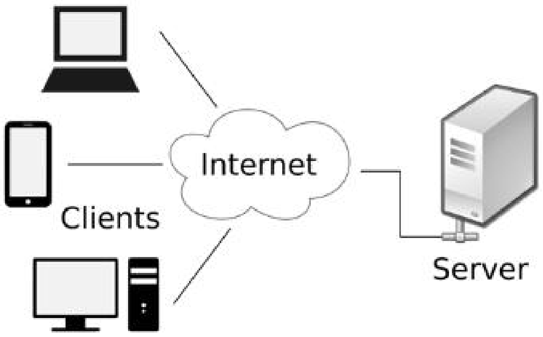
Nonstandard Application-Layer Protocols

o A programmer can create a nonstandard application-layer program if they can write two programs that provide service to the user by interacting with the transport layer.

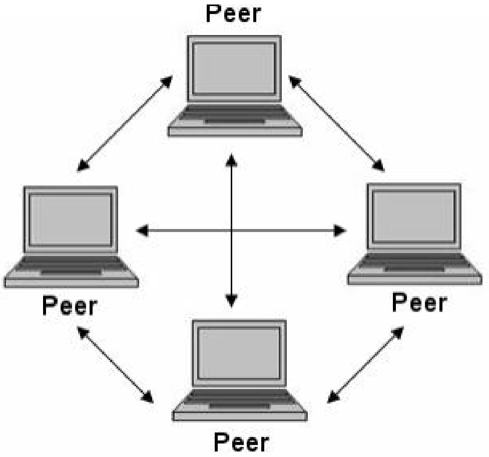
Application-Layer Paradigms

Two paradigms have been developed for Application Layer
1. Traditional Paradigm : Client-Server
2. New Paradigm : Peer-to-Peer

Client-Server Paradigm
o The traditional paradigm is called the client-server paradigm.
o It was the most popular Paradigm.
o In this paradigm, the service provider is an application program, called the server process; it runs continuously, waiting for another application program, called the client process, to make a connection through the Internet and ask for service.
o The server process must be running all the time; the client process is started when the client needs to receive service.
o There are normally some server processes that can provide a specific type of service, but there are many clients that request service from any of these server processes.



Peer-to-Peer(P2P) Paradigm
o A new paradigm, called the peer-to-peer paradigm has emerged to respond to the needs of some new applications.
o In this paradigm, there is no need for a server process to be running all the time and waiting for the client processes to connect.
o The responsibility is shared between peers.
o A computer connected to the Internet can provide service at one time and receive service at another time.
o A computer can even provide and receive services at the same time.



Mixed Paradigm

o An application may choose to use a mixture of the two paradigms by combining the advantages of both.

o For example, a light-load client-server communication can be used to find the address of the peer that can offer a service.

o When the address of the peer is found, the actual service can be received from the peer by using the peer-to-peer paradigm.

1.8.1 The HyperText Transfer Protocol (HTTP)

- The HyperText Transfer Protocol (HTTP) is used to define how the client- server programs can be written to retrieve web pages from the Web.
- It is a protocol used to access the data on the World Wide Web (WWW).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- HTTP is a stateless request/response protocol that governs client/server communication.
- An HTTP client sends a request; an HTTP server returns a response.
- The server uses the port number 80; the client uses a temporary port number.
- HTTP uses the services of TCP , a connection-oriented and reliable protocol.
- HTTP is a text-oriented protocol. It contains embedded URL known as links.
- When hypertext is clicked, browser opens a new connection, retrieves file from the server and displays the file.
- Each HTTP message has the general form

START_LINE <CRLF>
MESSAGE_HEADER <CRLF>
<CRLF> MESSAGE_BODY <CRLF>
where <CRLF> stands for carriage-return-line-feed.

Features of HTTP

o ***Connectionless protocol:***

HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.

o Media independent:

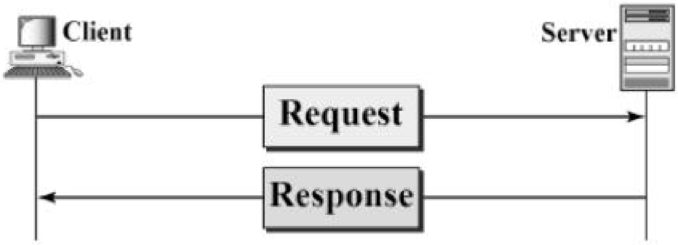
HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.

o Stateless:

HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

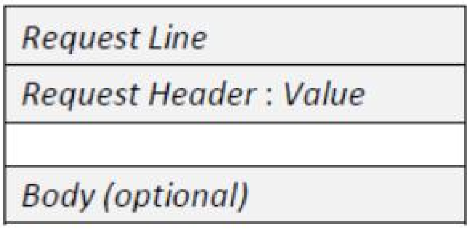
HTTP Request And Response Messages

- The HTTP protocol defines the format of the request and response messages.



- Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.
- Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.

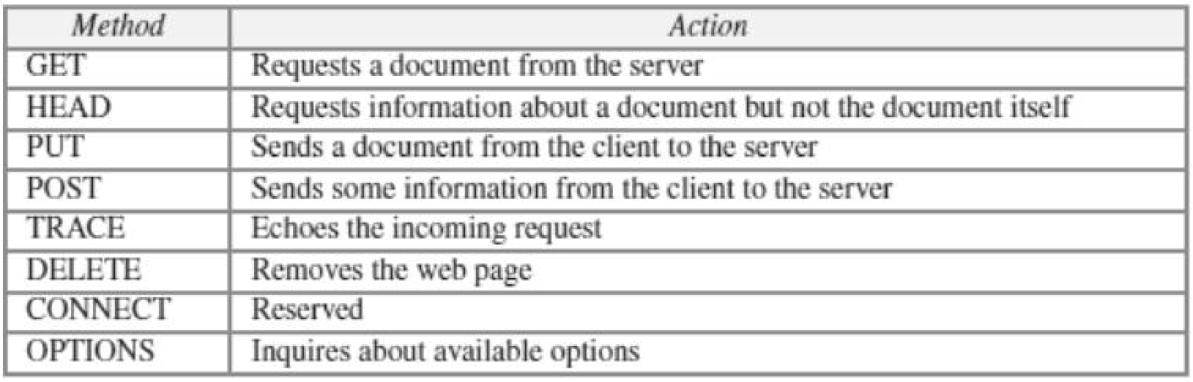
HTTP Request Message



- The first line in a request message is called a request line.
- After the request line, we can have zero or more request header lines.
- The body is an optional one. It contains the comment to be sent or the file to be published on the website when the method is PUT or POST.

Request Line

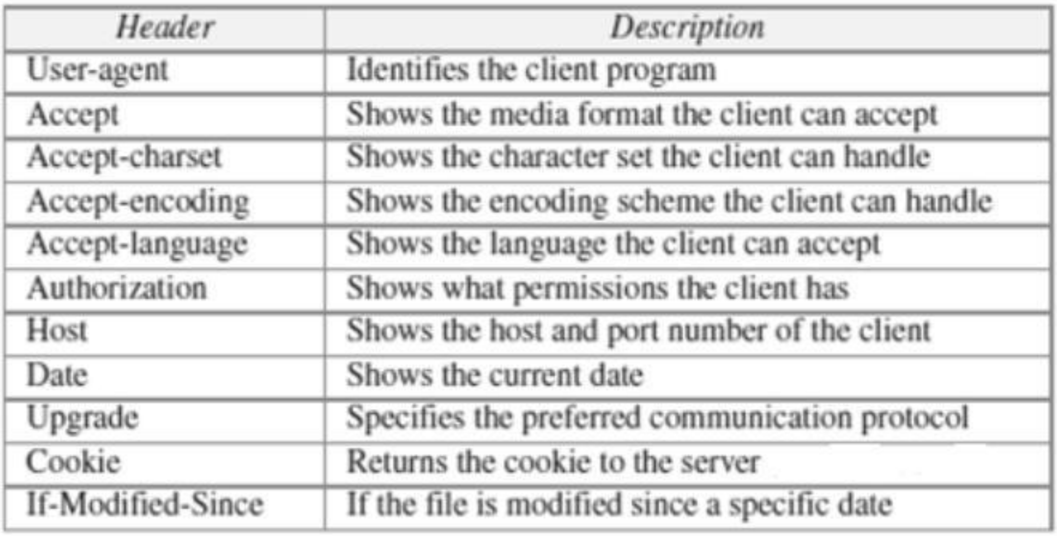
- There are three fields in this request line - Method, URL and Version.
- The Method field defines the request types.
- The URL field defines the address and name of the corresponding web page.
- The Version field gives the version of the protocol; the most current version of HTTP is 1.1.
- Some of the Method types are:



Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
PUT	Sends a document from the client to the server
POST	Sends some information from the client to the server
TRACE	Echoes the incoming request
DELETE	Removes the web page
CONNECT	Reserved
OPTIONS	Inquires about available options

Request Header

- Each request header line sends additional information from the client to the server.
- Each header line has a header name, a colon, a space, and a header value.
- The value field defines the values associated with each header name.
- Headers defined for request message include:



Header	*Description*
User-agent	Identifies the client program
Accept	Shows the media format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-encoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorization	Shows what permissions the client has
Host	Shows the host and port number of the client
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Cookie	Returns the cookie to the server
If-Modified-Since	If the file is modified since a specific date

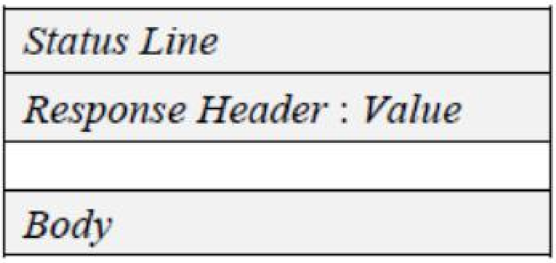
Body

- The body can be present in a request message. It is optional.
- Usually, it contains the comment to be sent or the file to be published on the website when the method is PUT or POST.

Conditional Request

- A client can add a condition in its request.
- In this case, the server will send the requested web page if the condition is met or inform the client otherwise.
- One of the most common conditions imposed by the client is the time and date the web page is modified.
- The client can send the header line If-Modified-Since with the request to tell the server that it needs the page only if it is modified after a certain point in time.

HTTP Response Message



Status Line

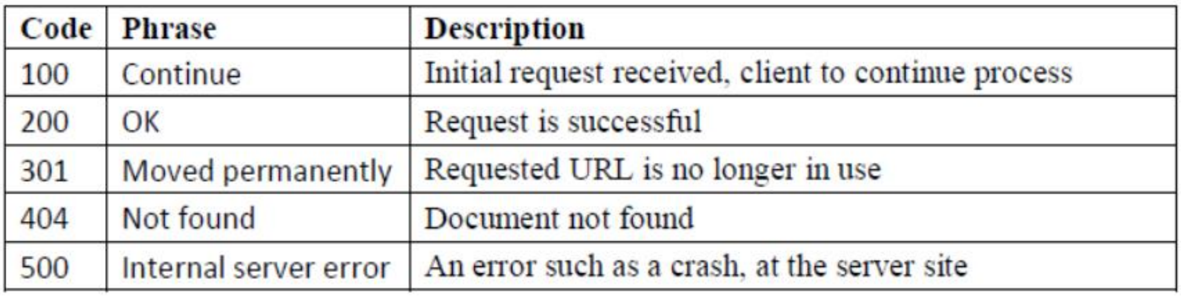
Response Header : Value

Body

- The first line in a request message is called a status line.
- After the request line, we can have zero or more response header lines.
- The body is an optional one. The body is present unless the response is an error message.

Status Line

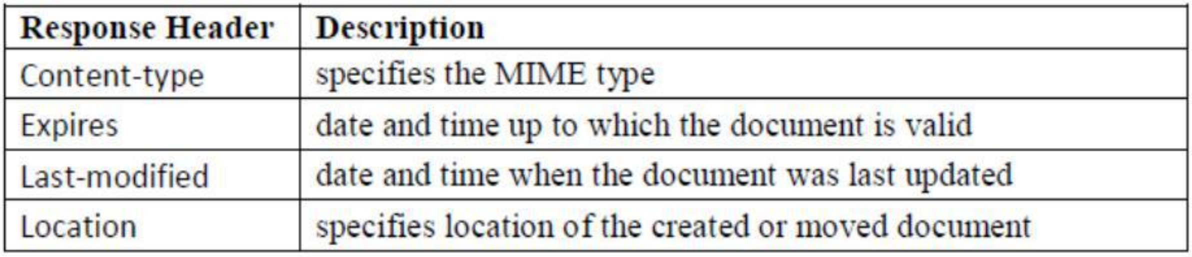
- The Status line contains three fields - HTTP version , Status code, Status phrase
- The first field defines the version of HTTP protocol, currently 1.1.
- The status code field defines the status of the request. It classifies the HTTP result. It consists of three digits.
1xx–Informational, 2xx– Success, 3xx–Redirection,
4xx–Client error, 5xx–Server error
- The Status phrase field gives brief description about status code in text form.
- Some of the Status codes are



Code	Phrase	Description
100	Continue	Initial request received, client to continue process
200	OK	Request is successful
301	Moved permanently	Requested URL is no longer in use
404	Not found	Document not found
500	Internal server error	An error such as a crash, at the server site

Response Header

- Each header provides additional information to the client.
- Each header line has a header name, a colon, a space, and a header value.
- Some of the response headers are:



Response Header	Description
Content-type	specifies the MIME type
Expires	date and time up to which the document is valid
Last-modified	date and time when the document was last updated
Location	specifies location of the created or moved document

Body

- The body contains the document to be sent from the server to the client.
- The body is present unless the response is an error message.

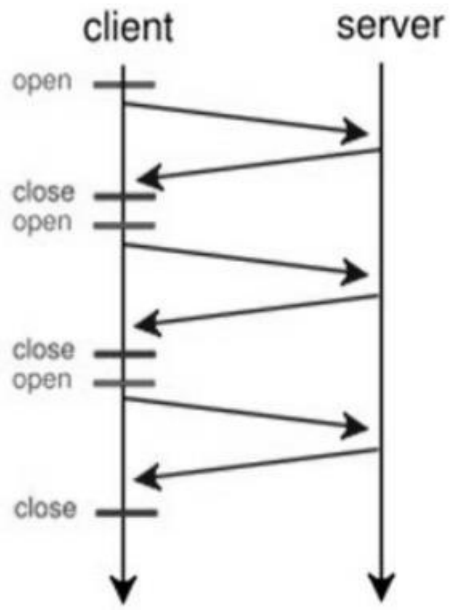
HTTP CONNECTIONS

- HTTP Clients and Servers exchange multiple messages over the same TCP connection.
- If some of the objects are located on the same server, we have two choices: to retrieve each object using a new TCP connection or to make a TCP connection and retrieve them all.
- The first method is referred to as a non-persistent connection, the second as a persistent connection.
- HTTP 1.0 uses non-persistent connections and HTTP 1.1 uses persistent connections .

Non-Persistent Connections

- In a non-persistent connection, one TCP connection is made for each request/response.
- Only one object can be sent over a single TCP connection
- The client opens a TCP connection and sends a request.
- The server sends the response and closes the connection.

- The client reads the data until it encounters an end-of-file marker.
- It then closes the connection.



Persistent Connections

- HTTP version 1.1 specifies a persistent connection by default.
- Multiple objects can be sent over a single TCP connection.
- In a persistent connection, the server leaves the connection open for more requests after sending a response.
- The server can close the connection at the request of a client or if a time-out has been reached.
- Time and resources are saved using persistent connections. Only one set of buffers and variables needs to be set for the connection at each site.
- The round trip time for connection establishment and connection termination is saved.

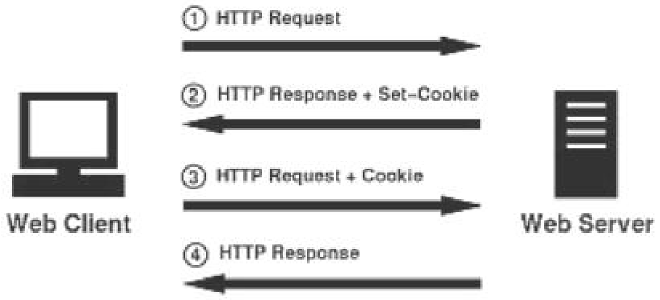
Http Cookies

- An HTTP cookie (also called web cookie, Internet cookie, browser cookie, or simply cookie) is a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing.

- HTTP is stateless , Cookies are used to add State.

- Cookies were designed to be a reliable mechanism for websites to remember stateful information (such as items added in the shopping cart in an online store) or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past).

- They can also be used to remember arbitrary pieces of information that the user previously entered into form fields such as names, addresses, passwords, and credit card numbers.



Components of Cookie

A cookie consists of the following components:

1. Name
2. Value
3. Zero or more attributes (name/value pairs). Attributes store information such as the cookie's expiration, domain, and flags.

Creating and Storing Cookies

The creation and storing of cookies depend on the implementation; however, the principle is the same.

1. When a server receives a request from a client, it stores information about the client in a file or a string. The information may include the domain name of the client, the contents of the cookie (information the server has gathered about the client such as name, registration number, and so on), a timestamp, and other information depending on the implementation.
2. The server includes the cookie in the response that it sends to the client.
3. When the client receives the response, the browser stores the cookie in the cookie directory, which is sorted by the server domain name.

Using Cookies

- When a client sends a request to a server, the browser looks in the cookie directory to see if it can find a cookie sent by that server.
- If found, the cookie is included in the request.
- When the server receives the request, it knows that this is an old client, not a new one.
- The contents of the cookie are never read by the browser or disclosed to the user. It is a cookie made by the server and eaten by the server.

Types of Cookies

1.Authentication cookies

These are the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in with. Without such a mechanism, the site would not know whether to send a page containing sensitive information, or require the user to authenticate themselves by logging in.

2.Tracking cookies

These are commonly used as ways to compile individuals browsing histories.

3.Session cookie

A session cookie exists only in temporary memory while the user navigates the website. Web browsers normally delete session cookies when the user closes the browser.

4.Persistent cookie

Instead of expiring when the web browser is closed as session cookies do, a persistent cookie expires at a specific date or after a specific length of time. This means that, for the cookie's entire lifespan , its information will be transmitted to the server every time the user visits the website that it belongs to, or every time the user views a resource belonging to that website from another website

Http Caching

¬ HTTP Caching enables the client to retrieve document faster and reduces load on the server.

¬ HTTP Caching is implemented at Proxy server, ISP router and Browser.

¬ Server sets expiration date (Expires header) for each page, beyond which it is not cached.

¬ HTTP Cache document is returned to client only if it is an updated copy by checking against If-Modified-Since header.

¬ If cache document is out-of-date, then request is forwarded to the server and response is cached along the way.

¬ A web page will not be cached if no-cache directive is specified.

HTTP SECURITY

¬ HTTP does not provide security.

¬ However HTTP can be run over the Secure Socket Layer (SSL).

¬ In this case, HTTP is referred to as HTTPS.

¬ HTTPS provides confidentiality, client and server authentication, and data integrity.

1.8.2 FTP (FILE TRANSFER PROTOCOL)

¬ FTP stands for File transfer protocol.

¬ FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

¬ It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.

¬ It is also used for downloading the files to computer from other servers.

¬ Although we can transfer files using HTTP, FTP is a better choice to transfer large files or to transfer files using different formats.

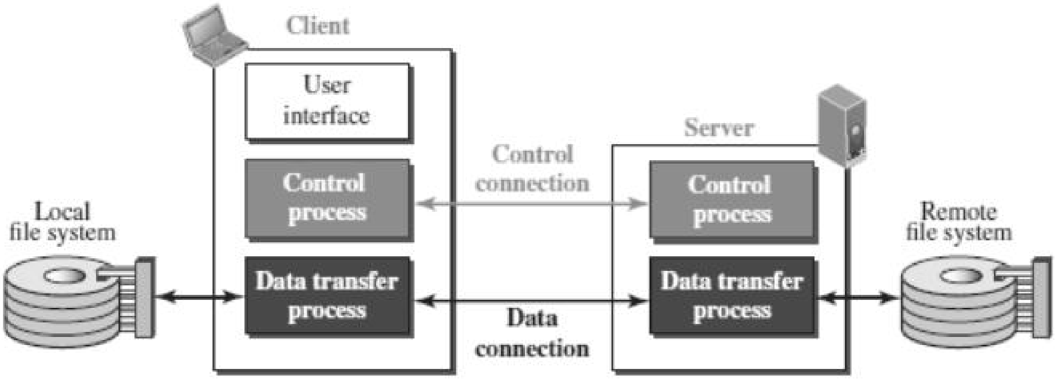
FTP OBJECTIVES

¬ It provides the sharing of files.

¬ It is used to encourage the use of remote computers.

¬ It transfers the data more reliably and efficiently.

FTP MECHANISM



¬ The above figure shows the basic model of the FTP.
¬ The FTP client has three components:
o user interface, control process, and data transfer process.
¬ The server has two components:
o server control process and server data transfer process.

FTP CONNECTIONS

¬ There are two types of connections in FTP - Control Connection and Data Connection.

¬ The two connections in FTP have different lifetimes.

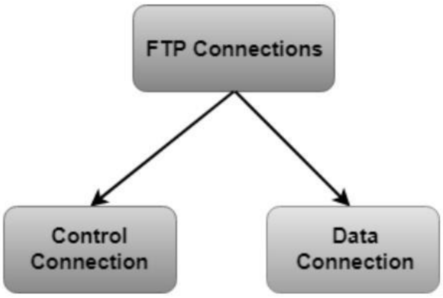
¬ The control connection remains connected during the entire interactive FTP session.

¬ The data connection is opened and then closed for each file transfer activity. When a user starts an FTP session, the control connection opens.

¬ While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.

¬ FTP uses two well-known TCP ports:

o Port 21 is used for the control connection
o Port 20 is used for the data connection.



Control Connection:

o The control connection uses very simple rules for communication.

o Through control connection, we can transfer a line of command or line of response at a time.

o The control connection is made between the control processes.

o The control connection remains connected during the entire interactive FTP session.

¬ Data Connection:

o The Data Connection uses very complex rules as data types may vary.

o The data connection is made between data transfer processes.

o The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP COMMUNICATION

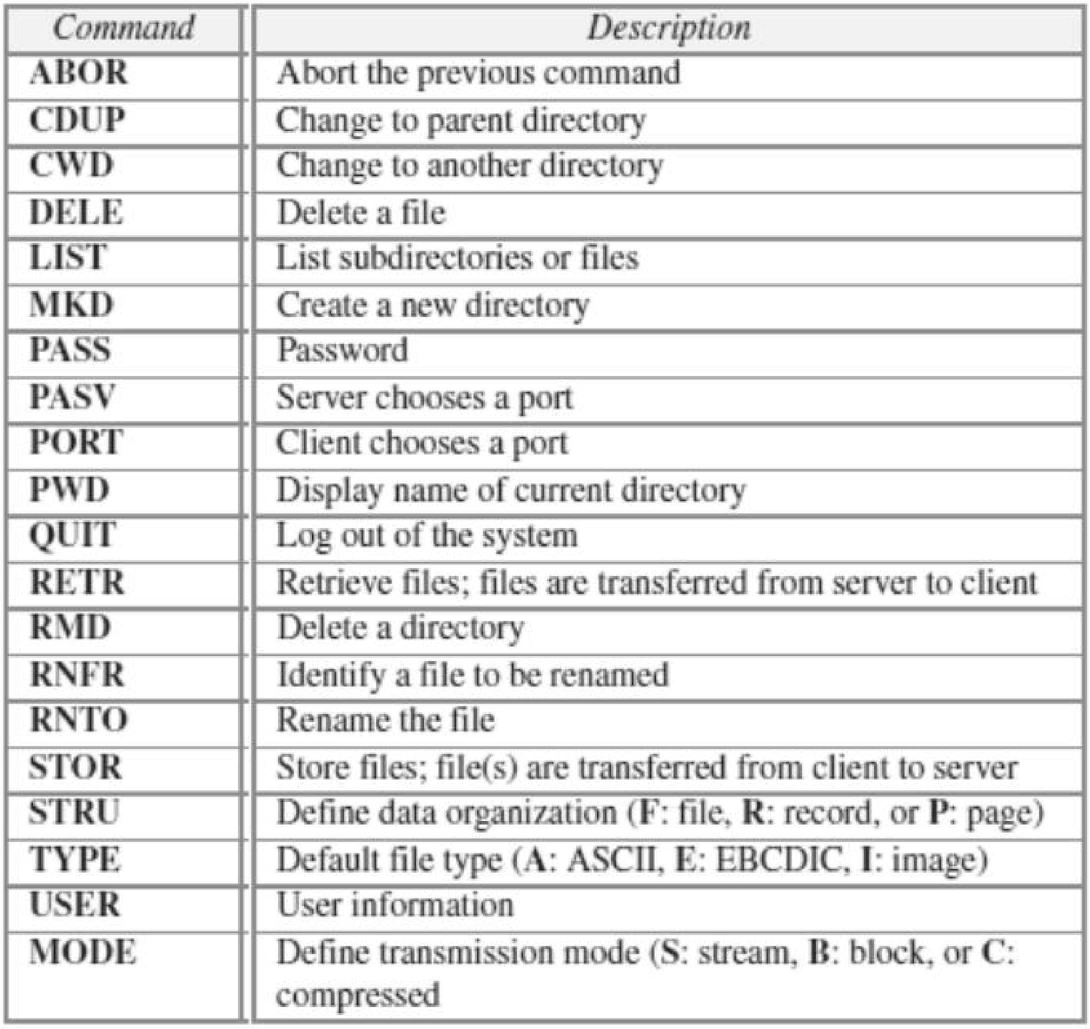
¬ FTP Communication is achieved through commands and responses.

¬ FTP Commands are sent from the client to the server

¬ FTP responses are sent from the server to the client.

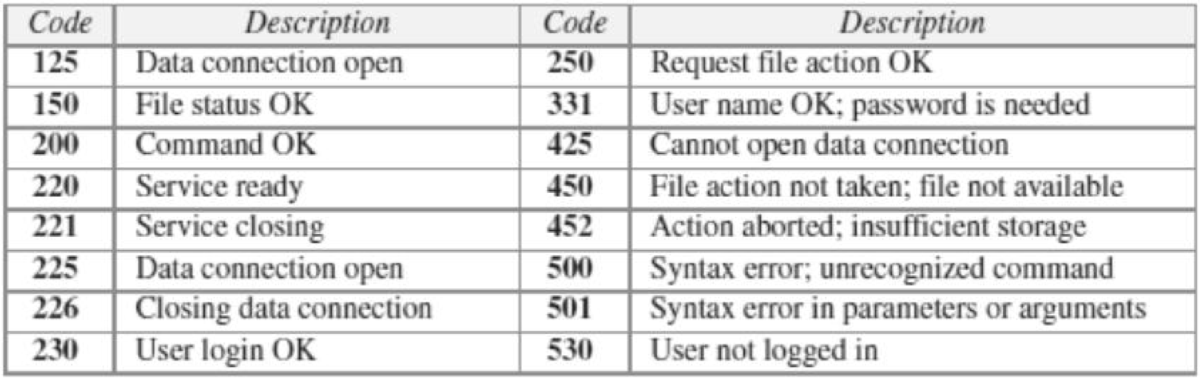
¬ FTP Commands are in the form of ASCII uppercase, which may or may not be followed by an argument.

¬ Some of the most common commands are:



Command	*Description*
ABOR	Abort the previous command
CDUP	Change to parent directory
CWD	Change to another directory
DELE	Delete a file
LIST	List subdirectories or files
MKD	Create a new directory
PASS	Password
PASV	Server chooses a port
PORT	Client chooses a port
PWD	Display name of current directory
QUIT	Log out of the system
RETR	Retrieve files; files are transferred from server to client
RMD	Delete a directory
RNFR	Identify a file to be renamed
RNTO	Rename the file
STOR	Store files; file(s) are transferred from client to server
STRU	Define data organization (**F**: file, **R**: record, or **P**: page)
TYPE	Default file type (**A**: ASCII, **E**: EBCDIC, **I**: image)
USER	User information
MODE	Define transmission mode (**S**: stream, **B**: block, or **C**: compressed

Every FTP command generates at least one response.
¬ A response has two parts: a three-digit number followed by text.
¬ The numeric part defines the code; the text part defines needed parameter.



Code	Description	Code	Description
125	Data connection open	250	Request file action OK
150	File status OK	331	User name OK; password is needed
200	Command OK	425	Cannot open data connection
220	Service ready	450	File action not taken; file not available
221	Service closing	452	Action aborted; insufficient storage
225	Data connection open	500	Syntax error; unrecognized command
226	Closing data connection	501	Syntax error in parameters or arguments
230	User login OK	530	User not logged in

FTP FILE TYPE

¬ FTP can transfer one of the following file types across the data connection:
ASCII file, EBCDIC file, or image file

FTP DATA STRUCTURE

¬ FTP can transfer a file across the data connection using one of the following data structure : file structure, record structure, or page structure.
¬ The file structure format is the default one and has no structure. It is a continuous stream of bytes.
¬ In the record structure, the file is divided into records. This can be used only with text files.
¬ In the page structure, the file is divided into pages, with each page having a page number and a page header. The pages can be stored and accessed randomly or sequentially.

FTP TRANSMISSION MODE

¬ FTP can transfer a file across the data connection using one of the following three transmission modes: stream mode, block mode, or compressed mode.
¬ The stream mode is the default mode; data are delivered from FTP to TCP as a continuous stream of bytes.
¬ In the block mode, data can be delivered from FTP to TCP in blocks.
¬ In the compressed mode, data can be compressed and delivered from FTP to TCP.

FTP FILE TRANSFER

¬ File transfer occurs over the data connection under the control of the commands sent over the control connection.
¬ File transfer in FTP means one of three things:
o retrieving a file (server to client)
o storing a file (client to server)
o directory listing (server to client).

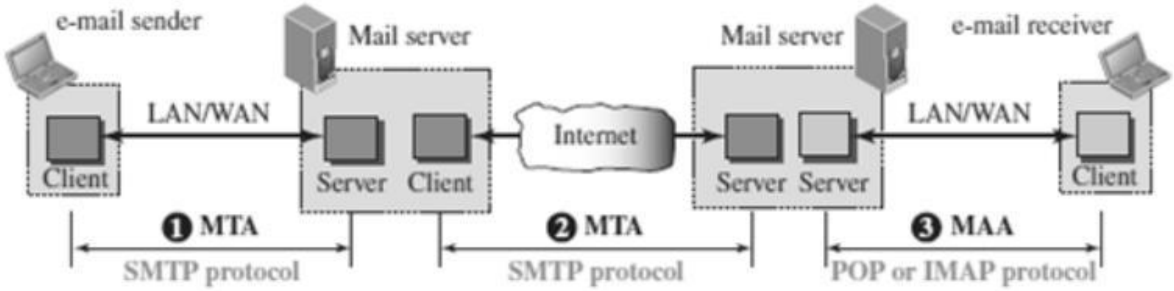
FTP SECURITY

¬ FTP requires a password, the password is sent in plaintext which is unencrypted. This means it can be intercepted and used by an attacker.
¬ The data transfer connection also transfers data in plaintext, which is insecure.

¬ To be secure, one can add a Secure Socket Layer between the FTP application layer and the TCP layer.
¬ In this case FTP is called SSL-FTP.

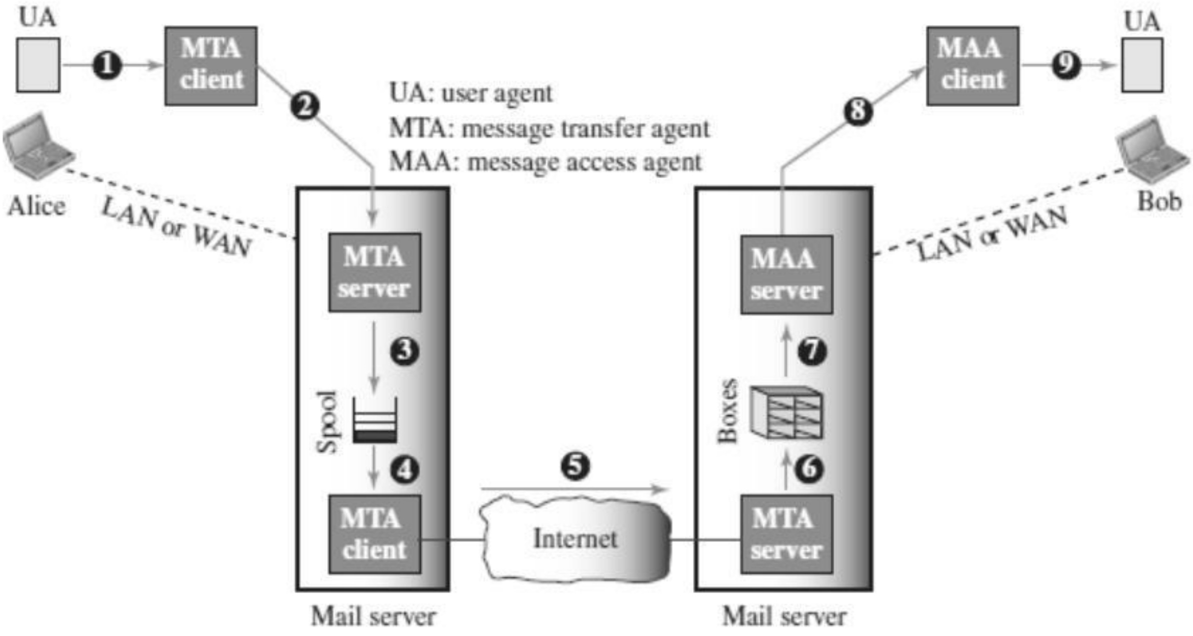
1.8.3 EMAIL (SMTP, MIME, IMAP, POP)

¬ One of the most popular Internet services is electronic mail (E-mail).
¬ Email is one of the oldest network applications.
¬ The three main components of an Email are
1. User Agent (UA)
2. Messsage Transfer Agent (MTA) – SMTP
3. Messsage Access Agent (MAA) - IMAP , POP



¬ When the sender and the receiver of an e-mail are on the same system, we need only two User Agents and no Message Transfer Agent
¬ When the sender and the receiver of an e-mail are on different system, we need two UA, two pairs of MTA (client and server), and two MAA (client and server).

WORKING OF EMAIL



¬ When Alice needs to send a message to Bob, she runs a UA program to prepare the message and send it to her mail server.

¬ The mail server at her site uses a queue (spool) to store messages waiting to be sent. The message, however, needs to be sent through the Internet from Alice's site to Bob's site using an MTA.

¬ Here two message transfer agents are needed: one client and one server.

¬ The server needs to run all the time because it does not know when a client will ask for a connection.

¬ The client can be triggered by the system when there is a message in the queue to be sent.

¬ The user agent at the Bob site allows Bob to read the received message.

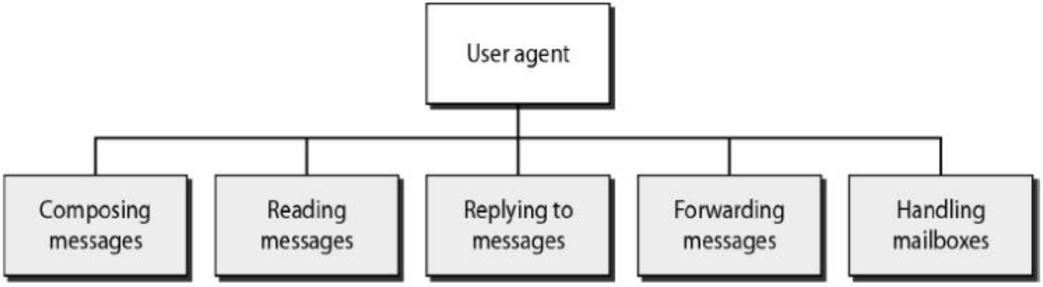
¬ Bob later uses an MAA client to retrieve the message from an MAA server running on the second server.

USER AGENT (UA)

¬ The first component of an electronic mail system is the user agent (UA).

¬ It provides service to the user to make the process of sending and receiving a message easier.

¬ A user agent is a software package that composes, reads, replies to, and forwards messages. It also handles local mailboxes on the user computers.



¬ There are two types of user agents: Command-driven and GUI-based.

Command driven

o Command driven user agents belong to the early days of electronic mail.

o A command-driven user agent normally accepts a one character command from the keyboard to perform its task.

o Some examples of command driven user agents are mail, pine, and elm.

GUI-based

o Modern user agents are GUI-based.

o They allow the user to interact with the software by using both the keyboard and the mouse.

o They have graphical components such as icons, menu bars, and windows that make the services easy to access.

o Some examples of GUI-based user agents are Eudora and Outlook.

MESSAGE TRANSFER AGENT (MTA)

¬ The actual mail transfer is done through message transfer agents (MTA).

¬ To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.

¬ The formal protocol that defines the MTA client and server in the Internet is called Simple Mail Transfer Protocol (SMTP).

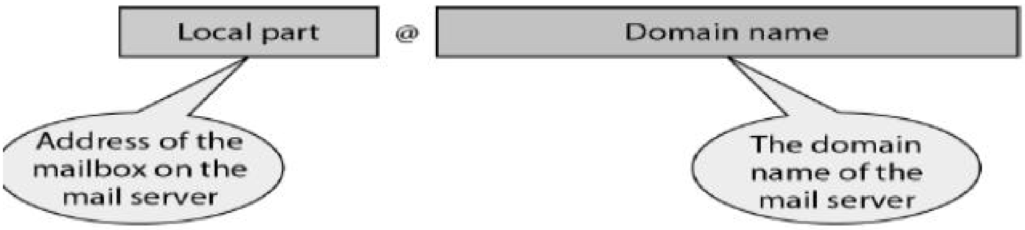
MESSAGE ACCESS AGENT (MAA)

¬ MAA is a software that pulls messages out of a mailbox.

¬ POP3 and IMAP4 are examples of MAA.

ADDRESS FORMAT OF EMAIL

¬ E-mail address is userid @ domain where domain is hostname of the mail server.


Local part
@
Domain name
Address of the mailbox on the mail server
The domain name of the mail server

MESSAGE FORMAT OF EMAIL

¬ Email message consists of two parts namely header and body.

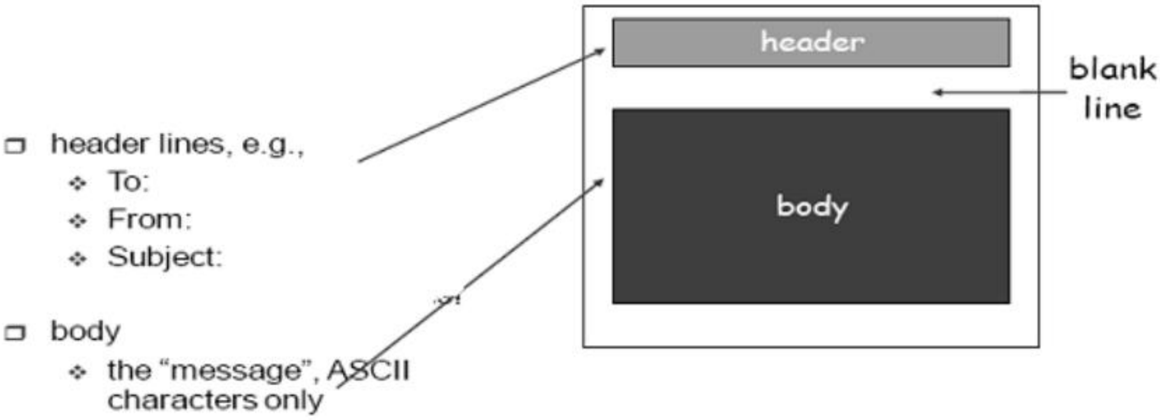
¬ Each header line contains type and value separated by a colon (:).

¬ Some header contents are:

o From: identifier sender of the message.
o To: mail address of the recipient(s).
o Subject: says about purpose of the message.
o Date: timestamp of when the message was transmitted.

¬ Header is separated from the body by a blank line.

¬ Body contains the actual message.



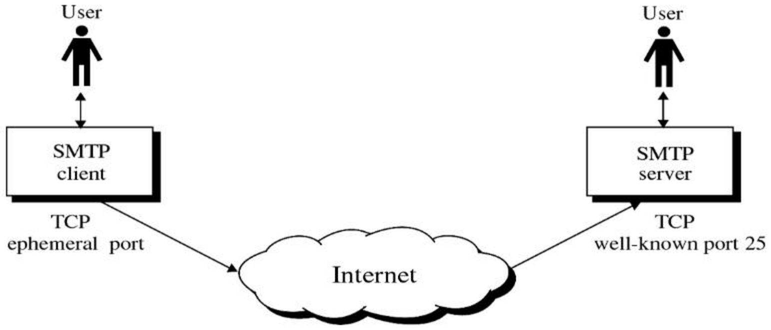
¬ Email was extended in 1993 to carry many different types of data: audio, video, images, Word documents, and so on.

¬ This extended version is known as MIME(Multipurpose Mail Extension).

1.8.4.1 SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

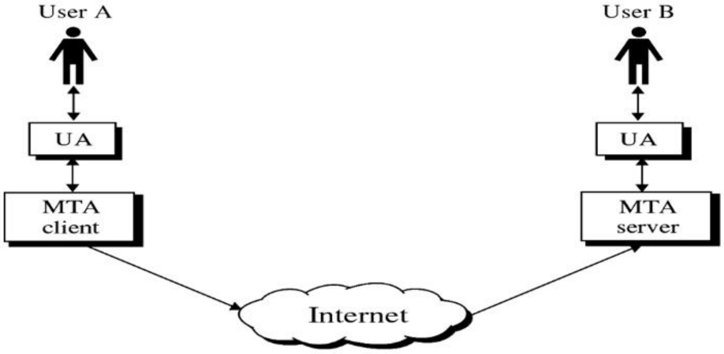
¬ SMTP is the standard protocol for transferring mail between hosts in the TCP/IP protocol suite.

¬ SMTP is not concerned with the format or content of messages themselves.
¬ SMTP uses information written on the envelope of the mail (message header), but does not look at the contents (message body) of the envelope.

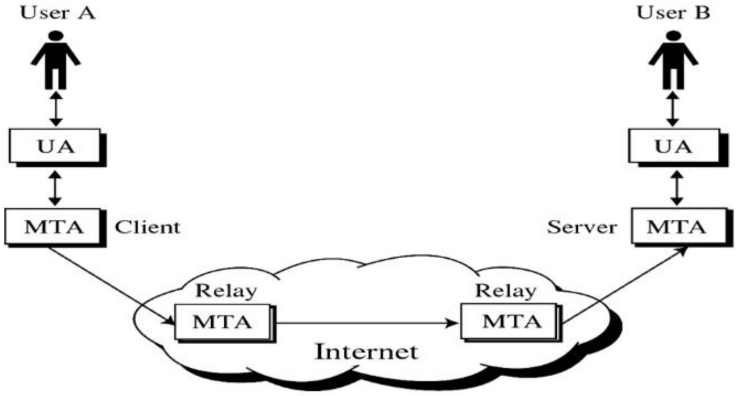


¬ SMTP clients and servers have two main components

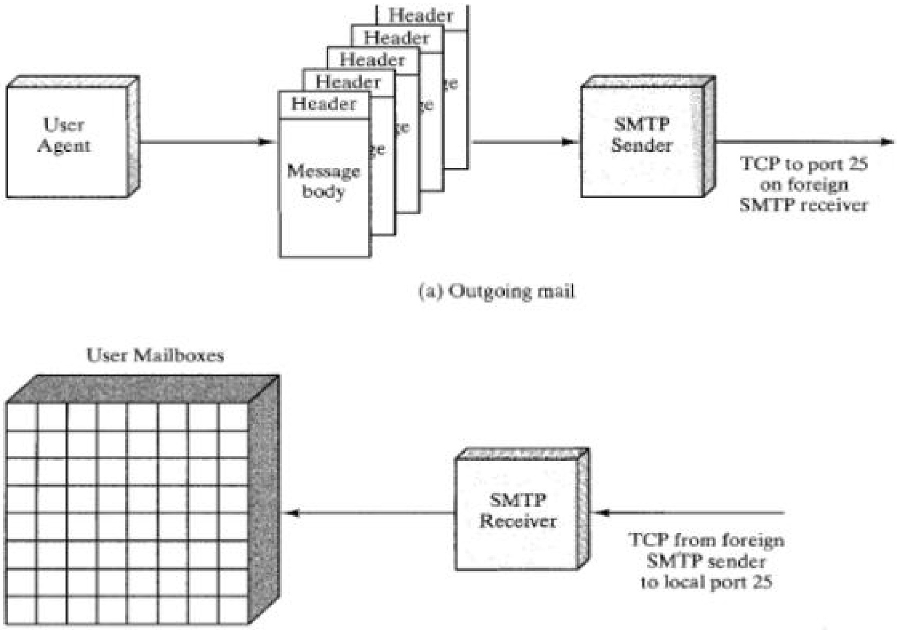
o User Agents(UA) – Prepares the message, encloses it in an envelope.
o Mail Transfer Agent (MTA) – Transfers the mail across the internet



¬ SMTP also allows the use of Relays allowing other MTAs to relay the mail.



SMTP MAIL FLOW



(a) Outgoing mail

¬ To begin, mail is created by a user-agent program in response to user input.
¬ Each created message consists of a header that includes the recipient's email address and other information, and a message body containing the message to be sent.
¬ These messages are then queued in some fashion and provided as input to an SMTP Sender program.

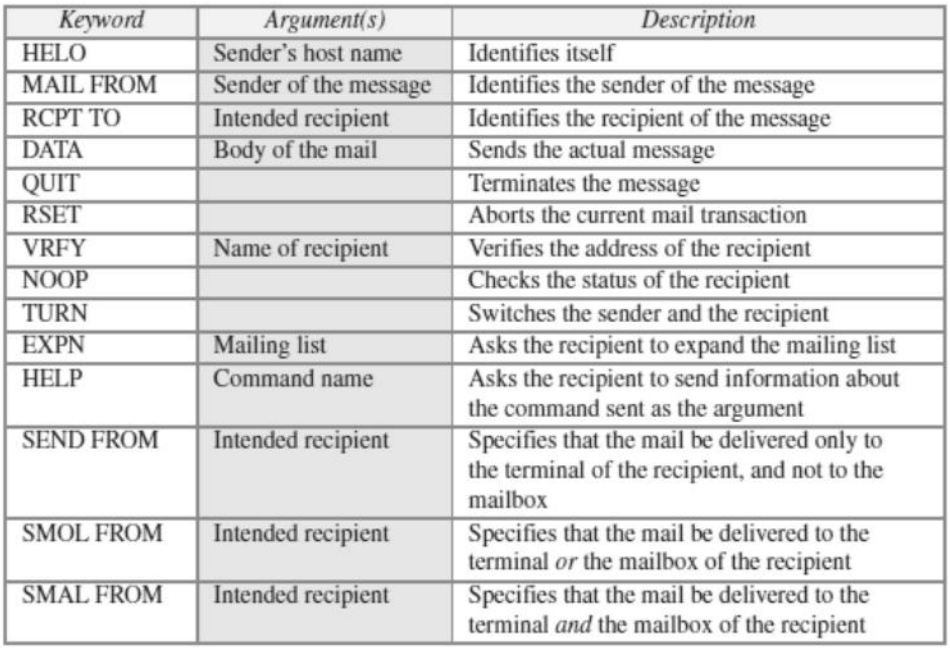
SMTP COMMANDS AND RESPONSES

¬ The operation of SMTP consists of a series of commands and responses exchanged between the SMTP sender and SMTP receiver.
¬ The initiative is with the SMTP sender, who establishes the TCP connection.
¬ Once the connection is established, the SMTP sender sends commands over the connection to the receiver.
¬ The command is from an MTA client to an MTA server; the response is from an MTA server to the MTA client.

SMTP Commands

¬ Commands are sent from the client to the server. It consists of a keyword followed by zero or more arguments. SMTP defines 14 commands.

SMTP commands



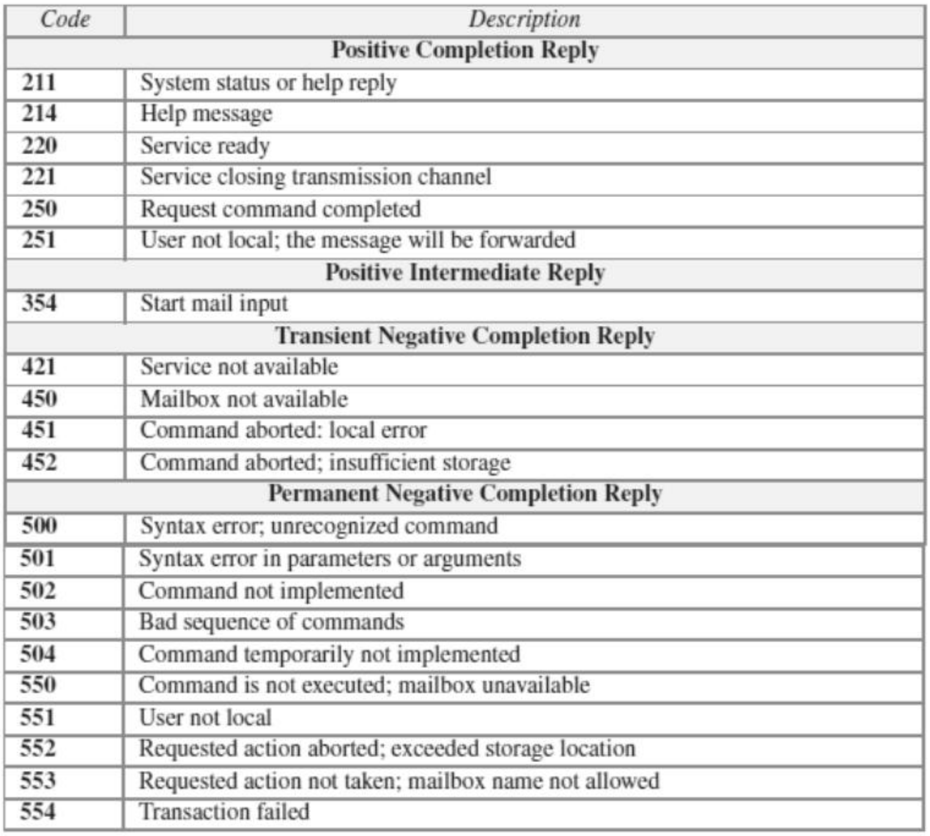
Keyword	*Argument(s)*	*Description*
HELO	Sender's host name	Identifies itself
MAIL FROM	Sender of the message	Identifies the sender of the message
RCPT TO	Intended recipient	Identifies the recipient of the message
DATA	Body of the mail	Sends the actual message
QUIT		Terminates the message
RSET		Aborts the current mail transaction
VRFY	Name of recipient	Verifies the address of the recipient
NOOP		Checks the status of the recipient
TURN		Switches the sender and the recipient
EXPN	Mailing list	Asks the recipient to expand the mailing list
HELP	Command name	Asks the recipient to send information about the command sent as the argument
SEND FROM	Intended recipient	Specifies that the mail be delivered only to the terminal of the recipient, and not to the mailbox
SMOL FROM	Intended recipient	Specifies that the mail be delivered to the terminal *or* the mailbox of the recipient
SMAL FROM	Intended recipient	Specifies that the mail be delivered to the terminal *and* the mailbox of the recipient

SMTP Responses

¬ Responses are sent from the server to the client.

¬ A response is a three digit code that may be followed by additional textual information.

SMTP Responses



Code	*Description*
	Positive Completion Reply
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
	Positive Intermediate Reply
354	Start mail input
	Transient Negative Completion Reply
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted; insufficient storage
	Permanent Negative Completion Reply
500	Syntax error; unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mailbox unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

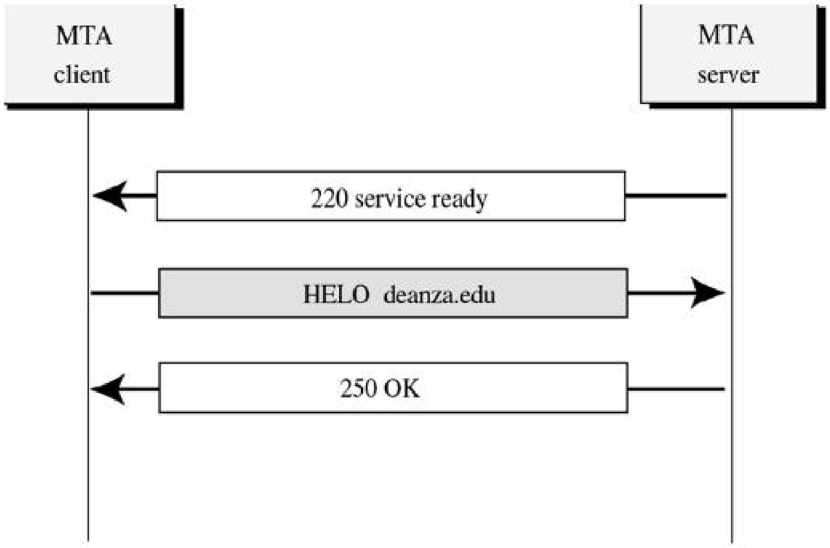
SMTP OPERATIONS

Basic SMTP operation occurs in three phases:
1. Connection Setup
2. Mail Transfer
3. Connection Termination

Connection Setup

¬ An SMTP sender will attempt to set up a TCP connection with a target host when it has one or more mail messages to deliver to that host.

¬ The sequence is quite simple:
1. The sender opens a TCP connection with the receiver.
2. Once the connection is established, the receiver identifies itself with "Service Ready”.
3. The sender identifies itself with the HELO command.
4. The receiver accepts the sender's identification with "OK".
5. If the mail service on the destination is unavailable, the destination host returns a "Service Not Available" reply in step 2, and the process is terminated.



Mail Transfer

¬ Once a connection has been established, the SMTP sender may send one or more messages to the SMTP receiver.

¬ There are three logical phases to the transfer of a message:
1. A MAIL command identifies the originator of the message.
2. One or more RCPT commands identify the recipients for this message.
3. A DATA command transfers the message text.

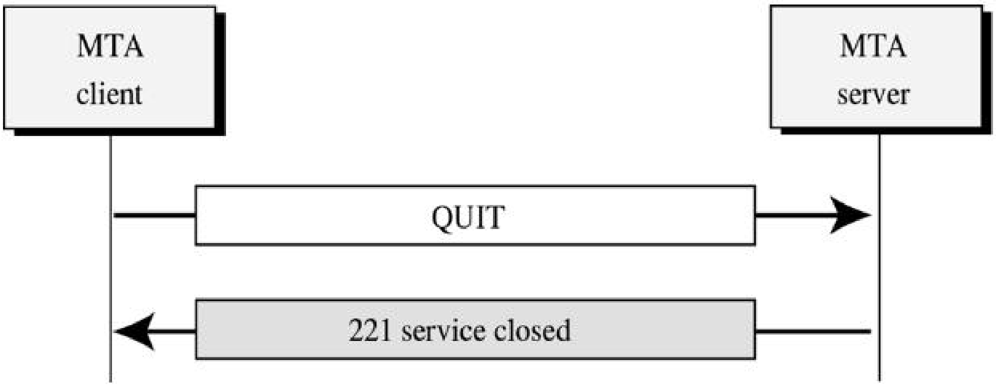
Connection Termination

¬ The SMTP sender closes the connection in two steps.

¬ First, the sender sends a QUIT command and waits for a reply.

¬ The second step is to initiate a TCP close operation for the TCP connection.

¬ The receiver initiates its TCP close after sending its reply to the QUIT command.



Limitations Of Smtp

¬ SMTP cannot transmit executable files or other binary objects.

¬ SMTP cannot transmit text data that includes national language characters, as these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to 7-bit ASCII.

¬ SMTP servers may reject mail message over a certain size.

¬ SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.

¬ Some SMTP implementations do not adhere completely to the SMTP standards defined.

¬ Common problems include the following:

1. Deletion, addition, or recording of carriage return and linefeed.
2. Truncating or wrapping lines longer than 76 characters.
3. Removal of trailing white space (tab and space characters).
4. Padding of lines in a message to the same length.
5. Conversion of tab characters into multiple-space characters.

1.8.4.2 MULTIPURPOSE INTERNET MAIL EXTENSION (MIME)

¬ SMTP provides a basic email service, while MIME adds multimedia capability to SMTP.

¬ MIME is an extension to SMTP and is used to overcome the problems and limitations of SMTP.

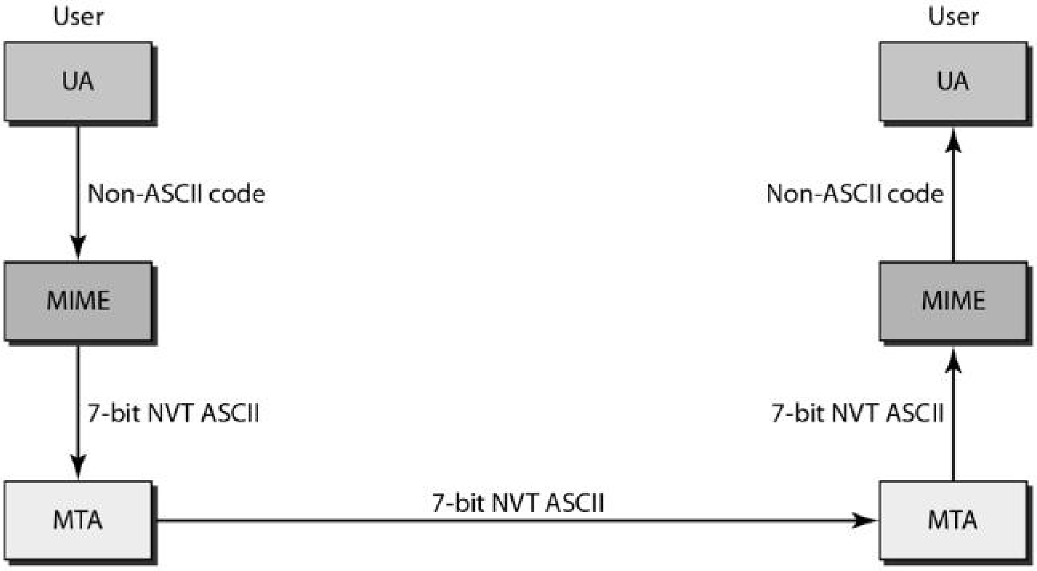
¬ Email system was designed to send messages only in ASCII format.

- Languages such as French, Chinese, etc., are not supported.
- Image, audio and video files cannot be sent.

¬ MIME adds the following features to email service:

- Be able to send multiple attachments with a single message;
- Unlimited message length;
- Use of character sets other than ASCII code;
- Use of rich text (layouts, fonts, colors, etc)
- Binary attachments (executables, images, audio or video files, etc.), which may be divided if needed.

¬ MIME is a protocol that converts non-ASCII data to 7-bit NVT(Network Virtual Terminal) ASCII and vice-versa.

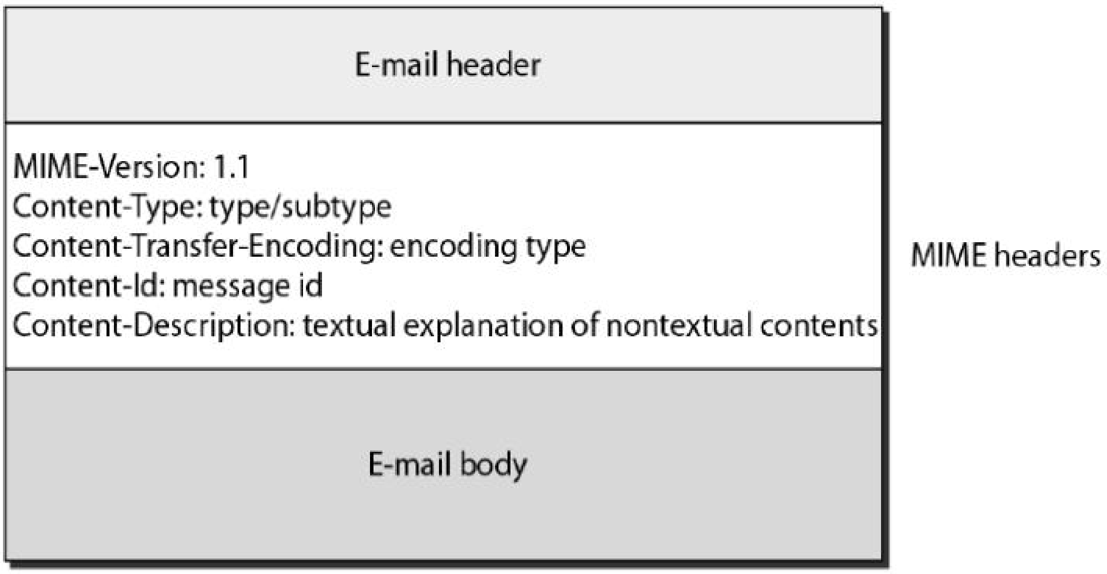


MIME HEADERS

¬ Using headers, MIME describes the type of message content and the encoding used.

¬ Headers defined in MIME are:

- MIME-Version- current version, i.e., 1.1
- Content-Type - message type (text/html, image/jpeg, application/pdf)
- Content-Transfer-Encoding - message encoding scheme (eg base64).
- Content-Id - unique identifier for the message.
- Content-Description - describes type of the message body.



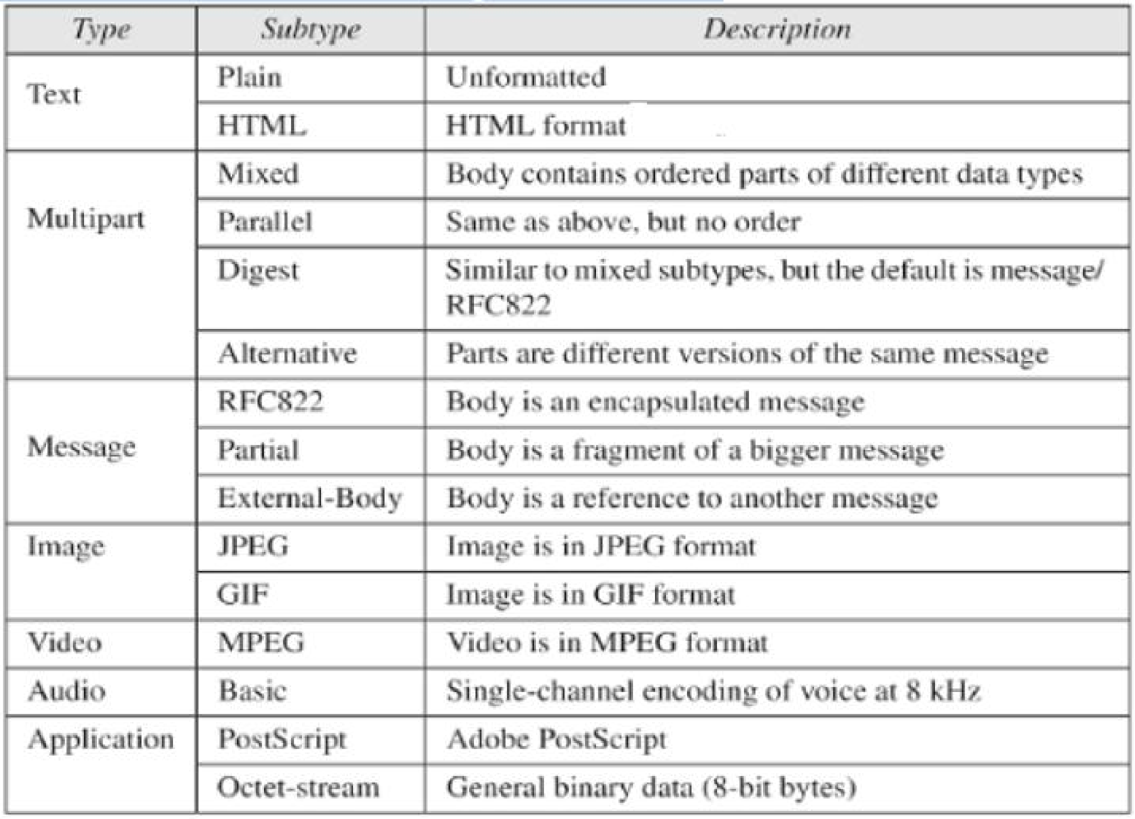
MIME-Version: 1.1
Content-Type: type/subtype
Content-Transfer-Encoding: encoding type
Content-Id: message id
Content-Description: textual explanation of nontextual contents

MIME CONTENT TYPES

¬ There are seven different major types of content and a total of 14 subtypes.

¬ In general, a content type declares the general type of data, and the subtype specifies a

particular format for that type of data.
¬ MIME also defines a multipart type that says how a message carrying more than one data type is structured.
¬ This is like a programming language that defines both base types (e.g., integers and floats) and compound types (e.g., structures and arrays).
¬ One possible multipart subtype is mixed, which says that the message contains a set of independent data pieces in a specified order.
¬ Each piece then has its own header line that describes the type of that piece.
¬ The table below lists the MIME content types:

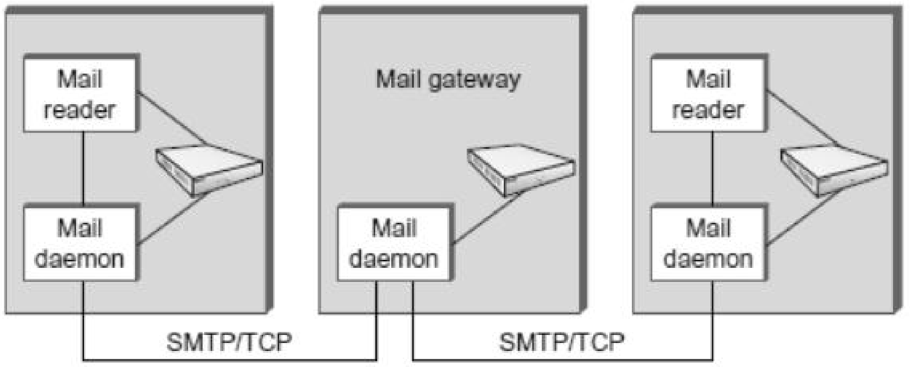


Type	*Subtype*	*Description*
Text	Plain	Unformatted
	HTML	HTML format
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to mixed subtypes, but the default is message/ RFC822
	Alternative	Parts are different versions of the same message
Message	RFC822	Body is an encapsulated message
	Partial	Body is a fragment of a bigger message
	External-Body	Body is a reference to another message
Image	JPEG	Image is in JPEG format
	GIF	Image is in GIF format
Video	MPEG	Video is in MPEG format
Audio	Basic	Single-channel encoding of voice at 8 kHz
Application	PostScript	Adobe PostScript
	Octet-stream	General binary data (8-bit bytes)

ENCODING FORMATS OF MIME

¬ MIME uses various encoding formats to convert binary data into the ASCII character set.
¬ To transfer binary data, MIME offers five encoding formats which can be used in the header transfer-encoding:
• 7-bit : 7-bit text format (for messages without accented characters);
• 8-bit : 8-bit text format;
• quoted-printable : Quoted-Printable format, recommended for messages which use a 7-bit alphabet (such as when there are accent marks);
• base-64 : Base 64, for sending binary files as attachments;
• binary : binary format; not recommended.
¬ Since MIME is very open, it can use third-party encoding formats such as:
• BinHex : A proprietary format belonging to Apple
• Uuencode : for UNIX-to-UNIX encoding
• Xencode : for binary-to-text encoding

MESSAGE TRANSFER IN MIME



¬ MTA is a mail daemon (send mail) active on hosts having mailbox, used to send an email.
¬ Mail passes through a sequence of gateways before it reaches the recipient mail server.
¬ Each gateway stores and forwards the mail using Simple mail transfer protocol (SMTP).
¬ SMTP defines communication between MTAs over TCP on port 25.
¬ In an SMTP session, sending MTA is client and receiver is server. In each exchange:
¬ Client posts a command (HELO, MAIL, RCPT, DATA, QUIT, VRFY, etc.)
¬ Server responds with a code (250, 550, 354, 221, 251 etc) and an explanation.
¬ Client is identified using HELO command and verified by the server
¬ Client forwards message to server, if server is willing to accept.
¬ Message is terminated by a line with only single period (.) in it.
¬ Eventually client terminates the connection.

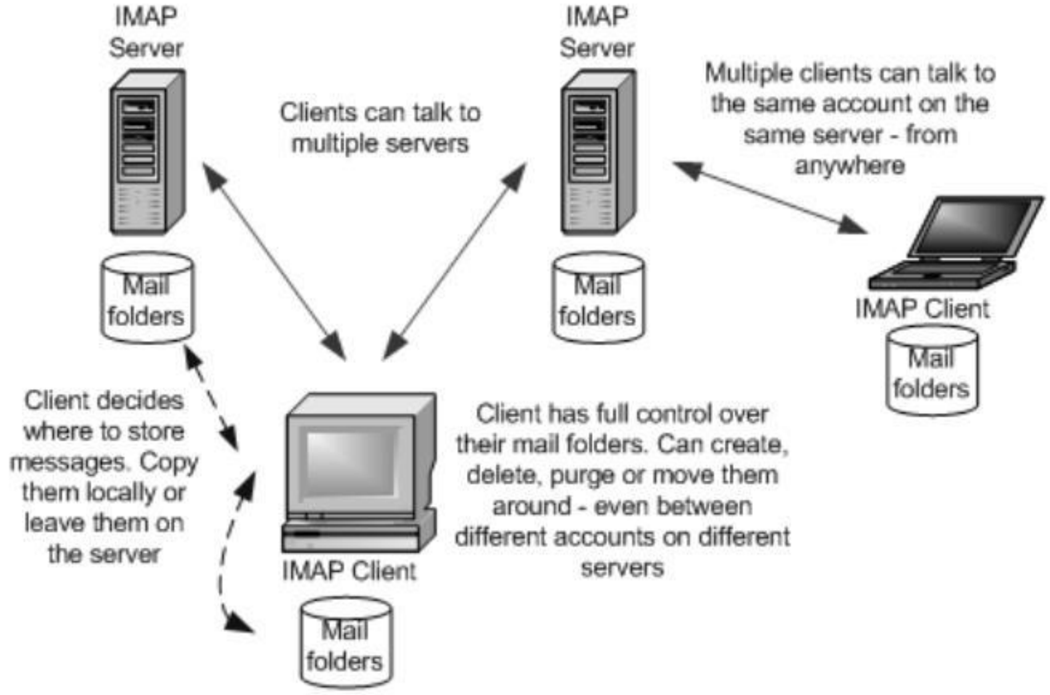
1.8.4.3 IMAP (INTERNET MAIL ACCESS PROTOCOL)

¬ IMAP is an Application Layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server.
¬ It is a method of accessing electronic mail messages that are kept on a possibly shared mail server.
¬ IMAP is a more capable wire protocol.
¬ IMAP is similar to SMTP in many ways.
¬ IMAP is a client/server protocol running over TCP on port 143.
¬ IMAP allows multiple clients simultaneously connected to the same mailbox, and through flags stored on the server, different clients accessing the same mailbox at the same or different times can detect state changes made by other clients.
¬ In other words, it permits a "client" email program to access remote message stores as if they were local.
¬ For example, email stored on an IMAP server can be manipulated from a desktop computer at home, a workstation at the office, and a notebook computer while travelling, without the need to transfer messages or files back and forth between these computers.
¬ IMAP can support email serving in three modes:
♣ Offline
♣ Online
Users may connect to the server, look at what email is available, and access it online. This

looks to the user very much like having local spool files, but they're on the mail server.

♣ Disconnected operation

A mail client connects to the server, can make a "cache" copy of selected messages, and disconnects from the server. The user can then work on the messages offline, and connect to the server later and resynchronize the server status with the cache.


IMAP Server
Mail folders
Clients can talk to multiple servers
IMAP Server
Mail folders
Multiple clients can talk to the same account on the same server - from anywhere
IMAP Client
Mail folders
Client decides where to store messages. Copy them locally or leave them on the server
IMAP Client
Mail folders
Client has full control over their mail folders. Can create, delete, purge or move them around - even between different accounts on different servers

OPERATION OF IMAP

¬ The mail transfer begins with the client authenticating the user and identifying the mailbox they want to access.

¬ Client Commands

LOGIN, AUTHENTICATE, SELECT, EXAMINE, CLOSE, and LOGOUT

¬ Server Responses

OK, NO (no permission), BAD (incorrect command),

¬ When user wishes to FETCH a message, server responds in MIME format.

¬ Message attributes such as size are also exchanged.

¬ Flags are used by client to report user actions.

SEEN, ANSWERED, DELETED, RECENT

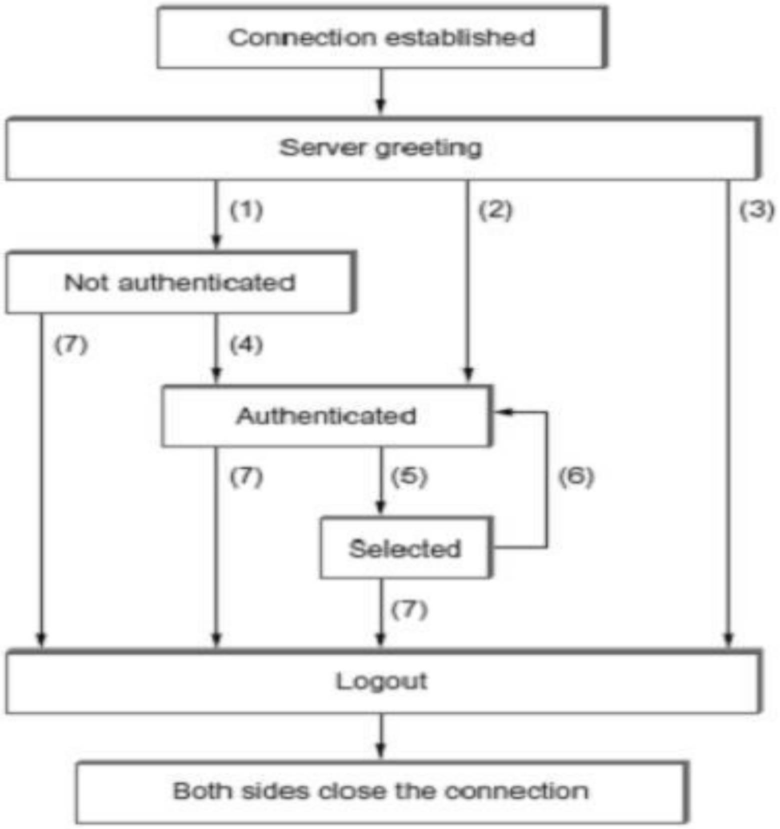
IMAP4

¬ The latest version is IMAP4. IMAP4 is more powerful and more complex.

¬ IMAP4 provides the 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 of characters prior to downloading.
- A user can partially download e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.

- A user can create, delete, or rename mailboxes on the mail server.
- A user can create a hierarchy of mailboxes in a folder for e-mail storage



(1) Connection without preauthentication (OK greeting)
(2) Preauthenticated connection (PREAUTH greeting)
(3) Rejected connection (BYE greeting)
(4) Successful LOGIN or AUTHENTICATE command
(5) Successful SELECT or EXAMINE command
(6) CLOSE command, or failed SELECT or EXAMINE command
(7) LOGOUT command, server shutdown, or connection closed

Advantages Of IMAP

¬ With IMAP, the primary storage is on the server, not on the local machine.

¬ Email being put away for storage can be foldered on local disk, or can be foldered on the IMAP server.

¬ The protocol allows full user of remote folders, including a remote folder hierarchy and multiple inboxes.

¬ It keeps track of explicit status of messages, and allows for user-defined status.

¬ Supports new mail notification explicitly.

¬ Extensible for non-email data, like netnews, document storage, etc.

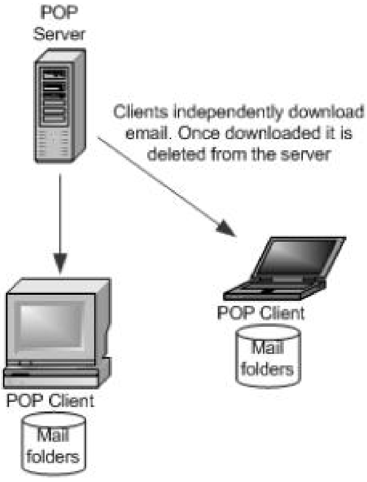
¬ Selective fetching of individual MIME body parts.

¬ Server-based search to minimize data transfer.

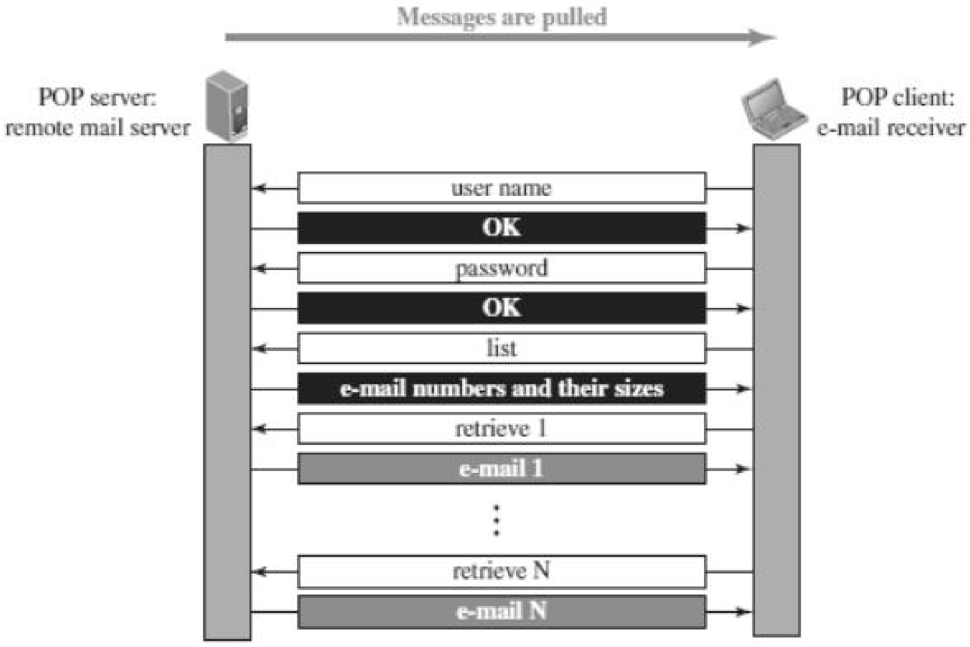
¬ Servers may have extensions that can be negotiated.

1.8.4.4 POST OFFICE PROTOCOL (POP3)

¬ Post Office Protocol (POP3) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
¬ There are two versions of POP.
• The first, called POP2, became a standard in the mid-80's and requires SMTP to send messages.
• The current version, POP3, can be used with or without SMTP. POP3 uses TCP/IP port 110.
¬ POP is a much simpler protocol, making implementation easier.
¬ POP supports offline access to the messages, thus requires less internet usage time
¬ POP does not allow search facility.
¬ In order to access the messages, it is necessary to download them.
¬ It allows only one mailbox to be created on server.
¬ It is not suitable for accessing non mail data.
¬ POP mail moves the message from the email server onto the local computer, although there is usually an option to leave the messages on the email server as well.
¬ POP treats the mailbox as one store, and has no concept of folders.
¬ POP works in two modes namely, delete and keep mode.
• In delete mode, mail is deleted from the mailbox after retrieval. The delete mode is normally used when the user is working at their permanent computer and can save and organize the received mail after reading or replying.
• In keep mode, mail after reading is kept in mailbox for later retrieval. The keep mode is normally used when the user accesses her mail away from their primary computer .


POP Server
Clients independently download email. Once downloaded it is deleted from the server
POP Client
Mail folders
POP Client
Mail folders

¬ POP3 client is installed on the recipient computer and POP server on the mail server.
¬ Client opens a connection to the server using TCP on port 110.
¬ Client sends username and password to access mailbox and to retrieve messages.


Messages are pulled
POP server: remote mail server
POP client: e-mail receiver
user name
OK
password
OK
list
e-mail numbers and their sizes
retrieve 1
e-mail 1
retrieve N
e-mail N

POP3 Commands

POP commands are generally abbreviated into codes of three or four letters
The following describes some of the POP commands:
1. UID - This command opens the connection
2. STAT - It is used to display number of messages currently in the mailbox
3. LIST - It is used to get the summary of messages
4. RETR -This command helps to select a mailbox to access the messages
5. DELE - It is used to delete a message
6. RSET - It is used to reset the session to its initial state
7. QUIT - It is used to log off the session

Advantages of IMAP over POP

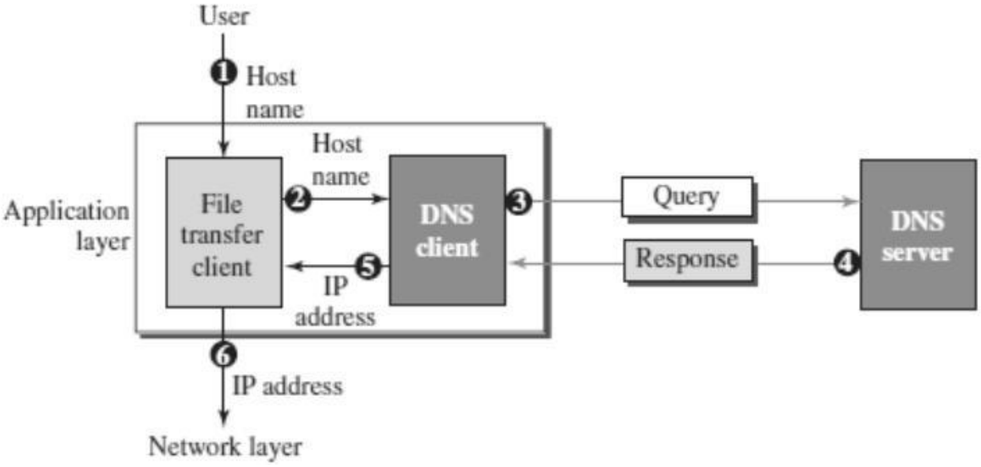
¬ IMAP is more powerful and more complex than POP.
¬ User can check the e-mail header prior to downloading.
¬ User can search e-mail for a specific string of characters prior to downloading.
¬ User can download partially, very useful in case of limited bandwidth.
¬ User can create, delete, or rename mailboxes on the mail server.

1.9 DNS (DOMAIN NAME SYSTEM)

¬ Domain Name System was designed in 1984.
¬ DNS is used for name-to-address mapping.
¬ The DNS provides the protocol which allows clients and servers to communicate with each other.
¬ Eg: Host name like www.yahoo.com is translated into numerical IP addresses like 207.174.77.131
¬ Domain Name System (DNS) is a distributed database used by TCP/IP applications to map

between hostnames and IP addresses and to provide electronic mail routing information.
¬ Each site maintains its own database of information and runs a server program that other systems across the Internet can query.

WORKING OF DNS



The following six steps shows the working of a DNS. It maps 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 a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server.
4. The DNS server responds 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 address to access the file transfer server.

NAME SPACE

¬ To be unambiguous, the names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP address.
¬ The names must be unique because the addresses are unique.
¬ A name space that maps each address to a unique name can be organized in two ways: flat (or) hierarchical.

<u>Flat Name Space</u>

- In a flat name space, a name is assigned to an address.
- A name in this space is a sequence of characters without structure.
- The main disadvantage of a flat name space is that it cannot be used in a large system such as Internet because it must be centrally controlled to avoid ambiguity and duplication.

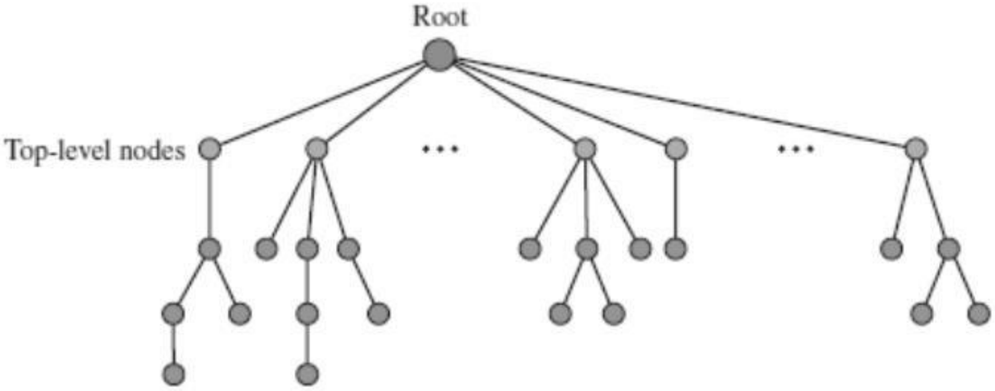
Hierarchical Name Space

- In a hierarchical name space, each name is made of several parts.
- The first part can define the organization, the second part can define the name, the third part can define departments, and so on.
- In this case, the authority to assign and control the name spaces can be decentralized.
- A central authority can assign the part of the name that defines the nature of the organization and the name.
- The responsibility for the rest of the name can be given to the organization itself. Suffixes can be added to the name to define host or resources.

• The management of the organization need not worry that the prefix chosen for a host is taken by another organization because even if part of an address is the same, the whole address is different.
• The names are unique without the need to be assigned by a central authority.
• The central authority controls only part of the name, not the whole name.

DOMAIN NAME SPACE

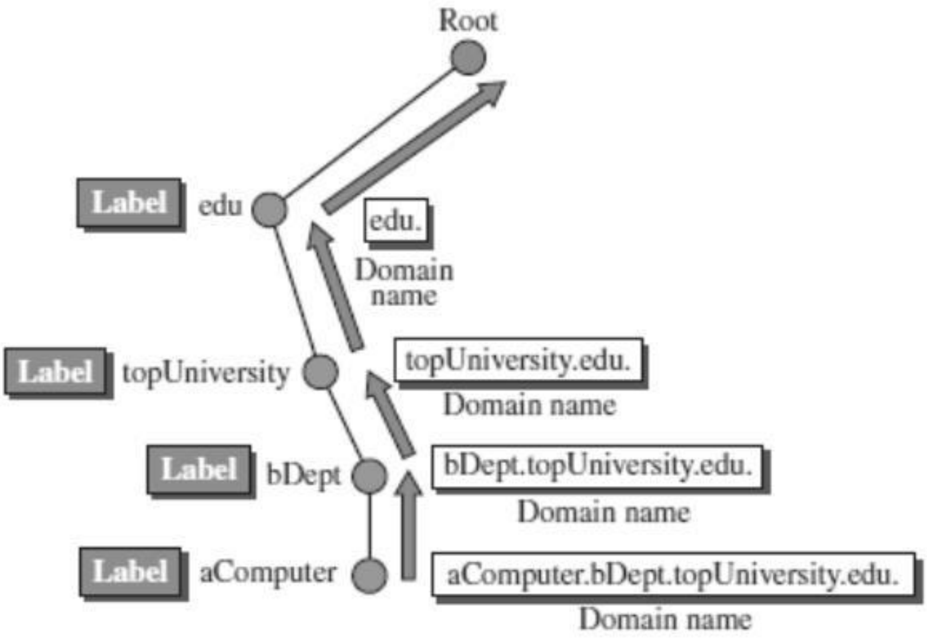
¬ To have a hierarchical name space, a domain name space was designed. In this design, the names are defined in an inverted-tree structure with the root at the top.
¬ Each node in the tree has a label, which is a string with a maximum of 63 characters.
¬ The root label is a null string.
¬ DNS requires that children of a node have different labels, which guarantees the uniqueness of the domain names.



¬ Each node in the tree has a label, which is a string with a maximum of 63 characters.
¬ The root label is a null string (empty string). DNS requires that children of a node (nodes that branch from the same node) have different labels, which guarantees the uniqueness of the domain names.

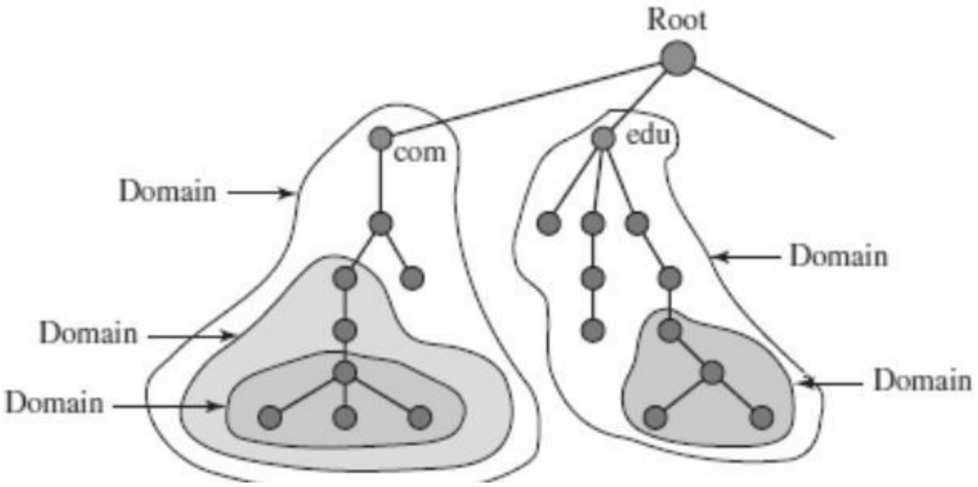
Domain Name

• Each node in the tree has a label called as domain name.
• A full domain name is a sequence of labels 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).
• This means that a full domain name always ends in a null label, which means the last character is a dot because the null string is nothing.
• If a label is terminated by a null string, it is called a fully qualified domain name (FQDN).
• If a label is not terminated by a null string, it is called a partially qualified domain name (PQDN).



Domain

- A domain is a subtree of the domain name space.
- The name of the domain is the domain name of the node at the top of the sub- tree.
- A domain may itself be divided into domains.



DISTRIBUTION OF NAME SPACE

¬ The information contained in the domain name space must be stored.

¬ But it is very inefficient and also not reliable to have just one computer store such a huge amount of information.

¬ It is inefficient because responding to requests from all over the world, places a heavy load on the system.

¬ It is not reliable because any failure makes the data inaccessible.

¬ The solution to these problems is to distribute the information among many computers called DNS servers.

HIERARCHY OF NAME SERVERS

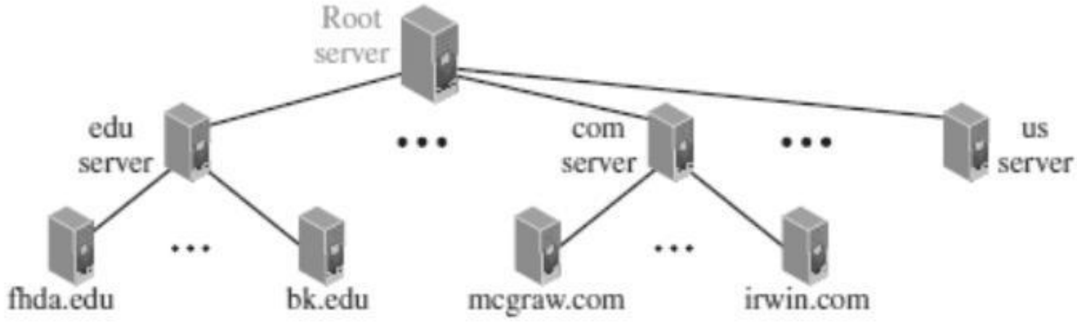
¬ The way to distribute information among DNS servers is to divide the whole space into many domains based on the first level.

¬ Let the root stand-alone and create as many domains as there are first level nodes.

¬ Because a domain created this way could be very large,

¬ DNS allows domains to be divided further into smaller domains.

¬ Thus we have a hierarchy of servers in the same way that we have a hierarchy of names.



ZONE

¬ What a server is responsible for, or has authority over, is called a zone.

¬ The server makes a database called a zone file and keeps all the information for every node under that domain.

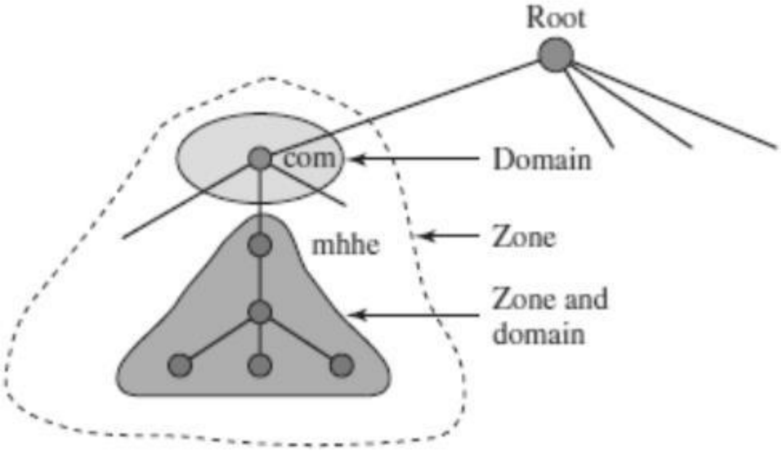
¬ If a server accepts responsibility for a domain and does not divide the domains into smaller domains, the domain and zone refer to the same thing.

¬ But if a server divides its domain into sub domains and delegates parts of its authority to other servers, domain and zone refer to different things.

¬ The information about the nodes in the sub domains is stored in the servers at the lower levels, with the original server keeping some sort of references to these lower level servers.

¬ But still, the original server does not free itself from responsibility totally.

¬ It still has a zone, but the detailed information is kept by the lower level servers.



ROOT SERVER

¬ A root sever is a server whose zone consists of the whole tree.

¬ A root server usually does not store any information about domains but delegates its authority to other servers, keeping references to those servers.

¬ Currently there are more than 13 root servers, each covering the whole domain

name space.
¬ The servers are distributed all around the world.

PRIMARY AND SECONDARY SERVERS

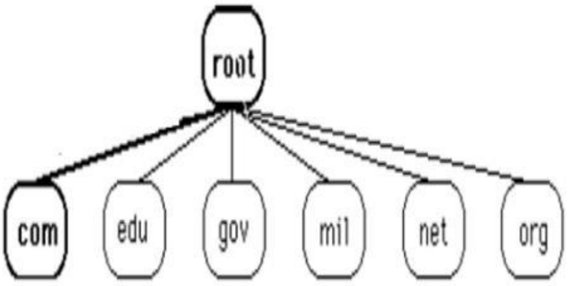
¬ DNS defines two types of servers: primary and secondary.
¬ A Primary Server is a server that stores a file about the zone for which it is an authority.
• Primary Servers are responsible for creating, maintaining, and updating the zone file.
• Primary Server stores the zone file on a local disc.
¬ A secondary server is a server that transfers the complete information about a zone from another server (Primary or Secondary) and stores the file on its local disc.
¬ If updating is required, it must be done by the primary server, which sends the updated version to the secondary.
¬ A primary server loads all information from the disk file; the secondary server loads all information from the primary server.

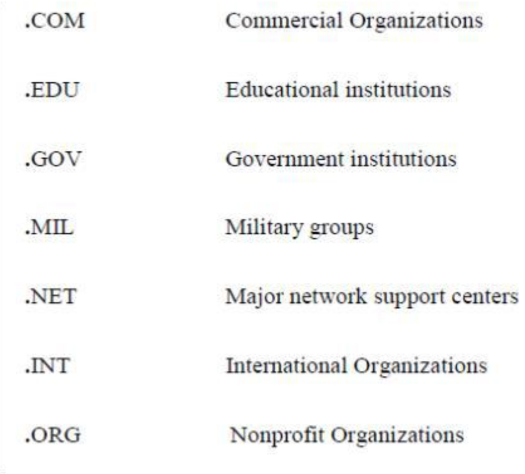
DNS IN THE INTERNET

¬ DNS is a protocol that can be used in different platforms.
¬ In the Internet, the domain name space (tree) is divided into three different sections - Generic domains, Country domains, and Inverse domain.

<u>Generic Domains</u>

¬ The generic domains define registered hosts according to their generic behavior.
¬ Each node in the tree defines a domain, which is an index to the domain name space database.
¬ The first level in the generic domains section allows seven possible three character levels.
¬ These levels describe the organization types as listed in following table.





.COM	Commercial Organizations
.EDU	Educational institutions
.GOV	Government institutions
.MIL	Military groups
.NET	Major network support centers
.INT	International Organizations
.ORG	Nonprofit Organizations

<u>Country Domains</u>

¬ The country domains section follows the same format as the generic domains but uses two characters for country abbreviations
¬ E.g.; in for India, us for United States etc) in place of the three character organizational abbreviation at the first level.
¬ Second level labels can be organizational, or they can be more specific, national designation.
¬ India for example, uses state abbreviations as a subdivision of the country domain us. (e.g., ca.in.)

Inverse Domains

¬ Mapping an address to a name is called Inverse domain.

¬ The client can send an IP address to a server to be mapped to a domain name and it is called PTR(Pointer) query.

¬ To answer queries of this kind, DNS uses the inverse domain.

DNS RESOLUTION

¬ Mapping a name to an address or an address to a name is called name address resolution.

¬ DNS is designed as a client server application.

¬ A host that needs to map an address to a name or a name to an address calls a DNS client named a Resolver.

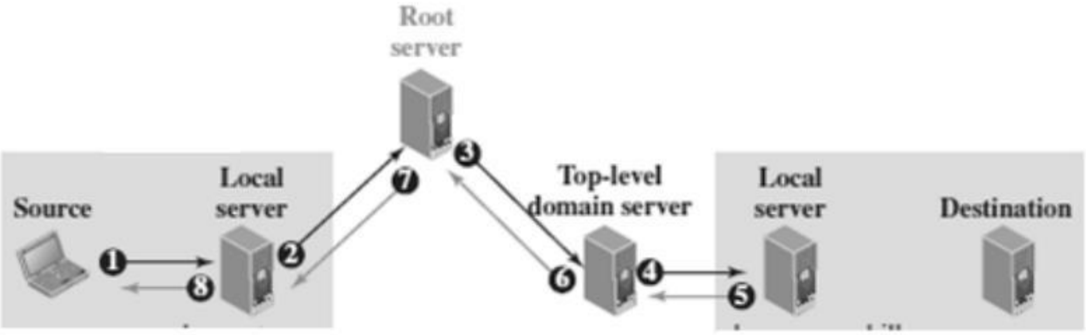
¬ The Resolver accesses the closest DNS server with a mapping request.

¬ If the server has the information, it satisfies the resolver; otherwise, it either refers the resolver to other servers or asks other servers to provide the information.

¬ After the resolver receives the mapping, it interprets the response to see if it is a real resolution or an error and finally delivers the result to the process that requested it.

¬ A resolution can be either recursive or iterative.

Recursive Resolution



• The application program on the source host calls the DNS resolver (client) to find the IP address of the destination host. The resolver, which does not know this address, sends the query to the local DNS server of the source (Event 1)

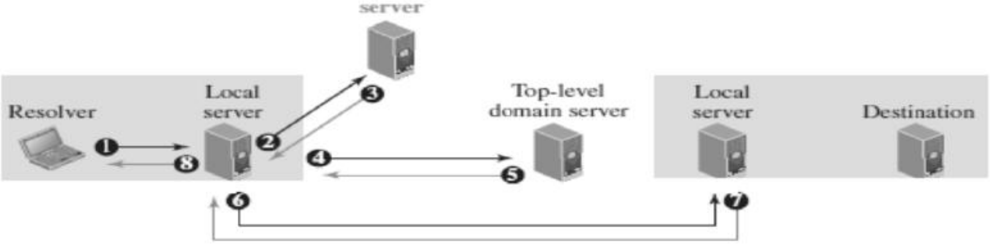
• The local server sends the query to a root DNS server (Event 2)

• The Root server sends the query to the top-level-DNS server(Event 3)

• The top-level DNS server knows only the IP address of the local DNS server at the destination. So it forwards the query to the local server, which knows the IP address of the destination host (Event 4)

• The IP address of the destination host is now sent back to the top-level DNS server(Event 5) then back to the root server (Event 6), then back to the source DNS server, which may cache it for the future queries (Event 7), and finally back to the source host (Event 8)

Iterative Resolution



• In iterative resolution, each server that does not know the mapping, sends the IP address of the next server back to the one that requested it.
• The iterative resolution takes place between two local servers.
• The original resolver gets the final answer from the destination local server.
• The messages shown by Events 2, 4, and 6 contain the same query.
• However, the message shown by Event 3 contains the IP address of the top- level domain server.
• The message shown by Event 5 contains the IP address of the destination local DNS server
• The message shown by Event 7 contains the IP address of the destination.
• When the Source local DNS server receives the IP address of the destination, it sends it to the resolver (Event 8).

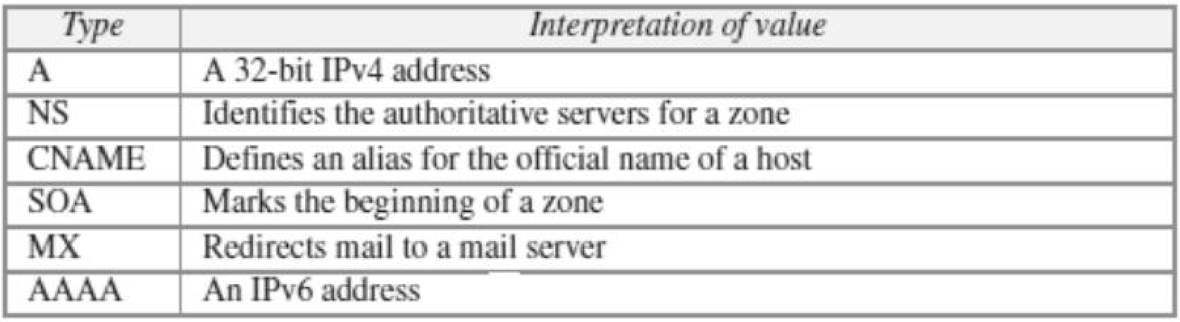
DNS CACHING

¬ Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address.
¬ DNS handles this with a mechanism called caching.
¬ When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client.
¬ If the same or another client asks for the same mapping, it can check its cache memory and resolve the problem.
¬ However, to inform the client that the response is coming from the cache memory and not from an authoritative source, the server marks the response as unauthoritative.
¬ Caching speeds up resolution. Reduction of this search time would increase efficiency, but it can also be problematic.
¬ If a server caches a mapping for a long time, it may send an outdated mapping to the client.
¬ To counter this, two techniques are used.
⎫ First, the authoritative server always adds information to the mapping called time to live (TTL). It defines the time in seconds that the receiving server can cache the information. After that time, the mapping is invalid and any query must be sent again to the authoritative server.
⎫ Second, DNS requires that each server keep a TTL counter for each mapping it caches. The cache memory must be searched periodically and those mappings with an expired TTL must be purged.

DNS RESOURCE RECORDS (RR)

• The zone information associated with a server is implemented as a set of resource records.
• In other words, a name server stores a database of resource records.
• A resource record is a 5-tuple structure : (Domain Name, Type, Class, TTL, Value)
• The domain name identifies the resource record.
• The type defines how the value should be interpreted.
• The value defines the information kept about the domain name.
• The TTL defines the number of seconds for which the information is valid.
• The class defines the type of network.

Types of Resource Records



Type	*Interpretation of value*
A	A 32-bit IPv4 address
NS	Identifies the authoritative servers for a zone
CNAME	Defines an alias for the official name of a host
SOA	Marks the beginning of a zone
MX	Redirects mail to a mail server
AAAA	An IPv6 address

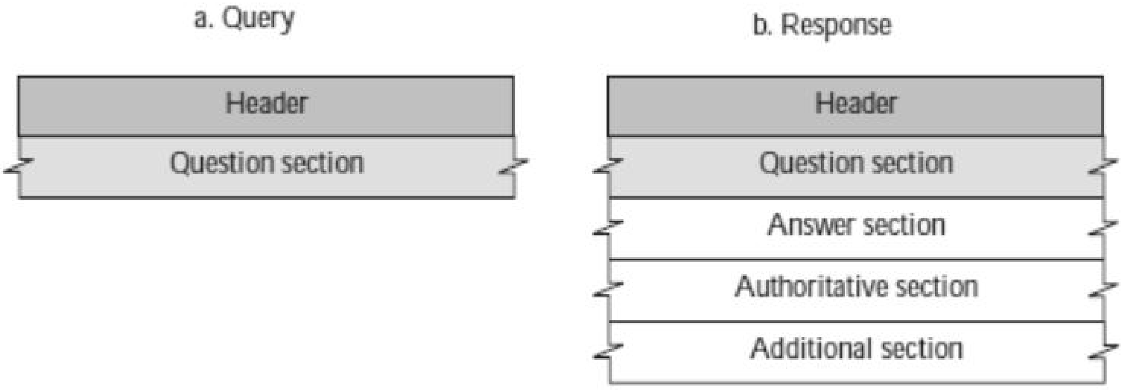
DNS MESSAGES

¬ DNS has two types of messages: query and response.

¬ Both types have the same format.

¬ The query message consists of a header and question section.

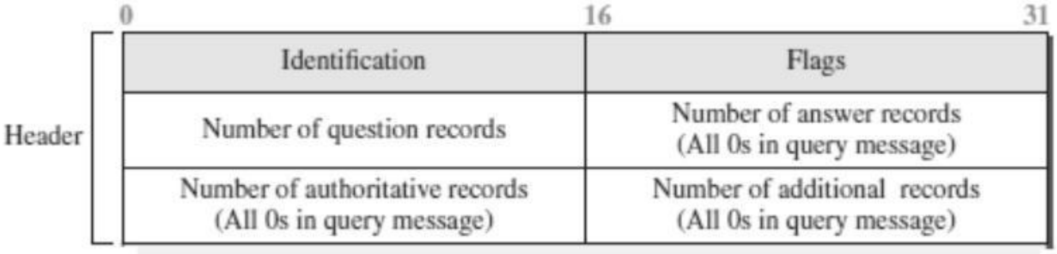
¬ The response message consists of a header, question section, answer section, authoritative section, and additional section .



¬ Header

• Both query and response messages have the same header format with some fields set to zero for the query messages.

• The header fields are as follows:



	0	16 31
Header	Identification	Flags
	Number of question records	Number of answer records (All 0s in query message)
	Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

• The identification field is used by the client to match the response with the query.

• The flag field defines whether the message is a query or response. It also includes status of error.

• The next four fields in the header define the number of each record type in the message.

¬ Question Section

• The question section consists of one or more question records. It is present in both query and response messages.

¬ Answer Section

• The answer section consists of one or more resource records. It is present only in response messages.

¬ ***Authoritative Section***

• The authoritative section gives information (domain name) about one or more authoritative servers for the query.

¬ ***Additional Information Section***

• The additional information section provides additional information that may help the resolver.

DNS CONNECTIONS

¬ DNS can use either UDP or TCP.

¬ In both cases the well-known port used by the server is port 53.

¬ UDP is used when the size of the response message is less than 512 bytes because most UDP packages have a 512-byte packet size limit.

¬ If the size of the response message is more than 512 bytes, a TCP connection is used.

DNS REGISTRARS

¬ New domains are added to DNS through a registrar. A fee is charged.

¬ A registrar first verifies that the requested domain name is unique and then enters it into the DNS database.

¬ Today, there are many registrars; their names and addresses can be found at http://www.intenic.net

¬ To register, the organization needs to give the name of its server and the IP address of the server.

¬ For example, a new commercial organization named wonderful with a server named ws and IP address 200.200.200.5, needs to give the following information to one of the registrars: Domain name: ws.wonderful.com IP address: 200.200.200.5.

DDNS (DYNAMIC DOMAIN NAME SYSTEM)

¬ In DNS, when there is a change, such as adding a new host, removing a host, or changing an IP address, the change must be made to the DNS master file.

¬ The DNS master file must be updated dynamically.

¬ The Dynamic Domain Name System (DDNS) is used for this purpose.

¬ In DDNS, when a binding between a name and an address is determined, the information is sent to a primary DNS server.

¬ The primary server updates the zone.

¬ The secondary servers are notified either actively or passively.

¬ In active notification, the primary server sends a message to the secondary servers about the change in the zone, whereas in passive notification, the secondary servers periodically check for any changes.

¬ In either case, after being notified about the change, the secondary server requests information about the entire zone (called the zone transfer).

¬ To provide security and prevent unauthorized changes in the DNS records, DDNS can use an authentication mechanism.

DNS SECURITY

¬ DNS is one of the most important systems in the Internet infrastructure; it provides crucial services to Internet users.

¬ Applications such as Web access or e-mail are heavily dependent on the proper operation of DNS.

¬ DNS can be attacked in several ways including:

- Attack on Confidentiality - The attacker may read the response of a DNS server to find the nature or names of sites the user mostly accesses. This type of information can be used to find the user's profile. To prevent this attack, DNS messages need to be confidential.
- Attack on authentication and integrity - The attacker may intercept the response of a DNS server and change it or create a totally new bogus response to direct the user to the site or domain the attacker wishes the user to access. This type of attack can be prevented using message origin authentication and message integrity.
- Attack on denial-of-service - The attacker may flood the DNS server to overwhelm it or eventually crash it. This type of attack can be prevented using the provision against denial-of-service attack.

¬ To protect DNS, IETF has devised a technology named DNS Security (DNSSEC) that provides message origin authentication and message integrity using a security service called digital signature.

¬ DNSSEC, however, does not provide confidentiality for the DNS messages.

¬ There is no specific protection against the denial-of-service attack in the specification of DNSSEC. However, the caching system protects the upper- level servers against this attack to some extent.

1.10 SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

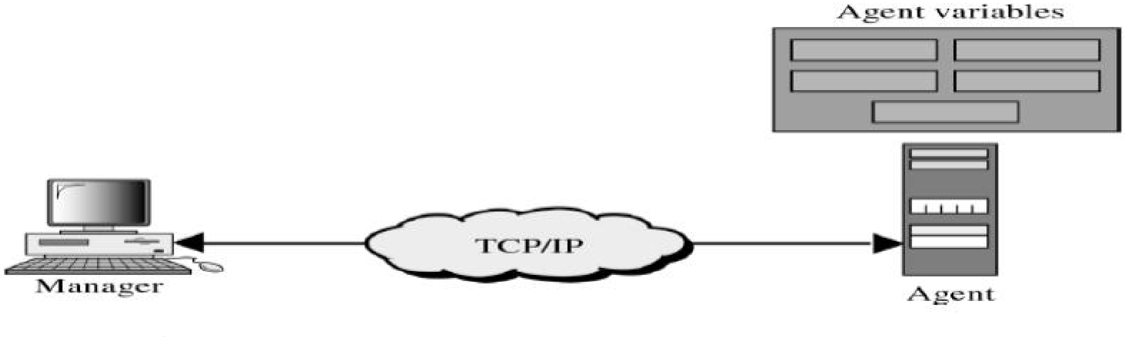
¬ The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite.

¬ SNMP is an application layer protocol that monitors and manages routers, distributed over a network.

¬ It provides a set of operations for monitoring and managing the internet.

¬ SNMP uses services of UDP on two well-known ports: 161 (Agent) and 162 (manager).

¬ SNMP uses the concept of manager and agent.



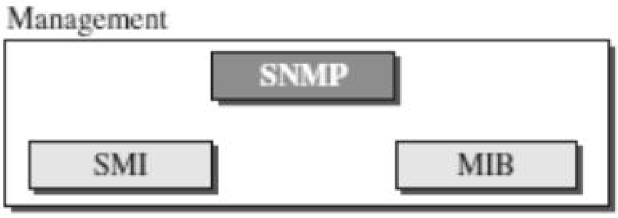
SNMP MANAGER

- A manager is a host that runs the SNMP client program
- The manager has access to the values in the database kept by the agent.

• A manager checks the agent by requesting the information that reflects the behavior of the agent.
• A manager also forces the agent to perform a certain function by resetting values in the agent database.
• For example, a router can store in appropriate variables the number of packets received and forwarded.
• The manager can fetch and compare the values of these two variables to see if the router is congested or not.

SNMP AGENT
• The agent is a router that runs the SNMP server program.
• The agent is used to keep the information in a database while the manager is used to access the values in the database.
• For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
• Agents can also contribute to the management process.
• A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

SNMP MANAGEMENT COMPONENTS
• Management of the internet is achieved through simple interaction between a manager and agent.
• Management is achieved through the use of two protocols:
o Structure of Management Information (SMI)
o Management Information Base (MIB).



Structure of Management Information (SMI)
• To use SNMP, we need rules for naming objects.
• SMI is a protocol that defines these rules.
• SMI is a guideline for SNMP
• It emphasizes three attributes to handle an object: name, data type, and encoding method.
• Its functions are:
ϖ To name objects.
ϖ To define the type of data that can be stored in an object.
ϖ To show how to encode data for transmission over the network.

Name
⎫ SMI requires that each managed object (such as a router, a variable in a router, a value,etc.) have a unique name. To name objects globally.
⎫ SMI uses an object identifier, which is a hierarchical identifier based on a tree structure.
⎫ The tree structure starts with an unnamed root. Each object can be defined using a sequence

of integers separated by dots.

⎫ The tree structure can also define an object using a sequence of textual names separated by dots.

Type of data

⎫ The second attribute of an object is the type of data stored in it.

⎫ To define the data type, SMI uses Abstract Syntax Notation One (ASN.1) definitions.

⎫ SMI has two broad categories of data types: simple and structured.

⎫ The simple data types are atomic data types. Some of them are taken directly from ASN.1; some are added by SMI.

⎫ SMI defines two structured data types: sequence and sequence of.

♣ Sequence - A sequence data type is a combination of simple data types, not necessarily of the same type.

♣ Sequence of - A sequence of data type is a combination of simple data types all of the same type or a combination of sequence data types all of the same type.

Encoding data

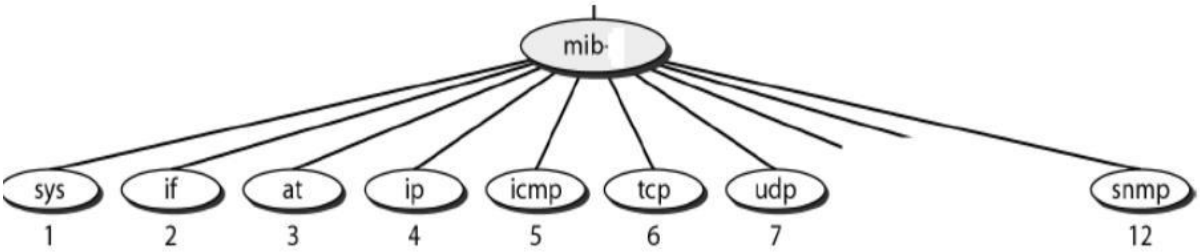
⎫ SMI uses another standard, Basic Encoding Rules (BER), to encode data to be transmitted over the network.

⎫ BER specifies that each piece of data be encoded in triplet format (TLV): tag, length, value

Management Information Base (MIB)

The Management Information Base (MIB) is the second component used in network management.

- Each agent has its own MIB, which is a collection of objects to be managed.
- MIB classifies objects under groups.



MIB Variables

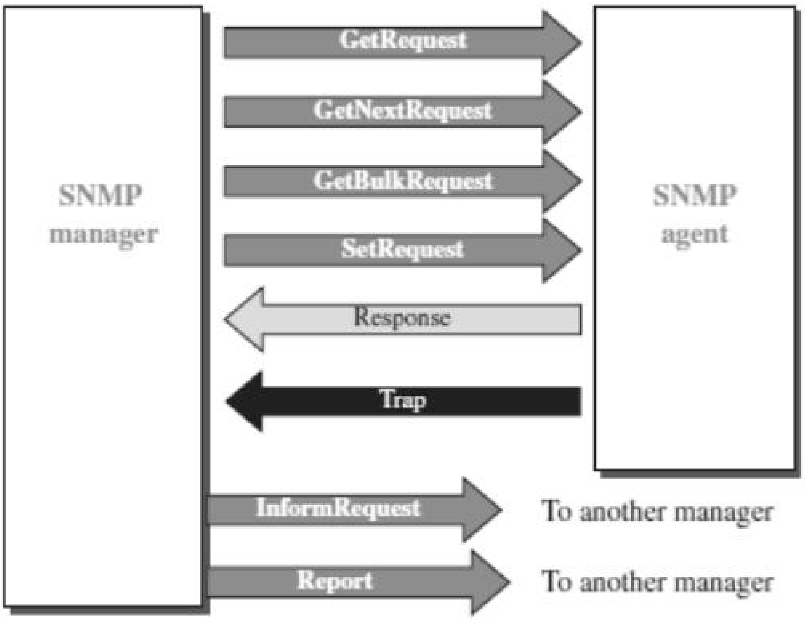
MIB variables are of two types namely simple and table.

- Simple variables are accessed using group-id followed by variable-id and 0
- Tables are ordered as column-row rules, i.e., column by column from top to bottom. Only leaf elements are accessible in a table type.

SNMP MESSAGES/PDU

SNMP is request/reply protocol that supports various operations using PDUs.
SNMP defines eight types of protocol data units (or PDUs):

GetRequest, GetNext-Request, GetBulkRequest, SetRequest, Response, Trap, InformRequest, and Report



GetRequest

♣ The GetRequest PDU is sent from the manager (client) to the agent (server) to retrieve the value of a variable or a set of variables.

GetNextRequest

♣ The GetNextRequest PDU is sent from the manager to the agent to retrieve the value of a variable.

GetBulkRequest

♣ The GetBulkRequest PDU is sent from the manager to the agent to retrieve a large amount of data. It can be used instead of multiple GetRequest and GetNextRequest PDUs.

SetRequest

♣ The SetRequest PDU is sent from the manager to the agent to set (store) a value in a variable.

Response

♣ The Response PDU is sent from an agent to a manager in response to

GetRequest or GetNextRequest. It contains the value(s) of the variable(s) requested by the manager.

Trap

♣ The Trap PDU is sent from the agent to the manager to report an event. For example, if the agent is rebooted, it informs the manager and reports the time of rebooting.

InformRequest

♣ The InformRequest PDU is sent from one manager to another remote manager to get the value of some variables from agents under the control of the remote manager. The remote manager responds with a Response PDU.

Report

♣ The Report PDU is designed to report some types of errors between managers.

Unit II: Transport Layer

Introduction - Transport Layer protocols: UDP-TCP: Connection management - Flow control - Congestion control - congestion avoidance (DEC bit, RED) - SCTP - Quality of service

2.1 Introduction:

The transport layer is the heart of the TCP/IP protocol suite; it is the end to end logical vehicle for transferring data from one point to another in the Internet. It is responsible for end to end delivery of entire message.

Functions:

- This layer is the first one which breaks the messages into packets.
- This layer ensures that data must be received in the same sequence in which it was sent.
- This layer provides end to end delivery of data between hosts

2.1.1 Services:

Each protocol provides a different type of service and should be used appropriately

- UDP: UDP is an unreliable connectionless transport - layer protocol used for its simplicity and efficiency.
- TCP: TCP is a reliable connection-oriented protocol that can be used in any application where reliability is important
- SCTP: New transport layer protocol that combines the [illegible] UDP and TCP.

2.1.2 Port numbers :

Transport layer usually has several responsibilities. One is to create a process to process communication; these protocols use port numbers to accomplish this. Some of the well known ports used with UDP TCP is given below

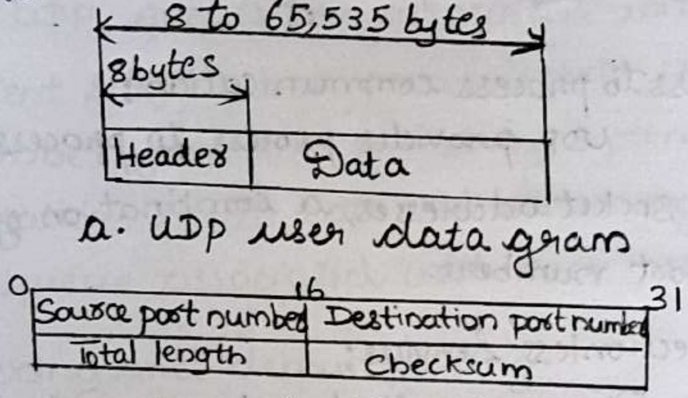
Port	Description	UDP	TCP	SCTP
7.	Echoes back a received datagram	✓	✓	✓
9.	Discards any datagram that is received	✓	✓	✓
11.	Active users	✓	✓	✓
13	Returns the date and time	✓	✓	✓
20.	File Transfer protocol	–	✓	✓
25	Simple Mail Transfer protocol	–	✓	✓
80	HyperText Transfer protocol	–	✓	✓

2.2 User Datagram Protocol

The User Datagram Protocol (UDP) is a connectionless, unreliable transport protocol. UDP is a very simple protocol using a minimum of overhead. If a process wants to send a small message and does not care much about reliability, It can use UDP. It also has no error recovery procedures. It performs very limited error checking.

2.2.1 User Datagram

UDP packets called user datagrams, have a fixed size header of 8 bytes made of four fields, each of 2bytes. Below figure shows the format of a user datagram.



a. UDP user datagram

b Header Format

Fig: User Datagram Packet format

The fields are as follows:

- Source port number: This is the port number used by the process running on the source host. It is 16 bits long, which means that the port number can range from 0 to 65,535
- Destination port number: This is the port number used by the process running on the destination host. It is also 16 bits long.
- Length: This is a 16 bit field that defines the total length of the user datagram, header plus data
- Checksum: This field is used to detect errors

2.2.2 UDP Services:

Below are the general services provided by UDP

- Process to process communication
- connectionless services
- Flow control

- Error Control
- Checksum
- congestion control
- Encapsulation and Decapsulation
- Queuing
- Multiplexing and Demultiplexing

- Process to process communication:

UDP provides process to process communication using socket addresses, a combination of IP addresses and port numbers.

- Connectionless Services:

This means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagram even if they are coming from the same source and going to the same destination.

- Flow control:

UDP is simple protocol. There is no flow control.

- Error control:—

There is no error control mechanism in UDP except for the checksum. This means that the sender does not know if a message has been lost or duplicated.

- Checksum:

It is used by the sender and receiver to check for data corruption.

- Congestion control:

UDP does not provide congestion control UDP assumes that the packets send are small and cannot create congestion in the network.

- Encapsulation and Decapsulation:

To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages.

- Queuing:

In UDP, queues are associated with ports. At the client site, when a process starts, it requests a port number from the operating system. Some implementations create both an incoming and an outgoing queue associated with each process.

- Multiplexing and demultiplexing:

In a host running a TCP/IP protocol suite, there is only one UDP but possibly several processes that may want to use the services of UDP. To handle this situation, UDP multiplexes and demultiplexes.

2.2.3 UDP Applications

1. UDP is suitable for a process that requires simple request-response communication.
2. UDP is suitable for a process with Internal flow and error control mechanisms.
3. UDP is a suitable transport protocol for multicasting
4. UDP is used for management processes.
6. UDP is normally used for interactive real time applications that cannot tolerate uneven delay between sections of a received message.

2.3 Transmission Control Protocol

TCP is a connection oriented reliable protocol. TCP is a process to process protocol. TCP uses flow and error control mechanism at the transport level.

2.3.1 TCP services:

The services offered by TCP to the processes is explained below:

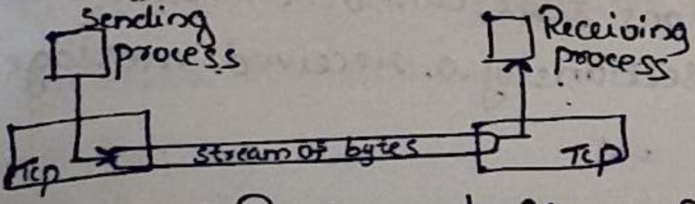
- Process to Process communication
- Stream Delivery services
- Full Duplex communication
- Multiplexing and Demultiplexing
- Connection oriented service
- Reliable service

- Process to process communication:

TCP provides process to process communication using port numbers.

- Stream Delivery Services:

TCP is stream oriented protocol. TCP allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes. TCP creates an environment in which the two processes seem to be connected by an imaginary tube that carries their data across the Internet



- Sending and Receiving buffers: Because the sending and the receiving processes may not write or read data at the same speed, TCP needs buffers for storage. There are two buffers the sending buffer and the receiving buffer, one for each direction

- Segments : At the transport Layer, TCP groups a number of bytes together into a packets called a segment.

- Full Duplex Communication:

TCP offers full duplex service, in which data can flow in both directions at the same time. Each TCP endpoints then has its own sending and receiving buffer and segments move in both directions.

- Multiplexing and Demultiplexing:

Like UDP, TCP performs multiplexing at the sender and demultiplexing at the receiver.

- Connection Oriented Service:

TCP is a connection-oriented protocol. When a process at site A wants to send and receive data from another process at site B, the following occurs:

1. The two TCPs establish a connection between them.
2. Data are exchanged in both directions
3. The connection is terminated.

- Reliable Service:

TCP is a reliable transport protocol. It uses an acknowledgement mechanism to check the safe and sound arrival of data.

2.3.2 Tcp Features :

- Numbering System:

Although the Tcp software keeps track of the segments being transmitted or received, their is no field for a segment number value in the segment header. Instead, there are two fields, called the sequence number and the acknowledgement number. These two field refer to a byte number and not a segment number.

■ Byte Number: When Tcp received bytes of data from a process, TCP stores them in the sending buffer and numbers them. The numbering does not necessarily start from 0. Instead, TCP chooses an arbitrary number between 0 and $2^{32}-1$

■ Sequence Number: After the bytes have been numbered, Tcp assigns a sequence number to each segment that is being sent. It is defined as follows:

1. The sequence number of the first segment is the ISN (initial sequence number) which is a random number.

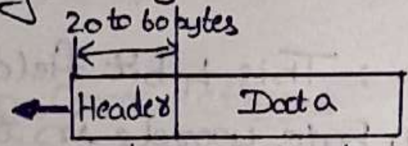
2. The sequence number of any other segmen is the sequence number of the previous segment plus the number of bytes carried by the previous segment.

- **Acknowledgment Number:** Both sender and receiver uses an acknowledgment number to confirm the bytes it has received. The acknowledgment number defines the number of the next byte that the party expects to receive.

2.3.3 Segment

A packet in TCP is called a segment.

The format of a segment is shown in figure:



a. segment

1 16 31

HLEN 4 bits	Reserved 6 bits	U R G	A C K	P S H	R S T	S Y N	F I N	
Source port address 16 bits								Destination port address 16 bits
Sequence number 32 bits								
Acknowledgment number 32 bits								
HLEN 4 bits	Reserved 6 bits	U R G	A C K	P S H	R S T	S Y N	F I N	Window size 16 bits
Checksum 16 bits								Urgent pointer 16 bits
Options and padding (up to 40 bytes)								

b. Header

1) Source port address: This is a 16 bit field that defines the port number of the application program in the host that is sending the segment

2) Destination port address: This is a 16 bit field that defines the port number of the application program in the host that is receiving the segment.

3) Sequence number: This 32 bit field defines the number assigned to the first byte of data contained in this segment

4) Acknowledgment number: This 32 bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number x from other party, it returns x+1 as the acknowledgement number.

5) Header Length : This 4 bit field indicates the number of 4 byte words in the TCP header. The length of the header can be between 20 and 60 bytes. Therefore the value of this field is always between 5(5x4=20) and 15(15x4=60).

6) Reserved: This 16 bit field is reserved for future use

7) Control: This field defines 6 different control bits or flags

URG : Urgent pointer is valid
ACK : Acknowledgment is valid
PSH : Request for push
RST : Reset the connection
SYN : Synchronize sequence numbers
FIN : Terminate the connection (finish)

8) Window Size: This field defines the size of the window, in bytes, that the other party must maintain.

9) Checksum: This 16 bit field contains the checksum. The use of checksum in the UDP datagram is optional, whereas the use of the checksum for TCP is mandatory.

10) Urgent pointer: This 16 bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data.

11) Options: There can be upto 40 bytes of optional information in the TCP header.

2.3.4. TCP Connections

TCP is a connection oriented transpor protocol establishes a logical path between the source and destination. TCP connection is logical not physical. In TCP, connection-oriented transmission requires three phases:

- connection establishment
- data transfer
- connection termination

■ Connection establishment:

Tcp transmits data in full-duplex mode. When two TCPs in two machines are connected, they are able to send segments to each other simultaneously.

Three way Handshaking:

The connection establishment in TCP is called three way handshaking. The three way handshaking process is shown below.

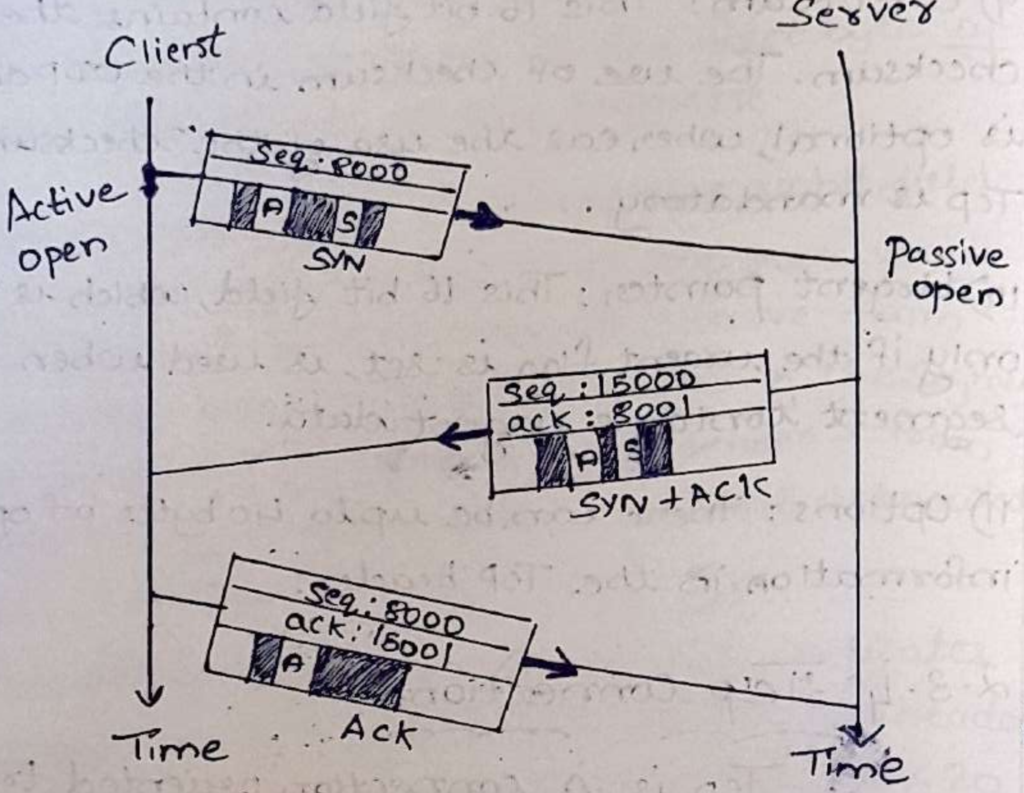


Fig: Connection establishment using three way handshaking

1. The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for Synchronization of sequence numbers. It consumes one sequence number. When the data transfer start, the sequence number is incremented by 1.
2. The sever sends the second segment, a SYN+ACK segment, with 2 flag bits set: SYN and ACK.
3. The client sends the third segment. This is Just an Ack segment. It acknowledges the receipt of the second segment with the Ack flag and acknowledgment number field.

- **Data transfer :**

After Connection is established, bidirectional data transfer can take place. The client and server can both send data and acknowledge. Figure Shows the example:

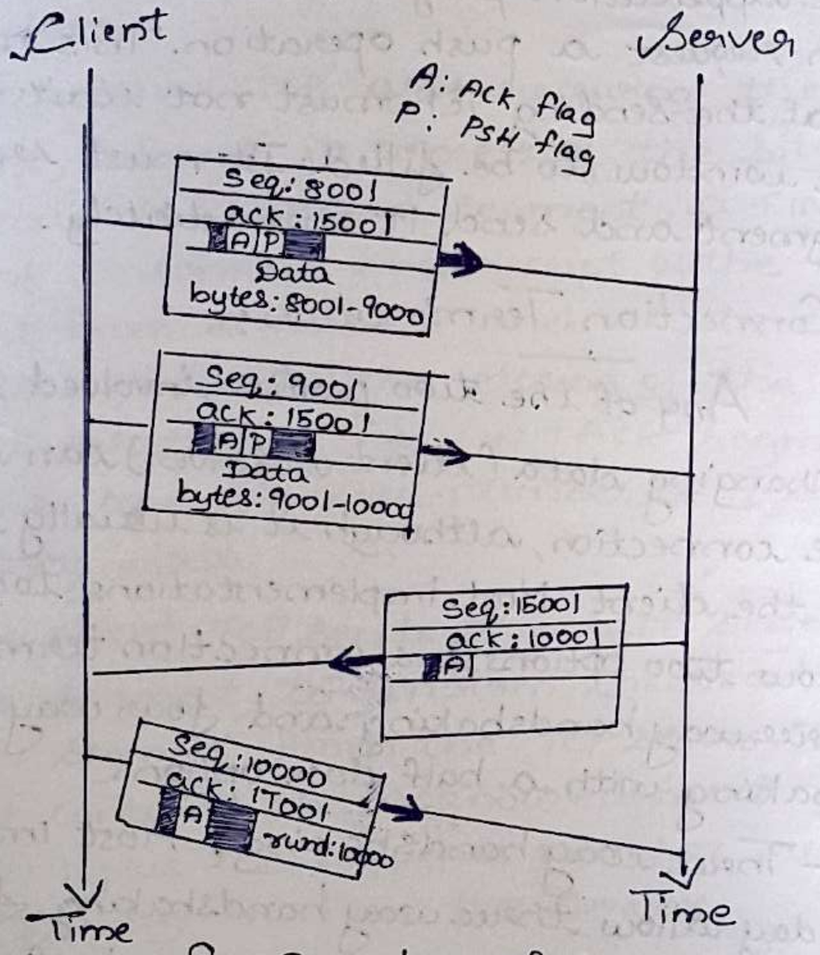


fig: Data transfer

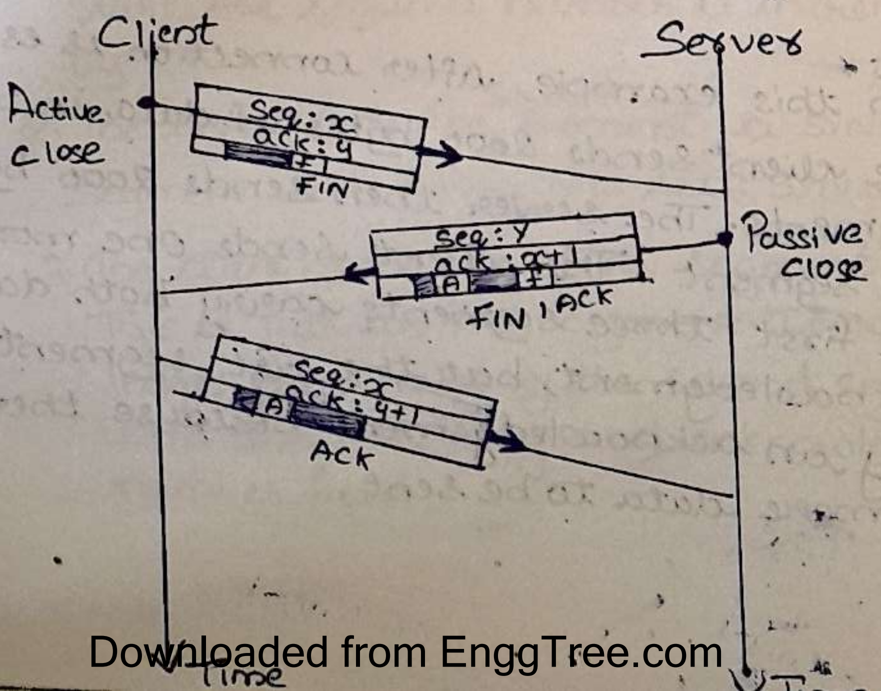
In this example, after connection is established the client sends 2000 bytes of data in two segments. The server then sends 2000 bytes in one segment. The client sends one more segment. The first three segments carry both data and acknowledgment, but the last segment carries only an acknowledgement because there are no more data to be sent.

Pushing data: The sending TCP uses a buffer to store the stream of data coming from the sending application program. The sending TCP can select the segment size. The application program at the sending site can request a push operation. This means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately.

- Connection Termination:

Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client. Most implementations today allow two options for connection termination: three way handshaking and four way handshaking with a half close option.

– Three way handshaking: Most implementations today allow three way handshaking for connection termination as shown in figure



1. In a normal situation, the client TCP, after receiving a close command from the client process, sends the first segment, a ~~f~~ FIN segment in which the FIN flag is set. The FIN segment consumes one sequence number if it does not carry data

2. The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN + ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in other direction. The FIN + ACK segment consumes one sequence number if it does not carry data.

3. The client TCP sends the last segment an ACK segment, to confirm the receipt to the FIN segment from the TCP server. This segment contains the acknowledgment number, which is 1 plus the sequence number received in the FIN segment from the server.

2.3.5 Flow Control

TCP uses a sliding window to handle flow control. The sliding window protocol used by TCP, however, is something between Go-Back-N and selective Repeat sliding window

The size of the window at one end is determined by the lesser of two values: receiver window (rwnd) or congestion window (cwnd)

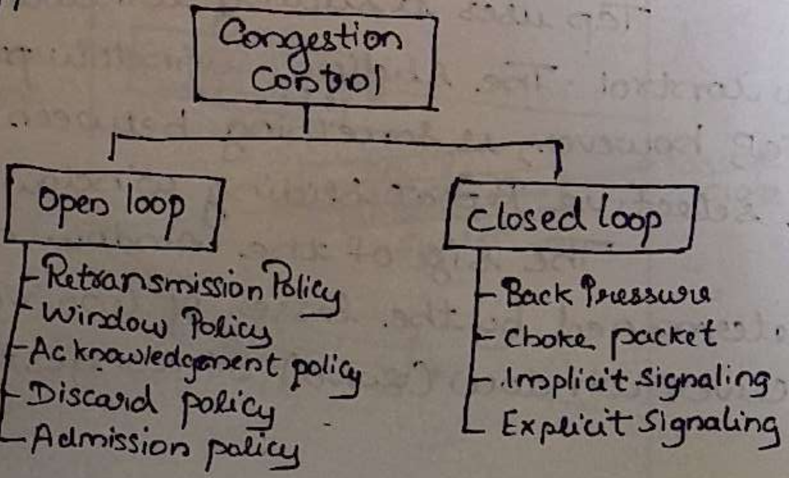
2.3.6 Error Control

TCP is a reliable transport layer protocol. This means that an application program that delivers a stream of data to TCP relies on TCP to deliver the entire stream to the application program on the other end in order, without error and without any part lost or duplicated

- Checksum: Each segment includes a checksum field which is used to check for a corrupted segment
- Acknowledgement: TCP uses acknowlegdment to confirm the receipt of data segments.
- Retransmission: The heart of the error control mechanism is the retransmission of segments.

2.4 Congestion Control

Congestion control refers to techniques and mechanisms that can either prevent congestion before it happens or remove congestion, after it has happened.



In general, we can divide congestion control mechanism into two broad categories

- Open loop congestion control (Prevention)
- closed loop congestion control (removal)

■ Open loop congestion control:

In open loop congestion control, policies are applied to prevent congestion before it happens In these mechanisms, congestion control is handled by either the source or the destination.

1) Retransmission Policy: Retransmission is Sometimes unavoidable. If the sender feels that a send packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However a good retransmission policy can prevent congestion.

2) Window policy: The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control. In the Go-Back-N window, when the timer for a packet times out, several packets may be resent

3) Acknowledgment Policy: The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.

4) Discarding policy: A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.

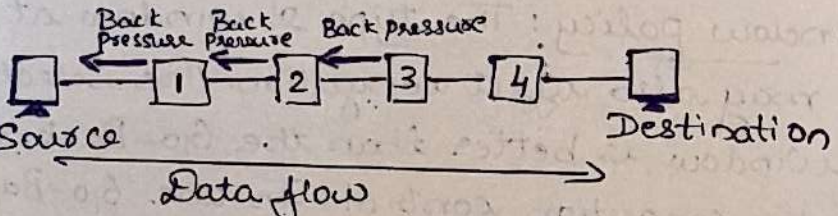
5) Admission Policy:

An admission policy, which is a quality of service mechanism, can also prevent congestion in virtual circuit networks.

■ Closed Loop Congestion Control

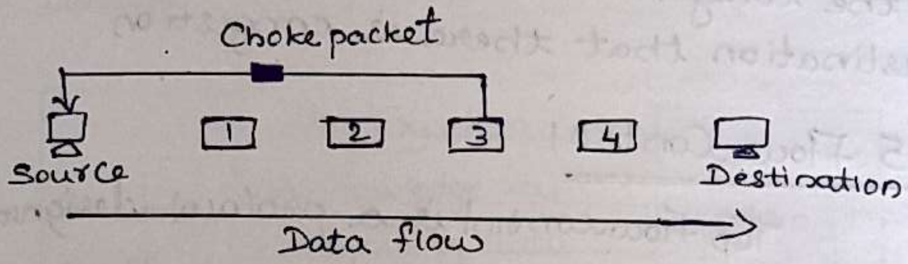
Closed loop congestion control mechanisms try to remove congestion after it occurs. Several mechanisms have been used by different protocols.

1) Backpressure: Backpressure is a node to node congestion control that start with a node and propagates, in the opposite direction of data flow, to the source. Figure shows the idea of backpressure..



Node 3 in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node 11 to slow down. Node 11, in turn, may be congested because it is slowing down the output flow of data. If node 2 is congested, it informs to node 1 to slowdown, which in turn may create congestion. If so, node 1 inform the source of data to slow down. This, in time, alleviates the congestion. The pressure on node 3 is moved backward to source to remove the congestion.

2) Choke Packet: A choke packet is a packet sent by a node to the source to inform it of congestion. In backpressure, the warning is from one node to its upstream node to reach the source station. But in choke packet method, the warning is from the router, which has encountered congestion, to the saurce station directly.



3) Implicit Signaling: In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested and the source should slow down.

4) Explicit Signaling: The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signaling method, the signal is included in the packets that carry data.

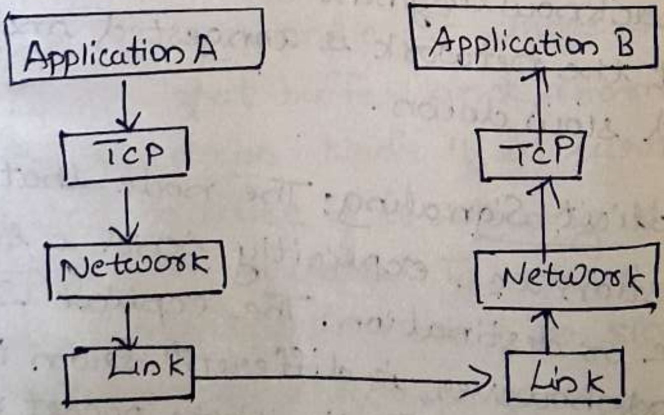
Explicit signaling can occur in either the forward or backward direction

(i) Backward Signaling: A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion

(ii) Forward Signaling: A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion

2.5 Flow Control

Tcp Flowcontrol is a protocol designed to manage the data flow between the user and the server. It ensures that there is a specific bandwidth for sending and receiving data so the data can be processed without facing any major issues. In order to achieve this, the TCP protocol uses a mechanism called the sliding window protocol.



- The Sliding window protocol:

In the sliding window protocol method, when we are establishing connection between sender and receiver, there are two buffers created. Each of these two buffers are assigned to the sender, called the sending window and to the receiver called the receiving window.

When the sender sends data to the receiver, the receiving window sends back the remaining receiving buffer space. As a result, the sender cannot send more data than the available receiving buffer space. We'll understand ~~the concept~~

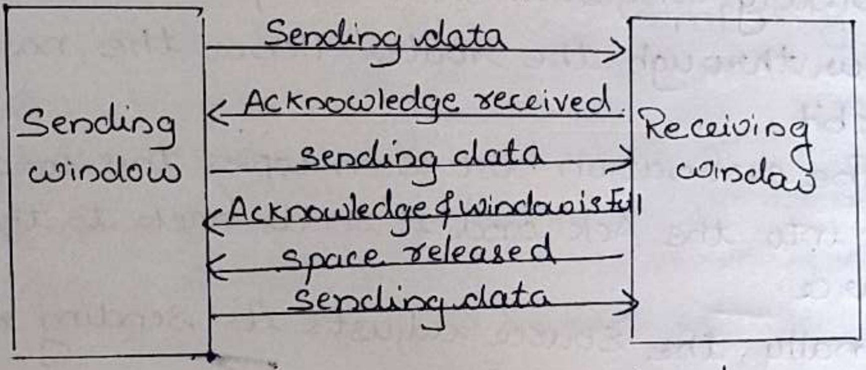


Fig: Sliding window protocol

2.6 Congestion avoidance (DECbit, RED)

To predict when congestion is about to happen and then to reduce the rate at which hosts send data just before packets start being discarded. It has three methods,

- DEC bit
- Random Early Detection (RED)
- Source based congestion control

■ DEC Bit:

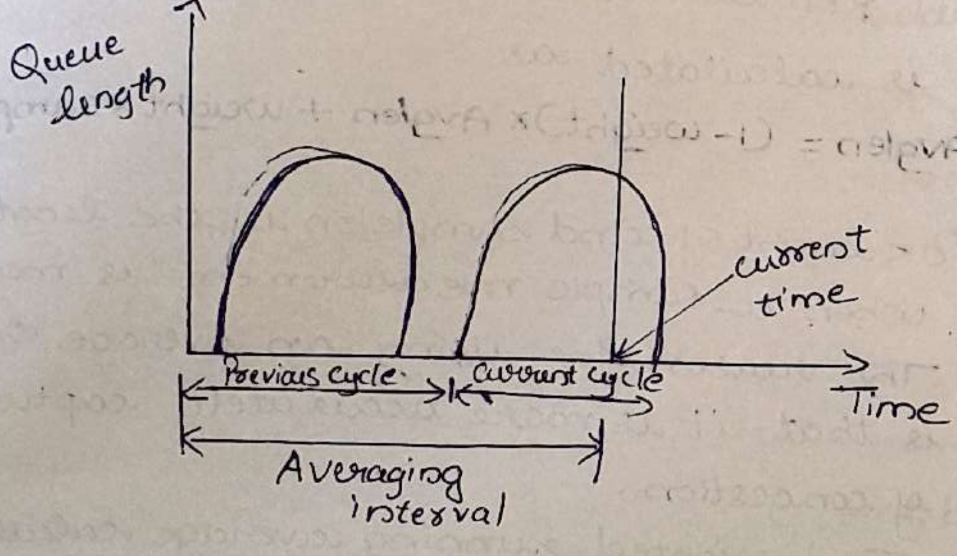
The first mechanism was developed for use on the Digital Network Architecture (DNA), a connectionless network with a connection

Oriented transport protocol. DEC bit is a TCP Congestion control technique implemented in routers to avoid congestion. Its utility is to predict possible congestion and prevent it. When a router wants to signal congestion to the sender it adds a bit in the header of packets sent.

When a packet arrives at the router the router calculates the average queue length for the last (busy + idle) period plus the current busy period. (The router is busy when it is transmitting packets and idle otherwise).

When the average queue length exceeds 1, then the router sets the congestion indication bit in the packet header of arriving packets.

This technique dynamically manages the window to avoid congestion.



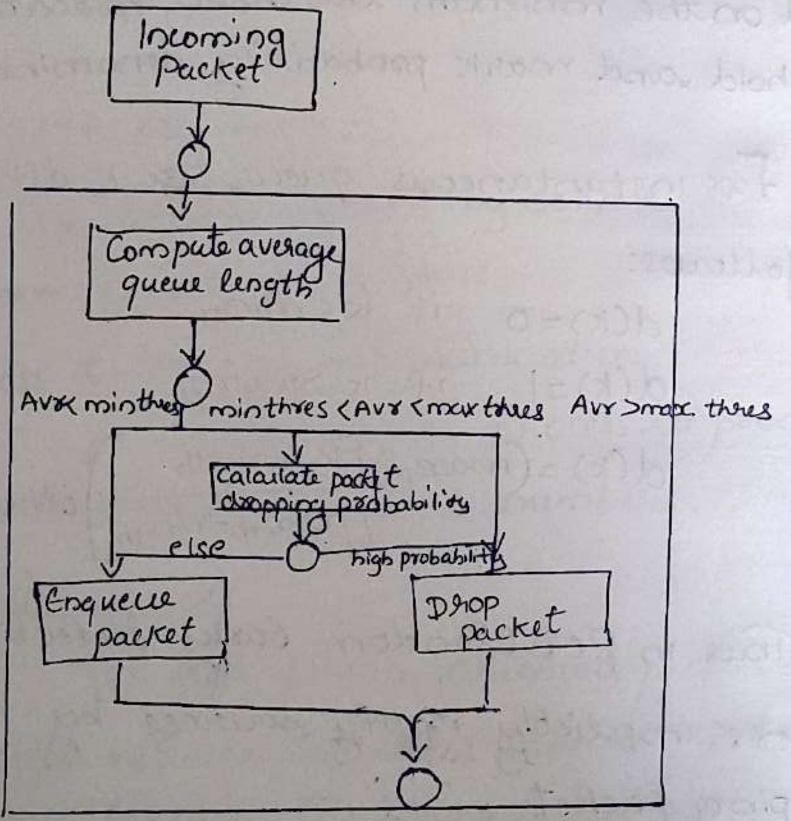
Thus In DECbit routers explicitly notify sources about congestion.

Random Early detection

→Random early detection (RED) also known as random early discard/drop is a queuing discipline for a network scheduler suited for congestion avoidance.

→RED aims to control the average queue size by informing the end host to slow down the transmission of packets. It monitors the average queue size and drops packets based on statistical probabilities.

The following process is performed:


Incoming Packet
Compute average queue length
Avr< minthres
minthres < Avr < maxthres
Avr > max. thres
Calculate packet dropping probability
else
high probability
Enqueue packet
Drop packet

1. We have an incoming packet
2. The Average queue length is computed
3. If avr < min length threshold then the packet is placed in the queue

4. If min<avr <max queue thres then check dropping probability (Pa)

1. If high probability => packet is dropped

2. If low probability => packet placed in the queue

5. If avr >max => Packet is dropped.

The rate of packet drop increases linearly as the average queue size increases until the average queue size reaches the maximum threshold.

The packet drop probability is based on the minimum threshold, maximum threshold and mark probability denominator.

For instantaneous queue size k, d(k) is as follows:

$$d(k)=0 \quad \text{if } k<min_{th}$$

$$d(k)=1 \quad \text{if } k>max_{th}$$

$$d(k)=(max_p)\left[\frac{k-min_{th}}{max_{th}-min_{th}}\right] \text{otherwise}$$

Thus in RED (Random Early Detection) routers implictly notify sources by dropping packets.

2.7 SCTP (Stream Control Transmission Protocol)

→ Stream Control transmission protocol (SCTP) is a transport layer protocol, serving similar role as TCP and UDP.

→ It is a new reliable, message oriented transport layer protocol,

→ SCTP combines the best features of UDP and TCP. It preserves the message boundaries, and at the same time, detects lost data, duplicate data and out of order data.

→ It has congestion and flow control mechanism.

2.7.1 SCTP Services:

The services offered by SCTP to the application layer processes are as follows:

1. Process to process communication:

SCTP provides process to process communication using port numbers.

2. Multistreams:

TCP is a stream oriented protocol. Each connection between TCP client and a TCP server involves one single stream. The problem with this approach is that a loss at any point in the stream blocks the delivery of rest of the data.

SCTP allows multi stream service in each connection, which is called association in SCTP terminology.

If one of the stream is blocked, the other streams can still deliver their data.

3. Multihoming:

A TCP connection involves one source and one destination IP address. This means that even if the sender or receiver is a multihomed host (connected to more than one physical address with multiple IP addresses), only one of these IP addresses per end can be utilized during the connection.

But SCTP supports multihoming service. The sending and receiving host can define multiple IP addresses in each end for an association.

In this fault tolerant approach, when one path fails another interface can be used for data delivery without interruption.

This feature is very helpful when we are sending and receiving a real time payload such as internet telephony.

4. Full duplex communication:

Like TCP, SCTP offers full duplex services in which data can flow in both directions at the same time.

Each SCTP has a sending and receiving buffer and packets are sent in both directions

5. Connection Oriented Service

In SCTP, a connection is called an association. When a process at site A wants to send and receive data from another processes at site B, the following occurs:

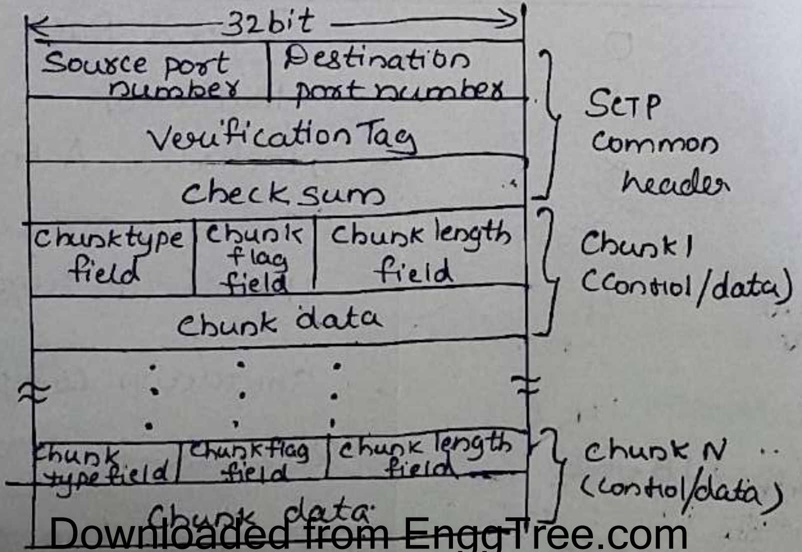
1. The two SCTPs establish an association between each other.
2. Data are exchanged in both directions.
3. The association is terminated.

6. Reliable Service :

Like TCP SCTP is a reliable transport protocol. It uses an acknowledgement mechanism to check the safe and sound arrival of data.

2.7.2 SCTP Packet format:

SCTP transmit data in the form of messages and each message contains one or more packets. The control chunks come before data chunks.



- General header

A SCTP packet contains a common header and one or more chunks. The SCTP common header contains the following information.

1. Source and destination port numbers to enable multiplexing of different associations at the same address.

2. A 32 bit verification tag that guards against the insertion of an out-of-date or false message into the SCTP association.

3. A 32 bit checksum for error detection

- Chunk Layout

1. A chunk can be either a control chunk or a data chunk. A control chunk incorporates different flags and parameters. Data chunk incorporates flags to control segmentation and reassembly

2. Chunk type field identifies the type of information contained in the chunk data field. SCTP consists of one Data chunk and 12 control chunks.

Chunk number	Chunk name
0	Payload Data
1	Initiation
2	Initiation Acknowledgement
3	Selective acknowledgement
4	Heartbeat request
⋮	⋮
14	Shutdown complete
15-62	Reserved for IETF
⋮	⋮
255	IETF-defined chunk extensions

3. Chunk length field represents the size of the fields chunk type, chunk flag, chunk length and chunk value in bytes.

4. chunk data are used to send actual data through the stream.

2.8 Quality of Services

Quality of service (Qos) is basically the ability to provide different priority to different applications in order to guarantee a certain level of performance to the flow of data.

Qos is basically the overall performance of the computer network.

Given below are four types of characteristics that are mainly attributed to the flow and these are as follows:

- Reliability
- Delay
- Jitter
- Bandwidth

→ Reliability:

It is one of the main characteristics that the flow needs. If there is a lack of reliability then it simply means losing any packet or losing an acknowledgement due to which retransmission is needed. Reliability becomes more important for electronic mail, file transfer & for internet access

→ Delay:

Another characteristic of the flow is the delay in transmission between the source and destination. During audio conferencing, telephony, video conferencing there should be a minimum delay.

→ Jitter:

It is basically the variation in the delay for packets that belongs to the same flow. Thus jitter is basically the variation in the packet delay. Higher the value of jitter means there is a large delay and the low jitter means the variation is small.

→ Bandwidth:

The different application need different bandwidth

- Types of Quality of Service Solutions:

1. Stateless Solution: Here, the server is not required to keep or store the server information or session details to itself. The routers maintain no fine grained state about traffic also it has weak services as there is no guarantee about the kind of performance delay. In the stateless solution, the server and client are loosely coupled

2. Stateful Solution: Here, the server is required to maintain the current state and session information, the routers maintain perflow state as the flow is very important in providing the Quality of Service which is providing powerful services such as guaranteed services. Here the server and client are tightly bounded.

- Quality of service parameters

QoS can be measured quantitatively by using ~~serv~~ several parameters:

→ packet loss
→ Jitter
→ Latency
→ Bandwidth

- Techniques to improve QoS

Generally, there are four techniques to improve Quality of service.

→ Scheduling
→ Traffic Shaping
→ Resource Reservation
→ Admission control

- Scheduling:

Packets from different flows arrive at a switch or router for processing. A good scheduling technique treats the different flows in a fair and appropriate manner.

Several Scheduling techniques are designed to improve the quality of service. They are

- FIFO Queuing
- Priority queuing
- Weighted fair queuing

- Traffic Shaping

It is a mechanism to control the amount and the rate of the traffic sent to the network. Two techniques can shape traffic: leaky bucket
token bucket

- Resource Reservation

A flow of data needs resources such as a buffer, bandwidth, cpu time and so on. The quality of service is improved if these resources are reserved beforehand.

- Admission control

Admission control refers to the mechanism used by a router or a switch to accept or reject a flow based on predefined parameters called flow specifications. Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity can handle new flow.

Question bank

1. what are the advantages of using UDP over TCP (Dec10

2. Give the approaches to improve the QoS. (May 11, Dec 17)

1. Fine grained approaches, which provide QoS to individual applications or flows.

2. Coarse-grained approaches, which provide QoS to large classes of data traffic

3. what is TCP ? (Dec 11)

4. Define congestion. (Dec 11)

5 What do you mean by slow start in TCP congestion? (May 16)

Slow start is part of the congestion control stratergy used by TCP. Slowstart is used in conjunction with other algorithms to avoid sending more data than the network is capable of transmitting.

6. what do you mean by QoS ? (Dec 14, 15, 16, 18)

7. Suppose TCP operates over a 1-Gbps link, utilizing the full bandwidth continuously. How long will it take for sequence numbers to wrap around, completely? Suppose an added 32 bit timestamp field increments, 1000 times during this wrap around time, how long will it take for the, timestamp field to wraparound? (may 13, 18)

TCP Advertised Window is 16 bits,

Sequence number is 32 bit

So there will be 2^{32} bytes on the fly in this 1 Gbps link

The corresponding transmission time is

$2^{32} \times 8 / 1 \times 10^{9} = 34{\cdot}36$ sec

So it will take 34·36 sec to wrap around the sequence number

Each Increment of time stamp $= 34{\cdot}36$ sec$/100$

$= 34{\cdot}36$ ms

So the total time can be expressed by this timestamp $= 34{\cdot}36 \times 10^{-3} \times 2^{32}$ sec

$= 1{\cdot}48 \times 10^{8}$ sec $= 4{\cdot}68$ year

So by adding this timestamp, it will take 4·68 year to wrap around the sequence number.

8. Differentiate between delay and jitter? (Dec 13)

9. List some ways to deal with congestion?

10. Differentiate UDP and TCP (may 14, 16)

11. what are the services provided by transport layer protocol

12. Define congestion control

Unit III Network Layer

Switching: Packet switching - Internet Protocol - IPV4 - IP Addressing - Subnetting - IPV6, ARP, RARP, ICMP, DHCP.

3.1 Network Layer:

Network Layer is the third layer of the OSI model. It handles the service requests from the transport layer and further forwards the service request to the data link layer. The network layer translates the logical addresses into physical addresses.

It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.

The main role of the network layer is to move the packets from sending host to the receiving host.

3.1.1 Network Layer services

Main task of the network layer is to move packets from the source host to the destination host. Network layer services are packetizing, routing & forwarding and other services.

- Packetizing: Encapsulating the payload in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination called packetizing.

- Routing: Network layer is responsible for finding the best One route from the source to the destination is called routing.
- Forwarding: Forwarding refers to the way apacket is delivered to the next node.
- Other services expected from the network layer is error control
  flow control
  congestion control
  Quality of service
  Security

3.2 Switching

A router infact is a switch that creates a connection between an input port and an output port, just as an electrical switch connects the input to the output to let electricity flow.

Switching techniques are divided into two broad categories: circuit switching and packet switching, but only packet switching is used at the network layer because the unit of data at this layer is a packet.

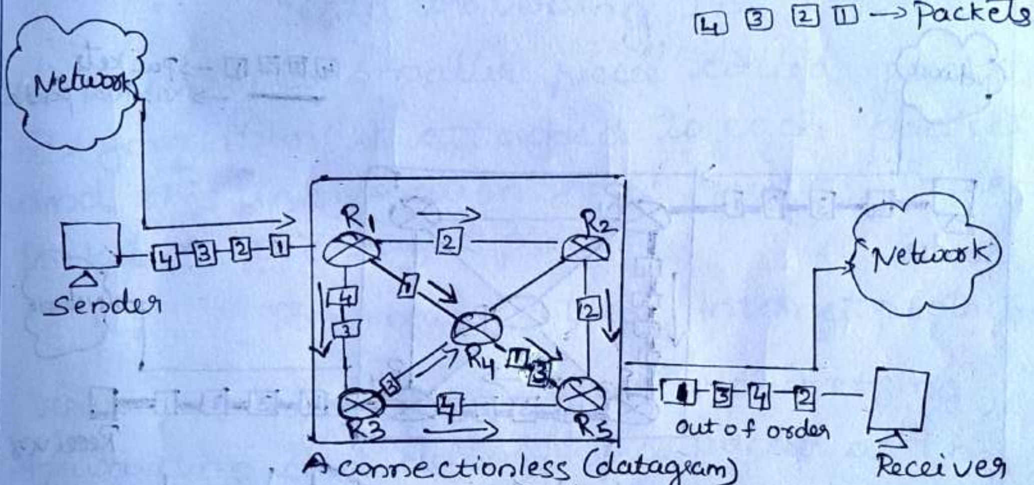
Packet switched network use two different approaches to route the packets:

- The datagram approach
- The virtual circuit approach

• Datagram Approach: Connectionless Service

When the network layer provides a connectionless service, each packet traveling in the internet is an independent entity; there is no relationship between packets belonging to the same message. The switches in this type of network are called routers.

A packet may be followed by a packet coming from the same or from a different source.



A connectionless (datagram) packet switched network

Fig: A connectionless packet Switched Network

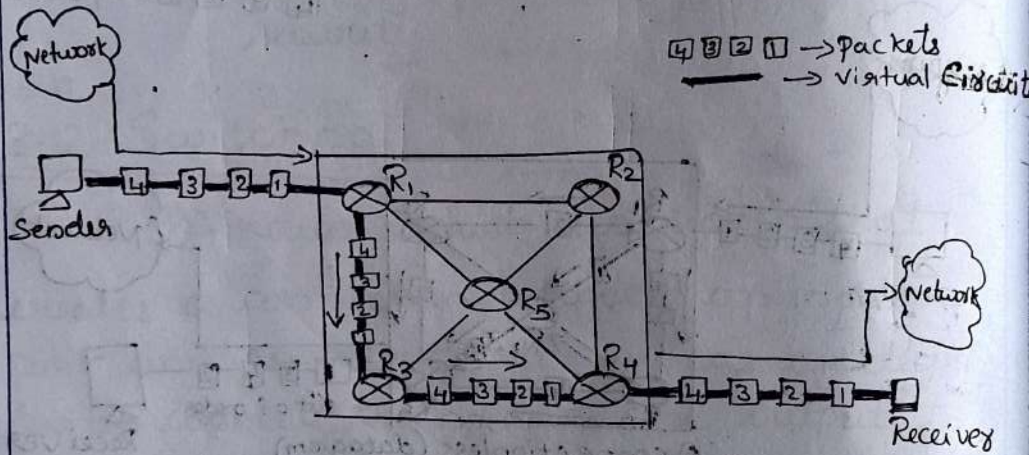
Each packet is routed based on the information contained in its header: source and destination addresses.

The router in this case routes the packet based only on the destination address. The router in this case routes the packet based only on the destination address. The source address may be used to send an error message to the source if the packet is discarded

- **Virtual-Circuit approach: connection oriented service:**

In connection-oriented service, there is a relationship between all packets belonging to a message. Before all datagrams in a message can be sent, a virtual connection should be setup to define the path for the datagrams. After connection setup, the datagrams can all follow the same path.

In this type, not only must the packet contain the source and destination addresses, it must also contain a flow label.



Each packet is forwarded based on the label in the packet. In this case, the forwarding decision is based on the value of the label.

To create a connection oriented service, a three phase process is used

- setup
- data transfer
- Teardown phase

In setup phase, the source and destination addresses of the sender and receiver are used to make table entries for the connection oriented Service

In teardown phase, the source and destination inform the router to delete the corresponding entiries.

Data transfer occurs between these two phases.

3.3 Internet Protocol

Internet protocol (IP) is a protocol or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.

Data traversing the internet is divided into smaller pieces called packets. IP information is attached to each packet and this information helps routers to send packets to the right place.

The main protocol, Internet protocol version 4 (IPv4) is responsible for packetizing, forwarding and delivery of a packet at the network layer.

3.3.1 IPV4

This protocol has the responsibility of identifying host based upon their logical addresses and to route data among them over the underlying network. Internet protocol version 4 uses 32 bit logical address

- IPv4 - Packet structure:

Internet protocol being a layer 3 protocol takes data segments from transport layer and divides it into packets.

(b)

IP Packet encapsulates data unit received from above layer and add to its own header information.

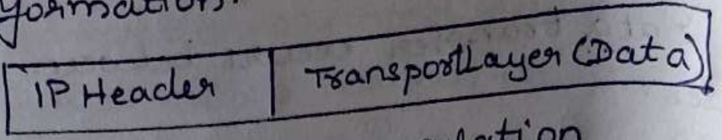
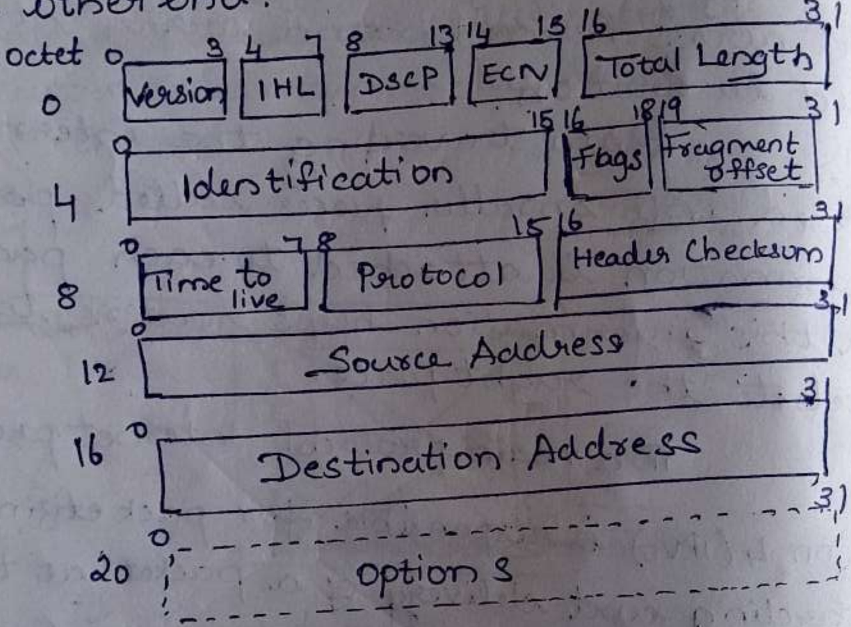


Fig: IP Encapsulation

The encapsulated data is referred to as payload. IP header contains all the necessary information to deliver the packet at the other end.



✓ Version — Version no. of internet protocol used.

✓ IHL — Internet Header Length; Length of entire IP header.

✓ DSCP — Differentiated Services Code Point; this is type of service.

✓ ECN — Explicit Congestion Notification: it carries information about the congestion seen in the route.

✓ Total Length — Length of entire IP packet (including IP header and IP Payload)

✓ Identification – If IP Packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.

✓ Flags – As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not.

✓ Fragment offset – This offset tells the exact position of the fragment in the original IP Packet.

✓ Time to Live – To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.

✓ Protocol – Tells the network layer at the destination host, to which protocol this packet belongs to, ie the next level protocol. Eg: Protocol number of TCP is 6 and UDP is 17

✓ Header checksum – This field is used to keep checksum value of entire header which is then used to check if the packet is received error free.

✓ Source Address – 32 bit address of the sender of the Packet.

✓ Destination Address – 32 bit address of the receiver of the packet.

✓ Options – This is optional field, which is used if the value of IHL is greater than 5.

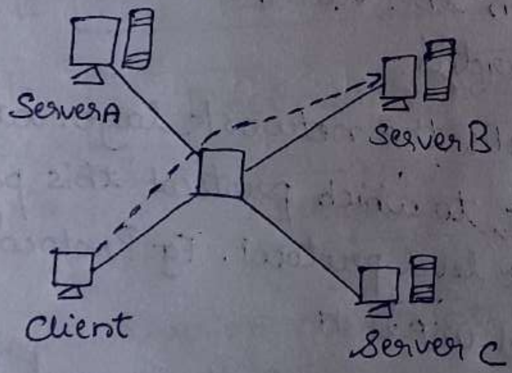
• IPV4 – Addressing:

IPV4 supports three different types of addressing modes.

- Unicast Addressing mode
- Broadcast Addressing mode
- Multicast Addressing mode

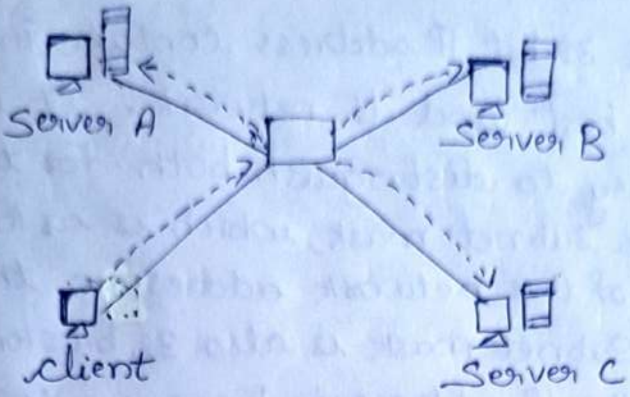
Unicast Addressing mode:

In this mode, data is sent only to one destined host. The destination address field contains 32 bit IP address of the destination host. Here the client sends data to the targeted server.



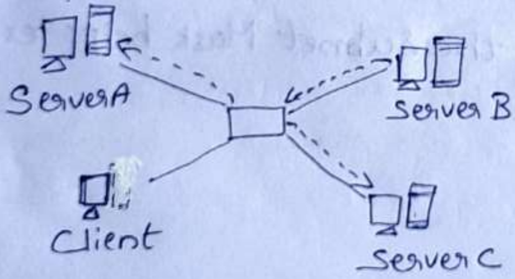
Broadcast Addressing mode:

In this mode, the packet is addressed to all the hosts in a network segment. The destination address field contains a special broadcast address ie, 255.255.255.255. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers.



Multicast Addressing Mode:

This mode is a mix of the previous two modes ie the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the destination address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.



Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the network number which represents the network and one IP address reserved for the broadcast address, which represents all the hosts in that network.

Hierarchical Addressing Scheme:

IPV$_4$ uses hierarchial addressing scheme. An IP address, which is 32 bits in length is divided into two or three parts as depicted -

8bits	8bits	8bits	8bits
Network	Network	Sub-Network	Host

Subnet Mask :

The 32 bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this; routers use Subnet Mask, which is as long as the size of the network address in the IP address.

Subnet Mask is also 32 bits long. if the IP address in binary is ANDed with its subnet mask, the result yields the network address. For example, say the IP address is 192.168.1.152 and the subnet mask is 255.255.255.0 then.

IP	192.168.1.152	11000000	10101000	00000001	10011000	ANDed
Mask	255.255.255.0	11111111	11111111	11111111	00000000	
Network	192.168.1.0	11000000	10101000	00000001	00000000	Result

This way the subnet mask helps extract the network ID and the host from an IP address. It can be identified now that 192.168.1.0 is the network number and 192.168.1.152 is the host on that network.

Binary Representation :

The positional value method is the simplest form of converting binary from decimal value. IP address is 32 bit value which is divided into 4 octets. A binary octet contains 8 bits and the value of ~~t~~ each bit can be determined by the position of bit value 1 in the octet.

MSB	8th	7th	6th	5th	4th	3rd	2nd	1st	LSB
	1	1	1	1	1	1	1	1	
Positional Value	128	64	32	16	8	4	2	1	

Positional value of bits is determined by 2 raised to power (position - 1), that is the value of a bit 1 at position 6 is 2^(6-1) that is 2^5 that is 32. The total value of the octet is determined by adding up the positional value of bits. The value of 11000000 is 128+64 = 192. Some examples are shown in the table below -

128	64	32	16	8	4	2	1	Value
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	0	2
0	0	0	0	0	0	1	1	3
0	0	0	0	0	1	0	0	4
0	0	0	0	0	1	0	1	5
0	0	0	0	0	1	1	0	6
			⋮					
1	1	1	1	1	1	1	1	255

- IPV$_4$ - Address Classes:

Internet protocol hierarchy contains several classes of IP addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPV$_4$ addressing system is divided into five classes of IP addresses. All the five classes are identified by the first octet of IP Address.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP address.

1st octet   2nd octet   3rd octet   4th octet

11000000 · 10101000 · 00000001 · 10011000

192 · 168 · 1 · 152

The number of networks and the number of host per class can be derived by this formula

Number of networks = 2^network_bits

Number of host /network = 2^host_bits - 2

When calculating hosts IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, ie. the first IP of a network is network number and the last IP is reserved for broadcast IP.

→ Class A Address:

The first bit of the first octet is always set to 0. Thus the first octet ranges from 1-127 ie 00000001 - 01111111
1 - 127.

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for class A IP address is 255.0.0.0 which implies that class A addressing can have 126 networks (2^7-2) and 16777214 hosts ($2^{24}-2$).

Class A IP address format is thus:

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

→ Class B Address:

An IP address which belongs to class B has the first two bits in the first octet set to 10 ie

10000000 - 1011111

128 - 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for class B is 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 ($2^{16}-2$) Host addresses

Class B IP address format is

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

→ Class C Address:

The first octet of class c IP address has its first 3 bits set to 110 that is:

11000000 - 1101111

192 - 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for class C is 255.265.255.x

Class C gives 2097152 (2^{21}) Network addresses and 254 ($2^{8}-2$) Host addresses.

Class C IP address format is:

110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

→ Class D Address:

Very first four bits of the first octet in class D IP addresses are set to 1110, giving a range of -

11100000 - 11101111

224 - 239

Class D has IP address range from 224.0.0.0 to 239.255.255.255. class D is reserved for multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address and class D does not have any subnet mask.

→ Class E Address:

This IP class is reserved for experimental purposes only for study. IP addresses in this class ranges for 240.0.0.0 to 255.255.255.254 Like Class D, this class too is not equipped with any subnet mask.

3.4 Subnetting:

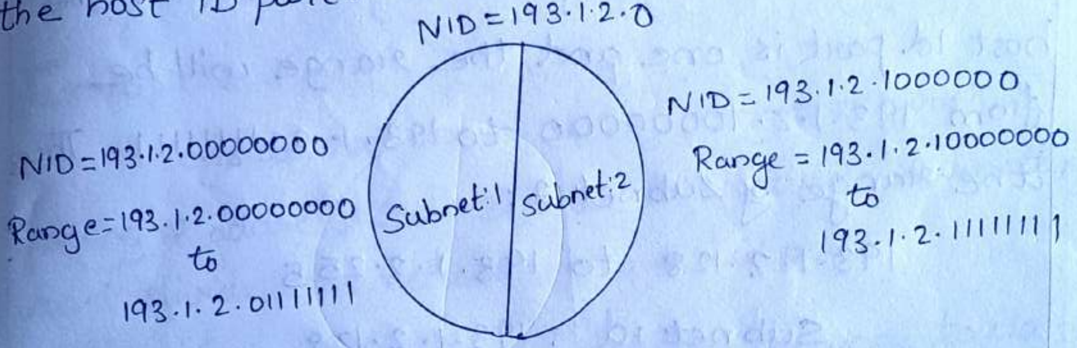
Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of networks and prefixed number of hosts per network.

Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more networks per IP class.

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 subnetworks which provide better network management capabilities.

"When a bigger network is divided into smaller networks, to maintain security then that is known as subnetting".

To divide a network into two parts, you need to choose one bit for each subnet from the host ID part.



In the above diagram, there are two subnets.

Note: It is a class C IP address, there are 24bits in the network id part and 8bits in the host Id part"

Subnetting for a network should be done in such a way that it does not affect the network bits. In class c the first 3 octets are network bits so it remains as it is.

→For subnet 1:

The first bit which is chosen from the host id part is zero and the range will be from

193.1.2.00000000 to 193.1.2.01111111 expect for the first bit which is chosen zero for subnet Id part. Thus the range of subnet 1:

193.1.2.0 to 193.1.2.127

∴ Subnet Id of subnet 1 is : 193.1.2.0

Direct Broadcast Id is : 193.1.2.127

Total number of host : 126 (out of 128 2 id's are used for subnet id of Direct broadcast id)

Subnet mask : 255.255.255.128

→ For Subnet 2: The first bit chosen from the host Id part is one and the range will be from 193.1.2.10000000 to 193.1.2.11111111. Thus the range of subnet 2:

193.1.2.128 to 193.1.2.255

Subnet id : 193.1.2.128

Direct broadcast ID : 193.1.2.255

Total number of host : 126

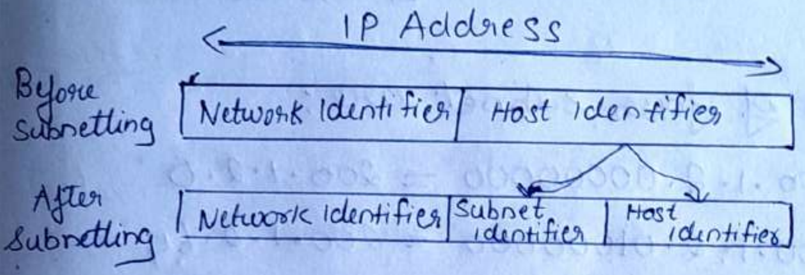
Subnet mask : 255.255.255.192

Finally after using the subnetting the total number of usable host are reduced from 254 to 252.

To divide a network into four (2^2) parts you need to choose two bits from the host Id part for each subnet ie 00, 01, 10, 11

To divide a network into eight (2^3) parts you need to choose three bits from the host id part for each subnet ie 000, 001, 010, 011, 100, 101, 110, 111.

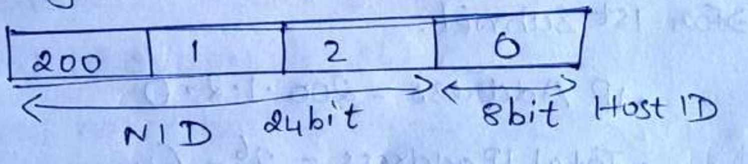
If the total number of subnet in a network increases the total number of usable hosts decreases.



Example 2:

Consider we have a big single network having IP address 200.1.2.0 we want to do subnetting and divide this network into 4 subnets.

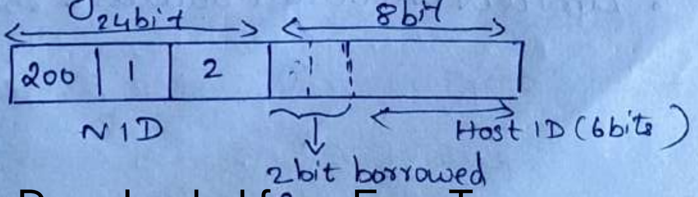
Clearly the given network belongs to class C.



For creating four subnets and to represent their subnets ID, we require 2 bits.

So,

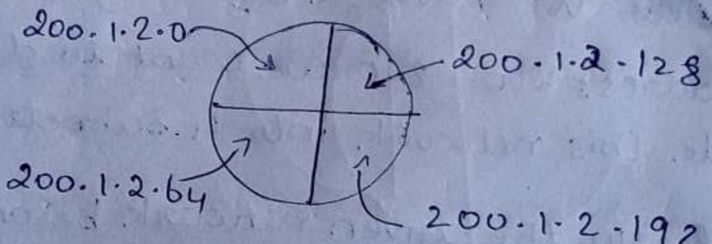
- We borrow two bits from the Host ID part
- After borrowing two bits, Host ID part remains with only 6 bits



- If borrowed bits = 00, then it represents 1st subnet
- If borrowed bits = 01, then it represents 2nd subnet.
- If borrowed bits = 10, then it represents 3rd subnet
- If borrowed bits = 11, then it represents 4th subnet

IP address of four subnet are:

- 200.1.2.00000000 = 200.1.2.0
- 200.1.2.01000000 = 200.1.2.64
- 200.1.2.10000000 = 200.1.2.128
- 200.1.2.11000000 = 200.1.2.192



→ For 1st Subnet:

- IP Address = 200.1.2.0
- Total IP address = $2^6 = 64$
- Total number of host = 64 − 2 = 62
- Range of IP address = 200.1.2.00000000 to 200.1.2.00111111
  ie 200.1.2.0 to 200.1.2.63
- Direct broadcast address = 200.1.2.63
- Limited broadcast address = 255.255.255.255

→ for 2nd Subnet

- IP address = 200.1.2.64
- Total IP address = $2^6 = 64$
- Total no: of host = 64-2 = 62
- Range = 200.1.2.01000000 to 200.1.2.01111111
  ie; 200.1.2.64 to 200.1.2.127
- Direct broadcast address = 200.1.2.127
- Limited broadcast address = 255.255.255.255

→ for 3rd Subnet

- IP address = 200.1.2.128
- Total IP address = $2^6 = 64$
- Total no: of host = 64-2 = 62
- Range = 200.1.2.10000000 to 200.1.2.10111111
  ie 200.1.2.128 to 200.1.2.191
- Direct broadcast address = 200.1.2.191
- Limited broadcast address = 255.255.255.255

→ for 4th Subnet

- IP address = 200.1.2.192
- Total IP address = $2^6 = 64$
- Total no: of host = 64-2 = 62
- Range = 200.1.2.11000000 to 200.1.2.11111111
  ie 200.1.2.192 to 200.1.2.255
- Direct broadcast address = 200.1.2.255
- Limited broadcast address = 255.255.255.255

Disadvantages of Subnetting.

1. Subnetting leads to loss of IP addresses
2. Subnetting leads to complicated Communication process.

3.5 IPV6

IPV6 is a network layer protocol that allows communication to take place over the network.

IPV6 is designed to overcome the shortfalls of the IPV4

Some advantages of IPV6 over IPV4 are mentioned below:

1. Addressspace : IPV6 has a 128 bit long address which is larger than IPV4
2. Header format: IPV6 has a new header format in which options are separated from the base header and inserted between the base header and upper layer data.
3. Extension: IPV6 is designed to allow the extension of the protocol, if required for new applications.
4. Security: Encryption and authentication mechanism provides confidentiality and integrity to the packets in IPV6

- IPV6 Addresses

A new notation has been devised for writing 16 byte addresses. They are written as eight groups of four hexadecimal digits with colons between the group like this

8000:0000:0000:0000:0123:4567:89AB:CDEF

Leading zeros within a group can be omitted so 0123 can be written as 123.

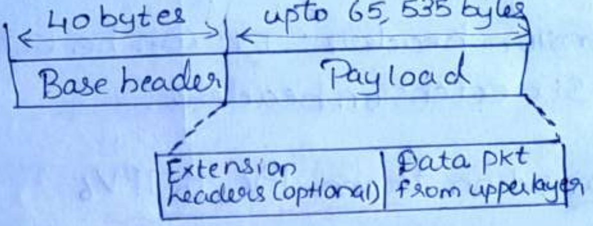
One or more groups of 16 zerobits can be replaced by a pair of colons. The address new becomes 8000::123:4567:89AB:CDEF

IPV6 Packet format :

Each packet is composed of a mandatory base header followed by the payload.

The payload consists of two parts optional extension headers and data from an upper layer.

The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65, 535 bytes of Information



-> Base header

Version	Priority	Flow label
Payload length	Next header	Hop Limit
Source address		
Destination address		
Extension headers !		

Version : This 4bit field defines the version number of the IP

Priority : This 4bit priority field defines the priority of the packet.

Flowlabel : The flow label is a 3byte (24bit) field used for control the flow of data

Payload length : The 2byte payload length field defines the length of the IP datagram excluding the base header

Next header : The next header is an 8bit field defining the header that follows the base header in the datagram.

Hop limit: This 8bit hop limit field used to indicati life time of the packet

Source address: The source address field is a 16byte (128 bit) internet address that identifies the original source of the datagram

Destination address: The destination address field is a 16 byte (128bit) internet address that usually identifies the final destination of the datagram.

Extension headers: It can be extended upto six extension headers.

- Transition from IPV_4 to IPV_6

Three strategies have been invented by IETF (Internet Engineering Task force) to help the transition:

1. Dual Stack

The host should run IPV_4 and IPV_6 simultaneously until the entire internet uses IPV_6. The source host queries the DNS to determine which version can be used at the time of sending a packet to destination. If DNS returns an IPV6 address, the source host sends an IPV6 Packet

2. Tunneling

When two computers uses IPV6 and want to communicate with each other and the packet passes through a region that uses IPV_4, it is called tunneling. The IPV_6 Packet is encapsulated in an IPV_4 packet, when it enters the region. It leaves the capsule when it exits the region

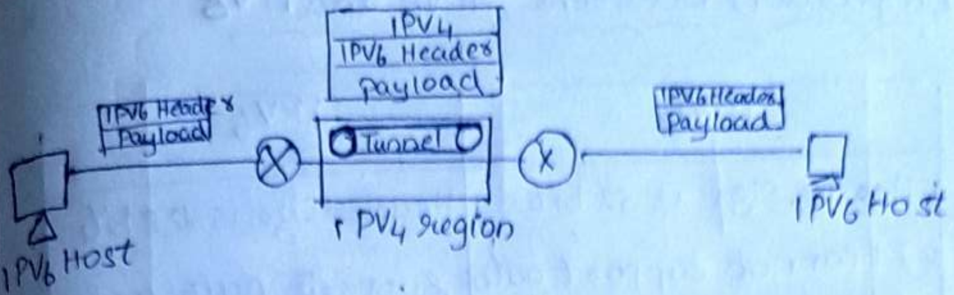
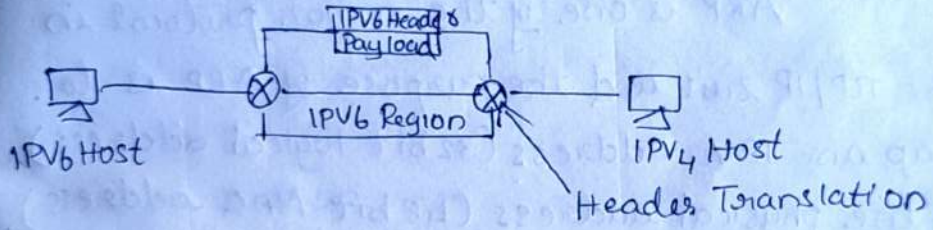


Fig: Tunneling

3. Header Translation:

It is used when some of the systems use the IPV4 and the sender wants to use IPV6 but the receiver does not understand IPV6.

· The header format should be totally changed through header translation. The header of the IPV6 Packet is converted to an IPV4 header



Header Translation procedure

1. Change the IPV6 mapped address to an IPV4 address by extracting the rightmost 32 bits
2. Discard the value of IPV6 Priority field
3. Set the type of service field in IPV4 to be zero
4. Calculate the checksum for IPV4 and insert in the corresponding field.
5. Ignore the IPV6 flow label
6. Convert the compatible extension headers to options and insert them in the IPV4 header
7. Calculate the length of IPV4 header and insert it into the corresponding field
8. Eventually, compute the total length of the IPV4 Packet and insert it into the corresponding field.

Comparison between IPV4 and IPV6

IPV4	IPV6
1. Header Size is 32 bits	Header Size is 128 bits
2. It cannot support auto configuration	Supports auto configuration
3. Cannot support real time application	Supports real time application
4. No security at network layer	Provides security at network layer
5. Throughput and delay is more	Throughpul and delay is less

3.6 ARP (Address Resolution Protocol)

ARP is one of the major protocol in the TCP/IP suit and the purpose of ARP is to map an IPV4 address (32 bit logical address) to the physical address (48 bit MAC address)

Network applications at the application layer use IPV4 address to communicate with another device. But at the data link layer, the addressing is MAC address and this address is burned into network card permanently.

The purpose of ARP is to find out the MAC address of a device in your LAN for the corresponding IPV4 address, which network application is trying to communicate

Types of mapping

- static mapping
- Dynamic mapping

- **Static mapping**

Static mapping means creating a table that associates a logical address with a physical address. This table is stored in each machine on the network. Each machine that knows, for example, the IP address of another machine but not its physical address can look it up in the table.

This has some limitations because physical addresses may change in the following ways:

1. A machine could change its NIC, resulting in a new physical address
2. In some LANs the physical address changes every time the computer is turned on.
3. A mobile computer can move from one physical network to another, resulting in a change in its physical address.

To implement these changes, a static mapping table must be updated periodically. This overhead could affect network performance.

- **Dynamic Mapping**

Here, each time a machine knowns the logical address of another machine, it can use a protocol to find the physical address. Two protocols have been designed to perform dynamic mapping

→ ARP (Address resolution Protocol)

→ RARP (Reverse Address Resolution Protocol)

ARP maps a logical address to a physical address

RARP maps a physical address to a logical address.

ARP Packet format

Hardware Type		Protocol type
Hardware Length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (for example, 6 bytes for Ethernet)		
Sender protocol address (for example, 4 bytes for IP)		
Target Hardware address (for example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address For example, 4 bytes for IP		

The fields in the Address resolution Protocol (ARP) message format are:

Hardware Type: Specifies the type of hardware used for the local network transmitting the ARP message. Ethernet is the common hardwa Type and the value for ethernet is 1. The size of this field in 2bytes.

Protocol type: Each protocol is assigned a number used in this field. IPv4 is 2048 (0x0800 in Hexa)

Hardware Address Length: is length in bytes a hardware (MAC) address. Ethernet MAC addresses are 6 bytes long.

Protocol Address Length: Length in bytes of a logical address (IPv4 address). IPv4 addresses are 4 bytes long.

Operation: Specifies the nature of the ARP message for 1. ARP request and 2. ARP reply.

Sender Hardware Address: address of the device sending the message.

Sender protocol address: The protocol address (IPV4 address) of the device sending the message.

Target Hardware Address: and MAC address of the Intended receiver. This field is ignored in requests.

Target Protocol Address: The protocol address (IPV4 address) of the intended receiver

- Encapsulation

An ARP packet is encapsulated directly into a data link frame. For example, in figure an ARP packet is encapsulated in an ethernet frame. The type field indicates that the data carried by the frame is an ARP Packet

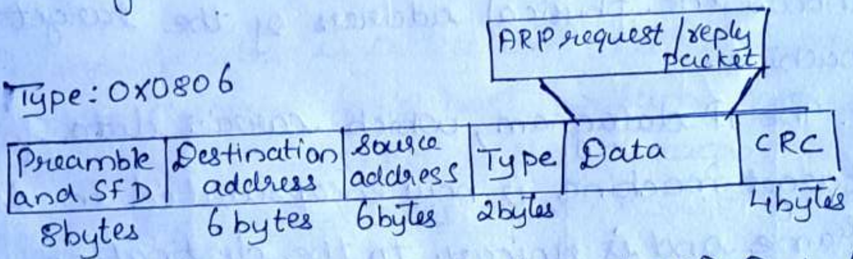


Fig: Encapsulation of ARP Packet

- Operation:

There are seven steps involved in an ARP process:

1. The Sender knows the IP address of the target.
2. IP Asks ARP to create as ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field is filled with 0's .

3. The message is passed to the data link layer where it is encapsulated in a frame using the physical address of the sender as the source address and the physical broadcast address as the destination address.

4. Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes the IP address.

5. The target machine replies with an ARP reply message that contains its physical address. The message is unicast

6. The sender receives the reply message. It now knows the physical address of the target machine.

7. The IP datagram, which carries data for the target machine, is now encapsulated in ~~the~~ a frame and is unicast to the destination.

■ Four Different cases:

The following are four different cases in which the services of ARP can be used.

Case 1: The sender is a host and wants to send a packet to another host on the same network. In this case, the logical address that must be mapped to a physical address is the destination IP address in the datagram header.

Case 2: The sender is a host and wants to send a packet to another host on another network. In this case, the host looks at its routing table and finds the IP address of the next hop (router) for this destination. If it does not have a routing table, it looks for the IP address of the default router. The IP address of the router becomes the logical address that must be mapped to a physical address.

Case 3: The sender is a router that has received a datagram destined for a host on another network. It checks its routing table and finds the IP address of next router. The IP address of the next router becomes the logical address that must be mapped to a physical address.

Case 4: The sender is a router that has received a datagram destined for a host in same network. The destination IP address of the datagram becomes the logical address that must be mapped to a physical address.

3.7 RARP (Reverse Address Resolution Protocol)

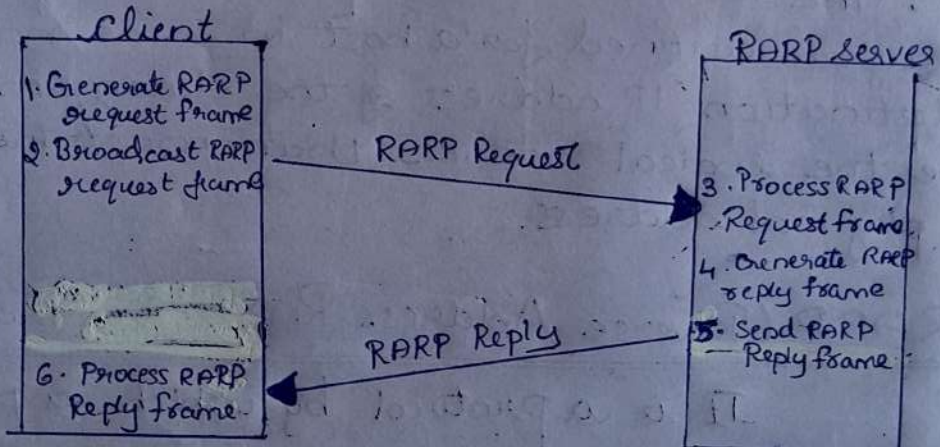
It is a protocol by which a physical machine in a local area network can request to learn its IP address from a gate way server's Address Resolution Protocol (ARP) table or cache.

A network administrator creates a table in a local area networks gateway router that maps the physical machine (MAC address) to corresponding Internet protocol addresses.

When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

There are four types of arp messages that may be sent by the arp protocol. These are identified by four values in the operation field of an arp message. The type of message are:

1. ARP request
2. ARP reply
3. RARP request
4. RARP reply



Client
1. Generate RARP request frame
2. Broadcast RARP request frame
6. Process RARP Reply frame
RARP Request
RARP Reply
RARP Server
3. Process RARP Request frame
4. Generate RARP reply frame
5. Send RARP Reply frame

1. Source device generates RARP request message:

The source device generates an RARP request message. Thus it uses the value 3 for the opcode in the message. It puts its own data link layer address as both the sender hardware address and also

Target hardware address. It leaves both the sender protocol address and the target protocol address blank, since it doesnt know either.

2. Source device broadcast RARP request message:

The source broadcasts the ARP request message on the local network.

3. Local Devices process RARP request message

The message is received by each device on the local network and processed. Devices that are not configured to act as RARP servers ignore the message.

4. RARP server generates RARP reply message

Any device on the network that is setup to act as an RARP server responds to the broadcast from the source device. It generates an RARP reply using an Opcode value of 4

5. RARP server sends RARP reply message:

The RARP server sends the RARP reply message unicast to the device looking to be configured.

6. Source Device processes RARP reply message:

The source device processes the reply from the RARP server. It then configures itself using the IPaddress in the target protocol address supplied by the RARP server. It is possible that more than one RARP server may respond to any request, if two or more are configured on any local network. The source device will typically use the first reply and discards the others.

3.7 ICMP (Internet Control Message Protocol)

The ICMP is the protocol that handles error and other control message. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. ICMP messages are encapsulated by IP Packets.

3.7.1 Message Types:

All ICMP messages fall in the following classes: 1. Error reporting
2. Query

Error reporting messages report problems that a router or a host may encounter when it processes an IP Packet.

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

3.7.2 Message Format:

0 8 16 31

Type	code	checksum
Reset of the header		
IP header and 64 bits of original datagram		

The above figure shows the basic error message format. An ICMP message is encapsulated into the data field of an IP Packet. An ICMP header is 8 bytes long and a variable size data section

1. Type: It is a 8bit field identifies the type of the message.

2. Code: Size of the code field is 8 bits. It provides the information of the message type

3. Checksum: This 16 bit field is used to detect errors in the ICMP messages.

4. IP header and original datagram: This field can be used for diagnostic purposes by matching the information in the ICMP message with the original data in the IP Packet

3.7.3 Error reporting

ICMP does not correct errors it simply reports them. ICMP handles five types of errors

1. Destination unreachable
2. Source quench
3. Time exceeded
4. Parameter problems
5. Redirection

1. Destination unreachable:

The ICMP destination unreachable message is sent by a router in response to a packet which it cannot forward because the destination is unreachable or a service is unavailable.

Type :.3	Code : 0to 5	Checksum
unused (All 0s)		
Part of the received IP datagram including IP header plus first 8 bytes of datagram data		

Fig: Destination unreachable format

.. Code field : The code field is used by the different message formats to indicate specific error conditions.

For destination unreachable, the code field is:

0 = Net unreachable
1 = Host unreachable
2 = Protocol unreachable
3 = Port unreachable
4 = Fragmentation needed and DF set
5 = Source route failed.

2. Source quench :

ICMP source quench messages to report congestion to the original source. A source quench message is a request for the source to reduce its current rate of datagram transmission

Type : 4	code : 0	Checksum
unused (All 0s)		
Part of the received IP datagram including IP header Plus the first 8 bytes of datagram data		

Fig: Source Quench format

3. Time exceeded message:

Type : 11	Code 0 or 1	Checksum
unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data.		

Fig: Time exceeded message format

Code field :

0 = Time to live exceeded in transit
1 = Fragment reassembly time exceeded.

4. Parameter Problem:

The parameter problem message identifies the octet of the original datagram's header where the error was detected.

Type: 11	code: 0 or 1	checksum
Pointer	unused (All 0s)	
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Fig: Parameter Problem message format

Code field: The code field is 0 when the pointer field indicates the error

5. Redirection:

Type: 5	Code: 0 or 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Fig: Redirection message format

Code field:

0 = Redirect datagrams for the network
1 = Redirect datagrams for the host
2 = Redirect datagrams for the type of service and network
3 = Redirect datagrams for the type of service and host

3.7.4 Query

ICMP query messages are of four types

1. Echo request and reply
2. Timestamp request and reply
3. Address-mask request and reply
4. Router solicitation and advertisement

1. Echo request and reply

The echo request and echo reply messages can be used to determine if there is communication at the IP level.

8: Echo request
0: Echo reply

Type: 8 or 0	code: 0	Checksum
Identifier		sequence number
optional data Send by the request message: Repeated by the reply mssg:		

Fig: Format of echo request & reply messages

2. Timestamp Request and Reply

used to calculate the round trip time between a source and destination machine

13: Request
14: Reply

Type: 13 or 14	code: 0	checksum
Identifier		Sequence number
original timestamp (32 bit)		
Receive timestamp (32 bit)		
Transmit timestamp (32 bit)		

3. Address Mask request and reply message

The address mask request is used by a host to determine what its address mask is on a network. The addrsss mask reply message is the reply from a router or a host to the source host with the correct address mask for the network

17: request
18: reply

Type: 17 or 18	Code: 0	Checksum
Identifier		Sequence number
Address Mask		

Fig: Mask request and reply message format

4. Router Solicitation and Advertisement

Type: 10	Code: 0	Checksum
Identifier		Sequence number

Fig: Router Solicitation Message format

This is the reply that comes back from the previous request. Lifetime field shows the number of seconds that the entries are considered to be valid.

Type: 9	Code: 0	Checksum
Number of addresses	Address entry Size	Lifetime
Router address 1		
Address Preference 1		
Router address 2		
Address Preference 2		
⋮		

Fig: Router advertisement message format

3.8 DHCP (Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol is a network management protocol used to dynamically assign an IP address to devices connected to the network using a client / server architecture.

When new devices appear on the network, they receive unique IP addresses. The addresses can be assigned by the network adminstiator manually or dynamically. However when the local network has multiple devices, it becomes inefficient to allocate IP addresses by hand. thus the DHCP protocol comes to the rescue

On residential network, router is a DHCP server that uses DHCP to assign IPs and send important information.

3.8.1 Components of DHCP Server:

- DHCP Server: A DHCP server can be either a server, dedicated computer or router that manages network configuration information including IP addresses

- DHCP client: A DHCP client is a network device that communicates with the DHCP server to receive the configuration Information

- DHCP relay agent: A DHCP relay agent is a host or a router that sends requests and replies between the local DHCP clients and a remote DHCP server.

- Default gateway address: A default gateway, also known as the gateway address, is the node that forwards information between local networks or subnets and the internet

- IP address pool: An IP address pool is a list of all IPs that are available for allocation.

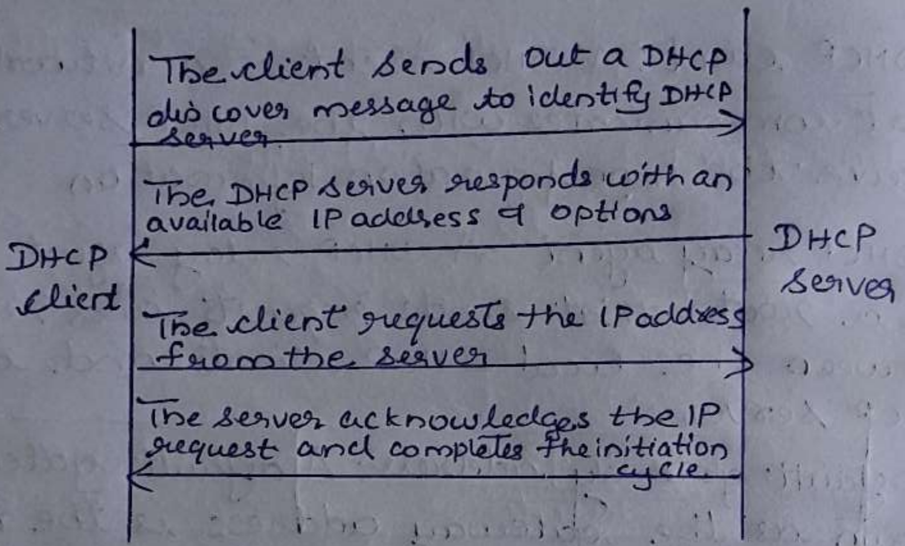
- Subnet mask: Subnet masks are the segments of an IP address. IP addresses are divided into subnet masks to differentiate between network and host bits. Thus, a subnet mask allows a host to determine the exact network it currently exists in

- DHCP options: DHCP has numerous configurations which are called options. Some of the more common DHCP options include:
    - option 3 (router option)
    - option 6 (DNS server option)

- option 33 (Static route option)
- option 51 (IP address lease option)

- Lease Time: The lease time defines the period, during which the client can use the IP address that was assigned to it

3.8.2 DHCP Handshake:


DHCP client
DHCP Server
The client sends out a DHCP discover message to identify DHCP server
The DHCP server responds with an available IP address & options
The client requests the IP address from the server
The server acknowledges the IP request and completes the initiation cycle.

3.8.3 Static Vs Dynamic DHCP leases:

With Dynamic DHCP, a client does not own the IP address assigned to it but instead leases it for a period of time. Each time a device with a dynamic IP address is powered up, it must communicate with the DHCP server to lease another IP address.

Wireless devices are examples of clients that are assigned dynamic IP addresses when they connect to a network.

On the other hand, static devices such as web servers and Switches are assigned permanent IP addresses.

3.8.4 DHCP uses and functions

1. Used to distribute IP addresses within a network.
2. Prevent IP conflict.
3. Updates IP address automatically.
4. Supports IP address Reuse

Problems

1. Change the following IPV4 addresses from binary notation to dotted-decimal notation
   a) 10000001 00001011 00001011 11101111
   b) 11000001 10000011 00011011 11111111

2. Change the following IPV4 addresses from dotted-decimal notation to binary notation.
   a) 111.56.45.78
   b) 221.34.7.82

3. Find the class of each address
   a) 00000001 00001011 00001011 11101111
   b) 11000001 10000011 00011011 11111111
   c) 14.23.120.8
   d) 252.5.15.111

For example 11100000, the number of 1s gives us 2^3 subnets. In this example there are 8 subnets.

2. **How many host per subnet ?**

Number of host per subnet = $2^y - 2$

Where y is the number of unmasked bits or the 0s (zeros)

For example 11100000, the number of 0s gives us $2^5 - 2$ hosts. In this example there are 30 hosts per subnet. Your need to subtract 2 for subnet address and the broadcast address.

3. **What are the valid subnets?**

For valid subnet = 256 – Subnet mask = Block size. An example would be 256 – 224 = 32. The block size of a 224 mask is always 32.

Start counting at zero in block of 32 until you reach the subnet mask value and these are your subnets. 0, 32, 64, 96, 128, 160, 192, 224.

4. **What is the broadcast address for each subnet ?**

Our subnets are 0, 32, 64, 96, 128, 160, 192, 224, the broadcast address is always the number right before the next subnet. For example, the subnet 0 ha a broadcast address of 31 because next subnet is 32. The subnet 32 has a broadcast address of 63 because next subnet is 64.

5. **What are the valid hosts ?**

Valid hosts are the numbers between the subnets, omitting the all 0s and all 1s. For example, if 32 is the subnet number and 63 is the broadcast address, then 32 to 63 is the valid host range. It is always between the subnet address and the broadcast address.

Example 3.3.2 What is the sub-network address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0 ?

Solution: Using AND operation, we can find sub-network address,

1. Convert the given destination address into binary format:

   200.45.34.56 =>11001000 0010110100100010 00111000

2. Convert the given subnet mask address into binary format:

   255.255.240.0 =>11111111 1111111111110000 00000000

3. Do the AND operation using destination address and subnet mask address.

   200.45.34.56 =>11001000 0010110100100010 00111000

   255,255.240.0 => 11111111 1111111111110000 00000000

   11001000 0010110100100000 00000000

Subnet work address is 200.45.32.0

Example 3.3.2 For a network address 192.168.10.0 and subnet mask 255.255.255.224 then calculate:

i) Number of subnet and number of host

ii) Valid subnet

Solution: Given network address 192.168.10.0 is class C address. Subnet mask address is 255.255.255.224. Here three bits is browse for subnet.

i) **Number of subnet and number of host**

255.255.255.224 convert into binary =>11111111 11111111 11111111 11100000

Number or subnet = $2^x = 2^3 = 8$

So there are 8 subnet.

Number of host per subnet = $2^y - 2 = 2^5 - 2 = 30$

ii) **Valid subnets**

For valid subnet = 256 - Subnet mask = Block size. An example would be 256 - 224 = 32. The block size of a 224 mask is always 32.

Start counting at zero in block of 32 until you reach the subnet mask value and these are your subnets. 0, 32, 64, 96,128,160,192, 224.

Example 3.3.3 Find the sub-network address for the fallowing;

Sr. No.	IP address	Mask
a)	140.11.36.22	255.255.255.0
b)	120.14.22.16	255.255.128.0

Solution

a) IP address Mask

140.11.36.22 255.255.255.0

The values of mask (i.e. 255.255.255.0) is boundary level. So

IP address 140.11.36.22

Mask 255.255.255.0

140.11.36.0

b) IP address 140.11.36.22

Mask 255.255.128.0

Example 3.3.4 Find the sub-network address for the fallowing;

Sr. No.	IP address	Mask
a)	141.181.14.16	255.255.224.0
b)	200.34.22.156	255.255.255.240
c)	125.35.12.57	255.255.0.0

Solution

a)

141.181.14.16 IP address

255.255.224.0 Mask

141.181.0.0 Sub-network address

b)

200.34.22.156	IP address
255.255.255.240	Mask
200.34.22.144	Sub-network address

c)

125.35.12.57	IP address
255.255.0.0	Mask
125.35.0.0	Sub-network address

(i.e. 128) So for byte-3 value use bite-wise AND operators. It is shown below.

120.14.22.16	IP address
255.255.128.0	Mask
125.14.0.0	Sub-network address

In the above example, the bite wise ANDing is done in between 22 and 128. It is as follows.

22	Binary representation	0 0 0 1 0 1 1 0
128	Binary representation	1 0 0 0 0 0 0 0
0		0 0 0 0 0 0 0 0

Thus the sub-network address for this is 120.14.0.0.

Example 3.3.5 Finde the class of the following address.

a) 1.22.200.10 b) 241.240.200.2 c) 227.3.6.8 d) 180.170.0.2

Solution:

a) 1.22.200.10	Class A IP address
b) 241.240.200.2	Class E IP address
c) 227.3.6.8	Class D IP address
d) 180.170.0.2	Class B IP address

Example 3.3.6 Find the retid and Hositd for the following.

a) 19.34.21.5 b) 190.13.70.10 c) 246.3.4.10 d) 201.2.4.2

Solution

a) netid => 19 Hostid => 13.70.10

b) netid => 190.13 Hostid => 70.10

c) No netid and No Hostid because 246.3.4.10 is the class E address.

d) netid =>201.2.4 Hostid =>2

Example 3.3.7: Consider sending a 3500 - byte datagram that has arrived at a router R_1that needs to be sent over a link that has an MTU size of 1000 bytes to R_2. Then it has to traverse a link with an MTU of 600 bytes. Let the identification number of the original datagram be 465.

How many fragments are delivered at the destination ? Show the parameters associated with each of these fragments.

Solution: The maximum size of data field in each fragment = 680 (because there are 20 bytes IP header). Thusthe number of required fragments) = [3500 - 20/680] - 5.11 ≃ 6.

Each fragment will have Identification number 465. Each fragment except the last one will be of size 700 bytes (including IP header). The last datagram will be of size 360 bytes (including IP header). The offsets of the4 fragments will be 0, 85, 70, 255. Each or the first 3 fragments will have flag=l; the last fragment will have flag=0.

Example 3.10

An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:

a) The first group has 64 customers; each needs 256 addresses.

b) The second group has 128 customers; each needs 128 addresses.

c) The third group has 128 customers; each needs 64 addresses.

Design the sub blocks and find out how many addresses are still available after these allocations.

Solution

Figure 3.11 shows the situation.

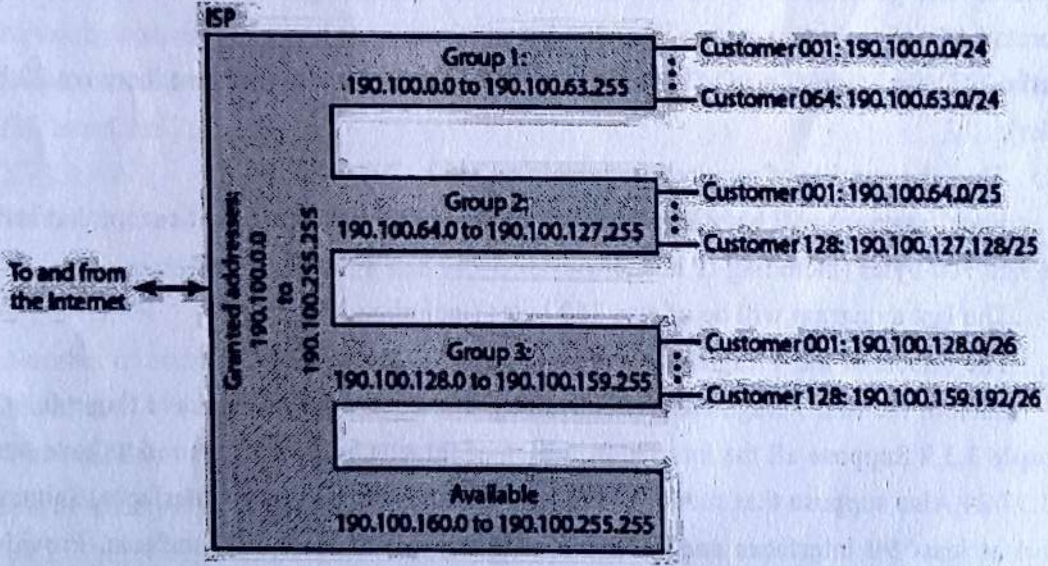

ISP
To and from the Internet
Granted addresses: 190.100.0.0 to 190.100.255.255
Group 1: 190.100.0.0 to 190.100.63.255
Customer 001: 190.100.0.0/24
Customer 064: 190.100.63.0/24
Group 2: 190.100.64.0 to 190.100.127.255
Customer 001: 190.100.64.0/25
Customer 128: 190.100.127.128/25
Group 3: 190.100.128.0 to 190.100.159.255
Customer 001: 190.100.128.0/26
Customer 128: 190.100.159.192/26
Available 190.100.160.0 to 190.100.255.255

Fig 3.11 An example of address allocation and distribution by an ISP

1. Group 1

For this group, each customer needs 256 addresses. This means that 8 (log2256) bits are needed to define each host. The prefix length is then 32 - 8 =24. The addresses are

1st Customer: 190.100.0.0/24 100.0.255/24

2nd Customer: 190.100.1.0/24190 190.100.1.255/24
64th Customer: 190.100.63.0/24 190.100.63.255/24
Total =64 X 256 =16,384

2. Group2

For this group, each customer needs 128 addresses. This means that 7 (10g2 128) bits are needed to define each host. The prefix length is then 32 - 7 =25. The addresses are

3. Group3

For this group, each customer needs 64 addresses. This means that 6 (log2 64) bits are needed to each host. The prefix length is then 32 - 6 =26. The addresses are

1st Customer: 190.100.128.0/26 190.100.128.63/26
2nd Customer: 190.100.128.64/26 190.100.128.127/26
128th Customer: 190.100.159.192/26 190.100.159.255/26
Total =128 X 64 =8192

Number of granted addresses to the ISP: 65,536
Number of allocated addresses by the ISP: 40,960
Number of available addresses: 24,576

Example 3.3.8 Consider sending a 2400-byte datagram into link that has an MTU of 700 bytes. Suppose the original datagram is stamped with the identification number 422. How many fragments are generated? What are the values in the various fields in the IP datagram(s) generated related to fragmentation.

Solution: The maximum size of data field in each fragment = 680 (because there are 20 bytes IP header).

Thus the number of required fragments = (2400 - 20) / 680 =4

Each fragment will have Identification number 422. Each fragment except that last one to be of size 700 bytes (including IP header.

The last datagram will be of size 360 bytes (including IP header).

The offsets of the 4 fragments will be 0, 85, 170, 255.

Each of the first 3 fragments will have flag = 1; last fragment will have flag = 0.

Example 3.3.9 Suppose all the interfaces in each of three subnets are required to have the prefix 223.1.17/24.Also suppose that subnet 1 is required to support at least 60 interfaces, Subnet 2 is to support at least 90 interfaces and subnet 3 is to support at least 22 interfaces. Provide three network addresses that satisfy these constraints.

Solution: The network address cannot be used for an interface (Network prefix + all zeros).

- The broadcast address cannot be used for an interface (Network prefix + all ones)

Subnet 2 (90 interfaces)

$2^n - 2 \geq 90$

Notice that we subtract 2 from the total number of available IP addresses because 2 IP addresses are reserved for the network and broadcast addresses.

$2^{n}\geq 92^{n} = 7$

Number of bits allocated to host part =n = 7

Number of bits allocated to network part = Pre filength = 32 - n = 32 - 7 = 25

The network address of the first subnet is always the address of the given address space.

Network address of first subnet = 223.1.17.0/25 = 223.1.17/25

To obtain the broadcast address of a subnet, we keep to network part of the subnet's network address as it is, and convert all bits in its host part to 1s.

Broadcast address of first subnet = 223.1.17.01111111 / 25 = 223.1.1.7.127/25

Subnet 1 (60 interfaces)

2n - 2 ≥ 60

Notice that we subtract 2 from the total number of available IP addresses because 2 IP addresses are reserved for the network and broadcast addresses.

$2^{n} \geq 60$ n =6

Number of bits allocated to host part = n = 6

Number of bits allocated to network part = Prefix length = 32 - n = 32 - 6 = 26 The network address of any subnet (that is NOT the first subnet) is obtained by adding one to the broadcast address of its preceding subnet.

Network address of second subnet = 223.1.17.128/26

Broadcast address of second subnet = 223.1.17.10111111/26 =223.1.17.191/26 Subnet 3 (12 interfaces) :

$2^{n} - 2 \geq 12$

Notice that we subtract 2 from the total number of available IP addresses because 2 IP addresses are reserved for the network and broadcast addresses.

$2^{n}\geq 14$ n = 4

Number of bits allocated to host part = n = 4

Number of bits allocated *to* network part = Prefix length = 32 - n = 32 - 4 = 28

Network address of third subnet = 223.1.17.192/28

c) 212.208.63.23 - Class C

d) 255.255.255.255 - Broadcast address.

2 **What is the purpose of the Address Resolution Protocol ?(May 11)**

Ans: ARP is a dynamic mapping method that finds a physical address for given a logical address, i.e. mapping IP address to physical address.

3 **Define an internetwork.**

Ans: A collection of interconnected networks is called an internetwork.

4 **Define geographic routing.**(May 10)

Ans: To decrease the size of the routing table even further, it necessary to extend hierarchical routing to include geographical routing. It divides the entire address space into a few large blocks.

5 **What is multicasting routing ?(May 18)**

Ans: Deliveryof information to a group of destinations simultaneously using themost efficient strategy to deliver the messages over each link of the network only once.

6 **What are the different kinds of multicast routing ?(May 11)**

Ans: Different kinds of multicast routing are reverse path multicasting and reverse path broadcasting.

7 **Define subnetting.(Dec 15)**

Ans: Subnetting is a technique that allows a network administrator to divide one physical network into smaller logical networks and thus, control the flow of traffic for security or efficiency reasons.

8 **What is multicast ? What is the motivation for developing multicast ?(May 11)**

Ans: Multicasting means delivering the same packet simultaneously to a group of clients. Motivation for developing multicast is that there are applications that want to send a packet to more than one destination hosts.

9 **What is the use of CIDR value in IP addressing ?**

Ans: Class C address's concept becomes meaningless on these routes between domains; the technique is call Classless Inter-domain Routing or CIDR. A key concept is to allocate multiple IP address in the way that allows summarization into a smaller number of routing table.

10 **Expand and define MTU.(May 12)**

Ans: MTU :. Maximum Transmission Unit. MTU is a networking term defines the biggest packet size that can be sent over a network connection.

11. Compare the Ethernet address with IP address

Sr. No.	Ethernet Address	IP Addresses
1.	Flat, i.e. switches look all the bits always.	Hierarchical, i.e., backbone routers may just look higher order bits.
2.	Assigned by ethernet hardware vendor	Statically or dynamically assigned by

	(Ethenet addresses are supposed to be unique)	ISP or IT managers.
3.	No geographical nor organizational association (Convenient for small Networks)	Geographical or organizational association.
4.	For example: 8-0-20-b-de-3e	For example: 172.16.16.1

12. Define Routing? (Dec 15)

Ans: Routing is the process of selecting paths in a network through which network trafrfic is sent.

13. Find the class of each address

a) 00000001 00001011 00001011 11101111

b) 14.23.120.8

Ans. a) The first bit is 0. This is a class A address.

b) The first byte is 14 (between 0 and 127). This is a class A address

14. What do you mean by unicast routing ?

Ans: Unicast routing is a process of forwarding unicasted traffic from a source to destination on an Internet.

15. What are the salient features of IPv6 ?(Dec 12)

Ans: Salient features are :

a. Efficient and hierarchical addressing and routing infrastructure

b. IPv6 networks provide auto-configuration capabilities.

c. Improved security features.

d. Better support for QoS.

e. Large address space.

f. Stateless and stateful address configuration.

16. Define source routing(Dec 13)

Ans: All the information about the network topology is required to switch a packet across the network is provided by the source host. For switching that uses neithervirtual circuits nor conventional datagrams is known as source routing.

17. What is the need of subnetting?(Dec 13)

Ans: Subnetting divides one large networkinto several smaller ones. Subnetting adds an intermediate level of hierarchy in IP addressing.

18. Define BGP. (Dec 14,17)

Ans: Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed routing and reachability information between autonomous systems on the Internet.

19. What are the metrics used by routing protocols ?(May 15)

Ans: 1. Traffic matrices

2. Distance matrices

3. Adjacency matrices

4. Service matrices
5. Performance matrices

20.Define VCI(Dec 16)

Ans: VCI is an acronym for virtual channel identifier. VCI is a 16-bit field in ATMcell header that identities the cell's next destination as it travels through ATM network. VCI is used in conjunction with Virtual Path Identifier (VPI).

21. What is fragmentation and reassembly (Dec 16)

Ans: IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. Large datagram are fragmented (divided) i.e. one datagram becomes several datagram of small sizes. This process is called fragmentation. At final destination the datagrams are reassembled with the help of IP header bits.

22. Give the comparison of unicast, multicast and broadcast routing.(Dec 16)

Ans:

Sr. No.	Unicast	Multicast	Broadcast
1.	Unicast is a type of communication where a piece of information is sent from one point to another.	The information is sent from one or more points to set of other points.	The information is sent from one point to other points.
2.	Only one sender and one receiver	One or more sender and set of receiver	One sender and several receivers.

23. How routers do differentiates the incoming unicast, multicast or broadcast IPpackets ?(May 17)

Ans: The Ethernet network uses two hardware addresses which identify the source and destination of each frame sent by the Ethernet. The MAC destination address (all 1 s) is used to identify a broadcast packet (sent to all connected computers in a broadcastdomain) or a multicast packet (lsb of 1st byte=1) (received by a selected group of computers).

Routers are operating at layer 3. Router use IP addresses to make forwarding decisions. Each port on a router is a member of a different network. When a router receives traffic from one network, it uses the destination IP address to determine which port to forward.

24. Differentiate between forwarding table and routing table. (Dec 17)

Ans: Routing means finding a suitable path for a packet from sender to destination and Forwarding is the process of sending the packet toward the destination based on routing information.

25. What are the benefits of Open Shortest Path First (OSPF) protocol ? (May 18)

Ans: **Benefits**

1. Low traffic overhead
2. Support for complex address structures
3. Fast convergence

4. Good security. OSPF supports interface-based plain text and MD5 authentication.
5. Area based topology. Large OSPF networks are organized as a set of areas linked by a backbone.

26. What is the network address in a class A subnet with the IP address of one of the hosts as 25.34.12.56 and mask 255.255.0.0 ? (May 14)

Ans: 25.34.12.56

255.255.0.0

25.34.0.0

Network address is 25.34.0.0

27. Expand ICMP and write the function.(May 16)

Ans: ICMP stands for internet control message control.

Functions of ICMP

1) Error reporting 2) Rechability testing 3) Congestion control 4) Route change notification 5) Performance measuring 6) Subnet addressing

28. When is ICMP redirect message used ?(May 17)

Ans: The ICMP Redirect message is used to notify a remote host to send data packets on an alternative route. A host SHOULD NOT send an ICMP Redirect message, Redirects SHOULD only be sent by gateways.

The ICMP "redirect" message indicates that the gateway to which the host sent the datagram is no longer the best gateway to reach the net in question. The gateway willhave forwarded the datagram, but the host should revise its routing table to have a different immediate address for this net.

29. Why is IPv4 to IPv6 transition is required ? (May 17)

Ans: As publicly available IPv4 addresses have been exhausted. IPv4, the current internet protocol version has crossed 30 years of time period. The expanding user base and increased number of IP-enabled devices created a need for an upgraded version.

From mobile apps to non-traditional computing devices populating the Internet of Things, businesses rely on ITs ability to deliver new services to both end users and customers. But these services and the infrastructure used to support them require IP addresses and that means an IPv6 migration.

30. Highlight the characteristics of datagram networks. (Dec 17)

Ans: Characteristics of datagram networks are as follows :

a. Host can send a packet anywhere at any time.
b. Each packet is forwarded independently.
c. Link failure would not have any serious effect on communication if it is possibleto find an alternate route around the failure and update the forwarding tableaccordingly.

31 Check whether the following IPv6 address notations are correct ? (Dec 18)

a) **: : OF53:6382:AB00:67DB:BB27:7332.**

b) **7803:42F2:::88EC-D4BA:B75D:11CD**

Ans: a) : : OF53:6382:AB00:67DB:BB27:7332 : Correct

b) 7803:42F2:::88EC-D4BA:B75D:11CD : Incorrect because of two many (:)

Prepared by **Verified by** **Approved by**

UNIT IV ROUTING

Routing and protocols: Unicast routing - Distance Vector Routing - RIP - Link State Routing – OSPF– Path-vector routing - BGP - Multicast Routing: DVMRP – PIM

4.1 Routing

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

The most common metric values are given below:

- **Hop count:** Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination. If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.
- **Delay:** It is a time taken by the router to process, queue and transmit a datagram to an interface. The protocols use this metric to determine the delay values for all the links along the path end-to-end. The path having the lowest delay value will be considered as the best path.
- **Bandwidth:** The capacity of the link is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.
- **Load:** Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second. If the traffic increases, then the load value will also be increased. The load value changes with respect to the change in the traffic.

- **Reliability:** Reliability is a metric factor may be composed of a fixed value. It depends on the network links, and its value is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links. Any reliability factor can be considered for the assignment of reliability ratings, which are generally numeric values assigned by the system administrator.

Types of Routing

Routing can be classified into three categories:

- Static Routing
- Default Routing
- Dynamic Routing

Static Routing

- Static Routing is also known as Nonadaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

Advantages Of Static Routing

Following are the advantages of Static Routing:

- **No Overhead:** It has ho overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.
- **Bandwidth:** It has not bandwidth usage between the routers.
- **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

Disadvantages of Static Routing:

Following are the disadvantages of Static Routing:

- For a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

Default Routing

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.

- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

Dynamic Routing

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

The Dynamic protocol should have the following features:

- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

Advantages of Dynamic Routing:

- It is easier to configure.
- It is more effective in selecting the best route in response to the changes in the condition or topology.

Disadvantages of Dynamic Routing:

- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing.

4.2 Unicast routing

Unicast – Unicast means the transmission from a single sender to a single receiver. It is a point-to-point communication between sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

- TCP is the most commonly used unicast protocol. It is a connection-oriented protocol that relies on acknowledgement from the receiver side.
- HTTP stands for HyperText Transfer Protocol. It is an object-oriented protocol for communication.

There are three major protocols for unicast routing:

1. Distance Vector Routing
2. Link State Routing

3. Path-Vector Routing

4.2.1 Distance Vector Routing

Distance vector routing algorithm is also called as **Bellman-Ford algorithm** or **Ford Fulkerson algorithm** as this algorithm is used to find the shortest route from one node to another node in the network.

The routing protocol is used to calculate the best route from source to destination based on the distance or hops as its primary metric to define an optimal path. The distance vector refers to the distance to the neighbor nodes, where routing defines the routes to the established node.

The **Distance Vector routing algorithm**(DVR) shares the information of the routing table with the other routers in the network and keeps the information up-to-date to select an optimal path from source to destination.

The Bellman-Ford algorithm is defined as :

$$d_x(y) = \min_v \{c(x, v) + d_v(y)\}$$

where, dx(y)=dx(y)= The least distance from x to y
c(x,v)=c(x,v)= Node x's cost from each of its neighbour v
dv(y)=dv(y)= Distance to each node from initial node
minv=minv= selecting shortest distance

It works in the following steps-

Step-01:

Each router prepares its routing table. By their local knowledge. each router knows about-

- All the routers present in the network
- Distance to its neighboring routers

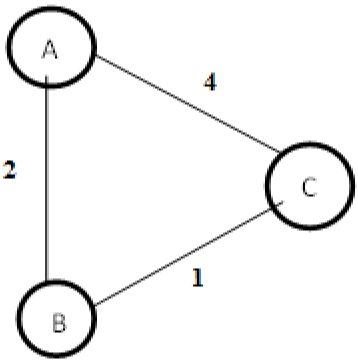
Step-02:

- Each router exchanges its distance vector with its neighboring routers.
- Each router prepares a new routing table using the distance vectors it has obtained from its neighbors.
- This step is repeated for (n-2) times if there are n routers in the network.
- After this, routing tables converge / become stable.

Example − Distance Vector Router Protocol

In the network shown below, there are three routers, A, B, and C, with the following weights − AB =2, BC =3 and CA =5.

Step 1 − In this DVR network, each router shares its routing table with every neighbor. For example, A will share its routing table with neighbors B and C and neighbors B and C will share their routing table with A.



Form A	A	B	C
A	0	2	3
B			
C			

Form B	A	B	C
A			
B	2	0	1
C			

Form C	A	B	C
A			
B			
C	3	1	0

Step 2 − If the path via a neighbor has a lower cost, then the router updates its local table to forward packets to the neighbor. In this table, the router updates the lower cost for A and C by updating the new weight from 4 to 3 in router A and from 4 to 3 in router C.

Form A	A	B	C
A	0	2	3
B			
C			

Form B	A	B	C
A			
B	2	0	1
C			

Form C	A	B	C
A			
B			
C	3	1	0

Step 3 − The final updated routing table with lower cost distance vector routing protocol for all routers A, B, and C is given below –

Router A

Form A	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

Router B

Form B	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

Router C

Form C	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

RIP Protocol

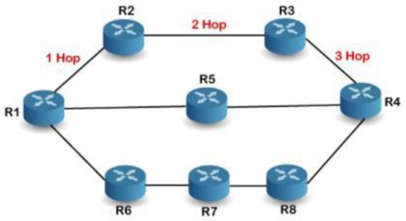
RIP stands for Routing Information Protocol. RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area. To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing table.

Before understanding the structure of the packet, we first look at the following points:

- RIP is based on the distance vector-based strategy, so we consider the entire structure as a graph where nodes are the routers, and the links are the networks.
- In a routing table, the first column is the destination, or we can say that it is a network address.
- The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.
- In RIP, infinity is defined as 16, which means that the RIP is useful for smaller networks or small autonomous systems. The maximum number of hops that RIP can contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.
- The next column contains the address of the router to which the packet is to be sent to reach the destination.

How is hop count determined?

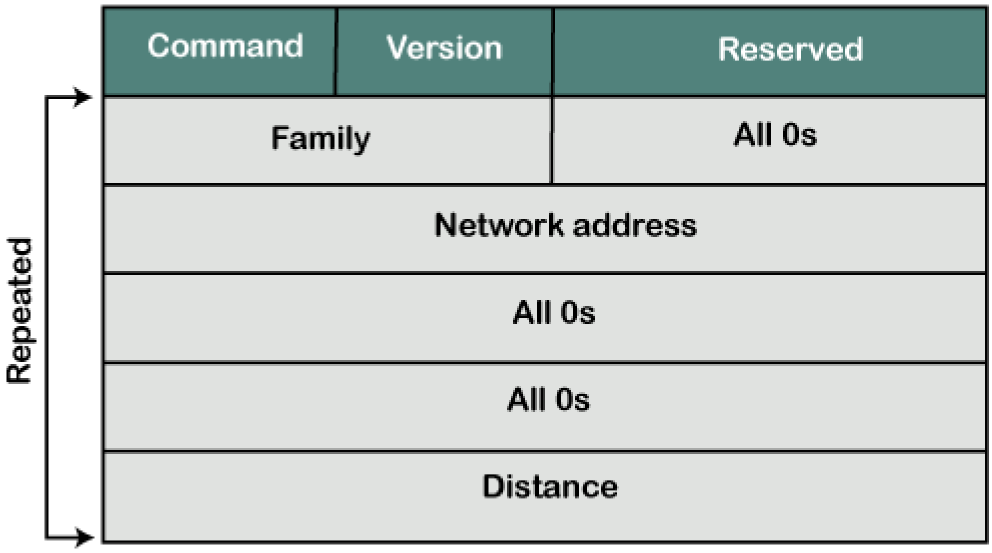
When the router sends the packet to the network segment, then it is counted as a single hop.



In the above figure, when the router 1 forwards the packet to the router 2 then it will count as 1 hop count. Similarly, when the router 2 forwards the packet to the router 3 then it will count as 2 hop count, and when the router 3 forwards the packet to router 4, it will count as 3 hop count. In the same way, RIP can support maximum upto 15 hops, which means that the 16 routers can be configured in a RIP.

RIP Message Format

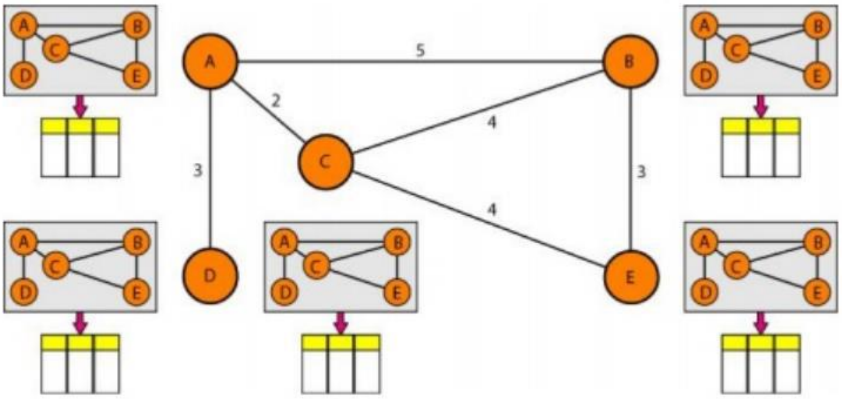
Now, we look at the structure of the RIP message format. The message format is used to share information among different routers. The RIP contains the following fields in a message:



- Command: It is an 8-bit field that is used for request or reply. The value of the request is 1, and the value of the reply is 2.
- Version: Here, version means that which version of the protocol we are using. Suppose we are using the protocol of version1, then we put the 1 in this field.
- Reserved: This is a reserved field, so it is filled with zeroes.
- Family: It is a 16-bit field. As we are using the TCP/IP family, so we put 2 value in this field.
- Network Address: It is defined as 14 bytes field. If we use the IPv4 version, then we use 4 bytes, and the other 10 bytes are all zeroes.
- Distance: The distance field specifies the hop count, i.e., the number of hops used to reach the destination.

4.2.2 Link State Routing

Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.



The figure shows a simple domain with five nodes. Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology. This is analogous to a city map. While each person may have the same map, each needs to take a different route to reach her specific destination

Building Routing Tables:

In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.

a) Creation of the states of the links by each node, called the link state packet (LSP).

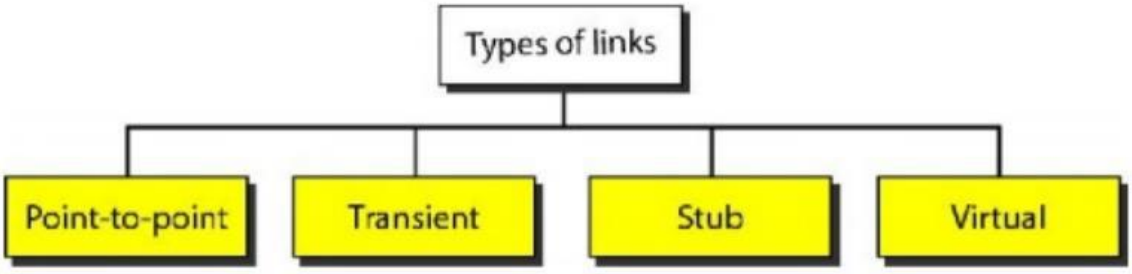
b) Dissemination of LSPs to every other router, called **flooding,** in an efficient and reliable way.

c) Formation of a shortest path tree for each node.

d)Calculation of a routing table based on the shortest path tree.

Types of Links

In OSPF terminology, a connection is called a *link.* Four types of links have been defined: point-to-point, transient, stub, and virtual.



In OSPF terminology, a connection is called a *link.* Four types of links have been defined: point-to-point, transient, stub, and virtual.

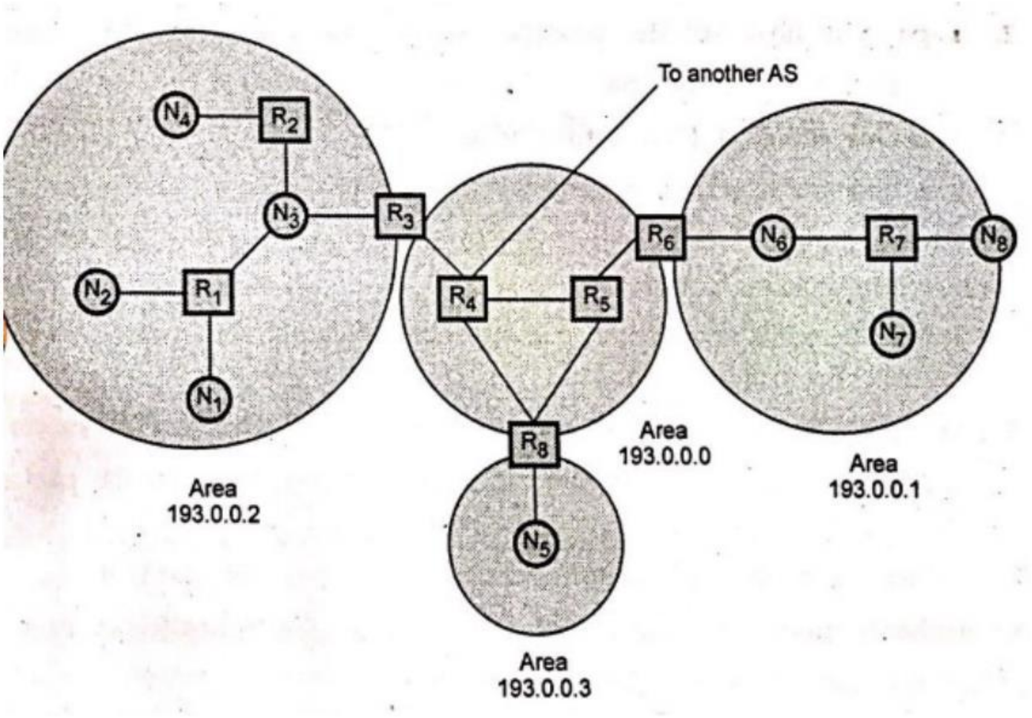
Open Shortest Path First (OSPF)

• OSPF is a link state routing protocol.

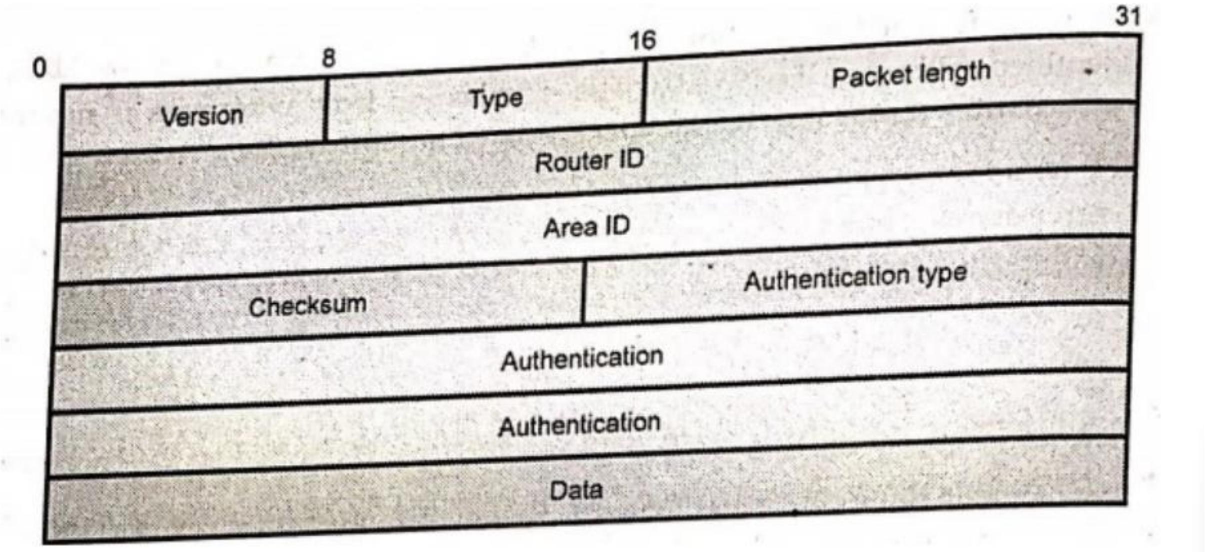
• Following is the features of the OSPF.
1. OSPF supports multiple circuit load balancing..
2. OSPF can converge very quickly to network topology change.
3. OSPF support multiple metrics.
4. OSPF support for variable length sub netting.

• OSPF uses four types of routers.
1. An internal router is a router with allits links connected to the networks within the same area.
2. An area border router is a router that has its links connected to more than one area.
3. A backbone router is a router that has its links connected to the backbone.
4. An Autonomous System Boundary Router (ASBR) is a router that has its links connected to another autonomous system.

• As shown in the Fig. routers R1, R2 andR7 are internal routers. Routers R3, R6, R8are area border routers. Routers R3, R4, R5, R6, R8are backbone routers. Router R4 is an ASBR



• The header format for OSPF is shown in the Fig.



- OSPF header analysis is given below :

1. Version: This field specifies the protocol version.
2. Type: This field indicates messages as one of the following type.

a. Hello b. Database description
c. Link status d. Link status update e. Link status acknowledgement.

3. Packet length: This field specifies the length of OSPF packet in bytes,
4. Router ID: It identifies the sending router.

5. Area ID: Network ID of destination networks.
6. Checksum: The checksum field is used to detect errors in the packet.
7. Authentication type: It identifies the authentication type that is used.
8. Authentication: This field includes a value from the authentication type.

OSPF Advantages

1.Low traffic overhead.
2. Fast convergence.
3. Larger network metrics.
4. Area based topology.
5. Route summaries.
6. Support for complex address structures.
7. Authentication.

OSPF Disadvantages
1. Memory overhead.
2. Processor overhead.
3. Configuration OSPF can be complex to configure.

4.2.3 Path Vector Routing

Distance vector and link state routing are both intradomain routing protocols. They can be used inside an autonomous system, but not between autonomous systems. These two protocols are not suitable for interdomain routing mostly because of scalability. Both of these routing protocols become intractable when the domain of operation becomes large. Distance vector routing is subject to instability if there are more than a few hops in the domain of operation. Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call path vector routing.

Path Vector Routing is a routing algorithm in unicast routing protocol of network layer, and it is useful for interdomain routing. The principle of path vector routing is similar to that of distance vector routing. It assumes that there is one node in each autonomous system that acts on behalf of the entire autonomous system is called Speaker node . It is different from the distance vector routing and link state routing. Each entry in the routing table contains the destination network, the next router and the path to reach the destination.

Functions

Prevention Of Loop

Policy Routing

Optimum Path

BGP

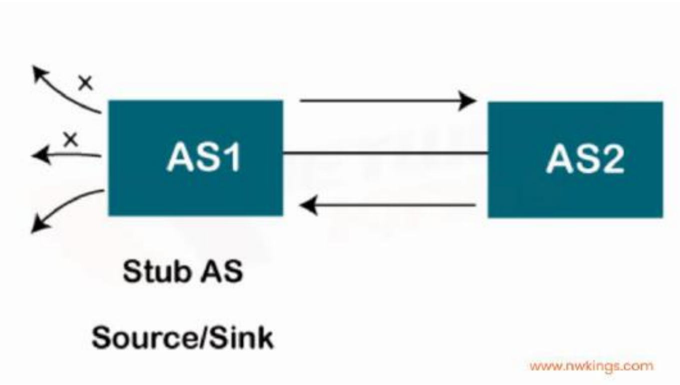
Border Gateway Protocol (BGP) is used to Exchange routing information for the internet, used to route traffic from one autonomous system (AS) to another.

Different Types of Autonomous Systems?

Since the BGP helps in routing between different autonomous systems, it is important to learn about different types of autonomous systems:

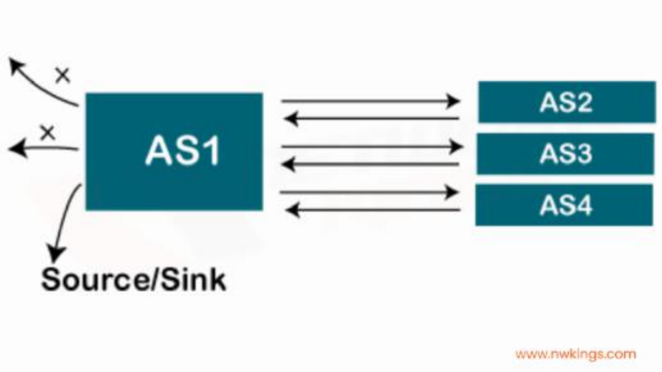
1. Stub AS:

- There is only one connection to another AS in the Stub AS.
- Data traffic cannot pass through a stub autonomous system.
- The traffic can move within an autonomous system.
- A stub is either a source or a sink



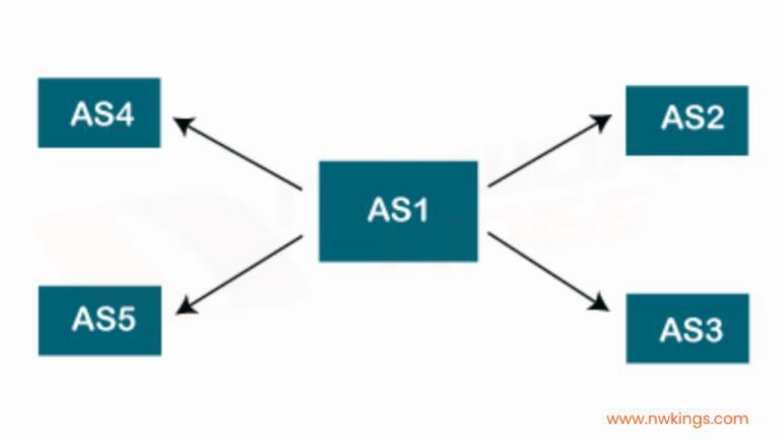
2. Multi-Homed AS:

- It has more than one connection to other Autonomous Systems.
- Still, it is still one source or sink for data traffic.
- There is no transient traffic.



3. Transit AS:

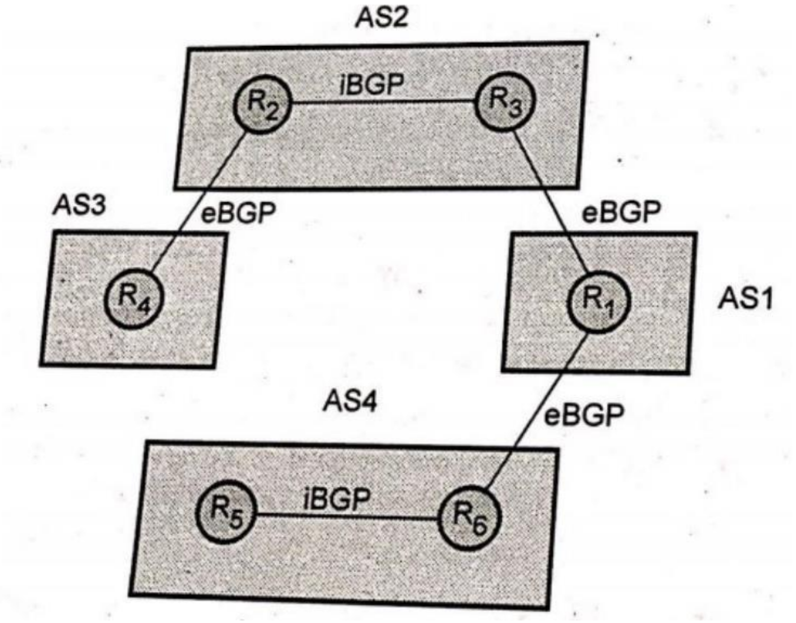
- It is a multi-homed autonomous system that allows transit traffic.
- For example, ISP (Internet Backbone) is a transit AS.



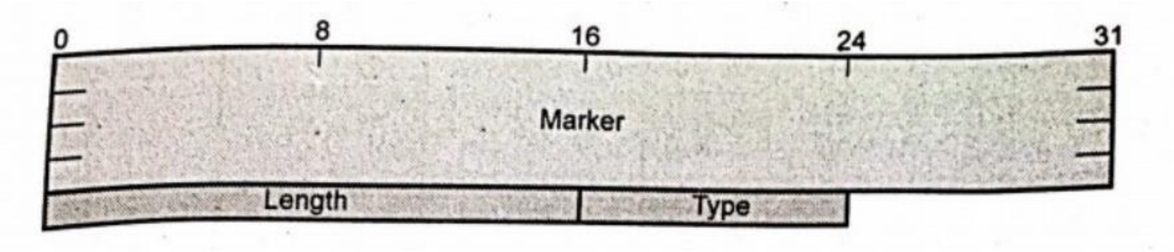
BGP performs three functional procedures

1. Neighbour acquisition 2. Neighbour reachability 3. Network reachability.
Neighbour acquisition procedures used for exchanging the routing information between two routers in different Autonomous System (AS).

BGP connections inside an autonomous system are called internal BGP (iBGP) and BGP connections between different autonomous systems are called external BGP(eBGP). Fig. shows the internal and external BGP

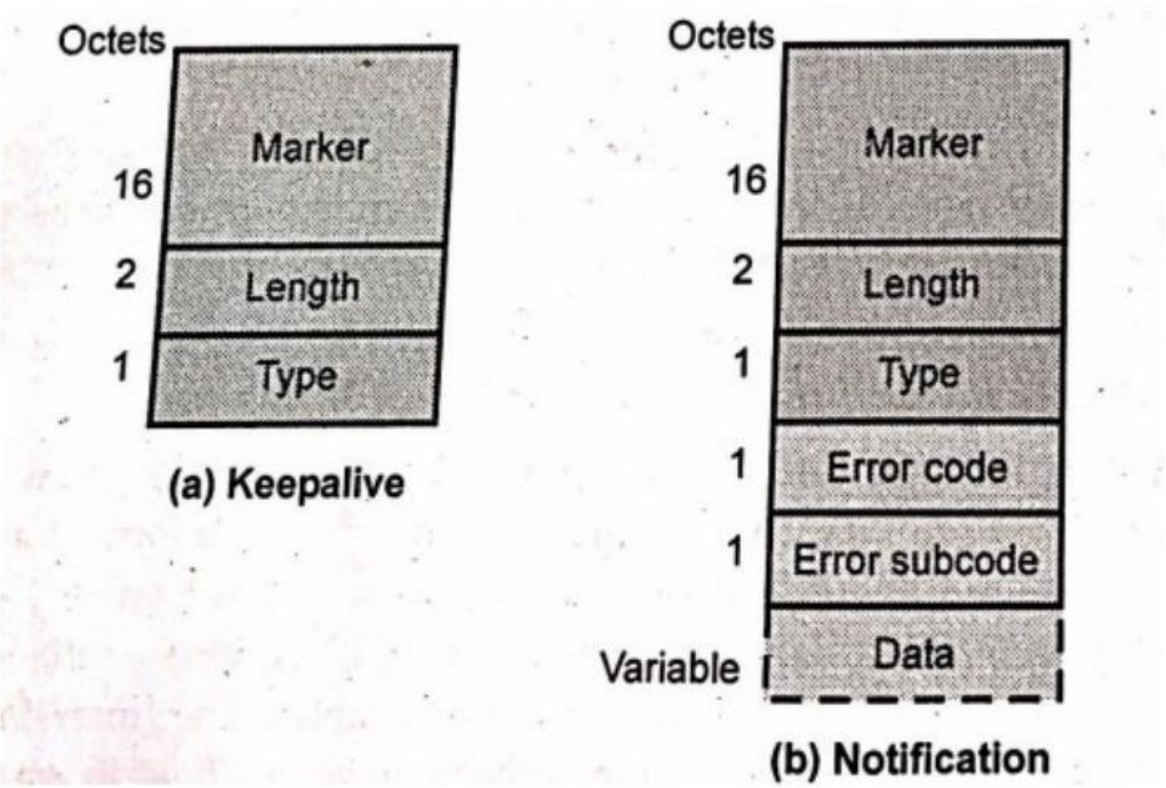


BGP messages : Header of the all BGP messages is fixed size that identifies the message type. Fig. shows the BGP message header format



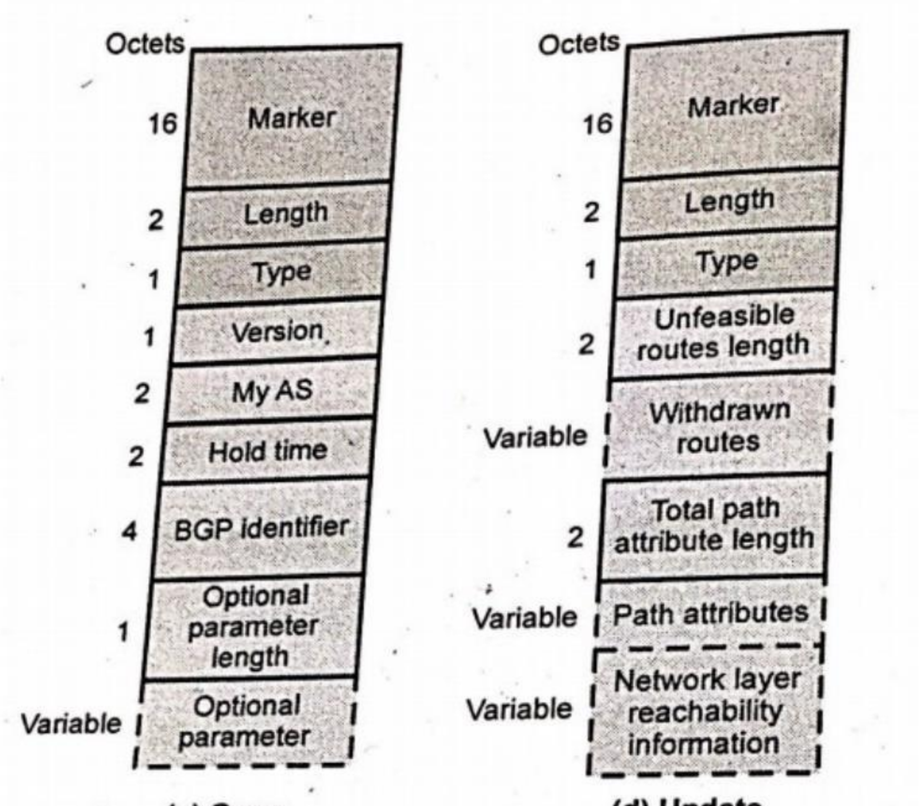
1.Marker: Marker field is used for authentication.
2. Length: This field indicates the total length of the message.
3. Type: Type field indicates type of message. BGP defines four message type.
a) OPEN b) UPDATE c) NOTIFICATION d) KEEPALIVE

Following Fig. 3.11.3 shows the four types of BGP message formats.



(a) Keepalive

(b) Notification



(c) Open

(d) Update

Advantages of BGP

1. BGP is a very robust and scalable routing protocol.

2. BGP easily solves the count-to-infinity problem.

Disadvantages of BGP
1. BGP is complex.
2. BGP routes to destination networks, rather than to specific hosts or routers.

Multicast Routing: DVMRP – PIM

Multicast is a method of group communication where the sender sends data to multiple receivers or nodes present in the network simultaneously. Multicasting is a type of one-to-many and many-to-many communication as it allows sender or senders to send data packets to multiple receivers at once across LANs or WANs. This process helps in minimizing the data frame of the network

There are different **Multicast Routing Protocols** used for multicst routing

- **Distance Vector Multicast Routing Protocol (DVMRP)**
- **Multicast Source Discovery Protocol (MSDP)**
- **MOSPF (Multicast OSPF)**
- **Multicast BGP**
- **Protocol Independent Multicast (PIM)**

Distance Vector Multicast Routing Protocol (DVMRP):

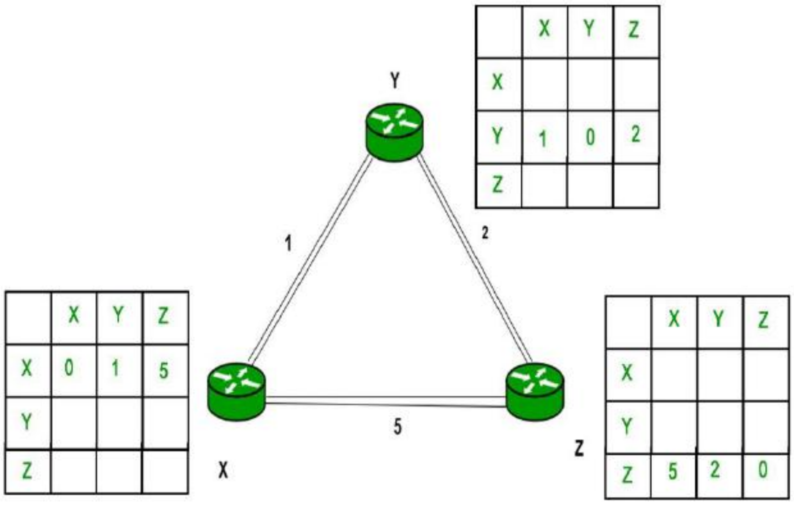
A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors of topology changes periodically.

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
   - It receives a distance vector from a neighbor containing different information than before.
   - It discovers that a link to a neighbor has gone down.

The DV calculation is based on minimizing the cost to each destination

Dx(y) = Estimate of least cost from x to y
C(x,v) = Node x knows cost to each neighbor v
Dx = [Dx(y): y ∈ N] = Node x maintains distance vector
Node x also maintains its neighbors' distance vectors
– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N]

Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



	X	Y	Z
X			
Y	1	0	2
Z			

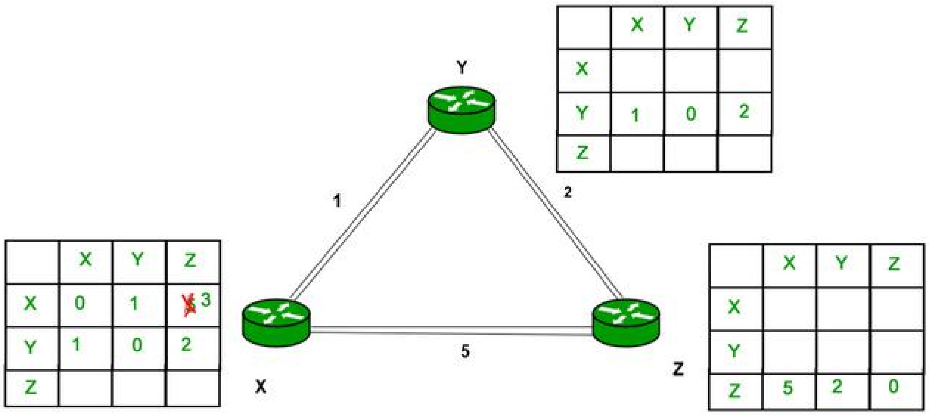
	X	Y	Z
X	0	1	5
Y			
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

Dx(y) = min { C(x,v) + Dv(y)} for each node y ∈ N

As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.

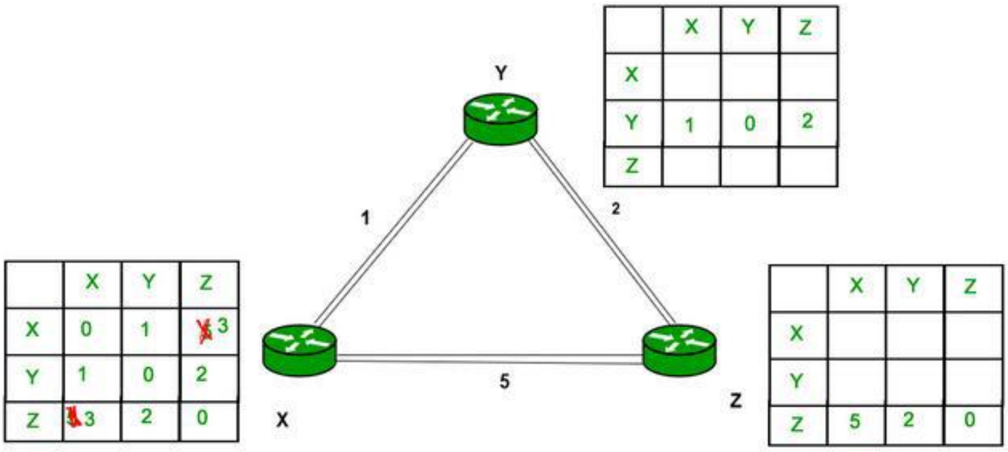


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Similarly for Z also –

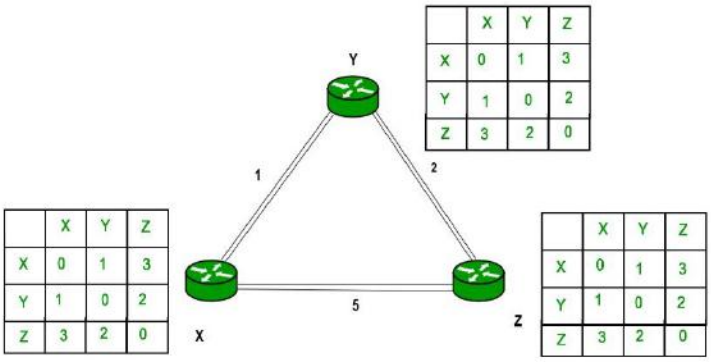


	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z	~~5~~ 3	2	0

	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Finally the routing table for all –



	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

Advantages of Distance Vector routing –

- It is simpler to configure and maintain than link state routing.

Disadvantages of Distance Vector routing –

- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.

PIM

PIM (Protocol Independent Multicast) is a multicast routing protocol, that is used to send traffic from a single source to multiple destinations across a network.

PIM is a collection of three protocols - PIM Sparse Mode, PIM Dense Mode and PIM Bi-directional . PIM is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols

PIM Sparse Mode

PIM Sparse Mode (PIM-SM) is a multicast routing protocol designed on the assumption that recipients for any particular multicast group will be sparsely distributed throughout the network. In other words, it is assumed that most subnets in the network will not want any given multicast packet. In order to receive multicast data, routers must explicitly tell their upstream neighbors about their interest in particular groups and sources. Routers use PIM Join and Prune messages to join and leave multicast distribution trees.

PIM Dense Mode

PIM Dense Mode (PIM-DM) is a multicast routing protocol designed with the opposite assumption to PIM-SM, namely that the receivers for any multicast group are distributed densely throughout the network. That is, it is assumed that most (or at least many) subnets in the network will want any given multicast packet. Multicast data is initially sent to all hosts in the network. Routers that do not have any interested hosts then send PIM Prune messages to remove themselves from the tree.

Bi-directional PIM

Bi-directional PIM (BIDIR-PIM) is a third PIM protocol, based on PIM-SM. The main way BIDIR-PIM differs from PIM-SM is in the method used to send data from a source to the RP. Whereas in PIM-SM data is sent using either encapsulation or a source-based tree, in BIDIR-PIM the data flows to the RP along the shared tree, which is bi-directional - data flows in both directions along any given branch.

UNIT V DATA LINK AND PHYSICAL LAYERS

Data Link Layer – Framing – Flow control – Error control – Data-Link Layer Protocols – HDLC –PPP - Media Access Control – Ethernet Basics – CSMA/CD – Virtual LAN – Wireless LAN (802.11)- Physical Layer: Data and Signals - Performance – Transmission media- Switching – Circuit

5.1 Data Link Layer

- In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data link layer has two sub-layers:

- **Logical Link Control:** It deals with protocols, flow-control, and error control
- **Media Access Control:** It deals with actual control of media

Following services are provided by the Data Link Layer:

- Framing
- Addressing
- Error Control
- Flow Control

5.2 Framing

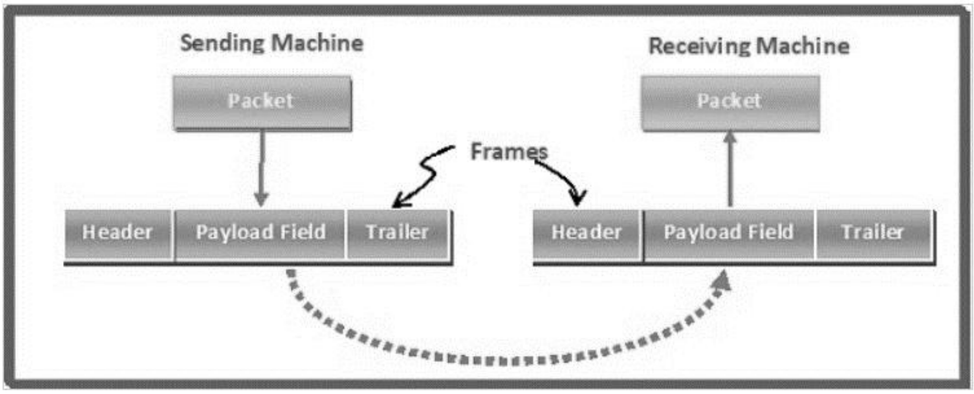
Framing is a point-to-point connection between two computers or devices consisting of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information.

Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Frames have headers that contain information such as error-checking codes.

At the data link layer, it extracts the message from the sender and provides it to the receiver by providing the sender's and receiver's addresses.

The process of dividing the data into frames and reassembling it is transparent to the user and is handled by the data link layer.

Framing is an important aspect of data link layer protocol design because it allows the transmission of data to be organized and controlled.

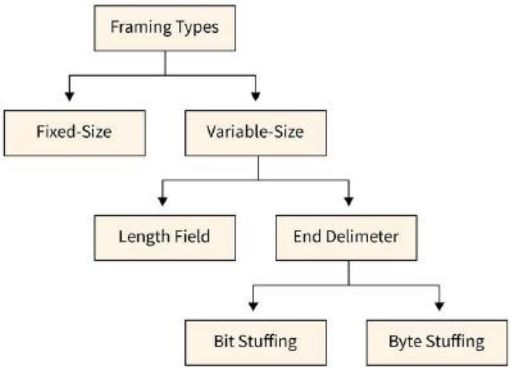


A frame has the following parts −

- Frame Header − 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.
- Flag − It marks the beginning and end of the frame.

Types of framing

There are two types of framing:



1. Fixed-size: The frame is of fixed size and there is no need to provide boundaries to the frame, the length of the frame itself acts as a delimiter.

> **Drawback:** It suffers from internal fragmentation if the data size is less than the frame size
>
> **Solution:** Padding

2. Variable size: The size of the frame is variable during this form of framing. In variable-size framing, we are in need of a way to outline the tip of the frame and also the starting of the succeeding frame. This can be utilized in local area networks (LAN).

There are 2 different methods to define the frame boundaries, such as length field and finish decimeters.

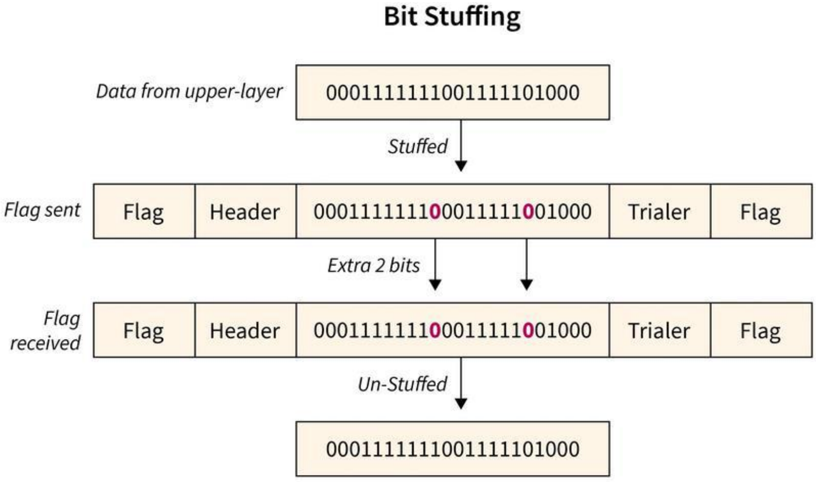
2.1 Length field–To confirm the length of the field, a length field is used. It is utilized in Ethernet (1EEE 802.3).

2.2 End Delimeter–To confirm the size of the frame, a pattern is worn as a delimiter. This methodology is worn in the token ring. In short, it is referred to as ED. Two different methods are used to avoid this condition if the pattern happens within the message.

2.2.1 Bit-Oriented Framing

Most protocols use a special 8-bit pattern flag 01111110 as a result of the delimiter to stipulate the beginning and so the end of the frame. Bit stuffing is completed at the sender end and bit removal at the receiver end.

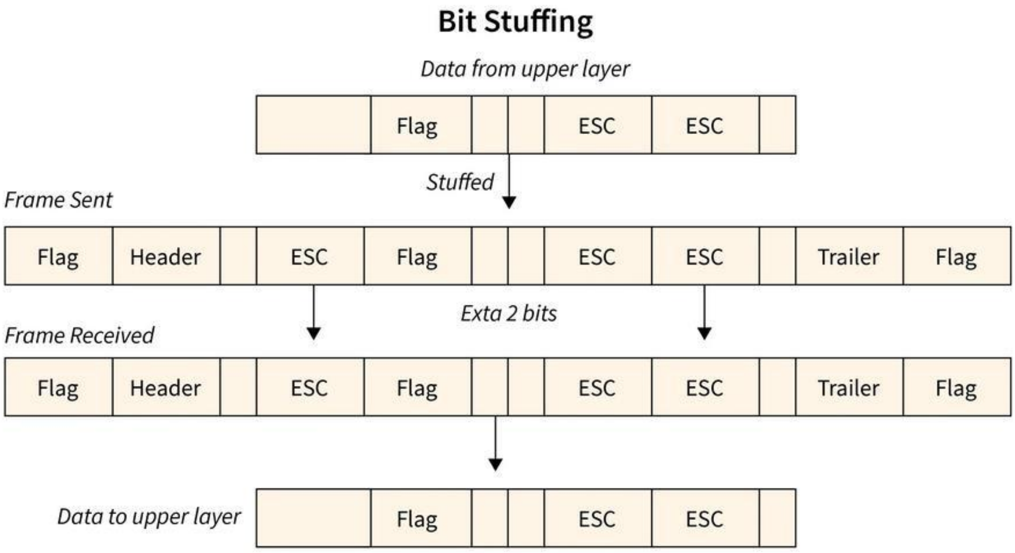
If we have a tendency to get a zero(0) after 5 1s. we have a tendency to tend to still stuff a zero(0). The receiver will remove the zero. Bit stuffing is in addition said as bit stuffing.



2.2.2 Byte-Oriented Framing

Byte stuffing is one of the methods of adding an additional byte once there is a flag or escape character within the text. Take an illustration of byte stuffing as appeared in the given diagram.

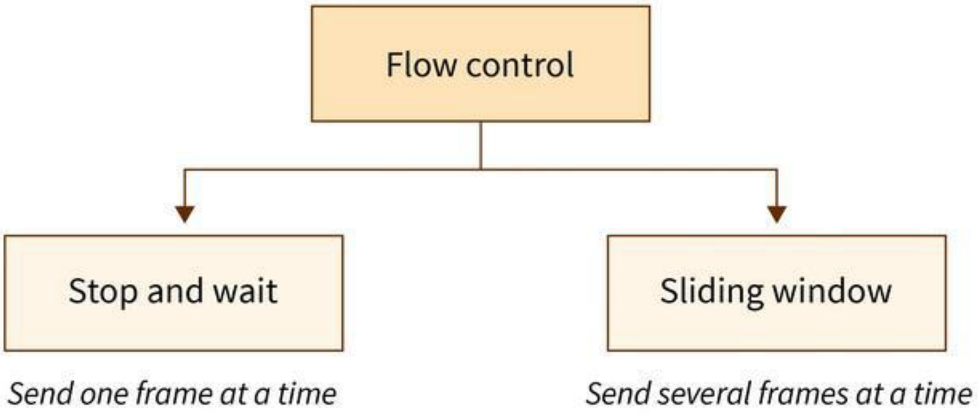
The sender sends the frame by adding three additional ESC bits and therefore the destination machine receives the frame and it removes the extra bits to convert the frame into an identical message.



5.3 Flow Control

Flow control is a set of procedures that restrict the amount of data a sender should send before it waits for some acknowledgment from the receiver.

- Flow Control is an essential function of the data link layer.
- It determines the amount of data that a sender can send.
- It makes the sender wait until an acknowledgment is received from the receiver's end.
- Methods of Flow Control are **Stop-and-wait**, and **Sliding window**.



Stop-and-wait Protocol

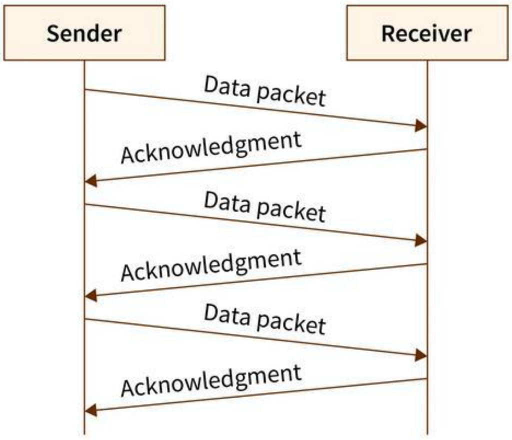
Stop-and-wait protocol works under the assumption that the communication channel is **noiseless** and transmissions are **error-free**.

Working :

- The sender sends data to the receiver.

- The sender stops and waits for the acknowledgment.
- The receiver receives the data and processes it.
- The receiver sends an acknowledgment for the above data to the sender.
- The sender sends data to the receiver after receiving the acknowledgment of previously sent data.
- The process is unidirectional and continues until the sender sends the **End of Transmission (EoT)** frame.

STOPN-AND-WAIT PROTOCOL



Sliding Window Protocol

The **sliding window protocol** is the flow control protocol for noisy channels that allows the sender to send multiple frames even before acknowledgments are received. It is called a **Sliding window** because the sender slides its window upon receiving the acknowledgments for the sent frames.

Working:

- The sender and receiver have a “window” of frames. A window is a space that consists of multiple bytes. The size of the window on the receiver side is always 1.
- Each frame is sequentially numbered from 0 to n - 1, where n is the window size at the sender side.
- The sender sends as many frames as would fit in a window.
- After receiving the desired number of frames, the receiver sends an acknowledgment. The acknowledgment (ACK) includes the number of the next expected frame.

5.4 Error Control

Error control in data link layer is the process of detecting and correcting data frames that have been corrupted or lost during transmission.

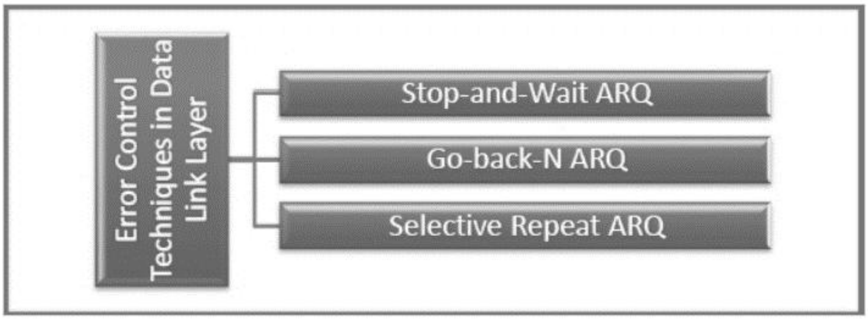
In case of lost or corrupted frames, the receiver does not receive the correct data-frame and sender is ignorant about the loss. Data link layer follows a technique to detect transit errors and take necessary actions, which is retransmission of frames whenever error is detected or frame is lost. The process is called Automatic Repeat Request (ARQ).

The error control mechanism in data link layer involves the following phases −

- **Detection of Error** − Transmission error, if any, is detected by either the sender or the receiver.
- **Acknowledgment** − acknowledgment may be positive or negative.
  - **Positive ACK** − On receiving a correct frame, the receiver sends a positive acknowledge.
  - **Negative ACK** − On receiving a damaged frame or a duplicate frame, the receiver sends a negative acknowledgment back to the sender.
- **Retransmission** − The sender maintains a clock and sets a timeout period. If an acknowledgment of a data-frame previously transmitted does not arrive before the timeout, or a negative acknowledgment is received, the sender retransmits the frame.

Error control technique

There are three main techniques for error control –



Stop and Wait ARQ

This protocol involves the following transitions −

- A timeout counter is maintained by the sender, which is started when a frame is sent.
- If the sender receives acknowledgment of the sent frame within time, the sender is confirmed about successful delivery of the frame. It then transmits the next frame in queue.
- If the sender does not receive the acknowledgment within time, the sender assumes that either the frame or its acknowledgment is lost in transit. It then retransmits the frame.
- If the sender receives a negative acknowledgment, the sender retransmits the frame.

Go-Back-N ARQ

The working principle of this protocol is −

- The sender has buffers called sending window.
- The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.

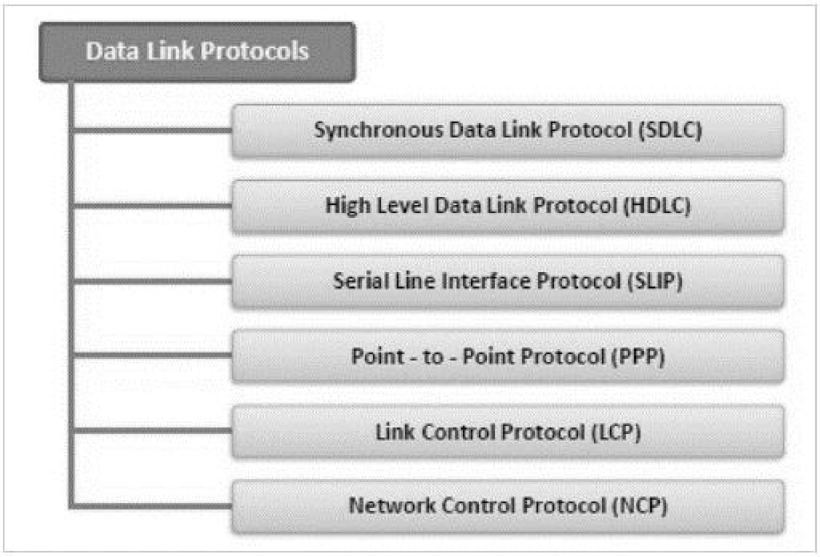
- The receiver receives frames one by one. It keeps track of incoming frame's sequence number and sends the corresponding acknowledgment frames.
- After the sender has sent all the frames in window, it checks up to what sequence number it has received positive acknowledgment.
- If the sender has received positive acknowledgment for all the frames, it sends next set of frames.
- If sender receives NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK

Selective Repeat ARQ

- Both the sender and the receiver have buffers called sending window and receiving window respectively.
- The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.
- The receiver also receives multiple frames within the receiving window size.
- The receiver keeps track of incoming frame's sequence numbers, buffers the frames in memory.
- It sends ACK for all successfully received frames and sends NACK for only frames which are missing or damaged.
- The sender in this case, sends only packet for which NACK is received.

5.5 Data Link Layer Protocols

Data link layer protocol is generally responsible to simply ensure and confirm that the bits and bytes that are received are identical to bits and bytes being transferred. SDLC, HDLC, SLIP, PPP, LCP, LAP, and NCP are some of the data link layer protocols.


Data Link Protocols
Synchronous Data Link Protocol (SDLC)
High Level Data Link Protocol (HDLC)
Serial Line Interface Protocol (SLIP)
Point - to - Point Protocol (PPP)
Link Control Protocol (LCP)
Network Control Protocol (NCP)

SDLC:

SDLC stands for synchronous data link control protocol, is a communication protocol of a computer.

It is usually used to carry system network architecture traffic. Synchronous data link protocol connects all the remote devices to the mainframe computer at the Central location.

This connection is done in two formats, point to point format i.e. one to one connection, and point to multipoint format, i.e. one to many connections.

SDLC support one to many connections even in case of error detection or error recovery.

SDLC ensures that all the received data units are correct and flow is right from one network point to the next network point.

HDLC:

HDLC stands for High-level data link control protocol, is a bit-orientated code transparent synchronous protocol developed by ISO (International organization for standardization) in1979.

It provides both connection-orientated and connectionless services. HDLC protocol contains various wide-area protocols.

It is based on the SDLC protocol that supports both point-to-point and multipoint communication.

HDLC frames are transferred over synchronous or asynchronous serial communication links. HDLC uses various modes such as normal response mode, asynchronous response mode, asynchronous balanced mode.

Normal response mode is used to share the secondary to primary link without contention. asynchronous response mode is used for full-duplex links. asynchronous balanced mode, support combined terminal which can act as both primary and secondary.

SLIP:

SLIP stands for Serial line interface protocol which is used to add framing byte at the end of the IP Packet. SLIP is a data link layer protocol That transforms the IP packets among ISP (Internet Service Providers) and home user over dial-up links.

SLIP is designed to work with ports and router connections. SLIP does not provide error detection, being reliant on upper-layer protocols for this. Therefore, SLIP on its own is not satisfactory over an error-prone dial-up connection.

PPP:

PPP stands for Point to point protocol. PPP is a data link layer protocol that provides the same services as the Serial line interface protocol.

It is a robust protocol that transfers the other types of pockets also with the IP packets. It provides two protocols LCP and NCP, that we will discuss in the next section. Point to point protocol uses framing methods that describe the frames.

Point to point protocol is also called character orientated protocol which is used to detect errors. PPC provides Connection authentication, data compression, encryption, and transmission. It is used over various networks such as phone lines, cellular telephones, serial cables, trunk lines, ISDNs, Specialized radio links, etc.

LCP:

LCP stands for Link control protocol, is a part of point-to-point control protocol. LCP packets determine the standards of data transmission.

LCP protocol is used to determine the identity of the linked devices, if the device is correct it accepts it otherwise it rejects the device.

It also determines whether the size of the packet is accepted or not. If requirements exceed the parameters, then the link control protocol terminates that link.

LAP:

LAP stands for Link access procedure is a data link layer protocol that is used for framing and transfer the data across point-to-point links.

There are three types of Link access procedure – LAPB (Link Access procedure balanced), LAPF (Link Access Procedure Frame-Mode Bearer Services), and LAPD (Link Access Procedure D-Channel.

LAP was originally derived from HDLC (High-Level Data Link Control), but was later updated and renamed LAPB (LAP Balanced).

NCP:

NCP stands for Network control protocol, is a part of the point-to-point protocol. The network control protocol is used to negotiate the parameter and facilities for the network layer.

For every higher-layer protocol supported by PPP, one NCP is there. IPCP (Internet Protocol control protocol), DNCP (DECnet Phase IV Control Protocol), OSINLCP (OSI Network Layer Control Protocol), IPXCP (Internetwork Packet Exchange Control Protocol), NBFCP (NetBIOS Frames Control Protocol), IPV6CP (IPv6 Control Protocol) are some of the NCPs.

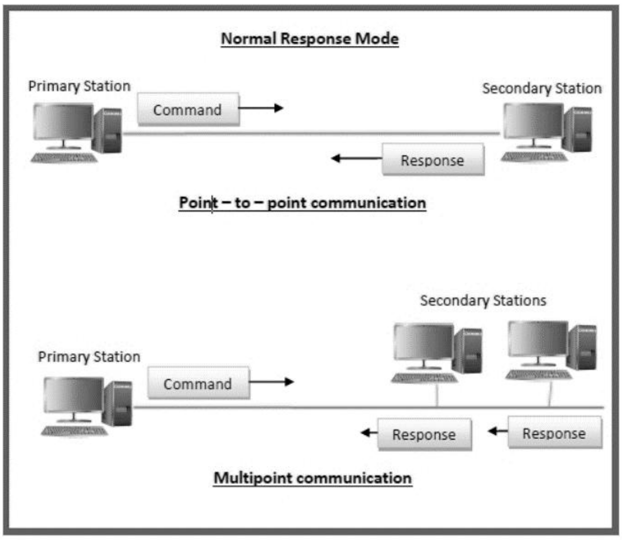
5.6 HDLC

High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

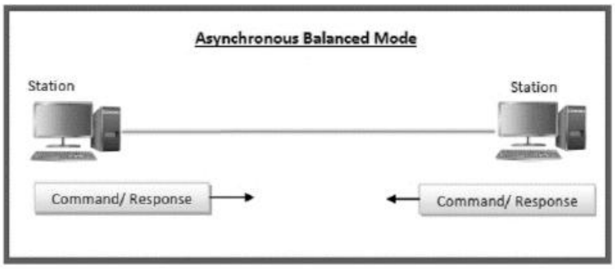
Transfer Modes

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

- **Normal Response Mode (NRM)** − Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.



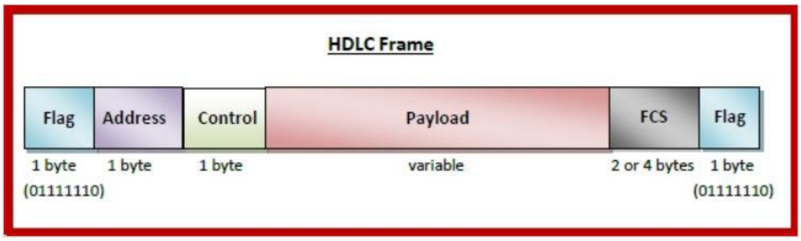
Asynchronous Balanced Mode (ABM) − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** − It is 1 or 2 bytes containing flow and error control information.
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



5.7 PPP

Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds.

Components of PPP

Point - to - Point Protocol is a layered protocol having three components −

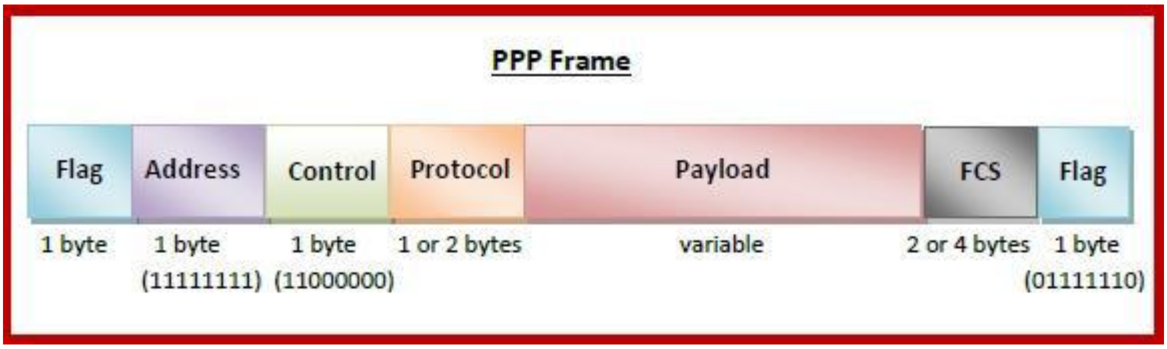
- **Encapsulation Component** − It encapsulates the datagram so that it can be transmitted over the specified physical layer.
- **Link Control Protocol (LCP)** − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
- **Authentication Protocols (AP)** − These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are −
    - Password Authentication Protocol (PAP)
    - Challenge Handshake Authentication Protocol (CHAP)
- **Network Control Protocols (NCPs)** − These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are −
    - Internet Protocol Control Protocol (IPCP)
    - OSI Network Layer Control Protocol (OSINLCP)
    - Internetwork Packet Exchange Control Protocol (IPXCP)
    - DECnet Phase IV Control Protocol (DNCP)
    - NetBIOS Frames Control Protocol (NBFCP)
    - IPv6 Control Protocol (IPV6CP)

PPP Frame

PPP is a byte - oriented protocol where each field of the frame is composed of one or more bytes. The fields of a PPP frame are −

- **Flag** − 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − 1 byte which is set to 11111111 in case of broadcast.
- **Control** − 1 byte set to a constant value of 11000000.
- **Protocol** − 1 or 2 bytes that define the type of data contained in the payload field.

- **Payload** − This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



5.8 Media Access Control

The medium access control (MAC) is a sublayer of the data link layer.

It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

5.8.1 MAC Layer in the OSI Model

The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into two sublayers −

- The logical link control (LLC) sublayer
- The medium access control (MAC) sublayer

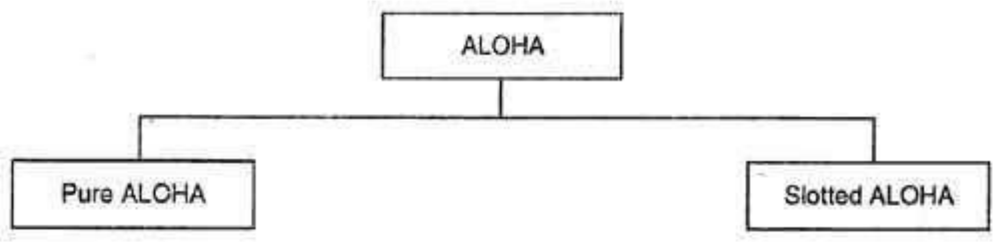
5.8.2 MAC Addresses

MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth. MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

5.8.3 ALOHA:

ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision.

There are two different versions of ALOHA



Types of ALOHA

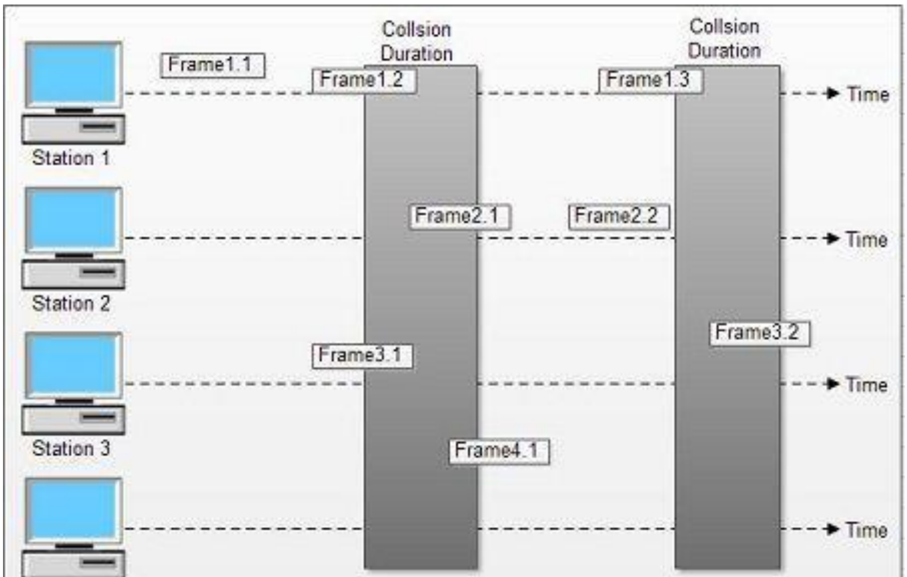
Pure ALOHA

- In pure ALOHA, 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.
- In pure ALOHA, 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 collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.

- Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

- Figure shows an example of frame collisions in pure ALOHA.



Frames in Pure ALOHA

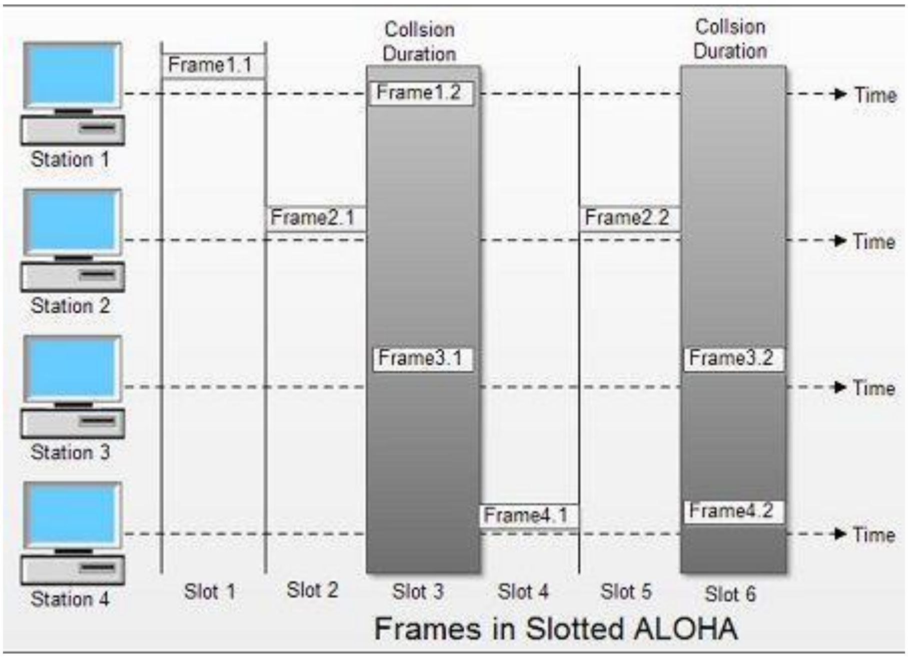
• In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames 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 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.

Slotted ALOHA

• Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.

• In slotted ALOHA, 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.



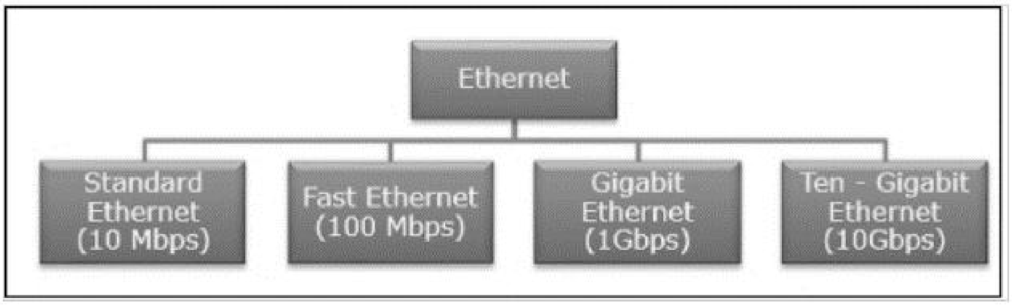
• In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.

• In slotted ALOHA, 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.

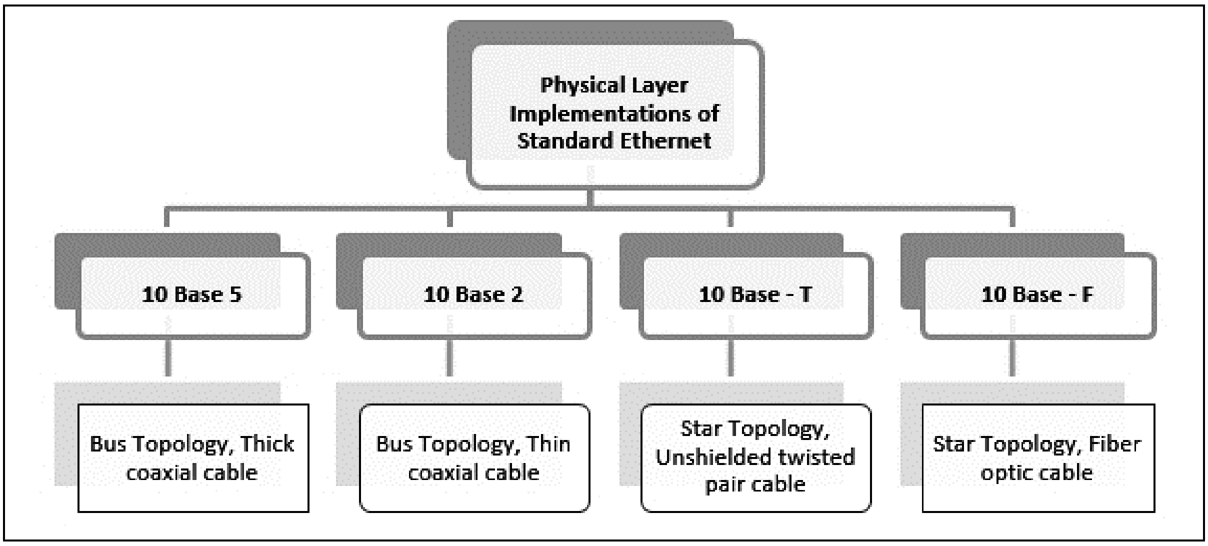
• Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

5.9 Ethernet Basics

Ethernet is a set of technologies and protocols that are used primarily in LANs. However, Ethernet can also be used in MANs and even WANs. It was first standardized in the 1980s as IEEE 802.3 standard. Since then, it has gone through four generations, as shown in the following chart



Standard Ethernet has many physical layer implementations. The four main physical layer implementations are shown in the following diagram


Physical Layer Implementations of Standard Ethernet
10 Base 5
10 Base 2
10 Base - T
10 Base - F
Bus Topology, Thick coaxial cable
Bus Topology, Thin coaxial cable
Star Topology, Unshielded twisted pair cable
Star Topology, Fiber optic cable

10Base5: Thick Ethernet

• The first implementation is called 10Base5, thick Ethernet, or Thicknet.
• 10Base5 was the first Ethernet specification to use a bus topology with an external transceiver(transmitter/receiver) connected via a tap to a thick coaxial cable.

10Base2: Thin Ethernet

•The second implementation is called 10Base2, thin Ethernet, or Cheapernet.

• 10Base2 also uses a bus topology, but the cable is much thinner and more flexible.
• In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

10Base-T: Twisted-Pair Ethernet

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

10Base-F: Fiber Ethernet

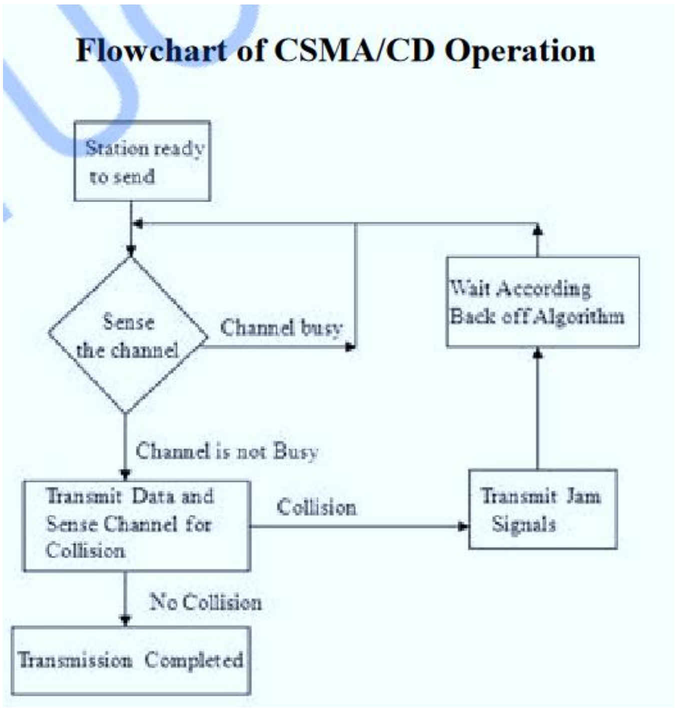
• Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-F.
• 10Base-F uses a star topology to connect stations to a hub.
• The stations are connected to the hub using two fiber-optic cables.

Fast Ethernet (100 Mbps)
Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems.
The 100BASE-T standard consists of three different component specifications –
1. 100 BASE-TX
2. 100BASE-T4
3. 100BASE-FX

Gigabit Ethernet (1 Gbps)
• The Gigabit Ethernet upgrades the data rate to 1 Gbps(1000 Mbps).
• Gigabit Ethernet can be categorized as either a two-wire or a four-wire implementation.
• The two-wire implementations use fiber-optic cable (1000Base-SX, short- wave, or 1000Base-LX, long-wave), or STP (1000Base-CX).
• The four-wire version uses category 5 twisted-pair cable (1000Base-T).

5.10 CSMA/CD

¬ Carrier Sense in CSMA/CD means that all the nodes sense the medium to check whether it is idle or busy.
• If the carrier sensed is idle, then the node transmits the entire frame.
• If the carrier sensed is busy, the transmission is postponed.
¬ Collision Detect means that a node listens as it transmits and can therefore detect when a frame it is transmitting has collided with a frame transmitted by another node.



Transmitter Algorithm in CSMA/CD

¬ Transmitter Algorithm defines the procedures for a node that senses a busy medium.

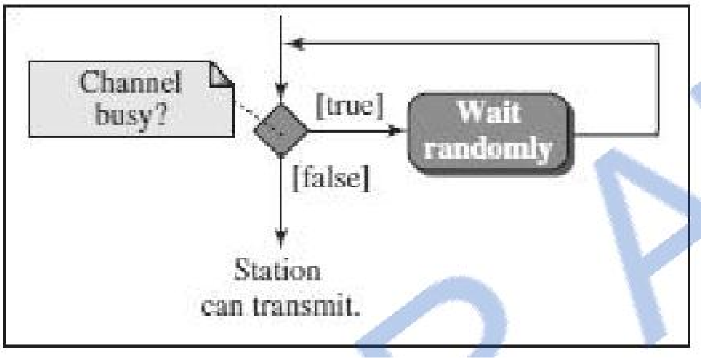
¬ Three types of Transmitter Algorithm exist.

¬ They are

1. Non-Persistent Strategy
2. Persistent Strategy : 1-Persistent & P-Persistent

Non-Persistent Strategy

- In the non-persistent method, a station that has a frame to send senses the line.
- If the line is idle, it sends immediately.
- If the line is not idle, it waits a random amount of time and then senses the line again.

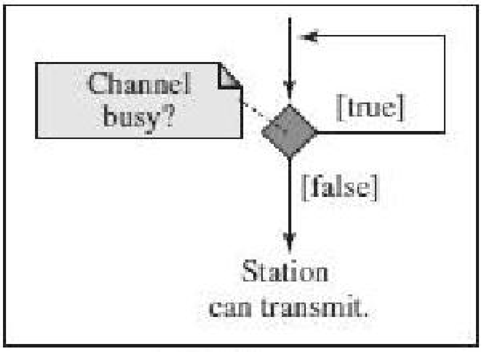


- The non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

Persistent Strategy

1-Persistent :

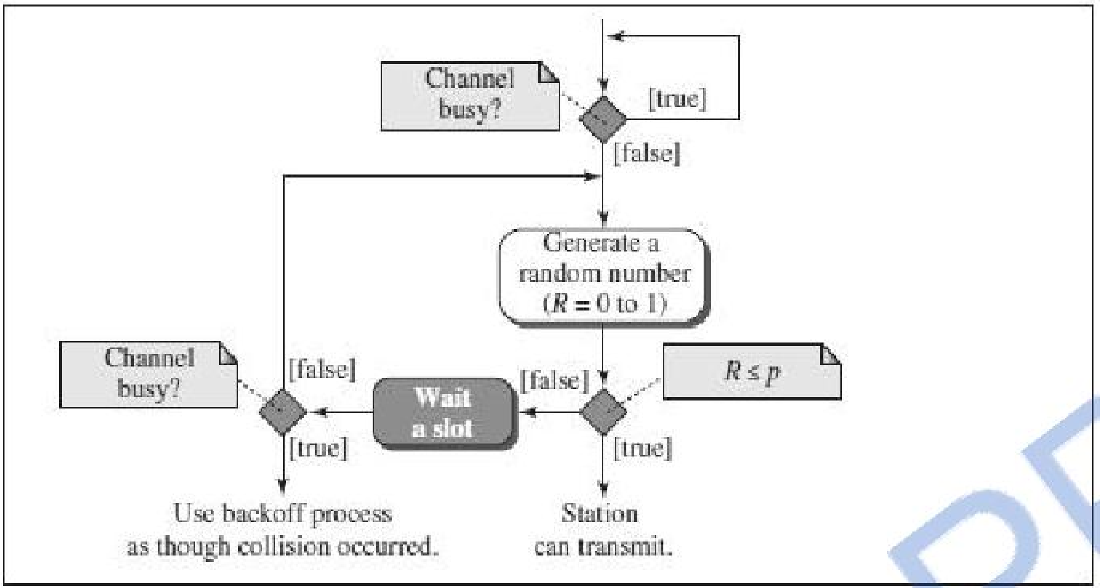
- The 1-persistent method is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).



- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

P-Persistent :

- In this method, after the station finds the line idle it follows these steps:
- With probability p, the station sends its frame.
- With probability q = 1 − p, the station waits for the beginning of the next time slot and checks the line again.



- The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency

EXPONENTIAL BACK-OFF

- Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again.
- Each time it tries to transmit but fails, the adaptor doubles the amount of time

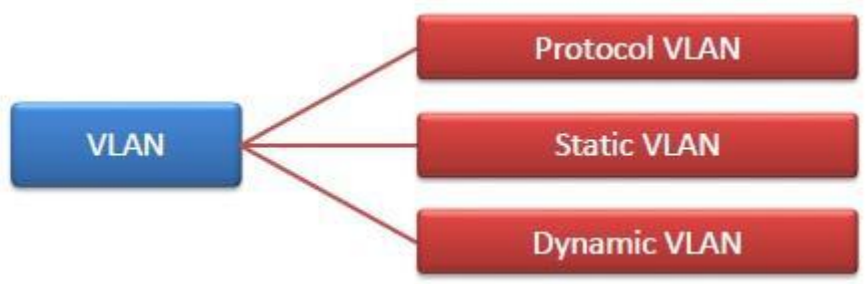
it waits before trying again.

• This strategy of doubling the delay interval between each retransmission attempt is a general technique known as **exponential back-off.**

5.11 Virtual LAN

Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network. Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges. This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.

Types of VLANs



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

5.12 Wireless LAN (802.11)

• Wireless communication is one of the fastest-growing technologies.

• The demand for connecting devices without the use of cables is increasing everywhere.

• Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

ADVANTAGES OF WLAN / 802.11

1. Flexibility: Within radio coverage, nodes can access each other as radio waves can penetrate even partition walls.
2. Planning : No prior planning is required for connectivity as long as devices follow standard convention
3. Design : Allows to design and develop mobile devices.
4. Robustness : Wireless network can survive disaster. If the devices survive,communication can still be established.

DISADVANTAGES OF WLAN / 802.11

1. Quality of Service : Low bandwidth (1 – 10 Mbps), higher error rates due to interference, delay due to error correction and detection.
2. Cost : Wireless LAN adapters are costly compared to wired adapters.
3. Proprietary Solution : Due to slow standardization process, many solution are proprietary that limit the homogeneity of operation.
4. Restriction : Individual countries have their own radio spectral policies. This restricts the development of the technology
5. Safety and Security : Wireless Radio waves may interfere with other devices. Eg; In a hospital, radio waves may interfere with high-tech equipment.

TECHNOLOGY USED IN WLAN / 802.11

¬ WLAN's uses Spread Spectrum (SS) technology.

¬ The idea behind Spread spectrum technique is to spread the signal over a wider frequency band than normal, so as to minimize the impact of interference from other devices.

¬ There are two types of Spread Spectrum:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS)

¬ Frequency hopping is a spread spectrum technique that involves transmitting the signal over a random sequence of frequencies.

¬ That is, first transmitting at one frequency, then a second, then a third, and so on.

¬ The random sequence of frequencies is computed by a pseudorandom number generator.

¬ The receiver uses the same algorithm as the sender and initializes it with the same seed and hence is able to hop frequencies in sync with the transmitter to correctly receive the frame.

Direct Sequence Spread Spectrum (DSSS)

¬ Each bit of data is represented by multiple bits in the transmitted signal.

¬ DSSS takes a user data stream and performs an XOR operation with a pseudo –random number.

¬ This pseudo random number is called as chipping sequence.

TOPOLOGY IN WLAN / 802.11

WLANs can be built with either of the following two topologies /architecture:

- Infra-Structure Network Topology
- Ad Hoc Network Topology

Infra-Structure Topology (AP based Topology)

- An infrastructure network is the network architecture for providing communication between wireless clients and wired network resources.
- The transition of data from the wireless to wired medium occurs via a Base Station called AP(Access Point).
- An AP and its associated wireless clients define the coverage area.

Ad-Hoc Topology (Peer-to-Peer Topology)

- An adhoc network is the architecture that is used to support mutual communication between wireless clients.

- Typically, an ad- hoc network is created spontaneously and does not support access to wired networks.
- An adhoc network does not require an AP.

5.13 Physical Layer

Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations.

Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data.The binary data is then sent over the wired or wireless media.

5.13.1 Data and signals

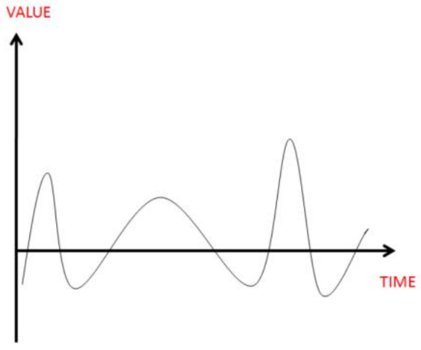
Data or the signal whichever is used in a network, it can be either digital or analog.

Analog and Digital Data

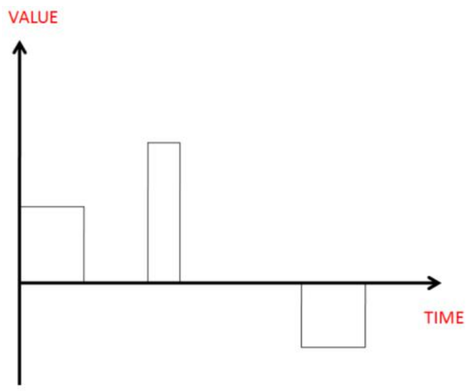
Analog data refers to data that is of continuous format whereas digital data is one which has discrete states. So the analog data takes continuous values and digital data takes discrete values. Analog data can be directly converted into an analog signal or sampled and converted to digital signal. In quite a similar fashion digital data can also be converted to digital signal or into analog signal after modulation. These are converted so that efficient transmission can take place.

Analog and Digital Signal

Similar to data, the signals which represent these can also be digital or analog. Analog signals are known to have many levels of intensity over a given period of time. As the wave moves from one value to another, along the path it traverses via infinite number of values. Digital signals rather have only definite set of values. These are represented using a pair of perpendicular axes. The vertical axis represents the strength of the signal and the horizontal axis gives the time period.



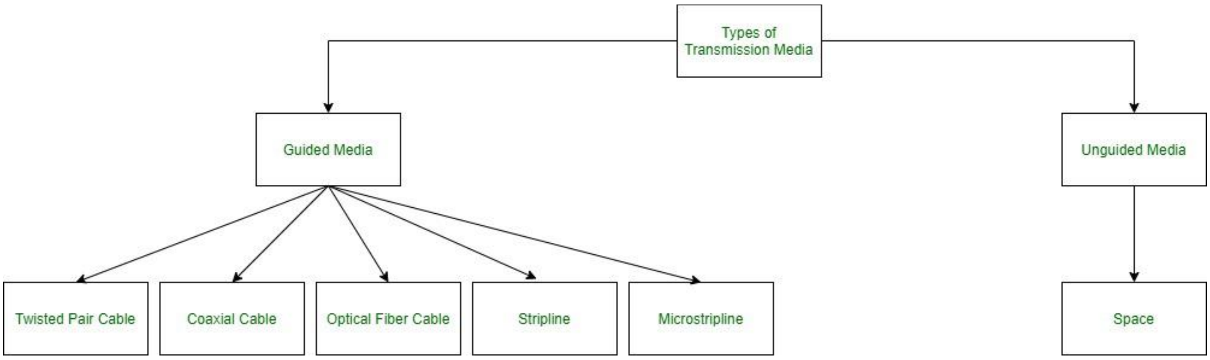
ANALOG SIGNAL



DIGITAL SIGNAL

5.13.2 Transmission Media

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



1. Guided Media: It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links. Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable –
It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP):**
  UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

- ⇢ Least expensive
- ⇢ Easy to install
- ⇢ High-speed capacity

Disadvantages:

- ⇢ Susceptible to external interference
- ⇢ Lower capacity and performance in comparison to STP
- ⇢ Short distance transmission due to attenuation

Applications:

- Used in telephone connections and LAN networks

- **Shielded Twisted Pair (STP):**
  This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

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

(ii) Coaxial Cable –
It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

iii) Optical Fiber Cable –
It uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

- The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

Advantages:

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

(iv) Stripline

Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett of the Air Force Cambridge Research Centre in the 1950s. Stripline is the earliest form of the planar transmission line. It uses a conducting material to transmit high-frequency waves it is also called a waveguide. This conducting material is sandwiched between two layers of the ground plane which are usually shorted to provide EMI immunity.

(v) Microstripline

In this, the conducting material is separated from the ground plane by a layer of dielectric.

2. Unguided Media:
It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 types of Signals transmitted through unguided media:

(i) Radio waves –
These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.

(ii) Microwaves –
It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

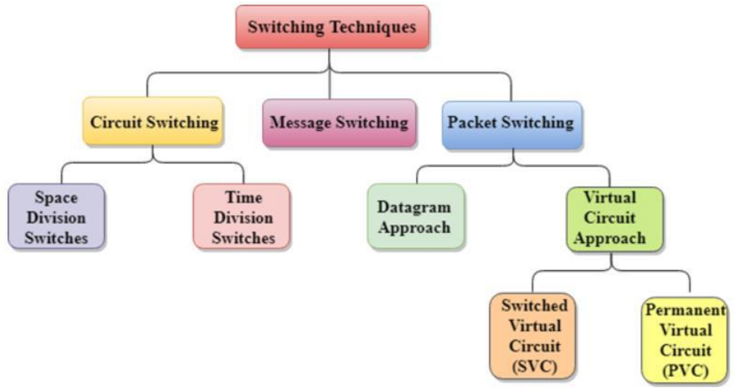
(iii) Infrared –
Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

5.13.3 Switching

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques



Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.

- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.

Time Division Switching

The incoming and outgoing signals when received and re-transmitted in a different time slot, is called **Time Division Switching.**

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the 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.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.

- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.

Approaches Of Packet Switching:

There are two approaches to Packet Switching:

Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.