CS3591 - Computer Networks

Unit - I

Introduction and Application Layer

Data Communication:

Data Communication means the exchange of data between two devices via some form of transmission medium.

1) Characteristics:

i) Delivery:

Data must deliver to the correct destination

ii) Accuracy:

Data must deliver accurately by the system

iii) Timeliness:

The communication system must deliver data in a timely manner.

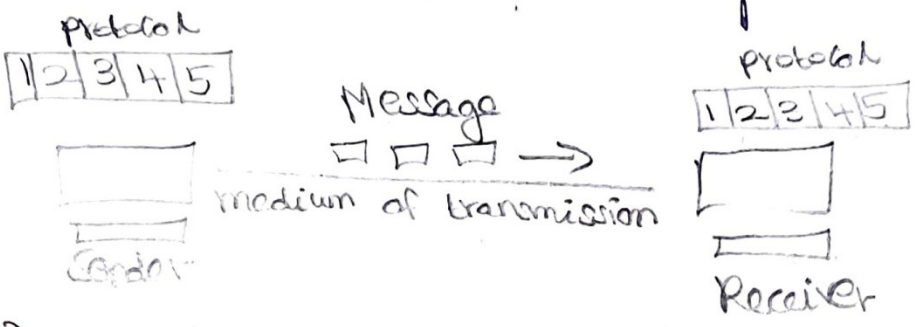
iv) Jitter:

It is a variation in the packet arrival time.

2) Components:

A data communication system

Consists of five components,



i) Message:

The message is data or information to be communicated. It can be text, numbers, pictures or sound.

ii) Sender:

The sender is device that sends data. Various devices can be used to send the data.

iii) Receiver:

The receiver receives the information or message transmitted by sender.

iv) Medium:

It is a physical path through which message passes from sender to receiver. The transmission medium can be twisted-pair cable, Co-axial cable, fiber-optic cable or radio waves.

v) Protocol:

Protocol is a set of rules that

governs data communications. protocol is a predecided terms for communication.

3) Data Representation:

Data is represented in different types:

i) Text:

Text is represented as a bit pattern, a sequence of bits ie 0 or 1. ASCII code is used.

ii) Numbers:

Numbers are also represented by bit patterns. ASCII is not used for numbers.

iii) Images:

Images are also represents by bit patterns. Image is composed of a matrix of pixels.

iv) Audio:

Audio is different from text, numbers and images. Audio refers to the recording or broadcasting of sound or music. It is continuous, not discrete.

v) Video:

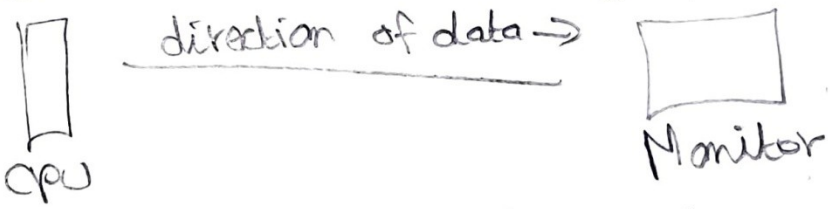
It refers to the recording or broadcasting of a picture or movie.

4) Data Flow:

Communication between two devices ie sender and receiver can be of three types:

i) Simplex:

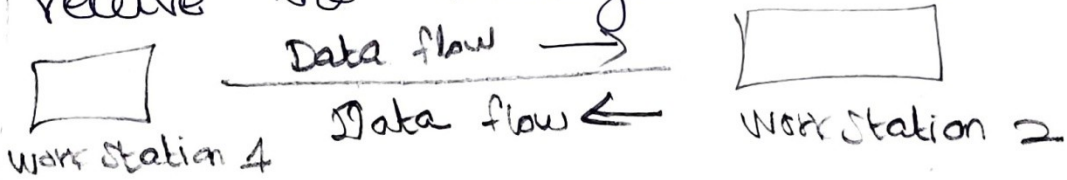
Data can flow in one direction only. one device can transmit data and other device accepts the data and works accordingly.



Typical example of simplex communication is a computer system, data flow from cpu to monitor or from keyboard to monitor in one direction only.

ii) Half-Duplex:

Each station can transmit or receive the message.



An important condition in half-duplex mode is that both devices can not transmit at a time. The entire channel capacity is used by any device transmitting at that time.

iii) Full-Duplex:

In full-duplex mode, both stations can transmit and receive simultaneously.

In full-duplex mode of communication, data flow in both directions share the channel capacity. Eg: Telephone network. Subscriber at both ends can talk and listen at same time.

Networks:

A network is a set of devices interconnected by a communication medium. Each device is referred to as a node. A node can be a computer, printer or any other computing device.

Network criteria:

A network must satisfy following criteria

i) Performance:

It can be measured by transit time and response time. performance is decided by many factors such as number of users, type of transmission medium, hardware and software.

ii) Reliability:

A network reliability is measured by accuracy, failure rate, establishment time and robustness.

iii) Security:

Network security concerned with protection of data from unauthorized access.

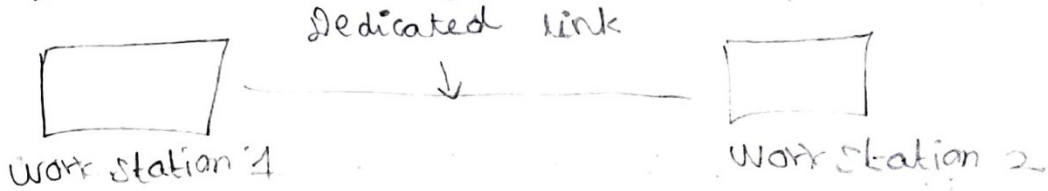
1) Physical Structure:

It includes some network attributes such as type of connections and topologies.

2) Type of Connections:

The nodes in computer network are interconnected by some link. The link can be of 2 types.

i) point-to-point:

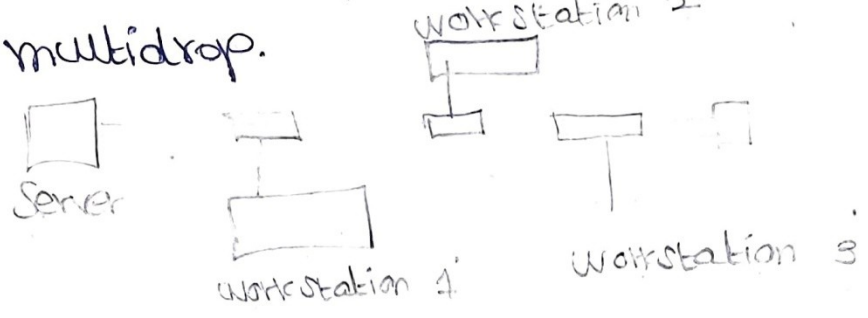


There is a dedicated link between two devices/nodes. The link capacity is shared between two nodes only. The link can be a cable or microwave link.

Eg: TV and its remote control.

ii) Multipoint:

When two or more devices/nodes share a common link. It is also called as multidrop.



Network Types:

i) Local Area Network (LAN):

* The IEEE 802. LAN is a popularly used shared medium peer-to-peer communications network that broadcasts informations for all stations to receive.

* The LAN enables stations to communicate directly using a common physical medium on a point-to-point basis without any intermediate switching node.

* A LAN is a system composed of computer hardware and transmission media and software.

* LANs are privately owned networks within a single building or campus of upto few km in range. It generally use only one type of transmission media.

* Depends upon application and cost, Various topology used in LAN, Eg: Star, bus, ring
* The basic idea of a LAN is to provide easy access to Data Terminal Equipment (DTEs) within the office. These DTEs are not only computers but other devices such as printer, plotters and electronic files and databases.

2) Metropolitan Area Networks (MAN):

* A MAN, while larger than LAN is limited to city or group of nearby corporate offices. It uses similar technology of LAN.
* Its sponsored by IEEE, ANSI and Regional bell operating companies. It is organized around a topology and technique called

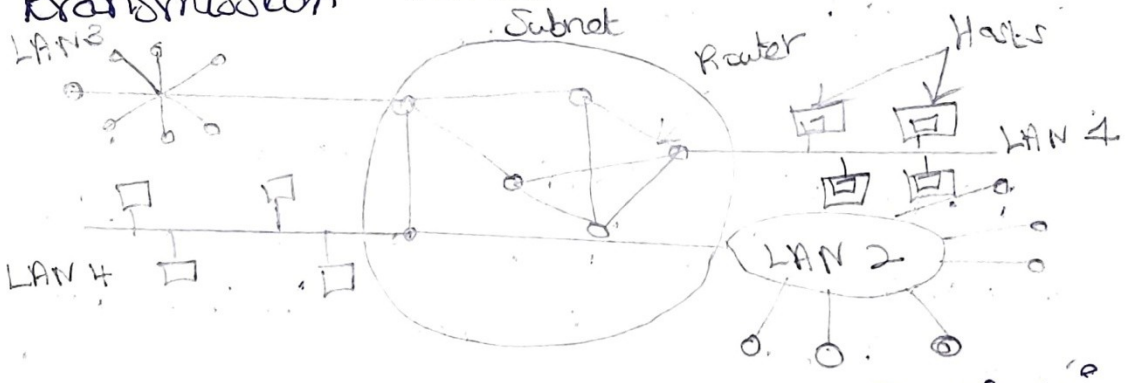
Distributed Queue Dual Bus (DQDB).

* MAN provides the transfer rates from 34 to 150 Mbps.
* MAN is designed with two unidirectional buses. Each bus is independent of the other in transfer of traffic. The topology can be designed as an open bus or a closed configuration.
* MANs are based on fiber optic transmission technology and provide high speed interconnection between sites. It can support both data and voice.
* MAN as a special category is a Standard has been adopted for them and Standard is now being implemented. It is called IEEE 802.6

3) Wide Area Networks (WAN):

* A WAN provides long distance transmission of data and voice.
* A WAN covers a larger area such as city, State, country or the world is called Wide Area Network.

* The WAN contains host and collection of machines. User program is installed on host and machines. All the host are connected by each other through communication subnet. Subnet carries messages from host to host.
* Subnet consists of transmission lines and switching elements. The transmission line is used for data transfer between two machines. Switching elements are used for connecting two transmission lines.



* Switching elements are specialized computers. It selects the proper outgoing line for incoming data and forward the data on that line.
* The switching elements are basically computers and they are called packet switching nodes, intermediate

Systems and data switching exchanges. These switching elements are also called routers.

* Each host is connected to a LAN on which router is present. Sometimes the host can be directly connected to the router. The interconnection of routers forms the Subnet.

* In the WAN, when the packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety. This packet is stored in that router until the required output line is free.

* The subnet uses this principle is called point-to-point, store and forward or packet switched subnet.

* Almost all WANs use store and forward Subnets. If the packets are small and of same size, they are also called cells.

* In the point-to-point subnet, the router interconnection topology becomes important. WANs can also use satellite or ground radio system. The routers have antenna, through which they can send or receive data, they can listen from satellite.
* WAN uses hierarchical addressing because they facilitate routing. Addressing is required to identify which network input is to be connected to which network output.

4) Wireless Networks:

* A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier. The last link with the users is wireless, to give a network connection to all users in a building or campus. The backbone network usually uses cables.
* Wireless LANs operate in almost the same way as wired LANs using the same networking protocols and supporting the most of same applications.

Protocol Layering:

* A computer network must provide general, cost effective, fair and robust connectivity among a large number of computers. Designing a network to meet these requirements is no small task.
* To deal with complexity, network designers have developed general blue prints- usually called network architectures. It guides the design and implementation of networks.

1) Layered Architecture:

* Computer network is designed around the concept of layered protocols or functions. For exchange of data between computers, terminals or other data processing devices, there is data path between two computers either directly or via a communication network.

Following factors should be considered.

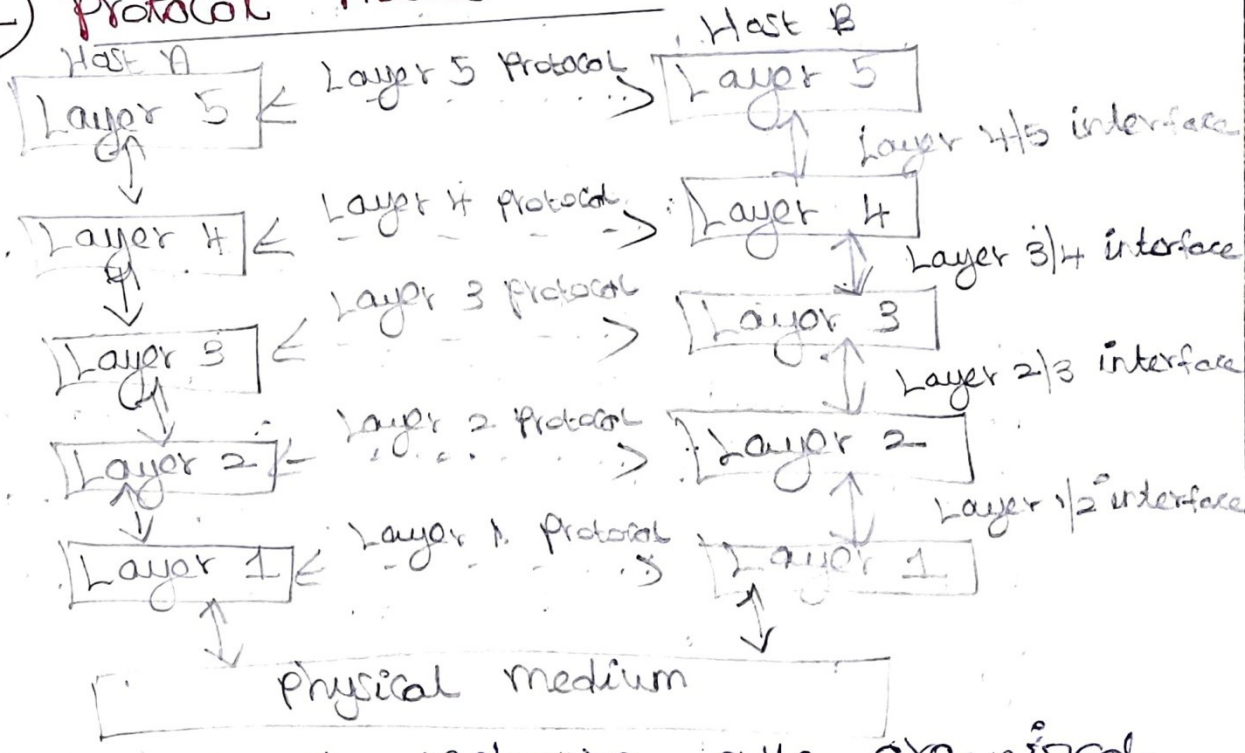
i) The source system must either activate the direct data communication path or inform the communication network to the identity of desired destination system.

ii) provide for standard interface between network functions.

iii) provide for symmetry in function performed at each node in the network. Each layer performs the same functions as its counter part in the other node of network.

The network software is now highly structured.

2) Protocol Hierarchies:

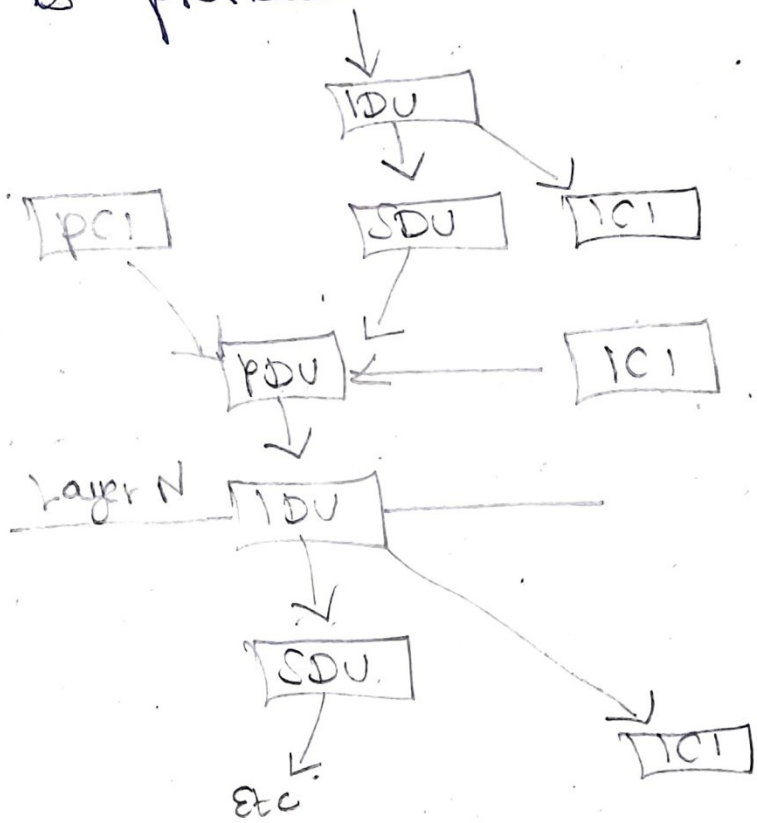


* Most of all networks are organized as a series of layers, each one built upon the one below it.
* A layer is a service provider and may consists of several service functions. Function is a sub system of a layer.

* Each subsystem may also be made up of entities. An entity is a specialized module of a layer or subsystem.
* Name of the layer, total number of layer, function and content of each layer differ from network to network.
* protocols are the rules that govern network communication.
* Layer n on one node carries on a conversation with layer n other node.
* The entities comprising the corresponding layers on different machine are called peers.
* The actual data flow is from upper layer to its below layer and then from physical medium to destination layer.
* Between each pair of adjacent layers is called interface. The interface defines which primitive operations and services the lower layer offers to the upper one.
* A set of layers and protocols is called a network architecture.

3) Interfaces and Services:

The process provides a common technique for the layer to communicate with each other. The Standard terminology used for layered networks to request services is provided.



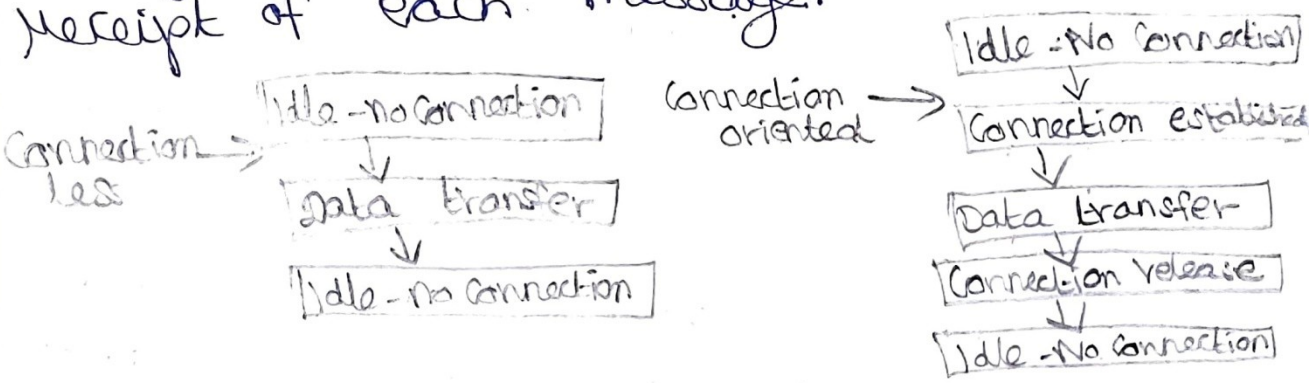
* The layers N+1, N and N-1 are involved in the communication process for layer communication with each other.
* When the IDU from layer N+1 passes to layer N, it becomes SDU to that layer. PCI is added to SDU at layer N. ICI performs its function and is discarded.

* Each layer adds header to data. This header is used by the peer layer entity at another node of network to invoke function. This process repeats itself through each layer.
* As each unit traverses through the layer, it has a header added to it ie user data and header. This full protocol data unit is passed on to the communication path, where it arrives at the receiving site.

ii) Connection oriented and Connectionless Services:

* Connection oriented and connectionless are the two types of services that is offered by the layer.
* In Connection oriented, direct path is established between source and destination. Eg: Telephone system.
* The connectionless service goes directly from an idle condition into a data transfer mode, followed directly by idle condition.

* It is comparable to mailing a letter. Each message carries the full destination address and each one is routed through the system independent of all the others.
* Each service can be characterized by QoS. Some services are reliable in the sense that they never lose data.
* A reliable service is implemented by having the receiver acknowledge the receipt of each message.



5) Relationship of services to protocols:

* Service interface provides an entry point that users use to access the functionality exposed by the application.
* Service interface is usually network addressable.
* It provides a much more coarse-grained interface while preserving the semantics and finer granularity of the application logic.

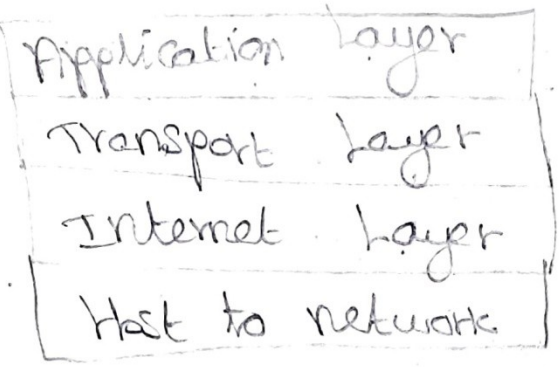
It also provides a barrier that enables the application logic to change without affecting the user of the interface.

* The service interface should encapsulate all aspects of the network protocol used for communication between the user and service.

TCP/IP Protocol Suite:

* The internet architecture is also sometimes called the TCP/IP architecture after its two main protocols.
* TCP/IP stands for Transmission Control Protocol/Internet protocol.
* The TCP/IP reference model is a set of protocols that allows communication across multiple diverse networks.
* TCP/IP is normally to be a four layer system. Layers of TCP/IP are Application Layer, Transport Layer, Internet Layer, Host to network layer.
* Host to network layer is also called physical and data link layer.

* The application layer in Tcp/ip can be equated with the combination of session, presentation, application layer of OSI reference model.
* Tcp/ip defines two protocol at transport layer: Tcp and Udp.
* User Datagram protocol is a connectionless protocol.
* Udp is used for application that requires quick but necessarily reliable delivery.



* Internet layer also called network layer It handles communication from one machine to the other.

i) Application layer:-

It includes all process and services use transport layer to deliver data. The most widely known

application protocols are: TELNET, FTP, SMTP and SNMP.

ii) Transport Layer:

Application programs send data to the transport layer protocols Tcp and UDP. An application is designed to choose either Tcp or UDP based on services.

iii) Internet Layer:

It handle machine to machine communications.

a) Addressing:

Determining the route to deliver data to the destination host.

b) Fragmentation:

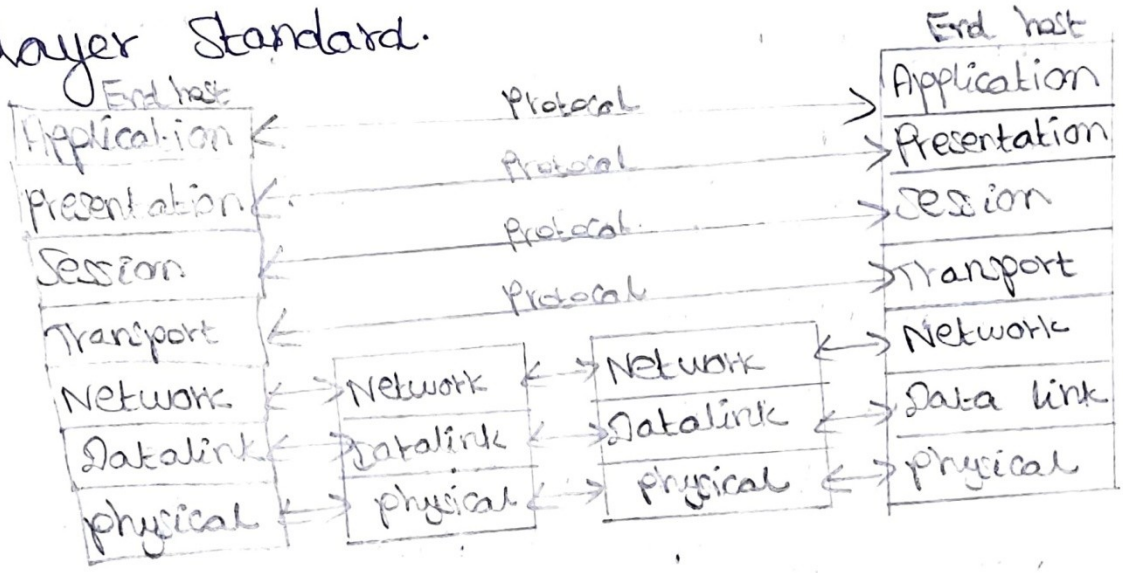
Breaking the messages into pieces if an intervening network cannot handle a large message.

iv) Host to network:

It is also called network interface layer. It is same as physical and data link layer of OSI model. Host to network layer cannot define any protocol.

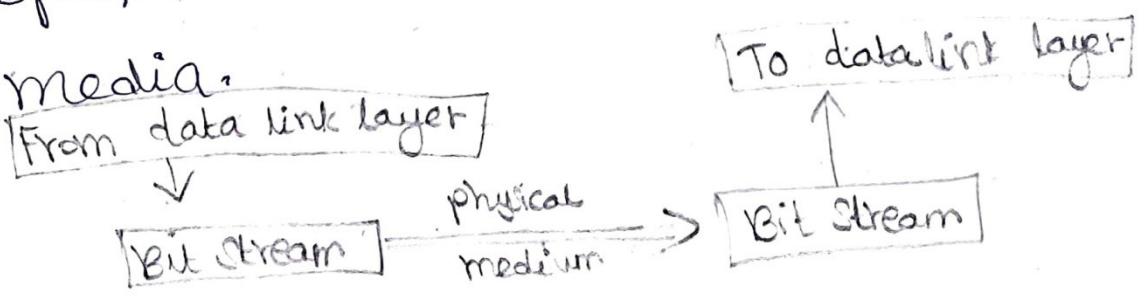
OSI Model:

The ISO was one of the first organizations to define a way to connect computers. Their architecture called the open System Interconnection (OSI) reference model. It is a Seven layer Standard.



1) Physical Layer:

* Physical layer is the lowest layer of the OSI model.
* It transmit a bit stream over a communication channel.
* It deals with electrical and mechanical specification of interface and transmission media.



i) Physical characteristics of interfaces and media:-

The design issue of physical layer considers the characteristics of interface between devices and transmission media.

ii) Representation of bits:-

Physical layer encodes the bit stream into electrical or optical signal.

iii) Data rate:-

It defines the duration of a bit is called as data rate or transmission rate.

iv) Synchronization of bits:-

The transmission rate and receiving rate must be same. It is done by synchronizing clocks at sender and receiver. It performs this function.

2) Data link layer:-

It is responsible for transmitting frames from one node to the next. It transforms the physical layer to a reliable link making it an error free link to upper layer.

i) Framing:-

The frames received from network layer is divided into manageable data

units called frames.

ii) Physical addressing:

When frames are to be sent to different LANs, the data link layer adds a header to the frame to define sender or receiver.

iii) Flow Control:

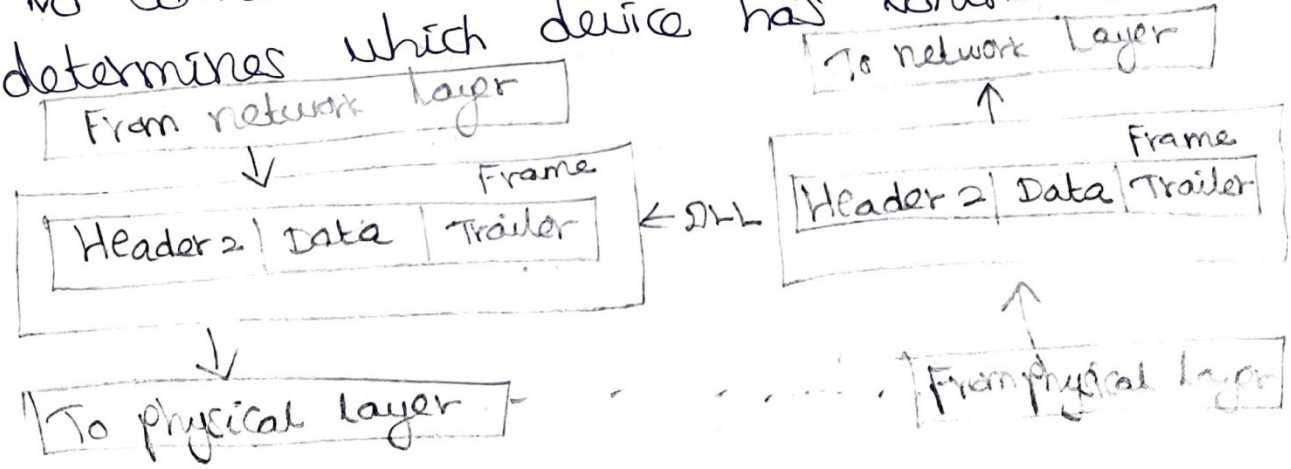
When the rate of the data transmitted and rate of data reception by receiver is not same, some data may be lost. It imposes flow control mechanism to prevent overwhelming the receiver.

iv) Error Control:

It incorporates reliability to the physical layer by adding mechanism to detect and retransmit damaged or lost frames.

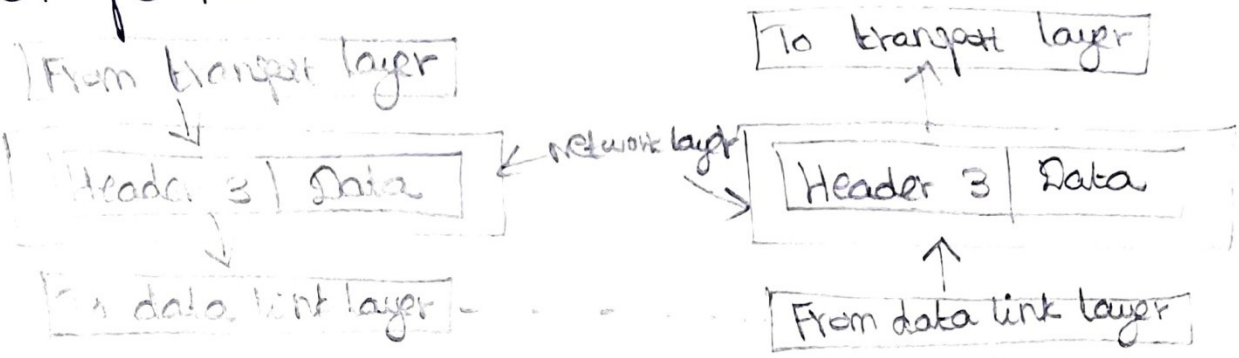
v) Access Control:

When multiple devices are connected to same link, the data link layer determines which device has control over link.



3) Network layer:

It is responsible for the delivery of packets from source to destination.



i) Logical Addressing:

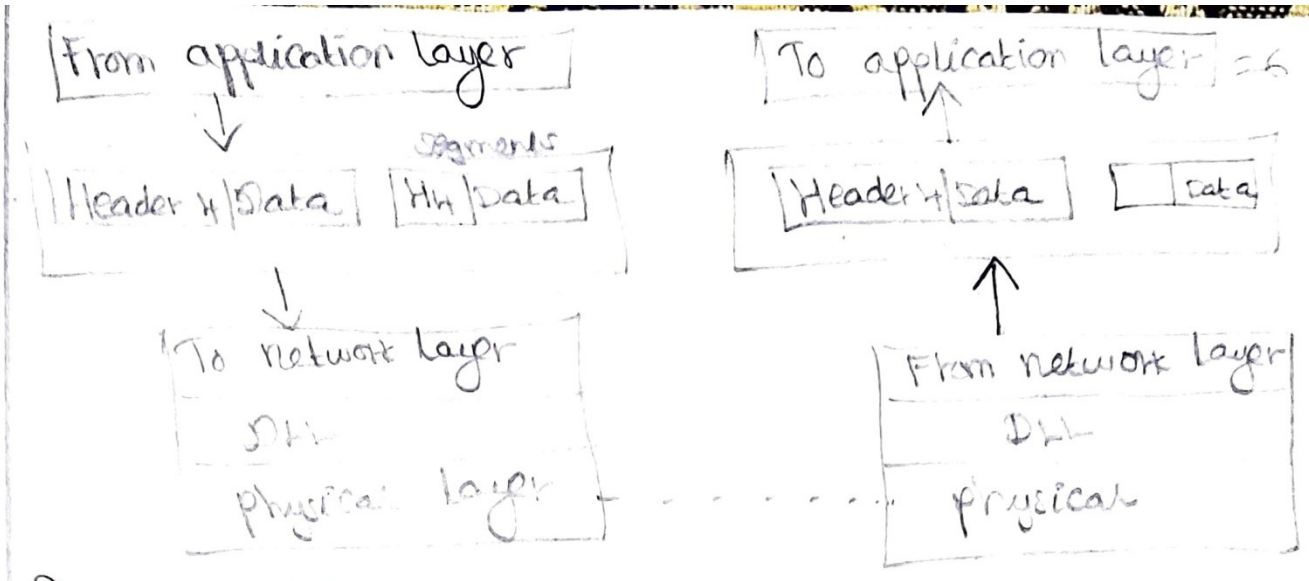
Data link layer implements physical addressing. When a packet passes network boundary, an addressing system is to distinguish source and destination, perform these function. It adds a header to the packet of upper layer includes logical addresses of sender and receiver.

ii) Routing:

It route or switch the packets to its final destination in an internet work.

4) Transport layer:

It is responsible for delivery of message from one process to another. It ensures the whole message arrives intact inorder with error control and Process control.



i) Port Addressing:

Computer performs several operations simultaneously. process-to-process delivery means specific process of one computer must be delivered to specific process on other computer. It include port address.

ii) Segmentation and reassembly:

A message is divided into segments, each segment contains a sequence number which enables transport layer to reassemble at destination.

iii) Connection Control:

It performs connectionless or connection oriented services with the destination machine.

iv) Flow control:

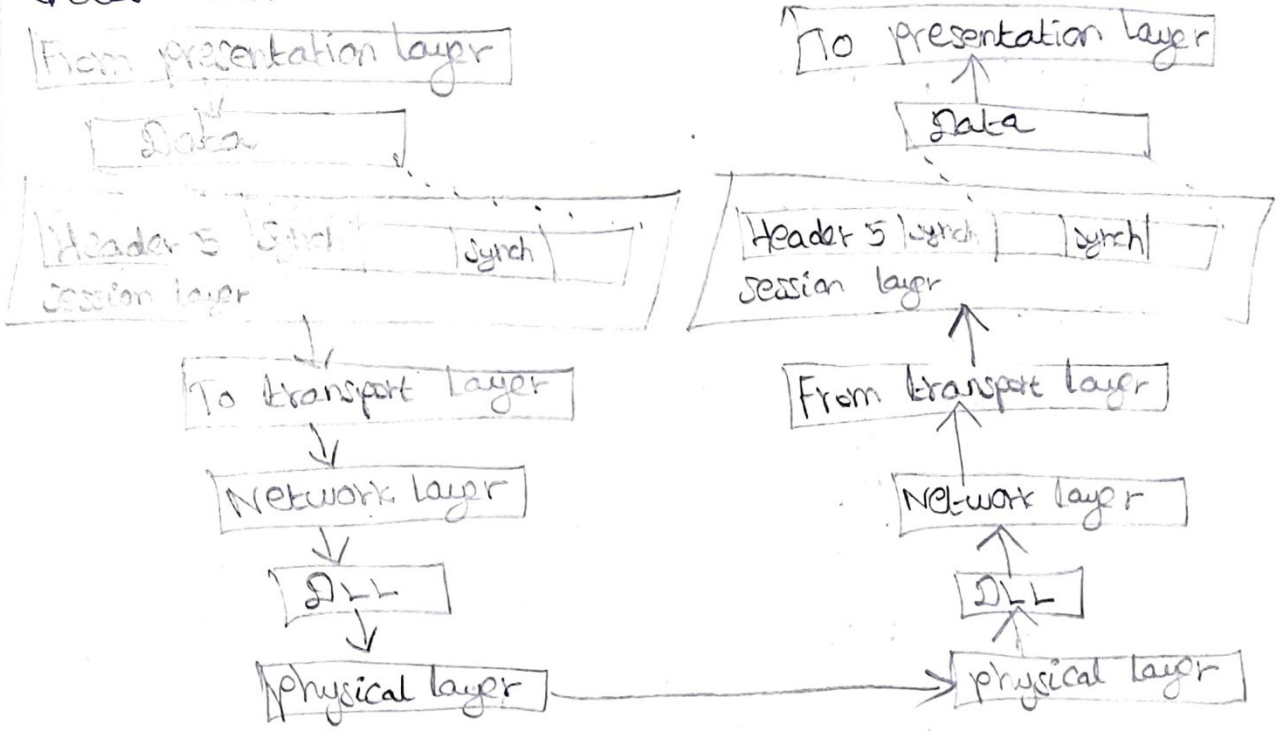
It performs end-to-end flow control while data link layer performs its link.

v) Error Control:

It is performed on end-to-end basis rather than across the link. It ensures error free transmission.

5) Session layer:

It is network dialog controller. ie it establishes and synchronizes the interaction between communication system.



i) Dialog Control:

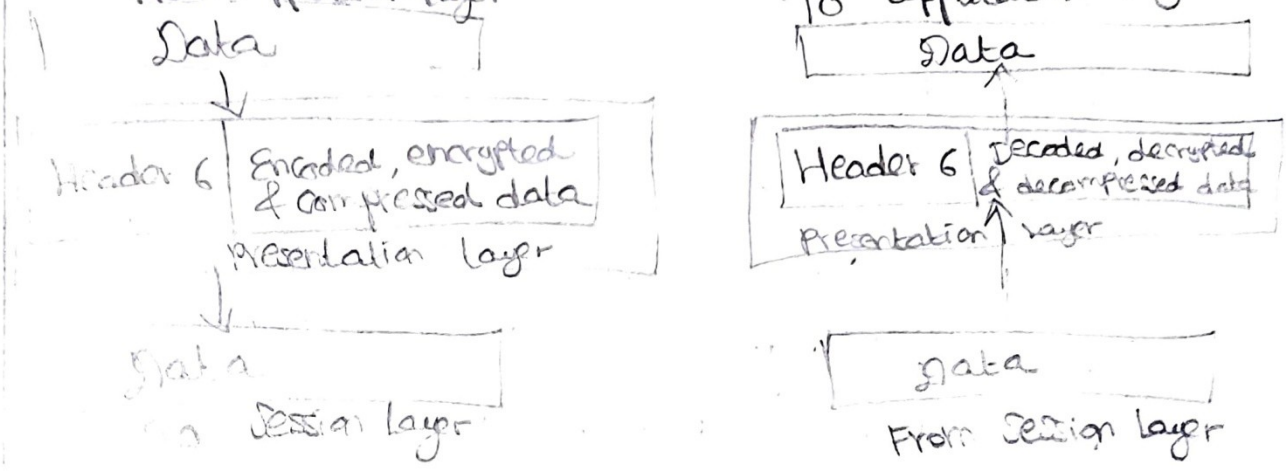
Communication between two processes take place in either half duplex or full-duplex mode. It manages dialog control for communication.

ii) Synchronization:

It adds synchronization points into stream of data.

6) Presentation layer:

It deals with Syntax and Semantics of the information being exchanged.



i) Translation:

Different computers use different encoding systems. The presentation layer maintains interoperability between two encoding systems.

ii) Encryption:

It is transforming sender information to other form to ensure privacy while transmission. Decryption is a reverse process.

iii) Compression:

It is a technique of reducing number of bits required to represent the data.

7) Application Layer:

It is responsible for accessing the network by user. It provides user interfaces and other supporting services such as e-mail, remote file access, file transfer, sharing database, message handling, directory services.

i) Network Virtual Terminal:

It is a software version of physical terminal that allows a user to log onto a remote host.

ii) File Transfer, Access and Management:

It allows user to access files in remote hosts, to retrieve files and to manage files in remote computer.

iii) Mail Services:

E-mail forwarding, storage are the services under this category.

iv) Directory Services:

It include access for global information and distributed database.

Introduction to Sockets:

* Clients and servers establish connections and communicate via socket. Sockets are the end points of internet communication. Connections are communication links are created over the internet using Tcp.
* Client create client socket and connect them to server sockets.
* Sockets are associated with host address and a port address. The host address is Ip address of the host where the client and server program is loaded. The port address is the communication port used by the client or server program.
* Server programs use the well-known port number associated with their application protocol. A client communicate with server by establishing a connection to the socket of the server. The client and server then exchange data over the connections.
* Before an application program can transfer any data, it must first create an end point for communication by calling

Socket. Socket facilities are provided in C language. To use these facilities, the header files <type.h> and <socket.h> must be included in the program. Its prototype is

int socket (int family, int type, int protocol);

* The type identifies the semantics of communication.
* The protocol identifies the specific protocol to be used. only one protocol is available for each family and type.
* After a socket is created, the bind system call can be used to assign an address to the socket. Its prototype is,

int bind (int sd, struct sockaddr *name, int namelen);

where sd is the socket descriptor returned by the socket call, name is a pointer to an address structure that contains local ip address and port number. Namelen is the size of address structure in bytes. The bind system call returns 0 on success and -1 for failure.

* A connection-oriented server indicates its response to receive connection request by calling listen the prototype is,

int listen(int sd, int backlog);

where sd is socket descriptor returned by the socket call and backlog specifies the maximum number of connection request that system should queue while it waits for server to accept them.

* Server can accept the connection request after listen call. The prototype for accept is:

int accept(int sd, struct sockaddr *addr, int *addrlen);

After this client and server transmit data using write and read system calls.

* The prototype used for close call is:

int close(int sd);

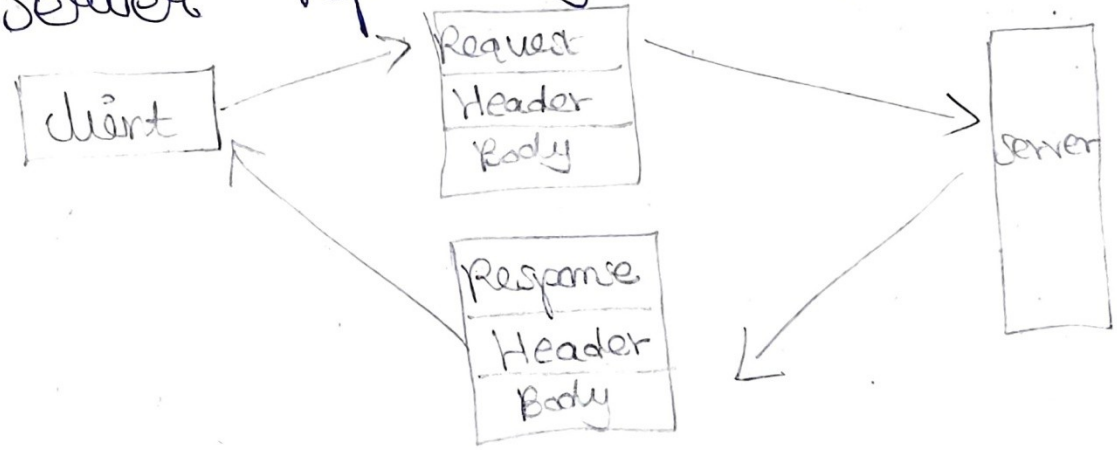
If socket is closed successfully, it returns 0 otherwise -1 for failure.

Application layer protocols:

* World wide web, electronic mail System and domain name system are the traditional application of the application layer network.
* Applications need their own protocols. These applications are part network protocol and part traditional application program.
* Two of the most popular applications are World wide web and Email system.
* HTTP is an application protocol. It is used to retrieve web pages from remote servers.
* A web client uses application programs like Internet Explorer, chrome, Firefox and mozilla. All of them use HTTP protocol for communication with web server.
* SMTP is used to exchange electronic mail.
* HTTP is used to communicate between web browsers and web servers.

HTTP:

* The Standard web transfer protocol is Hyper Text Transfer protocol.
* It consists of two fairly distinct items: The set of requests from browsers to servers and the set of responses going back the other way.
* HTTP uses the services of TCP, HTTP is a stateless protocol.
* The client initializes the transaction by sending a request message. The server replies by sending a response.



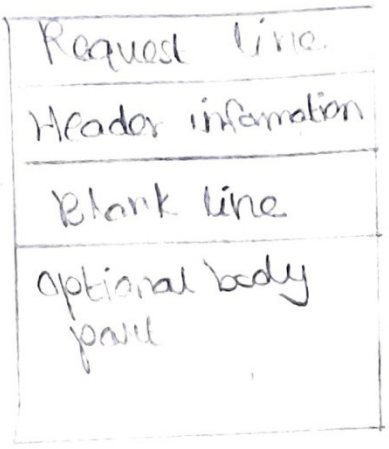
i) HTTP Messages:

HTTP messages are two types.

i) Request ii) Response

* Both message type used same format.
* Request message consists of a request

line, headers and a body.



* Request line defines the request type, resource, HTTP version.
* URL is a standard for specifying any kind of information on the internet. The URL defines 4 things. method, Host computer, port, path.
* The method is the protocol used to retrieve the document.
* The host is the computer where the information is located.
* The URL contain the port number of the server.
* path is the path name of the file where the information is located.

http://www.gracecoe.org/home.html

http: protocol
www: subdomain
gracecoe: domain name
org: Top level domain
home.html: File path

2) HTTP Headers:

* Header can be one or more header lines. Each header line is made of a header name, a colon, a space and a header value.
* The header exchange additional information between the client and server.
* A header line belongs to one of 4 categories:

i) General Header:

It includes general information about the message. Request and a response both contains general header.

ii) Request header:

It can be present only in a request message. It specifies the client configuration and the client preferred document format.

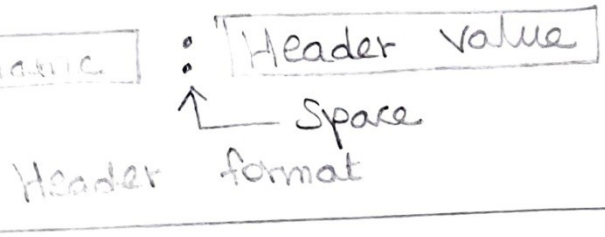
iii) Response header:

It can be present only in a response message. It specifies the server configuration and special information about the request.

iv) Entity header:

It gives information about the body

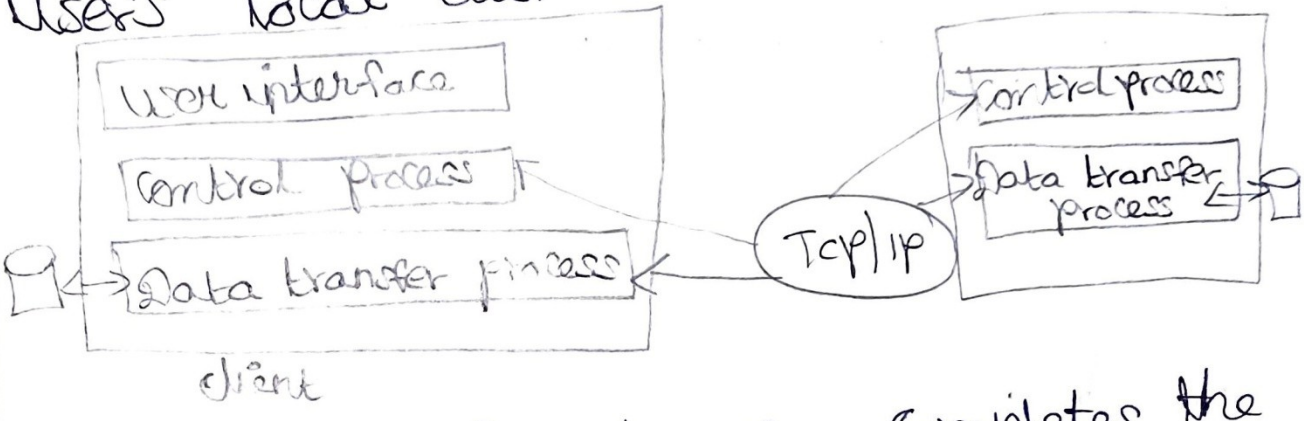
of the document. It is mostly present in response messages, Some request message such as post and put methods that contain a body also use this type of header.



FTP:

* File Transfer protocol is most frequently used Tcp/ip applications
* It is designed for distributing file to a number of users. It uses a client-server system in which files are stored at a central computer and transferred between computer and other, widely distributed computers.
* The central computer runs FTP server software and widely distributed computer runs FTP client software. FTP is interactive.
* FTP uses Tcp/ip software to contact the computer.
* FTP server locates the file that the user requested and uses Tcp to

Send a copy of entire contents of file across the Internet to the client. As the client program receives data, it writes the data into a file on the user's local disk.



* After the file transfer completes the client and server programs terminate Tcp connection used for the transfer. Ftp data transfer causes more traffic on Internet than any other application.

1) Trivial File Transfer protocol (TFTP):

* It is a Udp based file transfer program is frequently used to allow hosts to boot over the network. It is implemented by tftp client program and by tftp server program. TFTP has no user authentication; for unwanted file transfer to occur.

* TFTP is a simple protocol to transfer files. It is implemented on top of the internet UDP. TFTP can only read and write files from/to a remote server. It cannot list directories and currently has no provisions for user authentication.
* Each data packet contains one block of data and it must be acknowledged by an packet before sending the next packet.
* The sender has to keep just one packet on hand for retransmission, because lock step acknowledgement guarantees all older packets have been received.

E-mail protocols:

* E-mail is an asynchronous communication medium. It is used for sending a single message include text, voice, video or graphics to one or more recipient.
* It is fast, easy to distribute and inexpensive.

SMTP:

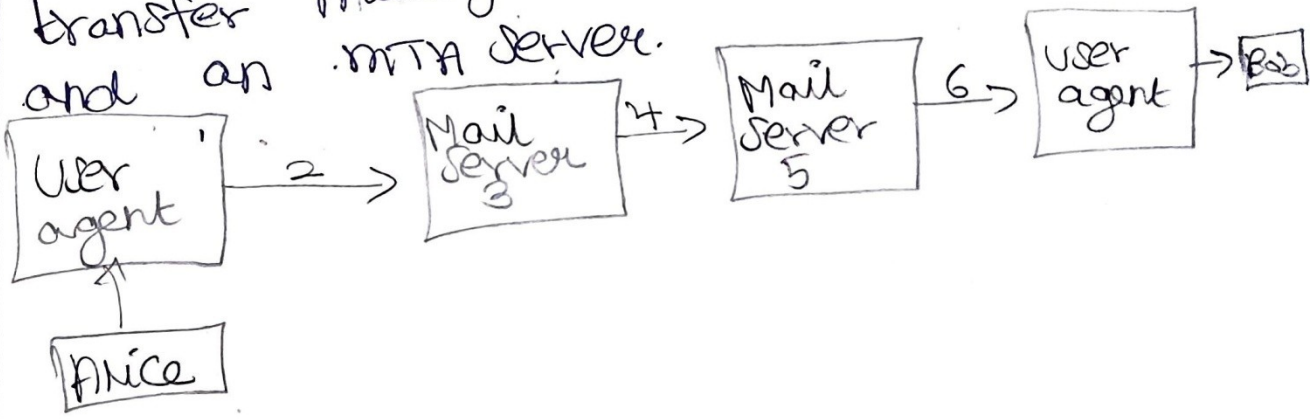
* Simple Mail Transfer Protocol is the Standard mechanisms for email in the internet. It is the TCP/IP mail delivery protocol.
* It is an application layer protocol of TCP/IP model.
* SMTP transfers message from sender's mail servers to the recipients mail servers.
* It interacts with local mail system and not the user.
* It uses a TCP socket on port 25 to transfer e-mail reliably from client to server.
* E-mail is temporarily stored on the local and eventually transferred directly to receiving server.
* Mail client application interacts with a local SMTP server to initiate the delivery of an e-mail message.
* There is an input queue and an output queue at interface between local mail system and client and server parts of SMTP.

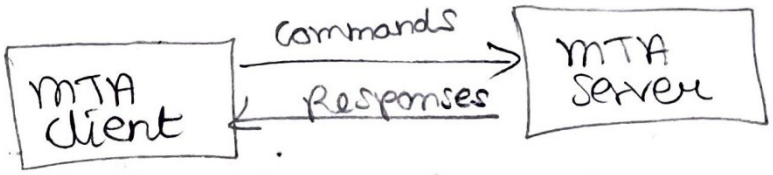
* SMTP uses different types of Component; They are MIME and pop.

Scenario: Alice sends message to Bob

i) Alice uses User Agent (UA) to compose message and to bob@Sinhgad.edu
ii) Alice's UA sends message to her mail server, message placed in message queue.
iii) Client side of SMTP opens Tcp connection with Bob's mail server.
iv) SMTP client sends Alice's message over the Tcp connection.
v) Bob's mail server places the message in Bob's mailbox.
vi) Bob invokes his user agent to read message.

* SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.





* Each command or reply is terminated by a two character end of line token.
* Commands are sent from the client to the server. SMTP defines 14 commands.
* SMTP commands consist of human readable ASCII strings.

SMTP Commands are as follows:

i) HELO:
Initiate a mail transaction, identifying the sender to the recipient.

ii) MAIL FROM:
Tells the remote SMTP that a new mail transaction is beginning.

iii) RCPT TO:
The sending SMTP sends a RCPT Command for each intended receiver.

iv) DATA:
If accepted, the sender transfers the actual message. End of message is indicated by sending a "." on a line by itself.

v) QUIT:
Terminate the connection

Sample SMTP Interaction:

Following are messages exchanged

between an SMTP client (C) and an SMTP server (S)

pop3:

* post office protocol 3 (pop3) is used to transfer e-mail message from a mail server to mail client software.
* pop3 begins when the user agent opens a TCP connection to the mail server.
* After TCP connection established, pop3 progresses 3 phases:

i) **Authorization phase:**
User agent sends a user name and a password to authenticate the user downloading the mail.

ii) **Transaction phase:**
User agent retrieves messages. User agent can also mark messages for deletion, remove deletion marks.

iii) **Update phase:**
It occurs after the client has issued the quit command, ending the pop3 session.

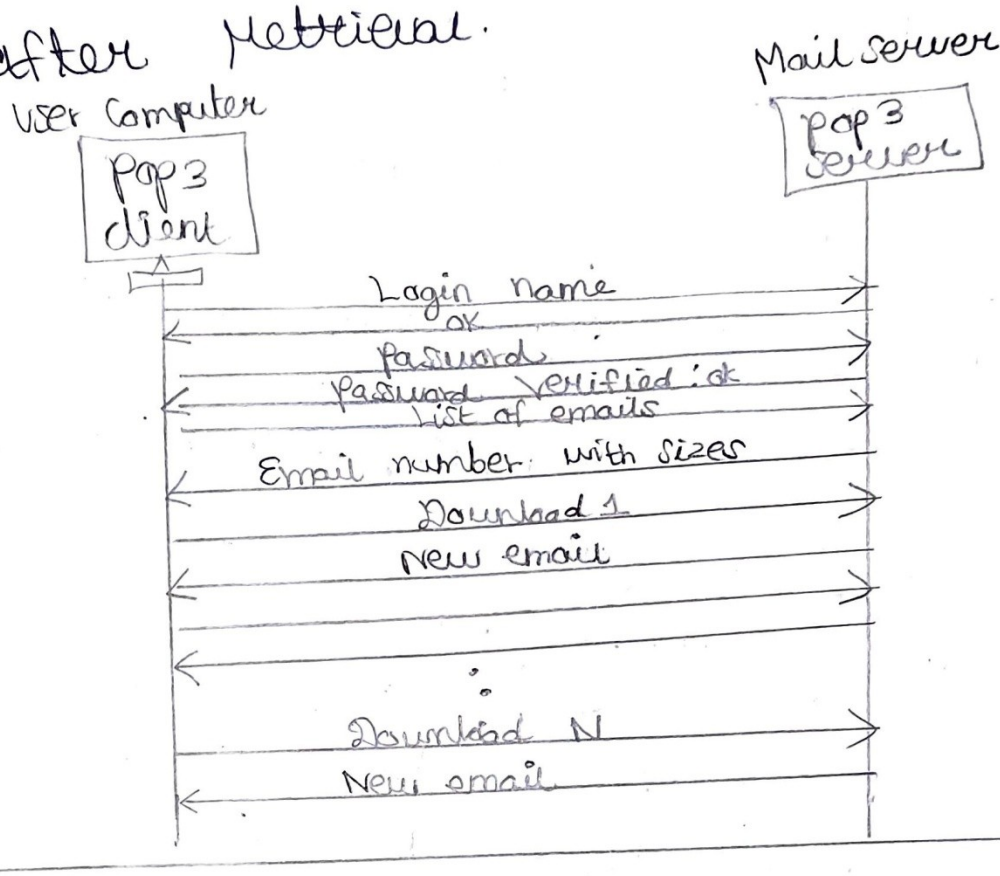
* pop3 has two modes:

i) **Delete mode:**
Mail is deleted from mailbox

after each retrieval.

ii) Keep mode:

The mail remains in the mailbox after retrieval.



IMAP:

* IMAP is the Internet Mail Access Protocol. It is more powerful and more complex. IMAP is similar to SMTP.
* IMAP doesn't copy e-mail to the user's personal machine. It was designed to help the user who uses multiple computers.
* IMAP client connects to a server by using TCP.

* IMAP supports the following modes for accessing e-mail messages:

i) Offline mode:

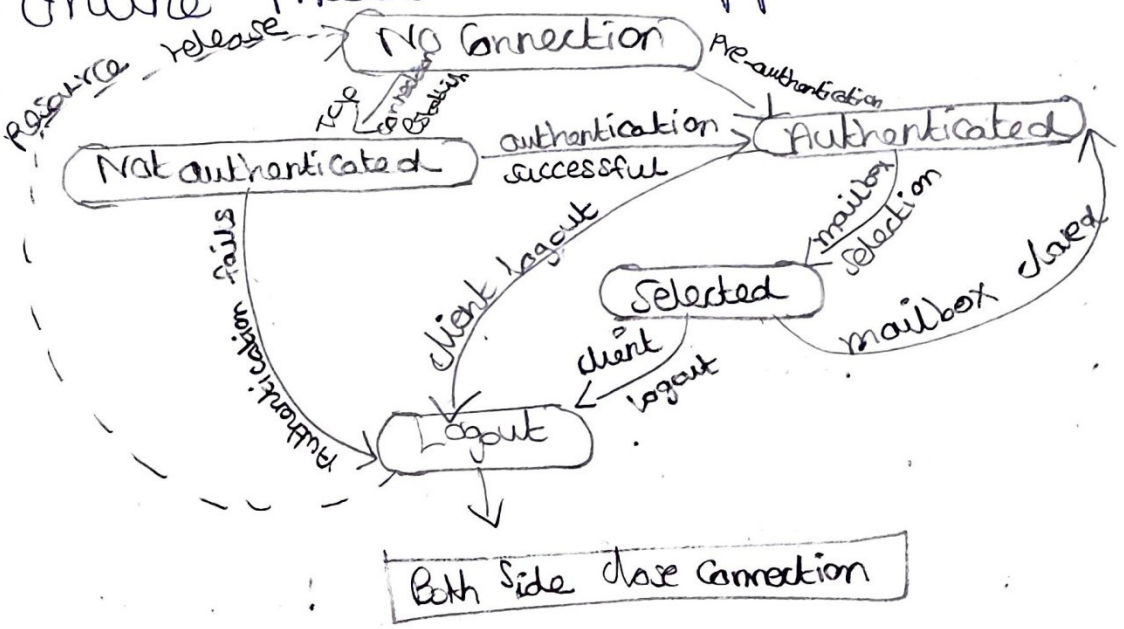
A client periodically connects to the server by downloading e-mail messages. After downloading, messages are deleted from the server. POP3 supports this mode.

ii) Online mode:

client process e-mail messages on the server. The e-mail messages are stored on the server itself but are processed by an application on client's end.

iii) Disconnected mode:

In this mode, both offline and online modes are supported.



IMAP State diagram:

i) Not authenticated:
Client provides authentication information to the server.

ii) Authenticated:
Server verify the information and client is now allowed to perform operations on a mailbox.

iii) Selected:
Client is allowed to access of manipulate individual messages within the mailbox.

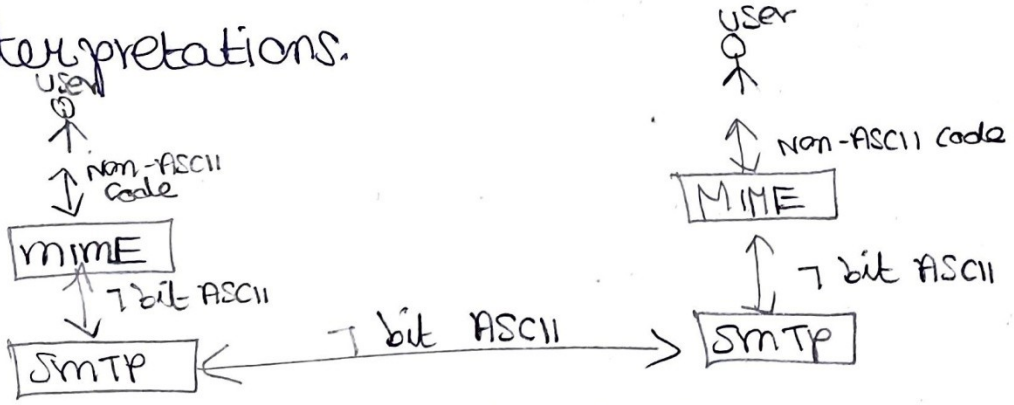
iv) Logout:
Client send logout command for closing IMAP session.

MIME:

Multipurpose Internet Mail Extensions

* It is a supplementary protocol that allows non-ASCII data to be sent through SMTP.
* MIME defined by IETF to allow transmission of non-ASCII data via e-mail.

* It allows arbitrary data to be encoded in ASCII for normal transmission.
* All media types are sent or received over the World Wide Web are encoded using different MIME types.
* Messages sent using MIME encoding include information that describes the type of data.
* RFC822 specifies the exact format for mail header as well as their semantic interpretations.



* MIME defines 5 headers.

i) MIME - Version
ii) Content - Type
iii) Content - Transfer - Encoding
iv) Content - Id
v) Content - Description

Mail Message Header:

From: Seetha@e-mail.com

To: rupali@annauniv.edu

MIME: Version: 1.0

Content-Type: image/gif

Content-Transfer-Encoding: base64

MIME Types and Subtypes:

* Each MIME Content-type must contain two identifiers:
  i) Content Type
  ii) Content subtype

Content-Transfer Encoding:

* This header defines the method to encode the messages into 0 and 1 for transport.

Content-Transfer-Encoding: <Type>

DNS:

Domain Name System

* DNS protocol is the application layer protocol.
* It is specified in RFC 1034 and RFC 1035.

i) Components of DNS:

DNS includes 5 components.

i) Domain:

gracecoe.org is the site for grace College of Engineering. Here, .org is the domain.

ii) Domain name:

It is defined by DNS as being the sequence of names and domain. Eg: gracecoe.org is the domain name.

iii) Name Server:

The software that maps names to addresses. It does by mapping domain name to ip addresses.

iv) Name Resolver:

It is a software that functions as a client interacting with a name server.

v) Name Cache:

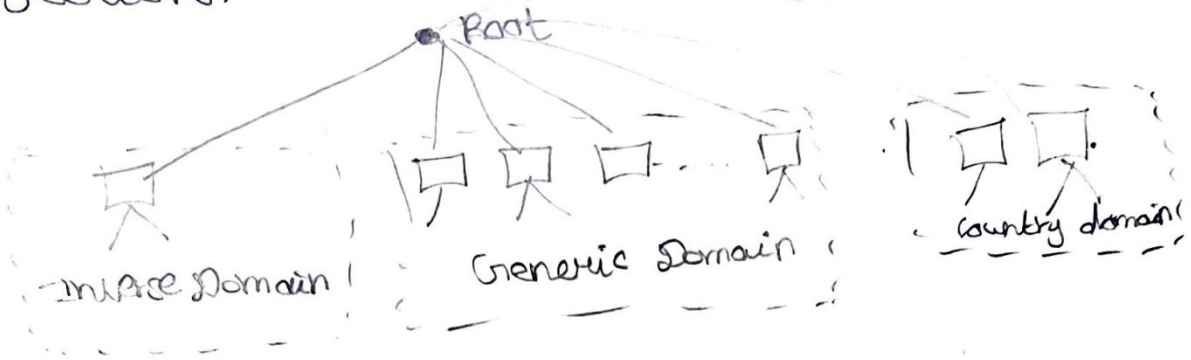
It is the storage used by the name resolver to store information frequently used.

vi) Zone:

It is a contiguous part of a domain.

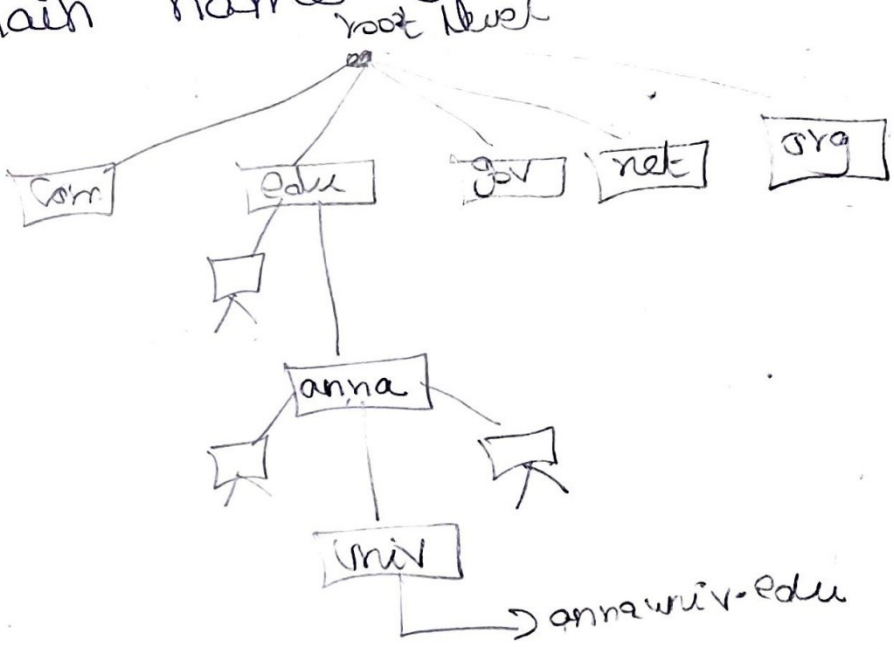
2) DNS in the Internet:

DNS is divided into 3 different sections in the Internet.



i) Generic Domain:

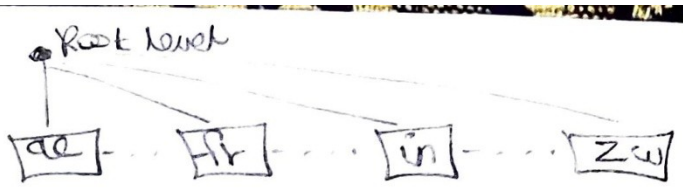
Each node in the tree defines a domain which is an index to the domain name space database.



ii) Country Domain:

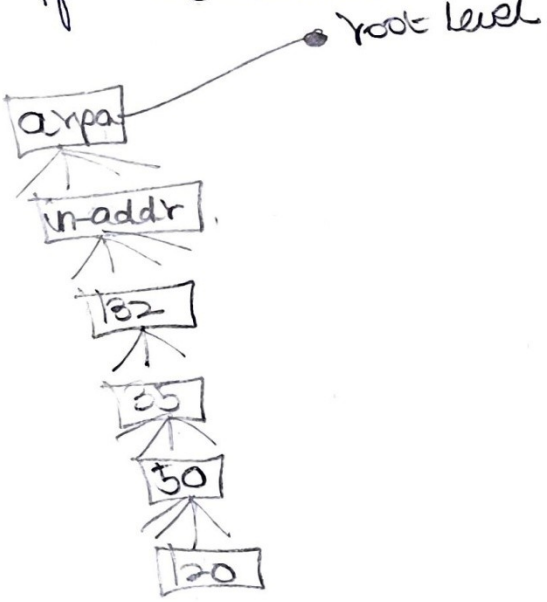
It uses two character country abbreviation at 1st level. 2nd level label can be more specific, national destinations.

Eg: India, the country domain is in.



iii) Inverse Domain:

It is used to map an address to a name. Server send a query to the inverse DNS server and ask for mapping of address to name for authorized client list. The above query is called an inverse or pointer query. The pointer query is handled by first level node called arpa. The second level is also one single node named in-addr. The rest of the domain defines IP addresses.



3) Name Spaces:

Name Spaces are of two types.

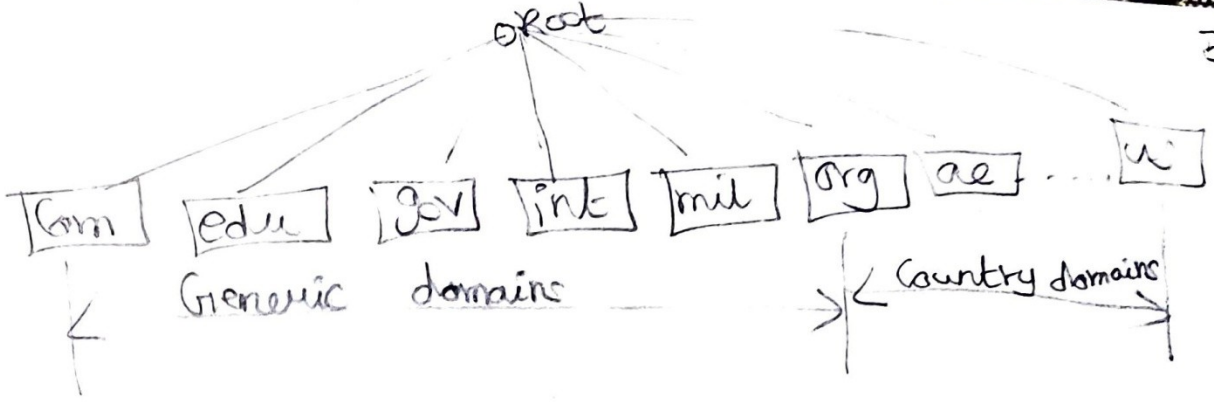
i) Flat name spaces:

The original set of machines on the Internet used flat namespaces. These namespaces consisted of sequence of characters with no further structure. A name is assigned to an address.

ii) Hierarchical Name:

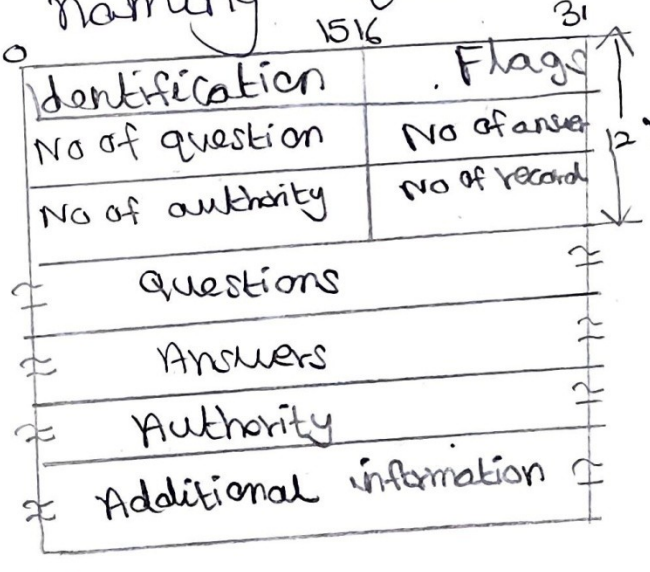
The partitioning of a namespace must be defined in such a way that it:

* Supports efficient name mapping
* guarantees autonomous control of name assignment
* The namespace is partitioned at top level.
* Authority for names in each partition are passed to each designated agent.
* The names are designed in an inverted-tree structure with the root at the top.
* The tree can have only 128 levels.



ii) Message Format:

Messages are sent between domain clients and domain servers with a specific format. All messages of this format are used for name resolution and naming queries.



i) Identification::

It is 16 bits fields and unique value used by the client to match responses to queries.

ii) Flags::

It is the collection of subfields that define the type of messages and type of answers requested & so on.

iii) Number of questions:

It contain the number of queries in the question section of the message.

iv) Number of answers:

It contain the number of answers record in the answer section of the response message.

v) Number of authority:

It contains the number of authority records in authoritative section of the response message.

vi) Number of additional records:

It contains the number of additional records in the additional section of response message.

SNMP:

Simple Network Management Protocol

* Network management system is a collection of tools for network monitoring and control.
* It consists of hardware and software implemented among existing network components

* A network management system is designed to view the entire network as a unified architecture with labels and addresses assigned to each point and specific attributes of each element and link known to the system.

* It can be defined as deployment, integration and co-ordination of hardware, software to monitor, test, analyze and evaluate.

1) Uses of Network Management:

Applications or uses of network management are,

i) Detecting failure of an interface card at a host or router.
ii) Host monitoring
iii) Monitoring traffic to aid in resource deployment
iv) Detecting changes in routing table
v) Monitoring for service level agreements
vi) Intrusion Detection

2) Areas of Network Management:

ISO has created a Network Management model. In this model, 5 areas of Network management are defined.

i) Fault Management:

It includes any tools or procedures for diagnosing, testing or repairing the Network when a failure occurs. Network administrator uses some fault management tools. They are,

a) Network management System
b) Protocol analyzer
c) Cable tester
d) Redundant System
e) Data archiving and backup devices

ii) Security Management:

It involves certain actions on the part of the administrator to minimize the risk from inside or outside the organization. It include theft or misuse of resources, unauthorized data access and damage to data or equipment.

iii) Accounting Management:

It involves the cost of the

System. The cost comparison should be between actual cost of the equipment and the anticipated performance of the equipment.

iv) Performance Management:

It is primarily concerned with collecting information periodically from the network and analyzing it to anticipate bottleneck to make predictions about future network growth.

v) Configuration Management:

It helps to track the devices on the network, hardware and software configuration also the requirements for IP based networks.

3) Infrastructure for Network Management:

Three important component of network management architecture are

i) Managing Entity:

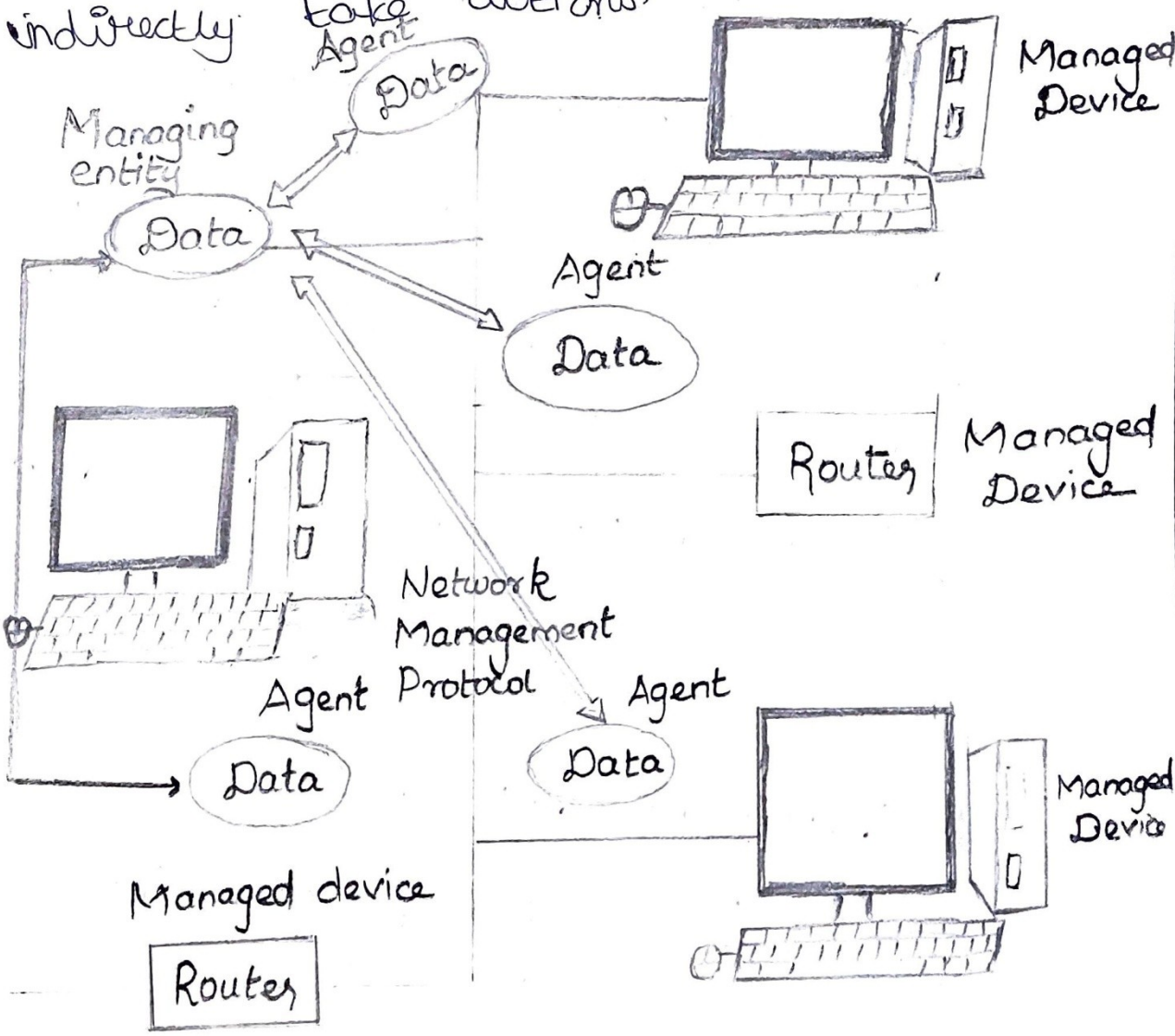
It is an application. It controls the collection, processing, analysis of network management information.

ii) Managed Devices:

It is a network equipment. It can be a host, router, bridge, hub, printer or modem. A managed device have information associated with them are collected into Management Information Base

iii) Network Management protocol:

It runs between managing entity and managed devices and indirectly take actions.



NETWORK MANAGEMENT ARCHITECTURE

UNIT-II

Transport layer

Introduction:-

* A transport layer protocol provides for logical communication between application processes running on different hosts.
* It is implemented in end systems but not in network routers.
* The transport service is to perform "peer to peer" communication with the remote transport entity.
* The transport layer is the fourth layer in the OSI layered architecture. It is responsible for reliable data delivery.
* The upper-layer protocols depends heavily on transport layer protocol. A high level of error recovery is provided in this layer.
* Data link is responsible for

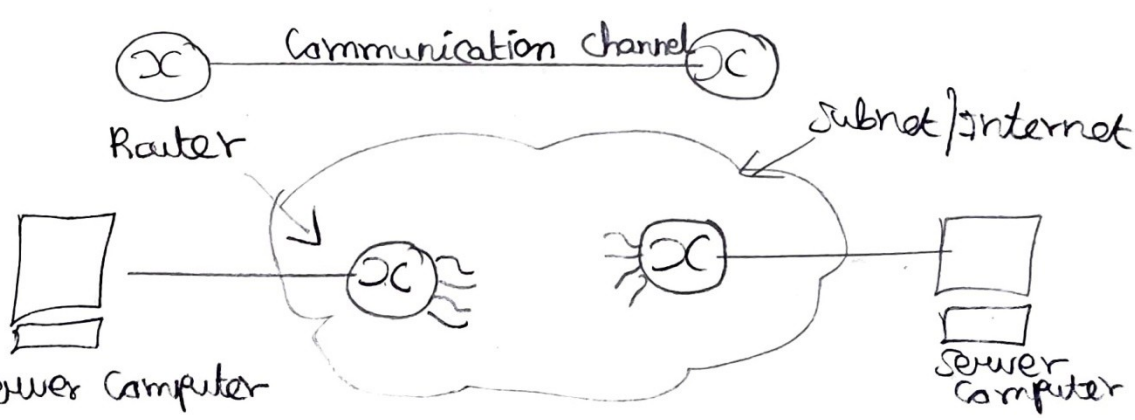
delivery of frames between two neighbouring nodes over a link is called node-to-node delivery.

* Network layer is responsible for host-to-host delivery. ie delivery of datagram between two hosts.

* Transport layer is responsible for process-to-process delivery ie the delivery of a packet, part of a message one process to another.

Transport Layer protocols:

The transport service is implemented by a transport protocol used between the two transport entities.



* At the data link layer, two routers communicate directly via a physical channel, whereas at transport layer physical channel is replaced by entire subnet.

1) Addressing:

* When a user of given transport entity to establish a connection with user of other transport entity.
* The source user needs to be specified by all information, user identification, transport entity identification, station address and network number.
* The user address is specified as station or port.
* The port variable represents a particular TS user at specified station in OSI is called Transport Service Access point (TSAP).
* The address should include designation of type of transport protocol. Eg: TCP, UDP

* In case of single network, station identifies an attached network device. In internet, station is a global internet address.
* port is included in a transport header to be used at destination by destination transport protocol.

2) Connection Establishment:

The connection establishment serves three main purposes.

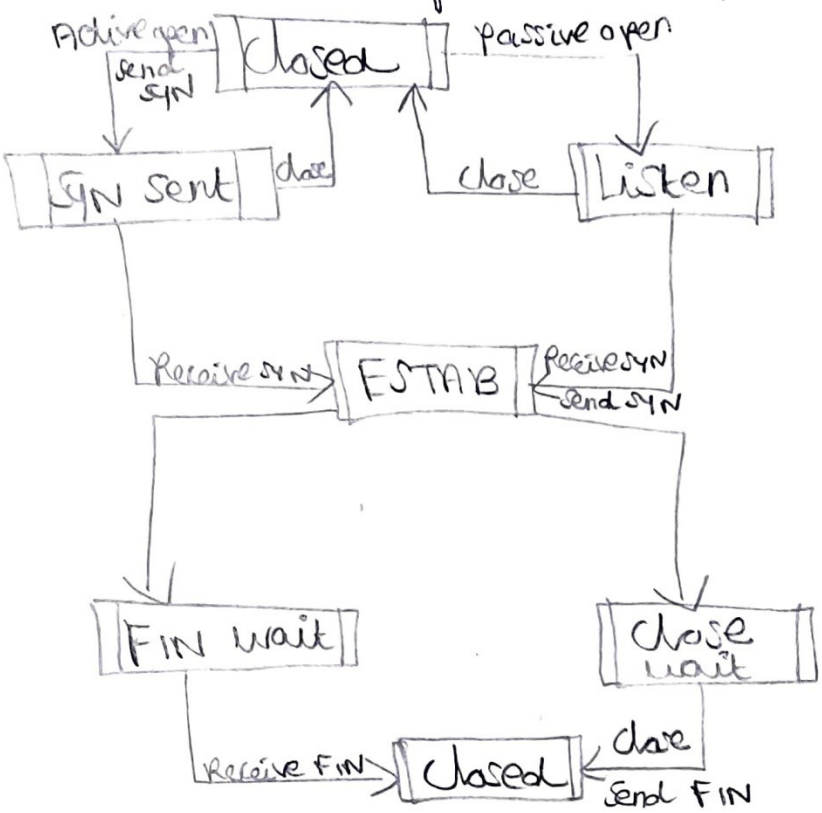
i) It allows each end to assure that the other exists.

ii) It allows negotiation of optional parameter like maximum segment size, maximum window size and quality of service.

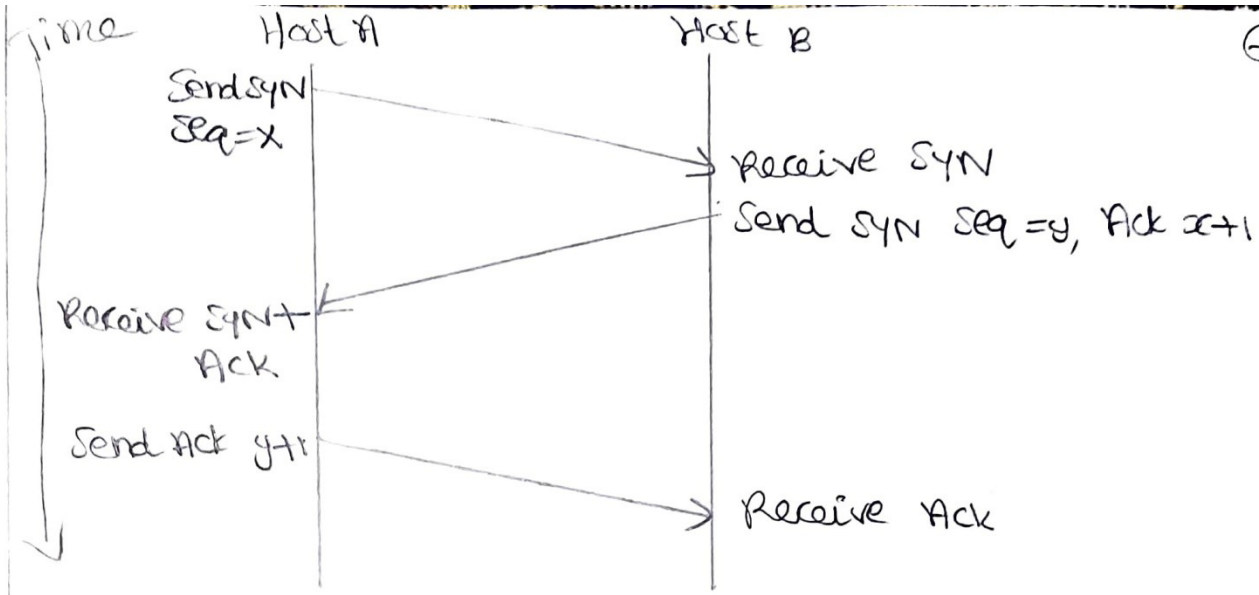
iii) It triggers allocation of transport entity resources like buffer space.

* It is accomplished by a simple set of user commands and control segments.
* Firstly, the transport service user is in the closed state.
* The Transport Service (TS) user

can signal passively wait for a request with a passive open command.

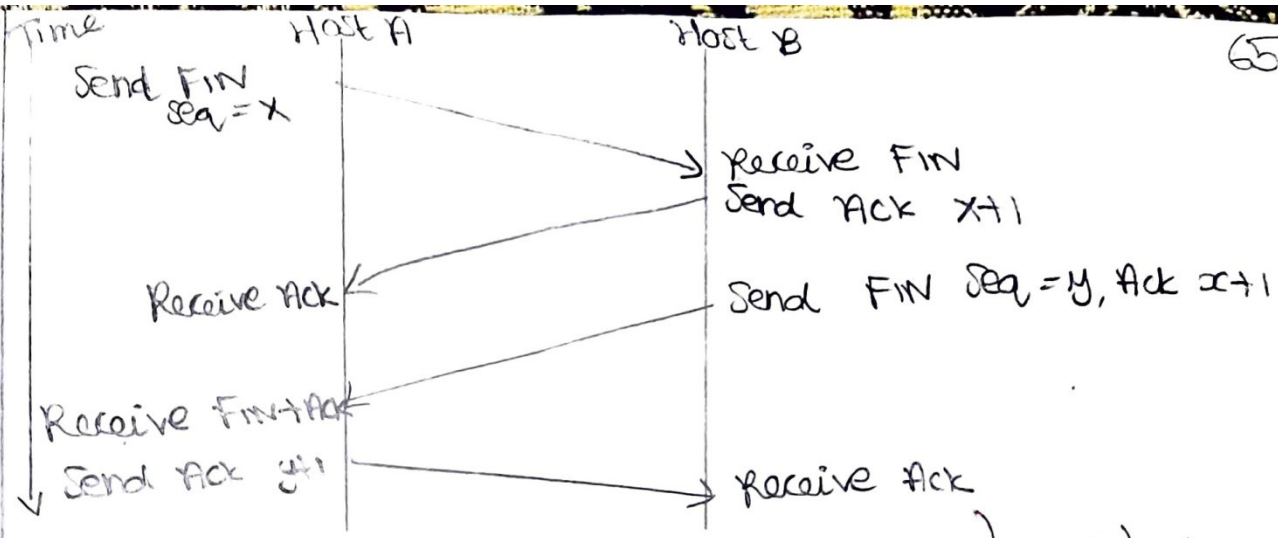


* The connection will establish if the destination transport entity is in the listen state.
* Signal the transport service user that a connection is open.
* Send an SYN as confirmation to the remote transport entity.
* put the connection object in an ESTAB state.
* There are 3 phases in any virtual connection. They are connection Establishment, data transfer & connection termination phase.

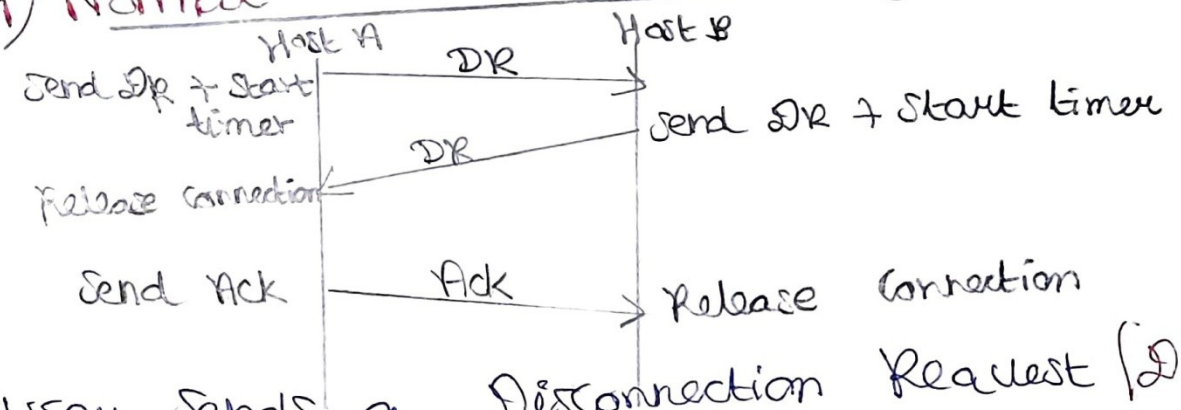


3) Connection Termination::

* For a connection to be released, four segments are required to completely close a connection.
* Instead of SYN control bit fields, the connection termination phase uses the FIN control bit fields to signal the close of a connection.
* To terminate the connection, the application running on host A signals TCP to close the connection. It generates first FIN segment from host A to host B.
* When host B receives the initial FIN segment, immediately acknowledges segment and notifies its destination.

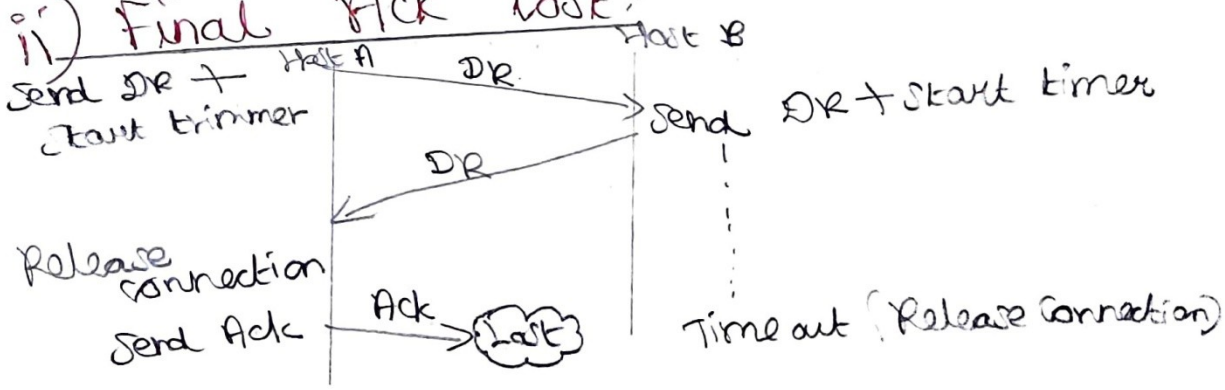


i) Normal case of three way handshake:



User sends a Disconnection Request (DR) to initiate the connection release. When it arrives, the receipent sends back and DR start a timer. When this DR arrives, the original sender sends back an Ack and releases the connection.

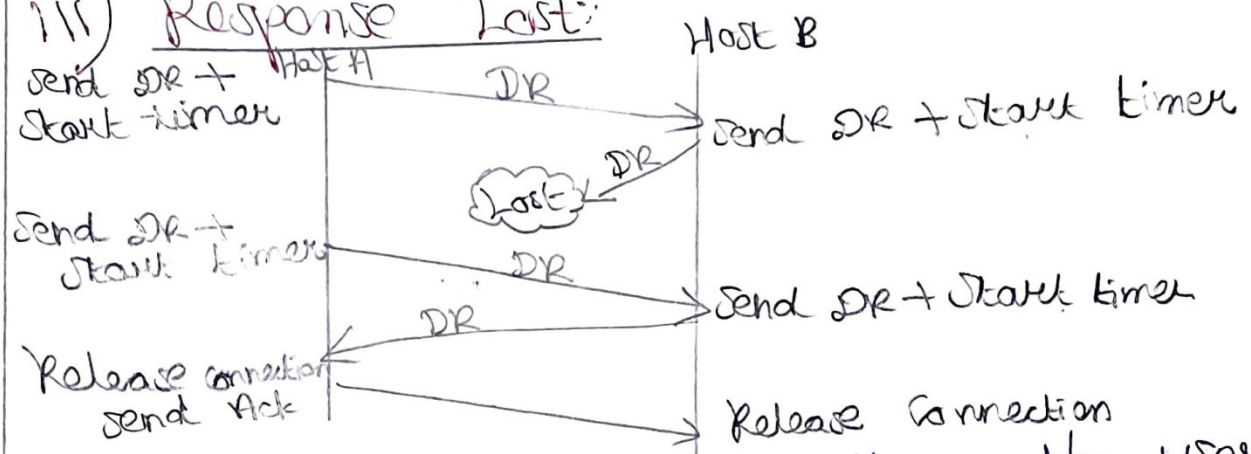
ii) Final Ack lost:



If final Ack is lost, the situation is

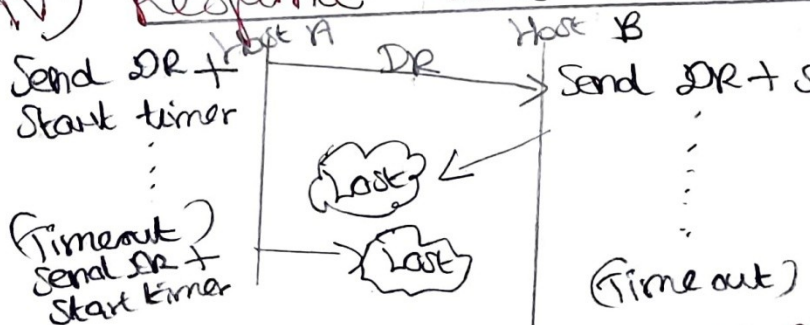
saved by the timer. when the timer expires, the connection is released anyway.

iii) Response Lost:



If the second DR lost then the user initiating this disconnection will not receive the expected response, will time out. The second time are lost are delivered correctly on time.

iv) Response lost and Subsequent DR lost:



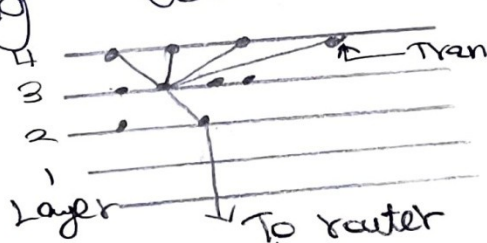
4) Flow control and Buffering:

* Flow control is implemented using modified form of Sliding window protocol. The window size is variable and is controlled by the receiver. The receiver sends a credit allocation to sender.

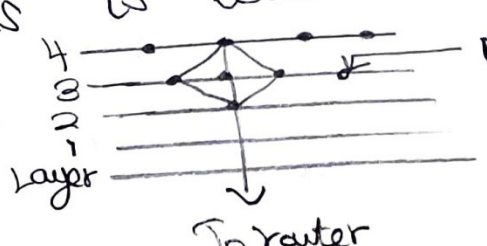
* The credit allocation indicates how many Transaction protocol Data Unit (TPDU) the receiver is ready to receive if the network service is unreliable, the sender must buffer all TPDUs sent.

5) Multiplexing:

* Many virtual circuits open for long periods of time is to make multiplexing of different transport connections onto the same network connection attractive. This form of multiplexing called upward multiplexing.



* The transport layer opens multiple network connections and distributes the traffic among them on a round-robin basis is called downward multiplexing.

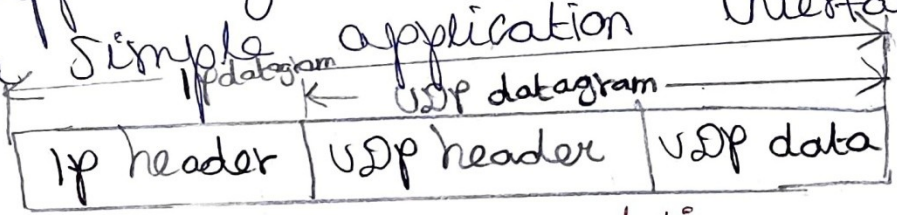


6) Crash Recovery:

* If the host computer (server) and routers are subject to crashes, the recovery from these crashes make some problem.
* When the server crash while receiving data from client, the outstanding TPDU is lost.
* The server might send a broadcast TPDU to all other host, for the status of all open connection.
* client can be in one of two states: TPDU outstanding (or) no TPDU outstanding Based on state information client must decide whether or not to retransmit the most recent TPDU.
* There are many situation for crash recovery. If the server send acknowledge and crash the server before writing the data.
* The writing data and sending acknowledgement both are different process.

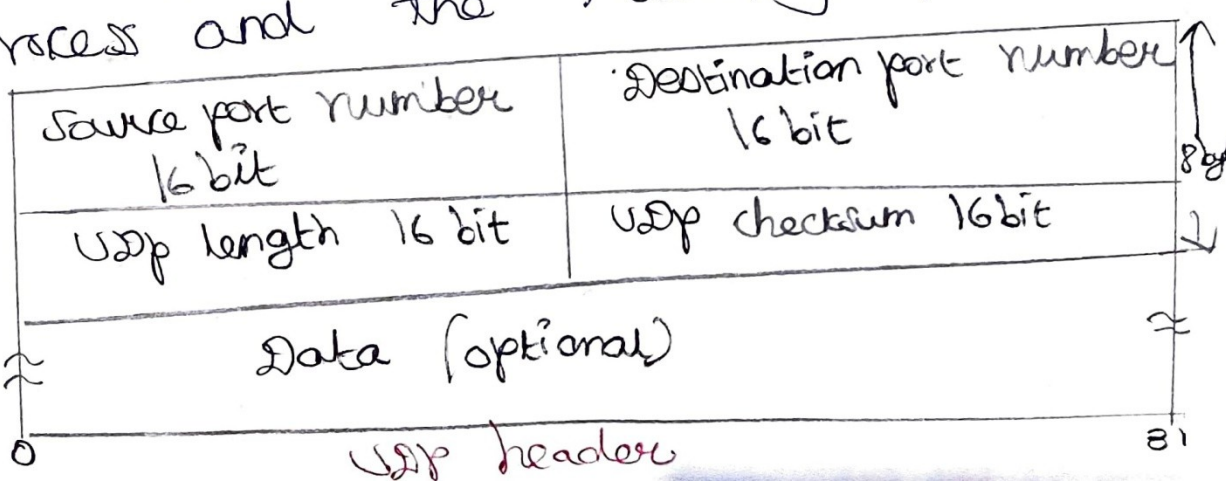
UDP:

* User Datagram protocol is a simple, datagram-oriented, transport layer protocol. It is used in place of Tcp. UDP is connectionless protocol. It provides no reliability or flow control mechanism. It also has no error recovery procedures.
* Several application layer protocols such as Trivial File Transfer Protocol (TFTP) and the Rpc use UDP. UDP makes use of the port concept to direct the datagram to the proper upper-layer applications. UDP serves as a simple application interface to IP.



UDP Encapsulation

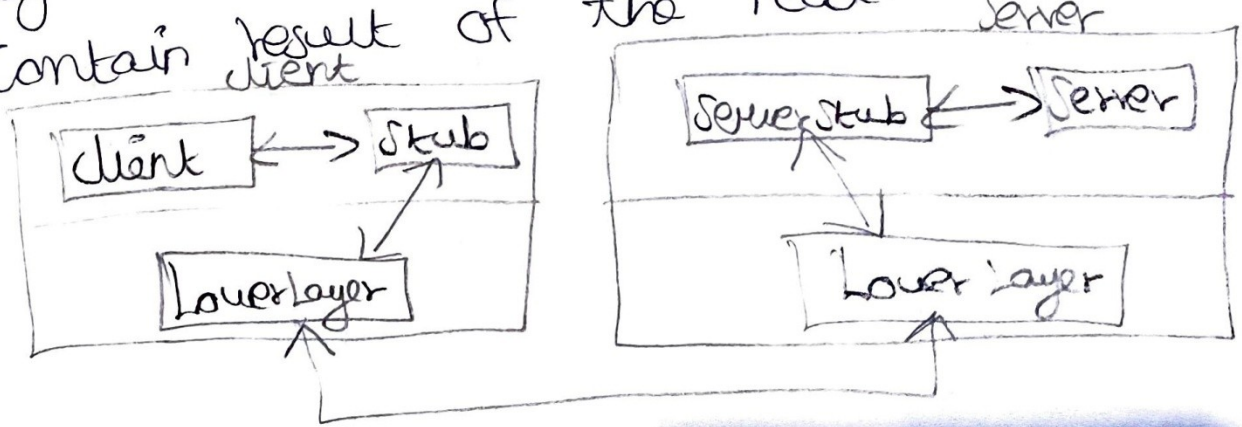
The port number identify the sending process and the receiving process.



* The UDP datagram contains a source port number and destination port number.
* Source port number identifies the port of sending application process.
* The destination port number identifies the receiving process on the destination host machine.
* The UDP length field is the length of the UDP header and UDP data in bytes. The minimum value for this field is 8 bytes.
* UDP checksum covers the UDP header and UDP data. Both UDP and TCP include a 12 byte pseudo-header with UDP datagram for the checksum computation. The pseudo-header includes certain fields from the IP header.
* UDP checksum is end-to-end checksum. It is calculated by the sender and then verified by receiver. It is designed to catch any modification of UDP header or data anywhere between sender and receiver.

1) Remote procedure calls (RPC):

* Rpc is based on a client-server model is an asymmetric type of communication. The ISO-OSI model and TCP/IP support the process of rpc. client server model widely used in local area networks in which dump terminals make access the server to obtain application software, files etc.
* Rpc is implemented in the client-server operation through a technique called STUB. Stub is a procedure such as read or write can be defined for each server's clients.
* The read procedures becomes library procedure and client can obtain the services through a simple read statement. It is file to be read, number of byte to be read and a buffer to contain result of the read.



* If the server fails problem will 72 occur in Rpc.

Eg: If client is sending request continuously to server and the request is not sent back to client before the server fails.

* If the client repeats the operation and resends the traffic then the reply is successfully executed and sent back. This type of operation is called idempotent.

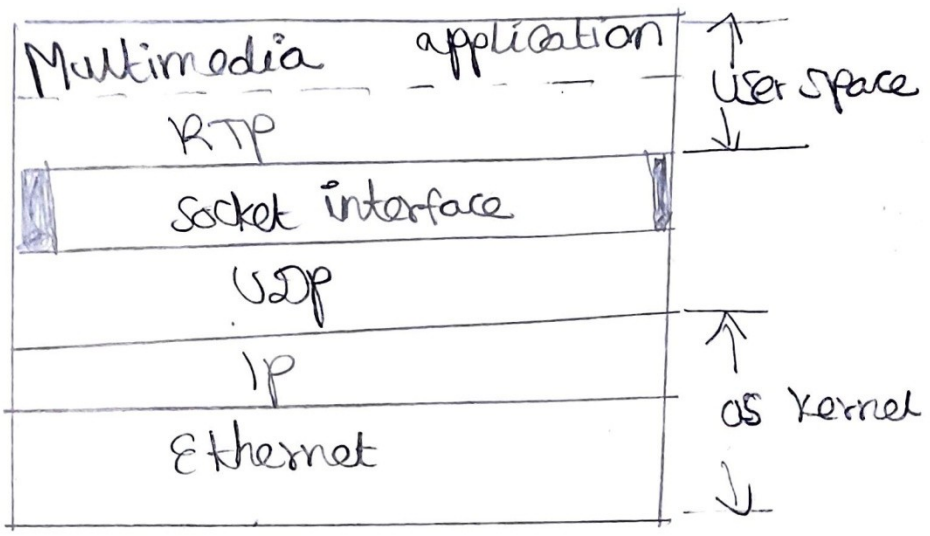
2) Real Time Transport protocol: (RTP)

* It run over UDP. It is used in multimedia applications, Video Conferencing, music-on-demand, video-on-demand. Audio, video and text are the content of the multimedia.

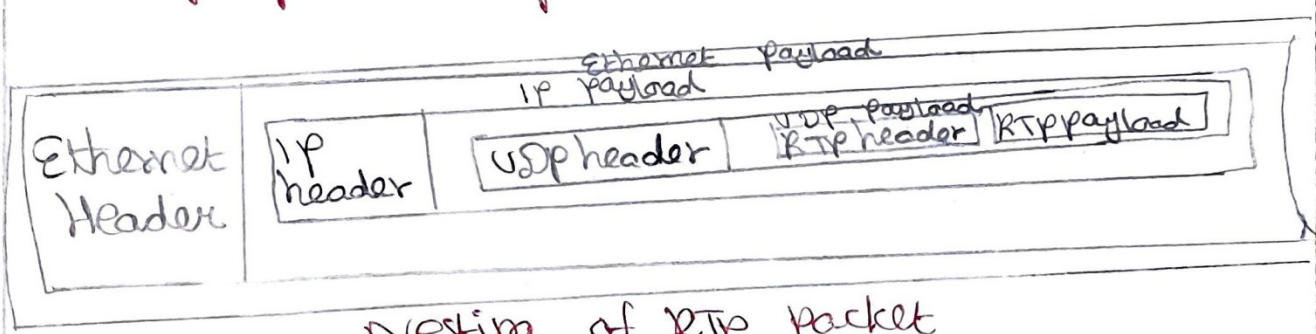
* Multimedia application also contains other types of data streams. All data is stored into RTP library in user space along with application.

* The library then multiplexes the streams and encode them in RTP packet then stuffs into a socket.

* Socket means communication end points. At the other sides of socket, UDP packets are generated and it is embedded in IP packets.

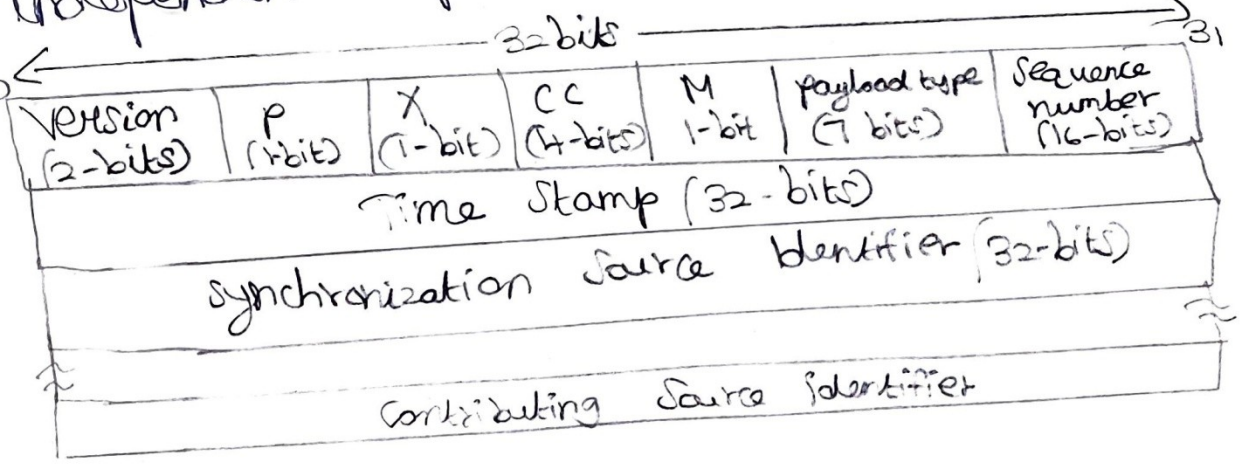


RTP in a protocol Stack



Nesting of RTP packet

* RTP is a generic and application independent protocol.



i) Version:
Size of Version is 2 bits. It indicates

version number. The current version is 2.

ii) p bit:
Size is 1 bit. It indicates the packet has been padded to multiple of 4 bytes.

iii) X bit:
Size is again 1-bit and it indicates the extension header is present.

iv) cc field:
Size of cc field is 4-bits. It is used for indicating number of source present. The range is from 0 to 15.

v) m bit:
Marker bit is of 1-bit size. It is used to indicate start of the frame. It may be video frame, start of a word in an audio channel.

vi) payload type:
Size of payload type field is 7 bits. It is used for indicating encoding algorithm has been used.

vii) Sequence number:
It is incremented by one each time an RTP is sent. The initial value is selected at random.

viii) Timestamp:

It specifies the sampling instant of first byte in RTP data packet. The initial value is selected at random.

ix) Synchronizing source identifier:

It tells which stream the packet belongs to. It is the method used to multiplex and demultiplex multiple data streams onto a single stream of UDP packets.

x) Contributing source identifier:

The list 0 to 15 thirty two bit item specifies the contributing sources for payload contained in the packet. It is used when mixers are present in the studio.

Tcp:

Transmission Control Protocol (TCP) is the connection oriented protocol whereas UDP is connectionless protocol. Both are internet protocol used in transport layer.

* Tcp provides a connection-oriented, reliable, byte stream service. The term connection oriented means the two applications using Tcp must establish a Tcp connection with each other before they can exchange data.

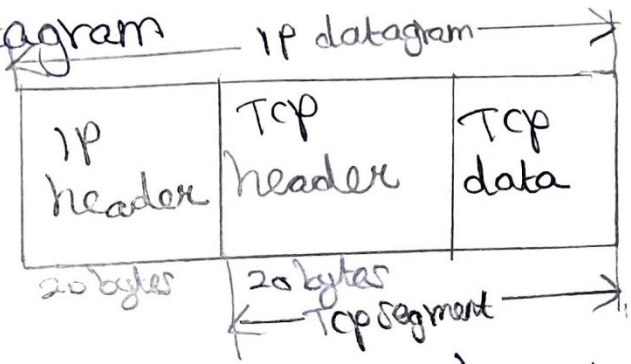
1) Tcp services:

* Tcp and Udp use the same Network layer (IP).
* Tcp does not support multicasting and broadcasting. The unit of information passed by Tcp to IP is called a Segment.
* When Tcp receives data from other end of the connection, it sends acknowledgement. Tcp maintains a checksum on its header and data.
* Tcp provides flow control. Each end of Tcp connection has a finite amount of buffer space.
* A Tcp connection is a byte stream, not a message stream. A stream of 8-bit bytes is exchanged across Tcp

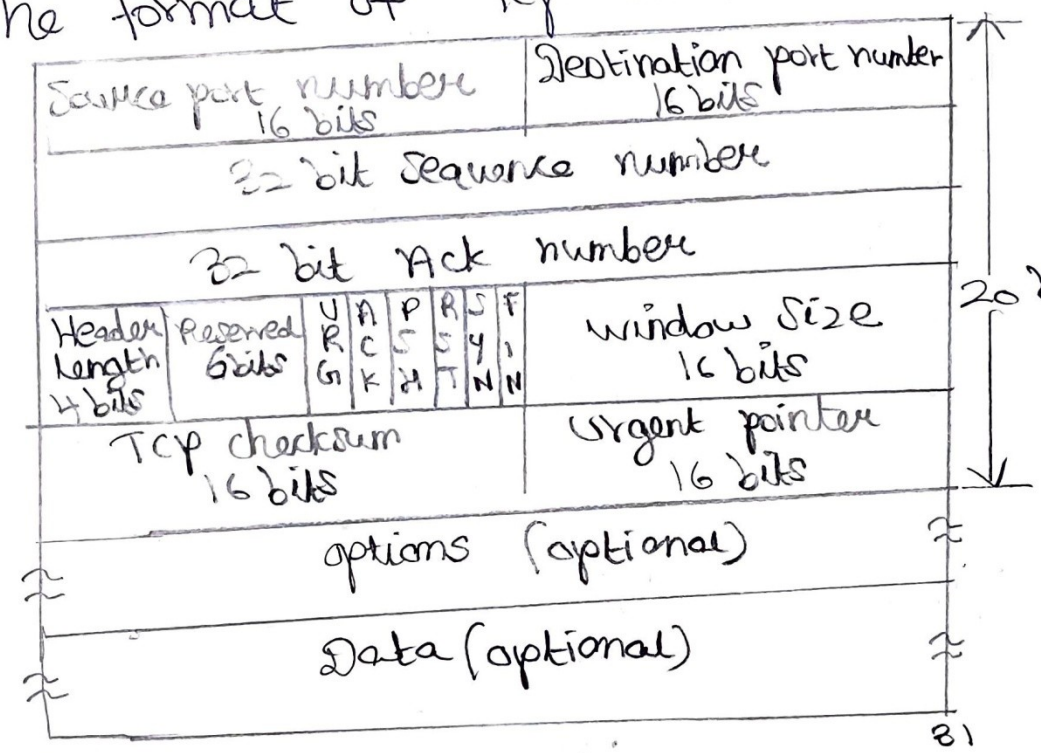
connection between two application.
It is called a byte stream service.

2) Tcp segment Format:

The Tcp data is encapsulated in an Ip datagram



The format of Tcp header.



Description of field in Tcp header are as follows.

i) Source port:

It specifies the application sending the segment. It is different from Ip

address which specifies an internet 78 address.

ii) Destination port:
It identifies the receiving application port numbers below 256 called well-known ports are assigned to commonly used applications.

iii) Sequence number:
Each byte in the stream that Tcp sends is numbered. The sequence number wraps back to 0 after $2^{32}-1$.

iv) Acknowledgement number:
It identifies the sequence number of next data by sender expects to receive if Ack bit is set. If Ack bit is not set, field has no effect.

v) Header length:
It specifies the length of the Tcp header in 32-bit words. Header length is used.

vi) Reserved:
It is reserved for future use and must set 0.

vii) Tcp header contains 6 flag bits.

a) URG:
The urgent pointer is valid if it set to 1.

b) Ack:
Ack bit is set to 1 to indicate the acknowledgement number is valid.

c) PSH: push
The receiver should pass this data to the application as soon as possible.

d) RST: Reset
It is used to reset the connection. It is also used to reject an invalid Segment.

e) SYN:
Synchronize Seaquence number to initiate a connection. The connection request has SYN = 1 and Ack = 0 to indicate piggyback acknowledgement field is not in use.

f) FIN:
It is used to release a Connection. It specifies the Sender finished sending data.

viii) Window Size:
It specifies the number of bytes the Sender is willing to accept. It can be used to control flow of

data and Congestion.

ix) Checksum:
used for transport layer error detection.

x) Urgent pointer:
If the URG flag bit is set, the segment contains urgent data meaning the receiver Tcp entity must deliver it to higher layer immediately.

xi) Options:
Size of the field is variable option field may be used to provide other functions that are not covered by header.

xii) Data:
Data field size is variable. It contains user data.

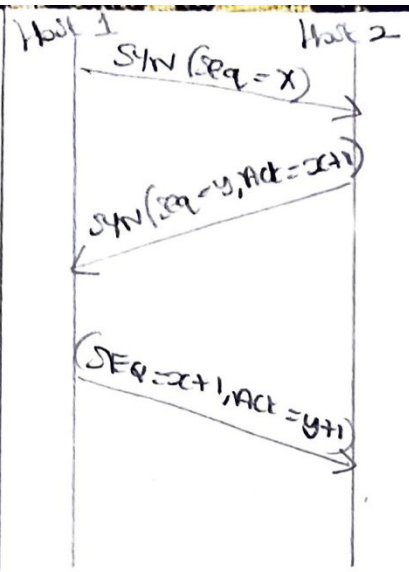
3) Tcp protocol:
Sending and receiving Tcp entities exchange data in the form of segments. It consists of fixed 20-byte header followed by 0 (or) more data bytes.
i) Each segment including Tcp header must fit in 65515 bytes Ip payload.

ii) Each network has a Maximum Transfer Unit (MTU) and each segment must fit in MTU.

* The basic protocol used by Tcp entities is Sliding window protocol.

iv) Tcp Connection Establishment:

* Connection establishment in a Tcp session is initialized through a three-way handshake. To establish the connection, one side (server) passively waits for incoming connection by executing LISTEN and ACCEPT primitives, either specifying a specific source.
* other side (client) executes a CONNECT primitive specifying the IP address and port to which wants to connect, maximum Tcp segment size and optionally some user data.
* A connection is established using a three-way handshake.
* The transmitter sends connection request to start a connection with transmitter message id x.



b) Tcp connection Release:

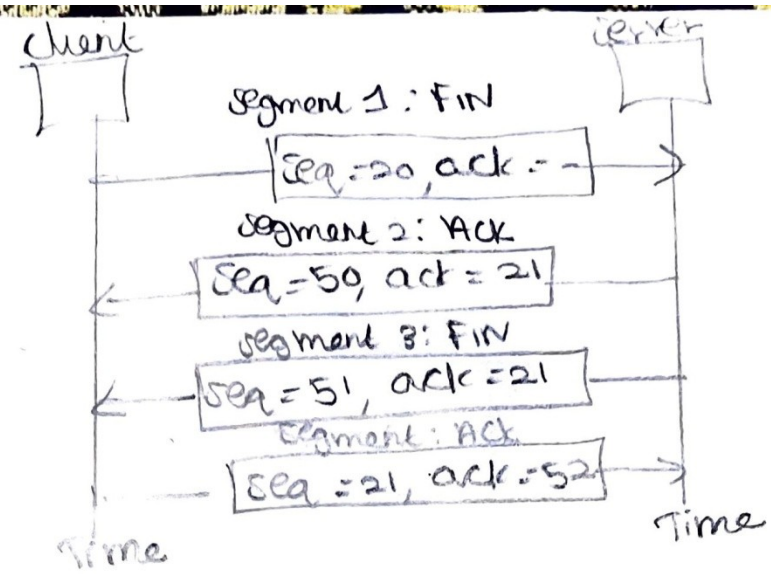
* Any of the two parties involved in exchanging data can close the connection. When connection in one direction is terminated, the other party can continue sending data in other direction.
* Four steps are required to close the connection in both direction.

i) The client Tcp sends the first segment, a FIN segment.

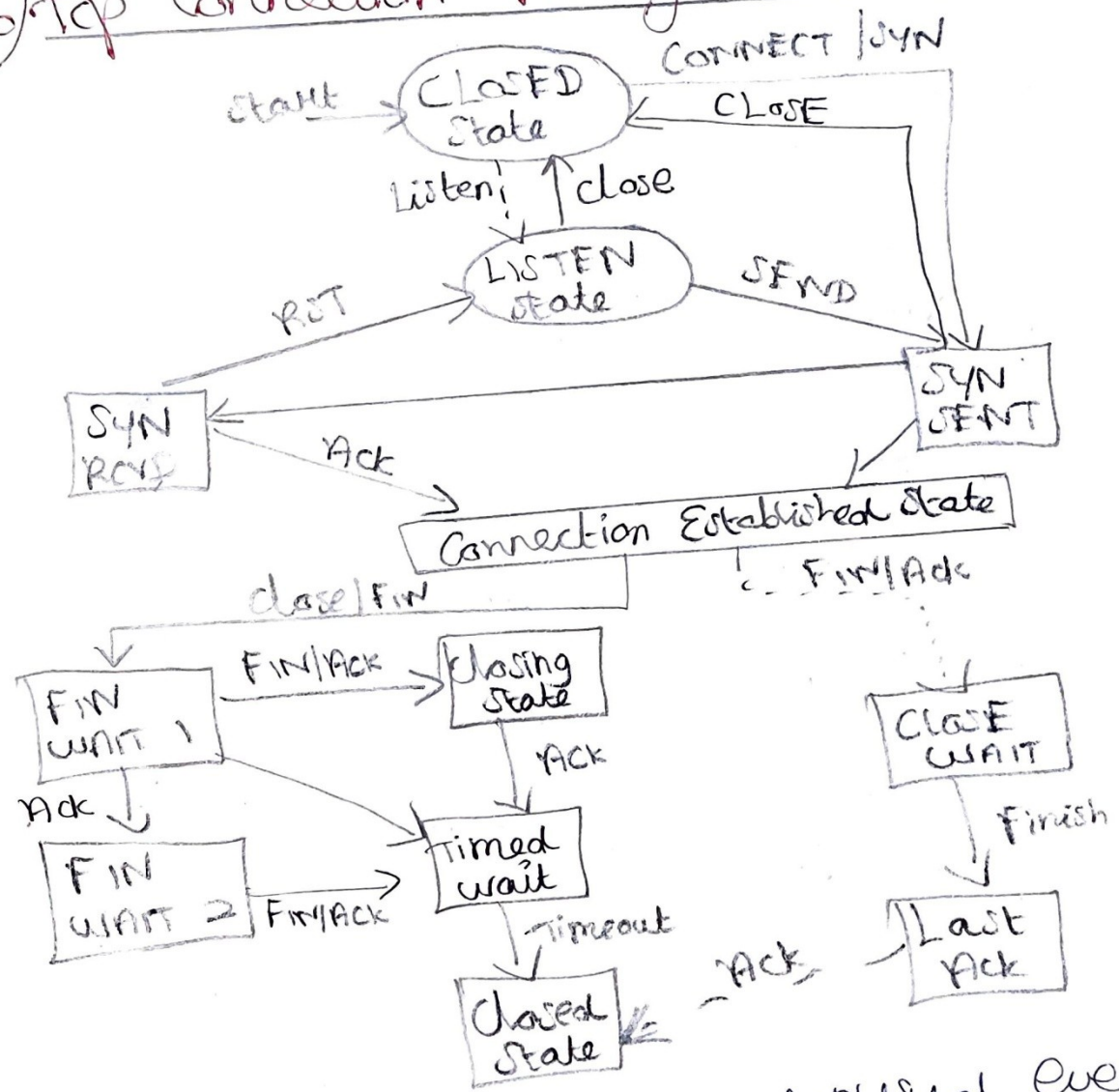
ii) The server Tcp sends 2nd segment, Ack segment to confirm the receipt of FIN segment.

iii) The server Tcp can continue sending data in server client direction. When it doesn't have any more data to send, it sends 3rd segment.

iv) The client Tcp sends 4th segment, Ack segment to confirm the receipt of FIN segment.



6) Tcp Connection Management Modeling:



* The lightface lines are unusual event sequences.
* Each line is marked by an event/action

pair.

* The event can either be a user-initiated system call, a segment arrival, timeout of maximum packet lifetime.

7) Tcp Timer Management:

Tcp manages four different timers for each connection.

i) Retransmission Timer:

It is used when excepting an acknowledgement from other end.

ii) persist Timer:

It keeps window size information flowing even if other end closes its receiver window.

iii) keep Alive Timer:

It detects when the other end on an otherwise idle connection crashes.

iv) 2 Maximum Segment Lifetime (2 MSL):

It measures the time a connection has been in TIME_WAIT state.

8) Tcp Congestion Control:

* When the load offered to any network is more than it can handle, congestion builds up.

* When a connection is established, the sender initializes the congestion window to the size of maximum segment
* The congestion window keeps growing exponentially until either a timeout occurs or the receiver's window is reached.

Congestion Control:

* TCP uses a form of end to end flow control. Both the sender and receiver agree on a common window size for packet flow. The window size represents the number of bytes that the source can send at a time.
* The window size varies according to the condition of traffic in the network to avoid congestion.
* A file of size 'f' with a total transfer time of 'Δ' on a TCP connection results in a TCP transfer throughput (r) ie

$$r = \frac{f}{\Delta}$$

Bandwidth utilization $(\rho_u) = \frac{r}{B}$

Where B = Link bandwidth

* Tcp has three Congestion Control 26 methods. Additive increase, Slow start and Retransmit

1) Additive Increase, Multiplicative Decrease Control (AIMD):

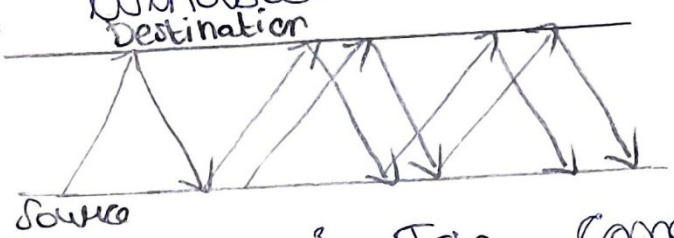
* Tcp maintains a new state variable for each connection called Congestion window, is used by Source to limit how much data is allowed to have in transit at a given time. It represent the amount of data in bytes.
* AIMD performs a Slow increase in Congestion window size when the congestion in network decreases and a fast drop in the window size when Congestion increases.
* Let Wm be the maximum window size in bytes representing the maximum amount of unacknowledged data that a sender is allowed to send.
* Let Wa be the advertised window sent by the receiver, based on its buffer size.

* TCP's effective window is revised as:

Max window = MIN (Congestion window, Advertised window)

Effective window = Max window - (Last byte sent - Last byte Acked)

* Max window replaces Advertised window in the calculation of Effective window.



* The challenge in TCP congestion control is for the source node to find a right value for the congestion window. TCP window size varies based on traffic conditions in the network.

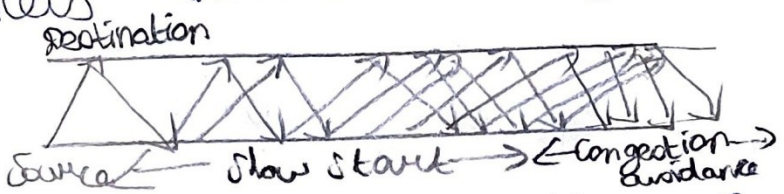
* TCP technique retries the timeout values be set properly. Two important factors in setting timeouts are,

i) Average round trip time (RTTs) and RTT standard deviation based to set timeouts

ii) RTTs are sampled once every RTT is completed.

2) Slow Start Method:

* It increases the congestion window size nonlinearly as compared to the linear increase in additive increase.
* The congestion window is again interpreted in packets instead of bytes.



* Source initially set the congestion window to one packet. When its corresponding acknowledgement arrives, the source sets the congestion window to two packets.
* Now the source sends two packets. On receiving the two corresponding acknowledgements, Tcp sets the congestion window size to 4. Thus the number of packets in transit doubles for each round-trip time.

The slow start method is normally used

i) Just after a Tcp connection is setup

ii) When a source is blocked, waiting for a timeout.

Congestion Avoidance:

A congestion avoidance scheme allows a network to operate in the region of low delay and high throughput. It is a prevention mechanism while Congestion Control is a recovery mechanism.

1) DEC bit scheme:

* DEC bit means Destination Experiencing Congestion bit.
* DEC bit method is developed on Digital Network Architecture (DNA). It split the responsibility between routers and end hosts. It is router based Congestion avoidance method.
* It uses a congestion-indication bit in packet header to provide feedback about congestion. Upon packet arrival, the average queue length is calculated for last period plus current busy period. When the average queue length exceeds one, the router sets the congestion-indicator bit in arriving packets header.

* If atleast half of packets in Source's last window have the bit set, decrease the Congestion window exponentially.
* Queue length is counted over the last busy period + idle + current busy period
* Source machine adjust the packet flow rate. Source machine maintains a Congestion window. It observes how many packets have the Congestion bit set to 1 in the last window width of packets
* If less than 50% of Acks have the DEC bit set then increase the window by 1 packet, otherwise set the window to 0.875 times the original value.

2) RED:

RED Stands for Random Early Detection.

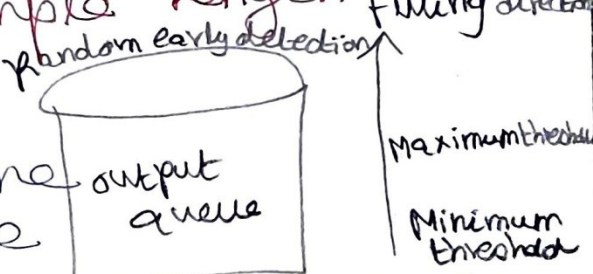
* The main idea is to provide Congestion Control at router for TCP flows. It is based on DEC bit.

* RED implicitly notifies sender by dropping packets. packet dropping probability is increased as the average queue length increases. The moving average of queue length is used to detect long term congestion, allow short term bursts to arrive.

* RED calculates the average queue length using a weighted running average.

Average length = (1 - weight) * Average length + weight * Sample length

where Sample length is queue length each time a packet arrives. The weight parameter is in between of 1 ie 0 < weight < 1



* RED uses a packet drop profile to handle packet discarding. It defines a set of dropping probabilities according to level of queue occupancy.

* A minimum and maximum threshold are defined as,

i) If the queue occupancy lies beneath the minimum threshold, then packet drop does not occur.

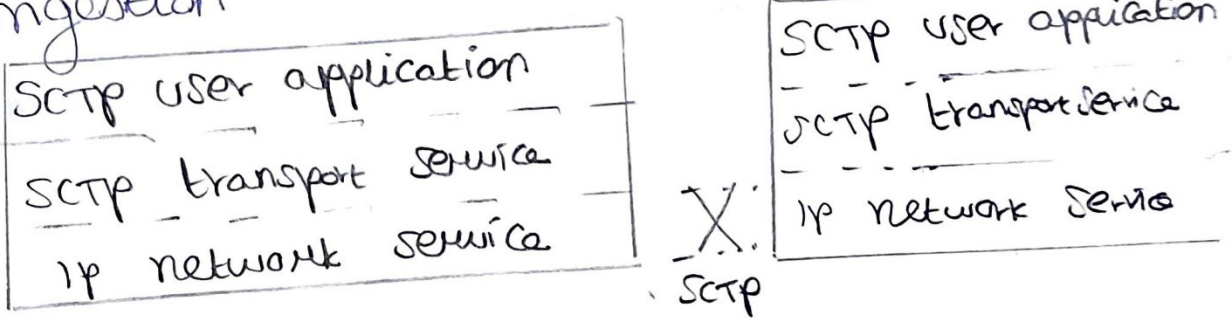
ii) If the queue occupancy is between minimum and maximum thresholds then packets are dropped according to the configured drop probability.

iii) When the queue occupancy crosses maximum threshold, then all new packets attempting to enter the queue are discarded.

Stream Control Transmission protocol (SCTP):

* It is a reliable transport protocol operating on top of potentially unreliable connectionless packet service such as IP.
* It offers acknowledged error-free non-duplicated transfer of datagrams.
* Detection of data corruption, loss of data and duplication of data is achieved by using checksums and sequence numbers.

* A selective retransmission mechanism is applied to correct loss or corruption of data.
* It is a transport layer protocol serving in similar role as the popular protocols Tcp and Udp. It provides some of the same service features of both ensuring reliable, in-sequence transport of messages with Congestion control.



1) SCTP Services:
Similar to Tcp, SCTP provides a reliable and in-order data transfer service to HTTP. SCTP provides other services unavailable in Tcp. The services are,
i) Multistreaming
ii) process to process communication
iii) 4-way handshake during association establishment

iv) No maximum segment lifetime
v) Multihoming for improved fault tolerance
vi) preserving application message boundaries
vii) Reliable services
viii) Connection oriented service
ix) Sequenced delivery of user datagram within a Stream.

2) Features:

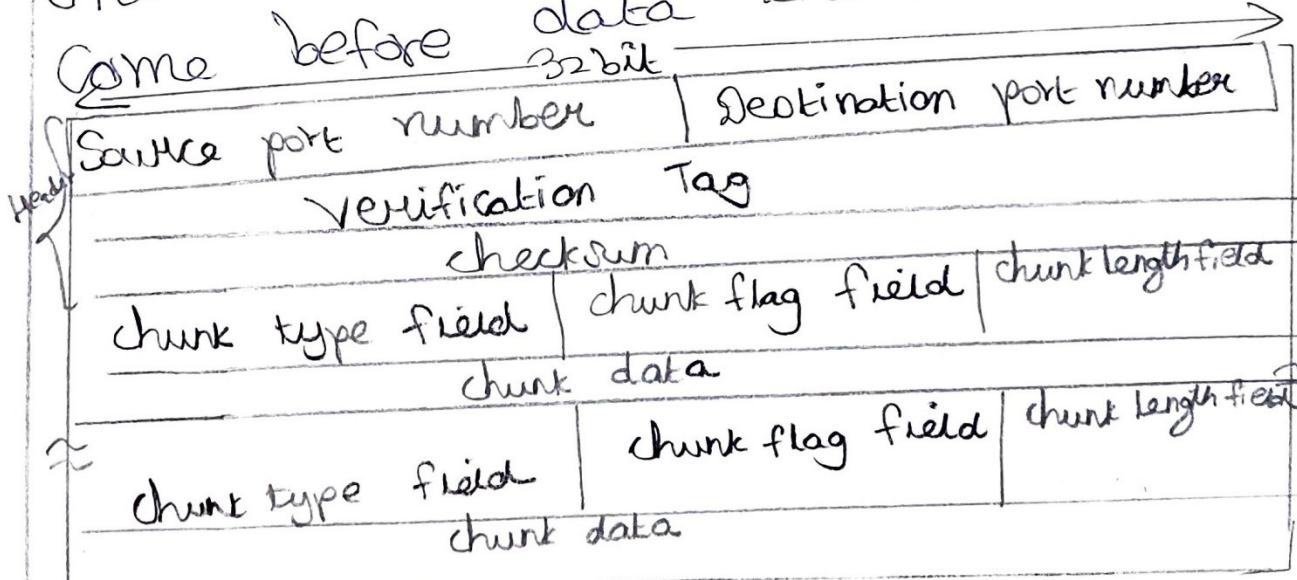
i) delivers datagrams reliably
ii) provides multiple streams to remove head-of line blocking
iii) delivers out-of-order datagrams
iv) provides destination address failover mechanism.
v) supports DNS interface to resolve hostname parameter.
vi) Supports path probing procedure
vii) Supports multi-homing
viii) provides extensive run-time error checking support.
ix) Supported user defined IP parameters.

3). Transmission Sequence Number:

* It allows multiple message streams to be exchanged on a single SCTP Connection.
* Data from multiple streams can be sent in a single SCTP message as chunks.
* Selective acknowledgements are supported at individual chunk level.
* Recent additions to SCTP protocol allow dynamic configuration of IP addresses.

4) SCTP packet Format:

It transmits data in the form of messages and each message contains one or more packets. The control chunks came before data chunks.



* Source and destination port numbers enable multiplexing of different SCTP

association at same address.
* A 32bit verification tag that guards against insertion of an out-of-date or false message into SCTP association.
* A 32-bit checksum for error detection. The checksum can be either a 32bit CRC checksum.
* Every SCTP packet contains the common header. The header contains 4 different fields and is set for every SCTP packet.

Quality of Service (QoS):

* In any multimedia application audio/video packets are delay sensitive but by internet all packets are treated equally ie QoS offered is same for all applications. It causes congestion in traffic followed by delay and loss of packets.
* Analyzing varying network scenarios principles of QoS needed for multimedia applications are derived.

principle 1:

Packet marking allows a router to distinguish among packets belonging to different classes of traffic.

Modified principle 1:

Packet classification allows a router to distinguish among packets belonging to different classes of traffic.

principle 2:

A degree of isolation is desirable among traffic flows, so that one flow is not adversely affected by another misbehaving flow.

principle 3:

For isolating flows, it is desired to use resources like BW and buffers as efficiently as possible.

principle 4:

A call admission process is needed where flow declare their QoS requirement.

1) policing:

policing is the regulation of the rate at which packet flow is injected into the network.

Three important policing criteria are,

i) Average rate:

It is defined as packets per time interval. It can be limited as a policy, It limits the traffic in network for a long period of time.

ii) peak rate:

It is defined as maximum number of packets that can be sent over a short period of time over a network.

iii) Burst size:

It is the maximum number of packets that can be sent into network over a extremely short interval of time.

2) Integrated Services:

It is a framework to provide guaranteed QoS to individual application session. A call step process involves following steps.

i) Traffic characterization and specification of desired QoS

ii) Signaling for call setup

iii) Per element call admission

3) Differentiated Services QoS:

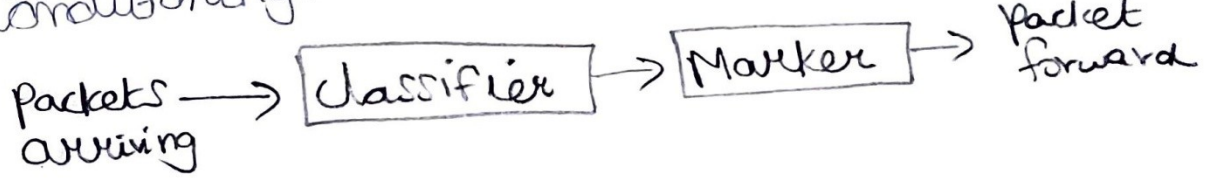
* The architecture has the ability to handle different classes of traffic in different ways within the internet. This approach is known as class-based QoS

i) Functional Elements of Differentiated Service:

It consists of two sets of functional elements.

a) Edge Function:

The packet arriving at edge of network are marked. It defines the class of traffic to which it belongs. Depending on the mark, the packet may be immediately forwarded into the network, delayed or discarded. It is called as packet classification and traffic conditioning.



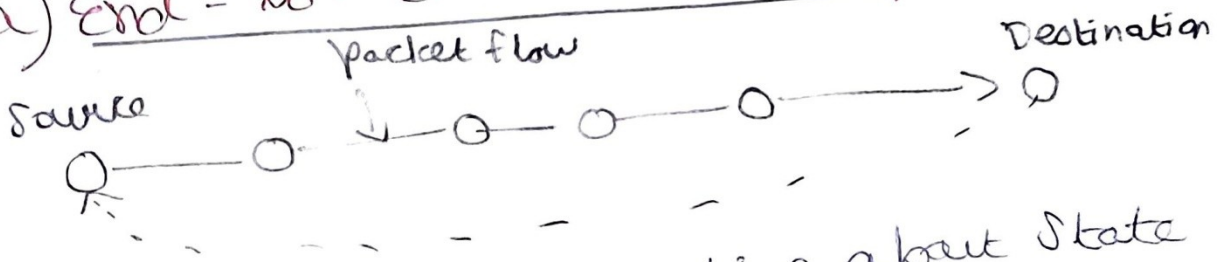
b) Core Function:

on forwarding the packet by router is then put on for next hop according to per hop behavior. It is a forwarding function of Diffserv.

ii) Closed loop control:

It try to alleviate congestion after it happens.

a) End-to-End closed loop control:



The feedback information about state of the network is propogated back to source can regulate packet flow rate.

b) Hop-by-Hop closed loop control:

* The feedback information may be forwarded directly by a node that detects congestion or it may be forwarded to destination first then relays the information to the source.
* The state of network is propogated to upstream node.
* When a node detects congestion on its outgoing link, can tell its upstream neighbour to slow down its transmission rate.

UNIT-III

Network Layer

Switching: packet Switching:-

* Packet Switching is often used in computer networks where individual users have need of the channel intermittenly.
* While using the channel the application requires high bandwidth but most of the time each user doesnot requre channel at all. Such applications characterized by a high peak to average requirement for capacity are called bursty and are ideal for packet Switching
* In packet switching, messages are broken into short blocks and interleared with other messages. Thus users queue for the channel and share it with one another efficiently. Data is sent in individual packets.
* Each packet is forwarded from Switch to Switch, eventually reaching its destination. Each Switching node has a small amount of buffer space to temporarily hold packets.

*If the outgoing line is busy, the packet stay in queue, until the line becomes available. packet switching handles burstly traffic well.

Packet Switching method uses two routing approaches:

i) Datagram
ii) Virtual circuit

i) Implementation of Connection-oriented Service:-

*Connection-oriented network is also known as Virtual circuit. It is similar to telephone system.

*A route which consists of a logical connection is established between two users.

*The connection is established is not a dedicated path between Stations.

*The path is generally shared by many other Virtual connections.

The process is completed in three main phases:

i) Establishment phase:

During setting up of logical connection, two users not only agree to setup a connection between them but also decide upon the quality of service associated with the connection. After this the sequence of packetized information are transmitted bidirectionally between the nodes. The information is delivered to the receiver in the same order as transmitted by sender.

ii) Data transfer phase:

During this phase, it performs flow control and error control services. It ensures correct sequencing of packets and correct arrival of packets. Flow control service ensures a slow receiver from being overwhelming with data from a faster transmitter.

iii) Connection Release:

When the stations wish to close down the virtual circuit, one station can terminate the connection with a clear-request packet.

IPV4 Addresses:

* Ip corresponds to the network layer in OSI reference model and provides a connectionless best effort delivery service to transport layer.
An Internet protocol (IP) address has a fixed length of 32 bits.
* The address structure was originally defined to have a two level hierarchy:
* The network ID identifies the network the host is connected to.
* The host ID identifies the network connection to the host rather than the actual host.

1) Classful Addressing:

The Ip address structure is divided into 5 address classes: Class A, Class B, Class C, Class D and class E identified by most significant bits of addresses.

* In class A network, the first byte is assigned to network address and the remaining three bytes used for the node addresses.

The class A format is

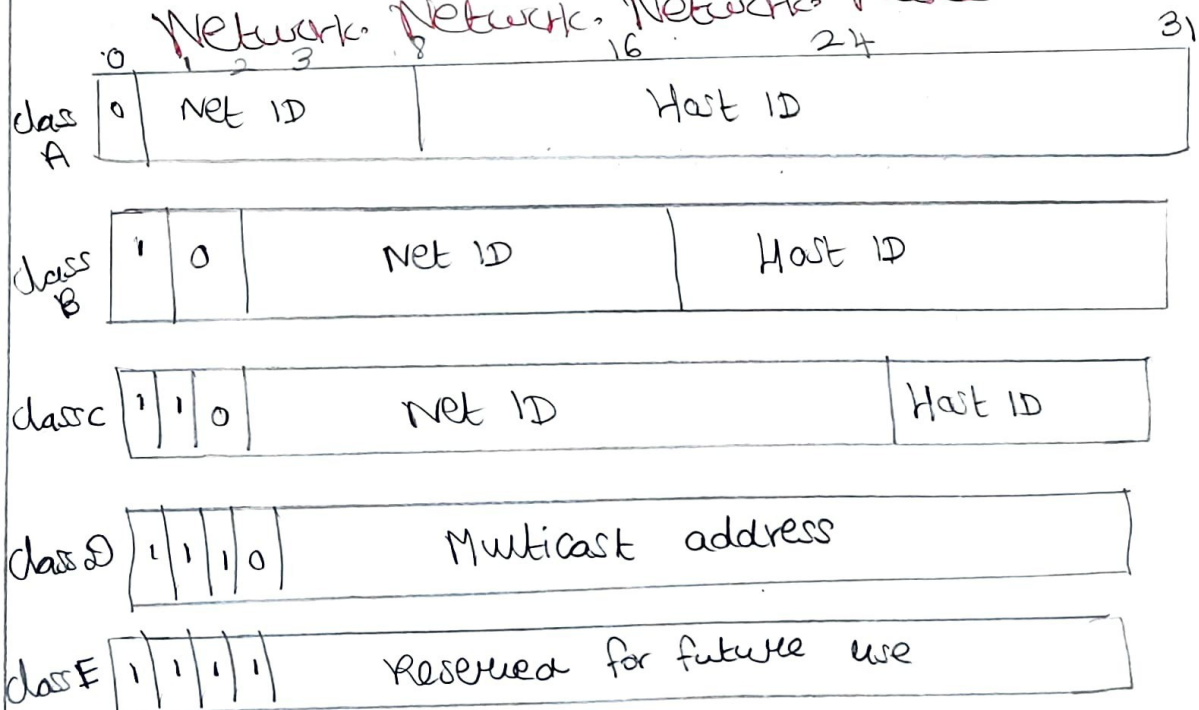
Network . Node . Node . Node

* In class B network, the first two bytes are assigned to the network address and remaining two bytes are used for node addresses. The format is

Network . Network . Node . Node

* In class C network, the first three bytes are assigned to network address and only one byte is used for node address. The format is

Network . Network . Network . Node

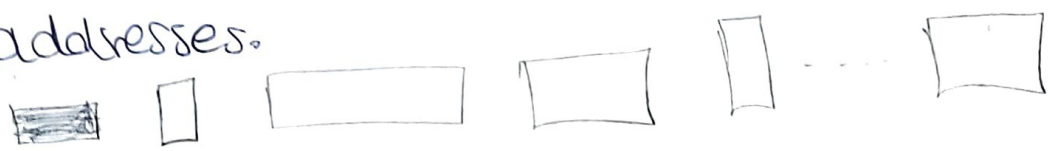


2) Classless Addressing:

* In classless addressing variable length blocks are assigned that belong to no class. The entire address space

is divided into blocks of different sizes. An organization is granted a block suitable for its purposes.

* When an entity, small or large needs to be connected to the internet is granted a block of addresses.



3) Header Format:

packets in IPV4 layer are called datagrams. A datagram is a variable length packet consisting of two parts: Header and data.

0 3	4 7	8 15 16	18 19 31
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits
Datagram Identification 16 bits			Flag 3 bits / Fragment offset 13 bits
Time to live 8 bits	Protocol 8 bits		Header checksum 16 bits
Source IP address 32 bits			
Destination IP address 32 bits			

i) VER is the field that contains IP protocol version. The current version is 4. 5 an experimental version. 6 is the version for IPV6.

ii) HLEN: is the length of ip header. The minimum value for correct header is 5, the maximum value is 15. 107

iii) Service type is an indication of QoS requested for ip datagram.

iv) Total length specifies the total length of datagram, header and data in octets.

v) Identification is a unique number assigned by sender used with fragmentation.

vi) Flags contain control flags: The 1st bit is reserved & must be 0. The 2nd bit is Do not Fragment. The 3rd is More Fragment.

vii) Fragment offset is used to reassemble the full datagram.

viii) Time to Live (TTL): Specifies the time the datagram is allowed to travel.

ix) Protocol number indicates higher level protocol to which ip should deliver data.

x) Header checksum is a checksum for the information contained in the header.

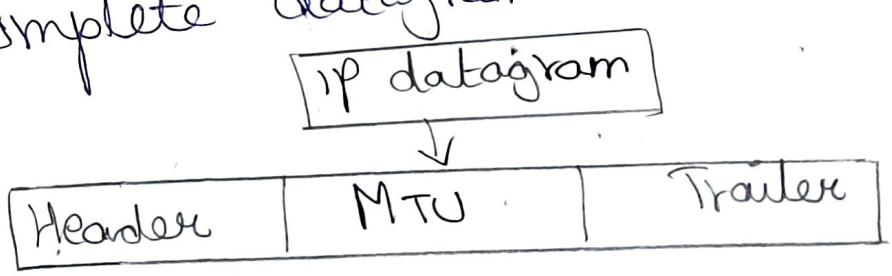
xi) Source/Destination ip address are 32 bit

xii) ip option is a variable-length field used for control and debugging measurement.

xiii) Padding is used to ensure IP header. The padding is 0.

4) IP Fragmentation:

* IP provides fragmentation/reassembly of datagrams. The maximum length is 65,535 octets.
* When an IP datagram travels from one host to another, it may pass through different physical networks.
* Each physical network has a maximum frame size called Maximum Transmission Unit (MTU) limit datagram length.
* The fragment of datagram each have a header.
* If one of fragment gets lost, the complete datagram is considered lost.



5) Options:

The header of IPv4 datagram is made of two parts: A fixed part

and a variable part. options used in IPv4 are,

i) Single byte:

No operation and end of operation

ii) Multiple byte:

Record route, Strict source route, loose source route and timestamp

a) No operation:

option is 1-byte option used as a fitter between options.

b) End of option:

It is a 1-byte option used for padding at end of the option field.

c) Record route option:

It is used to record the internet routers that handle the datagram. It can list upto 9 router addresses.

d) Strict Source route option:

It is used by source to predetermine a route for the datagram as it travels through the Internet.

e) Loose Source route option:

It is similar to Strict Source route but it is less rigid. Each router in the list must be visited.

f) Timestamp option:

It is used to record the time of datagram processing by a router.

g) Subnetting a Network:

If an organization is large or if it is dispersed to divide network into smaller ones, Computers are geographically connected together by routers. The benefits include,

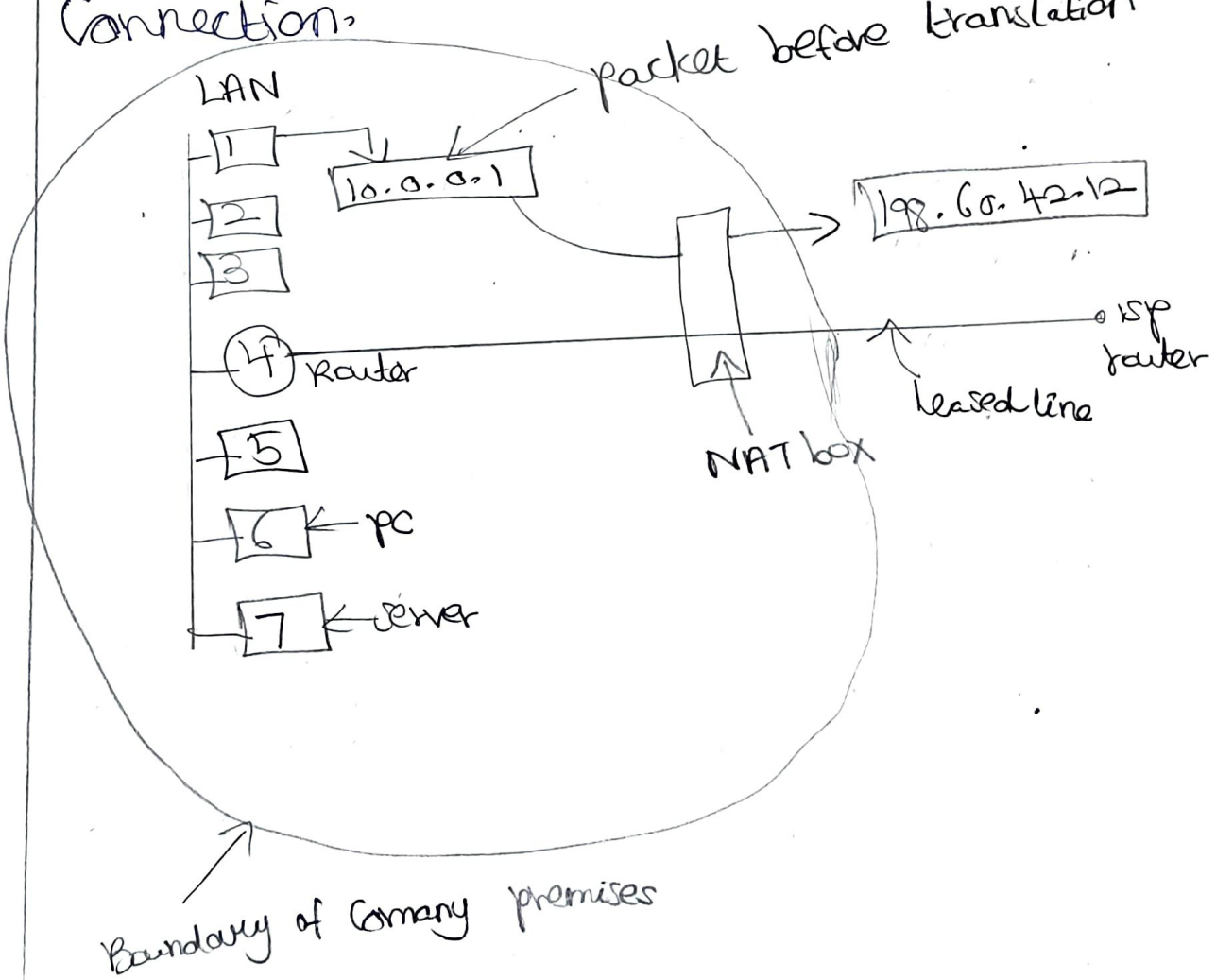
i) Reduced network traffic
ii) optimized network performance
iii) Simplified network management
iv) Facilities Spanning large geographical distances

* To allow a single network address to span multiple physical networks is called subnet addressing or subnet routing or Subnetting.
* It is a required part of IP addressing.

* A process that extracts the address of the physical layer network from an ip address is called masking

7) Network Address Translation (NAT):

When process want to establish a Tcp connection with a remote process, attached itself to an unused Tcp port on its own machine. It is called a source port and Tcp code to send incoming packets belonging to this connection.



8) Classless Inter Domain Routing (CIDR):112

* Dividing the Ip address space into A, B and C classes turned out to be inflexible.
* Ip is rapidly becoming a victim of its own popularity, it is running out of addresses.
* An arbitrary prefix length ~~to~~ indicate network number known as CIDR adopted in place of classful scheme.
* The entries in CIDR routing table contain 32-bit Ip address and a 32-bit mask.
* CIDR uses a technique called Supernetting so that a single routing entry covers a block of classful addresses.
* CIDR route packets according to the higher order bits of the Ip address.
* The use of variable length prefixed requires the routing tables are searched to find longest prefix match.

IPV6:

It provides the host to host communication between system in the Internet. It has played a central role in the internetworking environment for many years.

1) Address Types:

IPV6 allows three types of addresses.

i) Unicast:

An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.

ii) Anycast:

An identifier for a set of interfaces. A packet sent to an anycast address is delivered to one of the interfaces identified by address.

iii) Multicast:

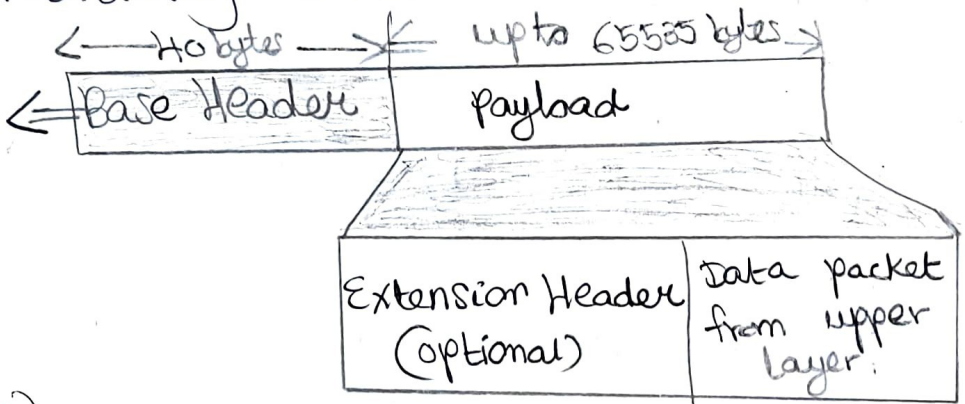
An identifier for a set of interfaces. A packet sent to a multicast address is delivered to all interfaces identified by that address.

* The first field of any IPV6 address is the Variable-length format prefix

which identifies various categories of address.

2) Packet Format:

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



i) Version:

The 4 bit field defines the version number of IP. The value is 6 for IPv6.

ii) Priority:

The 4 bits priority defines the priority of the packet with respect to traffic congestion.

iii) Flow label:

It is 24 bit field is designed to provide special handling for a particular flow of data.

iv) Payload length:

The 16 bits payload length field defines the length of IP datagram excluding base header.

v) Next Header:
It is an 8 bit field defining the header follows the base header in the datagram.

vi) Hop Limit:
It serves the same purpose as TTL field in IPV4.

vii) Source Address:
It is a 128 bit internet address that identifies the original

viii) Destination Address:
It identifies the final destination of the datagram.

4 bits	4 bits	8 bits	8 bits	8 bits
VER	PRI	Flow Label		
Payload length		Next header	Hop limit	
Source address				
Destination address				
Next header	Header length			
Next header	Header length			
Next header	Header length			

3) Extension Headers:
The length of the base header is fixed at 40 bytes. Types of extension headers are,

i) Hop by hop option:
It is used when the source needs

to pass information to all routers visited by datagram.

ii) Source routing:
It combines the concept of strict source and loose route route options of IPV4.

iii) Fragmentation:
It is same as in IPV4. In IPV6 only the original source can fragment.

iv) Authentication:
It has a dual purpose. It validates the message sender & ensures the integrity of data.

v) Encrypted security payload:
It is an extension that provides confidentiality and guards against eavesdropping

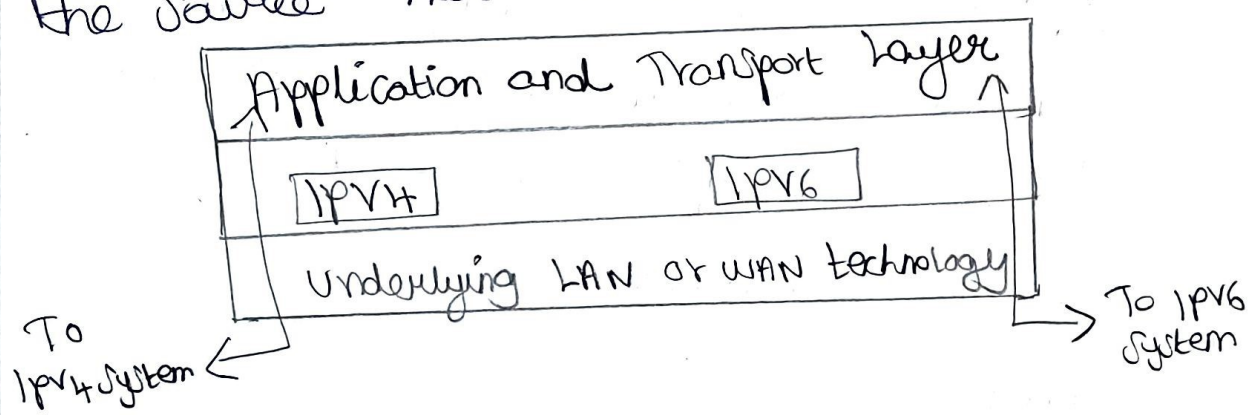
vi) Destination option:
It is used when the source needs to pass information to the destination only. Intermediate routers are not permitted access to this information.

4) Transition from IPV4 to IPV6:
Three strategies have been devised by IETF to help the transition.

i) Dual Stack:
All the host must run IPV4 and

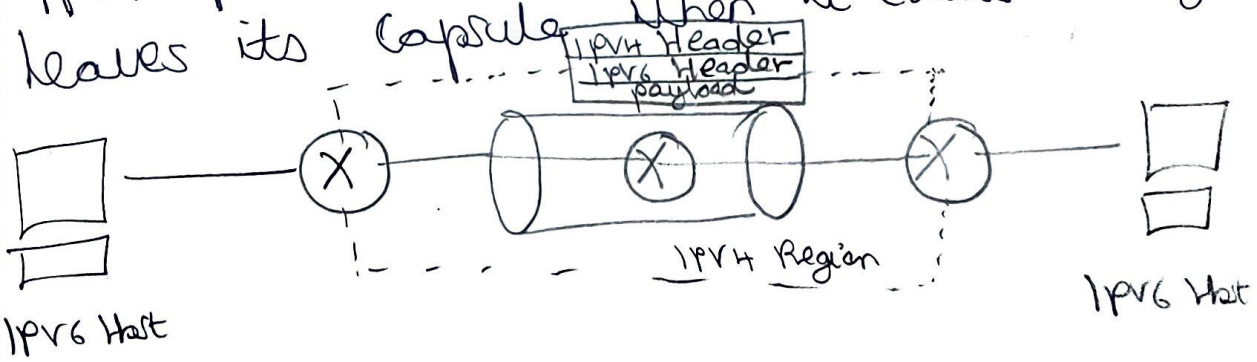
IPv6 simultaneously until all Internet uses IPv6.

* To determine which version to use when sending a packet to destination, source host queries the DNS.
* If the DNS returns an IPv4 address, the source host sends an IPv4 packet.
* If the DNS returns an IPv6 address, the source host sends an IPv6 packet.



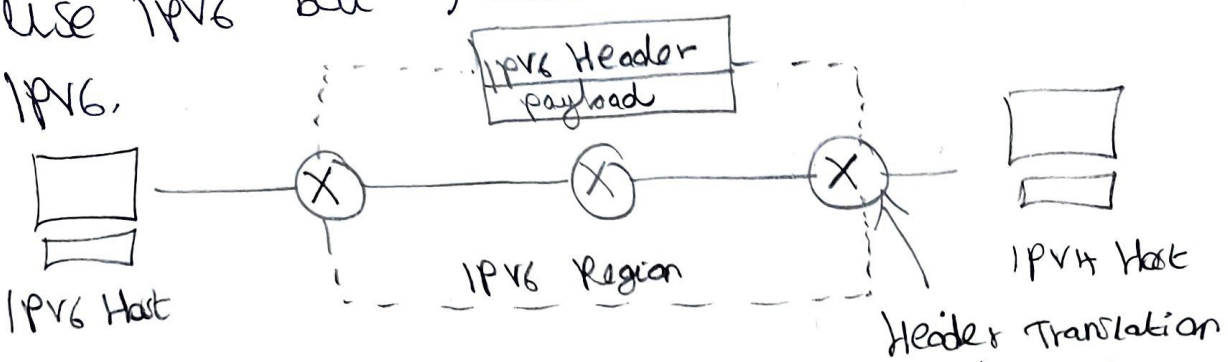
ii) Tunneling:

* When two computers using IPv6 want to communicate with each other and packet must pass through a region uses IPV4.
* The IPv6 packet is encapsulated in an IPv4 packet when it enters region and leaves its capsule when it exists the region.



iii) Header Translation:

It is used when some of the system uses IPV4. The sender wants to use IPV6 but receiver does not understand IPV6.

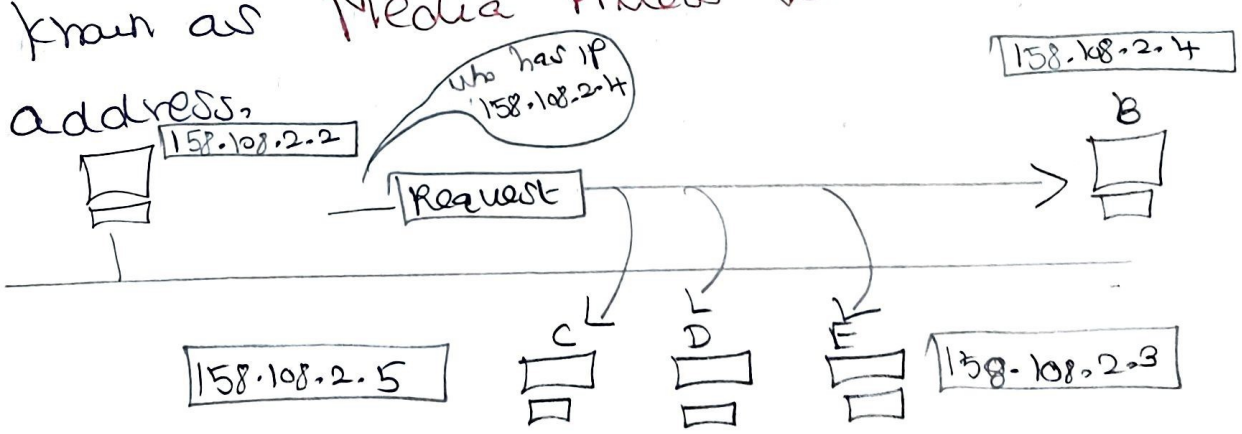


* The header format must be totally changed through header translation. The header of IPV6 packet is converted to IPV4 header.

ARP:

Address Resolution Protocol

It is a procedure for mapping a dynamic Ip address to a permanent physical machine address in a LAN. The physical machine address is also known as Media Access Control (MAC) address.



*Computer A and Computer B share a physical network. Each computer has an assigned IP address I_A and I_B physical address P_A and P_B. The problem of mapping high level to physical addresses is known as address resolution problem.

* physical addresses are of 2 types.

⇒ Ethernet has large and fixed physical addresses.

⇒ ProNET has small, easily configured physical addresses.

1) Packet Format:

Hardware type		protocol type
Hardware length	Protocol length	operation 1: Request 2: Reply
Sender hardware address		
Sender protocol address		
Target hardware address		
Target protocol address		

i) Hardware type:

It is defining the type of network on which ARP is running. Ethernet is given the type 1.

ii) Protocol type:

It is defining the protocol. The

Value of field for IPv4 protocol is 0800H. 120

iii) Hardware length:
It is an 8 bit field defining the length of the physical address in bytes. Ethernet is the value 6.

iv) protocol length:
It is defining the length of the logical address in bytes.

v) operation:
It is defining the type of packet. Its types are ARP Request (1), ARP reply(2)

vi) Sender Hardware Address:
It is a variable length field defining the physical address of the sender. Eg: Ethernet is 6 bytes long

vii) Sender protocol Address:
It is also a variable length field defining the logical address of the sender.

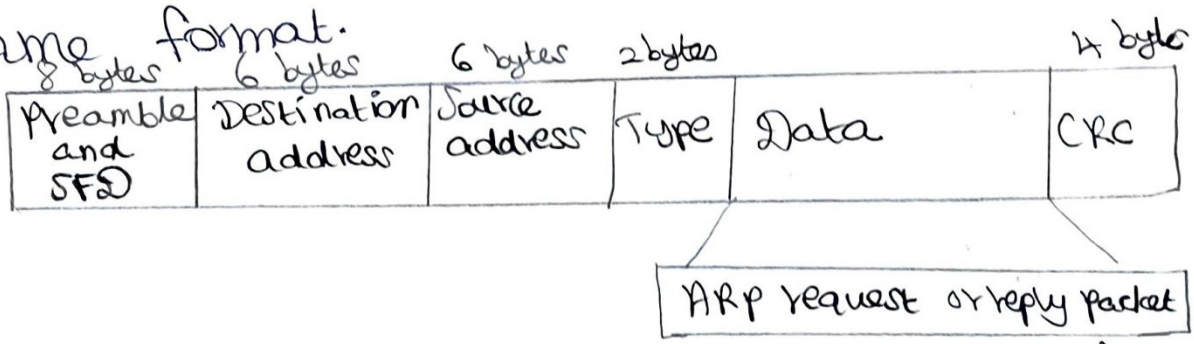
viii) Target Hardware Address:
It is a variable length field defining the physical address of the target.

iv) Target protocol Address:

It is also a variable length field defining the logical address of the target.

2) Encapsulation:

ARP request and reply have the same format.



* ARP table stores records on network hosts actively participate in network operations rather than on all network hosts.

* Such a method of storing information is known as caching, an ARP table is called an ARP cache

3) Proxy ARP:

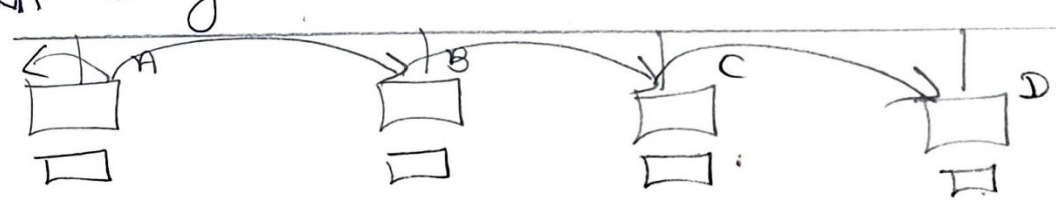
A technique called proxy ARP is used to create a subnetting effect. It is one of the variants of ARP allowing IP addresses to be mapped to

hardware addresses in network supporting broadcasting even when the requested host is located outside the boundaries of the current collision domain.

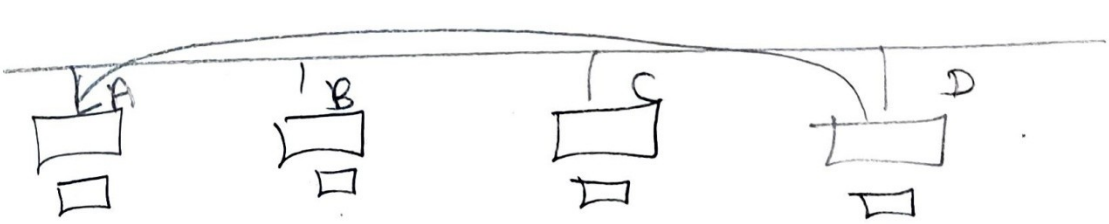
RARP:

Reverse Address Resolution Protocol

* The host know its MAC address but not its IP address.
* The problem of getting an IP address from MAC address can be handled by RARP is similar to ARP.
* The sender broadcast RARP request specifies as both the sender and target machine and supplies its physical address in target hardware address field.



ARP protocol



RARP Protocol

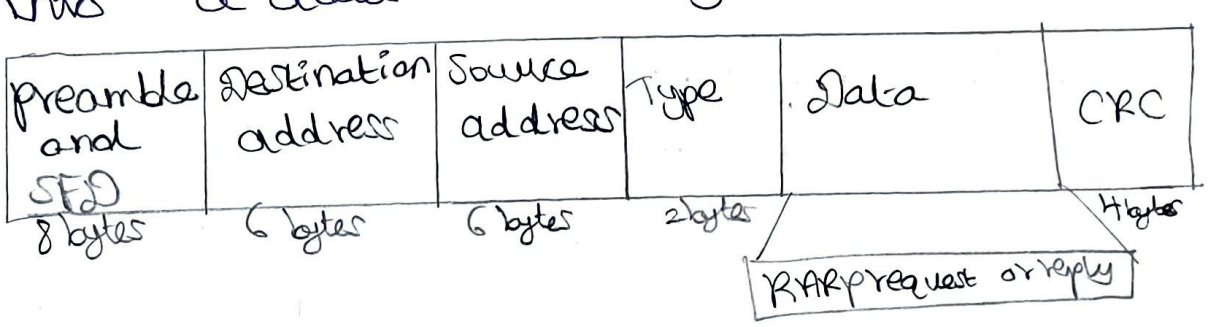
1) Frame Format of RARP:

Frame format is same as ARP frame format.

Hardware type		Protocol type
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware Address (6 bytes for Ethernet)		
Sender protocol Address (4 bytes for IP)		
Target Hardware Address (6 bytes for Ethernet)		
Target protocol Address (4 bytes for IP)		

2) Encapsulation:

RARP packet is encapsulated directly into a data link layer.

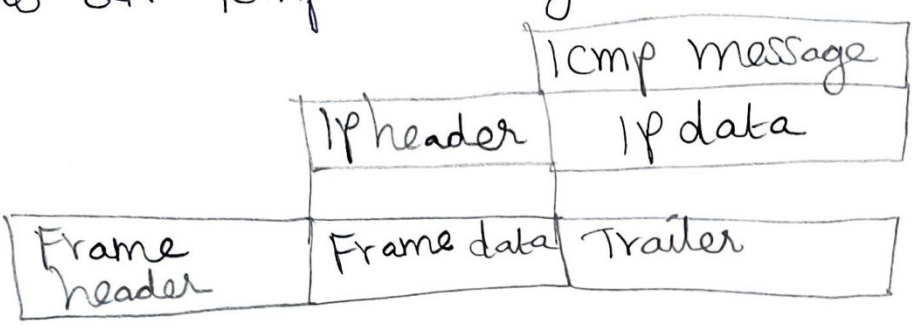


ICMP:

Internet Control Message protocol

It is a protocol that handles error and other control messages.

* ICMP is a network layer protocol.
* Its messages are not passed directly to data link layer.
* ICMP messages are encapsulated by IP packets.
* The value of the protocol field in IP datagram is -1 to indicate the IP data is an ICMP message.



i) Message Types:

All ICMP messages fall in the following classes:

i) Error Reporting:

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

ii) Query messages:

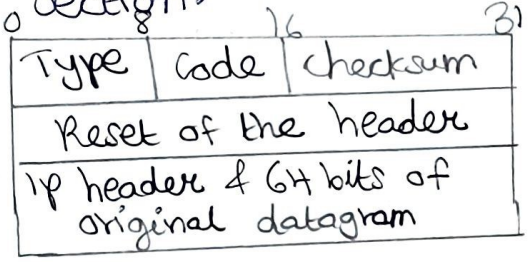
It occurs in pairs, help a host or a network manager get specific information from a router or another host.

The main functions associated with Icmp are,

i) Error Reporting
ii) Reachability testing
iii) Congestion control
iv) Route change notification
v) performance measuring
vi) Subnet addressing

2) 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.



i) Type:
It is 8 bit field identifies the type of the message.

ii) Code:
Size of the code field is 8 bits. It provides the information or parameter of the message type.

iii) Checksum:
It is used to detect errors in the Icmp message.

iv) IP header plus original datagram:

It can be used for diagnostic purposes by matching the information in ICMP message with the original data in the IP packet.

3) Error Reporting:

* ICMP does not correct errors, it simply reports them.
* Error correction is left to higher level protocols.
* Error messages are always sent to original source because the only information available in the datagram about the route is source and destination IP addresses.
* ICMP uses the source IP address to send the error message to the source of the datagram.

ICMP handles 5 types of errors.

i) Destination Unreachable:

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

ii) Source quench:

* A machine uses ICMP source quench messages to report congestion to the original source.
* It is a request for the source to reduce its current rate of datagram transmission.
* No ICMP message to reverse source quench message.
* Sources after receiving a quench message reduce their transmission rate and gradually increase their rate.

Type: 4	Code: 0	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus first 8 byte of datagram data		

iii) Time exceeded:

* Every IP datagram contains a field called "time to live" or TTL.
* On each hop along the path to the destination, TTL field is decremented by one.
* Whenever a router receives a datagram with a time-to-live value of zero, it discard the datagram and sends a time exceeded message to original source.

* When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source.

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		

(iv) Parameter problem:

* If the gateway or host processing a datagram finds a problem with header parameters such that it cannot complete processing the datagram it must discard the datagram.
* Devices that process datagrams may not be able to forward a datagram due to some type of error in header.
* It does not relate to the state of the destination host or network but still prevents the datagram from being processed and delivered.
* If a router or host find a problem with an IP header, it must discard the datagram.

* If a router or host finds a problem with an IP header, it must discard the datagram.
* The source host may be notified by being sent a parameter problem message.
* 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 received IP datagram including IP header plus the first 8 bytes of datagram data		

5) Redirection:

* ICMP redirect messages can only be sent by routers.
* The interface on which packet comes into router is the same interface on which packet gets routed out.
* The datagram is not source-routed.
* The router is configured to send redirects.

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

4) Echo Request and Reply:

* This query message is used for diagnostic purposes.
* Network manager and users utilize pair of messages to identify network problems.
* A host or router can send an echo request message to another host or router.
* The host or router that receives an echo request message creates an echo reply message and returns it to original sender.
* An echo request message can be sent by a host or router.
* An echo reply message is sent by host or router which receives an echo request message.

Type: 8 or 0	Code: 0	checksum
Identifier		Sequence number
Optional data Sent by request message: Repeated by reply message		

5) Timestamp Request and Reply:

* Timestamp-request and timestamp-reply messages can be used to calculate the round-trip time between a source and a destination machine if their clocks are not synchronized.
* The timestamp messages are best known as part of the trace route programs.
* The timestamp reply is the reply to a timestamp message.

Type: 13 or 14	Code: 0	checksum
Identifier		sequence number
original timestamp		
Receive timestamp		
Transmit timestamp		

6) Address Mask Request and Reply messages:

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

* To obtain its mask, a host sends an address mask request message to a Router on LAN.
* If host knows the address of the router, it sends request directly to router.
* If it does not know, it broadcasts the message.

Type: 17 or 18	Code: 0	checksum
Identifier		Sequence number
Address mask		

7) Router Solicitation and Advertisement:

* It can send out a router-Solicitation message.
* It can be broadcast on current network.
* The router receives the Solicitation message broadcast their routing information using router advertisement message.
* A router can also periodically send router advertisement messages if no host has solicited.

Type: 10	Code: 0	Checksum
Identifier		Sequence number

* Identifier and Sequence number fields are not used.

Type: 9	Code: 0	checksum
No of addresses	Address Entry size	Lifetime
Router Address 1		
Address preference 1		
Router Address 2		
Address preference 2		
⋮		

* It is the Reply that comes back from the previous Request.
* Lifetime field shows the number of seconds that the entities are considered to be valid.

DHCP:-

Dynamic Host Configuration Protocol

* It is a network management protocol.
* Bootstrap (BooTP) is a static Configuration protocol.
* Each client has a permanent network connection.
* When a client requests its IP address, BooTP server consults a table that

matches the physical address of the client with its ip address. The binding is predefined.

* If the client moves from one physical network to another then it creates problem.
* Wireless networking and portable Computer ie laptops and notebooks may move from one network to another.
* DHCP provides static and dynamic address allocation can be manual or automatic.
* The DHCP work like plug and play networking.
* When a Computer discovers a DHCP Server, the Computer saved the Server's address in a cache on permanent Storage. once it obtains an ip address, Computer saves ip address in a cache.

DHCP Message Format:

i) op field:

Specifies whether the message is a request or a response.

ii) HType:
It specifies the network hardware type.

iii) HLEN:
It specifies length of a hardware address.

iv) Hops:
It specifies how many servers forwarded the request.

v) Transaction Identifier:
It provides a value that a client can use to determine if an incoming response matches its request.

vi) Client ip address:
computer fills this field in a request.

vii) Your ip Address:
Server uses this field to supply the value if computer does not know its address.

viii) Server ip Address and server Host Name:
Use by server to give computer information about the location of a computer that runs server.

ix) Router ip Address Field:
Contains ip address of default router.

x) Flags and options Field:

Use to encode additional information. To distinguish among various messages that a client uses to discover server or request an address or that a server uses to acknowledge.

Working of DHCP:

A DHCP infrastructure consists of following elements:

i) DHCP Servers:

Computers that offer dynamic configuration of IPv4 addresses and related to DHCP clients.

ii) DHCP clients:

Network nodes that support the ability to communicate with DHCP server to obtain dynamically leased IPv4 address and related configuration parameters.

iii) DHCP Relay agents:

Network nodes, typically routers listen for broadcast & unicast DHCP message relay them between DHCP server

and Dhcp clients.

Dhcp options and message type:

Dhcp message is either a boot request (1) or a boot Meply (2)

* One option with value 53 for the tag subfield is used to define the type of interaction between client and server.
* other options define parameters such as lease time and so on.

Tag (8 bit)	length (8 bit)	value (variable length)

Renewal and Rebinding Timers:

* The process of renewal and rebinding are designed to ensure a client's lease can be extended before it is scheduled to end
* Each time an address is allocated or reallocated, the client starts two timers that control the renewal and rebinding process:

i) **Renewal Timer (T1):**

The timer is set by default to

50% of lease period. When it expires, the client will begin the process of renewing the lease. It is simply called "T1" in DHCP Standards.

ii) Rebinding Timer (T_2):

This timer is set by default to 87.5% of the length of the lease. When it expires the client will try to rebind. It is given the snappy name "T2" in DHCP Standards.

* If the client successfully renews the lease when T1 timer expires, will result in a "fresh lease" and both timers will be reset. T2 only comes into play if the renewal is not successful.
* It is possible to change the amount of time to which these timers are set, but T1 must expire before T2 which in turn expire before the lease itself ends. These usually are not changed from the default, but may be modified.

UNITIV ROUTING

Routingandprotocols:Unicastrouting-DistanceVectorRouting-RIP-LinkState Routing – OSPF– Path-vector routing - BGP - Multicast Routing: DVMRP – PIM

Routing

- A Router is a process of selecting path along which the data can be transferred from sourcetothedestination.Routingisperformedbyaspecialdeviceknownasarouter.
- ARouterworksatthenetworklayerintheOSImodelandinternetlayerinTCP/IP model
- Arouterisanetworkingdevicethatforwardsthepacketbasedontheinformation available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothingbutasoftwareresponsiblefordecidingtheoptimalpaththroughwhichpacket can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery.Themetricisthestandardofmeasurementsuchashopcount,bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- Theroutingalgorithminitializesandmaintainstheroutingtablefortheprocessof path determination.

Themostcommonmetricvaluesaregivenbelow:

- **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 primarymetricvalue,thenthepathwiththeleasthopcountwillbeconsideredasthe best path to move from source to the destination.
- **Delay:**Itisatimetakenbytheroutertoprocess,queueandtransmitadatagramtoan 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 protocolwilldeterminethebandwidthcapacityforallthelinksalongthepath,andthe 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,packetsprocessedpersecond.Ifthetrafficincreases,thentheloadvalue 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 dependsonthenetworklinks,anditsvalueismeasureddynamically.Somenetworks 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.

TypesofRouting

Routingcanbeclassified intothree categories:

- Static Routing
- DefaultRouting
- DynamicRouting

Static Routing

- StaticRoutingisalsoknownasNonadaptive Routing.
- Itisatechniqueinwhichtheadministratormanuallyaddstheroutesinarouting table.
- ARoutercansendthepacketsforthedestinationalongtheroutedefinedbythe administrator.
- Inthistechnique,routingdecisionsarenotmadebasedontheconditionortopology of the networks

AdvantagesOfStatic Routing

FollowingaretheadvantagesofStatic Routing:

- **NoOverhead:**IthashooverheadontheCPUusageoftherouter.Therefore,the cheaper router can be used to obtain static routing.
- **Bandwidth:**Ithasnotbandwidthusagebetweentherouters.
- **Security:**Itprovidessecurityasthesystemadministratorisallowedonlytohave control over the routing to a particular network.

DisadvantagesofStatic Routing:

FollowingarethedisadvantagesofStatic Routing:

- Foralargenetwork,itbecomesaverydifficulttasktoaddeach routemanuallytothe routing table.
- Thesystemadministratorshouldhaveagoodknowledgeofatopologyashehasto add each route manually.

DefaultRouting

- DefaultRoutingisatechniqueinwhicharouterisconfiguredtosendallthepackets 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.

- DefaultRoutingisusedwhennetworksdealwiththesingleexitpoint.
- Itisalsousefulwhenthebulkoftransmissionnetworkshavetotransmitthedatato the same hp device.
- When a specific route is mentioned in the routing table, the router will choose the specificrouteratherthanthedefaultroute.Thedefaultrouteischosenonlywhena specific route is not mentioned in the routing table.

DynamicRouting

- ItisalsoknownasAdaptiveRouting.
- Itisatechniqueinwhich arouteraddsanewrouteintheroutingtableforeachpacket in response to the changes in the condition or topology of the network.
- Dynamicprotocolsareusedtodiscoverthenewroutestoreachthedestination.
- InDynamicRouting,RIPandOSPFaretheprotocolsusedtodiscoverthe new routes.
- Ifanyroutegoesdown,thentheautomaticadjustmentwillbemadetoreachthe destination.

TheDynamicprotocolshouldhavethefollowingfeatures:

- Alltheroutersmusthavethesamedynamicroutingprotocolinordertoexchangethe routes.
- Iftherouterdiscoversanychangeintheconditionortopology,thenrouterbroadcast this information to all other routers.

AdvantagesofDynamicRouting:

- Itiseasiertoconfigure.
- Itismoreeffectiveinselectingthebestrouteinresponsetothechanges inthe condition or topology.

DisadvantagesofDynamicRouting:

- Itismore expensiveintermsofCPUandbandwidth usage.
- Itislesssecureascomparedtodefaultandstatic routing.

Unicastrouting

Unicast–Unicastmeansthetransmissionfromasinglesendertoasinglereceiver.Itisa point-to-point communication between sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

- TCPisthemostcommonlyusedunicastprotocol.Itisaconnection-orientedprotocol that relies on acknowledgement from the receiver side.
- HTTPstandsforHyperTextTransferProtocol.Itisanobject-orientedprotocolfor communication.

Therearethreemajorprotocolsforunicast routing:

1. DistanceVectorRouting
2. Link StateRouting

3. Path-VectorRouting

DistanceVector Routing

Distance vector routing algorithm is also called as **Bellman-Ford algorithm** or **Ford Fulkersonalgorithm**asthisalgorithmisusedtofindtheshortestroutefromonenodeto another node in the network.

The routing protocol is used to calculate the best route from source to destination based onthedistanceorhopsasitsprimarymetrictodefineanoptimalpath.Thedistancevectorrefers to the distance to the neighbor nodes, where routing defines the routes to the establishednode.

The**DistanceVectorroutingalgorithm**(DVR)sharestheinformationoftheroutingtable with the other routers in the network and keeps the information up-to-date to select an optimal path from source to destination.

TheBellman-Fordalgorithmisdefinedas:

$$d_x(y) = \min_v \{c(x, v) + d_v(y)\}$$

where, dx(y)=dx(y)= The least distance from x to y
c(x,v)=c(x,v)=Nodex'scostfromeachofitsneighbourv
dv(y)=dv(y)= Distance to each node from initial node
minv=minv= selecting shortest distance

Itworksinthefollowingsteps-

Step-01:

Eachrouterpreparesitsroutingtable.Bytheirlocalknowledge.eachrouterknowsabout-

- Alltheroutierspresentinthe network
- Distancetoitsneighboringrouters

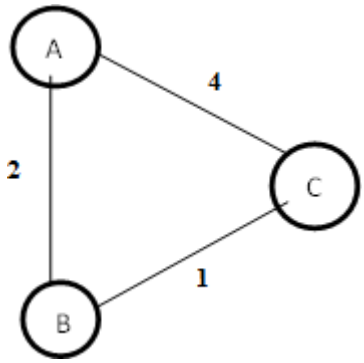
Step-02:

- Eachrouterexchangesitsdistancevector withitsneighboringrouters.
- Eachrouterpreparesanewroutingtableusingthedistancevectorsithasobtained from its neighbors.
- Thisstep isrepeatedfor(n-2) timesif there arenroutersinthenetwork.
- Afterthis,routingtablesconverge/becomestable.

Example–DistanceVectorRouterProtocol

Inthenetworkshownbelow,therearethreerouters,A,B, andC,with thefollowing weights –AB=2, BC=3 andCA=5.

Step1–InthisDVRnetwork,eachroutersharesitsroutingtablewitheveryneighbor.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.



FormA	A	B	C
A	0	2	3
B			
C			

FormB	A	B	C
A			
B	2	0	1
C			

FormC	A	B	C
A			
B			
C	3	1	0

Step2−Ifthepathviaaneighborhasalowercost,thentherouterupdatesitslocaltableto forward packets to the neighbor. In this table, the routerupdates 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.

FormA	A	B	C
A	0	2	3
B			
C			

FormB	A	B	C
A			
B	2	0	1
C			

FormC	A	B	C
A			
B			
C	3	1	0

Step3−Thefinalupdatedroutingtablewithlowercostdistancevectorroutingprotocolfor all routers A, B, and C is given below –

RouterA

FormA	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

RouterB

FormB	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

RouterC

FormC	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

RIPProtocol

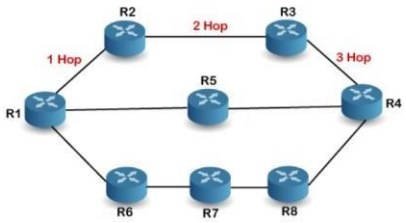
RIP stands for Routing Information Protocol. RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area. To understand the RIP protocol,ourmainfocus istoknowthestructureofthepacket,howmanyfieldsitcontains, and how these fields determine the routing table.

Beforeunderstandingthestructureofthepacket,we firstlookatthefollowingpoints:

- RIPisbasedonthedistancevector-basedstrategy,soweconsidertheentirestructure as a graph where nodes are the routers, and the links are the networks.
- In aroutingtable,thefirstcolumnisthedestination,orwecansaythatitisanetwork address.
- Thecostmetricisthenumberofhopstoreachthedestination.Thenumberofhops available in anetwork would be thecost. The hop count isthe number ofnetworks required to reach the destination.
- In RIP, infinity is defined as 16, which means that the RIP is useful for smaller networksorsmallautonomoussystems.ThemaximumnumberofhopsthatRIPcan contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.
- Thenextcolumncontainstheaddressoftheroutertowhichthepacketistobesentto reach the destination.

Howishopcount determined?

Whentherouter sendsthepackettothe networksegment, thenitiscountedasasinglehop.

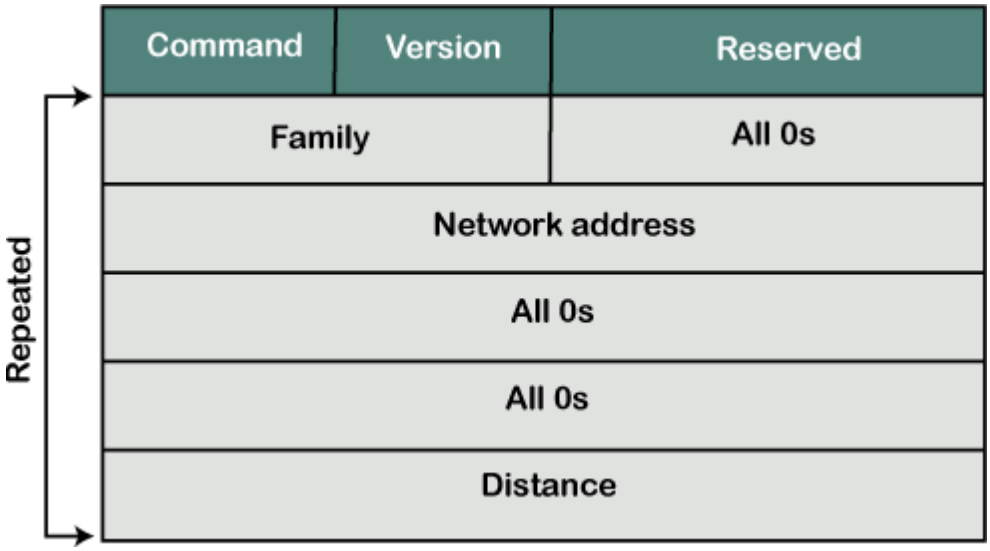


In the above figure, when the router 1 forwards the packet to the router 2 then it will count as 1hopcount.Similarly,whentherouter2 forwardsthepackettotherouter3thenitwillcount

as2hopcount,andwhen therouter3forwardsthepackettorouter4,itwillcountas3hop count. In the same way, RIPcan support maximum upto 15 hops, which means that the 16 routers can be configured in a RIP.

RIPMessageFormat

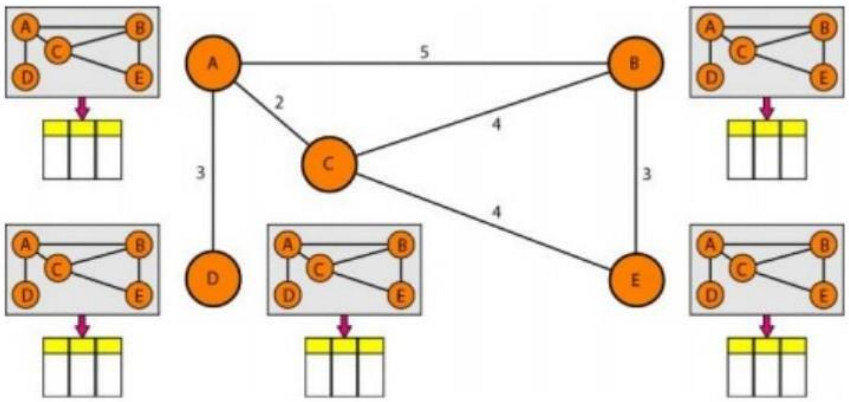
Now,welookatthestructureoftheRIPmessageformat.Themessageformatisusedto share information among different routers. The RIP contains the following fields in a message:



- Command:Itisan8-bitfieldthatisusedforrequestorreply.Thevalueoftherequest is 1, and the value of the reply is 2.
- Version:Here,versionmeansthatwhichversionoftheprotocolweareusing. Suppose weare using the protocol of version1, then weput the 1 in this field.
- Reserved:Thisisareservedfield,soitisfilledwith zeroes.
- Family:Itisa16-bitfield.AsweareusingtheTCP/IPfamily,soweput2valuein this field.
- NetworkAddress:Itisdefinedas14bytesfield.IfweusetheIPv4version,thenwe use 4 bytes, and the other 10 bytes are all zeroes.
- Distance:Thedistancefieldspecifiesthehopcount,i.e.,thenumberofhopsusedto reach the destination.

LinkStateRouting

Linkstateroutinghasadifferentphilosophyfrom thatofdistancevectorrouting.Inlinkstate routing,ifeachnodeinthedomainhastheentiretopologyofthedomainthelistofnodesand links, how they areconnected 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 eachpersonmayhavethesamemap,eachneedstotakeadifferent routeto reachherspecific destination

BuildingRoutingTables:

Inlinkstaterouting,foursetsofactionsarerequiredtoensurethateachnodehastherouting table showing the least-cost node to every other node.

a) Creationofthestatesofthelinksby eachnode, calledthe linkstate packet (LSP).

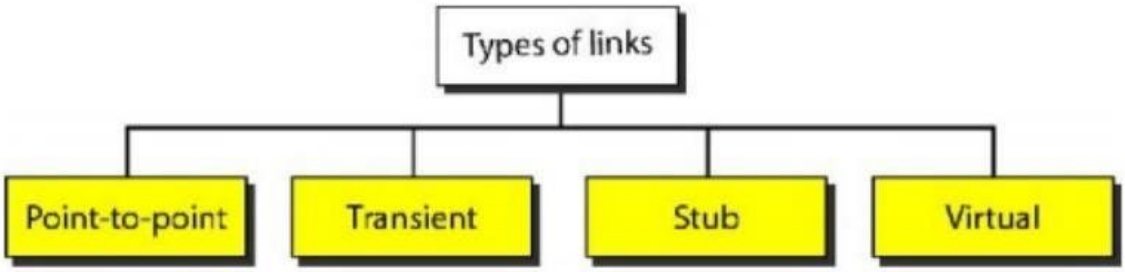
b) Dissemination of LSPs to every other router, called **flooding,** in an efficient andreliableway.

c) Formation of a shortest path tree for each node.

d)Calculationofaroutingtablebasedontheshortestpathtree.

Types of Links

InOSPFterminology,aconnectioniscalleda*link.*Fourtypesoflinkshavebeendefined: 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.

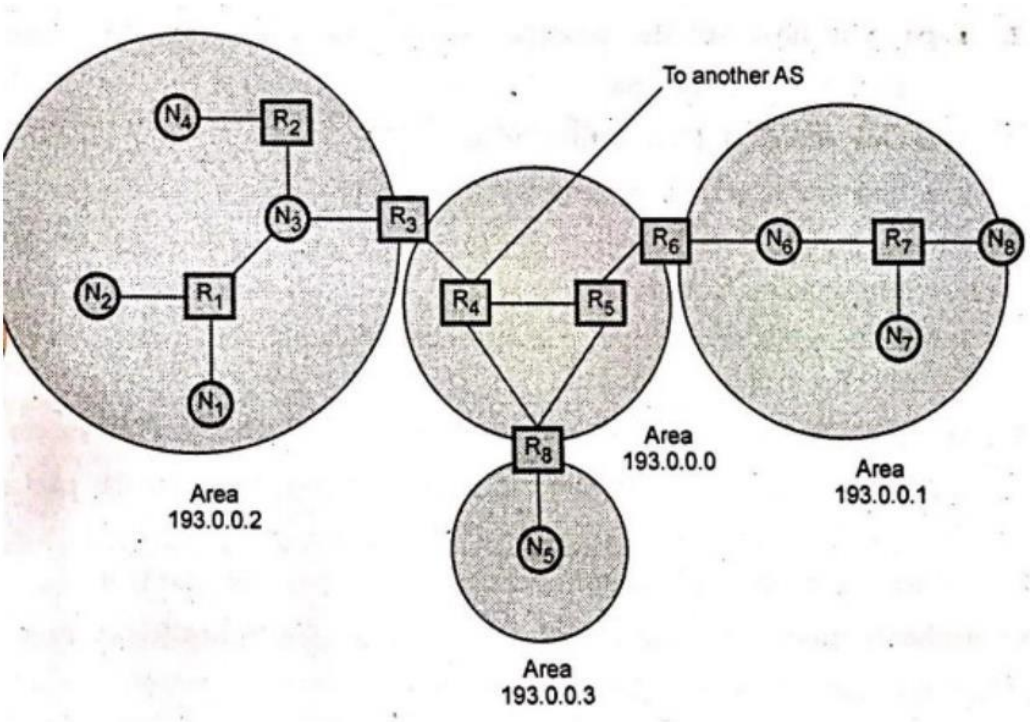
OpenShortestPathFirst (OSPF)

• OSPFisalinkstaterouting protocol.

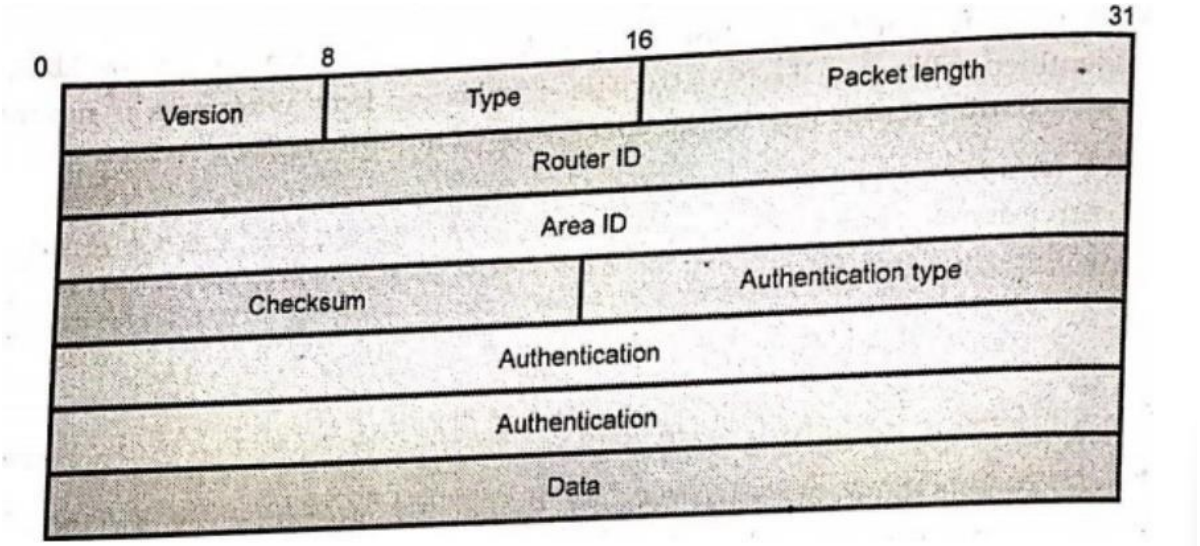
• FollowingisthefeaturesoftheOSPF.
1. OSPFsupportsmultiplecircuitloadbalancing..
2. OSPFcan convergevery quicklyto network topology change.
3. OSPFsupportmultiplemetrics.
4. OSPFsupportforvariablelengthsubnetting.

• OSPFusesfourtypesof routers.
1. Aninternalrouteris arouterwithallitslinksconnectedtothenetworkswithinthesame area.
2. Anareaborder routerisa routerthat hasitslinksconnected tomorethanonearea.
3. Abackbone routerisa routerthat hasitslinksconnectedtothe backbone.
4. AnAutonomousSystemBoundaryRouter(ASBR)isarouterthathasitslinksconnected to another autonomous system.

• AsshownintheFig. routers R1,R2andR7areinternalrouters.RoutersR3, R6, R8areareaborderrouters.RoutersR3,R4,R5,R6,R8arebackbonerouters.RouterR4is an ASBR



• Theheaderformat for OSPFisshown inthe Fig.



- OSPFheaderanalysisisgivenbelow:

1. Version:Thisfieldspecifiestheprotocolversion.
2. Type:Thisfieldindicatesmessagesasoneofthefollowing type.

a.Hellob.Database description
c.Linkstatusd.Linkstatusupdatee.Linkstatusacknowledgement.

3. Packetlength:ThisfieldspecifiesthelengthofOSPFpacketinbytes,
4. RouterID: Itidentifiesthesending router.

5. AreaID:NetworkIDofdestinationnetworks.
6. Checksum:Thechecksumfield isusedtodetect errorsinthepacket.
7. Authenticationtype:Itidentifiestheauthenticationtypethatisused.
8. Authentication:Thisfieldincludesavalue from theauthenticationtype.

OSPFAdvantages

1. Lowtraffic overhead.
2. Fastconvergence.
3. Largernetworkmetrics.
4. Areabased topology.
5. Route summaries.
6. Supportforcomplexaddress structures.
7. Authentication.

OSPFDisadvantages

1. Memory overhead.
2. Processoroverhead.
3. ConfigurationOSPFcanbecomplexto configure.

PathVector Routing

Distancevectorandlinkstateroutingarebothintradomainroutingprotocols.Theycanbeused 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 staterouting needs ahuge amount ofresources to calculaterouting tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call path vector routing.

PathVectorRoutingisaroutingalgorithminunicastroutingprotocolofnetworklayer,andit is useful for interdomain routing. The principle of path vector routing issimilar to that of distancevectorrouting. Itassumesthatthereisonenodeineach autonomoussystemthatacts 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
PreventionOfLoop

Policy Routing

Optimum Path**BGP**

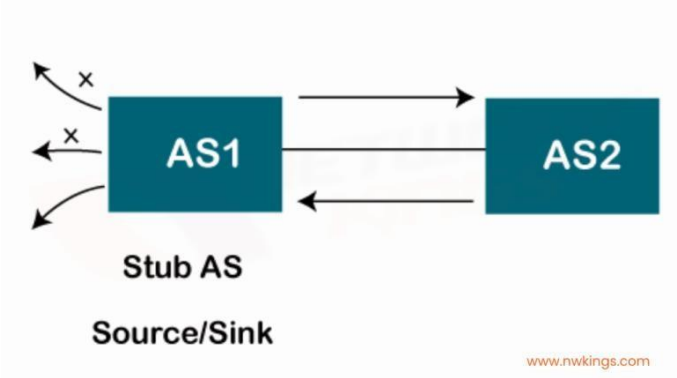
BorderGatewayProtocol(BGP)isusedtoExchangeroutinginformationfortheinternet, used to route traffic from one autonomous system (AS) to another.

DifferentTypesofAutonomous Systems?

SincetheBGPhelpsinroutingbetweendifferentautonomoussystems,itisimportantto learn about different types of autonomous systems:

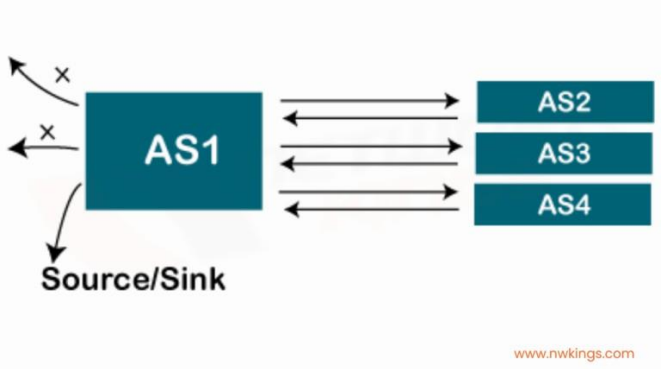
1. StubAS:

- Thereisonlyone connectionto anotherAS intheStub AS.
- Datatrafficcannotpassthroughastubautonomoussystem.
- Thetrafficcan move within an autonomoussystem.
- Astub iseither asourceorasink



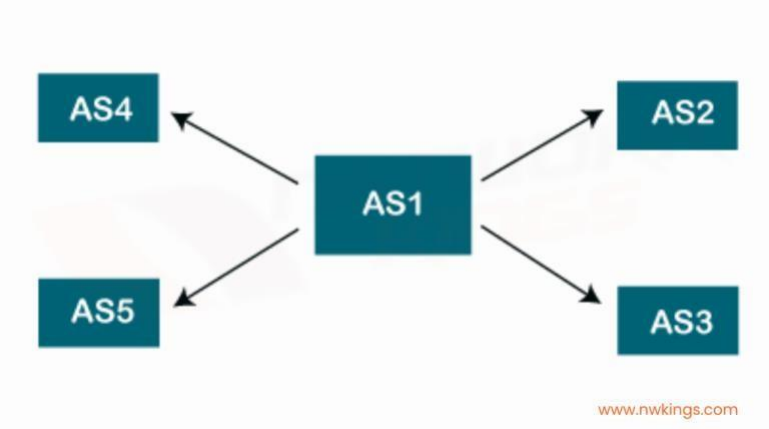
2. Multi-HomedAS:

- Ithasmorethan oneconnection toother Autonomous Systems.
- Still,itisstillonesourceorsinkfordatatraffic.
- Thereisnotransienttraffic.



3. TransitAS:

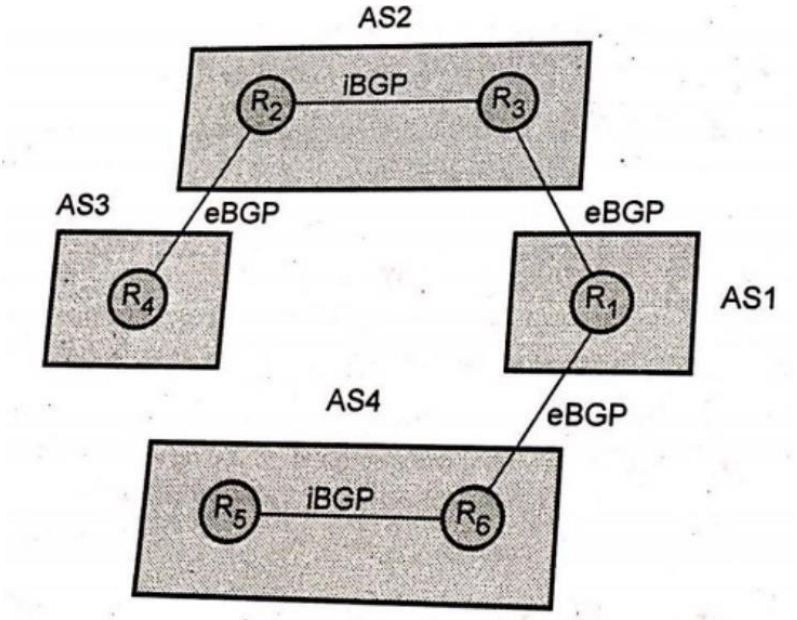
- Itisamulti-homedautonomoussystemthatallowstransit traffic.
- Forexample,ISP(InternetBackbone)isatransitAS.



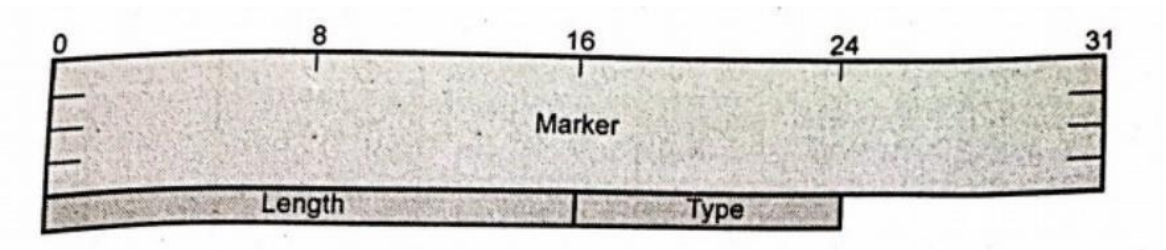
BGPperformsthreefunctionalprocedures

1.Neighbouracquisition2.Neighbourreachability3.Network reachability. Neighbouracquisitionproceduresusedforexchangingtheroutinginformationbetweentwo routers in different Autonomous System (AS).

BGPconnectionsinsideanautonomoussystemarecalledinternalBGP(iBGP)andBGP connectionsbetweendifferentautonomoussystemsarecalledexternalBGP(eBGP).Fig. shows the internal and external BGP



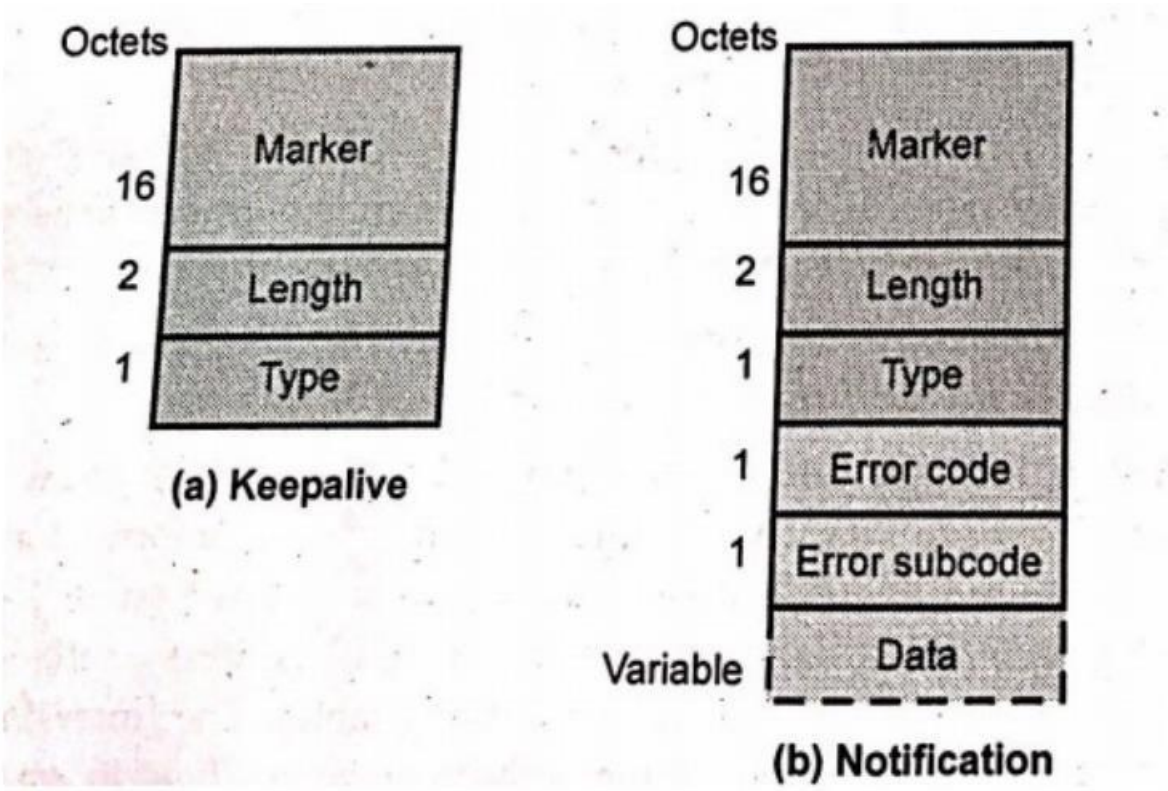
BGPmessages:HeaderoftheallBGPmessages isfixedsizethatidentifiesthemessage type. Fig. shows the BGP message header format

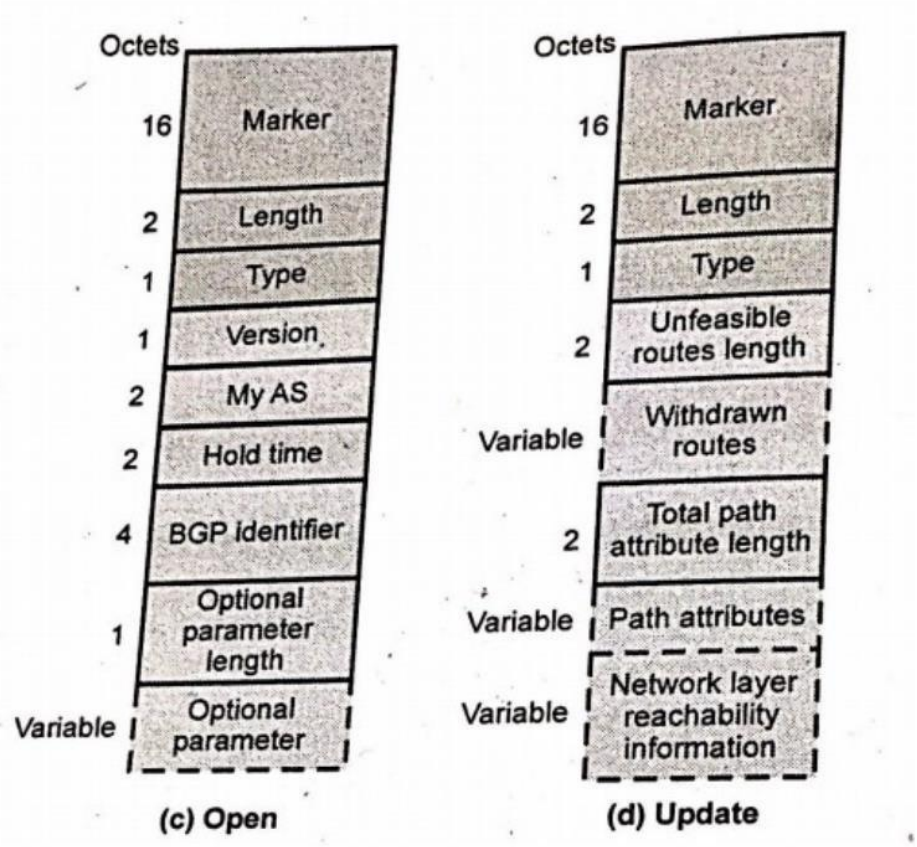


1. Marker:Markerfieldisusedfor authentication.
2. Length:Thisfield indicatesthetotallength ofthemessage.
3. Type:Typefieldindicatestypeofmessage.BGPdefinesfourmessage type.

a)OPENb)UPDATEc)NOTIFICATIONd) KEEPALIVE

FollowingFig.3.11.3showsthefourtypesofBGPmessage formats.





-

AdvantagesofBGP

1. BGPisaveryrobustandscalablerouting protocol.

2. BGPeasilysolvesthecount-to-infinityproblem.

DisadvantagesofBGP
1. BGPiscomplex.
2. BGProutestodestinationnetworks,ratherthantospecifichostsorrouters.

MulticastRouting: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-manyandmany-to-manycommunicationasitallowssenderorsenderstosenddatapackets to multiple receivers at once across LANs or WANs. This process helps in minimizing the data frame of the network

Therearedifferent**MulticastRoutingProtocols**usedformulticstrouting

- **DistanceVectorMulticastRoutingProtocol (DVMRP)**
- **MulticastSourceDiscoveryProtocol (MSDP)**
- **MOSPF(Multicast OSPF)**
- **MulticastBGP**
- **ProtocolIndependentMulticast(PIM)**

DistanceVectorMulticastRoutingProtocol (DVMRP):

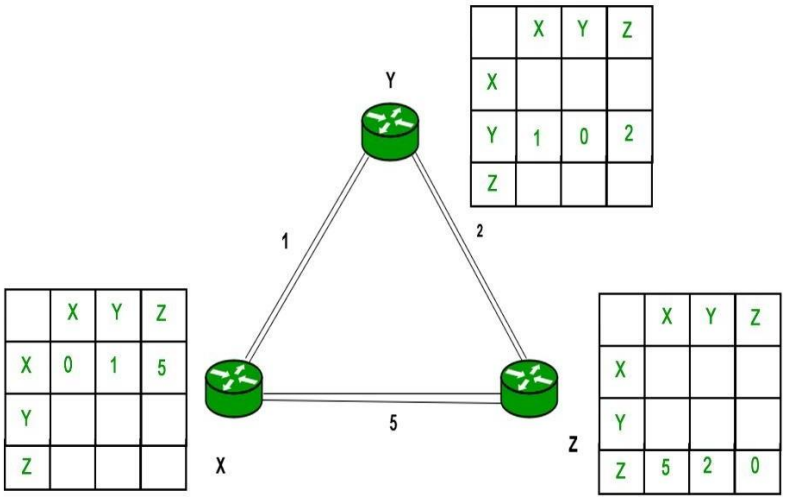
A**distance-vectorrouting(DVR)**protocolrequiresthatarouterinformitsneighborsof topology changes periodically.

1. Aroutertransmitsitsdistancevector toeachof itsneighborsin arouting packet.
2. Eachrouterreceivesandsavesthemostrecentlyreceiveddistancevectorfromeach of its neighbors.
3. Arouterrecalculatesitsdistancevectorwhen:
    - Itreceivesadistancevectorfromaneighborcontainingdifferentinformation than before.
    - Itdiscoversthat alink toaneighbor hasgonedown.

TheDVcalculationisbasedonminimizingthecosttoeachdestination Dx(y) =

Estimate of least cost from x to y
C(x,v)=Nodex knowscostto each neighbor v
Dx=[Dx(y):y∈ N]=Nodexmaintainsdistancevector Node x also
maintains its neighbors' distance vectors
–For eachneighbor v, x maintainsDv=[Dv(y): y ∈N]

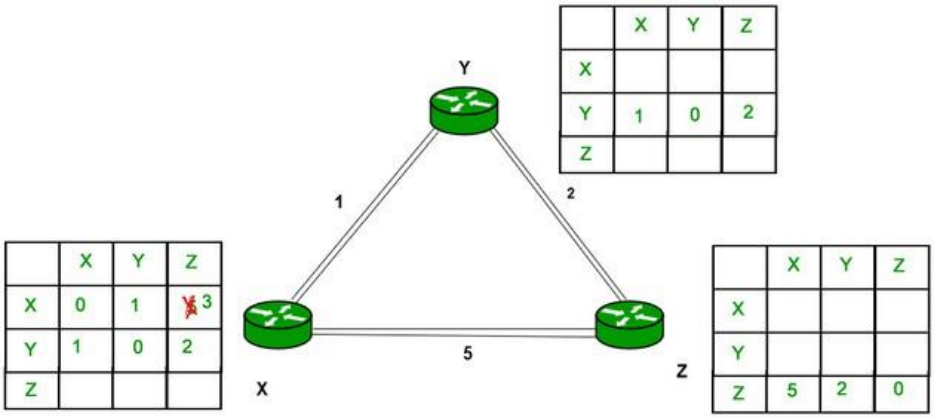
Example–Consider3-routersX,YandZasshowninfigure.Eachrouterhavetheirrouting table. Every routing table will contain distance to the destination nodes.



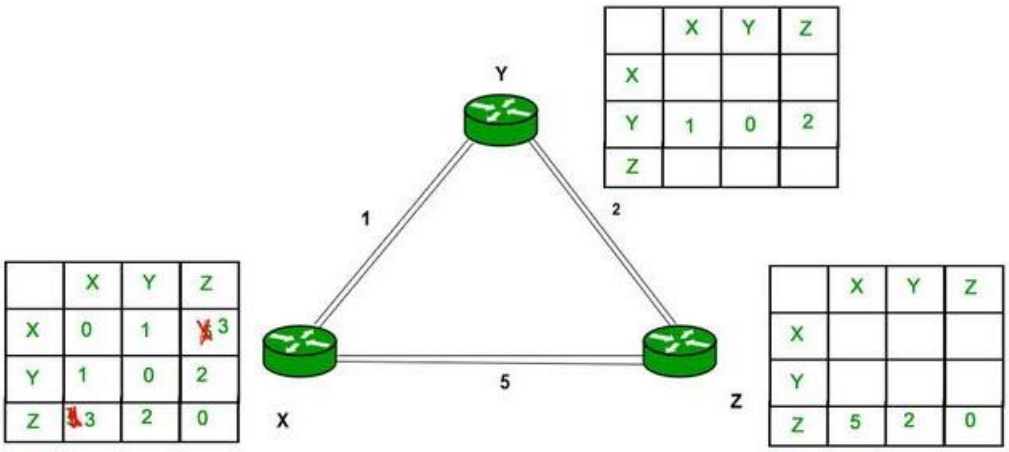
ConsiderrouterX,Xwillshareitroutingtabletoneighborsandneighborswillshareit routing table to it to Xand distancefrom node Xto destination will becalculated using bellmen-ford equation.

Dx(y)=min{ C(x,v)+ Dv(y)}foreachnodey ∈N

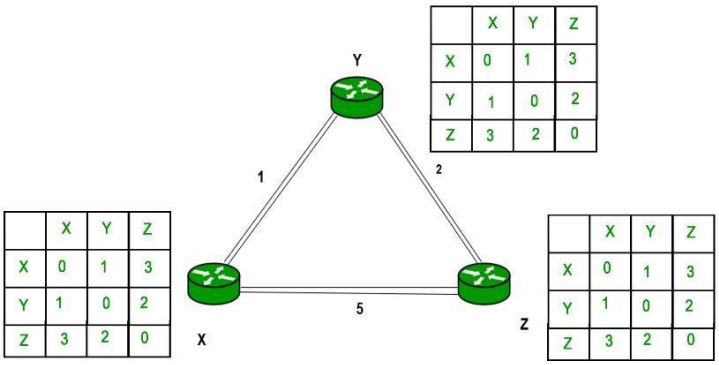
AswecanseethatdistancewillbelessgoingfromXtoZwhenYisintermediatenode(hop) so it will be update in routing table X.



SimilarlyforZalso –



Finallytherouting tableforall–



AdvantagesofDistanceVectorrouting–

- Itissimplertoconfigureandmaintainthanlinkstaterouting.

  DisadvantagesofDistanceVectorrouting –

  - Itisslowertoconvergethanlinkstate.
  - Itisatriskfromthecount-to-infinity problem.

PIM

PIM(ProtocolIndependentMulticast)isamulticastroutingprotocol,thatisusedtosend traffic from a single source to multiple destinations across a network.

PIMisacollectionofthreeprotocols -PIMSparseMode,PIMDenseModeandPIMBi- directional .PIM is termed protocol-independent because PIM does not include its own

topologydiscoverymechanism,butinsteadusesroutinginformationsuppliedbyother routing protocols

PIMSparseMode

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.Inotherwords,itisassumedthatmostsubnetsinthenetworkwillnotwantanygiven multicast packet. In order to receive multicast data, routers must explicitly tell their upstream neighborsabouttheirinterestinparticulargroupsandsources.RoutersusePIMJoinandPrune messages to join and leave multicast distribution trees.

PIMDenseMode

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 thenetworkwillwantanygivenmulticastpacket.Multicastdataisinitiallysenttoallhostsin the network. Routers that do not have any interested hosts then send PIM Prune messages to remove themselves from the tree.

Bi-directionalPIM

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 themethod used to send datafromasourceto theRP. Whereas in PIM-SM data is sent using either encapsulation or a source-based tree, in BIDIR-PIMthedataflowstotheRPalongthesharedtree,whichisbi-directional-dataflowsinboth directions along any given branch.

UNIT-V

Data link and physical layers

Data link layer:

* The data link layer include well defined service interface to the network layer, framing, flow control, error detection and error control frame formatting and sequencing.
* The primary responsibility of data link layer is to provide services to the network layer.
* The principle service is transferring data from the network layer on the source machine to the network layer on the destination machine.
* The two data link layer communicates with each other by data link control protocol.
* The important services provided by data link layer to network layer are,

i) Unacknowledged connectionless service
ii) Acknowledged connectionless service
iii) Acknowledged connection-oriented service

Framing:

* Framing in the data link layer separates a message from one source to a destination or from other messages to other destinations by adding a sender address and a destination address.
* To service the network layer, data link layer uses the service provided to it by the physical layer.
* physical layer accepts the raw bit stream and delivers it to destination. This bit stream may contain error ie number of bits received may not be equal to number of bits transmitted.
* The data link layer breaks the stream into discrete frames and computes the checksum for each frame.
* At the destination the checksum is recomputed.
* The breaking of bit stream by inserting spaces or time gaps is called framing.

Fixed-size framing:

Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining the boundaries of the frames,

the size itself can be used as a delimiter. 191

Eg: ATM

1) Variable size Framing:

In Variable size framing, end of the frame and the beginning of the next frame is defined.

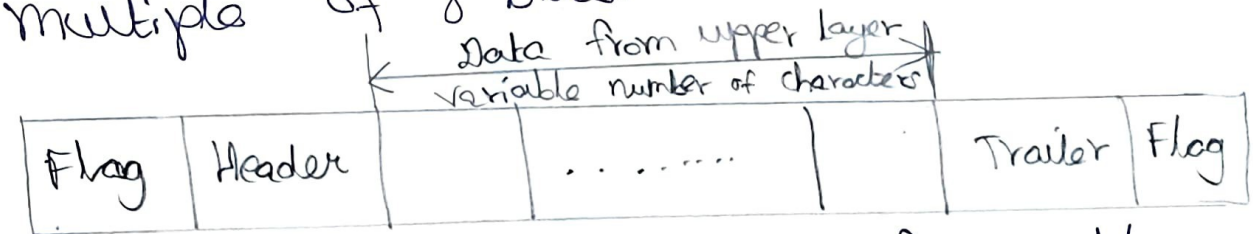
Two methods are used for this purposes:

i) Character oriented protocol:

* In this type, data to be carried are 8-bit characters from a coding system such as ASCII.

* Header contains source and destination address and other control information are also multiple of 8 bits.

* Trailer contains error detection or error correction redundant bits are also multiple of 8 bits.



* To separate one frame from the next, 8-bit flag is added at the beginning and the end of a frame.

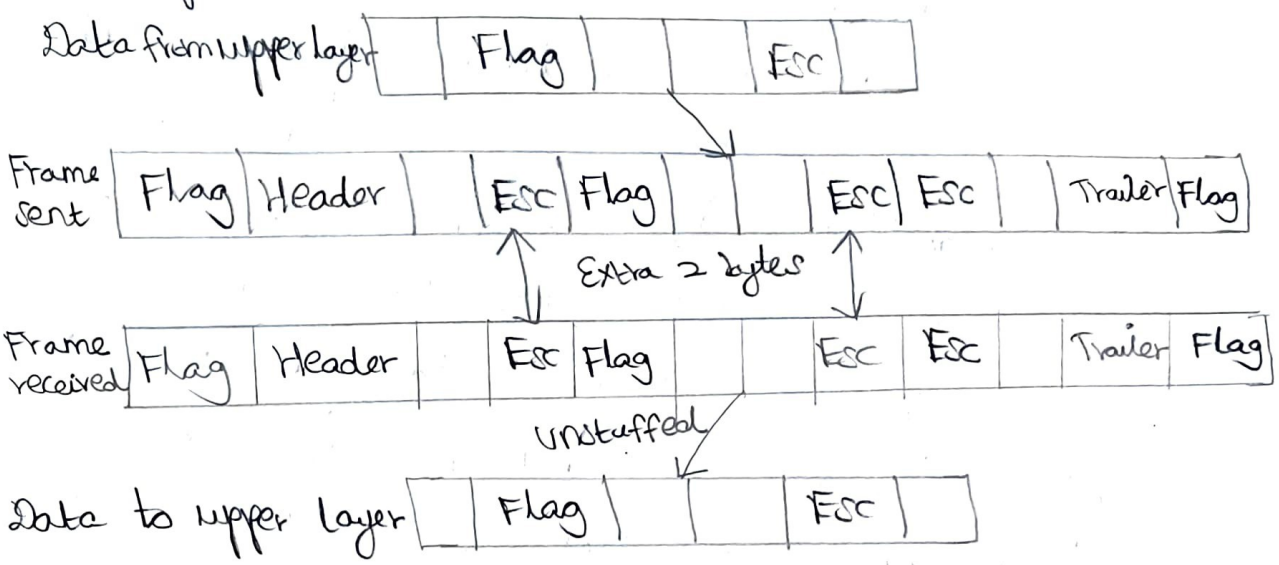
* The flag consists of protocol dependent special characters, signals the start or end of a frame.
* It is suitable only for text data transmission. The flag could be selected to be any character not used for text communication.
* When send other types of information such as graphs, audio and video, the flag could also be part of the information. So it creates problem for receiver.
* When receiver encounters this pattern in the middle of the data, it has reached the end of the frame.

To solve this problem, byte stuffing was used.

i) Byte stuffing:

A special byte is added to the data section of the frame. When there is a character with the same pattern as flag. The data section is stuffed with an extra byte.

This byte is usually called the Escape character (Esc) has a predefined bit pattern.



* Whenever the receiver encounters the Esc character, it removes it from the data section and treats the next character as data, not a delimiting flag.
* If the escape character is part of the text an extra one is added to show that the second one is part of the text.

Flow Control:

* When the sender is running on fast machine or lightly loaded machine and receiver is on slow or heavily

loaded machine. Then the transmitter will transmit frames faster than the receiver can accept them.

* Even if the transmission is error free at a certain point the receiver will simply not be able to handle the frames as they arrive and will start to lose some.
* To prevent this, flow control mechanism is incorporated which includes a feedback mechanism requesting transmitter a retransmission of incorrect message block.
* The most common retransmission technique is known as Automatic-Repeat-Request
* Error control in Data Link layer is based on Automatic Repeat Request ie transmission of data in three cases.
  i) Damaged frames
  ii) Lost frames
  iii) Lost acknowledgements

Flow control:

* To ensure the proper sequencing and safe delivery of frames at the destination, an acknowledgement should be sent by the destination network.
* The receiver sends back special control frames bearing positive or negative acknowledgements about the incoming frames.
* If the sender receives a positive acknowledgement it means the frame has arrived safely.
* If the negative acknowledgement arrives means, something has gone wrong and frame is to be retransmitted.
* A timer at sender's and receiver's end is introduced.
* Also sequence numbers to the outgoing frames are maintained so that the receiver can distinguish retransmissions from originals.
* It is one of the most important part of data link layer duties.

Data-link layer protocols - HDLC:

* HDLC stands for High level Datalink Control.
* It is the most important data link protocol.
* It is an international standard that has been defined by Iso for point-to-point and multipoint data links.
* HDLC defines 3 types of stations.

They are,

i) Primary Station:

It has the responsibility for controlling the operation of the link. Frames issued by primary are called Command.

ii) Secondary Station:

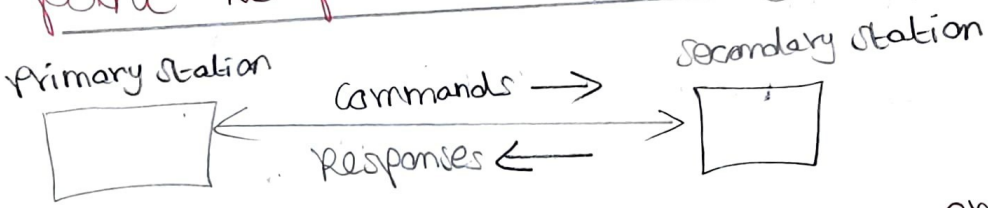
It operates under the control of the primary station. Frames issued by a secondary are called responses. The primary maintains separate logical links with each secondary station of line.

iii) Combined Station:

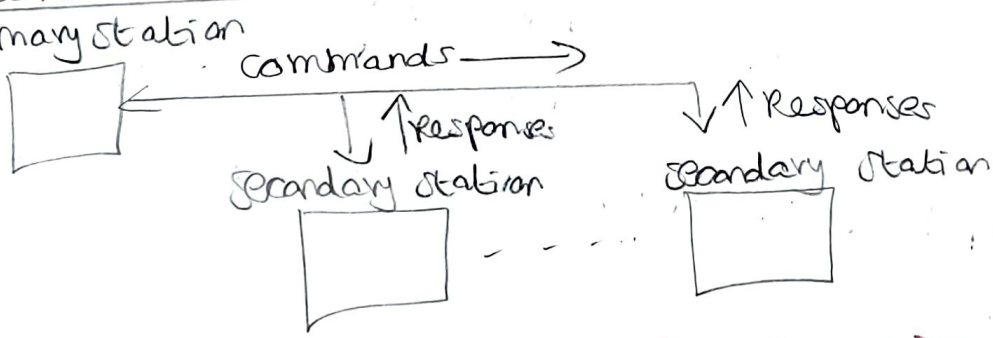
It combines the features of primary and secondary. A combined station may issue both commands and responses.

* The stations can be configured in different network configuration as,

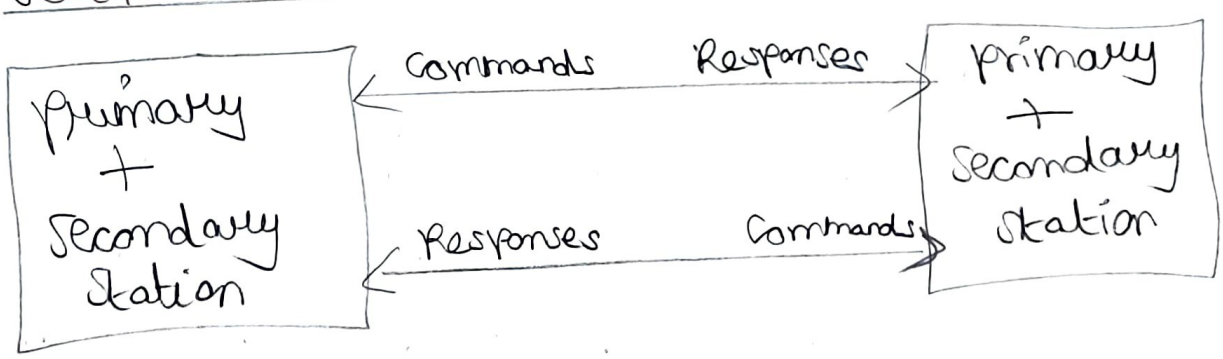
i) point-to-point with single primary & secondary



ii) Multipoint with single primary and multiple secondaries:



iii) point-to-point with 2 primaries and 2 secondaries:



* The frames sent by primary Station to the secondary Station are known as Commands and those from secondary to primary are known as responses.

* Two configuration in part (i) and (ii) have a single primary station are known as unbalanced configurations. It supports both full duplex and half duplex transmission.

* The configuration in part (iii) has two primary stations is known as balanced configuration. It supports both full duplex and half duplex transmission. Since each station has both primary and secondary are known as combined stations.

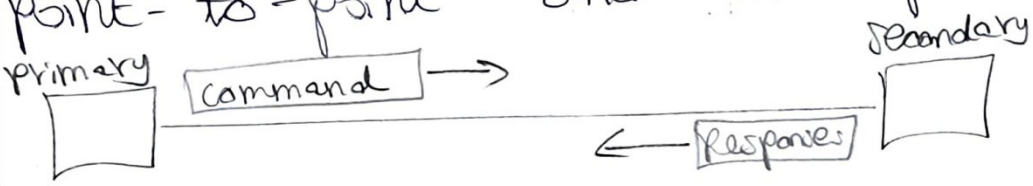
1) Operational Mode of HDLC:

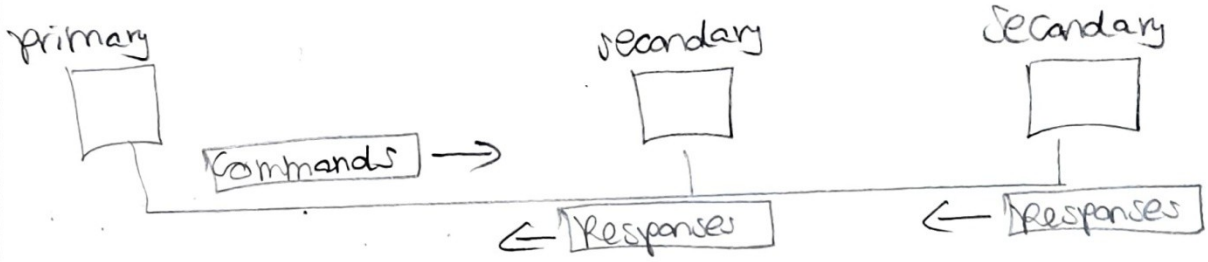
HDLC has following data transfer modes:

i) Normal Response Mode (NRM):

It is used in unbalanced configurations. There are one primary

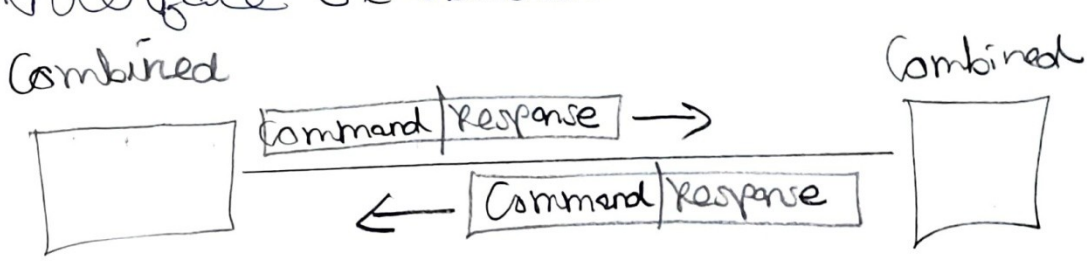
Station and multiple Secondary Stations. A primary Station can send Commands, a Secondary Station can only respond. It is used for both point-to-point and multipoint links.





ii) Asynchronous Balanced Mode (ABM):

In ABM, the configuration is balanced. The link is point to point and each station can function as primary and secondary. Either station can send data, control information or commands. It is typical in connection between two computers and X.25 interface standard.



2) Frames:

In HDLC, both data and control messages are carried in a standard format frame. Three classes of frame are used in HDLC.

i) Unnumbered frames (U-frames):

Its used for functions such as link setup and disconnection. It do not contain any acknowledgment information is contained in sequence numbers.

Flag	Addres	Control	Management Information	FCS	Flag

ii) Information frames (I-frames):

It carry the actual information or data and normally referred as I-frames. It can be used to piggy back acknowledgement information relating to the flow of I-frames in reverse direction

Flag	Addres	Ctrl	user information	Fcs	Flag

iii) Supervisory frames (S-frames):

It is used for error and flow control and contain send and receive sequence numbers.

Flag	Address	Control	FCS	Flag

* The flag, address and control bits before the information or data fields are known as a header.
* The Fcs and flag fields following the data fields are referred as a trailer.

Flag field:
It has a unique pattern at both the ends of the frame structure. It identifies the start and end of frame. The length of flag field is 8-bit.

Address field:
It states the destination address. It is usually 8 bit long but can be extended.

Control field:
It contain frame numbers. It controls the acknowledgment of frames. It is 8 or 16 bits in length.

Information field:
Data field contains the user data received from the network layer. It can be of variable length

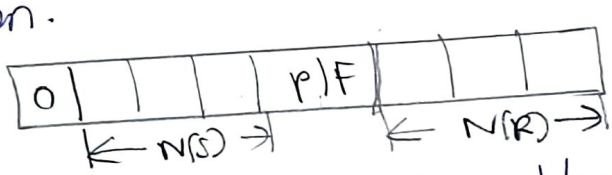
Frame check sequence (FCS):

It is an error detecting code calculated from the remaining bits of frame. It can be 16 or 32 bits long.

3) Control Field:

i) Control field for I-frames:

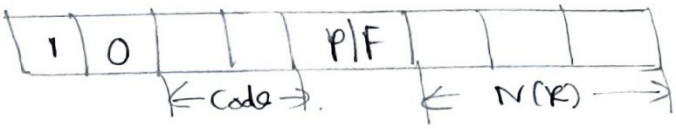
* It is designed to carry user data from the network layer. It also include flow and error control information.



* The first bit defines the type. If it is 0, the frame is an I-frame. Next 3 bit defines the sequence number (N(S)). Its range is 0 to 7.
* P/F field is 1 bit with dual purpose. It is set when it is 1. It may be poll or Final
* Last 3 bit corresponds to acknowledgement number when piggy backing is used.

ii) Control field for S-frames:

S-frames do not have information fields.



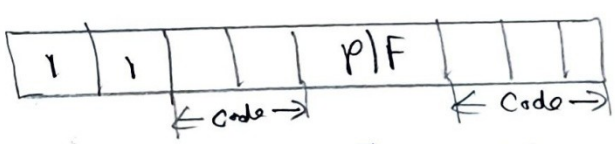
* If the first 2 bits of control field is 10 means the frame is S-frame.
* The last 3 bits called N(R) corresponds to acknowledgment number (Ack) or negative acknowledgment number (NAk) depending on type of S-frame

Types of S-frames are:

i) Receive Ready (RR)
ii) Receive Not Ready (RNR)
iii) Reject (REJ)
iv) Selective Reject (SREJ)

iii) Control field for U-frames:

It contain an information field, but one used for system management information, not user data.



Its divided into 2 sections 2-bit prefix before P/F and 3-bit suffix after P/F bit.

Point-to-point protocol:

It is the most commonly used protocol for point-to-point transfer of data. The services provided by ppp are,

i) Formatting of frames to transfer
ii) Negotiation between devices to establish link
iii) Encapsulation of data in data link frame
iv) Authentication of devices

* It can operate between point-to-point transmission link in full duplex mode.
* It can be used as a data link control to connect two routers.

i) Frame Control:

It is similar to HDLC. It has 7 fields.

	Flag	Address	Control	Protocol	Data or Padding	FCS	Flag
No of bytes	1 byte	1 byte	1 byte	1/2 byte	variable	1/2	1 byte

i) flag field:

It identifies the boundaries of ppp frame ie each frame begins and ends with flag field.

ii) Address Field:
It indicates the address of destination.

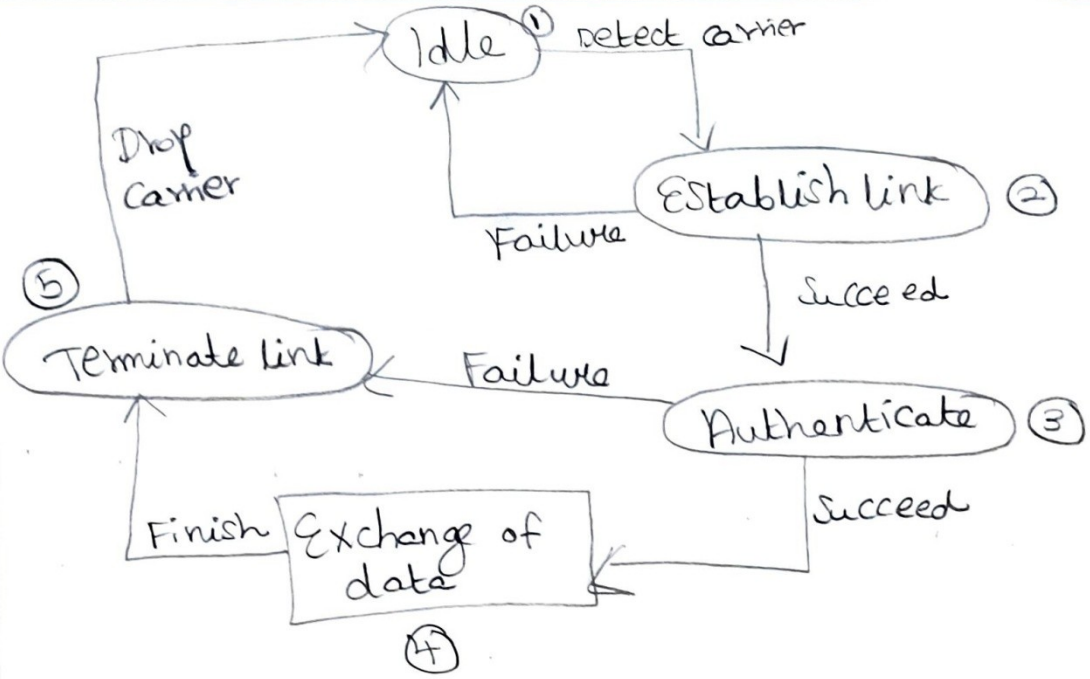
iii) Control Field:
It normally runs in connectionless mode. It indicates unnumbered frames ie frame does not contain sequence numbers and there is no flow or error control

iv) protocol Field:
It defines the information of data field.

v) Data field:
It contains the actual data to transmit. The length of this field is variable.

vi) Frame check sequence (FCS):
It is 2 byte long and contains CRC code. It checks length of all fields in frame.

2) Transition States:
It is used to indicate the phases through which ppp connection passes. The ppp connection passes through five important states.



i) Idle State:

In the idle State the link is not in use. The carrier is not activated in this State.

ii) Link Establishing State:

When carrier is detected, one of the end points starts the transmission then connection enters into link establishing State. There is negotiation between devices.

iii) Authenticate State:

It is mutually decided by the Stations. The stations sent several authentication packets.

iv) Exchange of data State:

This State is also referred as networking State. In this State exchange of data started. The connection is terminated

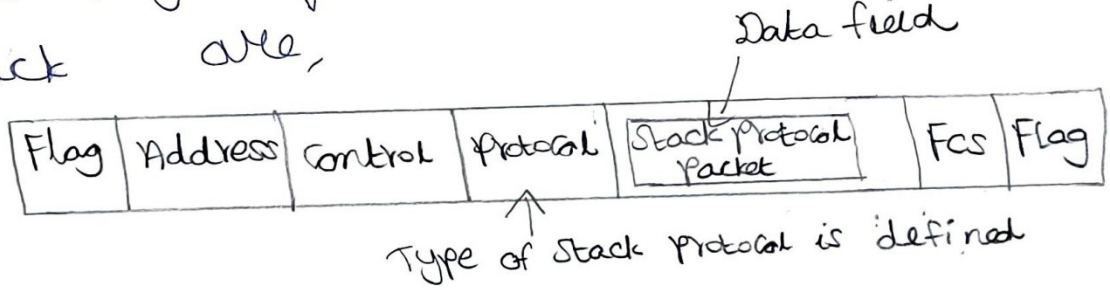
only after any of end points wants to terminate.

v) Terminate link State:

After data exchange is over several packets are exchanged between and points for closing the link.

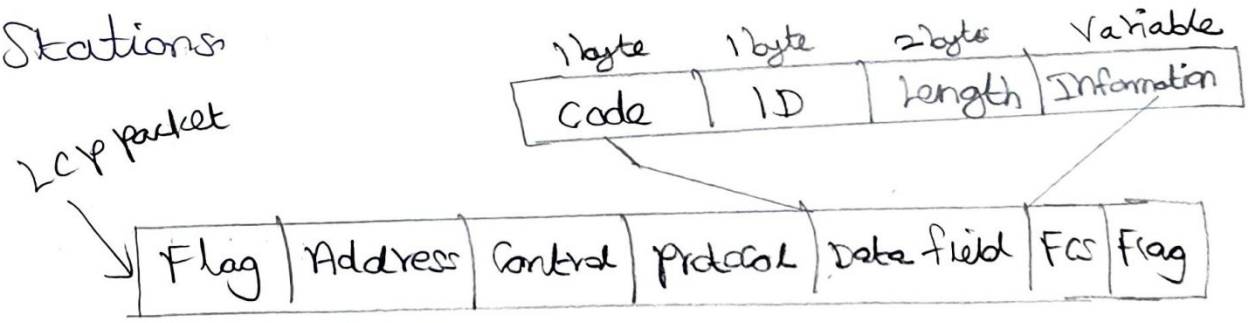
3) ppp Stack:

It uses a stack of other protocols for establishing link & authentications. Two major protocols are used in ppp Stack are,



i) Link Control protocol (LCP):

It perform the function of establishing, maintaining, configuring and termination of links. It also involves in negotiating mechanism between stations



a) Code field:
It defines the type of Lcp packet. There are 3 types of Lcp packets - Configuration packet, link termination & link monitoring packets.

b) ID:
It is used to match the request packet with its reply packet. It inserts a value in this field is copied in corresponding field in reply packet.

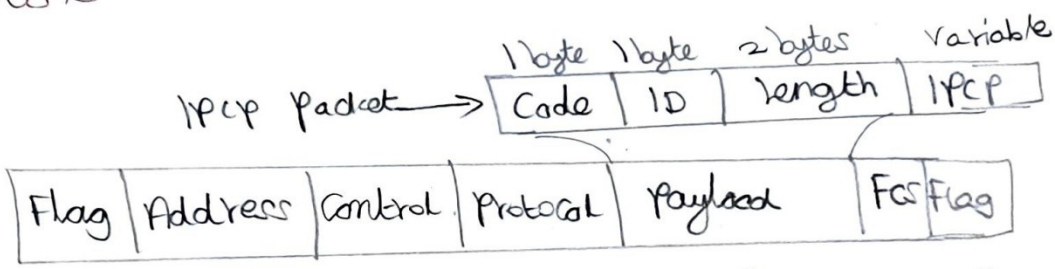
c) length:
It defines the entire length of Lcp packet.

d) Information:
It is a variable length field.

ii) Network Control protocol (NCP):
It uses when it enters in exchange of data state. It is a set of protocols allows encapsulation of data from network layer into ppp frame.

* It extends the negotiation not only in data link layer but in network layer also.

The set of packets that establish and terminate a network layer connection for IP packets is called Internetwork Protocol Control protocol (IPCP).



The protocol field value for IPCP packet is $(8021)_H$. There exists 7 types of IPCP packets each having unique code value.

Media Access Control:

* One feature of LAN is that its backbone is a shared channel or transmission link provides all user to access the transmission facilities.
* It may be possible that two or more stations transmitting simultaneously causing their signals to interfere and becomes garbled.
* The asynchronous TDM Mechanism is further divided into contention methods

(random access) and deterministic methods (controlled methods).

Random access techniques are

i) ALOHA
ii) Carrier Sense Multiple-Access (CSMA)
iii) CSMA with Collision-Detection (CSMA/CD)
iv) Register insertion

Controlled access to LAN can be performed in two types.

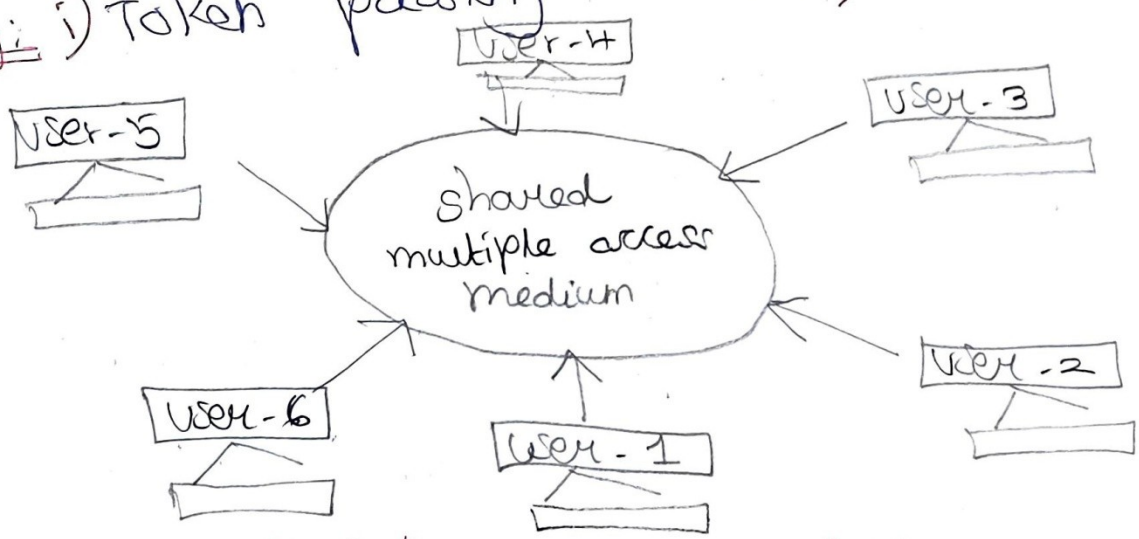
1) Centralized Technique:

Master node decides which node is to access the channel at any one time. Eg: polling

2) Distributed Technique:

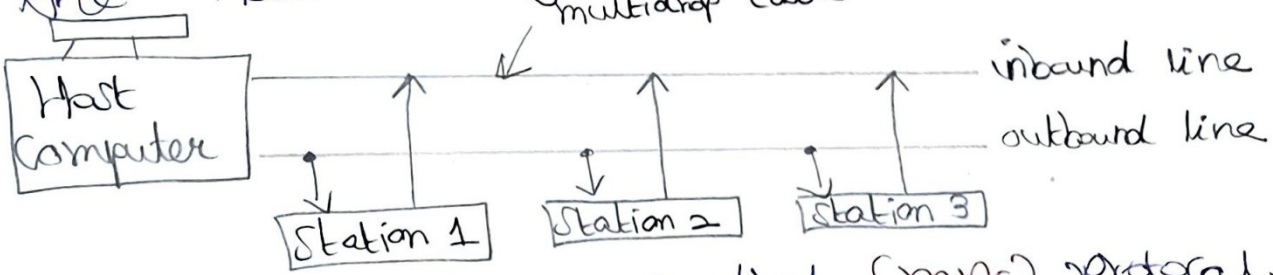
Each station is given an opportunity to transmit on the channel.

Eg: i) Token passing method ii) Slotted ring method



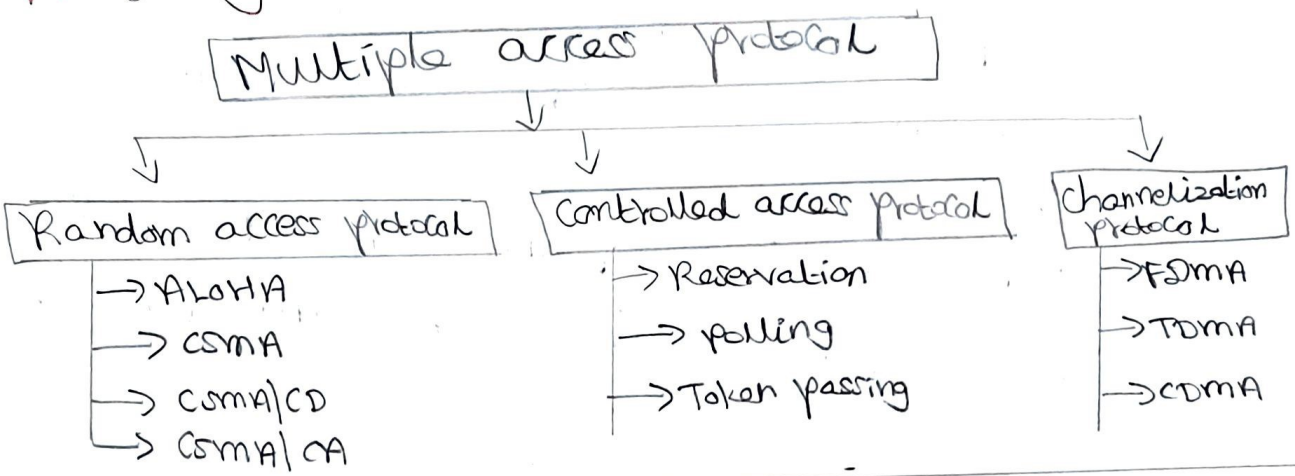
Multiple access communication

* The sharing techniques are used in wired communications and networks based on radio communication.
* In wired communication multidrop cables are used in data networks to connected number of stations to a host computer.
* The host computer broadcasts information to the user on the outbound line.
* The stations transmit information to the host using the inbound line.



* A medium access control (MAC) protocol is developed for this system. Hence the host computer issues polling messages to each stations providing it with permission to transmit on the inbound line.
* In radio communication several stations share two frequency bands one for transmitting and one for receiving.

* In Satellite Communication each Station is assigned a channel in an uplink frequency band uses to transmit to the satellite. The satellite sends back the signals on different frequency band called down link frequency band.



Ethernet Basics - CSMA/CD:

Generations of Ethernet

i) Standard Ethernet (10 Mbps)
ii) Fast Ethernet (100 Mbps)
iii) Gigabit Ethernet (1 Gbps)
iv) Ten-Gigabit Ethernet (10 Gbps)

1) MAC sublayer Frame Format:

* MAC Sublayer frames data received from the upper layer and passes them to the physical layer.
* Ethernet does not provide any mechanism

for acknowledging received frames, making it is known as an unreliable medium.

Preamble 7 bytes	SFD 1 byte	Destination address 6 bytes	Source address 6 bytes	Length or Type 2 bytes	Data & Padding	CRC 4 bytes

802.3 frame format

i) preamble:
A 7-byte pattern of alternating 0s and 1s is is used by receiver to establish bit synchronization. Each frame contains bit pattern 10101010. It provides only an alert and a timing pulse.

ii) Start Frame Delimiter (SFD):
The sequence 10101011 indicates the actual start of the frame and enables the receiver to locate the first bit of the rest of the frame.

iii) Destination Address (DA):
It specifies the station for which frame is intended. It may be a unique physical address, a group address or a global address.

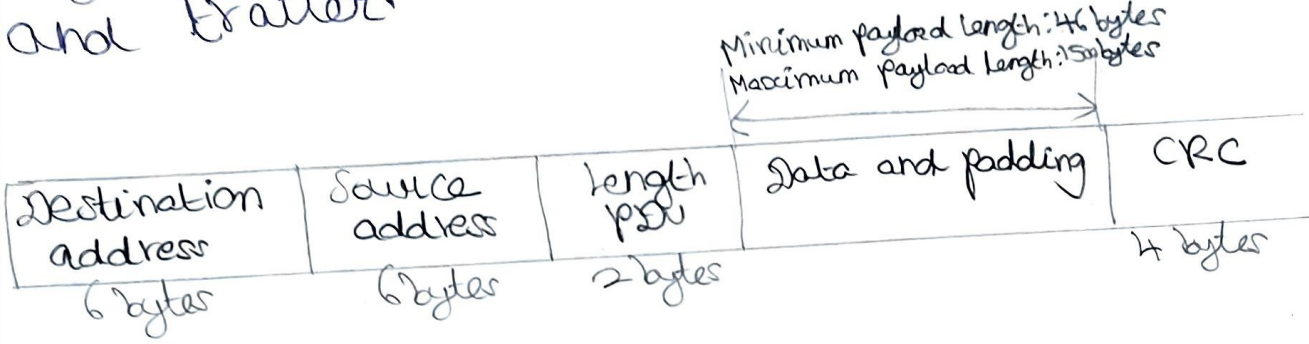
iv) Source Address (SA):
It contains the physical address of the sender of the packet.

v) Length or Type:
It depend on whether the frame conforms to IEEE 802.3 standard or earlier.

vi) Data:
Data unit supplied by LLC.

vii) CRC:
It contains error detection information

2) Frame Length:
An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. part of this length is header and trailer.



Access method: CSMA/CD
Standard Ethernet uses 1-persistent CSMA/CD

Slot time = Round trip time + Time required to send jam sequence

Maximum length = propagation speed x $\frac{\text{Slot time}}{2}$

3) Ethernet Specifications:
CSMA/CD offers various options in terms of transmission medium, signaling technique, data rate and maximum electrical cable segment length.

i) 10BASE 5:

It is popularly called as thick ethernet. It operates at 10Mbps uses baseband signaling. The length of network can be extended using repeaters.

ii) 10BASE 2:

It is popularly called as cheapernet (or) thin ethernet. It uses thin coaxial cable.

iii) 1BASE 5:

It is also known as Star LAN. It specifies operation at 1 Mbps using a passive star topology.

iv) 10BASE T:

It is a 10 MHz ethernet running over UTP cable. It also uses passive star topology. The maximum cable segment allowed is 100-150 metres.

v) 10 BROAD 36:

It is a 10 Mbps broadband option. It provides support to more stations over greater distance than baseband versions.

vi) 10 BASE F:

It is 10Mbps running over fibre optic cabling. It depends on signaling

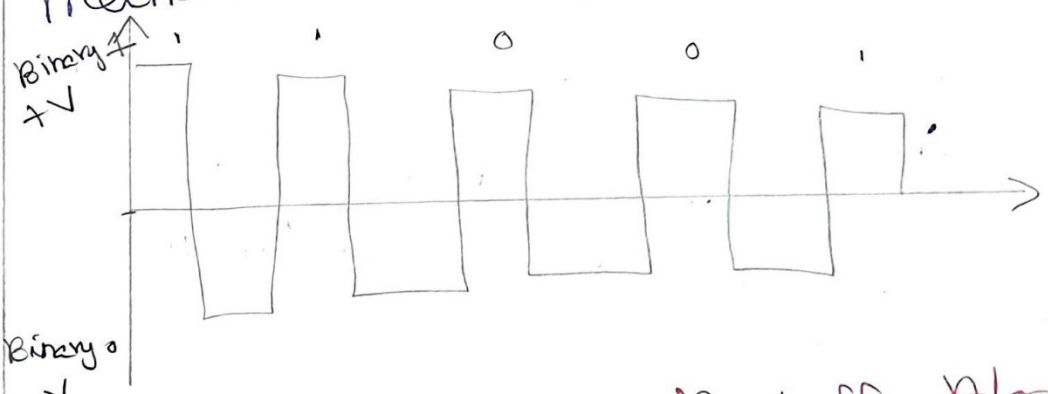
technology and medium used but 216 can go upto 2km unrepeated segment.

4) Manchester Encoding::

* In order to transport digital bits of data across carrier waves, encoding techniques developed with their own merits and demerits.

* Digital signal is a sequence of discrete, discontinuous voltage pulses. Data is represented in binary.

* It is called self clocking encoding method.



5) Binary Exponential Backoff Algorithm::

After a collision, time is divided into discrete slots whose length is equal to worst-case round-trip propagation time on either (2τ)

After first Collision::

Each station uses either 0 or 1 slot

tries before trying again. If 2 217
Station collide and each one pick the same random number, they will collide again.

After second collision:

Each one picks either 0 or 1 or 2 or 3 at random and waits number of slot times.

After third collision:

If a third collision occurs, then next the number of slots to wait is chosen at random from the interval 0 to 2^3-1.

After i^{th} collision:

A random number between 0 and 2^e-1 is chosen and number of slots is skipped.

This algorithm called binary exponential backoff was chosen to dynamically adapt to number of stations trying to send

6) Ethernet performance:

$$\text{Channel Efficiency} = \frac{P}{P + 2\tau/A} \longrightarrow (1)$$

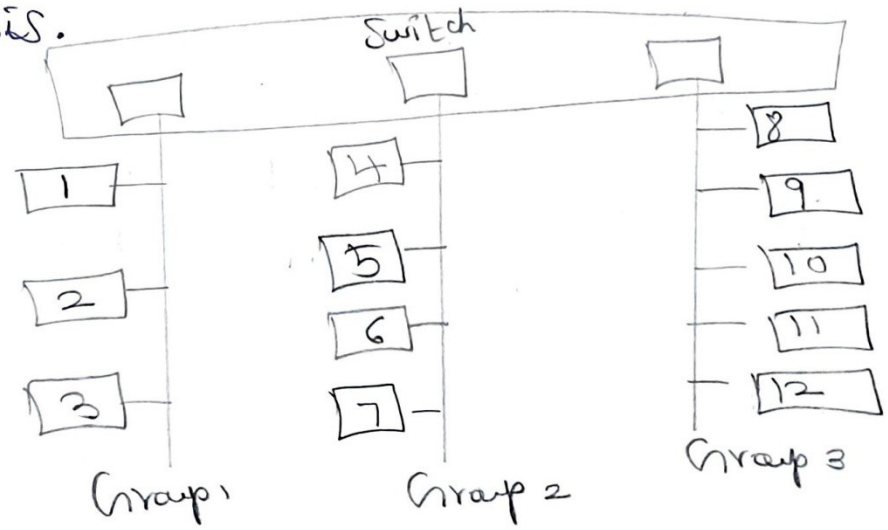
With $p = F/B$ then

$$\text{channel efficiency} = \frac{1}{1 + 2BLe/cf} \longrightarrow (2)$$

B → Bandwidth, L → Cable length, e → Signal propagation, f → Frame length

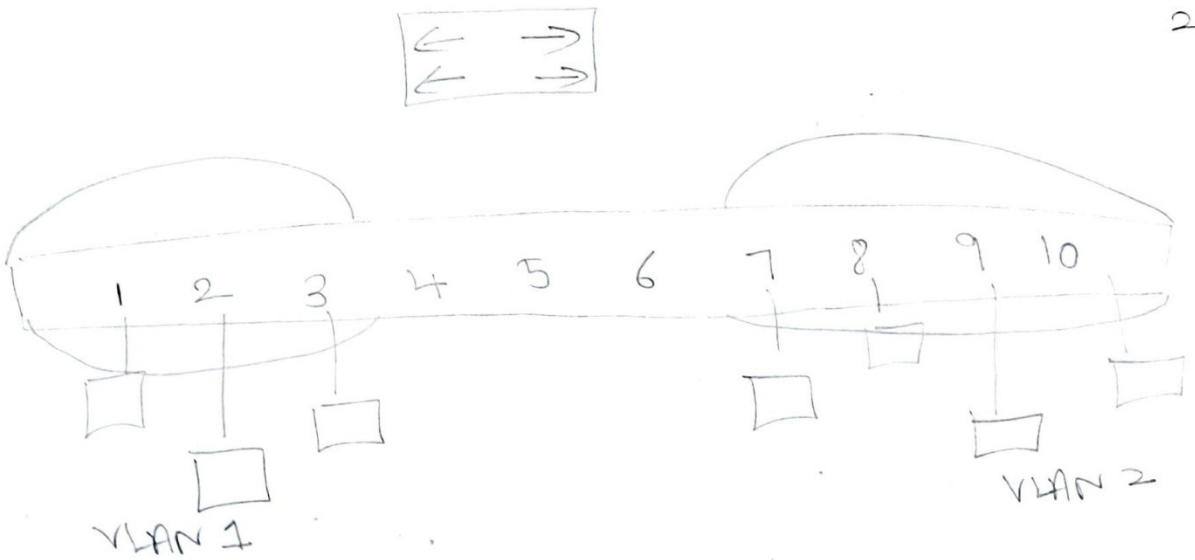
Virtual LAN:

* Virtual local area network define as a local area network configured by software not by physical wiring.
* A VLAN is a switched network is logically segmented on organizational basis.



1) Membership:

Following characteristic (parameters) are used for grouping the nodes in a VLAN.



i) port numbers:

Nodes connecting to switch ports 1,2,3,4 are VLAN 1 nodes Connecting to port 6,7,8,9,10 belongs to VLAN 2

ii) MAC Addresses:

Each computer is based on MAC address of the computer. Some VLAN vendors use 48-bit MAC address as a membership characteristic.

iii) Ip Addresses:

Some VLAN vendors use 32bit Ip address as a membership characteristic.

iv) multicast Ip Addresses:

Multicasting at Ip layer is now translated to multicasting at the data link layer.

2) VLAN Configuration:

Stations are configured in following ways.

i) Manual Configuration:

The network administrator uses VLAN software to manually assign the stations into different VLANs at setup. It is a logical configuration.

ii) Automatic Configuration:

The stations are automatically connected or disconnected from a VLAN using criteria defined by the administrator

iii) Semiautomatic Configuration:

It is between a manual configuration and an automatic configuration. The initializing is done manually with migrations done automatically.

3) Communication between Switches:

Each switch not only which station belongs to VLAN but also the membership of stations connected to other switches. Three methods have been devised for this purpose.

i) Table Maintenance:

When a Station sends a broadcast frame to its group members, the Switch creates an entry in a table and records Station membership.

ii) Frame Tagging:

When a frame is traveling between switches, an extra header is added to MAC frame to define the destination VLAN

iii) TDM:

The connection between switches is divided into timeshared channels.

iv) IEEE Standard:

* The IEEE 802.1 subcommittee passed a Standard called 802.1Q defines the format for frame tagging.

* The Standard defines the format to be used in multiswitched backbones and enables the use of multivendor equipment in VLANs.

Wireless LAN (802.11)

Wireless networks have many applications. IEEE 802.11 protocol supports both the types of Configuration.

1) IEEE 802.11x:

* 802.11 refer to family of specifications developed by IEEE for wireless LAN technology.

* There are 3 specifications in the family: 802.11, 802.11a and 802.11b. All three specifications use CSMA/CD as the path sharing protocol.

i) 802.11:

It is wireless LAN and provides 1 Mbps or 2 Mbps transmission in 2.4 GHz. It uses Frequency Hopping spread spectrum (FHSS) or Direct Sequence spread spectrum (DSSS)

ii) 802.11a:

It provides upto 54 Mbps in 5 GHz band. It uses orthogonal frequency division multiplexing encoding scheme.

iii) 802.11b:

It also refers to Wi-Fi. It provides 11 Mbps transmission in 2.4 GHz band. It uses only DSSS.

* 802.11 LAN is based on cellular architecture. The system is subdivided into cell. Each cell is controlled by a base station. Cell is called as Basic Service set (BSS)

and Base Station is Access point (AP). 2-3

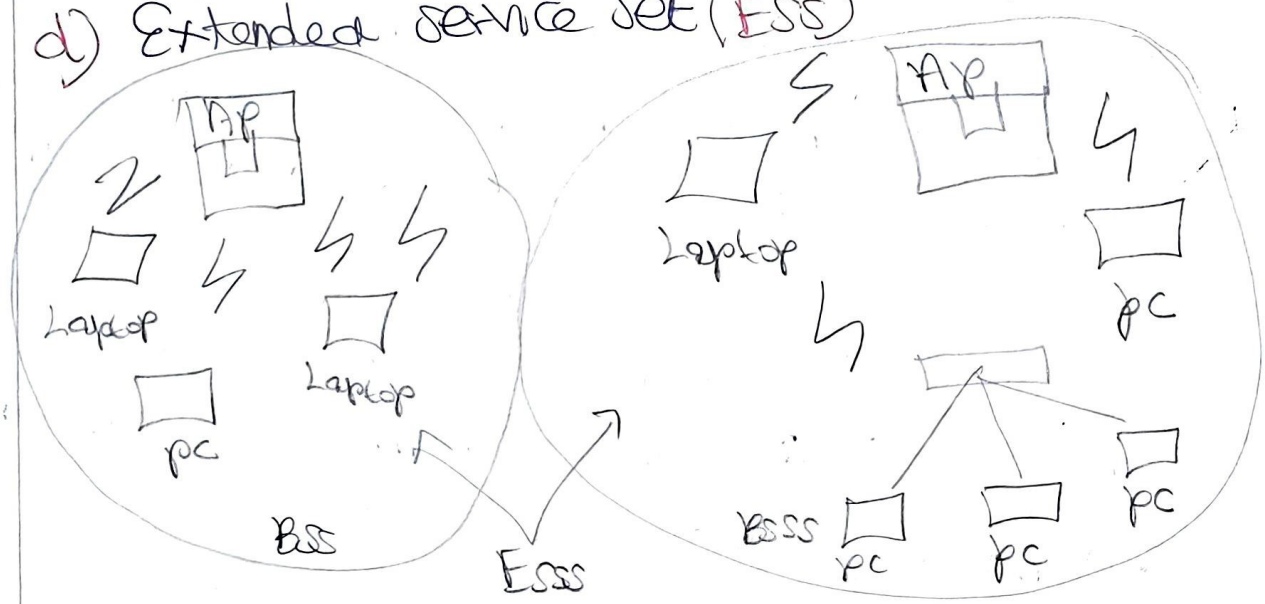
IEEE 802.11 architecture consists of

a) Distribution System (DS)

b) Access point (AP)

c) Basic Service Set (BSS)

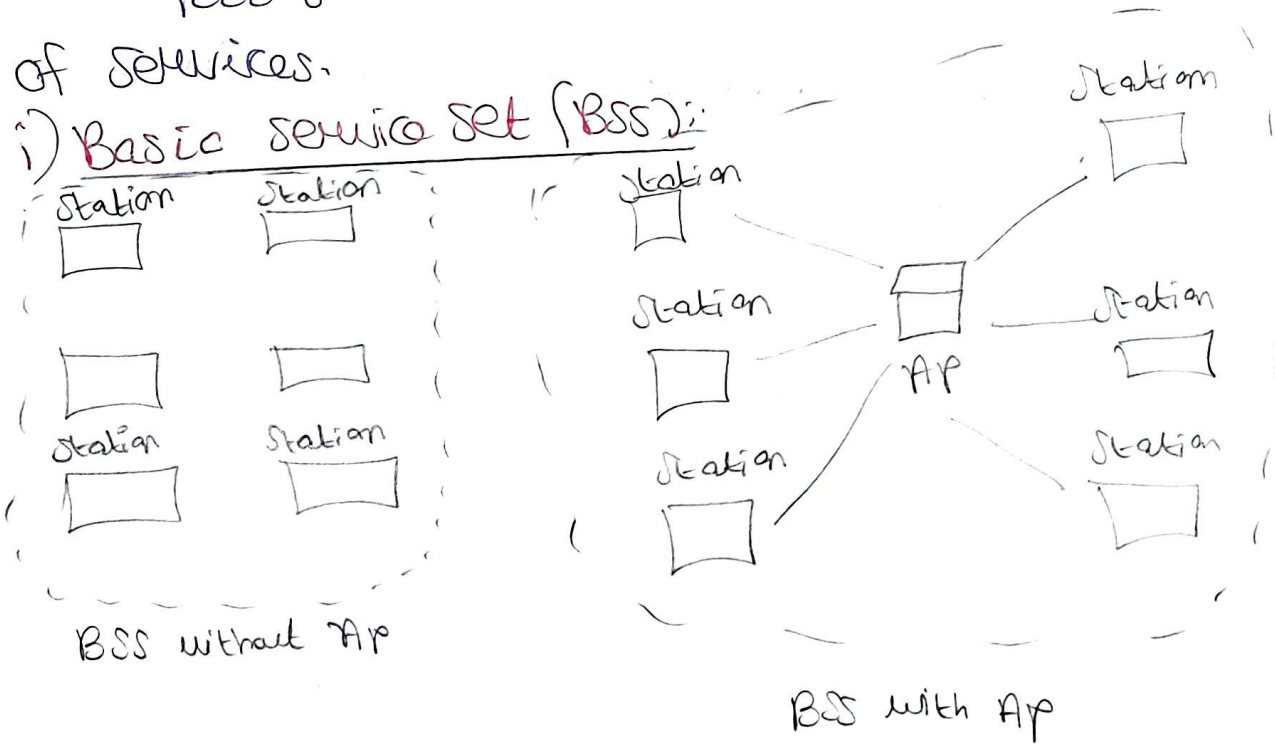
d) Extended service set (ESS)



2) Architecture:

IEEE 802.11 standard defines two types of services.

i) Basic service set (BSS):



* BSS is the building block of IEEE 802.11 architecture.

* BSS is defined as a group of stations that co-ordinates their access to the medium under medium access control.

* Each BSS has an access point and provides access to distributed system.

* BSS without an AP is a stand-alone network and cannot send data to other BSS.

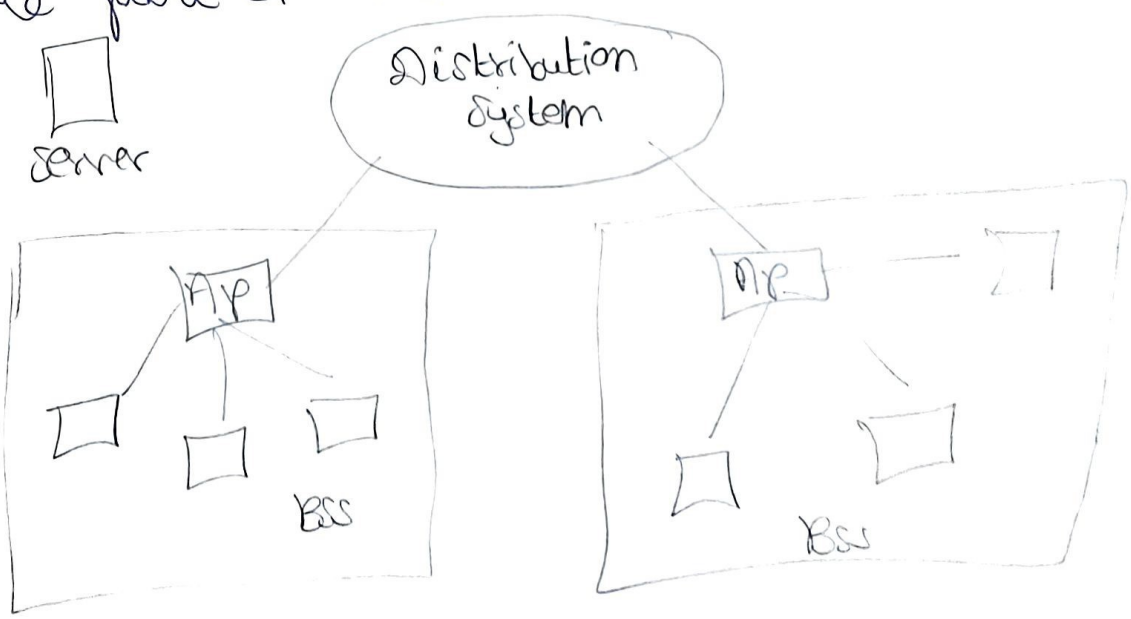
ii) Extended service set (ESS):

* A set of BSS can be interconnected by a distribution system to form an extended service set.

* ESS uses 2 types of stations: mobile & stationary

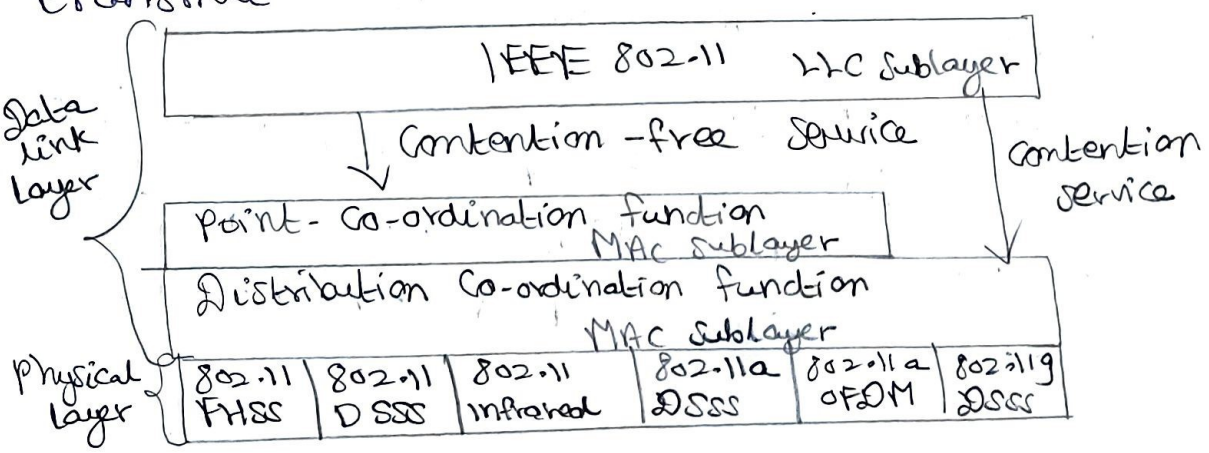
* The mobile stations are normal stations inside BSS.

* The stationary stations are AP stations that are part of wired LAN.



3) MAC Sublayer:

* MAC Sublayer is responsible for channel access procedures, protocol Data Unit (PDU) addressing, frame formatting, error checking and fragmentation.
* IEEE 802.11 defines two MAC sublayers:
i) Distributed Co-ordination Function (DCF)
ii) point Co-ordination Function (PCF)
* The DCF is the basic access method to support asynchronous data transfer on a best effort basis.
* The PCF is an optional capability to provide connection oriented, Connection-free services by enabling polled stations to transmit without channel.



4) Frame Format:

The MAC layer frame consists of 9 fields.

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312	4 bytes
Fc	D	Address 1	Address 2	Address 3	SC	Address 4	frame body	Fcs

Frame Control										
protocol version 2 bits	Type 2bits	Subtype 4 bits	To DS 1 bit	From DS 1bit	More flag 1 bit	Retry 1 bit	pwr mgt 1 bit	more data 1 bit	wep 1 bit	Rsvd 1 bit

i) Frame Control (fc):
It is 2 bytes long and define the type of frame and control information.

ii) D:
It defines the duration of transmission is used to set the value.

iii) Address:
There are 4 address fields, each 6 bytes long. It depends on value of To DS and from DS sub fields.

iv) Sequence Control:
It defines the sequence number of frames to be used in flow control.

v) Frame body:
It is between 0 and 2312 bytes contains information based on type and subtype defined in Fc field.

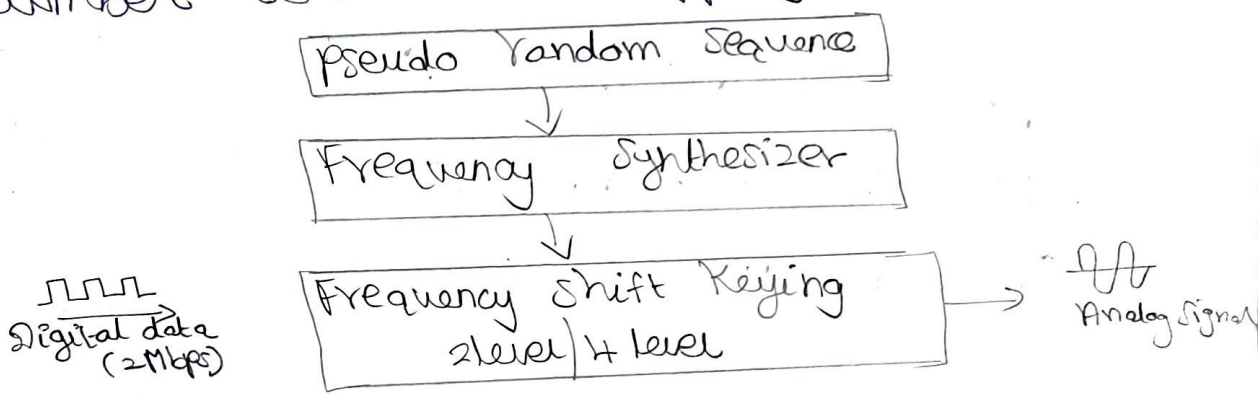
vi) FCS:
It is 4 bytes long and contains a CRC-32 error detection sequence.

5) Physical Layer:

The IEEE 802.11 LAN has several physical layers defined to operate with its MAC layer.

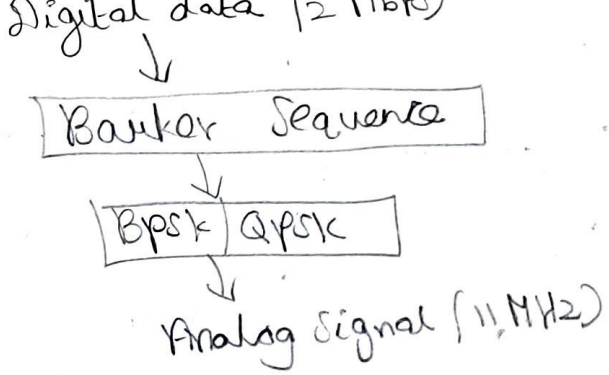
i) IEEE 802.11 FHSS:

It uses frequency hopping spread spectrum method. A pseudo random number selects the hopping sequence.



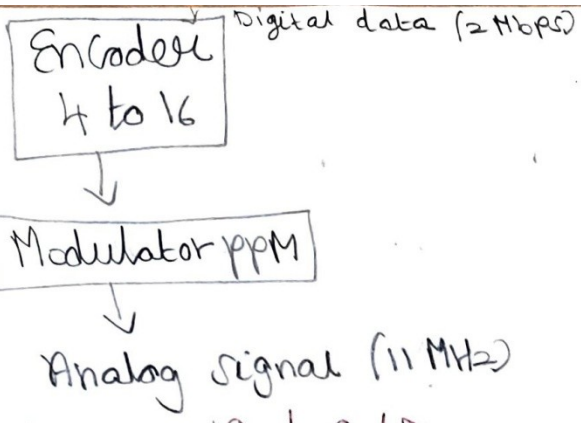
ii) IEEE 802.11 DSSS:

It uses direct sequence spread spectrum. It uses 2.4 GHz ISM band.



iii) IEEE 802.11 infrared:

It uses infrared light in the range of 800 to 900 nm. The modulation technique is called pulse position Modulation (ppm)



6) Wireless LAN protocols:

It is an extension of Cabled Networks, not a replacement. It requires Special MAC Sublayer protocol. The protocol designed for wireless LAN is MACA - Multiple Access with Collision Avoidance.

1) Requirements of wireless LAN:

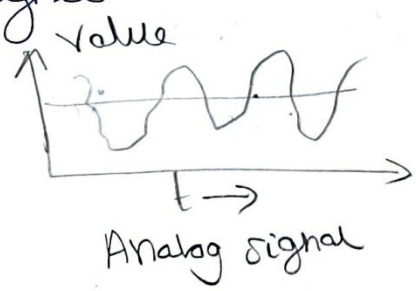
i) Number of nodes
ii) Throughput
iii) Connection to backbone LAN
iv) Service area
v) Battery power consumption
vi) License free operation
vii) Hard off / roaming
viii) Dynamic configuration
ix) Transmission robustness and security

Data and Signals:

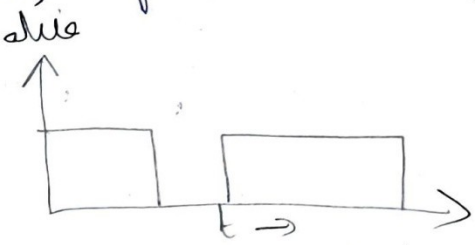
* Both data and signals represent them can be either analog or digital in form.
* Data can be of 2 types; analog and digital.
* Analog data take on continuous values on some interval. Eg: voice & video
* Digital data take on discrete values. Eg: Text or character strings

Analog and Digital Signal:

Analog signals are continuous-valued, digital signals are discrete-valued. The independent variable of signal could be time, space or integers.



Analog signal



Digital signal

Digital signal have only a limited number of defined values, usually two values 0 and 1.

i) periodic and Nonperiodic Signals:

i) periodic Signals:

A signal is periodic

Signal if it completes a pattern within a measurable time frame. A periodic signal is characterized by amplitude, frequency and phase. A Single frequency voltage waveform is,

$$v(t) = V \sin(2\pi f t + q)$$

Where,

$v(t)$ = Time varying voltage sine wave

V = peak amplitude (volts)

f = Frequency (hertz)

t = Time (seconds)

q = phase (degrees or radians)

Non-periodic signals:

* It is also called as aperiodic signal. A non-periodic signal never repeat. It does not satisfy the periodicity property.

* Both analog and digital signals can be periodic or non-periodic. But in data communications periodic signals are analog signals and non-periodic signals are digital signals.

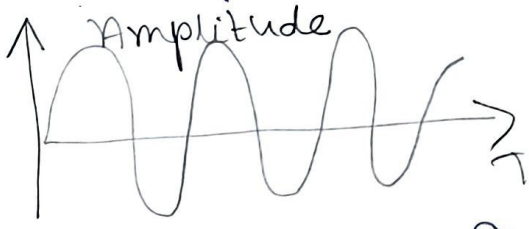
2) Periodic Analog Signals:

Periodic analog signals are of 2 types: Simple or Composite

* A Simple periodic analog signal is sine wave and it cannot be decomposed into simpler signals.
* A Composite periodic analog signal is composed of multiple sine waves.

1) Sine wave:

A sine wave is a geometric waveform that oscillates periodically and is defined by function. Analog signals are denoted by sin waves. Minimum and maximum values can be either positive or negative. They can be periodic or non-periodic.



Eg: Human voice is an example of analog signals.

2) Frequency and phase:

Frequency refers to the number of periods in 1sec. period is the inverse of

frequency and frequency is the inverse of period.

$$\text{Frequency } (f) = \frac{1}{\text{period } (T)} \quad \text{and}$$

$$T = \frac{1}{f}$$

period is expressed in seconds. Frequency is expressed in Hertz which is cycle per second.

3) Wavelength:

Wavelength is another characteristic of a signal traveling through a transmission medium. Wavelength binds the period of frequency of simple sine wave to the propagation medium of the speed.

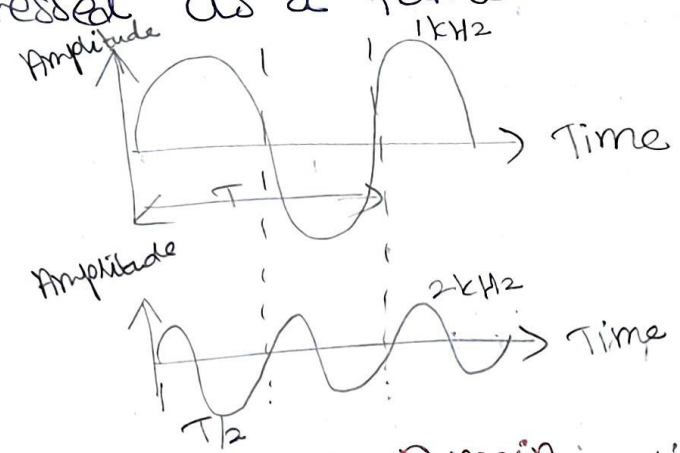
Wavelength = propagation speed x period

$$\text{Wavelength } (\lambda) = \frac{\text{propagation speed } (c)}{\text{Frequency } (f)}$$

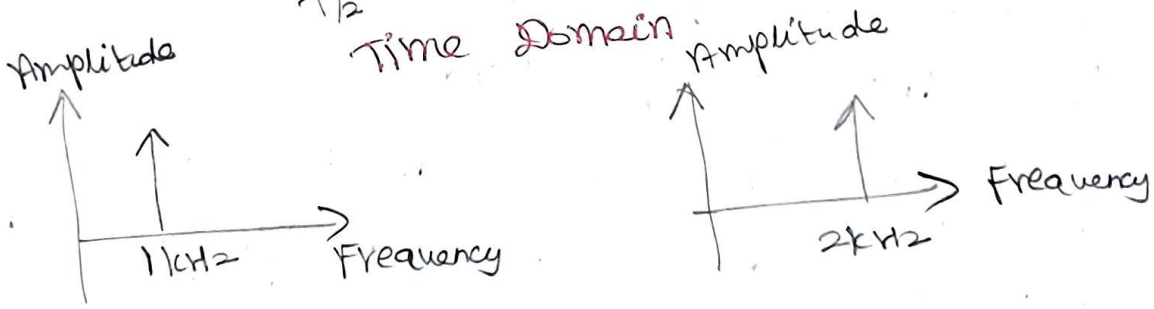
Wavelength is denoted by Greek letter lambda.

4) Time and Frequency Domain:

Electrical signals have both time and frequency domain representations. In the time domain, voltage or current is expressed as a function of time.

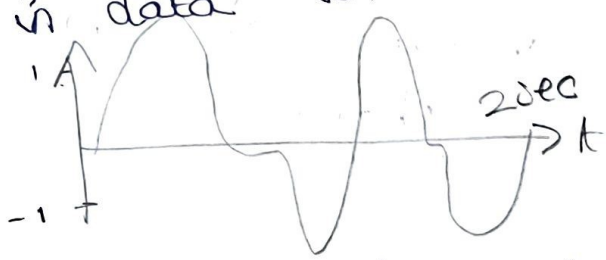


Time Domain



5) Composite Signals:

A single-frequency sine wave is not useful in data communications.



A single-frequency signal, a signal made of many simple sine waves.

to send a composite

6) Bandwidth:

Bandwidth is the amount of data can be

transmitted in fixed amount of time. For 234
digital devices, the bandwidth is expressed
in bits per second or bytes per second.

3) Digital Signals:

Digital means discrete form. The data in communication can be represented in digital form ie in 0 and 1 form.

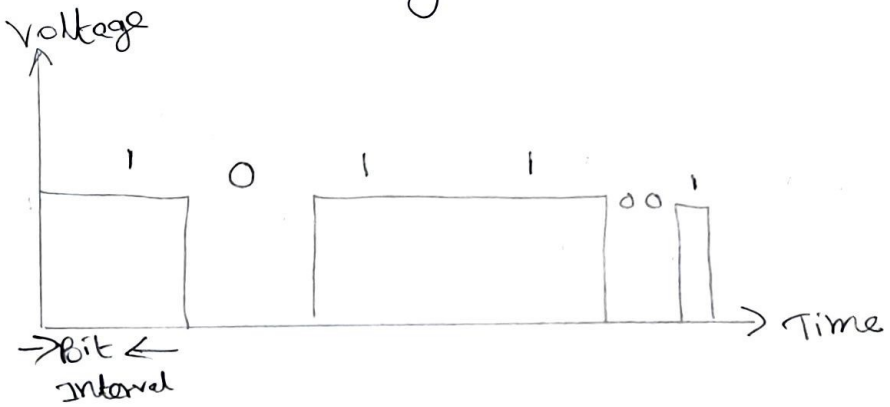
i) Bit Interval: is the time required to send one single bit.

ii) Bit rate: is defined as the number of bits intervals per second.

iii) Digital bandwidth: is the maximum bit rate a medium can propagate through it.

iv) Frequency Spectrum: is used to analyze and synthesize a signal.

v) Baud rate: indicates the rate at which signal level changes over a period of time.



Performance:

The Network performance is measured in various parameters such as,

1) **Bandwidth:**
It is a characteristic of Network. It can be measured in hertz and bits per second.

i) **Bandwidth in Hertz:**
It refers to range of frequencies in a composite signal or the range of frequencies that a transmission channel can pass.

ii) **Bandwidth in bps:**
It refers to speed of bit transmission in a channel or link.

2) **Throughput:**
It is an actual measurement of how fast data can be transmitted where as bandwidth is a potential measurement of link. It is usually less than bandwidth.

3) **Latency:**
It is termed as delay. It is time required for a message to completely

arrive at the destination from source.
It has 4 components.

i) propogation time
ii) Transmission time
iii) Queuing time
iv) processing delay

4) Bandwidth - Delay product:

The bandwidth and delay are two performance parameters of a link. It defines the number of bits that can fill the link.

5) Jitter:

It is a parameter related to delay. It is introduced since different packets of data encounter different delays. The data packets reaching at receiver at different times causing jitter.

latency = propagation time x Transmit time x Queue size

$$\text{propagation time} = \frac{\text{Distance}}{\text{Speed of light}}$$

$$\text{Transmit time} = \frac{\text{packet size}}{\text{Bandwidth}}$$

$$\text{Throughput} = \frac{\text{packet transfer size}}{\text{packet transfer time}}$$

$$\text{Transfer time} = \text{Round trip time} + \frac{1}{\text{Bandwidth} \div \text{packet transfer size}}$$

Transmission Media:

* Media is the general term used to describe the data path that forms the physical channel between sender and receiver.
* It can be twisted pair wire such as used for telephone installation, wire media are referred to as bounded media and wireless media are referred to as unbounded media.
* The transmission medium is the physical path between transmitter and receiver in a data transmission system. Communication is in the form of electromagnetic waves.

1) Classification of Transmission Media:

The transmission medium can be mainly classified into 2 types.

i) Bounded or Guided Media:

Depending on the type of transmission medium can be classified into 3 types.

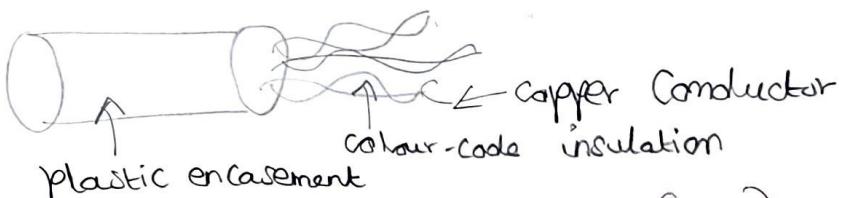
a) Twisted pair (TP) Cable:

It is least expensive and most widely used. It consists of two insulated

Copper wires arranged in a regular spiral pattern. Twisted pair cable comes in two varieties.

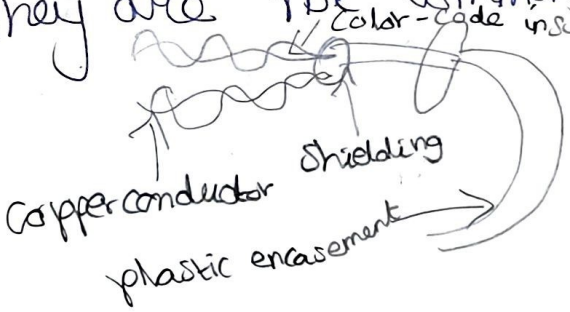
* Unshielded Twisted pair (UTP) Cable:

It is a set of twisted pair of cable within a plastic sheet. UTP is ordinary telephone wire.



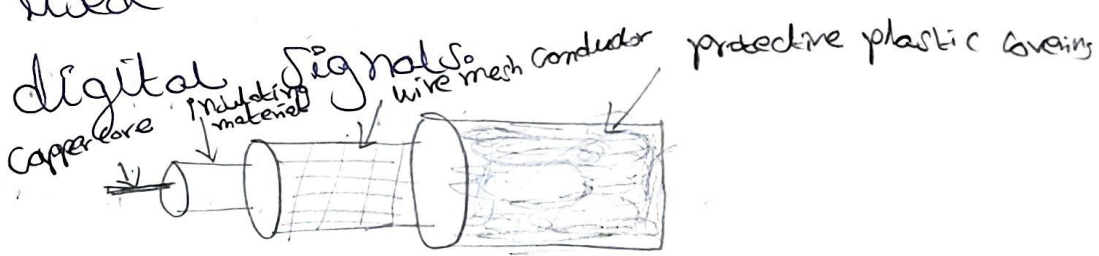
* Shielded Twisted pair (STP) Cable:

It offers a protective sheathing around the copper wire. It provides better performance at lower data rates. They are not commonly used in networks.



b) Co-axial Cable:

It is made up of two conductors that share the common axis. It is used to transmit both analog and digital signals.



c) Fiber optic Cable (FoC):

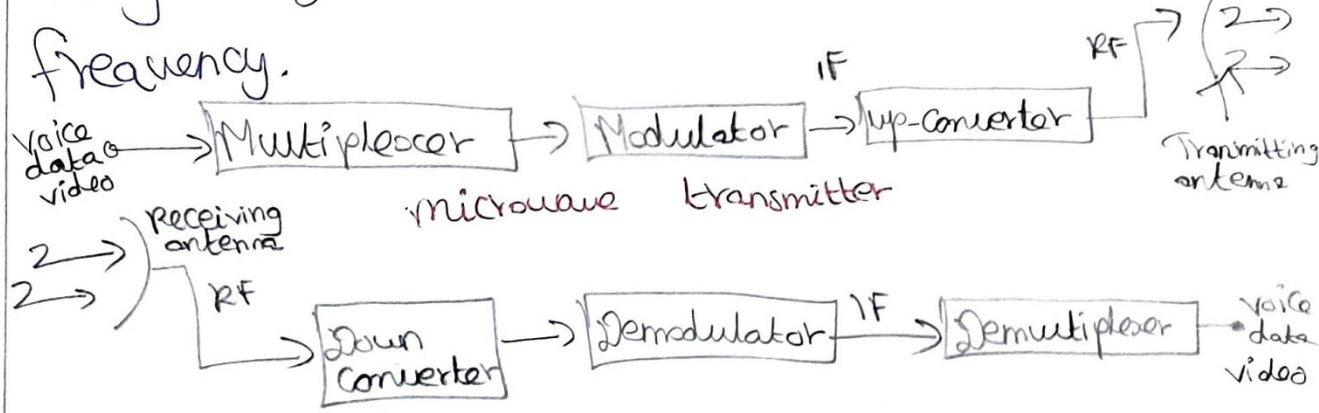
It is a light pipe used to carry a light beam from one place to another. It may be multimode or Signal mode. Multimode fibers use multiple light paths whereas Signal mode fibers allows a single light path and are typically used with laser signaling.

ii) Unbounded or unguided media:

Depending on the method of transmission the unbounded media can be further classified into two types.

a) Microwave links or radio links:

Radio waves have frequencies between 10 kHz and 1GHz. Radio waves include the following types: Short wave, very high frequency and ultra high frequency.

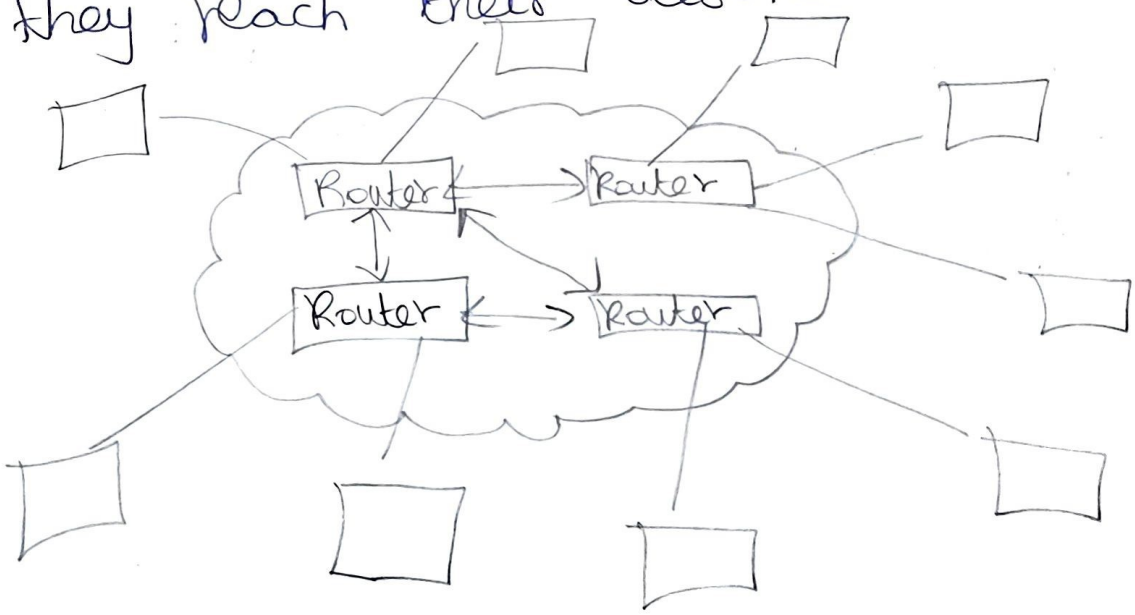


b) Infrared Light wave Transmission::

* Unguided infrared light are widely used for short range communication.
* The remote control used in TV, VCR and Stereos all use infrared communication.

Switching:

* Long distance transmission between devices is typically done over a network of switching nodes.
* Switching nodes do not concern with content of data. Their purpose is to provide a switching facility that move the data from node to node until they reach their destination.



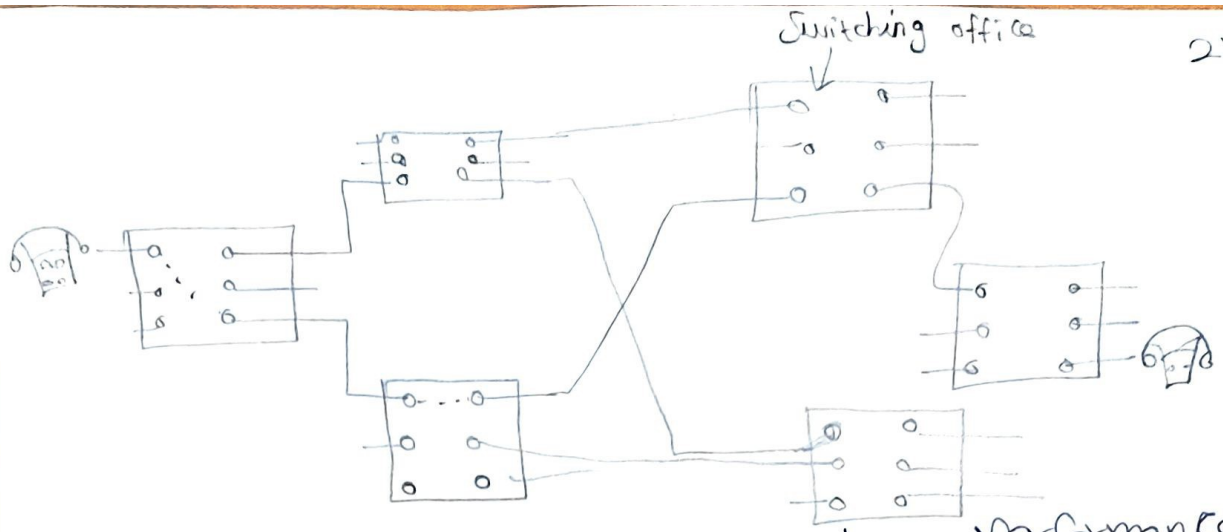
Switched Network

* Data entering the network from a station are routed to destination switched from node to node.

Circuit Switching:

* The telephone system as it historically developed was designed for voice and analog signals. Sending data requires bandwidth. The amount of bandwidth needed is directly related to the data rate is desired. An analog voice signal contains its data in a relatively narrow bandwidth in proportion to the amount of data it carries.
* For voice signals, a relatively large amount of distortion is acceptable, since the human ear can understand voice even with distortion looks severe to the eye.
* For digital signals, these distortions cause the receiver to misinterpret the signal that is sent and produce an error.
* The regular telephone loop from local office to the phone is guaranteed by the phone company to have specific characteristics. This type of line is the lowest performance line called voice grade conditioning.

* Similar line characteristics are offered by telephone companies on the line that go between phone company offices. These inter office lines are called trunks. Any phone line can connect one user to another user through the phone system, the user has a line assigned randomly through the phone offices. It is called the dial-up (or) Switched network.
* Telephone networks are connection oriented because they require the setting up of connection before the actual transfer of transmission can take place.
* An end-to-end path setup beginning of a session, dedicated to the application and then released at the end of session is called Circuit Switching
* It is effective for application which make comparitively use of channel.



* For application need greater performance than these dial up lines can offer, telephone companies offer specially conditional lines. These lines both from the phone to the office and between phone offices, provide better frequency response and time delay characteristics. The kind of conditioned line is leased by the user. The term dedicated and leased are used when the phone company has set aside a conditional line for a communication link.