Unit - I

Introduction and Physical Layer

1.1 NETWORKS:

A network is the interconnection of a set of devices capable of communication.

A device can be a host such as a large computer, desktop, laptop or cellular phone. or a connecting device such as a router,

1.1.1 Network Criteria:

The most important of network criteria are

- Performance
- Reliability and
- Security

Performance:

* Performance can be measured in many ways including transit time and response time.

* Transit time is the amount of time required for a message to travel from one device to another.

* Response time is the elapsed time between an inquiry and a response.

* The performance of a network depends on a number of factors including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

* Performance is evaluated by two networking metrics : throughput and delay.

↳ Reliability :

* Network Reliability is measured by the frequency of failure, the time it takes a link to recover from a failure and the network's robustness.

↳ Security :

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

1.1.2 Physical Structures :

↳ Types of Connection :

* A network is two or more devices connected through links.

* A link is a communications pathway that transfers data from one device to another.

* For communication to occur, two devices must be connected in some way to the same link at the same time.

* There are two possible types of connections :

1. Point to point
and 2. multi point.

1. Point to point:

* A point to point connection provides a dedicated link between two devices.

* The entire capacity of the link is reserved for transmission between those two devices.

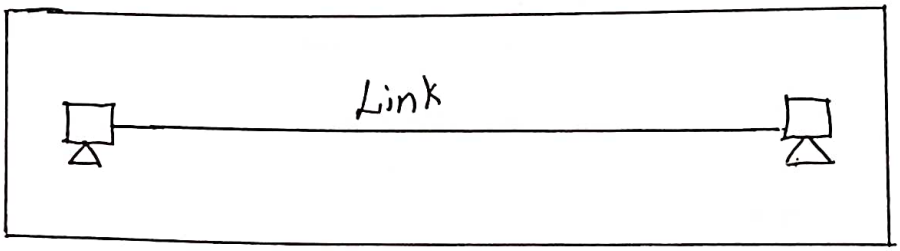


Figure: point to point.

2. Multipoint:

* A multipoint or multidrop connection is one in which more than two specific devices share a single link.

* The capacity of the channel is shared either spatially or temporally

* If several devices can use the link simultaneously, it is a spatially shared connection.

* If users must make take turns, it is a timeshared connection.

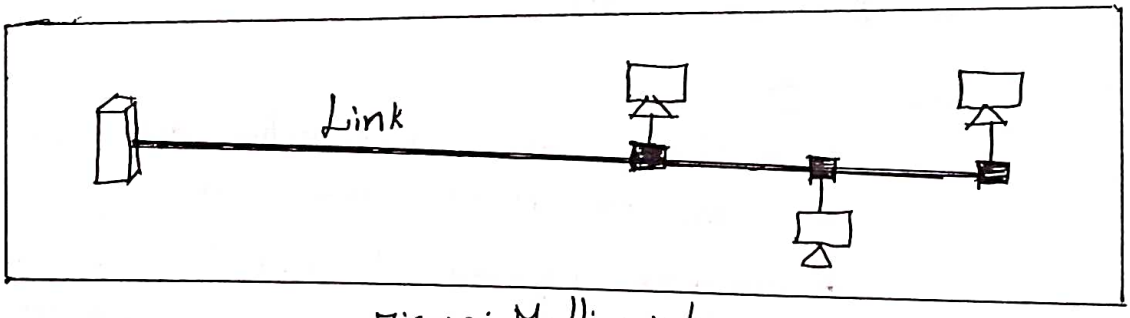


Figure: Multi point.

Physical Topology:

Physical topology refers to the way in which a network laid out physically.

There are four basic topologies:

1. Mesh
2. Star
3. Bus and
4. Ring

1. Mesh Topology:

↳ In mesh topolgy, every device has a dedicated point to point link to every other device.

↳ Node 1 must be connected to n-1 nodes, node 2 must be connected to n-1 nodes and finally node n must be connected to n-1 nodes.

↳ In a mesh topology there is. n(n-1)/2 duplex mode links.

Advantages:

* Eliminates the traffic problems
* A mesh topology is robust
* Advantage of privacy or security
* Fault identification and fault isolation is easy.

Disadvantages:

* Installation and reconnection are difficult.
* Accomodate more space due to bulk of wiring
* Hardware required to connect each link can be expensive.

Practical Example:

* Connection of telephone regional offices.

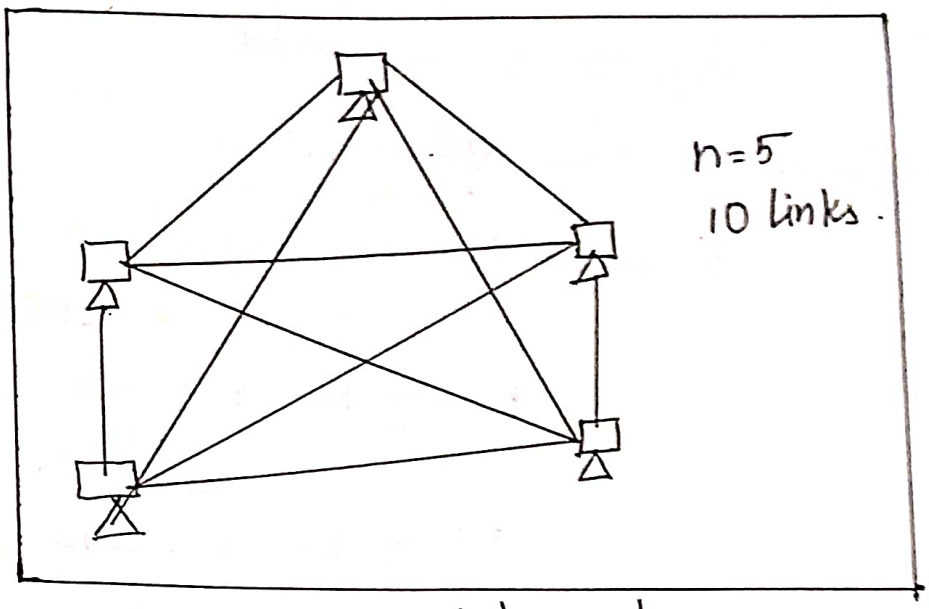


Figure: Mesh Topology.

2. Star Topology:

↳ In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.

↳ The devices are not directly linked to one another.

Advantages:

* Less expensive than a mesh topology.
* Easy to install and reconfigure.
* Less cabling is needed
* Robustness - If one link fails, only that link is affected.

Disadvantage:

* Dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

Example:

* Local Area Networks (LANs)

— continuation is on page no. (7)

1.2.3 Metropolitan Area Network (MAN)

↳ A MAN is designed to extend over an entire city.

* May be a single network such as cable tv network

* May be a means of connecting a numba of LANs into a larger network.

↳ Resources may be shared LAN to LAN as well as device to device.

↳ Example: Company can use a MAN to connect the LANs in all its offices throughout a city.

↳ A MAN can be owned by a private company or it may be a service provided by a public company such as local telephone company.

↳ The telephone companies provide a popular MAN service called Switched Multi megabit Data Services (SMDS).

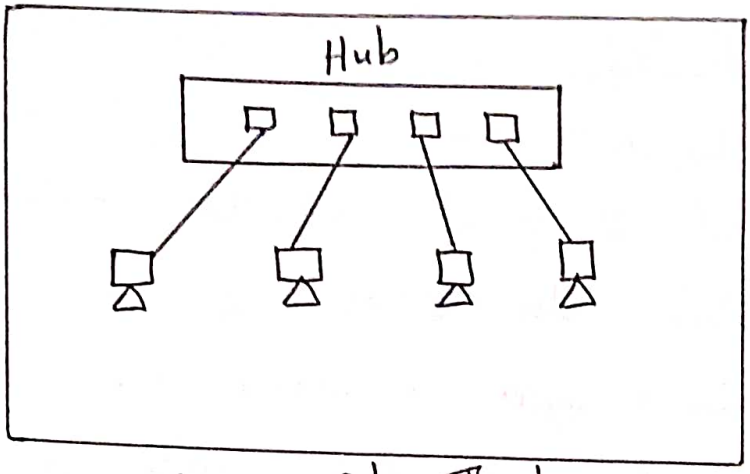


Figure : Star Topology

3. Bus Topology:

↳ A bus topology is a multipoint connection.

↳ One long cable acts as a backbone to link all the devices in the network.

↳ Nodes are connected to the bus cable by droplines and taps.

Advantages:

* Easy installation
* Redundancy ~~is eliminated~~
* Uses Less cabling when compared to mesh and star topology.

Disadvantages:

* Difficult reconnection and fault isolation.
* A fault or break in the bus cable, stops all transmission.

Example:

* Traditional Ethernet LANs.

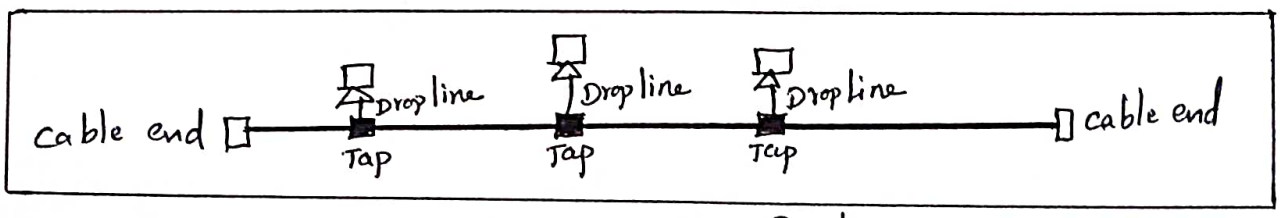


Figure : Bus Topology.

4. Ring Topology:

↳ In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.

↳ A signal is passed along the ring in one direction, from device to device until its destination.

↳ Each device in the ring incorporates a repeater.

Advantages:

* Easy to install and reconfigure.
* Fault isolation is simplified.

Disadvantage:

* Unidirectional traffic.

Example:

* Token Ring, which is a Local Area Network introduced by IBM.

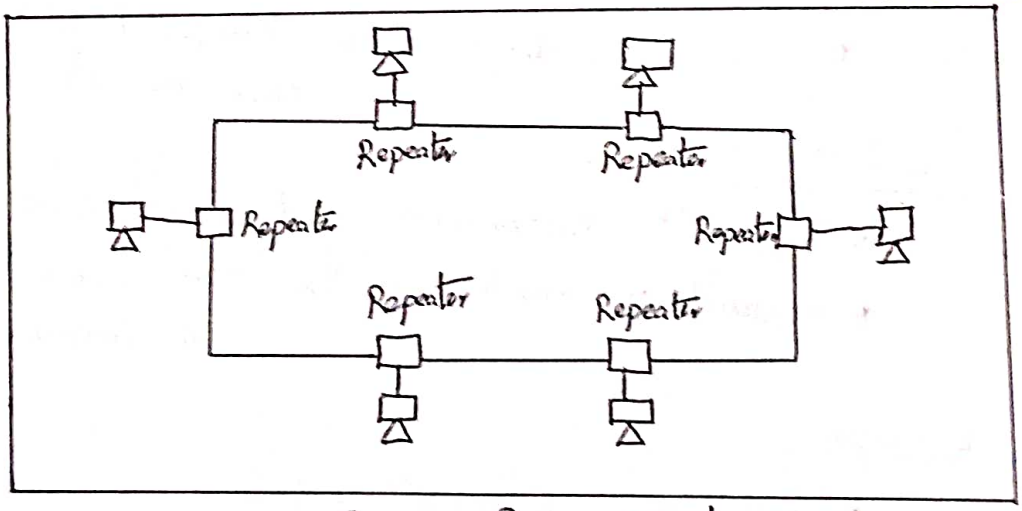


Figure: Ring Topology

1.2 NETWORK TYPES:

1.2.1 Local Area Network:

↳ A Local Area Network (LAN) is usually privately owned and connects some hosts in a single office, building or campus.

↳ Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN.

↳ A packet sent by a host to another host carries both the source host's and the destination host's address.

↳ In the past, all hosts in a network were connected through a common cable. The packet carries both the source and destination host's addresses.

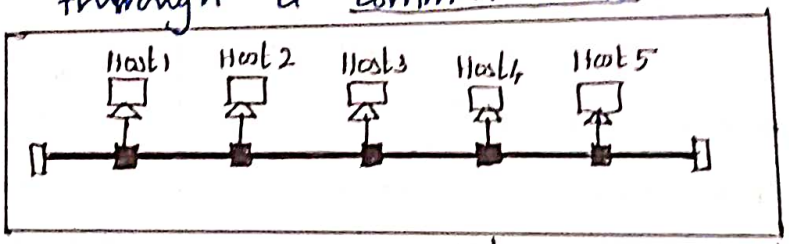


Figure: LAN with a common cable (past)

↳ Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other host.

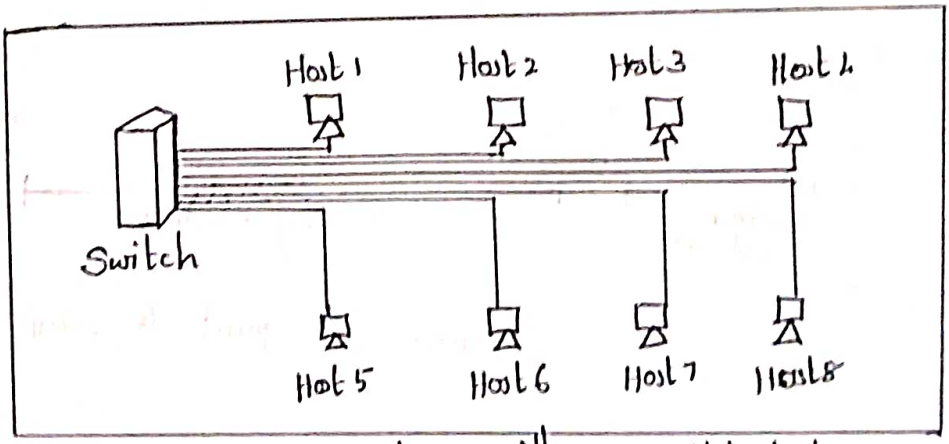


Figure: LAN with a switch (today)

1.2.2 Wide Area Network:

↳ A Wide Area Network (WAN) is also an interconnection of devices capable of communication.

Differences between LAN and WAN

LAN	WAN
1. A LAN is normally limited in size, spanning an office, a building or a campus	1. A WAN has a wider geographical span, spanning a town, a state, a country, or even the world
2. A LAN interconnects hosts.	2. A WAN interconnects connecting devices such as switches, routers or modems.
3. A LAN is normally privately owned by the organization that uses it.	3. A WAN is normally created and run by communication companies and leased by an organization that uses it.

Point to Point WAN:

↳ A point to point WAN is a network that connects two communicating devices through a transmission media.

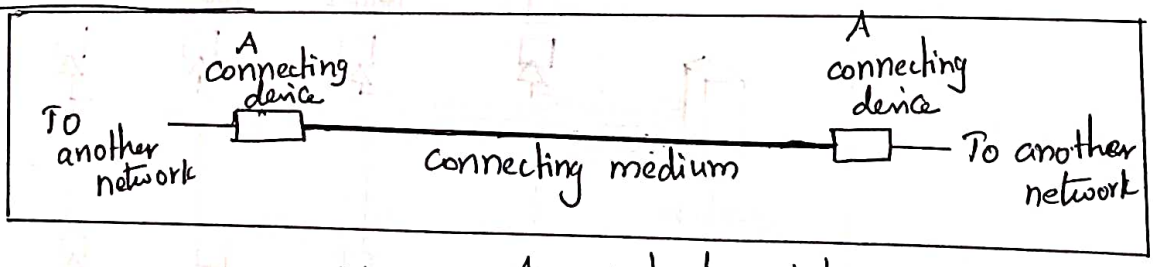


Figure: A point to point WAN

Switched WAN:

↳ A switched WAN is a network with more than two ends.

↳ A switched WAN is a combination of several point to point WANs that are connected by switches.

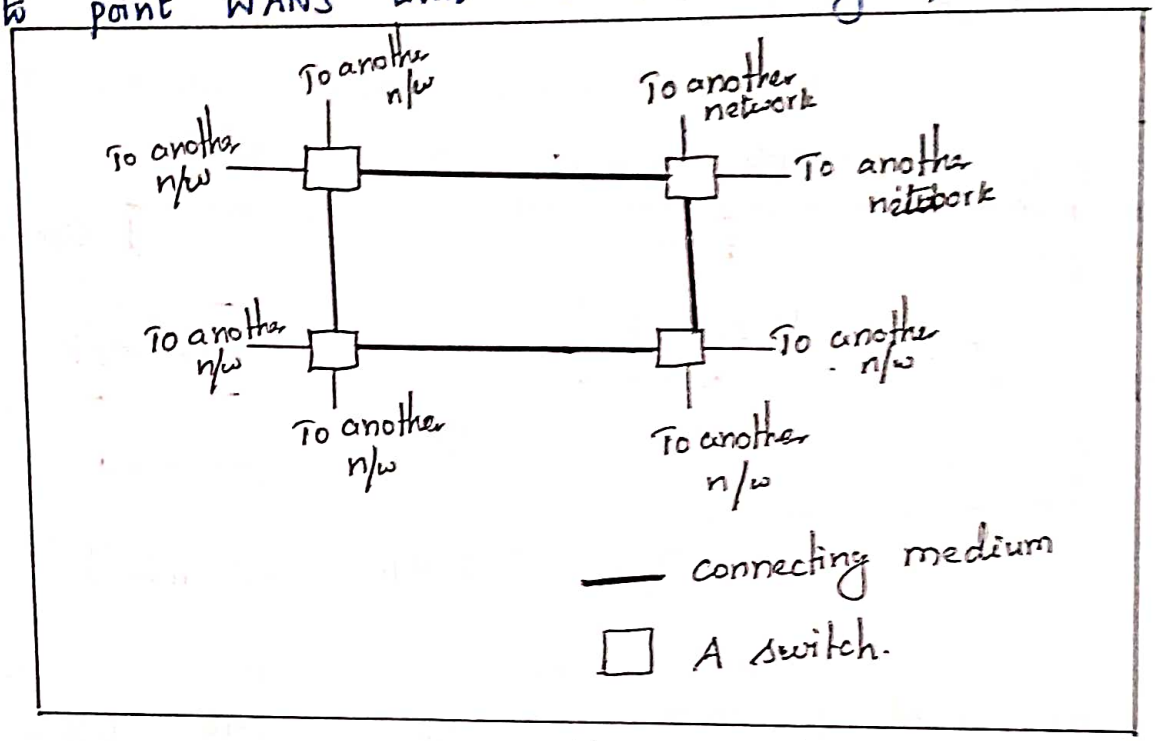


Figure: A switched Network

Internetwork:

↳ When two or more networks are connected, they make an internetwork or internet.

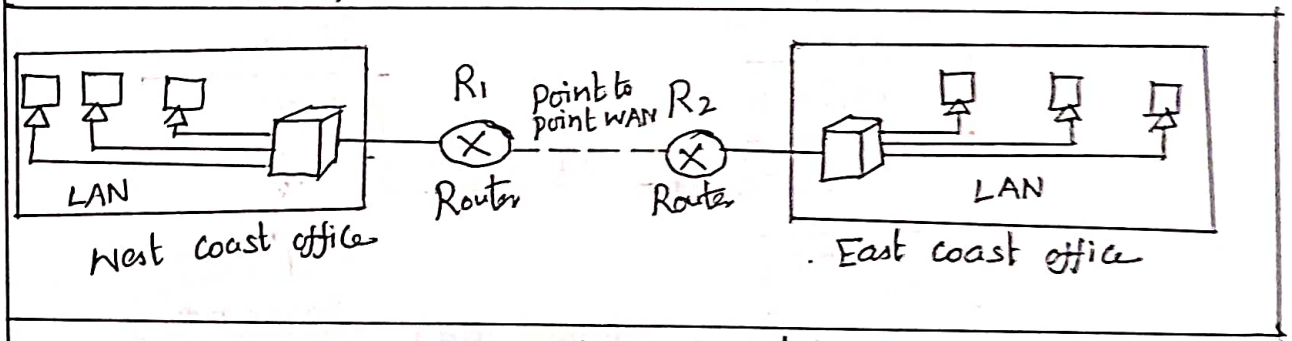


Figure: An Internetwork

1.2.3: Metropolitan Area Network (MAN):

Refer page no. 6

1.3 PROTOCOL LAYERING:

↳ A protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.

↳ When communication is simple, we may need only one simple protocol.

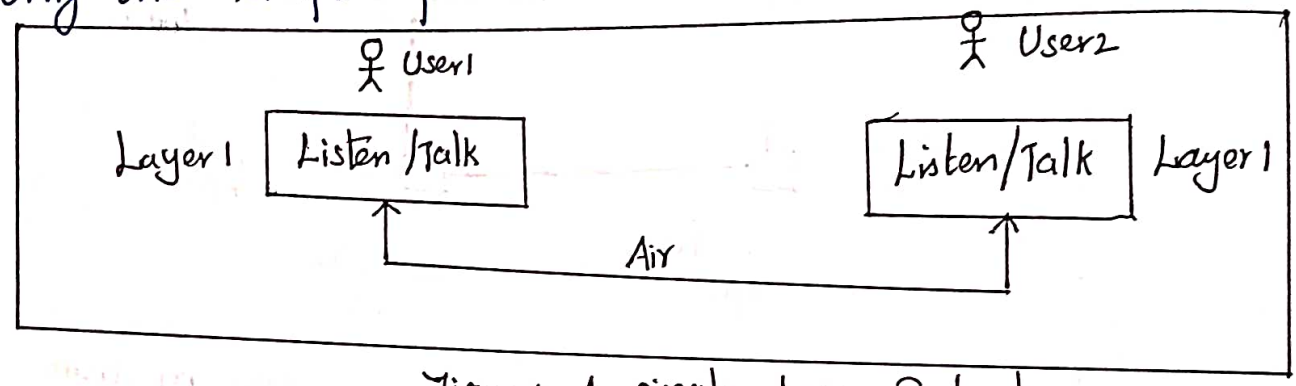


Figure: A single Layer Protocol.

↳ When the communication is complex, we may need to divide the task between different layers.

↳ In this case, we need a protocol at each layer or protocol layering.

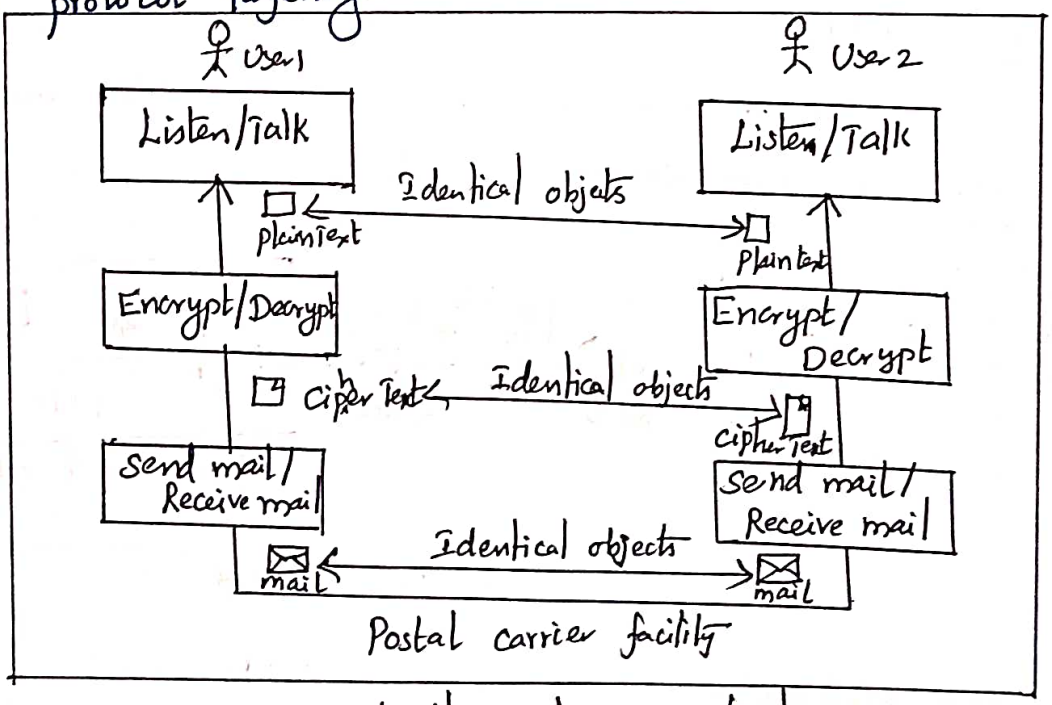


Figure: A three Layer protocol.

↳ Protocol layering enables us to divide a complex task into several smaller and simpler tasks. This is referred to as modularity.

↳ The advantage of protocol layering is that it allows us to separate the services from the implementation.

Principles of protocol Layering:

↳ There are two principles of protocol layering.

First Principle:

The first principle dedicates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.

Second Principle:

The second principle that we need to follow in protocol layering is that the two objects under each layer at both site should identical.

Logical connections:

↳ Each Layer have Layer-to-Layer communications.

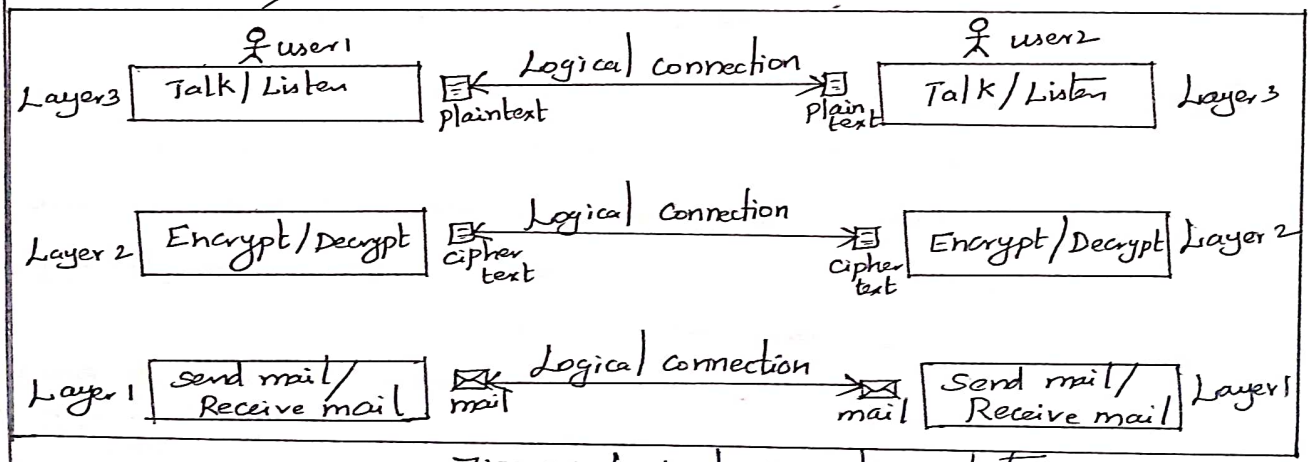


Figure: Logical connection between peer Layers.

1.4 TCP/IP PROTOCOL SUITE

↳ TCP/IP (Transmission Control Protocol / Internet Protocol) is a set of protocols organized in different layer.

↳ TCP/IP is a protocol suite used in the Internet today.

↳ It is a hierarchical protocol made up of interactive modules, each of which provide a specific functionality.

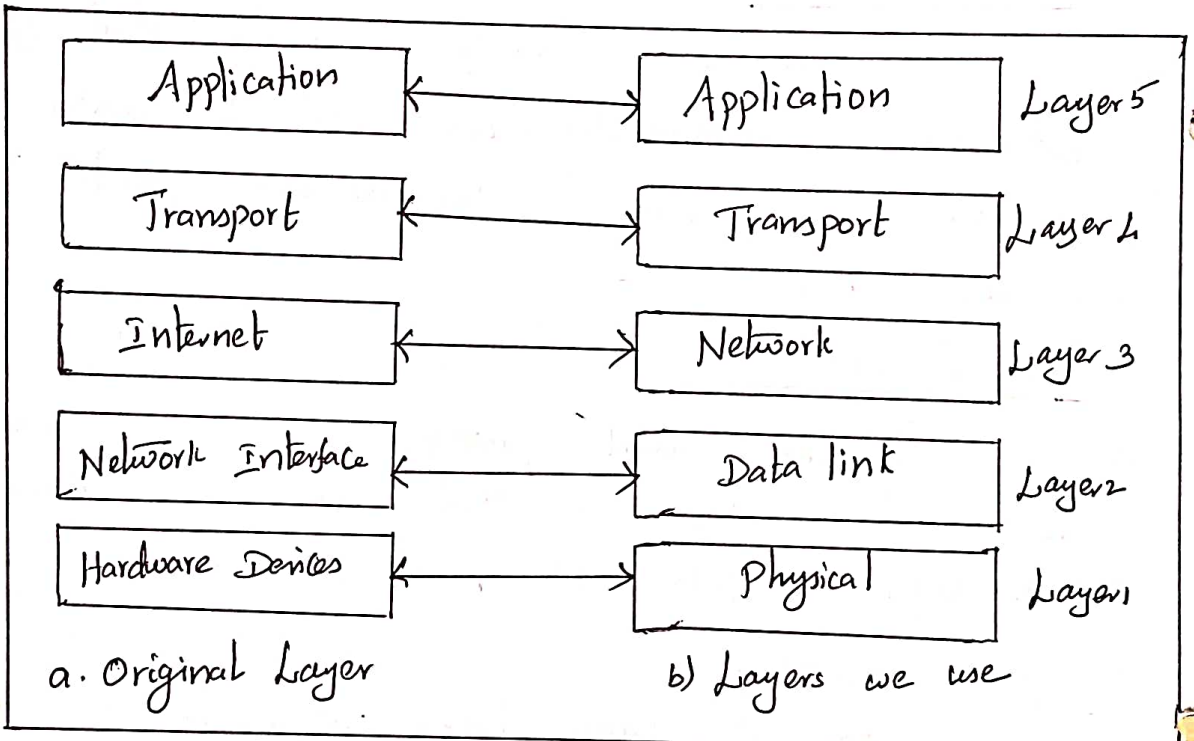


Figure: Layers in the TCP/IP protocol suite

Physical Layer:

↳ The physical layer is responsible for carrying individual bits in a frame across the link.

↳ There is a hidden layer, the transmission media under the physical layer.

↳ Two devices are connected by a transmission medium.

↳ The transmission medium does not carry bits; it carries electrical or optical signals.

Data Link Layer:

↳ The data link layer is responsible for taking the data gram and moving it accross the link.

↳ The link can be a wired LAN with a link layer switch, a wireless LAN, a wired WAN or a wireless WAN

↳ TCP/IP does not define any specific protocol for the datalink layer.

↳ The data link layer takes a datagram and encapsulates it in a packet called a frame.

↳ Each link layer protocol may provide a different services such as complete error detection and correction, only error correction.

Network Layer:

↳ The network layer is responsible for creating a connection between the source compute and the destination computer.

↳ The communication at the network layer is host-to-host.

↳ The network layer includes the main protocol Internet Protocol (IP).

* IP defines the format and the structure of addresses used in this layer.

* IP is also responsible for routing a packet from its source to its destination.

* IP is a connection less protocol that provides no flow control, no error control and no congestion control services.

↳ The network layer also includes unicast and multicast routing protocols.

* A routing protocol does not take part in routing but it creates forwarding tables for routers to help them in the routing process.

↳ The network layer also has some auxiliary protocols that help IP in its delivery and routing tasks.

* The Internet control Message Protocol (ICMP) helps IP to report some problems when routing a packet.

* The Internet Group Management Protocol (IGMP) helps IP in multitasking.

* The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network layer address for a host.

* The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link layer address of a host.

Transport layer:

↳ The transport layer is responsible for giving services to the application layer.

↳ TCP/IP model defines 3 protocols for /17/ transport layer.

↳ Transmission Control Protocol (TCP)

* TCP is a connection oriented protocol.

* It creates a logical pipe between two TCP's for transferring a stream of bytes.

* TCP provides flow control, error control and congestion control to reduce the loss of segments due to congestion in the network.

↳ User Datagram Protocol (UDP)

* UDP is a connectionless protocol

* It does not provide flow, error or congestion control.

↳ Stream Control Transmission Protocol (SCTP)

* It is designed to respond to new applications that are emerging in the multimedia.

Application Layer:

↳ The two application layers exchange messages between each other.

↳ Process to process communication is the duty of the application layer.

↳ The application layer includes many predefined protocols.

* The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (www.

* The Simple Mail Transfer protocol (SMTP) is used in electronic mail (e-mail) service.

* The File Transfer Protocol (FTP) is used for transferring files from one host to another.

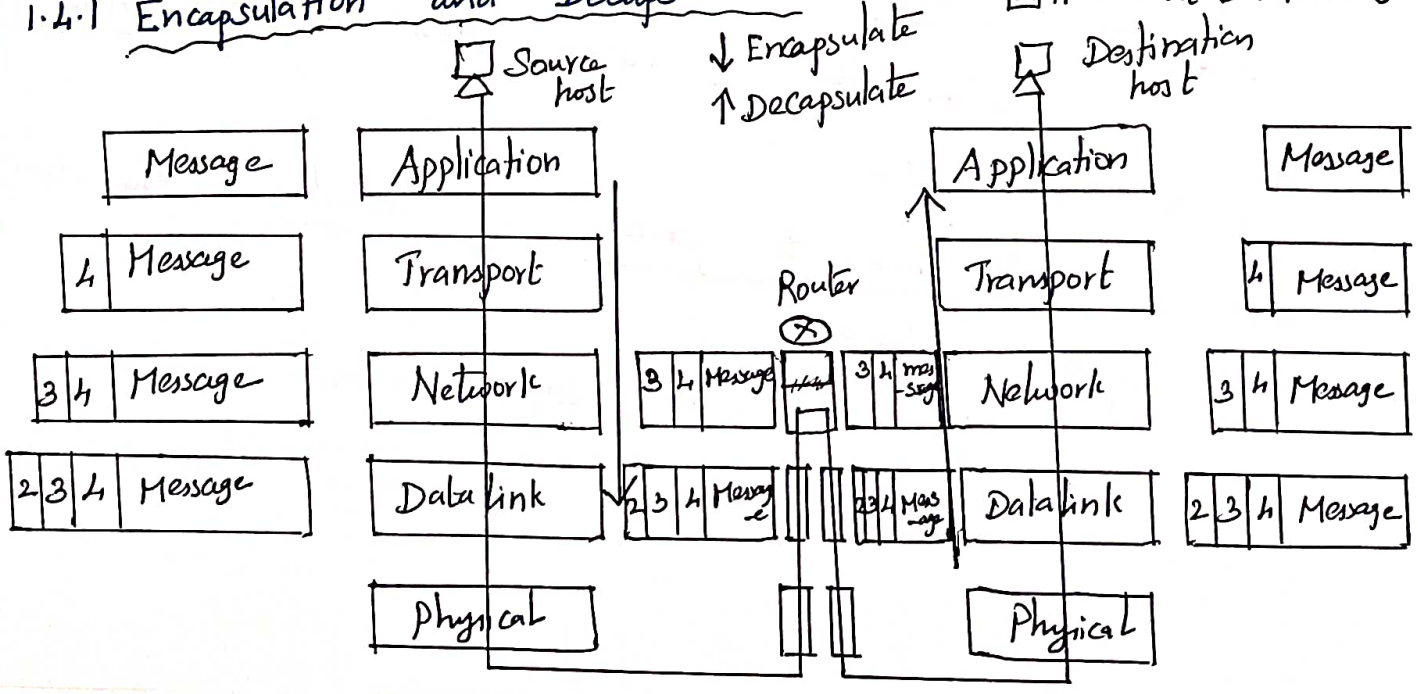
* The Terminal Network (TELNET) and Secure shell (SSH) are used for accessing a site remotely.

* The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet a global and local levels.

* The Domain Name System (DNS) is used by other protocols to find the network layer address of a computer.

* The Internet Group Management Protocol (IGMP) is used to collect membership in a group.

1.4.1 Encapsulation and Decapsulation:



Encapsulation at the source host:

↳ At the application layer, the data to be exchanged is referred to as a message

* A message does not contain any header or trailer.
* The message is passed to the transport layer.

↳ The transport layer takes the message as a payload.

* Transport layer adds its own header to the payload.
* The header contains identifiers of the source and destination application programs and information needed for flow, error control or congestion control.
* The transport layer packet is called the segment in TCP and the user datagram in UDP.
* The segment is passed to the network layer.

↳ The network layer takes the transport layer packet as payload.

* NL adds its own header to the payload.
* The header contains the addresses of the source and destination host.
* The network layer packet is called a frame.

↳ The data link layer takes the network layer packet as payload.

* DLL adds its own header to the payload.
* The header contains the physical addresses of the host.
* The link layer packet is called a frame.
* The frame is passed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router:

↳ At the router, we have both encapsulation and encapsulation.

↳ Data Link Layer
- * receives frames from physical layer
- * decapsulates the datagram from the frame and
- * passes the datagram to the network layer.

↳ The Network layer
- * Inspects the source and destination addresses in the datagram header and
- * Consults forwarding table to find next hop to which the datagram is to be delivered.
- * The datagram is then passed to the data link layer of the next link

↳ The data link layer of the next link
- * Encapsulates the datagram in a frame and
- * Passes the frame to the physical layer for transmission.

Decapsulation at the Destination host:

↳ At the destination host, each layer decapsulates the packet received from lower layer and removes the payload then delivers the payload to the next higher layer.

1.2.2: Addressing:

↳ Any communication that involves two parties needs two addresses

1. Soura address and
2. Destination address

↳ there are 4 pairs of addresses.

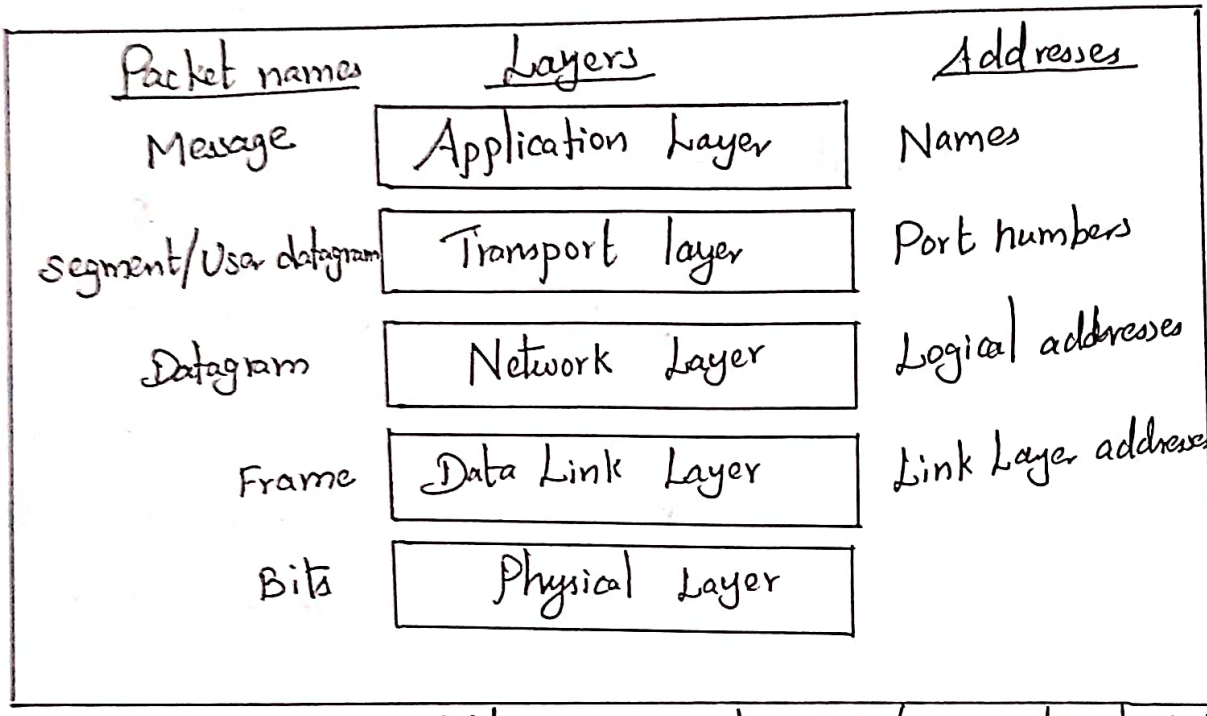


Figure: Addressing in the TCP/IP protocol suite

↳ At the application layer

* the names are used to define the site that provides services such as abc.com or email address such as somebody@coldmail.com.

↳ At the transport layer, address are called port numbers

* Port numbers define the application layer programs at the source and destination.
* Port numbers are local addresses that distinguish between several programs running at the same time.

↳ At the network layer, addresses are called IP addresses.

* IP address uniquely defines the connection of a device to the Internet
* IP addresses are global, with the whole internet as the scope.

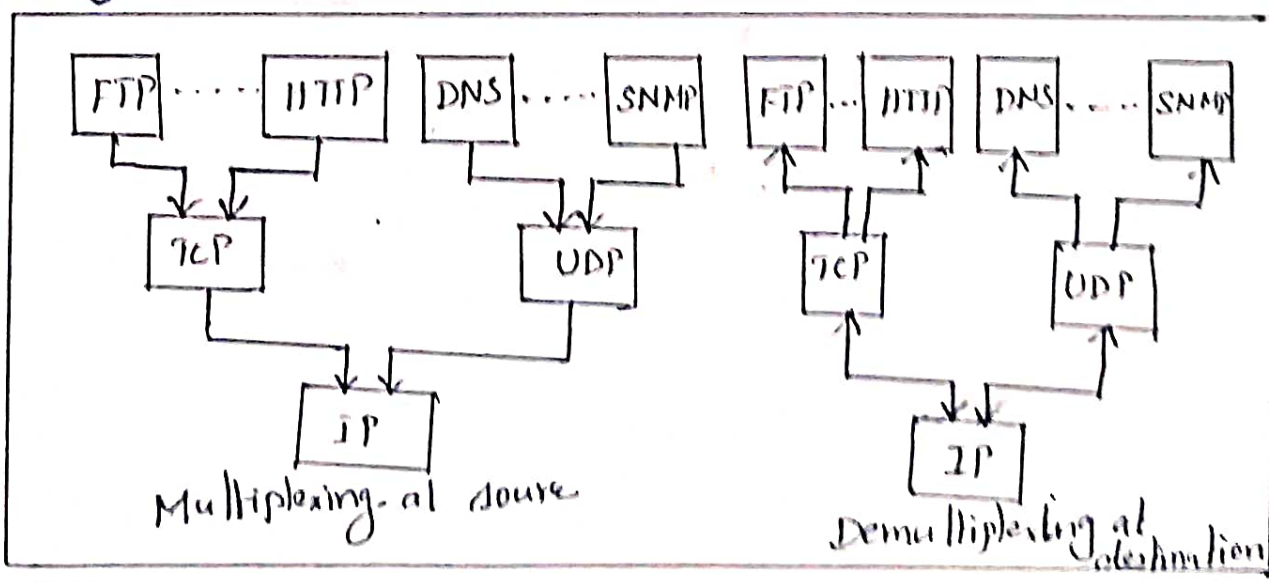
↳ At the data link layer, addresses are called MAC addresses.

* The MAC addresses defines a specific host or router in a network (LAN or WAN)
* The MAC addresses are locally defined addresses.

1.4.3 Multiplexing and Demultiplexing:

↳ Multiplexing means a protocol at a layer can encapsulate a packet from several next protocols one at a time.

↳ Demultiplexing means a protocol can decapsulates and deliver a packet to several next higher layer protocols one at a time.



↳ At transport layer

* either UDP or TCP can accept a message from several application layer protocols.

↳ At network layer, IP can accept

* a segment from TCP or user datagram from UDP

* a packet from ICMP or IGMP

↳ At data link layer, a frame may carry the payload coming from IP or ARP.

1.5. OSI MODEL

↳ The Open System Interconnection (OSI) is a model for understanding and designing a network architecture that is flexible, robust and interoperable.

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

↳ It consists of seven seperate but related layers, each of which defines a part of the process of moving information across a network.

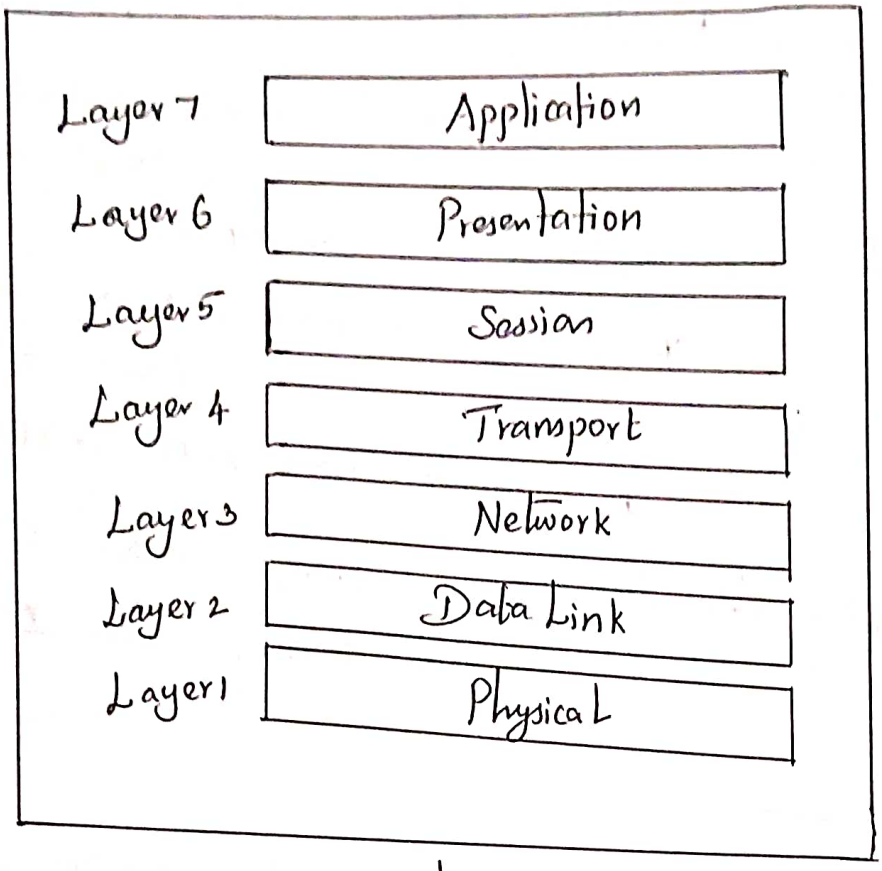


Figure: The OSI model

Physical Layer:

↳ The main functionality of the physical layer is to transmit the individual bits from one node to another node.

↳ It is the lowest layer of the osi model.

↳ Physical layer defines the procedures and functions that physical devices and interfaces have to perform for transmission of data.

a) Physical charateristics of interfaces and medium: Defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

b) Synchronization of bits: The sender and receiver clocks must be synchronized.

c) Line configuration: The devices are connected physically by using point to point and multi point connection.

d) physical Topology: Defines how devices are connected to make a network

c) Transmission mode: Defines the direction of transmission between two devices such as simplex, half-duplex or full duplex

Data Link Layer:

↳ The data link layer is responsible for moving frames from one hop (node) to the next.

↳ Other responsibilities of the data link include the following:

a) Framing: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

b) Physical addressing: It adds a header to the frame to define the sender/or receiver of the frame.

c) Flow control: It imposes a flow control mechanism to avoid overwhelming the receiver.

d) Error control: It adds reliability by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames by adding the trailer to the end of the frame.

d) Access control: It determine which device has control over the link at any given time, when two or more devices are connected to the same link.

Network Layer:

↳ The network layer is responsible for the delivery of individual packets from the source host to the destination host.

↳ Other responsibilities of the network layer include the following:

a) Logical addressing: When a packet passes the network boundary, the network layer adds the logical addresses of the sender and receiver.

b) Routing: The connecting devices called routers route or switch the packets to their final destination.

Transport layer:

↳ The transport layer is responsible for the delivery of a message from one process to another.

↳ Other responsibilities of the transport layer include the following.

a) Service-point addressing: The transport layer adds the header that contains the address known as a service-point address

b) Segmentation and reassembly: It divides the message into multiple segments and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, the transport layer reassembles the message based on their sequence numbers.

c) Connection control: Transport layer provides two services connection oriented service and connectionless service. A connectionless service treats each segment as an individual packet and they all travel in different routes to reach the destination. In A connection oriented service, all the packets travel in the single route.

d) Flow control: Flow control is performed from end to end rather than across a single link.

e) Error control: Error control is performed in a process to process rather than across a single link.

Session layer:

↳ The session layer is responsible for dialog control and synchronization.

↳ Specific responsibilities of the session layer include the following:

a) Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex or full duplex.

b) Synchronization: The session layer allows a process to add checkpoints or synchronization points to a stream of data.

Presentation Layer:

↳ The presentation layer is responsible for translation, compression and encryption.

↳ Specific responsibilities of the presentation layer include the following:

a) Translation: The presentation layer is responsible for the interoperability between different encoding methods.

b) Encryption: Encryption is a process of transforming the original information to another form and sends the resulting message out over the network. Decryption reverses the transformed message to the original information.

c) Compression: Data compression reduces the number of bits contained in the information.

Application Layer:

↳ The application layer is responsible for providing services to the user.

↳ Specific services provided by the application layer include the following:

a) Network Virtual Information: A network Virtual Information is a software version of a physical terminal and it allows a user to log on to a remote host.

b) File transfer, access and management: allows the user to access file in a remote host, retrieve files and to manage or control files in a remote computer locally.

c) Mail services: This application provides the basis for email forwarding and storage.

d) Directory services: This application provides distributed database sources and access for global information about various objects and services.

Layer	Data unit	Protocols/ Examples	Devices.
7. Application Layer	Message	HTTP, FTP, SMTP	
6. Presentation Layer	Message	JPEG	
5. Session Layer	Message	RPC, PAP	Gateway
4. Transport Layer	Segment	TCP, UDP	Firewall
3. Network Layer	Packet	IPV4, IPV6	Router
2. Data Link layer	Frame	IEEE 802.3/802.2	Switch, Bridge
1. Physical Layer.	Bits	Fibre, Copper Twisted wires.	Hub, Repeater, Modem, cables.

Figure: Various Layers in OSI model.

1.6 PHYSICAL LAYER:

↳ The physical layer is the first and lowest layer of the open system Interconnection model (OSI).

↳ The physical layer deals with bit level transmission between different devices and supports electrical or mechanical interfaces connecting to the physical medium for synchronized communication.

1.7. PERFORMANCE:

a) Bandwidth:

↳ The term bandwidth can be used in two different contexts with two different measuring values:

1. Bandwidth in Hertz
2. Bandwidth in bits per second.

1. Band width in Hertz:

↳ Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass.

↳ Example: the bandwidth of a subscriber telephone line is 4 KHz

2. Band width in Bits Per second:

↳ It refers to the speed of bit transmission in a channel or link.

↳ Example: The bandwidth of a Fast Ethernet network is a maximum of 100 Mbps

b) Throughput:

↳ A throughput is a measure of how fast we can actually send data through a network.

c) Latency (Delay):

↳ The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

↳ Latency is made of 4 components: propagation time, transmission time, queueing time and processing delay.

> Latency = propagation time + transmission time + queueing time + processing delay

1. Propagation Time:

↳ Propagation time measures the time required for a bit to travel from the source to the destination.

↳ The propagation time is calculated by dividing the distance by the propagation speed.

> Propagation time = Distance / propagation speed

↳ In a vacuum, light is propagated with a speed of 3×10^8 m/s.

2. Transmission Time:

↳ The transmission time of a message depends on the size of the message and the bandwidth of the channel.

> Transmission time = Message size / Bandwidth

3. Queueing Time:

↳ Queueing time is the time needed for each intermediate or end device to hold the message before it can be processed.

d) Jitter:

↳ Jitter is a problem if different packets of data encounter different delays.

Problems based on Performance:

1. A network with bandwidth of 10 Mbps can pass only an average of 12000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution:

Bandwidth = 10 Mbps

Frames = 12000 frames/minute

Bits = 10000 bits

Throughput = ?

Throughput = (12000 x 10000)/60

= 2 Mbps

---

2. What is the propagation time if the distance b/w the two points is 12,000 km? Assume the propagation speed to be 2.4×10^8 m/s in cable.

Solution:

Distance = 12,000 km

= 12000 x 1000 m

= 12×10^6 m

Propagation speed = 2.4×10^8

= 24×10^7

Propagation time = Distance / propagation speed

= $\frac{12 \times 10^6}{24 \times 10^7}$ = $1/2 \times 10$

= 0.05 s = 0.05 x 1000 ms

= 50 ms

3. What are the propagation time and the transmission time for a 2.5 KB (Kilobyte) message, if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12000 km and that light travels at 2.4×10^8 m/s.

Solution:

Message size = 2.5 KB
$= 2.5 \times 1000$ Bytes
$= 2500$ Bytes

Bandwidth = 1 Gbps
$= 1 \times 10^9$ bps

Distance = 12000 km
$= 12000 \times 10^3$ m
$= 12 \times 10^6$ m

propagation speed $= 2.4 \times 10^8$ m/s
$= 24 \times 10^7$ m/s

Propagation time = distance / propagation speed

$= \frac{12 \times 10^6}{24 \times 10^7} = \frac{1}{2 \times 10}$

$= 0.05$s $= \underline{50}$ ms

Transmission time = Message size / Bandwidth
$= 2500 \times 8 / 1 \times 10^9$
$= \underline{0.020}$ ms

4. How many bits can fit on a link with a 2ms delay if the bandwidth of the link is 10 Mbps?

Solution:

Bandwidth = 10 Mbps
$= 10 \times 1000$ bps $= 10000$ bps

Delay = 2ms

Number of bits = Bandwidth x delay
$= 10000 \times 2$
$= \underline{20000}$ bits

1.8. TRANSMISSION MEDIA:

↳ Transmission media are actually located below the physical layer and are directly controlled by the physical layer.

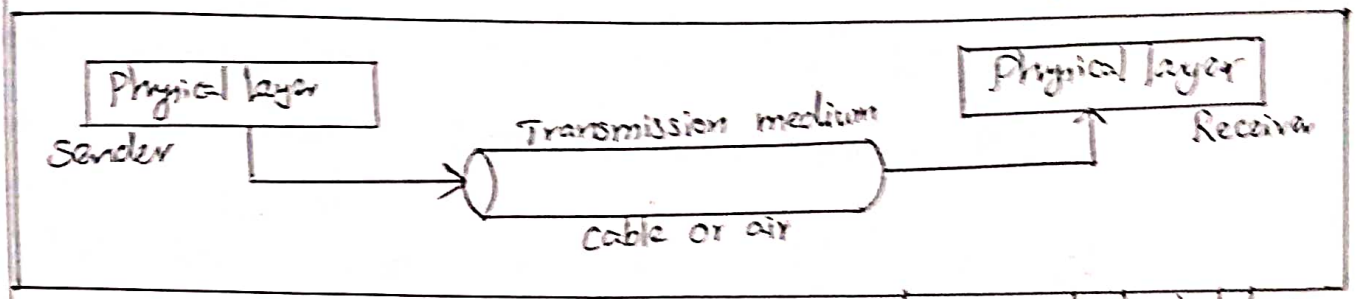


Figure: Transmission medium and physical layer.

↳ A transmission medium can be broadly defined as anything that can carry information from a source to a destination.

↳ The transmission medium is usually free space, metallic cable or fibre optic cable.

↳ The transmission media can be divided into two broad categories: guided and unguided.

↳ Guided media include twisted pair cable, coaxial cable and fibre optic cable.

↳ Unguided medium is free space.

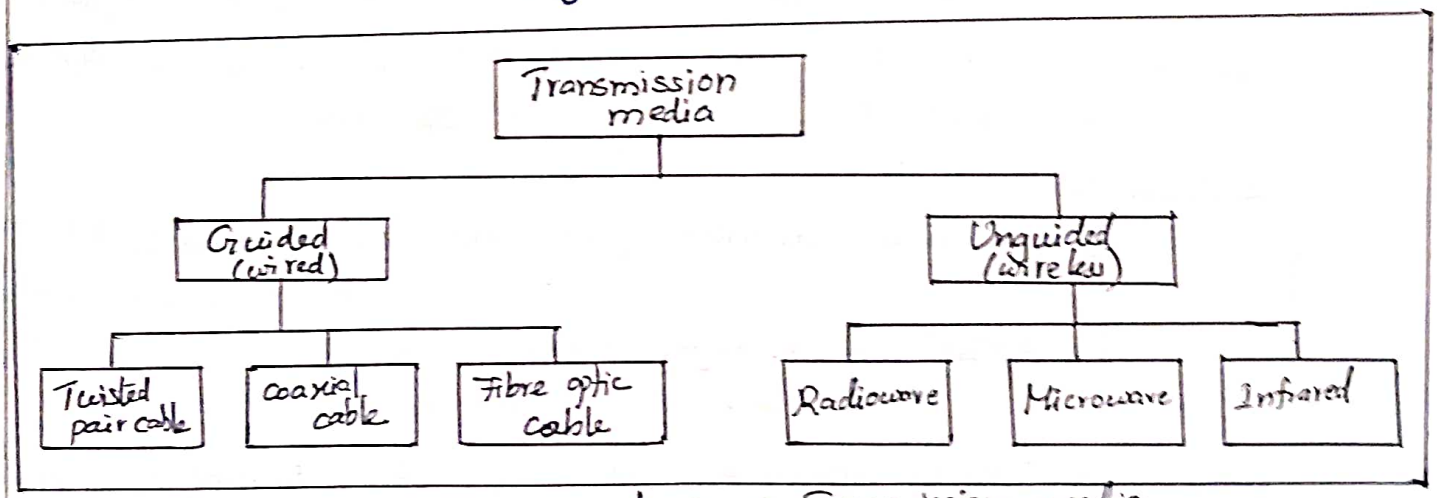


Figure: classes of Transmission media

1.8.1:

Guided Media:

↳ Guided media provide a conduit from one to another, it includes twisted pair cable, coaxial cable and fibre optic cable.

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

↳ Optic fibre cable is a cable that accepts and transports signals in the form of light.

Twisted Pair cable:

↳ A twisted pair consists of two conductors, each with its own plastic insulation, twisted together.

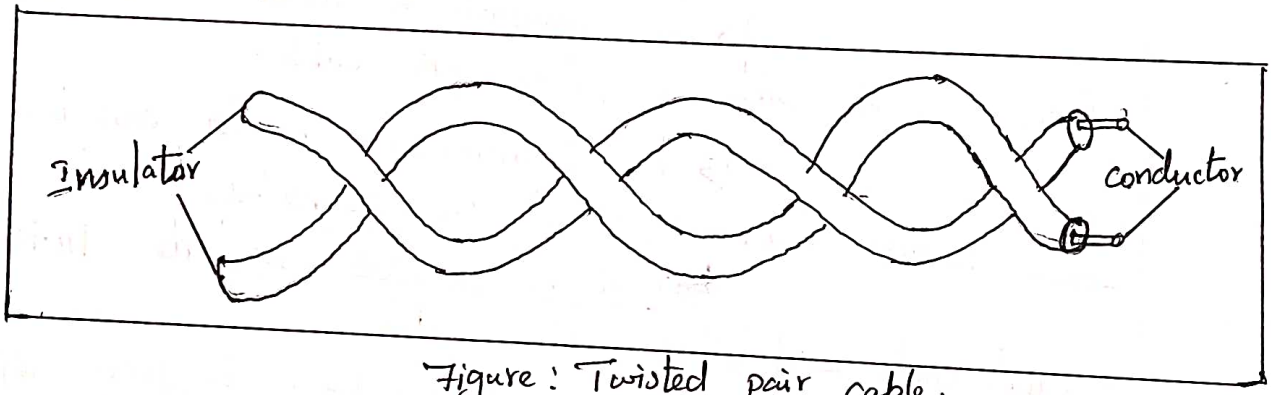


Figure: Twisted pair cable.

↳ One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

Connectors:

↳ The most common UTP connector is RJ45 (RJ stands for Registered Jack).

↳ RJ45 is a keyed connector, meaning the connector can be inserted in only one way.

Performance: ↳ With increasing frequency, the attenuation sharply increases.

Applications: ↳ Twisted pair cables are used in telephone lines to provide voice and data channels.

Coaxial cable:

↳ Coaxial cable or coax carries signals of higher frequency ranges than those in twisted pair cable.

↳ Coax has a central core conductor of solid wire enclosed in an insulating sheath, which is, in turn encased in an outer conductor of metal foil.

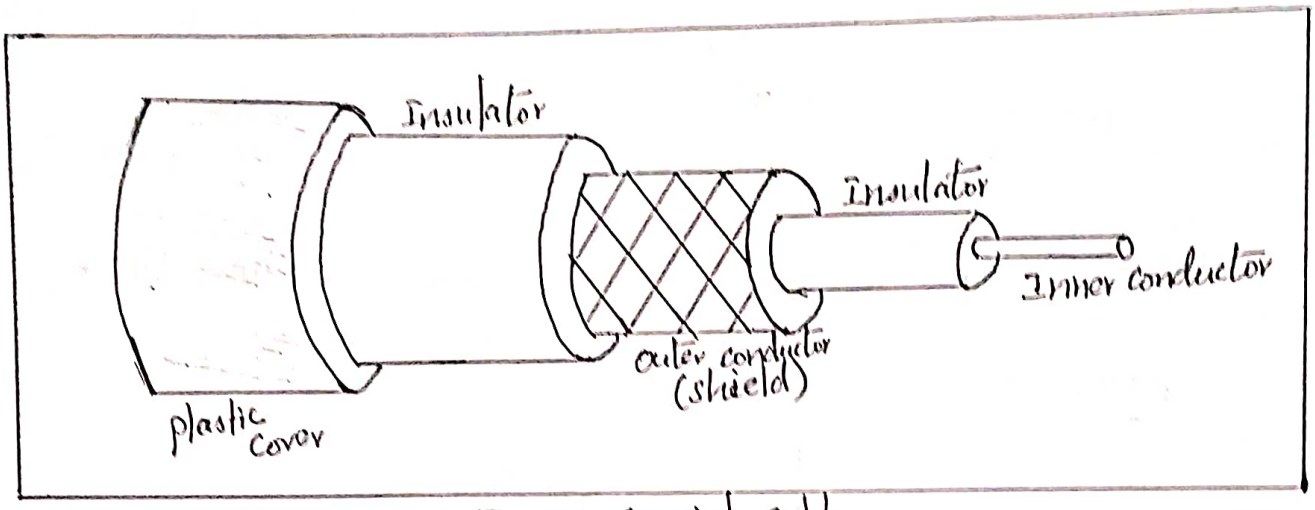


Figure: Coaxial cable.

Connectors:

↳ The most common type of connector used today is the Bayonet Neil - Concelman (BNC) connector.

↳ The three popular types of the connectors are

1. BNC connector → used to connect the end of the cable to a device, such as a TV set.
2. BNC T connector → used in Ethernet networks to branch out to a connection to a computer.
3. BNC terminator → used at the end of the cable to prevent the reflection of the signal.

Performance:

↳ The attenuation is much higher in coaxial cable than in twisted pair cable.

↳ Although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

Applications:

↳ Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10000 voice signals.

↳ Cable TV networks also use coaxial cables in

Fibre-optic cable:

↳ A fibre optic cable is made of glass or plastic and transmits signals in the form of light.

↳ Optical fibers use reflection to guide light through a channel.

↳ A glass or plastic core is surrounded by a cladding of less dense glass or plastic.

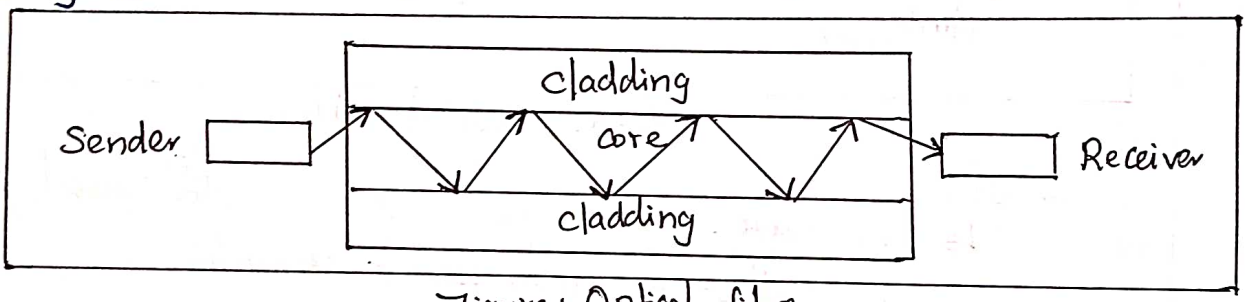


Figure: Optical fibre.

Propagation modes:

↳ Current technology supports two modes (multimode and single mode) for propagating light along optical channels.

↳ Multimode can be implemented in two forms: step-index or graded index.

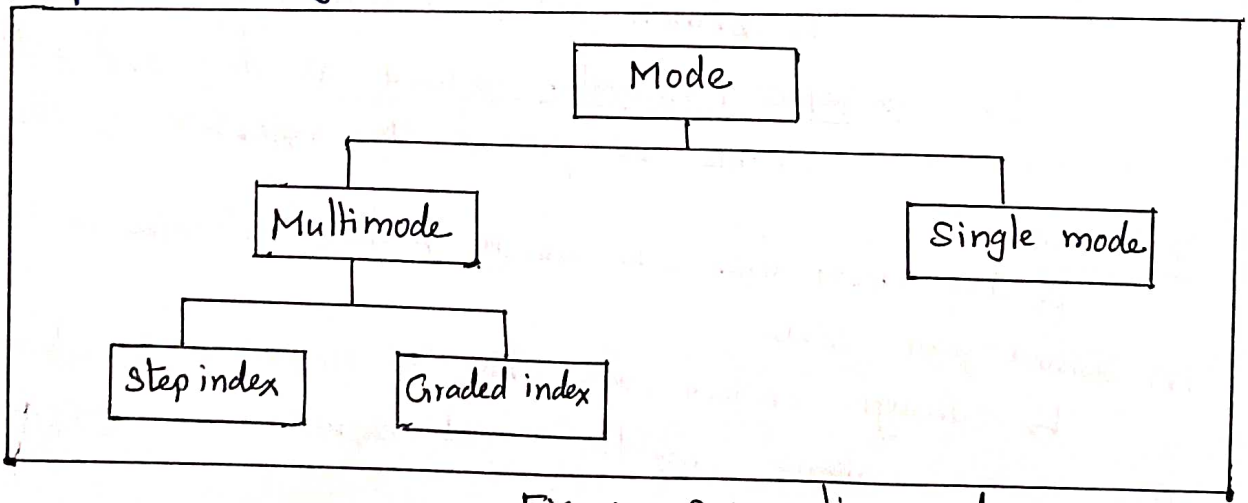


Figure: propagation modes.

Single mode → It is manufactured with a much smaller diameter and lower density

Multimode → Multiple beams from a light source move through the code in different paths

Multimode step index fiber → the density of the core remains constant from the centre to the edges.

Multimode graded index fiber → Density is highest at the center of the core and decreases gradually to its lowest at the edge.

Connectors:

↳ There are 3 types of connectors for fiber optic cables.

1. **Subscriber channel (SC) connector** → used for cable TV. It uses push/pull locking system.
2. **Straight-tip (ST) connector** → used for connecting cable to networking devices. It uses a bayonet locking system.
3. **MT-RJ** → same size as RJ45

Performance:

↳ Attenuation is flatter than in case of twisted pair cable and coaxial cable.

Applications:

↳ Fiber optic cable is often found in backbone networks.

↳ Local-area Networks such as **100Base-FX network** and **1000 Base-X** also use fiber optic cable.

Advantages:

* Higher bandwidth
* Less signal attenuation
* Immunity to electromagnetic interference
* Resistance to corrosive materials
* Light weight.
* Greater immunity to tapping

Disadvantages:

* Installation and maintenance require expertise.
* Unidirectional light propagation
* More expensive.

1.8.2. Unguided media : Wireless:

↳ Unguided medium transport electromagnetic waves without using a physical conductor.

↳ This type of communication is often referred to as wireless communication.

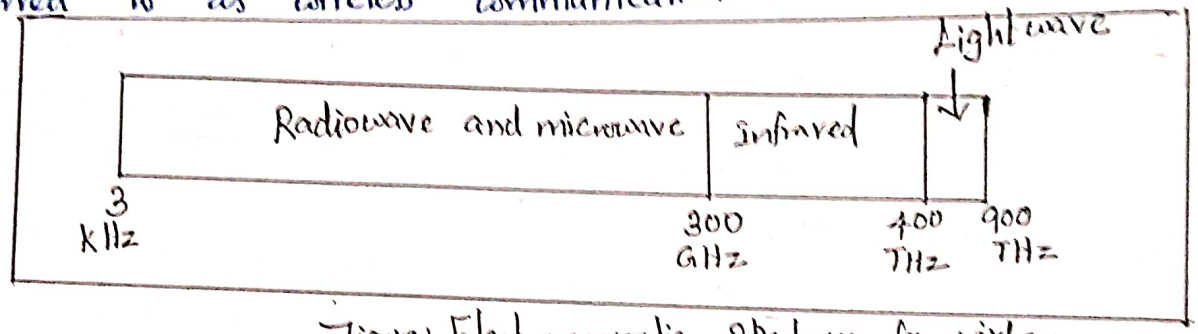


Figure: Electromagnetic Spectrum for wireless communication

↳ In ground propagation, radio waves travel through the lowest portion of the atmosphere.

↳ In sky propagation, higher frequency radio waves radiate upward into the ionosphere.

↳ In line of sight propagation, very high frequency signals are transmitted in straight lines directly from antenna to antenna.

Radio waves:

↳ Electromagnetic waves ranging in frequencies between 3kHz and 1GHz are normally called radio waves.

↳ Electromagnetic waves ranging in frequencies between 1 and 300 GHz are called microwaves.

↳ Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions.

↳ Radio waves that propagate in the sky mode, can travel long distances

↳ Radio waves of low and medium frequencies, can penetrate walls.

Applications:

↳ Radio waves are used for multicast communications, such as radio and television and paging systems.

Microwaves:

↳ Electromagnetic waves frequencies between 1 and 300GHz are called microwaves.

↳ Microwaves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused.

↳ Two types of antennas are used for microwave communications.

1. the parabolic dish → based on the geometry of a parabola.
2. the horn antenna → looks like a gigantic scoop.

↳ Some characteristics of microwave propagation are

* Microwave propagation is line of sight
* Very high frequency microwaves cannot penetrate walls.
* The microwave band is relatively wide almost 299GHz
* Use of certain portions of the band requires permission from authorities.

Applications:

↳ Microwaves are used for unicast communication such as cellular telephones, satellite networks and wireless LANs.

Infrared:

↳ Infrared waves, with frequencies from 300 GHz to and can be used for short range communication.

↳ Infrared waves, having high frequencies, cannot penetrate walls.

↳ The advantageous characteristic prevents interference between one system and another.

↳ The infrared waves cannot be used outside the building because the sun's rays contain infrared waves that can interfere with the communication.

Applications:

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

1.9. SWITCHING:

↳ A switched network consists of a series of interlinked nodes, called switches.

↳ Switches are devices capable of creating temporary connections between two or more devices linked to the switch.

↳ In a switched network, some of these nodes are connected to the end systems.

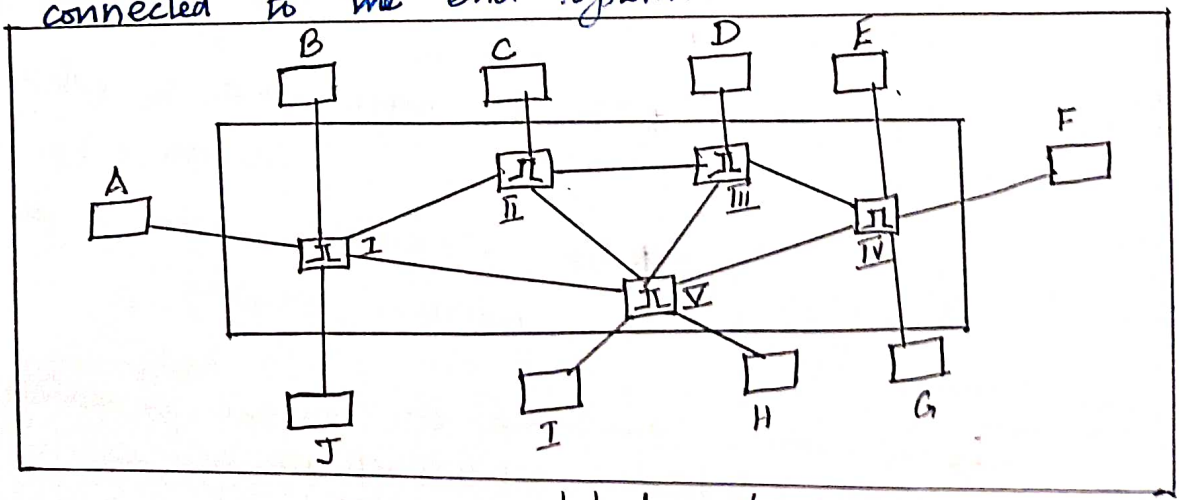


Figure: Switched network

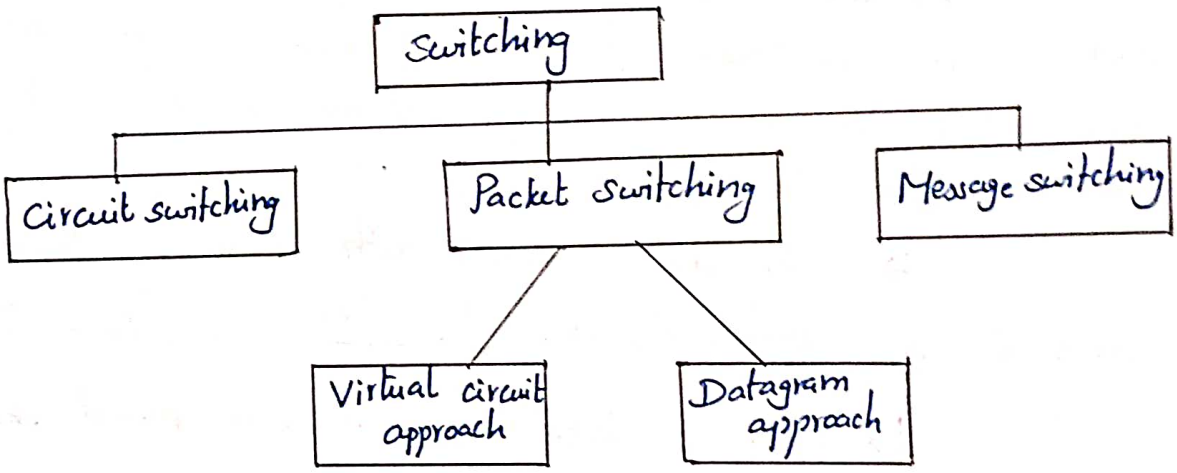
↳ The end systems are labeled A, B, C, D and so on and the switches are labeled I, II, III, IV and V.

↳ Each switch is connected to multiple links.

Three methods of switching:

↳ Three methods of switching are
* circuit switching
* Packet switching
and * message switching

↳ Packet switching are divided into two sub categories
* Virtual circuit approach
and * datagram approach.



1.9.1 CIRCUIT-SWITCHED NETWORKS

↳ A circuit switched network consists of a set of switches connected by physical links.

↳ A connection between two stations is a dedicated path made of one or more links.

↳ Each link is normally divided into n channels by using FDM or TDM.

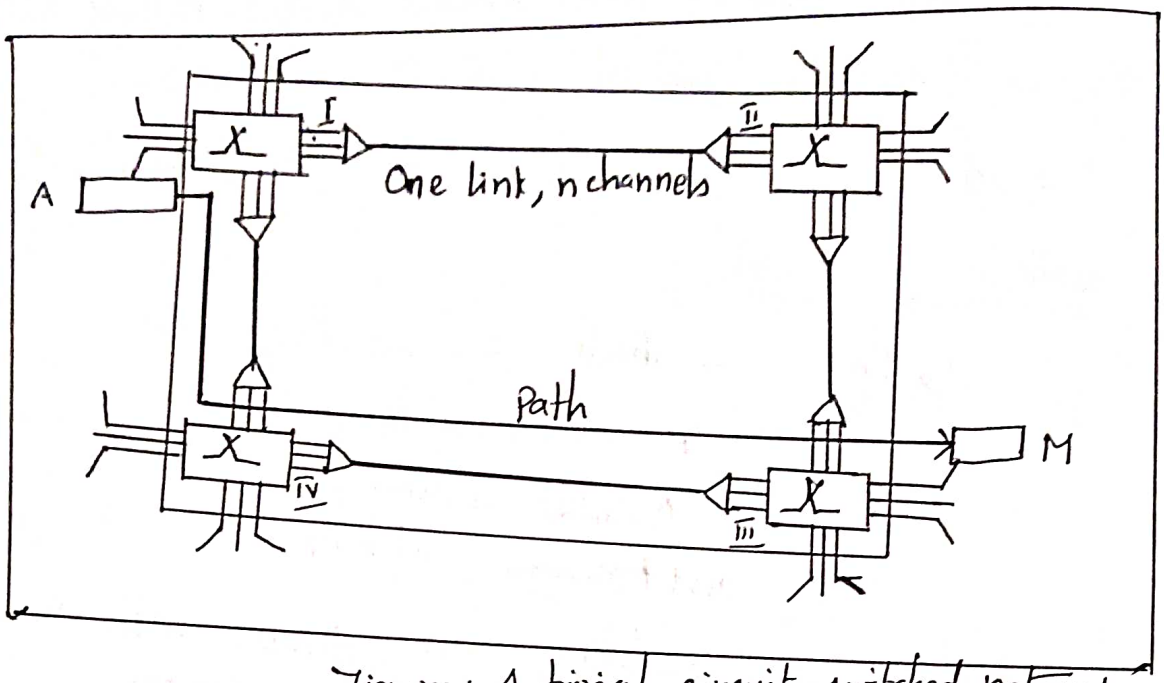


Figure: A trivial circuit switched network

↳ The end systems such as computers or telephones are directly connected to a switch.

↳ When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M iteself. This is called the setup phase.

↳ After the dedicated path made of connected circuits is established, the data transfer phase can take place.

↳ After all data have been transferred the circuits are torn down.

Three phases:

↳ The actual communication in a circuit switched network requires three phases.

1. Connection setup
2. data transfer

and 3. Connection teardown.

1) Setup phase:

↳ Before the communication, a dedicated circuit needs to be established.

↳ The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.

↳ When a system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I.

↳ Switch I find a channel between itself and switch IV that can be dedicated for this purpose.

↳ Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III.

↳ Switch III informs system M of system A's intention at this time.

↳ In the next step to making a connection, an acknowledgement from system M needs to be sent in the opposite direction to system A.

↳ Only after system A receives this acklowledgement is the connection established.

2) Data Transfer phase:

↳ After the establishment of the dedicated circuit, the two parties can transfer data.

3) Teardown phase:

↳ When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

1.9.2 Packet Switching:

↳ If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size.

↳ The size of the packet is determined by the network and the governing protocol.

↳ In packet switching, there is no resource allocation for a packet.

↳ Resources are allocated on demand.

↳ The allocation is done on the first come first served basis.

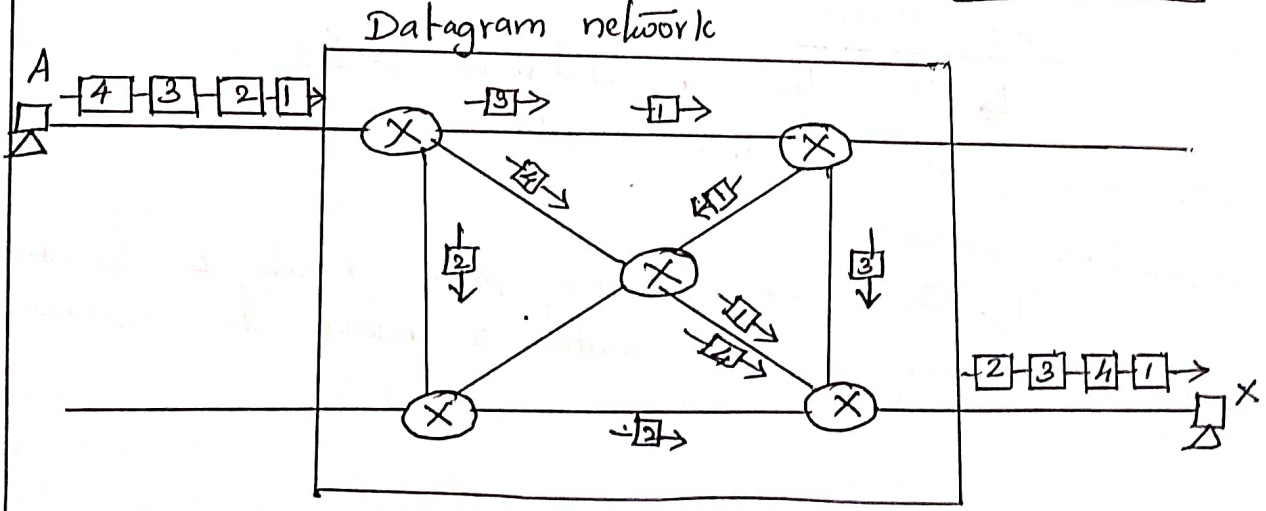
↳ There are two types of packet switched networks: datagram networks and virtual circuit networks.

Datagram networks:

↳ In a datagram network, each packet is treated independently of all others.

↳ Packets in this approach are referred to as datagrams.

↳ Datagram switching is normally done at the network layer.



↳ The figure shows how the datagram approach is used to deliver four packets from station A to station X.

↳ The switches in a datagram network are referred to as routers.

↳ All four packets belong to the same message, but may travel different paths to reach their destination.

↳ The datagrams arrive at their destination out of order with different delays between the packets.

↳ Packets may also be lost or dropped because of a lack of resources.

↳ In most protocols, it is the responsibility of an upper layer protocol to reorder the datagrams.

↳ The datagram networks are referred to as connectionless networks.

↳ There is no setup or teardown phase.

Routing table:

↳ Each switch has a routing table which is based on the destination address.

↳ The routing tables are dynamic and are updated periodically.

↳ The destination addresses and the corresponding forwarding output ports are recorded in the tables.

Destination Address: ↳ The datagram carries a header that contains, the destination address and it remains same during the entire journey of the packet.

Efficiency:

↳ The efficiency of a datagram network is better than that of a circuit switched network.

↳ Resources are allocated only when there are packets to be transferred.

Delay: There may be greater delay in a datagram network than in a virtual circuit network

Virtual Circuit Networks:

↳ A virtual circuit network is a cross between a circuit - switched network and a datagram network.

↳ It has some characteristics of both. They are

i) As in a circuit switched network, there are setup, data transfer and teardown phase.

ii) Resources can be allocated during the setup phase, as in a circuit switched network or on demand, as in a datagram network.

iii) As in a datagram network, data are packetized and each packet carries an address in the header.

iv) As in a circuit switched network, all packets follow the same path established during the connection.

v) A virtual circuit network is implemented in the DLL; a circuit switched network is implemented in the physical layer and a datagram network in the network layer.

Classification:

↳ Virtual Circuit Networks are again classified into two types. They are,

i) Switched VC – Different VC is provided between two users.

ii) Permanent VC – The same VC is provided between two users on a continuous basis.

Addressing:

↳ Two types of addressing

i) Global – used to create Virtual circuit Identifier (VCI)

ii) Local – Data transfer.

Virtual Circuit Identifier:

↳ The identifier is a small numba used by a frame between two switches.

↳ When a frame arrives at a switch, it has a VCI

↳ When it leaves, it has a different VCI

Three phases:

↳ Virtual circuit network consists of the following three phases.

i) Setup phase: The source and destination use their global addresses to help switches make table entries for the connection.

ii) Data transfer phase: Data transfer occurs between the two phases.

iii) Teardown phase: The source and destination inform the switches to delete the corresponding entry.

Efficiency:

↳ In virtual circuit switching, all packets belonging to the same source and destination travel the same path, but the packets may arrive at the destination with different delays.

↳ There is a big advantage, if the resource allocation is on demand.

UNIT-II DATA LINK LAYER & MEDIA ACCESS

Introduction - Link Layer Addressing - DLC Services - Data Link Layer Protocols - HDLC - PPP - Media Access Control - Wired LANs Ethernet - Wireless LANs - Introduction - IEEE 802.11 ; Bluetooth - Connecting Devices.

Introduction:

→ In OSI model, the data link layer is the second layer of bottom

→ It is responsible for transmitting frames from one node to next node.

→ The other responsibilities are,

(i) Framing

(ii) Physical Addressing

(iii) Flow Control

(iv) Error Control

(v) Medium Access Control.

Nodes and Links:

→ Communication at the data link layer is node to node.

→ Two categories,

(i) Point - to - Point Link

(ii) Broadcast Link.

Data Link Layer Services:

→ The data link layer is located between the physical and the network layers.

→ Two sublayers,

(i) Data Link Control (DLC)

(ii) Media Access Control (MAC)

Link-Layer Addressing:

→ A link layer address is sometimes called a link address sometimes a physical address and sometimes a MAC address

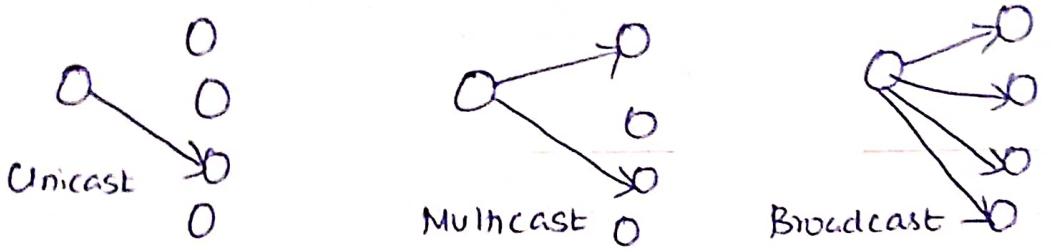
Types of Addresses:

→ three types

(i) Unicast Address

(ii) Multicast Address

(iii) Broadcast Address.



Address Resolution Protocol: (ARP):

→ ARP is the most important protocol in Data link Layer

→ ARP is a network layer protocol used to convert a IP address into MAC address.

→ Two types of ARP messages are,

(i) ARP request

(ii) ARP reply.

ARP Operation:

→ ARP maintains a cache table in which MAC addresses are mapped to IP addresses.

→ Source stores target Logical and physical address pair in its ARP table from ARP response.

→ Destination host constructs an ARP response packet.

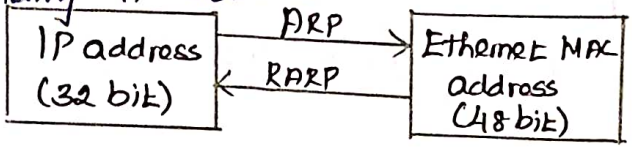
→ ARP response is unicast and sent back to source host.

ARP Packet:

Hardware Type		Protocol Type
Hardware Length	Protocol length	Operation Request 1, Reply 2
Source hardware Address		
Source Protocol Address		
Destination hardware Address		
Destination Protocol Address		

RARP – Reverse ARP:

→ allows a host to convert its MAC address to the corresponding IP address.



DLC Services:

→ The data link control (DLC) deals with procedures for communication between two adjacent nodes, node-to-node communication - no matter whether the link is dedicated or broadcast.

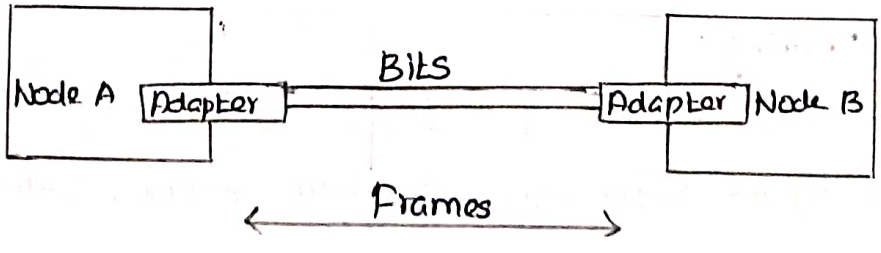
(1) Framing

(2) Flow Control

(3) Error Control.

Framing:

→ The data link layer packs the bits of a message into frames, so that each frame is distinguishable from another



Frame Size:

→ Frames can be fixed or variable size.

→ Frames of fixed size are called cells

→ variable size framing - to define the need of one frame and the bagining of next

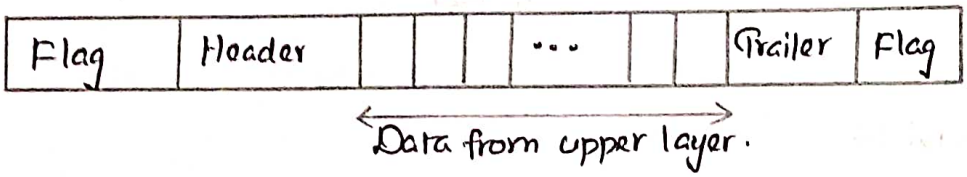
→ Two approaches

(1) character oriented Framing

(2) Bit oriented Framing.

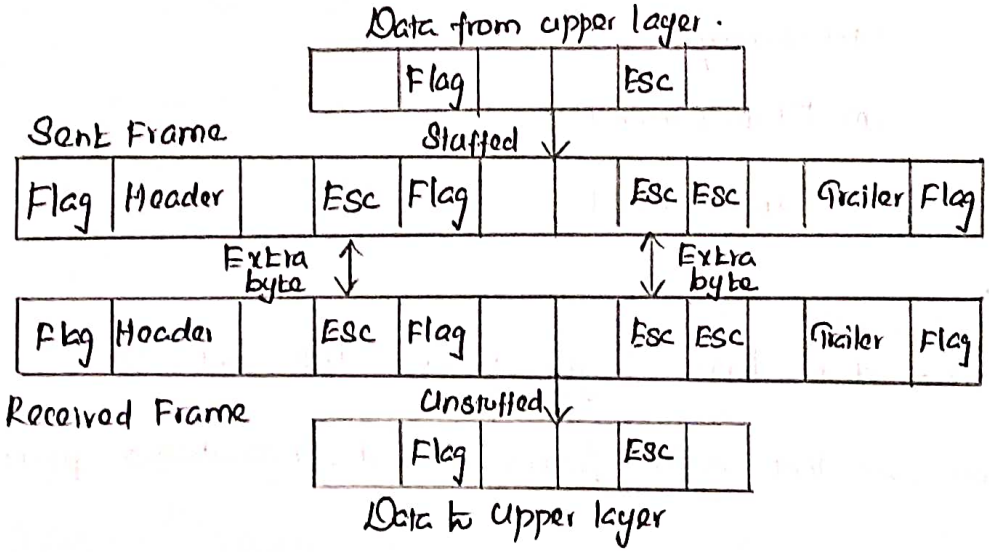
Character Oriented Framing:

→ data to be carried are 8 bit characters.



Byte Stuffing (or) Character stuffing

→ Byte stuffing is the process of adding one extra byte whenever there is a flag or escape character in the text.

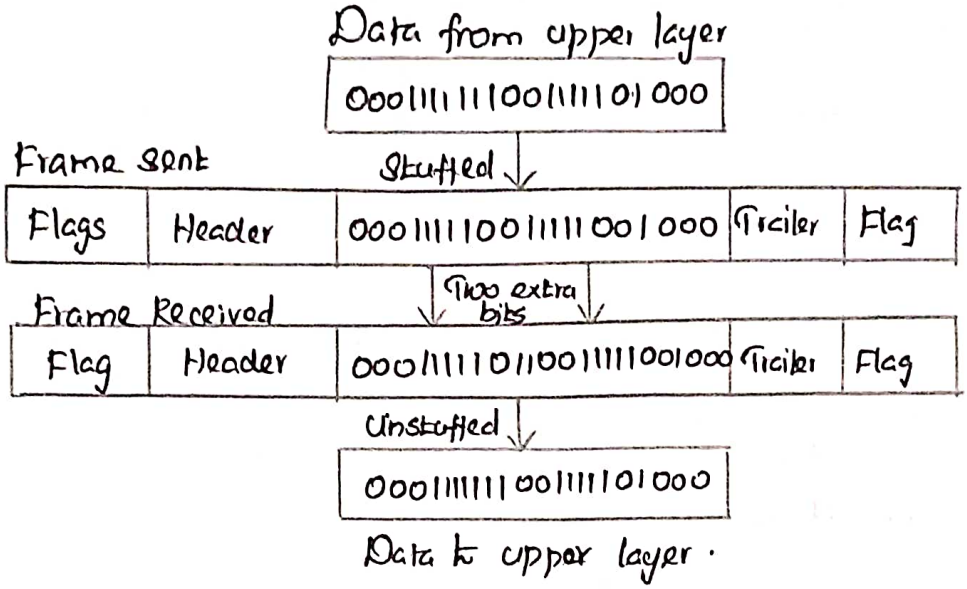


Bit-Oriented Framing:

→ The data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.

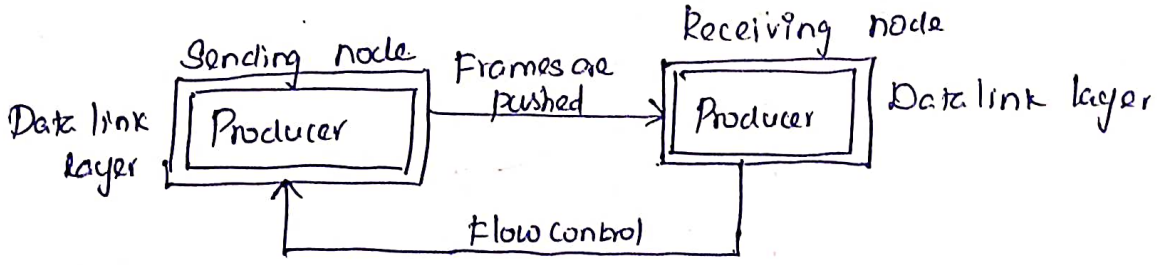
Bit Stuffing :

→ Is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.



Flow Control :

→ refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.



Two methods :

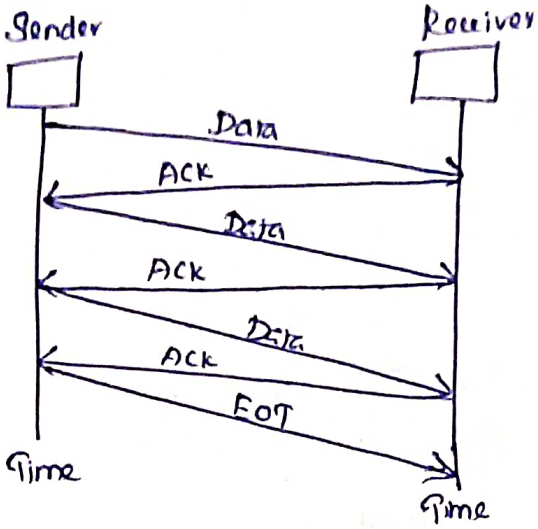
(a) Stop and Wait

(b) Sliding Window.

STOP - AND - WAIT :

→ The sender waits for an acknowledgment after every frame it sends.

→ When acknowledgment is received then next frame is sent.



→ The acknowledgment may not arrive because of the following three scenarios,

(i) Original frame is lost

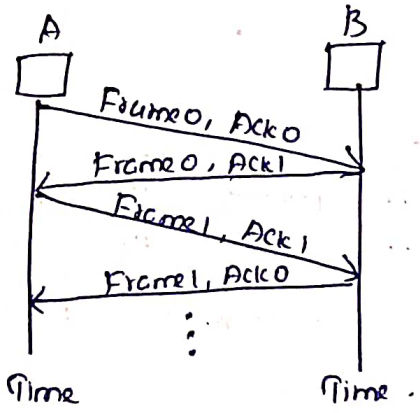
(ii) Ack is lost

(iii) Ack arrives after the timeout.

Piggybacking:

→ Piggybacking saves bandwidth.

→ A method to combine a data frame with Ack.



Sliding Window:

→ Is a method of flow control in which a sender can transmit the several frames before getting an acknowledgment.

→ refers to imaginary boxes at both sender and receiver end.

Error Control:

→ Data can be corrupted during transmission

→ For reliable communication errors must be detected and corrected.

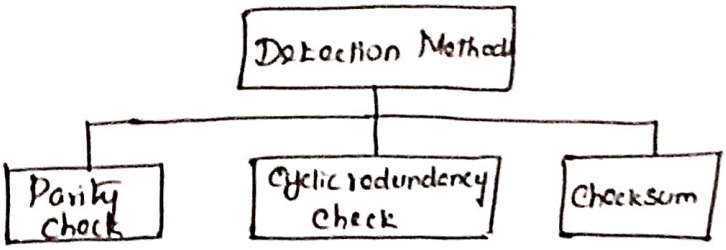
→ Error control is a technique of error detection and retransmission.

Types of Errors:

(i) Single bit Error

(ii) Burst Error.

Error Detection Techniques / Methods.



Parity Check:

→ One bit called parity bit is added to every data unit so that the total number of 1's is in the data unit becomes even or odd.

(i) Even Parity – Maintain even number of 1's

1011 → 10111

(ii) Odd Parity – Maintain odd number of 1's

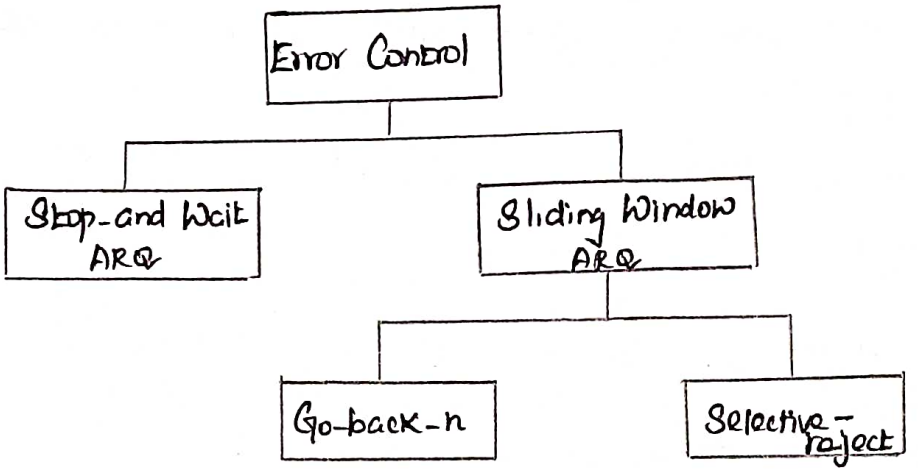
1011 → 10110

Cyclic Redundancy Check:

→ Cyclic code refers to encoding messages by adding a fixed length check value.

→ It analyse mathematically and particularly good at detecting common errors caused in transmission channels.

Categories of Error Control.



Stop and Wait ARQ:

→ Is a technique used to retransmit the data in case of damaged or lost frames.

→ Two possibilities,

(i) Damaged Frame

(ii) Lost Frame

Sliding Window ARQ:

→ Is a technique used for continuous transmission error control.

→ Two Protocols.

(i) Go back-n ARQ (ii) Selective Reject ARQ.

Go-back-N ARQ:

→ If one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Selective Reject ARQ:

→ In this only the frames are retransmitted for which negative acknowledgment (NAK) has been received.

Data-link layer Protocols:

→ Four protocols

(a) Simple Protocol

(b) Stop and Wait Protocol

(c) Go back N Protocol

(d) Selective Repeat Protocol.

Simple Protocol:

→ The data link layers of Sender and receiver provide transmission services for their network layers.

→ The data link layer at the receiver receives a frame from the link, extracts the packet from the frame and delivers the packet to its network layer.

Stop and Wait Protocol:

→ Is a technique used to retransmit the data in the case of damaged or lost frames.

→ Two possibilities

(a) Damaged Frame

(b) Lost Frame.

Go-back-N Protocol:

→ If one frame is lost or damaged then it retransmits all the frames after which it does not receive the positive ACK.

Selective Repeat Protocol:

→ In this only the frames are retransmitted for which negative acknowledgment (NAK) has been received.

High-level Data link Control (HDLC):

→ HDLC is a bit oriented Protocol.

→ HDLC is used for communication over point to point and multipoint links.

→ HDLC implements Stop-and-Wait Protocol.

HDLC Configurations and Transfer Modes:

→ Two common transfer modes

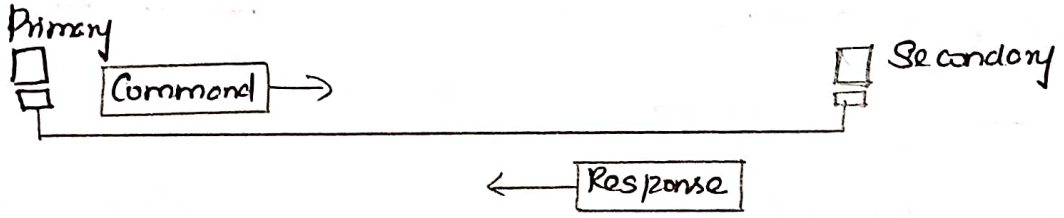
(i) Normal Response Mode (NRM)

(ii) Asynchronous balanced Mode (ABM)

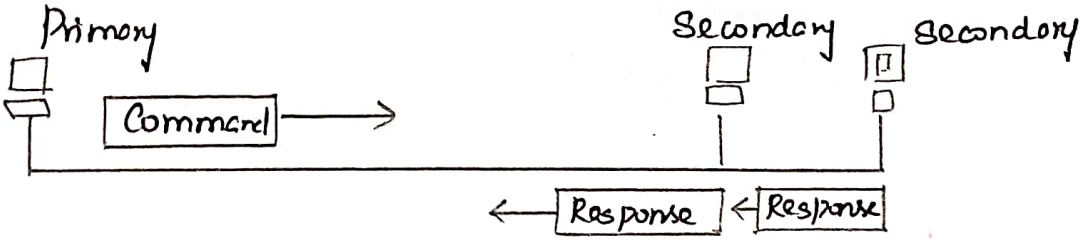
Normal Response Mode (NRM):

→ the station configuration is unbalanced.

→ one primary station and multiple secondary stations.



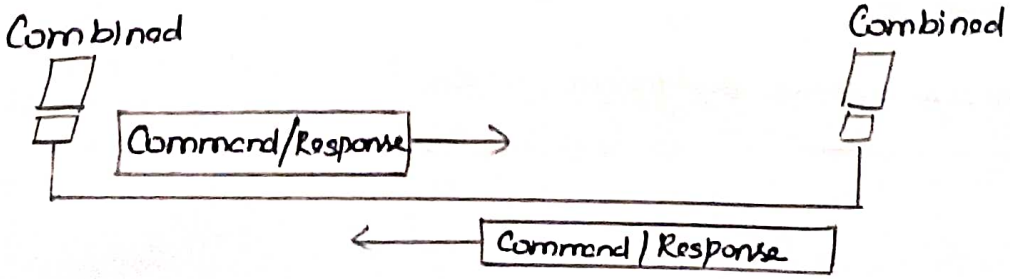
Point-to-Point.



Multipoint

Asynchronous Balanced Mode (ABM)

→ the link is point to point and each station can function as a primary and a secondary.



HDLC Frames:

→ three types of frames

(i) Information frames (I-frame) – Used to carry user data.

(ii) Supervisory frames (S-frame) – Used to carry control information

(iii) Unnumbered frames (U-frame) – reserved for system management

⇒ Six fields of HDLC:

(i) Beginning flag field

(ii) Address field

(iii) Control field

(iv) Information field

(v) Frame Check sequence field (FCS)

(vi) Ending flag field.

Point-To-Point Protocol (PPP)

→ PPP is a data link layer communications protocol used to establish a direct connection between two nodes.

→ It connects two routers directly without any host or any other networking device in between.

Services Provided by PPP:

(i) Defining the frame format.

(ii) Defining the procedure link between two points

(iii) Encapsulation of network layer.

(iv) Authentication rules

(v) Providing address for network communication

(vi) Providing Connections

(vii) Supporting network layer protocols.

PPP - Frame:

→ PPP is a byte oriented protocol where each field of the frame is composed of one or more bytes.

Flag	Address	Control	Protocol	Payload	Fcs	Flag

Byte Stuffing in PPP Frame:

→ Byte stuffing is used in PPP payload field whenever the flag sequence appears in the message.

Transition Phases in PPP:

(1) Dead
(2) Establish
(3) Authenticate
(4) Network
(5) Open
(6) Terminate.

Components / Protocols of PPP:

(1) Link Control Protocol (LCP)
(2) Authentication Protocols (AP)
(3) Network Control Protocols (NCP)

LCP ⇒ establishing, configuring, testing, maintaining and terminating links for transmission

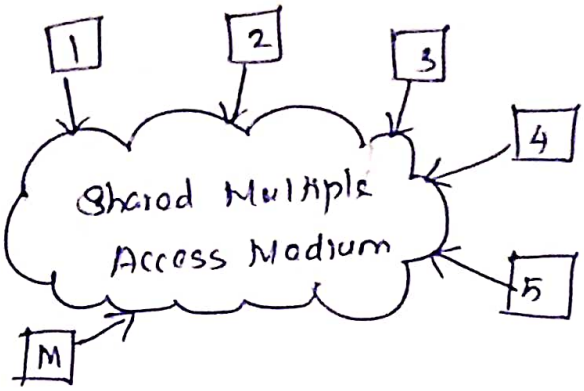
AP ⇒ Validating the identity of user
(1) Password Authentication Protocol (PAP)
(2) Challenge Handshake Authentication Protocol (CHAP)

NCP ⇒ multiple network layer protocol.

Media Access Control (MAC):

→ MAC defines rules for orderly access to the shared medium.

→ When two or more nodes transmit data at same time, their frames will collide and link bandwidth is wasted during collision.



Issues Involved in MAC:

(i) Where the control is exercised

(ii) How the control is exercised.

Goals of MAC:

(i) Fairness in sharing

(ii) Efficient sharing of bandwidth

(iii) Need to avoid packet collisions at the receiver due to interference.

MAC Management:

(i) Medium Allocation (collision avoidance)

(ii) Contension Resolution (collision handling)

MAC Types:

(i) Round Robin

(ii) Reservation

(iii) Contension (Random Access)

Mechanisms used:

(i) Wired Networks

→ CSMA/CD – Carrier Sense Multiple Access / Collision Detection.

(ii) Wireless Networks.

→ CSMA/CA – Carrier Sense Multiple Access / Collision Avoidance.

Carrier Sense Multiple Access / Collision Detection (CSMA/CD)

Carrier Sense:

→ In CSMA/CD means that all the nodes sense the medium to check whether it is idle or busy.

Collision Detect:

→ means that a node listens as it transmits and can therefore detect when a frame it is transmitting has collided with a frame transmitted by another node.

Transmitter Algorithm in CSMA/CD:

→ defines the procedure for a node that senses a busy medium.

→ Three types of transmitter Algorithm

(i) Non Persistent Strategy

(ii) Persistent Strategy – 1-Persistent, P-Persistent.

Non Persistent Strategy:

→ a station that has a frame to send senses the line

→ the line is idle, it sends immediately

→ If the line is not idle, it waits a random amount of time and then senses the line again.

Persistent Strategy:

1 -Persistent:

→ Simple and straightforward.

→ the station finds the line idle, its sends the frame immediately.

P- Persistent:

→ the station finds the line idle it follows these steps

(i) With probability p, the station sends its frame.

(ii) With probability $q = 1-p$, the station waits for the begining of next time slot and checks the line again.

Exponential Backoff.

→ Each time it tries to transmit but fails, the adapter doubles the amount of time it waits before trying again.

→ The strategy of doubling the delay interval between each retransmission attempt is a general technique known as exponential back-off.

Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)

→ Invented for wireless networks.

→ Wireless protocol would follow exactly the same algorithm as the Ethernet - wait until the link becomes idle before transmitting and back-off should a collision occur.

→ Collisions are avoided through the use of CSMA/CA's in three strategies,

(i) Interframe Space (IFS)

(ii) Contension Window

(iii) Acknowledgment.

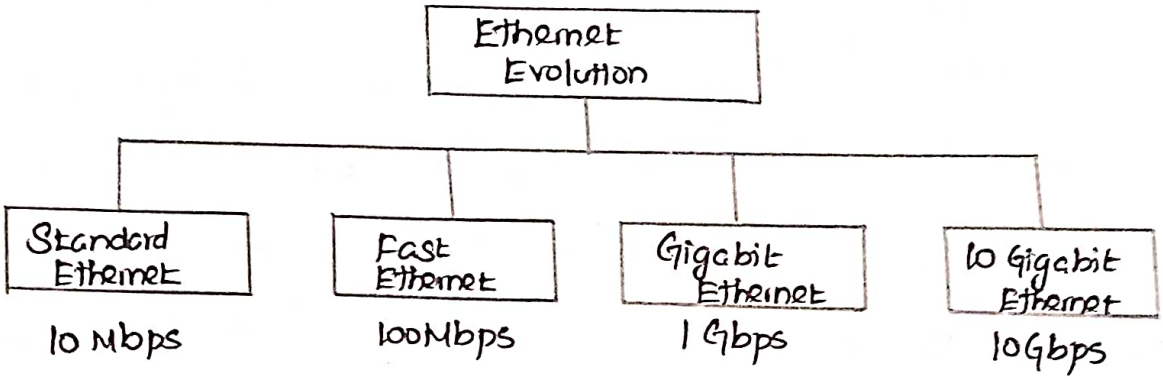
Wired LAN: Ethernet (IEEE 802.3)

→ IEEE controls the Ethernet standards.

→ The Ethernet is multiple-access networks that is set of nodes send and receive frames over a shared link.

→ Ethernet uses the CSMA/CD mechanism.

Evolution of Ethernet:



Standard Ethernet (10Mbps):

→ data rate of 10Mbps as the standard Ethernet

→ Ethernet types are

(i) 10Base5 : Thick Ethernet

(ii) 10Base2 : Thin Ethernet

(iii) 10Base T : Twisted-Pair Ethernet

(iv) 10BaseF : Fiber Ethernet

Fast Ethernet (100Mbps):

→ provides transmission speeds up to 100 megabits per second. and is typically used for LAN backbone systems.

(i) 100 BASE-TX

(ii) 100 BASE-T4

(iii) 100 BASE-FX

Gigabit Ethernet (1 Gbps):

→ upgrades the data rate to 1 Gbps (1000 Mbps)

→ categorized as two-wire or four-wire implementations.

⇒ two wire implementation use fibre optic cable

1000 Base-SX – shortwave

1000 Base-LX – Long wave.

10 Gigabit Ethernet (10 Gbps):

→ upcoming Ethernet technology that transmits at 10 Gbps.

→ enables a network technology to be used in LAN, MAN and WAN architectures.

(i) 10G Base-SR

(ii) 10G Base-LR

(iii) 10G Base-EW

(iv) 10G Base-X4

Collision Detection in Ethernet:

→ Ethernet supports collision detection, senders are able to determine a collision

→ 32-bit jamming sequence and 64 bit preamble. These 96 bits are sometimes called Runt Frame.

Frame Format of Ethernet:

64	48	48	16		12
Preamble	Dest addr	Src addr	Type	Body	CRC

Advantages of Ethernet:

(i) It is extremely easy to administer and maintain

(ii) It is inexpensive. Cable is cheap.

Wireless LAN (IEEE 802.11)

→ Wireless LAN can be found on college campuses, in office buildings and in many public areas.

Advantages of WLAN / 802.11

(a) Flexibility

(b) Planning

(c) Design

(d) Robustness.

Disadvantages of WLAN / 802.11

(a) Quality of service

(b) Cost

(c) Proprietary solution

(d) Restriction

(e) Safety and security

Technology used in WLAN / 802.11.

→ WLAN uses spread spectrum technology

→ Two types

(a) Frequency Hopping Spread Spectrum (FHSS)

(b) Direct Sequence Spread Spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS):

→ Involves transmitting the signal over a random sequence of frequencies.

→ The random sequence of frequencies is computed by a pseudorandom number generator.

→ Able to hop frequencies in sync with the transmitter to correctly receive the frame.

Direct Sequence Spread Spectrum (DSSS)

→ DSS takes a user data stream and performs an XOR operation with a pseudo random number.

→ this pseudo random number is called as chipping sequence

Topology in WLAN / 802.11

→ two topologies

(i) Infra structure Network Topology

(ii) Ad Hoc Network Topology.

Architecture of WLAN / 802.11

→ two kinds of services.

(i) Basic Service Set (BSS)

(ii) Extended Service Set (ESS)

Basic Service Set (BSS)

→ BSS is made of stationary or mobile wireless stations and an optional central base station known as the access point (AP)

Extended Service Set (ESS):

→ the mobile stations are normal stations inside a BSS

→ the stationary stations are AP stations that are part of a wired LAN.

Station Types:

→ three types of stations

(i) No transition

(ii) BSS transition

(iii) ESS transition.

Collision Avoidance in WLAN / 802.11

→ wait until the link becomes idle before transmitting and back off should a collision.

(i) Hidden Node problem

(ii) Exposed Node problem.

Multiple Access with Collision Avoidance (MACA):

→ MACA is used to avoid collisions caused by the hidden terminal problem and exposed terminal problem.

→ MACA uses short signalling packets called RTS (Request To-send) and CTS (Clear-To-Send) for collision avoidance.

Distribution System in WLAN / 802.11:

→ In wireless network nodes can move freely. Some nodes are allowed to roam and some are connected to a wired network infrastructure called Access Points (AP), and they are connected to each other by distribution system.

Scanning Process in Distribution System:

→ The technique for selecting an access point called scanning.

→ It involves four steps.

(i) The node sends a Probe request frame.

(ii) All AP's within reach reply with a probe Response frame.

(iii) The node selects one of the access points and sends that AP an association request frame.

→ Two types of scanning.

(i) Active scanning → node is actively searching for access point

(ii) Passive Scanning → APs periodically send a Beacon frame to nodes

Frame Format of WLAN:

16	16	48	48	48	16	48	0-18496	32
Control	Duration	Addr1	Addr2	Addr3	SeqCtrl	Addr4	PayLoad	CRC

→ The Control field contains three fields.

(i) Type field

(ii) To DS

(iii) From DS

Bluetooth (IEEE 802.15.1)

→ A bluetooth is an adhoc network, which means that the network is formed spontaneously.

→ The standard defines wireless personal Area Network (PAN)

→ Bluetooth supports two kinds of links,

(a) Asynchronous Connectionless (ACL) Links - for data

(b) Synchronous Connection Oriented (SCO) Links - for audio/voice

Bluetooth Architecture:

→ two types of networks

(a) Piconet (b) Scatternet

Piconet:

→ The basic bluetooth configuration is called a piconet.

→ A piconet is a collection of eight bluetooth devices which are synchronized.

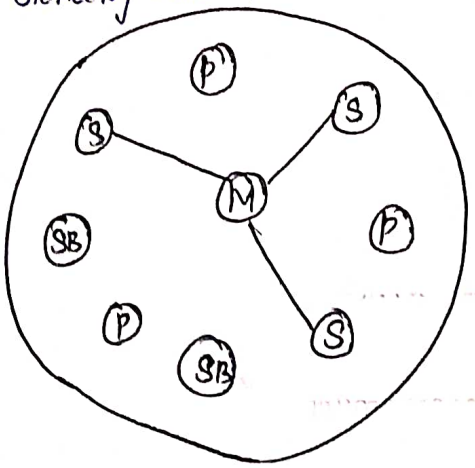
→ The slaves do not communicate directly with each other.

→ three types/states.

(a) Active Device/state - 3 bit address (AMA)

(b) Parked Device/state - 8 bit parked member address (PMA)

(c) Stand by Device/state - do not need an address.

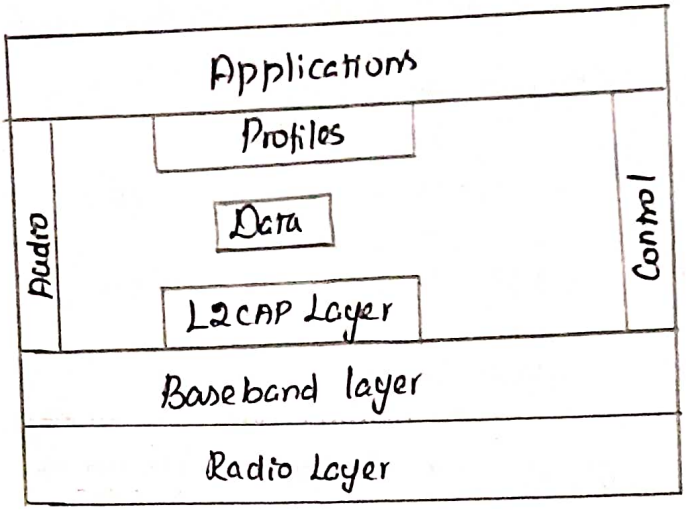


Scatternet:

→ Piconets can be combined to form what is called scatternet

→ Many piconets with overlapping coverage can exist simultaneously called scatternet.

Bluetooth Layers:



Radio Layer:

→ Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks.

Baseband Layer:

→ The primary and secondary stations communicate with each other using time slots. The length of time slot is exactly 625 μs.

L2CAP:

→ Logical link Control and Adaptation Protocol.

→ It is used for exchange the data on an ACL Link.

→ The L2CAP functions are,

(i) Multiplexing

(ii) Segmentation

(iii) Reassembly

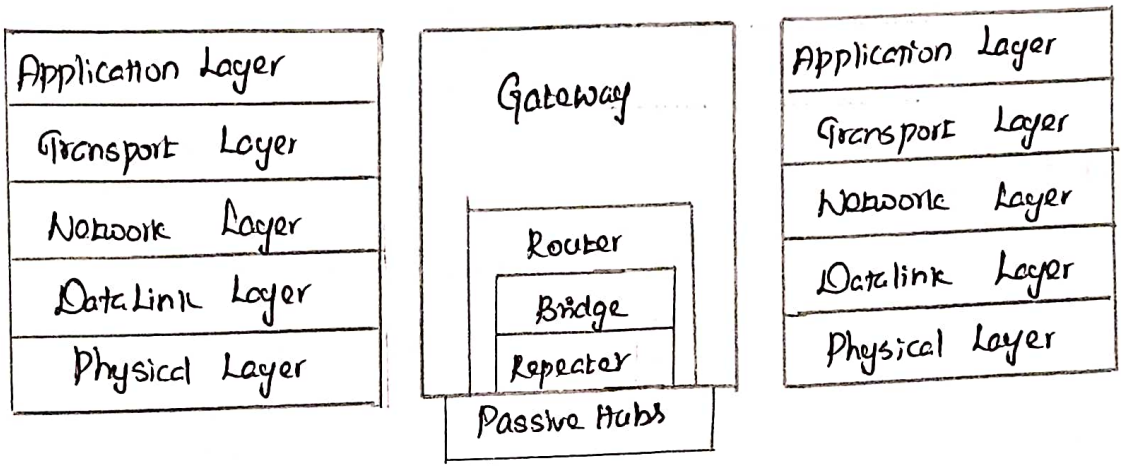
(iv) Quality of service

(v) Group management.

Connecting Devices:

→ Used to connect host together to make a network or to connect networks together to make an internet.

→ Connecting devices can operate in different layers of the Internet model.



1) Devices which operate below the physical layer – Passive hub.

2) Devices which operate at the physical Layer – Repeater.

3) Devices which operate at the physical and data link layers – Bridge

4) Devices which operate at the physical layer, data link layer and network layer – Router.

5) Devices which operate at all five layers – Gateway.

Hubs:

→ Several networks need a central location to connect media segments together. These Central locations are called as hubs.

→ three types.

(a) Passive hub

(b) Active hub

(c) Intelligent hub

Repeaters:

→ repeaters receives the signal and it regenerates the signal in original bit pattern before the signal gets too weak or corrupted

→ A repeater has no filtering capability.

Bridges:

→ Bridges operate in physical layer as well as data link layer

→ Bridges are used to connect two or LANS working on the same protocol.

→ three types

(i) Transparent Bridges

(ii) Source Routing Bridges

(iii) Translation Bridges.

Switches:

→ Switch is a small hardware device which is used to join multiple computers together one local area network.

→ Switch is a multi port bridge with a buffer.

→ two types

(i) Two Layer switch (ii) Three Layer Switch.

Routers:

→ a router is a device like a switch that routes data packets based on their IP addresses.

→ A router is an internetworking device

Gateway:

→ is a device which operates in all five layers of the Internet or seven layers of OSI model.

→ It is usually a combination of hardware and software.

→ Gateway connects two independent networks.

Brouter:

→ Brouter is a hybrid device.

→ Brouter is a combination of Bridge and router.

→ Functions as a bridge for non routable protocols and a router for routable protocols.

Unit III NETWORK LAYER

Network Layer Services – Packet Switching – Performance – IPV4 Addresses – Forwarding of IP Packets – Network Layer Protocols: IP, ICMPV4 – Unicast Routing Algorithms – Protocols – Multicasting Basics – IPV6 Addressing – IPV6 Protocol.

Network Layer Services:

→ It provides services to the transport layer and receives services from the data link layer.

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

Services Provided by Network Layer:

(i) Packetizing
(ii) Routing and Forwarding
(iii) Error control
(iv) Flow control
(v) Congestion control
(vi) Security.

Packetizing:

→ Encapsulating the payload in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination.

Routing and Forwarding:

Routing:

→ Routing is the concept of applying strategies and running routing protocols to create the decision making tables for each router.

Forwarding:

→ can be defined as the action applied by each router when a packet arrives at one of its interfaces.

Error Control:

→ The network layer in the internet does not directly provide error control.

→ It adds a checksum field to the datagram to control any corruption in the header but not in whole datagram.

Flow Control:

→ Flow control regulates the amount of data a source can send without overwhelming the receiver.

→ The network layer in the internet, however, does not directly provide any flow control.

Congestion Control:

→ Congestion in the network layer is a situation in which too many datagrams are present in the area of internet.

Security:

→ To provide security for a connectionless network layer, we need to have another virtual level that changes the connectionless service to a connection oriented service. The virtual layer is called as IPSec (IP security).

Network Layer Performance:

→ The performance can be measured by,

(i) Delay (ii) Throughput (iii) Packet loss

→ Congestion control is an issue that can improve the performance

Delay:

→ A packet from its source to destination encounters delays.

→ Four types

(i) Transmission Delay (ii) Propagation Delay.

(iii) Processing Delay (iv) Queuing Delay.

Transmission Delay:

→ A source host or a router cannot send a packet instantaneously

$Delay_{tr}$ = (Packet length) / (Transmission rate)

Propagation Delay:

→ is the time it takes for a bit to travel from point A to point B in the transmission media.

$Delay_{pg}$ = (Distance) / (Propagation speed)

Processing Delay:

→ The processing delay may be different for each packet but normally is calculated as an average.

$Delay_{pr}$ = Time required to process a packet in router or a destination host

Queuing Delay:

→ The queuing delay for a packet in a router is measured as the time a packet waits in the input queue and output

queue of a router.

$Delay_{qu}$ = The time a packet waits in input and output queues in a router.

Total Delay:

→ The total delay of a packet can be calculated if we know the number of routers n, in the whole path.

$$\text{Total Delay} = (n+1)(Delay_{tr} + Delay_{pg} + Delay_{pr}) + (n)(Delay_{qu})$$

Throughput:

→ is defined as the number of bits passing through th point in a second, which is actually the transmission rate of data at that point.

$$\text{Throughput} = \text{minimum}(TR_1, TR_2, \ldots TR_n)$$

Packet Loss:

→ a router has an input buffer with a limited size.

→ the packet needs to be resend, which in turn may create overflow and cause more packet loss.

Congestion Control:

→ two issues

(i) Throughput (ii) Delay.

Based on Delay:

→ The minimum delay is composed of propagation delay and processing delay both of which are eligible.

Based on Throughput:

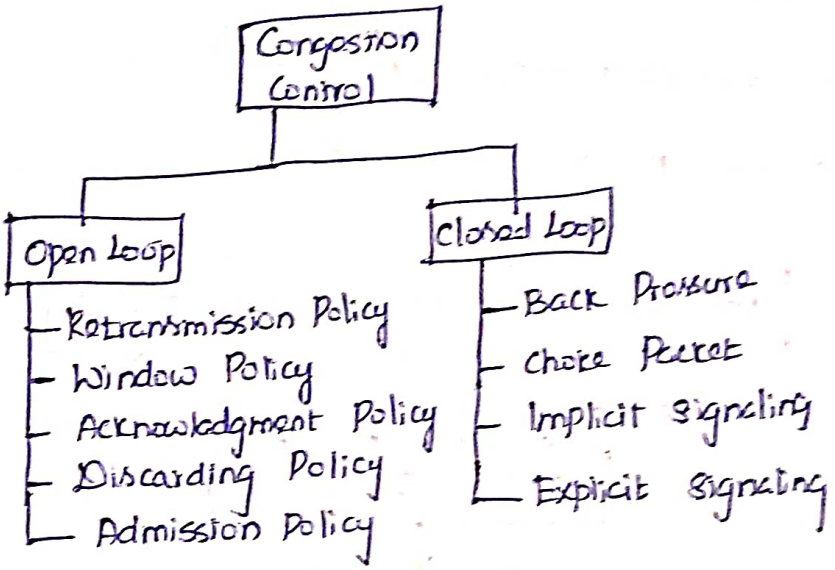
→ to remain constant after the load reaches the capacity but instead the throughput declines sharply.

Congestion Control Mechanisms:

→ to improve performance.

(i) Open loop Congestion Control (Prevention)

(ii) Closed loop Congestion Control (removal)



IPv4 Addresses:

→ IPv4 addresses are unique in the sense that each address define one, and only one connection to the internet.

→ If a device has two connections to the internet via two networks, it has two IPv4 addresses

→ IPv4 addresses are universal, in the sense that the addressing system must be accepted by any host that wants to be connected to the internet.

IPV4 Address Space:

→ An address space is the total number of addresses used by the protocol.

→ 4 billion devices could be connected to the internet.

→ IPV4 uses 32 bit addresses.

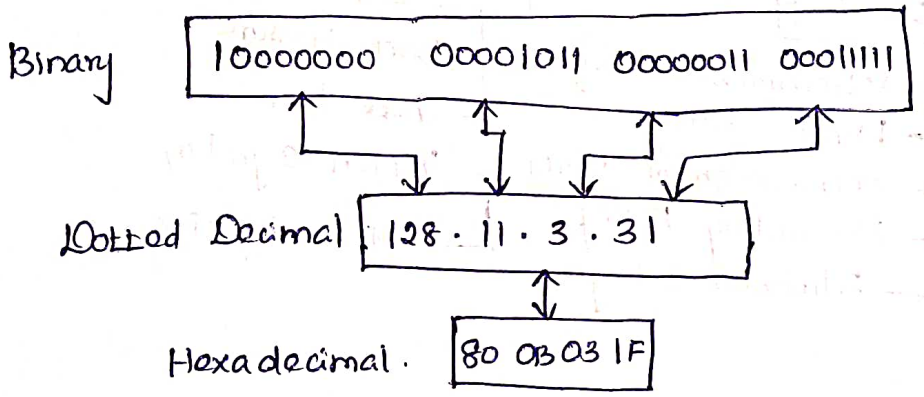
IPV4 Address Notation:

→ three common Notations.

(1) Binary Notation (Base 2)

(2) Dotted Decimal Notation (base 256)

(3) Hexadecimal notation (base 16)



Binary Notation:

→ an IPV4 address is displayed as 32 bits. To make the address more readable one or more spaces are usually inserted between bytes (8 bits)

Dotted Decimal Notation:

→ IPV4 addresses are usually written in decimal form with a decimal point separating the bytes. Each number in the dotted decimal notation is between 0 and 255

Hexadecimal notation:

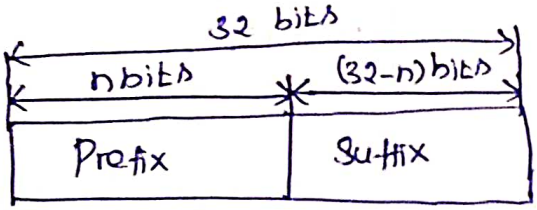
→ Each hexadecimal digit is equivalent to four bits. This means that a 32 bit address has 8 hexadecimal digits. This is often used in network programming.

Hierarchy in IPV4 Addressing:

→ A 32 bit IPV4 address is also hierarchical but divided only into two parts.

→ The first part of the address called the prefix, defines the network (NOT ID), the second part of the address called the suffix defines the node (HOST ID)

→ The prefix length is n bits and the suffix length is (32-n) bits.



Categories of IPV4 Addressing:

→ two categories.

(1) Classfull Addressing

(2) classless Addressing

Classful Addressing:

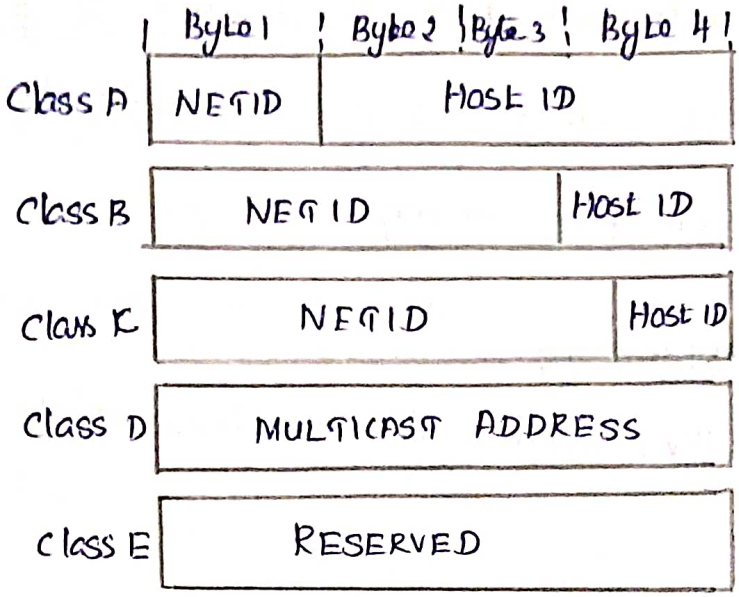
→ An IPV4 address is 32 bit long (4 bytes)

→ An IPV4 address is divided into two subclasses.

(1) Class A (2) Class C (3) class E

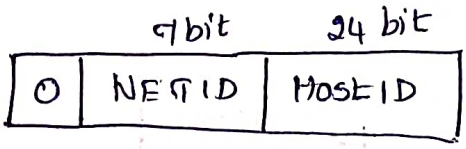
(2) Class B (2) Class D

Classful Addressing:



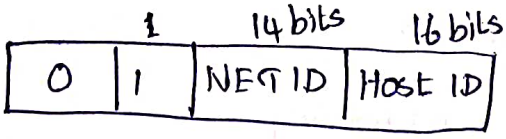
Class A:

→ In class A, an IP address is assigned to those networks that contain a large number of hosts.



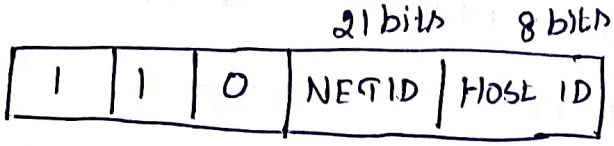
Class B:

→ In class B an IP address is assigned to those networks that range from small sized to large sized networks.



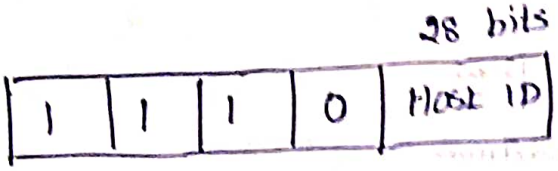
Class C:

→ In class C, an IP address is assigned to only small sized networks.



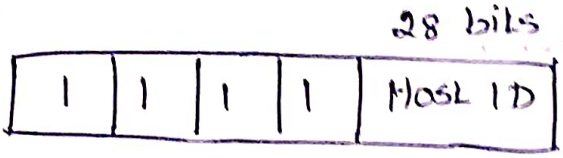
Class D:

→ In class D, an IP address is reserved for multicast addresses.



Class E:

→ In Class E, an IP address is used for the future use or for the research and development purposes.



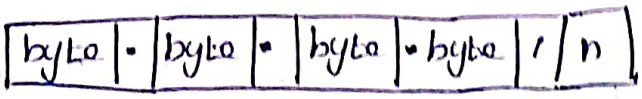
Classless Addressing:

→ In classless Addressing variable length blocks are used that belong to no classes.

→ The prefix length in classless addressing is variable.

Notation used in classless Addressing:

→ is formally referred to as slash notation and formally as classless inter domain routing or CIDR.



⇒ For example,

192.168.100.14/24

IP address – 192.168.100.14

Its Subnet mask – 255.255.255.0, which has 24 leading 1-bits

Address Aggregation:

→ One of advantage of CIDR strategy is address aggregation.

→ ICANN assigns a large block of addresses to an ISP.

Special Addresses in IPv4:

(i) this host address

(ii) Limited broadcast address.

(iii) Loop back Address.

(iv) Private address

(v) Multicast address.

This host address:

→ The only address in the block 0.0.0.0/32 is called this-host address.

Limited Broadcast Address:

→ The only address in the block 255.255.255.255/32 is called limited Broadcast address.

Loop back Address:

→ The block 127.0.0.0/8 is called the loop back addre..

Private Addresses:

→ Four blocks are assigned to Private addresses

(i) 10.0.0.0/8 (ii) 172.16.0.0/12

(iii) 192.168.0.0/16 (iv) 169.254.0.0/16

Multicast Addresses:

→ The block 224.0.0.0/4 is reserved for multicast addresses.

DHCP

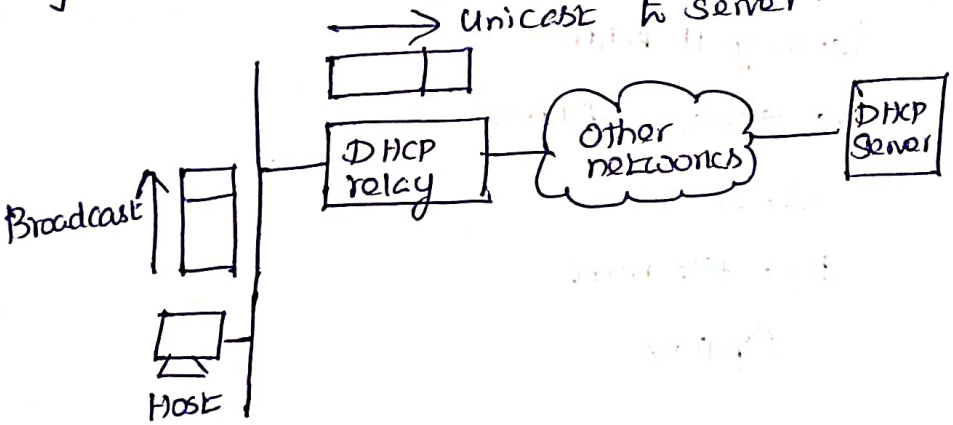
→ Dynamic Host Configuration Protocol.

→ Is used to simplify the installation and maintenance of networked computers.

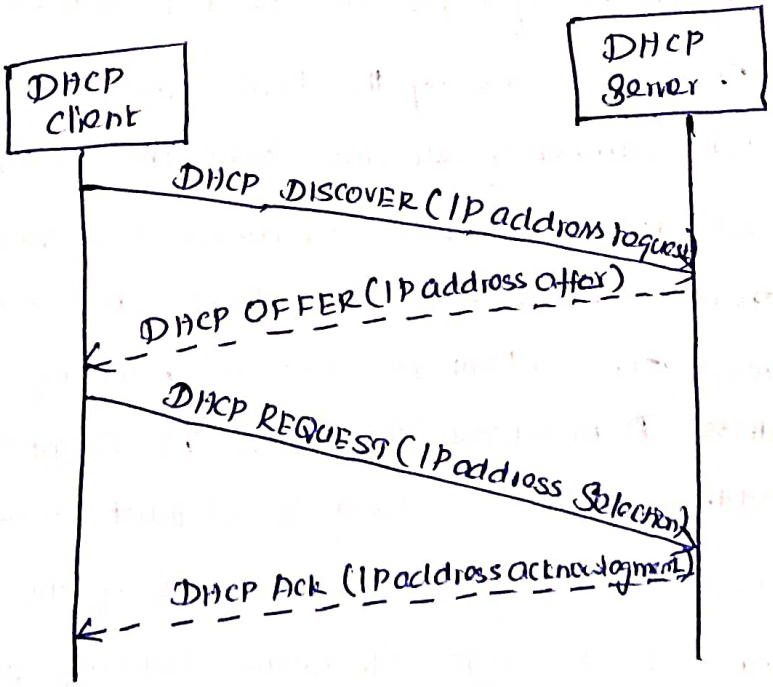
→ DHCP is derived from an earlier protocol called BOOTP.

→ DHCP is based on Client/Server Model.

→ DHCP Server can function just as a centralized repository for host configuration information.



→ DHCP relay agent is configured with the IP address of the DHCP server.



DHCP Message Format:

→ A DHCP packet is actually sent using a protocol called the User Datagram Protocol (UDP)

Opcode	Htype	Hlen	Hcount
Transaction ID			
Time Elapsed	Flags		
Client IP Address			
Your IP Address			
Server IP Address			
Gateway IP Address			
Client Hardware Address			
Server Name			
Boot file name			
Options			

Opcode: Operation Code, request(1) or reply(2)

Htype: Hardware type (Ethernet, ...)

Hlen: Length of hardware address

Hcount: Maximum no. of hops the packet can travel.

TransactionID: An integer set by the client and repeated by the server.

Time Elapsed: The number of seconds since the client started to boot.

Flags: First bit defines unicast(0), or multicast(1), other 15 bits not used.

Client IP Address: Set to 0 if the client does not know it.

Your IP Address: The client IP address sent by the server.

Server IP Address: A broadcast IP address if client does not know it.

Gateway IP Address: The address of default router.

Server name: A 64 byte domain name of the server.

Boot file Name: A 128 byte file name holding extra information.

Options: A 64 byte field with dual purpose described in text.

Network Address Translation (NAT)

→ A technology that can provide the mapping between the private and universal addresses, and at the same time support virtual private network is called as Network Address Translation.

→ The private network uses private addresses.

Types of NAT:

→ two types

(i) One-to-One translation of IP addresses

(ii) One-to-Many translation of IP addresses.

Address Translation:

→ All of the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address.

→ All incoming packets also pass through the NAT router, which replaces the destination address in the packet, with the appropriate private address.

Translation Table:

→ may be tens or hundreds of private IP addresses, each belonging to the one specific host.

→ The problem arises when we want to translate the source address to an external address. This is solved if the NAT router has a translation table.

Translation with two columns:

→ has only two columns, the private address and the external address.

Private Address	External Address
172.18.3.1	25.8.3.2
172.18.3.2	25.8.3.2
⋮	⋮

Translation with Five Columns:

→ a many to many relationship between private network host and external server programs, we need more information in the translation table.

Private Address	Private Port	External Address	External Port	Transport Protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
⋮	⋮	⋮	⋮	⋮

Forwarding of IP Packets:

→ Forwarding means to deliver the packet to the next hop

→ When IP is used as a connectionless protocol, forwarding is based on the destination address of the IP datagram.

→ When the IP is used as a connection oriented protocol forwarding is based on the label attached to an IP datagram.

Forwarding Based on Destination Address:

→ This is a traditional approach

→ forwarding requires a host or a router to have a forwarding table.

→ When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the next hop to deliver the packet to.

Forwarding Algorithm:

if (NetworkNum of destination = NetworkNum of one of my interfaces) then

deliver packet to destination over that interface

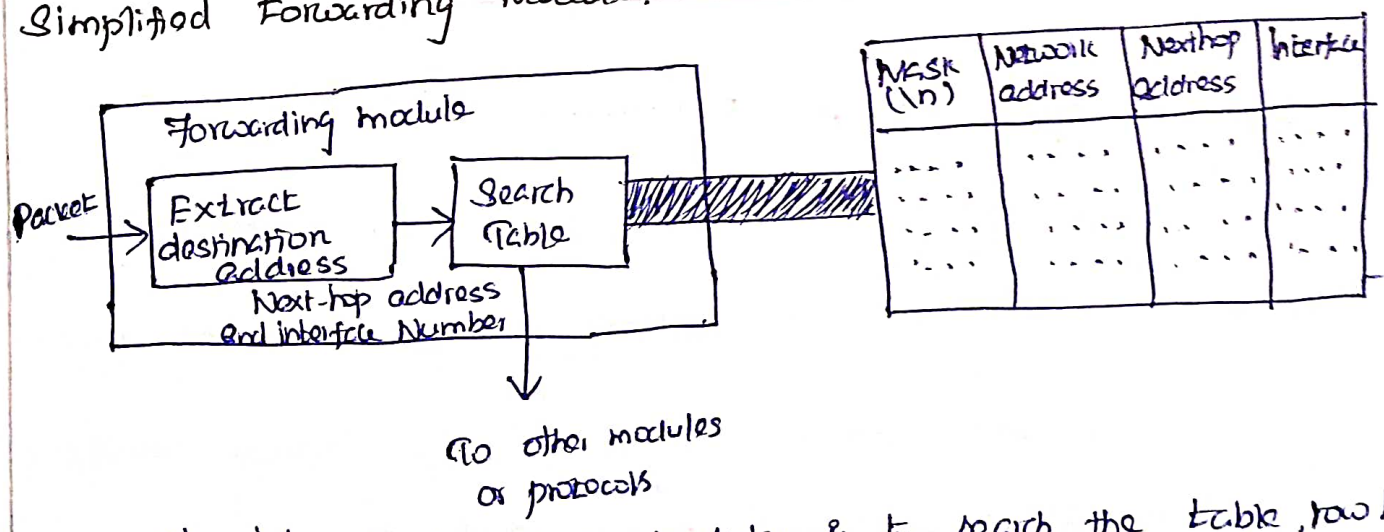
else
if (NetworkNum of destination is in my forwarding table) then

deliver packet to Nexthop router

else

deliver packet to default router.

Simplified Forwarding Module:



→ The job of forwarding module is to search the table, row by row.

→ Routing in classless addressing uses another principle longest mask matching.

Forwarding Based on Label:

→ In a connection oriented network, a switch packet based on the label attached to the packet.

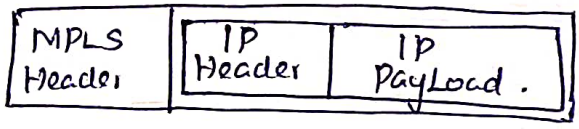
→ Routing is normally based on searching the contents of a table, switching can be done by accessing a table using an index.

→ In other words, routing involves searching, switching involves accessing.

Multi-Protocol Label Switching (MPLS)

→ In this some conventional routers, in the internet can be replaced by MPLS routers, which can behave like a router and a switch.

→ When behaving like a router, MPLS can forward the packet based on the destination address, when behaving like a switch it can forward a packet based on the label.



Network Layer Protocols : IP, ICMPV4.

→ The main internet protocol is responsible for packetizing, forwarding and delivery of a packet at the network layer.

→ The Internet Control Message Protocol version 4 (ICMPv4) helps IPV4 to handle some errors that may occur in the network layer delivery.

IP- Internet Protocol:

→ The Internet Protocol is the key tool used today to build scalable, heterogenous internetworks.

→ IP runs on all the nodes in a collection of networks.

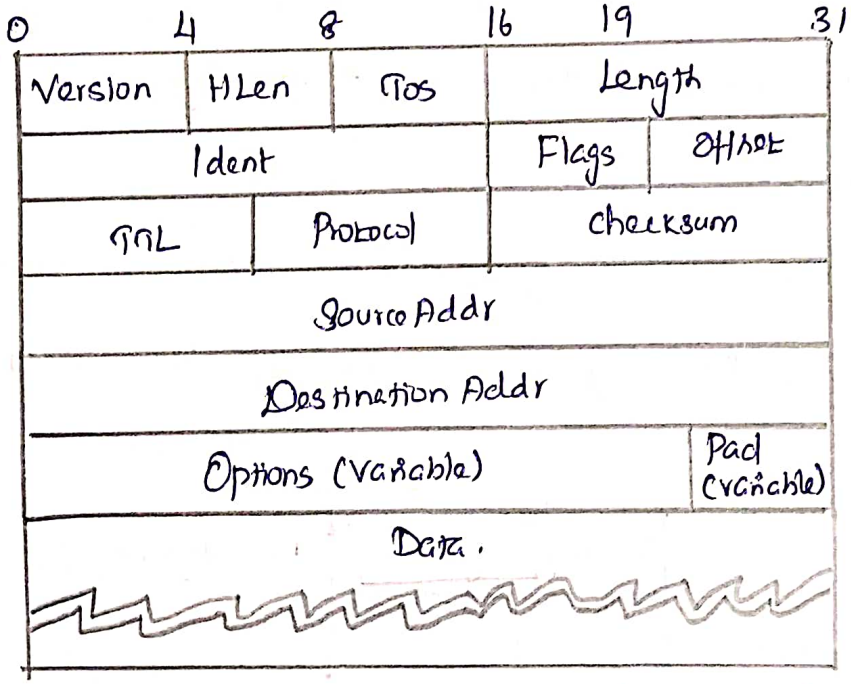
IP Service Model:

→ two parts.

A Global Addressing scheme: — Which provides a way to identify all hosts in the internetwork.

A Datagram Delivery model: — A connectionless model of data delivery.

IP Packet format / IP Datagram format:



Version: — Two versions, IPv4 and IPv6

HLen: Specifies the length of header.

TOS: Types of service — Precedence, Delay, Throughput and Reliability.

length: maximum size is 65535 (2^{16}) bytes.

Ident: Identifies the packet sequence number.

Flags : If a packet is fragmented, this flag value is 1, if not flag value is 0.

Offset : The fragment offset is measured in units of 8 octets.

TTL : Indicates the maximum time the datagram is allowed to remain in the network.

Protocol : Indicates the next level protocol used in data portion.

Checksum : to detect the processing errors introduced in to the packet.

Source Address : IP address of original sender of a packet.

Destination Address : IP address of final destination of packet.

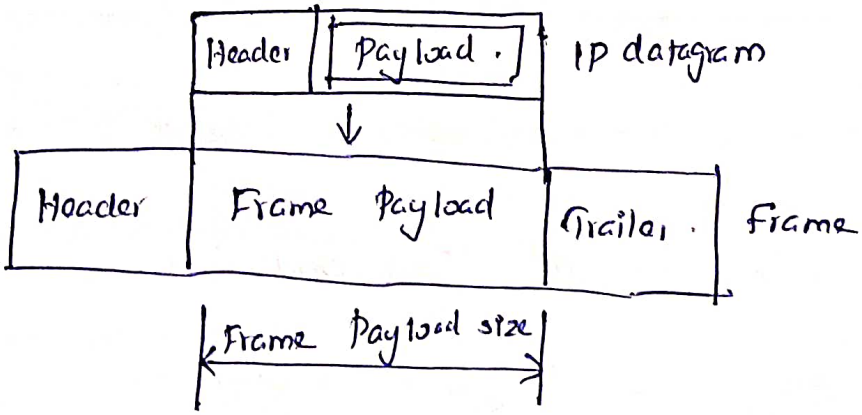
Options : Security, Record Route, Time Stamp etc.

Pad : Used to measure that the internet header ends on a 32 bit boundary. The padding is zero.

IP Datagram : Fragmentation and Reassembly :

Fragmentation :

→ Every network type has a maximum transmission unit (MTU) which is the largest IP datagram that it can carry in a frame.



→ Each IP datagram is reencapsulated for each physical network over which it travels.

Reassembly:

→ Reassembly is done at the receiving host and not at each router.

→ To enable these fragments to be reassembled at the receiving host, they all carry the same identifier in the Ident field.

IP Security:

→ three security issues.

(i) Packet Sniffing

(ii) Packet Modification

(iii) IP Spoofing.

Packet Sniffing:

→ An intruder may intercept an IP packet and make a copy of it.

→ Packet Sniffing is a passive attack, in which the attacker does not change the contents of the packet.

Packet Modification:

→ The attacker intercepts the packet, changes its contents, and sends the new packet to the receiver.

→ The receiver believes that the packet is coming from the original sender.

→ This attack can be detected using a data integrity mechanism.

IP Spoofing:

→ An attacker can masquarde as somebody else and create an IP packet that carries the source address of another computer.

→ This can be prevented using an origin authentication mechanism.

IPSec:

→ The IP packets today can be protected from the previously mentioned attacks using a protocol called IPSec.

→ This protocol is used in conjunction with IP protocol.

→ four services.

(i) Defining Algorithms and keys.

(ii) Packet Encryption.

(iii) Data Integrity

(iv) Origin Authentication.

ICMPV4 - Internet Control Message Protocol version 4.

→ ICMP is a network layer protocol.

→ It is a companion to the IP protocol.

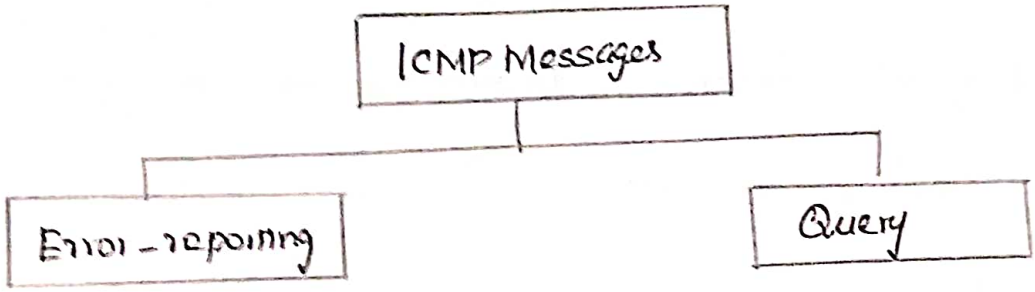
→ Internet Control Message Protocol (ICMP) defines a collection of error messages that are sent back to the source host whenever a router or host is unable process an IP datagram successfully.

ICMP Message Types:

→ divided into two categories

(i) Error reporting messages

(ii) query messages.



Type	Message
3	Destination Unreachable
4	Source quench
11	Time exceeded
12	Parameter Problem
5	Redirection

Type	Message
8/0	Echo (request/reply)
13/14	Timestamp (req./rep)
18/18	Address mask (req/rep)
10/9	Router Solicitation/ Advertisement.

ICMP Error Reporting Messages:

→ ICMP error messages report-error conditions

→ Typically sent when a datagram is discarded.

→ Error message is often passed-from ICMP to the application program.

Destination Unreachable:

→ a router cannot route a datagram the datagram is discarded and sends a destination unreachable message to the host

Source quench:

→ a router or host discards a datagram due to congestion

it sends a source quench message to the source host.

Time Exceeded:

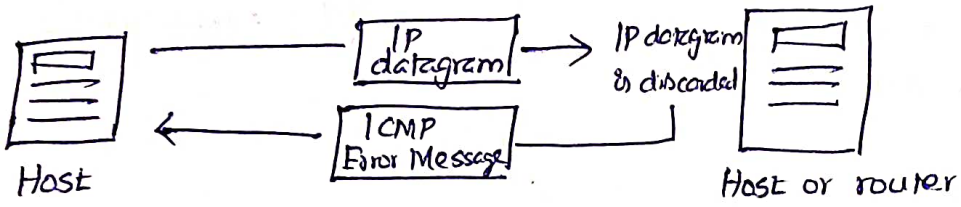
→ Router discards a datagram when TTL field becomes 0 and time exceeded message is sent to source host.

Parameter Problem:

→ a router discovers ambiguous or missing value in any field of the datagram, it discards the datagram and sends parameter problem message to source.

Redirection:

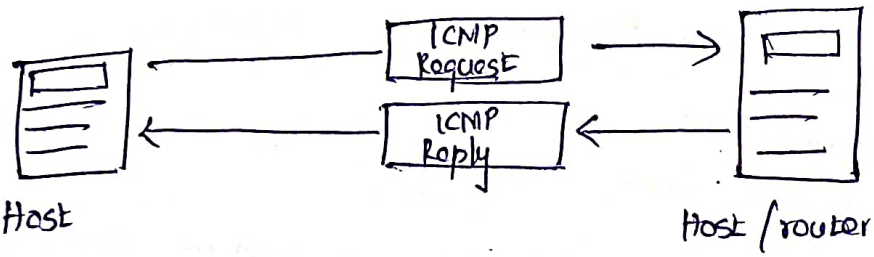
→ Redirect messages are sent by the default router to inform the source host to update its forwarding table when the packet is routed on a wrong path.



ICMP Query Messages:

→ Request sent by host to a router or host

→ Reply sent back to querying host.



Echo Request and Reply:

→ Combination of echo request and reply messages determines whether two systems communicate or not.

Timestamp Request and Reply:

→ Two machines can use the timestamp request and reply messages to determine the round-trip-time (RTT)

Address Mask Request and Reply:

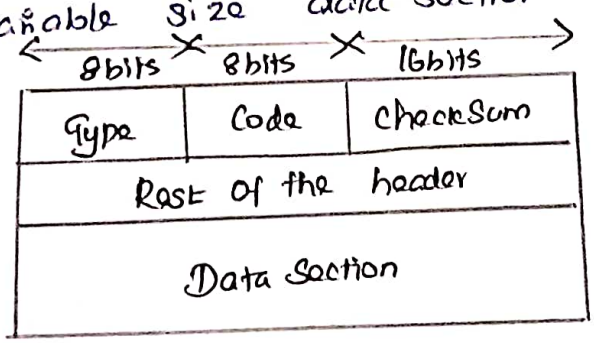
→ A host to obtain its subnet mask, sends an address mask request message to a router, which responds with an address mask reply message.

Router Solicitation / Advertisement:

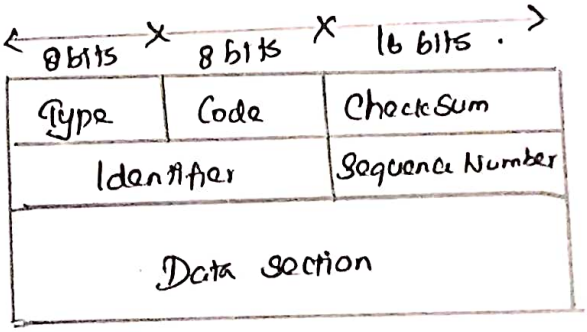
→ A host broadcasts a router solicitation message to know about the router.

ICMP Message format:

→ An ICMP message has an 8 byte header and a variable size data section.



Error reporting Messages



Query Messages.

ICMP Debugging Tools:

→ Two tools

(a) Ping (b) Traceroute

Ping:

→ used to find if a host is alive and responding

```
$ ping google.com
```

Traceroute or Tracert:

→ Windows can be used to trace the path of a packet from a source to destination. `$ traceroute google.com`.

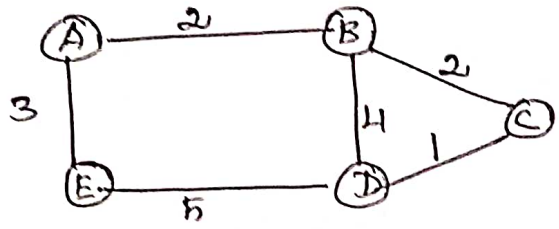
Unicast Routing:

→ is the process of selecting best paths in the network.

→ In unicast routing, a packet is routed, hop by hop, from its source to its destination by the help of forwarding tables.

→ Only the intermediate routers in the networks need forwarding tables.

Networks as a Graph:



→ The nodes of the graph labeled A through E may be hosts, switches, routers or networks.

→ The edges of the graph correspond to the network links.

→ Each edge has an associated cost.

Unicast Routing Algorithms:

→ three main classes

(a) Distance vector Routing Algorithm – Routing Information Protocol

(b) Link State Routing Algorithm – Open Shortest Path First Protocol

(c) Path vector Routing Algorithm – Border Gateway Protocol.

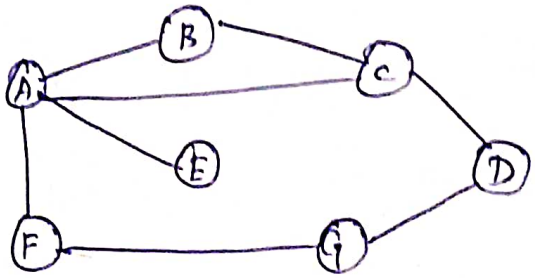
Distance Vector Routing (DSR)

Routing Information Protocol (RIP)

Bellman-Ford Algorithm.

→ Distance vector routing is distributed (i) algorithm is run on all nodes.

→ Each node knows the distance (cost) to each of its directly connected neighbours.



→ In a given network cost of each link is 1hop.

→ Each node sets a distance of 1 (hop) to its immediate neighbor and cost to itself as 0.

→ Distance for non neighbors is marked as unreachable with value ∞.

Destination	Cost	Nexthop
A	0	A
B	1	B
C	1	C
D	∞	–
E	1	E
F	1	F
G	∞	–

Node A's Initial Table

Destination	Cost	Nexthop
A	1	A
B	∞	–
C	∞	–
D	∞	–
E	∞	–
F	0	F
G	1	G

Node F's Initial Table

⇒ The Initial Table for all nodes.

Initial Distances Stored at Each Node							
Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	∞	∞	1	0	∞	∞	1
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

→ For each destination, total cost is computed as

Total Cost = Cost (Node to Neighbor) + cost (Neighbor to Destination)

→ If Total cost < cost then

Cost = Total cost and Nexthop = Neighbor.

→ The final distances stored at each node is given below,

Final Distances Stored at Each Node							
Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Updation of Routing Tables:

→ There are two different circumstances under which a given node decides to send a routing update to its neighbors.

Periodic Update:

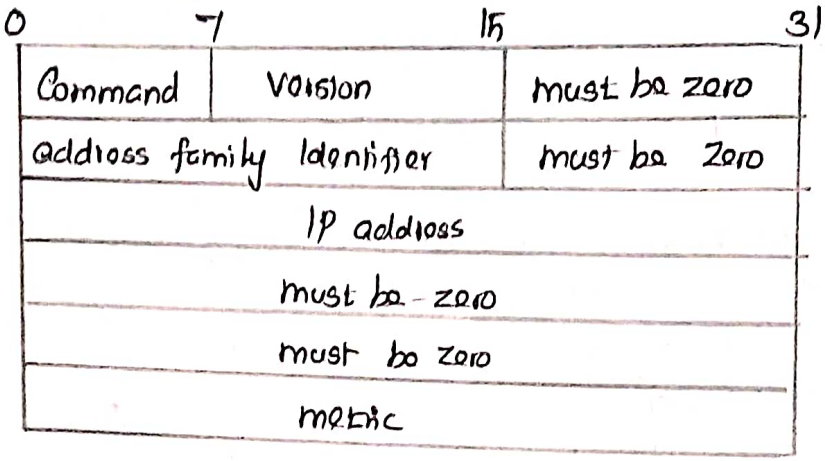
→ each node automatically sends an update message every so often even if nothing has changed.

Triggered Update:

→ Whenever a node notices a link failure or receives an update from one of its neighbors that causes it to change one of the routes in its routing table.

Routing Information Protocol (RIP)

→ RIP is an Intra domain routing protocol based on distance vector algorithm.



Command:

→ It indicates the packet type.

Version:

→ It indicates RIP version number. For RIPv1 the value is 0x01

Address family identifier:

→ When the value is 2, it represents IP Protocol.

IP address:

→ It indicates the destination IP address of the route

Metric:

→ It indicates the hop count of a route to its destination

Link State Routing (LSR)

Open Shortest Path Protocol (OSPF)

Dijkstra's Algorithm:

→ Each node knows state of link to its neighbors and cost

→ Nodes create an update packet called link state packet (LSP) that contains,

(n) ID of the node
(n) List of neighbors for that node
(n) 64 bit sequence number
(n) Time to Leve.

Mechanisms:

→ two mechanisms

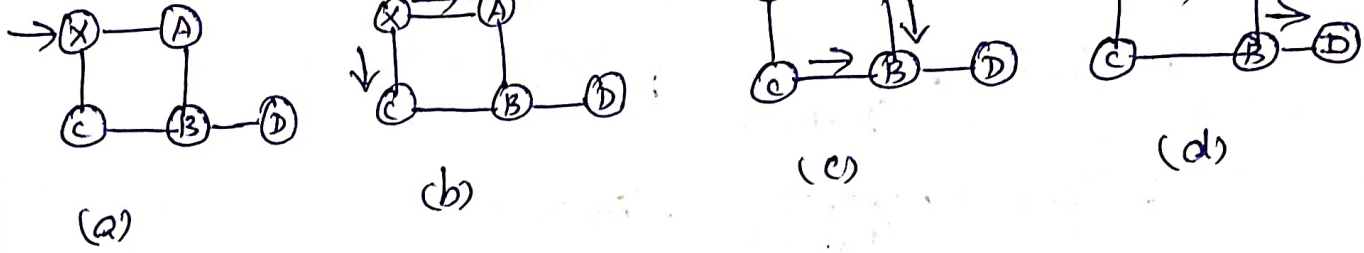
(i) Reliable flooding

(ii) Route calculation.

Reliable flooding:

→ link state information to all other nodes.

→ Each node sends its LSP out on each of its directly connected links.



(a) (b) (c) (d)

Route calculation:

→ Each node knows entire topology once it has LSP from every other node.

→ Forward search algorithm is used to compute routing table from the received LSPs.

→ Each node maintains two lists namely Tentative and Confirmed with entries of the form (Destination, Cost, Next hop)

Dijkstra's Shortest Path Algorithm:

(Forward Search Algorithm)

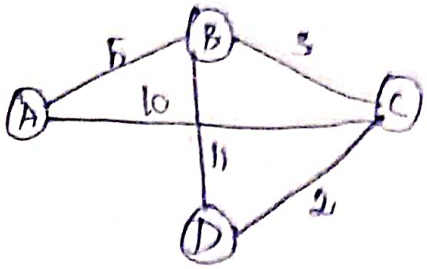
1) Each host maintains two lists known as Tentative and Confirmed.

2) Initialize the Confirmed list with an entry for the node (Cost = 0)

3) Node just added to Confirmed list is called Next. Its LSP is examined

4) For each neighbor of Next, calculate Cost to reach each neighbor as Cost (Node to Next) + Cost (Next to Neighbor)

5) If Tentative list is empty then stop. Otherwise move least Cost entry from tentative list to Confirmed List. Go to step 2.



Step	Confirmed	Tentative
1	(D, 0, -)	
2	(D, 0, -)	(B, 11, B) (C, 2, C)
3	(D, 0, -) (C, 2, C)	(B, 11, B)
4	(D, 0, -) (C, 2, C)	(B, 5, C) (B, 12, C)
5	(D, 0, -), (C, 2, C), (B, 5, C)	(B, 12, C)
6	(D, 0, -) (C, 2, C). (B, 5, C)	(B, 10, C)
7	(D, 0, -) (C, 2, C) (B, 5, C) (A, 10, C)	

Open Shortest Path First Protocol: (OSPF)

→ OSPF is a non-proprietary widely used link state routing protocol.

→ OSPF Features are.

(i) Authentication:

↳ Malicious host can collapse a network by advertising to reach every host with cost 0.

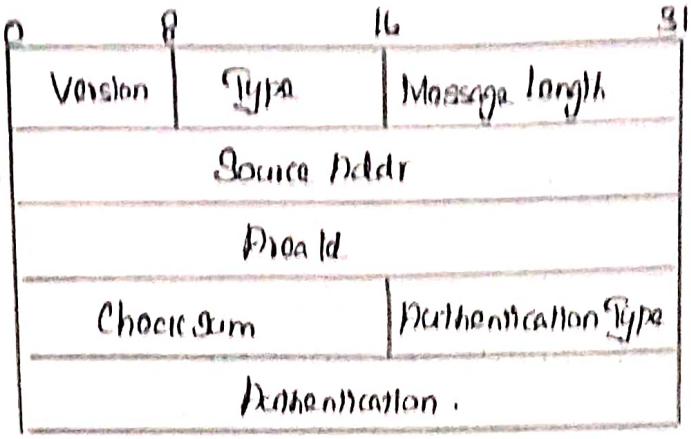
(ii) Additional hierarchy:

↳ Domain is partitioned into areas, i) OSPF is more scalable.

(iii) Load Balancing.

↳ Multiple routes to the same place are assigned same cost.

Link State Packet Format:



Version: represents the current version

Type: represents the type. (1-5) of ospf message

Type 1 - hello message

Type 2 - request

Type 3 - send

Type 4 - acknowledge the receipt of link state messages

Type 5 - reserved.

Source Addr: Identifies the sender

Area Id: 32 bit identifier of the area in which the node is located

Check sum: 16 bit internet check sum.

Authentication Type: 1 (simple password), 2 (cryptographic authentication)

Authentication: contains password or cryptographic checksum.

Difference between Distance vector and Link State Algorithms

Distance Vector Routing	Link State Routing
Each node talks only to its directly connected neighbors but it tells them everything it has learned. (i.e distance to all nodes)	Each node talks to all other nodes but it tells them only what it knows for sure (i.e) only the state of its directly connected links)

Path vector Routing (PVR)

Border Gateway Protocol (BGP)

→ Path vector routing is an asynchronous and distributed routing algorithm.

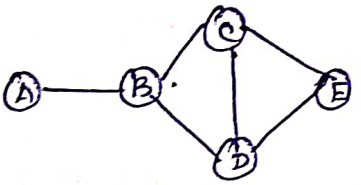
→ The path vector routing is based on least cost routing.

→ the source can control the path.

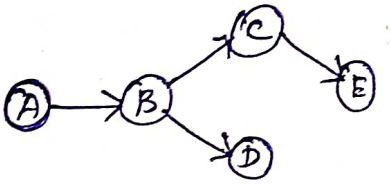
Spanning Trees:

→ In path vector routing the path from a source to all destinations is determined by the best spanning tree.

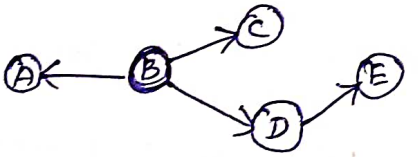
→ The best spanning tree is not the least cost tree.



A's Spanning Tree ⇒



B's Spanning Tree ⇒



Border Gateway Protocol:

→ BGP is the only interdomain routing protocol used in the internet today.

→ BGP views internet as a set of autonomous systems interconnected arbitrarily

iBGP - Interior BGP:

→ A variant of BGP

→ used by routers to update routing information learnt from other speakers to routers inside the autonomous system.

Unicast Routing Protocols:

→ A protocol is more than an algorithm.

→ A routing protocol specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network.

Internet Structure:

→ Internet has a million networks. Routing table entries per router should be minimized.

→ Link state routing protocol is used to partition domain into areas. Area introduces an additional level of hierarchy.

Inter domain Routing:

→ Internet is organized as autonomous system (AS) each of which is under the control of a single administrative entity.

→ Inter domain routing shares reachability information between autonomous system.

Traffic on the Internet:

→ two types.

1) Local Traffic - with in an autonomous system.

2) Transit Traffic - Traffic that passes through an autonomous system.

Autonomous system Classification:

(1) Stub AS - Connected to only one autonomous system.

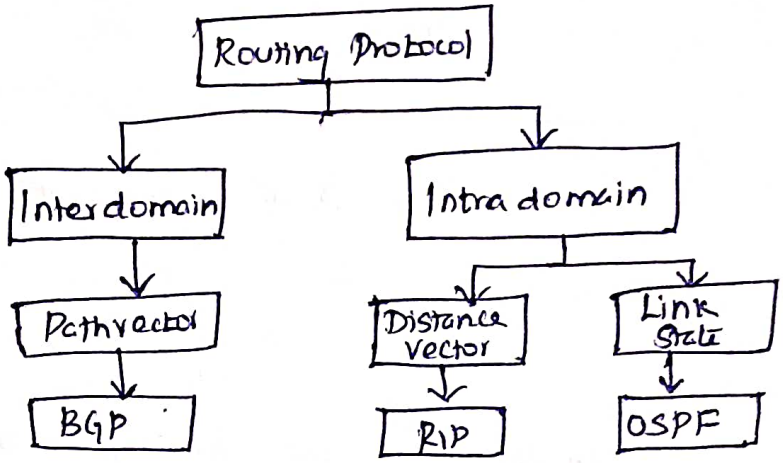
(2) Multihomed AS - Connections to multiple autonomous system. but refuses to carry transit traffic.

(3) Transit AS - Connections to multiple autonomous system and is designed to carry transit traffic.

Policies of Autonomous System:

(1) Provider - customer. (2) Customer - Provider (3) Peer

Types of Routing Protocols:



(1) Intradomain Routing:

↳ Routing within a single autonomous system.

→ Routing Information Protocol – based on distance vector.

→ Open Shortest Path First – based on link state Algorithm

(2) Inter domain Routing:

→ Routing between autonomous system.

→ Border Gateway Protocol – based on path vector algorithm.

Multicasting:

→ One source and a group of destinations

→ the relationship is one to many or many to many.

One to Many:

→ Source specific multicast

(1) Radio station broadcast

(2) Transmitting news, stock price.

(3) Software updates to multiple hosts.

Many to Many:

→ Any Source Multicast.

(1) Multimedia teleconferencing

(2) Online multiplayer games

(3) Distributed simulations.

IGMP or MLD Protocol:

→ Hosts communicate their desire to join/leave a multicast group to a router using Internet Group Message Protocol (IGMP) in IPv4 or Multicast Listener Discovery (MLD) in IPv6

Multicast Addressing:

→ Multicast address is associated with a group, whose members are dynamic.

→ Each group has its own IP multicast address.

Multicasting versus Multiple Unicasting:

→ Multicasting starts with a single packet from source that is duplicated by the routers.

→ In multiple unicasting several packets start from the source.

Types of multicasting:

(i) Source Specific Multicast (One-to-many Model)

(ii) Any Source Multicast (many-to-many Model)

Multicast Applications:

(i) Access to distributed databases

(ii) Information Dissemination

(iii) Teleconferencing

(iv) Distance Learning.

IPv6 Next Generation IP:

→ IPv6 was evolved to solve address space problem and offers rich set of services.

→ Some hosts and routers will run IPv4 only, some will run IPv4 and IPv6 and some will run IPv6 only.

Features of IPv6:

(i) Better header format

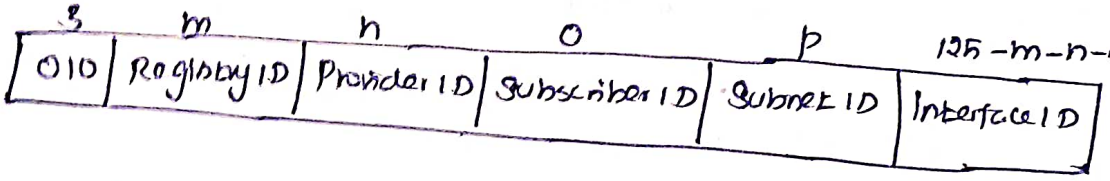
(ii) New options

(iii) Allowance for extension

(iv) Support for resource allocation

Address Aggregation of IPv6:

→ IPv6 provides aggregation of routing information to reduce the burden on routers.



Prefix — All address in same Continent

Registry ID — Identifies the Continent

Provider ID — Identifies the provider for Internet Access

Subscriber ID — Specifies the subscriber identifier

Subnet ID — Contains subnet of the subscriber.

Interface ID — Contains link level or physical Address

Advanced Capabilities of IPv6:

(i) Auto Configuration

(ii) Advanced Routing

(iii) Additional Functions

(iv) Security

(v) Resource Allocation.

Advantages of IPv6:

(i) Address Space (ii) Header Format (iii) Extensible.

Unit IV

TRANSPORT LAYER

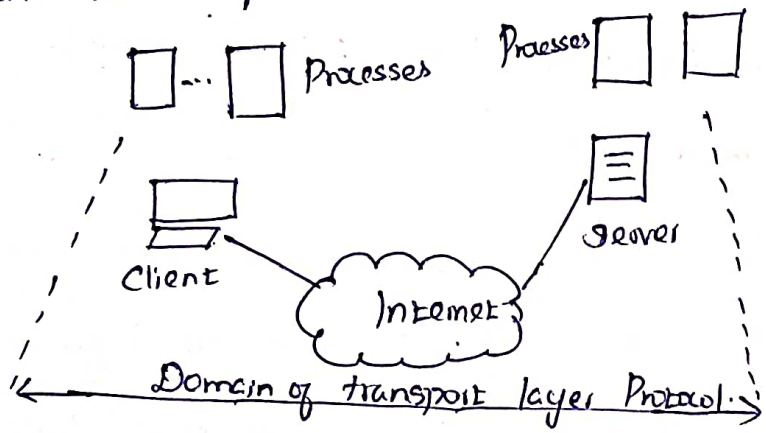
Introduction – Transport layer Protocols – Services – Port Numbers – User Datagram Protocol – Transmission Control Protocol – SCTP.

Introduction:

→ The transport layer is the fourth layer of the OSI model and is the core of the Internet model.

→ The transport layer provides transparent transfer of data between hosts.

→ It is the first true end-to end layer implemented in all End systems.



Transport Layer Functions / Services:

→ The transport layer is located between the network layer and the application layer.

→ The services can be provided by transport layer are,

(i) Process to Process Communication

(ii) Addressing: Port Numbers.

(iii) Encapsulation and Decapsulation

(iv) Multiplexing and Demultiplexing

(b) Flow Control

(c) Error Control

(d) Congestion Control.

Process - to - Process Communication:

→ The Transport layer is responsible for delivering data to the appropriate application process on the host computers.

Addressing: Port Numbers:

→ Ports are the essential ways to address multiple entities in same location.

(a) Well known ports: 0 - 1023

(b) Registered ports: 1024 to 49151

(c) Ephemeral ports (Dynamic Ports): 49152 - 65535

Encapsulation and Decapsulation:

→ Encapsulation happens at the sender site. The Transport layer receives the data and adds the transport layer header.

→ Decapsulation happens at the receiver site. When the message arrives at the destination transport layer, the header is dropped and the transport layer delivers the message to the process running at the application layer.

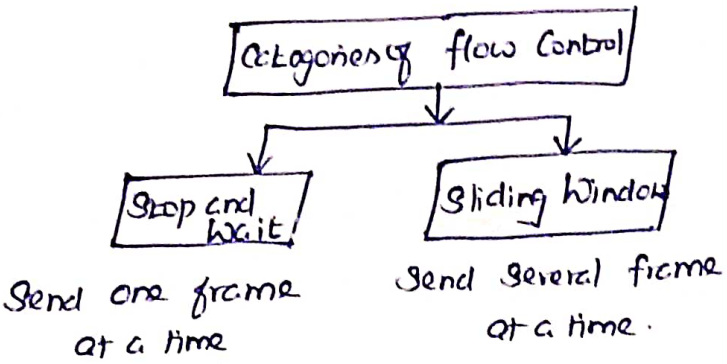
Multiplexing and Demultiplexing:

Multiplexing - an entity accepts items from more than one source

Demultiplexing - an entity delivers items to more than one source.

Flow Control:

→ process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver.



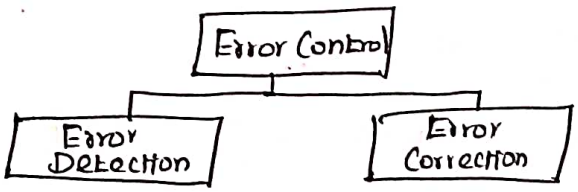
Error Control:

(i) Detecting and discarding corrupted packets.

(ii) keeping track of lost and discarded packets and resending them.

(iii) Recognizing duplicate packets and discarding them.

(iv) Buffering out-of-order packets until the missing packets arrive.



Congestion Control:

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

(i) Open loop - Prevent the congestion before it happens

(ii) Closed loop - remove the congestion after it happens.

Port Numbers:

→ Processes are assigned a unique 16 bit port number on that host.

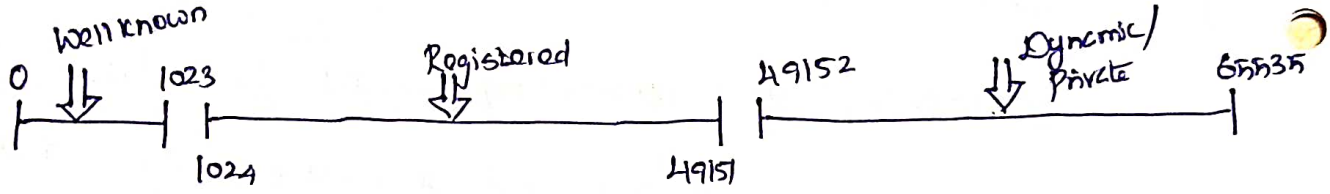
→ Port numbers provide end-to-end addresses at the transport layer.

→ Port numbers are integers between 0 and 65535

(i) Well-known Ports.

(ii) Registered Ports

(iii) Ephemeral ports (Dynamic Ports)



Well-known Ports:

→ These are permanent port numbers used by servers.

→ They range between 0 to 1023

→ This port number cannot be choosen randomly.

Ephemeral Ports (Dynamic Ports):

→ The client program defines itself with a port number called the ephemeral port number.

→ The word ephemeral means "short-lived" and is used because the life of a client is normally short.

→ These port numbers ranges from 49152 to 65535

Registered Ports:

→ The ports ranging from 1024 to 49151 are not assigned or controlled.

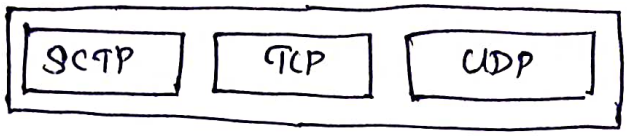
Transport Layer Protocols:

→ Three protocols are associated with the transport layer.

(i) UDP – User Datagram Protocol.

(ii) TCP – Transmission Control Protocol.

(iii) SCTP – Stream Control Transmission Protocol.



User Datagram Protocol:

→ UDP is connectionless, reliable transport protocol.

→ UDP adds process-to-process communication to best effort service provided by IP.

UDP ports:

Some well known UDP ports are,

7 – Echo, 53 – DNS, 111 – RPC, 161 – SNMP etc.

→ When a message arrives UDP appends it to end of queue

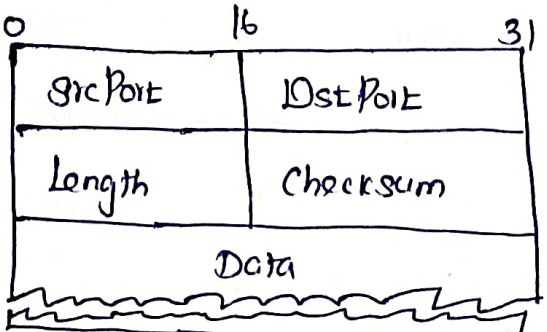
→ When queue is full the message is discarded.

→ When a message is read it is removed from the queue.

UDP Datagram Format:

→ UDP packets are known as user datagrams

→ The user datagrams have a fixed size header of 8 bytes made of four fields each of 2 bytes (16 bits).



Source Port Number:

→ Port number used by process on source host with 16 bits long

→ If the source is server then it is well known port number.

Destination port number:

→ Port number used by process on Destination host with 16 bits long

→ If the destination host is the server, then the port number is a well known port number.

Length:

→ This field denotes the total length of the UDP packet.

→ The total length of any UDP datagram can be from 0 to 65535 bytes.

Checksum:

→ UDP computes its checksum over the UDP header, the contents of the message body, and something called the pseudoheader.

Data:

→ Data field defines the actual payload to be transmitted.

→ Its size is variable.

UDP Services:

(i) Process-to-Process Communication

(ii) Connectionless Services.

(iii) Flow Control

(iv) Error Control

(v) Check sum

(vi) Congestion Control

(vii) Encapsulation and Decapsulation

(viii) Queuing

(ix) Multiplexing and Demultiplexing.

Applications of UDP:

(i) UDP is used for management processes such as SNMP

(ii) UDP is used for route updating protocols such as RIP

(iii) Suitable Simple request-response communication.

(iv) Used for interactive real time applications.

Transmission Control Protocol (TCP)

→ TCP is a reliable, connection oriented, byte stream protocol.

→ TCP guarantees the reliable, in-order delivery of a stream of bytes.

TCP Services:

(i) Process-to-Process Communication

(ii) Stream Delivery Service

(iii) Full-Duplex Communication

(iv) Multiplexing and Demultiplexing.

(v) Connection-Oriented service

(vi) Reliable Service.

TCP Segment:

→ A packet in TCP is called a segment.

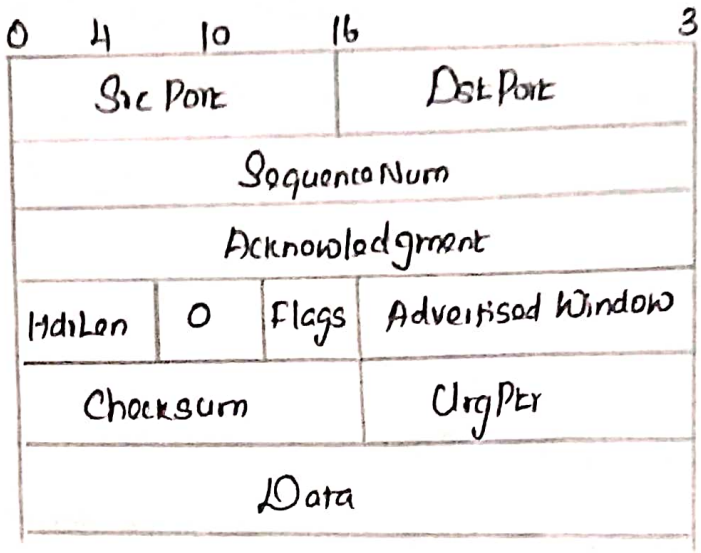
→ Data unit exchanged between TCP peers are called segments.

TCP packet Format:

→ Each TCP segment contains the header plus Data.

→ The segment consists of a header of 20 to 60 bytes, followed by data from the application program.

→ The header is 20 bytes if there are no options and up to 60 bytes if it contains options.



Src Port and DstPort : Port number of source and Destination Process

Sequence Num : Contains Sequence Number, first byte of data segment

Acknowledgment : byte number of segment, the receiver expects next

HdrLen : Length of TCP header as 4-byte words

Flags : Contains six control bits known as Flags

Advertised Window : defines receiver's window size and acts as flow ctrl.

Check Sum : TCP header, Data, Pseudo header containing IP fields.

UrgPtr : Segment Contains Urgent data.

Options : 40 bytes of optional information in the TCP header.

TCP Connection Management :

→ A Connection oriented Transport protocol establishes a logical path between the source and destination.

→ Three phases

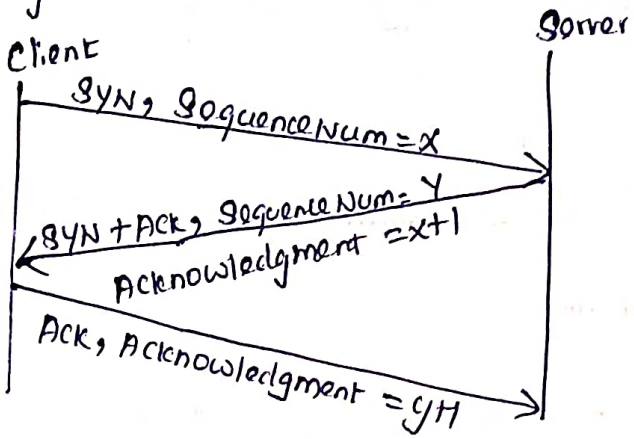
(i) Connection Establishment

(ii) Data Transfer

(iii) Connection Termination.

Connection Establishment:

→ Connection establishment in TCP is a three-way handshaking.



(i) Client sends a SYN segment to the server

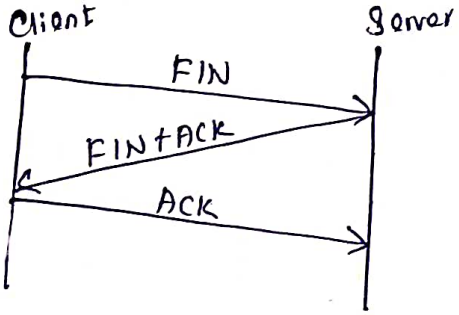
(ii) Server responds with a segment

(iii) Finally client responds with a segment.

Connection Termination

→ two ways

Three-way close: Both client and server close simultaneously.



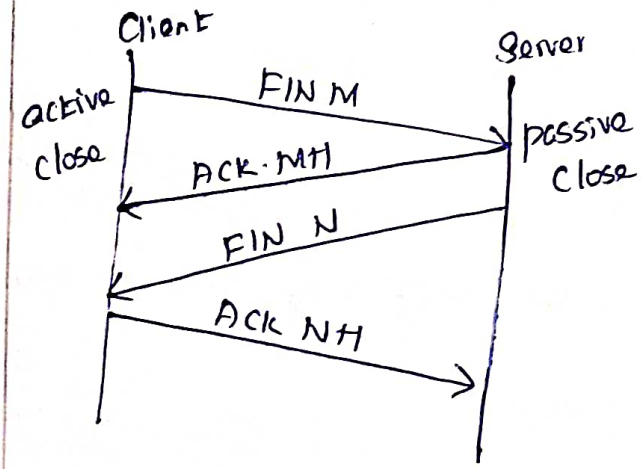
⇒ Client sends a FIN segment

⇒ FIN segment include chunk of data

⇒ Server responds with FIN+ACK

⇒ Finally client sends ACK.

Half-way close: Client stops sending but receives data.



⇒ client half closes the connection by FIN segment

⇒ Server sends ACK

⇒ Data transfer from client to server stops

⇒ Server sends FIN segment to client.

Data Transfer:

→ After connection is established, bidirectional data transfer can take place.

→ The acknowledgment is piggybacked with the data.

TCP Flow Control:

→ TCP uses variant of sliding window known as adaptive flow control that,

(i) guarantees reliable delivery of data

(ii) ensures ordered delivery of data

(iii) enforces flow control at the sender.

Send Buffer:

→ 3 segments

(i) acknowledged data

(ii) unacknowledged data

(iii) data to be transmitted.

Receive Buffer:

→ three pointers

(i) Last Byte Read

(ii) Next Byte Expected

(iii) Last Byte Received.

TCP Transmission:

→ two mechanisms

(i) Maximum Segment Size (MSS) - Silly Window Syndrome

(ii) Timeout - Nagle's Algorithm.

Silly Window Syndrome:

→ When either the sending application program creates data slowly or the receiving application program consumes data slowly or both problems arise.

Nagle's Algorithm:

→ It may want to wait some amount of time before sending the available data.

When the application produces data to send

If (both the available data and the window) = MSS

Send the full segment

else

If (there is unAcked data)

Buffer the new data until an Ack arrives

else

send all the new data now.

TCP Congestion Control:

→ Congestion occurs if load is greater than capacity of the network.

→ TCP maintains a variable called Congestion Window for each connection.

→ TCP Congestion Control mechanisms are,

(i) Additive Increase / Multiplicative Decrease (AIMD)

(ii) Slow Start

(iii) Fast Retransmit and Fast Recovery.

Additive Increase / Multiplicative Decrease (AIMD)

→ TCP Source initializes Congestion Window based on Congestion level in the network.

Increment = Mss × (Mss / CongestionWindow)

CongestionWindow += Increment.

Slow Start:

→ Slow Start is used to increase Congestion Window exponentially from a cold start.

→ Source TCP initializes Congestion Window to one packet.

CongestionThreshold = CongestionWindow/2

CongestionWindow = 1

Fast Retransmit and Fast Recovery:

→ TCP Timeouts lead to long periods of time during which the connection went dead while waiting for a timer to expire.

→ Fast retransmit is a heuristic approach that triggers retransmission of a dropped packet sooner than the regular timeout mechanism.

TCP Congestion Avoidance:

→ Congestion avoidance mechanisms prevent congestion before it actually occurs.

→ Congestion avoidance mechanisms are,

(1) DEC bit - Destination Experiencing Congestion Bit.

(2) RED - Random Early Detection.

DEC bit - Destination Experiencing Congestion Bit:

→ The first mechanism developed for use on Digital Network Architecture (DNA).

→ The idea is to evenly split the responsibility for Congestion Control between the routers and the end nodes.

Red - Random Early Detection.

→ The second mechanism of congestion avoidance is called as Random Early Detection (RED)

$$\text{AvgLen} = (1 - \text{Weight}) \times \text{AvgLen} + \text{Weight} \times \text{SampleLen}$$

where $0 < \text{Weight} < 1$ and

SampleLen - is the length of the queue when a sample measurement is made.

Stream Control Transmission Protocol (SCTP):

→ SCTP is a reliable, message oriented, transport layer protocol.

→ SCTP has mixed features of TCP and UDP.

→ SCTP provides congestion control as well as flow control.

SCTP Services:

(1) Process to Process Communication

(2) Multiple Streams

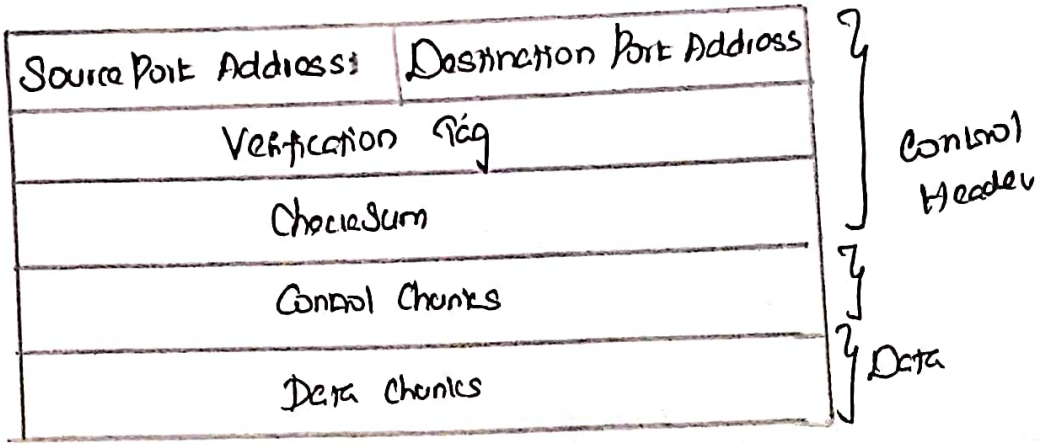
(3) Multihoming

(4) Full Duplex Communication.

(5) Connection oriented Service

(6) Reliable Service.

SCTP Packet Format:



General Header:

→ defines the endpoint of each association to which the packet belongs.

Destination Port: → Identifies the receiving port

Source port: → Identifies the sending port.

Verification Tag: → to distinguish stale packets from a previous connection.

Checksum: The size is 32 bits - SCTP uses CRC-32 checksum

Chunks:

→ Control mechanism or user data are carried in Chunks.

Type	Flag	Length
Chunk Information (multiple of 4 bytes)		

Types of Chunks:

(1) DATA
(2) INIT
(3) INIT ACK
(4) SACK
(5) HEARTBEAT
(6) HEARTBEAT ACK
(7) ABORT
(8) SHUTDOWN
(9) SHUTDOWN ACK
(10) ERROR
(11) COOKIE ECHO
(12) COOKIE ACK
(13) FORWARD TSN
(14) SHUTDOWN COMPLETE

SCTP Association:

→ SCTP is a connection oriented protocol.

→ three phases

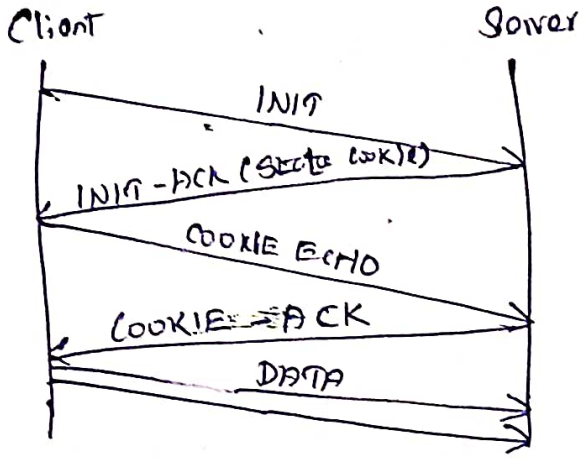
(i) Association Establishment.

(ii) Data Transfer

(iii) Association Termination.

Association Establishment:

→ SCTP requires a four-way handshake.



Data Transfer:

→ to transfer data between two ends.

→ SCTP supports piggybacking

Types of SCTP data transfer:

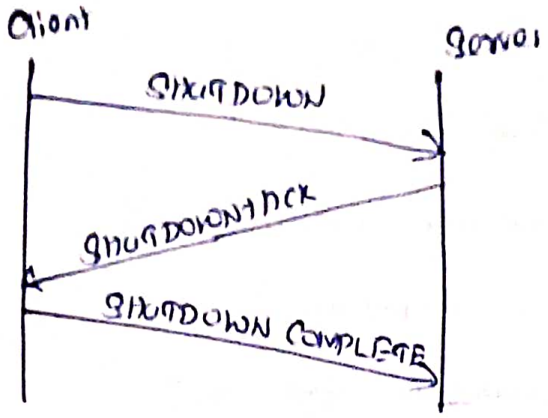
(i) Multihoming Data Transfer.

(ii) Multistream Delivery.

Association Termination:

→ either two parties involved in exchanging data can close the connection.

→ Association termination uses three packets.



SCTP Flow Control:

(i) Flow Control in SCTP is similar to that in TCP.

(ii) SCTP implementations are use a byte oriented window for flow control.

SCTP Error Control:

→ SCTP is a reliable transport layer protocol.

→ It uses SACK chunk to report the state of the receiver buffer to the sender.

SCTP Congestion Control:

→ SCTP is a transport layer protocol which packets subject to congestion in the network.

→ The SCTP designers have used the same strategies for congestion control as those used in TCP.

UNIT-V APPLICATION LAYER

WWW and HTTP – FTP – Email – Telnet – SSH – DNS – SNMP

Introduction:

→ The application layer is the highest layer in the protocol suite.

→ The application layer provides services to the user.

→ Types of application protocols.

(i) Standard application Protocols

(ii) Non Standard Application Layer Protocols.

Standard Application Layer protocols:

→ Standardized and documented by Internet Authority.

(i) SMTP – Simple Mail Transfer Protocol

(ii) HTTP – Hyper Text Transport Protocol.

Non Standard Application Layer Protocols:

→ Can write two programs that provide service to the user by interacting with the transport layer.

Application Layer Paradigms:

→ Two Paradigms.

(i) Traditional Paradigm – Client and Server.

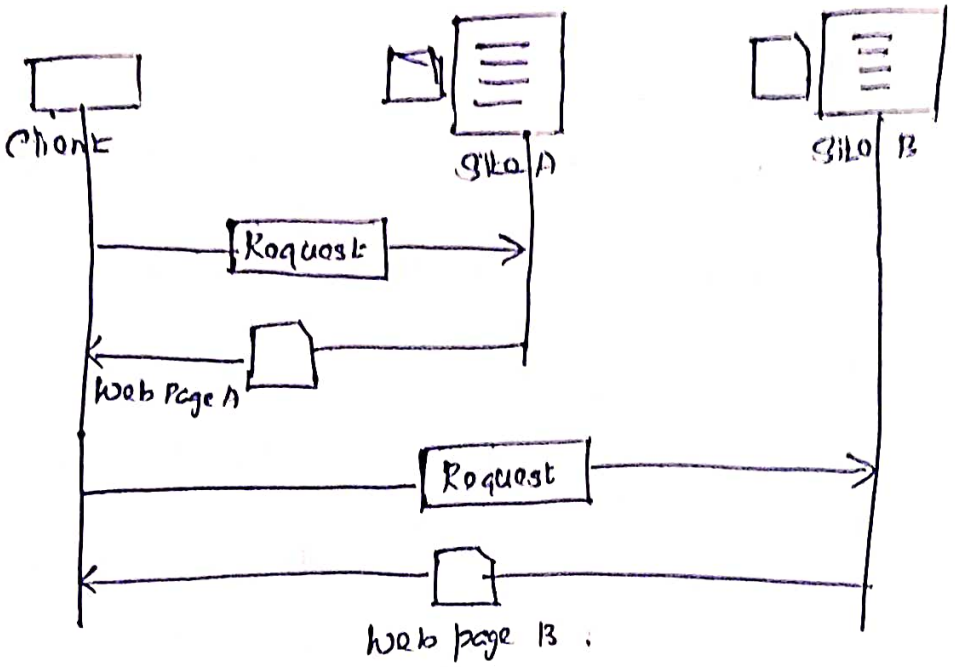
(ii) Now Paradigm – Peer-to-Peer (P2P)

WWW - World Wide Web:

→ It is a distributed client/server service, in which a client can access services at a server.

→ This allows document search and retrieval from any part of the Internet.

→ The documents were having HyperText as the context.



Components of the Web:

Structural Components:

1) Web clients / Browsers
2) Web servers
3) Web caches
4) Internet

Semantic Components.

1) HyperText Transfer Protocol (HTTP)
2) HyperText MarkUp Language (HTML)
3) Extensible Markup Language (XML)
4) Uniform Resource Identifier (URI)

→ Clients use browser application to send URLs via HTTP to servers requesting a web page.

Web Clients (Browsers):

→ A browser is a software on the client on the web which initiates the communication with server.

→ Examples are Internet Explorer, Mozilla firefox, Netscape Navigator, Safari etc.

Web Servers:

→ All the combination between the web client and web server use the standard protocol called as HTTP

→ The server also runs as a background process.

Proxy Server:

→ A proxy server is a computer that keeps copies of responses to recent requests.

→ The web client sends a request to the proxy server.

→ The proxy server checks its cache.

URL - Uniform Resource Locator:

→ uniquely identify resources in the Internet.

→ URL provides information about its location on the web.

Protocol	: //	Host	:	Port	/	Path

→ URL defines four parts

(1) Method

(2) Host

(3) Port :

(4) Path .

URL Paths:

→ The path of the document for a http protocol is same as that for a document or file or directory in a client

→ A path which includes all the directories is a complete path also it is a partial path.

URI - Uniform Resource Identifiers:

→ URI is a string that identifies resources such as document, image, service etc.

→ It is of the form scheme : scheme - specific.

Web Documents:

(i) The documents in the WWW can be grouped into three broad categories,

(i) Static

(ii) Dynamic

(iii) Active.

Static Documents:

→ fixed content documents that are created and stored in a server.

→ The client can get a copy of the document only.

→ Can be prepared using one of several languages

(i) Hyper Text Markup Language (HTML)

(ii) Extensible Markup Language (XML)

(iii) Extensible Style Language (XSL)

(iv) Extensible Hypertext Markup Language (XHTML)

Dynamic Documents:

→ A dynamic document is created by a web server whenever a browser requests the document.

→ Dynamic documents can be retrieved using one of several scripting languages.

(i) Common Gateway Interface (CGI)

(ii) Java Server Pages (JSP)

(iii) Active Server Pages (ASP)

(iv) Cold Fusion.

Active Documents:

→ The program definitely needs to be run at the client site where the animation or interaction takes place.

→ The document is then run at the client site.

→ Can be created by using one of several languages.

(i) Java Applet

(ii) Java Script.

HTTP (Hyper Text Transfer Protocol)

→ It is used to define how the client server programs can be written to retrieve web pages from the web.

→ It is a protocol used to access the data on the world wide web (WWW)

→ HTTP is a stateless request/response protocol that governs client/server communication.

→ HTTP message has the general form,

START_LINE <CRLF>

MESSAGE_HEADER <CRLF>

<CRLF> MESSAGE_BODY <CRLF>

Where <CRLF> stands for Carriage_return-line-feed.

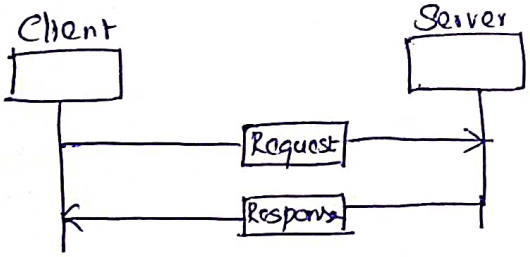
Features of HTTP:

(i) Connectionless Protocol.

(ii) Media Independent

(iii) Stateless

HTTP Request and Response Messages:



Request Message:

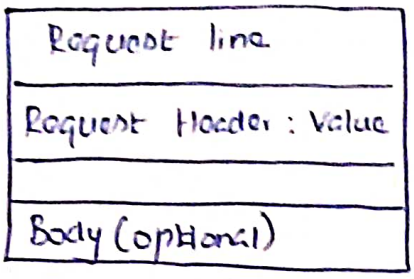
→ The request message is sent by the client that consists of a request line, headers and sometimes a body.

Response Message:

→ The response message is sent by the server to the client that consists of a status line, headers and sometimes a body.

HTTP Request Message:

→ The first line in a request message is called a request line.



Request Line :

→ Three fields ,

(i) Method ,

(ii) URL

(iii) Version

→ Some of the method types are ,

(i) GET (ii) HEAD

(iii) PUT (iv) POST

(v) TRACE (vi) DELETE

(vii) CONNECT (viii) OPTIONS

Request header :

→ Sends additional information from the client to the server

→ headers defines the message include ,

(i) User Agent (ii) Accept

(iii) Accept - Charset (iv) Accept - encoding

(v) Accept - language (vi) Authorization

(vii) Host (viii) Date

(ix) Upgrade (x) Cookie

(xi) If - modified - Since .

Body :

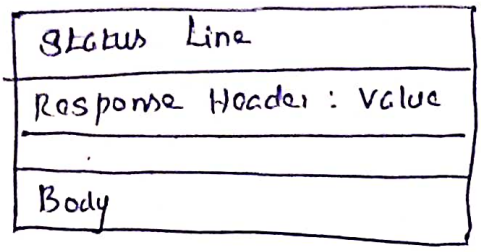
→ The body can be present in a request message . It is optional .

Conditional Request:

→ A Client can add a condition in its request

→ The Client can send the header-line if-Modified-Since, with the request to tell the server that it needs the page only if it is modified after a certain point in time.

HTTP Response Message:



→ The first line in a request message is called a status line.

→ After the request line, we can have zero or more response header lines.

→ The body is an optional one.

HTTP Connections:

→ HTTP Clients and Servers exchange multiple messages over the same TCP Connection.

→ HTTP 1.0 uses non-persistent connections and HTTP1.1 uses persistent connections.

Persistent Connections:

→ the server leaves the connection open for more requests, after sending a response

→ The round trip time for connection establishment and connection termination is saved.

Non-Persistent Connections:

→ only one object can be sent over a single TCP Connection

→ The server sends the response and closes the Connection

→ The client reads the data until it encounters an end to end file marker. It then closes the Connection.

HTTP Cookies:

→ HTTP Cookie also called Web Cookie, Internet Cookie, browser Cookie, or simply Cookie is a small piece of data sent from a website and stored on the users computer by the users web browser while the user is browsing.

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

Components of Cookie:

(1) Name

(2) Value

(3) Zero or more attributes.

→ Attributes store information such as the cookies expiration, domain and flags.

Types of Cookies:

(1) Authentication Cookies

(2) Tracking Cookies

(3) Session Cookies

(4) Persistent Cookies

HTTP Caching:

→ HTTP caching enables the client to retrieve document faster and reduces load on the server.

→ HTTP caching is implemented at proxy server, ISP router and Browser.

HTTP Security:

→ HTTP does not provide security.

→ HTTP can be run over the secure socket layer.

→ HTTP is referred to as HTTPS.

→ HTTP provides Confidentiality, client and server authentication, and data Integrity.

FTP (File Transfer Protocol):

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

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

FTP objectives:

→ It provides sharing of files.

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

→ It transfers the data more reliably and efficiently.

FTP Mechanism:

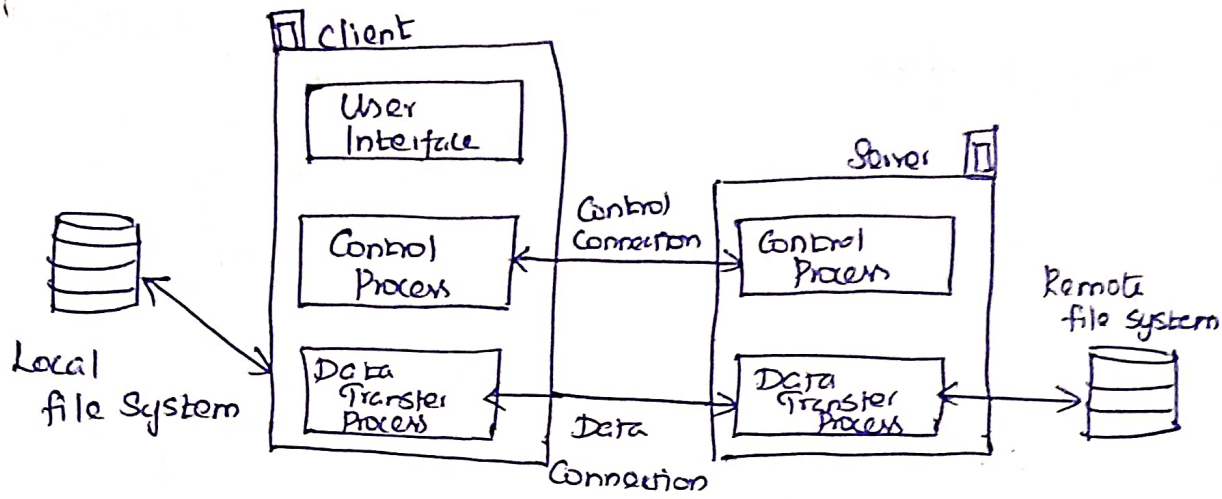
→ The FTP client has three components.

(1) User Interface (2) Control Process (3) Data Transfer Process

→ The FTP server has two components

(1) Server Control Process

(2) Server data transfer Process.

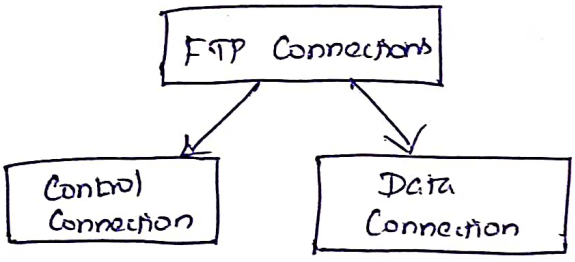


FTP Connections:

→ Two types

(1) Control Connection

(2) Data Connection.



Control Connection:

→ is made between the control processes.

→ Connection remains connected during the entire interactive FTP session.

Data Connection:

→ Uses very complex rules as data types may vary.

→ is made between data transfer Processes.

FTP Communication:

→ It achieved through commands and responses.

→ Commands are sent from the Client to the server.

→ Responses are sent from the server to the Client.

FTP File Type:

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

FTP Data Structure:

→ FTP can transfer a file across the data connection using one of the following data structure.

(i) File Structure

(ii) Record Structure.

(iii) Page Structure.

FTP Transmission mode:

→ Three transmission modes,

(i) Stream mode

(ii) Block Mode

(iii) Compressed Mode.

FTP File Transfer:

→ Three things,

(i) Retrieving a file (Server to Client)

(ii) Storing a file (Client to Server)

(iii) Directory listing (Server to Client)

FTP Security:

→ FTP requires a password, the password is sent in plain text, which is unencrypted. This is intercepted and used by attacker.

EMail: (SMTP, MIME, IMAP, POP)

→ most popular Internet Services is electronic mail (e-mail)

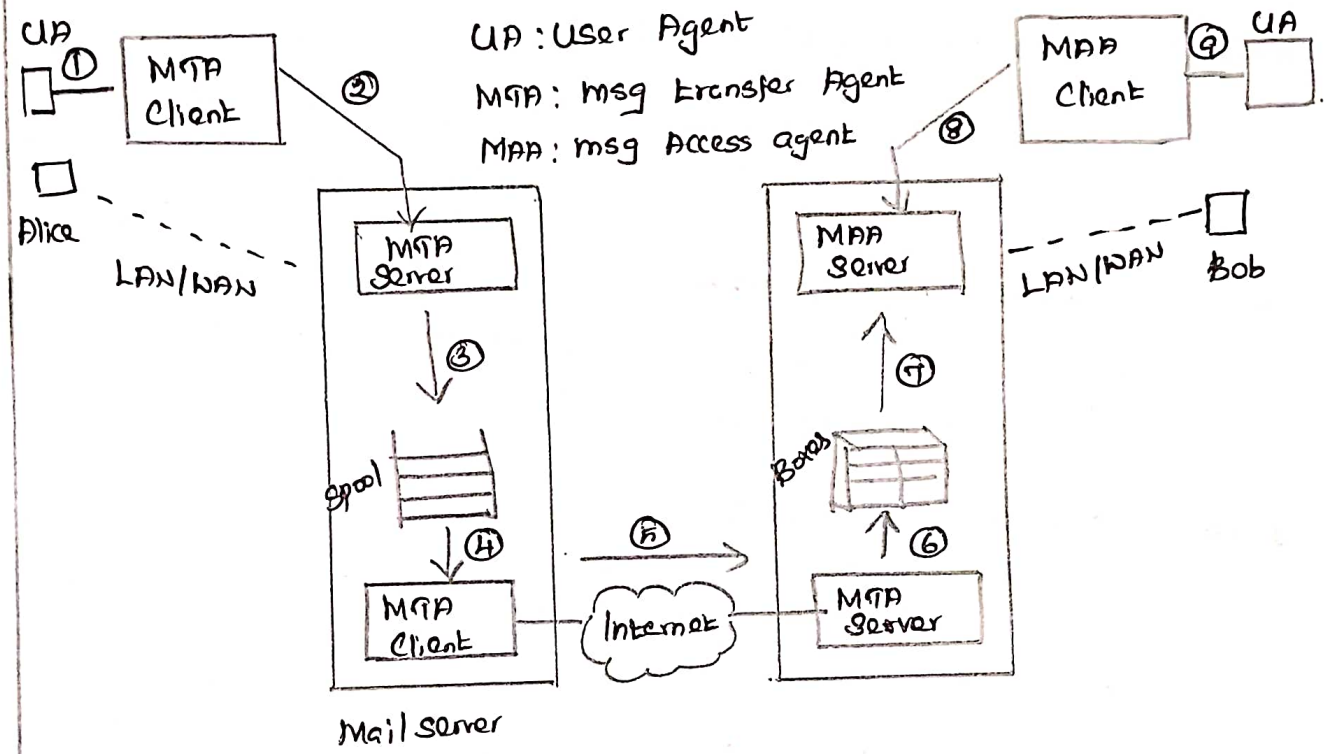
→ three components,

(a) User Agent (UA)

(b) Message Transfer Agent (MTA) - SMTP

(c) Message Access Agent (MAA) - IMAP, POP

Working of E-Mail:



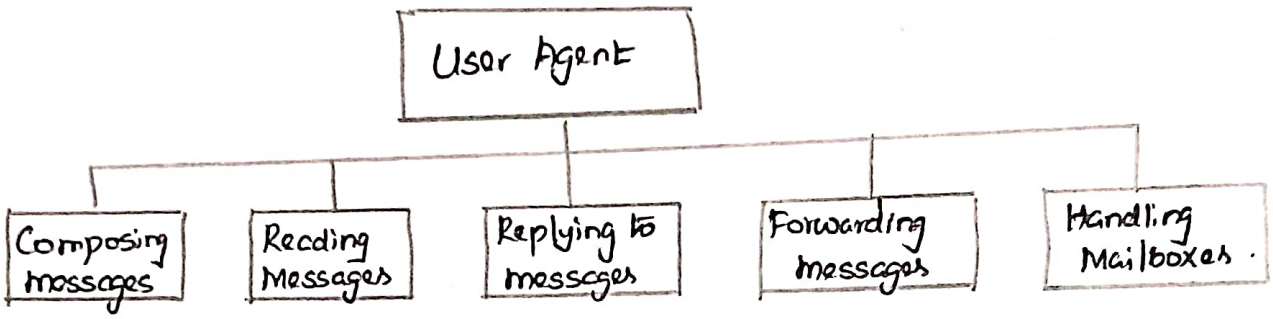
→ The server needs to run all the time because it does not know when a client will ask for connection.

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

User Agent: (UA):

→ The first component of mail system.

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



→ Two types

(i) Command Driven

(ii) Gui based.

Message Transfer Agent (MTA)

→ The formal protocol that defines the MTA client and server in the Internet is called SMTP.

Message Access Agent (MAA)

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

→ POP3 and IMAP4 are examples of MAA.

Address Format of Email:

→ Email address is userid@domain where domain is hostname of the mail server.

Message Format of E-mail:

→ two parts namely header and body.

→ header contents are,

(i) From: Identifier sender of a message
(ii) To: mail address of the recipient.
(iii) Subject: purpose of message
(iv) Date: timestamp of message.

→ Body contains the actual message.

⇒ Header lines:
To:
From:
Subject:

⇒ Body,
the "message"
Ascii characters only.

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

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

→ SMTP uses information written on the envelope of the mail, but does not look at the contents of the envelope.

SMTP Mail Flow:

→ mail is created by user agent program in response to user input.

→ The messages are queued in some fashion provided as input to an SMTP sender program.

SMTP Commands and Responses:

→ The operation of SMTP consists of a series of commands and responses exchanged between the SMTP sender and the SMTP receiver.

SMTP Commands:

→ The commands are sent from the client to the server. It consists of a keyword followed by zero or more arguments.

→ SMTP defines 14 commands.

(1) HELO	(5) RESET	(9) HELP
(2) MAIL FROM	(6) VRFY	(10) SEND FROM
(3) RCPT TO	(7) NOOP	(11) SMOL FROM
(4) DATA	(8) TURN	(12) SMAL FROM
(5) QUIT	(9) EXPN	

SMTP Responses:

→ Responses are sent from the server to the client

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

SMTP Operations:

→ three phases

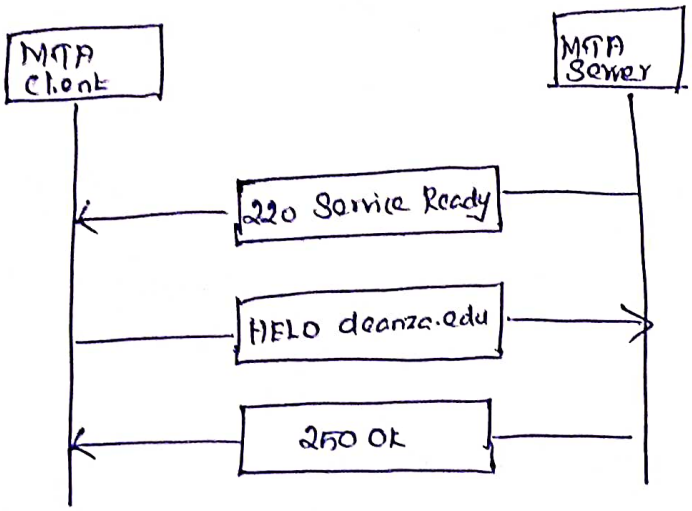
(a) Connection Setup

(b) Mail Transfer

(c) Connection Termination

Connection Setup:

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



Mail Transfer:

→ Three logical phases

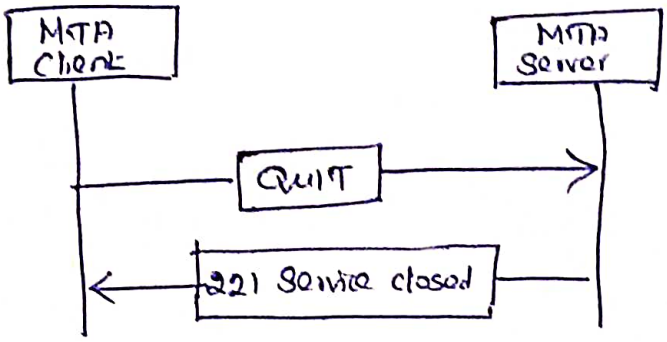
(a) A mail command identifies the originator of the message

(b) One or more RCPT commands identify the recipients for this message.

(c) A Data command transfers the message text

Connection Termination:

→ The receiver initiates its TCP close after sending its reply to the Quit command.



Limitations of SMTP:

(i) Cannot transmit executable files or binary objects.

(ii) Cannot transmit text data

(iii) SMTP servers may reject mail message over a certain size.

(iv) Some SMTP implementations do not adhere completely.

Multipurpose Internet Mail Extension (MIME)

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

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

Features of MIME:

→ able to send multiple attachments with a single message

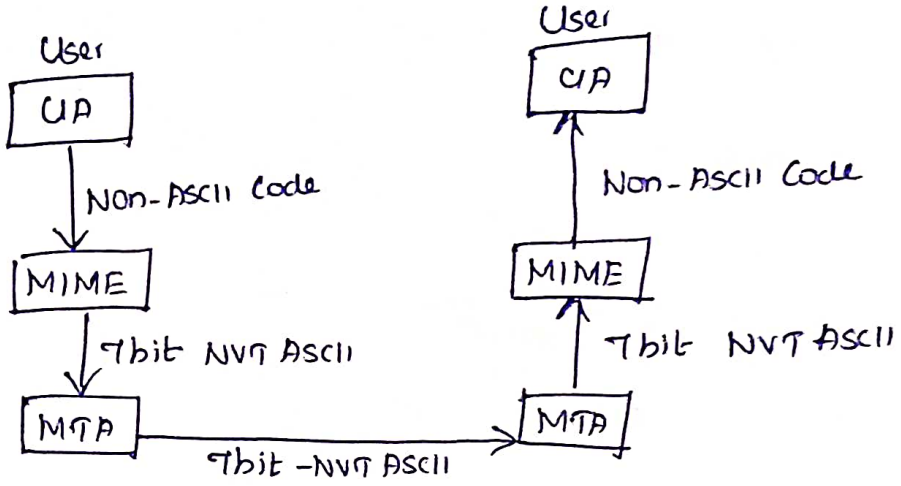
→ Unlimited message length.

→ Use of character sets other than ASCII code.

→ Use of rich text

→ Binary attachments (executables, images, audio/video etc)

→ MIME is a protocol that converts non-ASCII data to 7-bit NVT ASCII and vise versa.



MIME headers:

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

E-mail header
MIME version: 1.1 Content Type : type/subtype Content-Transfer-Encoding : encoding Type Content-Id: message id Content-Description: Textual explanation
E-mail body

MIME Content types:

→ defines a multipart type that says how a message carrying more than one data type is structured.

→ Content types are,

(a) Text
(b) Video
(c) Multipart
(d) Audio
(e) Message
(f) Application.
(g) Image

Encoding Formats of MIME:

→ To transfer binary data:

(i) 7 bit : 7 bit text format

(ii) 8 bit : 8 bit text format

(iii) Quoted Printable : 7 bit alphabet

(iv) base-64 : Sending binary files.

(v) binary : binary format

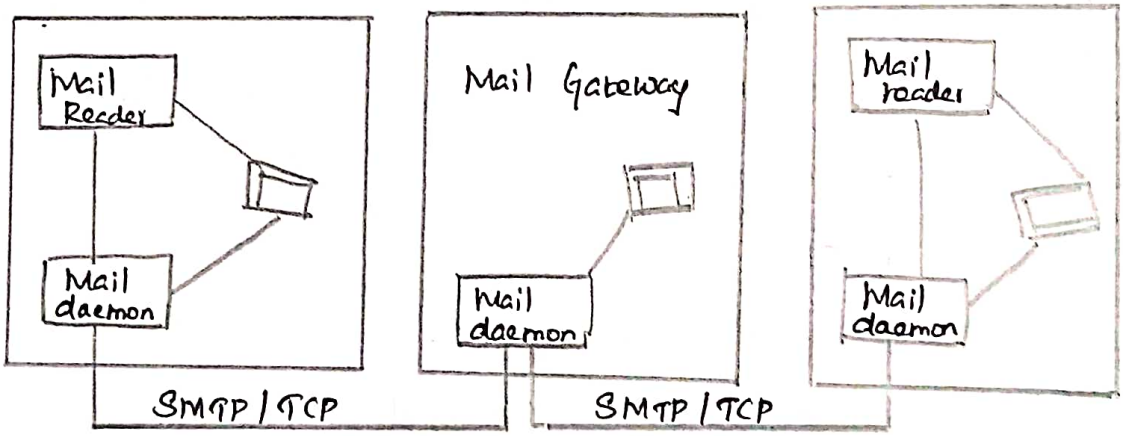
→ Third party encoding formats,

(i) BinHex : Proprietary format belonging to Apple.

(ii) Uuencode : for UNIX to UNIX encoding

(iii) Xencode : for binary to text encoding

Message Transfer of MIME:



→ MTA is a mail daemon (sendmail) active on hosts having mailbox, used to send email.

→ Mail passes through a sequence of gateways before it reaches the recipient mail server.

Internet Mail Access Protocol (IMAP):

→ Is an application Layer Internet protocol.

→ more capable wire protocol.

→ Similar to SMTP in many ways.

→ Is a Client/Server protocol running over TCP on port 143.

→ IMAP support three modes,

(i) offline

(ii) Online

(iii) Disconnected operation.

Operations of IMAP:

→ Client Commands,

(i) LOGIN

(ii) AUTHENTICATE

(iii) SELECT

(iv) EXAMINE

(v) CLOSE

(vi) Logout

→ Server Responses,

(i) OK

(ii) NO (NO Permission)

(iii) BAD (Incorrect Command.

→ Flags are used by Client to report user actions,

(i) SEEN

(ii) ANSWERED

(iii) DELETED

(iv) RECENT

IMAP4 :

(i) A user can check the e-mail header prior to downloading

(ii) A user can create, delete or rename mailboxes on the mail server.

(iii) A user can create a hierarchy of mailboxes in a folder for email storage.

Advantages of IMAP:

→ Supports new mail notification explicitly

→ Selective fetching of individual MIME body parts

→ Server-based search to minimize data transfer.

→ Servers may have extensions that can be negotiated.

Post Office Protocol (POP3)

→ POP3 is an application layer Internet Standard Protocol used by local e-mail clients to retrieve email from a remote server over a TCP/IP connection.

Versions of POP:

(i) The first called POP2

(ii) The current version POP3

Modes of POP:

(i) Delete mode – mail is deleted from the mailbox after retrieval.

(ii) Keep mode – mail after reading is kept in mailbox for later retrieval.

POP3 Commands :

(i) USER → opens the connection

(ii) STAT → display number of messages

(iii) LIST → get summary of messages

(iv) RETR → mailbox to access the messages

(v) DELE → delete a message

(vi) RSET → reset the session to its initial state

(vii) QUIT → log off the session

Advantages of IMAP over POP :

(i) IMAP is more powerful and more complex than POP

(ii) User can check the e-mail header prior to downloading

(iii) User can download partially, very useful in case of limited bandwidth.

(iv) User can create, delete or rename mailboxes on mailserver.

TELNET (Terminal Network)

→ TELNET is the original remote logging protocol, based on client-server program.

→ TELNET requires a logging name and password.

→ TELNET allows us to explain the issues and challenges related to the concept of remote logging.

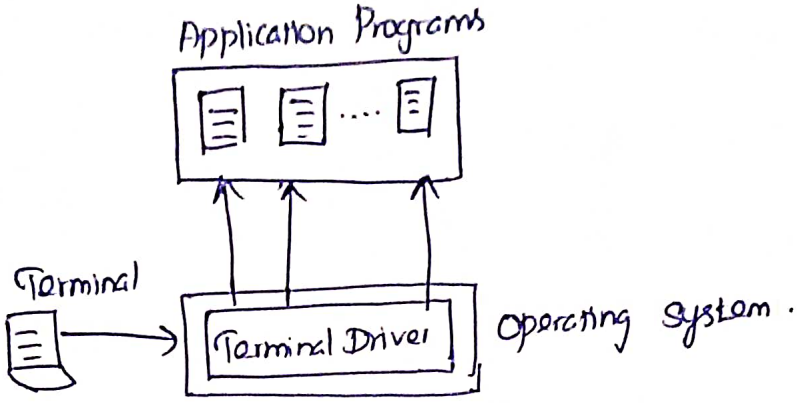
Types of TELNET Logging :

→ two types

(i) Local Logging

(ii) Remote Logging

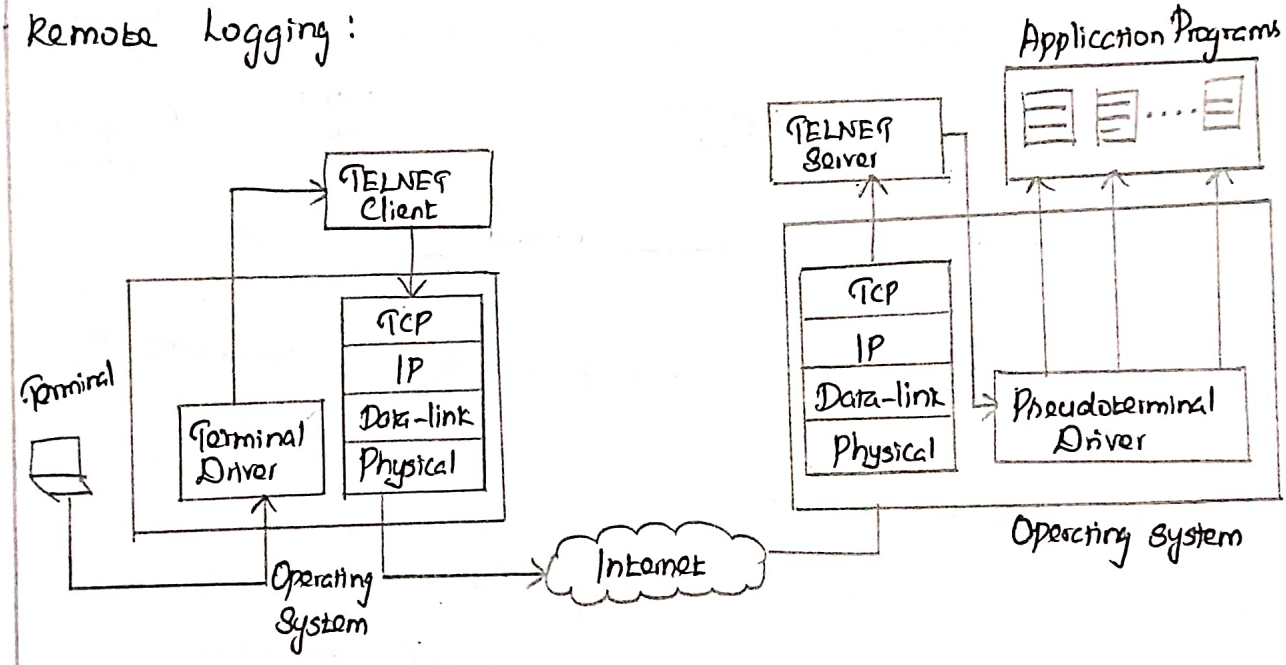
Local Login:



→ When a user logs into a local system, it is called local logging.

→ The terminal driver passes the characters to the operating system.

Remote Logging:



→ Remote Logging uses TELNET Client and TELNET server programs.

→ The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them.

TELNET Options:

→ TELNET lets the client and server negotiate options before or during the use of the service.

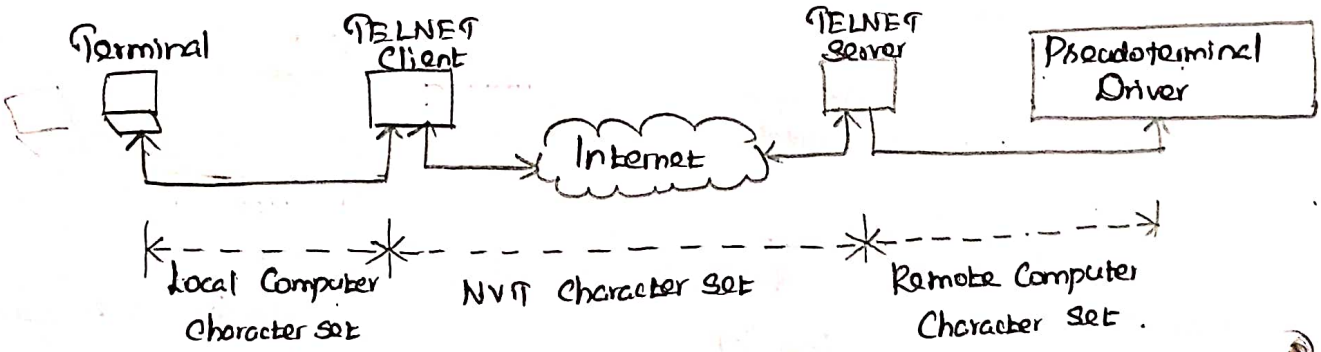
→ Users with simpler terminals can be default features.

TELNET Commands:

(i) Open
(ii) close
(iii) display
(iv) mode
(v) set
(vi) status
(vii) send
(viii) quit

Network Virtual Terminal: (NVT):

→ TELNET solves the problem by defining a universal interface called the Network Virtual Terminal (NVT) character set.

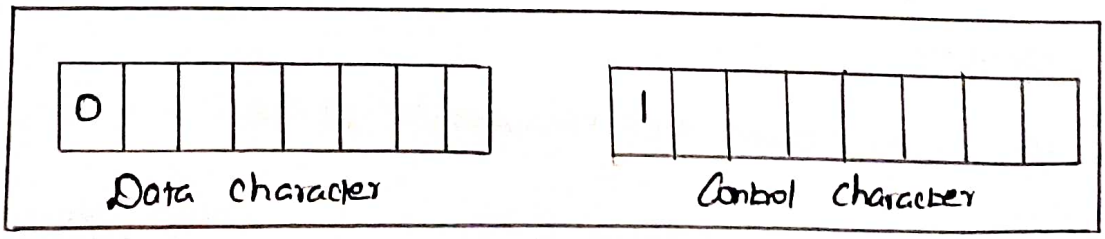


NVT Character Format:

→ NVT uses two sets of characters

(i) Data character – highest order bit is 0

(ii) Control character – highest order bit is 1



NVT Character format.

SSH (Secure Shell):

→ SSH is a secure application program that can be used today for several purposes such as remote logging and file transfer it was originally designed to replace TELNET.

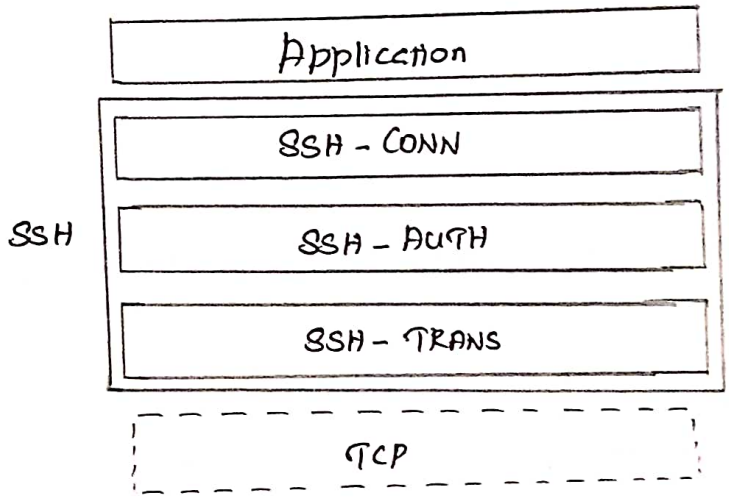
SSH Components:

→ three Components.

(i) SSH Transport Layer Protocol (SSH - TRANS)

(ii) SSH Authentication Protocol (SSH - AUTH)

(iii) SSH Connection Protocol (SSH - CONN)



SSH Transport - Layer Protocol (SSH - TRANS):

→ SSH first uses a protocol that creates a secured channel on the top of the TCP.

→ Exchange of several security parameters to establish a secure channel on the top of TCP.

SSH Authentication Protocol (SSH - AUTH):

→ After a secure channel is established between the client and the server and the server is authenticated for the client.

→ SSH can call another procedure that can authenticate the client for the server.

SSH Connection Protocol (SSH-CONN)

→ One of the services provided by the SSH-CONN protocol is multiplexing.

→ SSH-CONN takes the secure channel established by the two previous protocols and lets the client create multiple logical channels over it.

SSH Applications:

(i) SSH for Remote logging

(ii) SSH for file transfer

(iii) Port forwarding.

SSH Packet Format:

Length	Padding	Type	Data	CRC

Length → length of packet

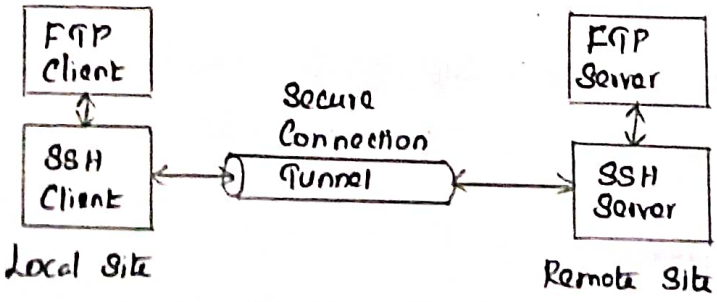
Padding → added to the packet.

Type → type of packet in SSH

Data → data transferred by packet.

CRC → error detection.

Securing FTP Applications Using SSH:



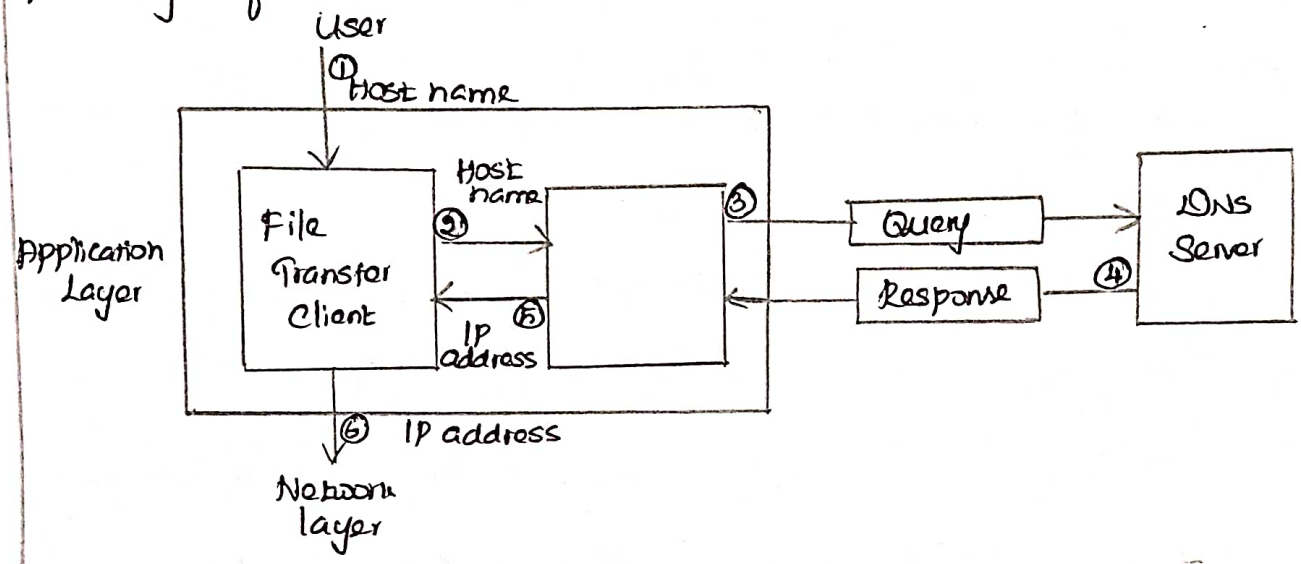
→ The FTP client can use the SSH client on the local site to make a secure connection with SSH server on the remote site.

Domain Name System (DNS):

→ DNS is used for name-to-address mapping

→ The DNS provides the protocol which allows clients and servers to communicate with each other.

Working of DNS:



Six steps:

(i) The user passes the host name to file transfer client.

(ii) The file transfer client passes the host name to DNS client

(iii) knows the address of one server.

(iv) DNS server responds with the IP address of the desired file transfer server.

(v) DNS server passes the IP address to the file transfer client.

(vi) The received IP address to access the file transfer server.

Name Space:

→ The names must be unique because the addresses are unique. two types,

(i) Flat (ii) Hierarchical.

Flat Name Space → name is assigned to an address.

Hierarchical Name space → each name is made of several parts.

Domain Name:

→ Each node in the tree has a label called as domain name.

→ A full domain name is a sequence of labels separated by dots(.)

→ If a label is terminated by a null string, it is called a fully qualified domain name (FQDN)

→ If a label is not terminated by a null string, it is called a partially qualified domain name (PQDN)

Distribution of Name Space:

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

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

Zone:

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

Root Server:

→ A root server is a server whose zone consists of a whole tree.

→ The servers are distributed all around the world.

DNS in the Internet:

→ In the Internet, domain name space (tree) is divided into three different sections.

(1) Generic domain

(2) Country domain

(3) Inverse domain.

DNS Resolution:

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

→ A resolution can be either recursive or iterative.

DNS Caching:

→ DNS handles this with a mechanism called caching.

(1) Time to live (TTL)

(2) TTL counter.

DNS Resource Record (RR):

→ The zone information associated with a server is implemented as a set of resource records.

→ five tuple structure.

(Domain Name, Type, class, TTL, value)

Types of Resource Records:

(1) A → 32 bit IPV4 address

(2) NS → Servers for zone

(3) CNAME → official name of a host

(4) SOA → beginning of a zone

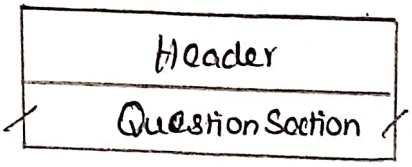
(5) MX → mail to mail server.

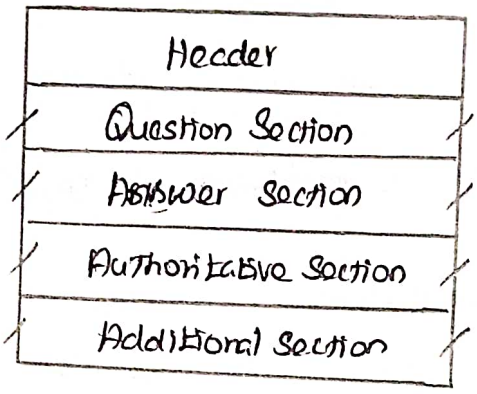
(6) AAAA → IPV6 address.

DNS Messages:

→ two types

(i) query (ii) response.





DNS Connections:

→ use either TCP or UDP.

→ well known port used by the server is port 53.

→ response message size is more than 512 bytes.

DNS Registrars:

→ New domains are added to DNS through a registrar.

→ registrars name and address can be found at,

http://www.internic.net.

DDNS (Dynamic Domain Name System):

→ The DNS master file must be updated dynamically.

→ The primary server updates the zone.

DNS Security:

→ DNS attacked in several ways including,

(i) Attack on Confidentiality

(ii) Attack on authentication and integrity

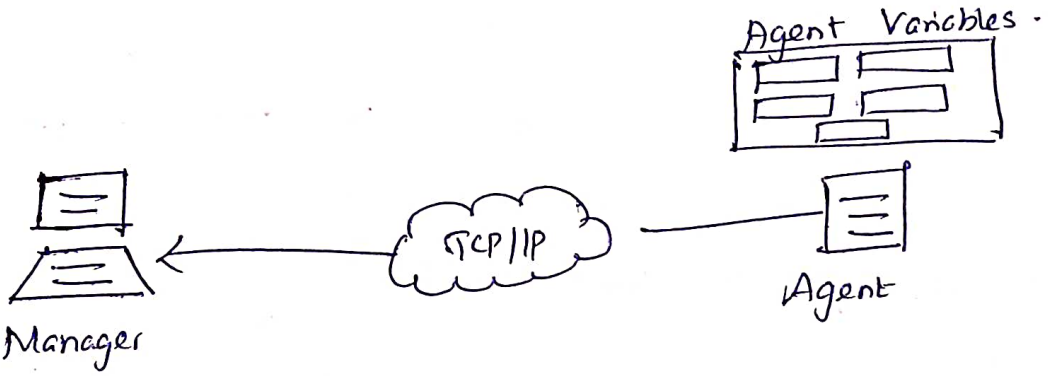
(iii) Attack on denial of service.

SNMP (Simple Network Management Protocol):

→ SNMP is a framework for managing devices in an internet using the TCP/IP Protocol Suite.

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

→ SNMP uses the concept of manager and agent.



SNMP Manager:

→ A manager is a host that runs the SNMP client program.

→ The manager has access to the values in the database kept by the agent.

SNMP Agent:

→ The agent in a router that runs the SNMP server program.

→ Agents can also contribute to the management process.

SNMP Management Components:

→ Management of internet is achieved through

Simple interaction between a manager and a agent.

→ Two protocols -

(a) Structure of Management Information (SMI)

(b) Management Information Base (MIB)

Structure of Management Information (SMI):

→ To use SNMP, we need rules for naming objects.

→ SMI is a protocol that define these rules.

→ Its functions are,

(i) To name objects

(ii) To define the type of data, that can be stored in an object.

(iii) To show how to encode data for transmission over the network.

Management Information Base (MIB)

→ Each agent has its own MIB, which is a collection of objects to be managed.

→ MIB classifies objects under groups.

SNMP Messages:

→ SNMP defines eight types of protocol data units (PDU)

(i) Get Request

(ii) GetNext Request

(iii) GetBulk Request

(iv) SetRequest

(v) Response

(vi) Trap

(vii) InformRequest

(viii) Report.