Computer Networks (CSC258)

Note By:

- **Roshan Bist**
- SNSC, Mahendranagar
- https://www.facebook.com/roshanbist.roshanbist.3
- https://www.facebook.com/notejunction/
- notejunction360@gmail.com

If my note really helps you, then you can support me on eSewa for my hard work.

eSewa ID: 9806470952

Unit-1

Introduction to Computer Network:-

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to process communication and resource sharing among wide range of users.

Uses:

i) Process communication through email, video conferencing, instant messanging etc.
ii) Enable multiple users to share a single hardware device like a printer or scanner.
iii) Enable file sharing across network.
iv) Make information easier to access and maintain among network users.
v) Allows sharing of software or operating programs on remote systems.

Benefits/Advantages:

i) It is highly flexible.
ii) It is an inexpensive system.
iii) It makes file sharing easier.
iv) It boosts storage capacity.
v) It increases cost efficiency.
vi) It allows for more convinent resource sharing.

Disadvantages:

i) It comes with the risk of security issues.
ii) It encourages people to become dependent on computers.
iii) It opens up a doorway for computer viruses and malware.
iv) If a computer network's main server breaks down, the entire system would become useless. Hence, it lacks robustness.
v) It requires an efficient handler.

⊛. Network Topologies:-

Network topology refers to the physical or logical layout of a network. It defines the way different nodes are placed and interconnected with eachother. Network topology also describes how the data is transfered between these nodes. Network topology is categorized into five basic models as follows:-

i) **Bus topology:** All the devices/nodes are connected sequentially to the same transmission line. This is simple, low-cost topology, but its single point of failure presents a risk.

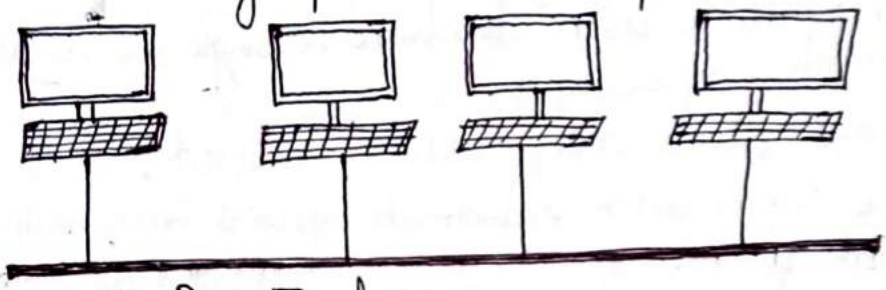


Fig. Bus Topology.

ii) **Star Topology:** All the nodes in the network are connected to a central device like a switch via cables. Failure of individual node or cable does not necessarily create downtime in the network but the failure of central device can. This topology is the most preferred and popular model.

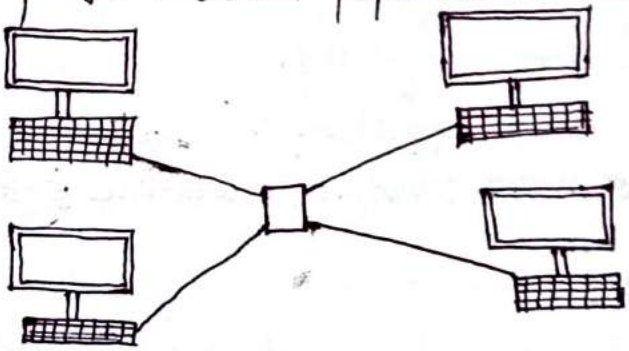


Fig. Star Topology

iii) **Ring Topology:** All network devices are connected sequentially to same transmission line like bus topology except that the transmission line ends at the starting node, forming a ring. It overcomes many of the limitations of bus topology.

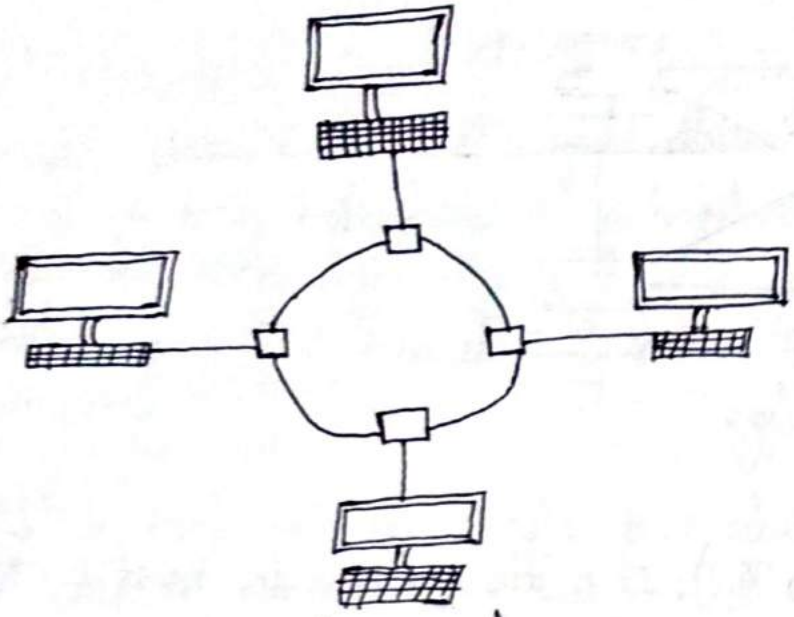


Fig. Ring Topology

iv) Tree Topology: A root node is connected to two or more sub-level nodes, which themselves are connected hierarchically to sub-level nodes. Physically, the tree topology is similar to bus and star topology; the network transmission line may have a bus topology, while low-level nodes connect using star topology.

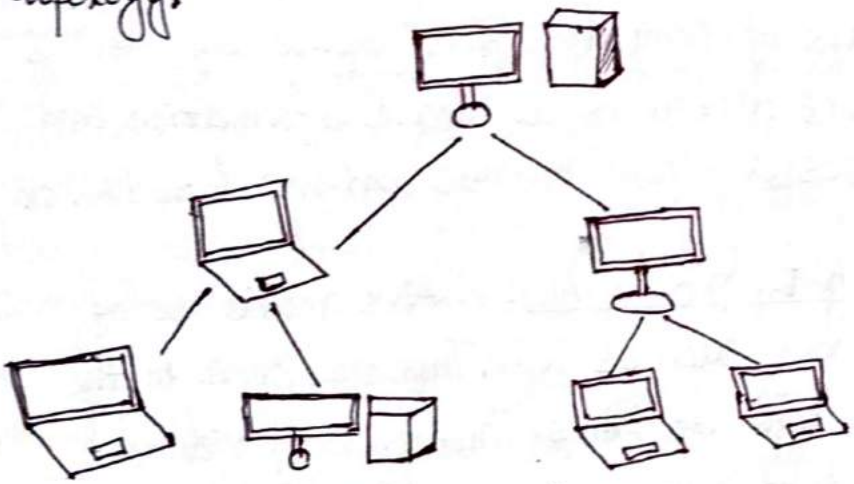


Fig. Tree Topology

v) Mesh Topology: In mesh topology each computer and network device is interconnected with one another. There are two forms of this topology: full-mesh and partially-connected mesh. In full mesh topology, every computer in the network has a connection and number of connections in network can be calculated as $n(n-1)/2$. where, n is number of computers in network. In partially connected mesh topology at least two of the computers in the network have connections to multiple other computers in that network.

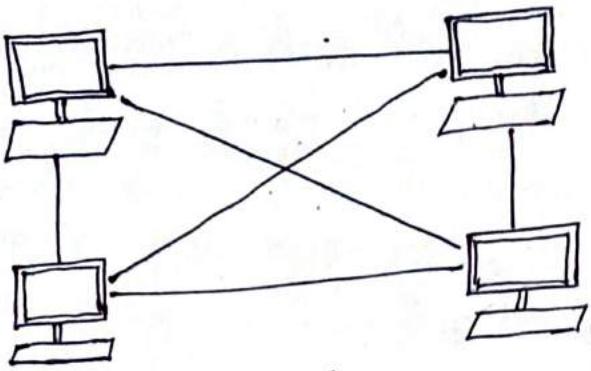


Fig. Mesh Topology

⊛ Network Types:

i) Personal Area Network (PAN): It is the smallest and most basic type of network. A PAN is made up of a wireless modem, one or two, phones, printers, tablets etc, and revolves ~~ab~~ around one person in the building. These types of networks are typically found in small offices or residences and are managed by one person or organization from a single device.

ii) Local Area Network (LAN): It is one of the simplest network. LAN's connect groups of computers and low-voltage devices together across short distances. to share information and resources. Enterprises typically manage and maintain LAN's.

iii) Wireless Local Area Network (WLAN): WLAN's make use of wireless network technology such as WiFi. Typically seen in the same types of applications as LAN's. These types of networks don't require devices that rely on physical cables to connect to the network.

iv) Campus Area Network (CAN): Larger than LAN's but smaller than MAN's. These types of networks are typically seen in universities, large K-12 schools, districts or small business. They can be spread across several buildings that are fairly close to each other so users can share resources.

v) Metropolitan Area Network (MAN): These types of networks are larger than LAN's but smaller than WAN's and incorporate elements from both types of networks. MAN's span an entire geographic area typically a town or city. Ownership and maintenance is handeled by either a single person or company.

vi) Wide Area Network (WAN): It is slightly more complex than a LAN. A WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other and one large network to communicate even when they are miles apart. The internet is the most basic example of a WAN connecting all computers together around the world.

⊛ Networking Types:-

i) Peer-To-Peer Network (P2P Network):- A peer-to-peer (P2P) network is group of computers each of which acts as a node for sharing files within the group. Instead of having a central server to act as a shared drive, each computer acts as the server for the files stored upon it.

These are same as a home network or office network. When P2P networks are established over the internet, the size of the network and the files available allow huge amounts of data to be shared. Peer-to-peer networks are usually associated with internet piracy and illegal file sharing.

ii) Multi-point Architectures:- Multipoint architecture means the channel is shared among multiple devices or nodes. In this architecture there is one transmitter and many receivers. In this architecture link is provided all times for sharing the connection among nodes. It does not provide security and privacy because communication channel is shared.

Client/Server Architecture: Client/Server architecture is a computing model in which the server hosts, delivers and manages most of the resources and services to be consumed by the client. This type of architecture has one or more client computers connected to a central server over a network or internet connection. This architecture is also known as a networking computing model because all the requests and services are delivered over a network.

Client/Server architecture is a producer/consumer computing architecture where the server acts as the producer and the client as a consumer. A server computer can manage several clients simultaneously, whereas one client can be connected to several servers at a time, each providing a different set of services.

Network Protocals:-

A network protocal is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. Network protocals are the reason we can easily communicate with people all over the world, and thus play a critical role in modern digital communications.

Similar to the way that speaking the same language simplifies communication between two people, network protocals make it possible for devices to interact with each other because of predetermined rules built into devices software and hardware. There are thousands of different network protocals, but they all perform one of three primary actions:

- → Communication
- → Network Management
- → Security.

Following are the few examples of the most commonly used network protocols:

- Hypertext Transfer Protocal (HTTP): This Internet protocal defines how data is transmitted over the internet and determines how web servers and browsers should respond to commands. This protocal appears at the beginning of various URLs or web addresses online.
- Secure Socket Shell (SSH): This protocal provides secure access to a computer, even if is on an unsecured network. SSH is particularly useful for network administrators who need to manage different systems remotely.
- Short Message Service (SMS): This communication protocal was created to send and receive text messages over cellular networks.

⇒ In short Protocal is a set of rules that governs communication. The key elements of protocal are syntax, semantics and timing.

Syntax → It refers to the structure and format of the information data.

Semantics → It refers to the meaning of each section of bits. It does an route identify the route to be taken or the final destination of the message.

Timing → It refers to two characteristics: when data should be sent and how fast it should be sent.

⊛. Network Standards:

Network standards define the rules for data communications that are needed for interoperability of networking technologies and processes. Standards help in creating and maintaining open markets and allow different vendors to compete on the basis of the quality of their products while being compatible with existing market products.

Types:

1. **De facto** → These are the standards that are followed without any formal plan or approval by any organization. They have come into existence due to traditions or facts. For example, the HTTP has started as a de facto standard.

2. **De jure** → These standards are the ones which have been adopted through legislation by any officially recognized standards organization. Most of the communication standards that are used today are de jure standards.

Standards Organizations:

Following are some of the noted standard organizations.

- → International Standards Organization (ISO).
- → International Telecommunication Union (ITU).
- → Instute of Electronics and Electrical Engineers (IEEE).
- → American National Standards Institute (ANSI).
- → Electronic Industries Association (EIA).

⊛ OSI Refrence Model:

OSI stands for Open Systems Interconnection. It has been developed by ISO → 'International Organization of Standardization', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

- → Application layer
- → Presentation layer } Software layers
- → Session layer
- → Transport layer ← Heart of OSI
- → Network layer
- → Data Link layer } Hardware layers
- → Physical layer

1. Physical Layer (Layer 1):- It is the lowest layer of the OSI refrence model. ~~is the physical layer.~~ It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s, and send them to Data Link layer, which will put the frame back together.

Network Layer, Data Link layer and Physical layer are also known as Lower layers or Hardware layers. Example of Physical layer devices are Hub, Repeater, Modem, Cables etc.

Functions of physical layer:

i) Bit synchronization → Clock controls both sender and receiver providing synchronization at bit level. (i.e. clock signal)

ii) Bit rate control → It defines transmission rate i.e, number of bits sent per second.

iii) Physical topologies → It specifies which network topology is used to arrange nodes/devices.

iv) Transmission mode → It defines the way in which data flows, like simplex, half-duplex and full-duplex.

2. Data Link Layer (Layer 2):- It is responsible for node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. It is divided into two sub layers:

i) Logical Link Control (LLC)
ii) Media Access Control (MAC).

Packet in Data Link Layer is called Frame. Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines. Switch & Bridge are Data Link Layer devices.

Functions of data link layer:

i) Framing → It provides a way for a sender to transmit a set of bits that are meaningful to the receiver.

ii) Physical Addressing → After creating frames data link layer adds physical address (MAC address) of sender and receiver in the header of each frame.

iii) Error Control → This layer detects and retransmits damaged or lost files.

iv) Flow Control → The data rate must be constant on both sides else the data may get corrupted.

3. Network Layer (Layer 3): It works for the transmission of data from one host to the other located in different networks. It also takes care of selection of shortest path to transmit the packet, from the number of routes available. Segment in network layer is refered as packet.

Functions:

i) Routing → The network layer protocals determine which route is suitable from source to destination. This function of network layer is known as routing.

ii) Logical Addressing → The sender & receiver's IP address are placed in the header by network layer to endentify each device.

4. Transport Layer (Layer 4): Transport layer provides services to application layer and takes services from network layer. It is responsible for the End to End delivery of the complete message.

- At sender's side → Transport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow and Error control to ensure proper data transmission.
- At receiver's side → Transport layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reasembling of the segmented data.

Data in the transport layer is called as segments. This layer is operated by the Operating System. It is called as Heart of OSI model.

Functions:

i) Segmentation and Reassembly → This layer accepts the message from the (session) layer, breaks into smaller units. The transport layer at the destination station reassembles the message.

ii) Service Point Addressing → This layer includes service point address which makes sure that the message is delivered to the correct process.

5. Session Layer (layer 5):

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

Functions:-

i) Session establishment, maintenance and termination → This layer allows the two processes to establish, use and terminate connection.

ii) Synchronization → This layer has check points considered as synchronization points and help to identify the errors and data loss is avoided.

iii) Dialog Controller → The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

6. Presentation Layer (layer 6):

Presentation layer is also called Translation layer. The data from application layer is extracted here and manipulated as per the required format to transmit over the network.

Functions:

i) Translation → for example ASCII to EBCDIC

ii) Encryption/Decryption → Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data known as plain text. A key value is used for encrypting as well as decrypting data.

iii) Compression → Reduces no. of bits that need to be transmitted on network.

7. Application Layer (Layer 7):-
This layer is implemented by network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
Example:- Applications, Browsers, Skype, Messenger etc.
Application layer is also called Desktop layer.

Functions:
→ Network Virtual Terminal
→ FTAM – File transfer access and management.
→ Mail Services
→ Directory Services.

⊛. TCP/IP Model and its comparision with OSI:

The OSI model was designed to describe functions of communication systems. But TCP/IP model was designed and developed by Department of Defence (DoD) in 1960s and is based on standard protocals. It stands for Transmission Control Protocal/Internet Protocal. It contains following four layers:-

1. Network Access Layer:- This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocals present in this layer allows for the physical transmission of data.

2. Internet Layer:- This layer corresponds to the functions of Network layer of OSI Model. It defines the protocals which are responsible for logical transmission of data, over the entire network. The main protocals residing at this layer are:
- IP → IP stands for Internet Protocal and is responsible for delivering packets. It has two versions IPv4 and IPv6.

- ICMP → It stands for Internet Control Message Protocal. It is responsible for providing hosts with information about network problems.
- ARP → It stands for Address Resolution Protocal. It's job is to find the hardware address of a host from a known IP address.

3. Host-to-Host Layer: This layer corresponds to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. The two main protocals present in this layer are:-

- Transmission Control Protocal (TCP) → It provides reliable and error-free communication between end systems. It also performs sequencing and segmentation of data. It is very effective protocal but lot of overheads leads to increase its cost.
- User Datagram Protocal (UDP) → It is good protocal if your application does not require reliable transport as it is very cost-effective. TCP is connection-oriented protocal but UDP is connectionless.

4. Process Layer:-

This layer performs functions of Application, Presentation and Session layer. It is responsible for node-to-node communication and controls user-interface specifications. Following are some of the protocals present on this layer:

- HTTP and HTTPS → HTTP stands for Hypertext transfer protocal. It is used by world wide web (www) to manage communication between web browsers and servers. HTTPS stands for HTTP-Secure. It is combination of HTTP with SSL (Secure Socket Layer).
- SSH → SSH stands for Secure Socket layer. It is a terminal emulation software and is more preferred because of its ability to maintain the encrypted connection. It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.

• **NTP** → NTP stands for Network Time Protocal. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions.

TCP/IP Comparision with OSI

TCP/IP	OSI
i) TCP refers to Transmission Control Protocal.	i) OSI refers to Open Systems Interconnection.
ii) TCP/IP has 4 layers.	ii) OSI has 7 layers.
iii) TCP/IP is more reliable.	iii) OSI is less reliable.
iv) TCP/IP does not have very strict boundries.	iv) OSI has strict boundries.
v) TCP/IP follow a horizontal path.	v) OSI follows vertical path.
vi) TCP/IP uses both session and presentation layer in application layer itself.	vi) OSI uses different session and presentation layers.
vii) TCP/IP developed protocals then model.	vii) OSI developed model then protocal.

⊛. Connection-less and Connection-Oriented Network Services:-

Both connection-less and connection oriented service are used for the connection establishment between two or more than two devices. These type of services are offered by network layer.

Connection-oriented service is related to the telephone system. It includes the connection establishment and connection termination. In this ~~method~~ service, handshake method is used to establish the connection between sender and receiver. This connection is preferred by long and steady communication.

Connection-less service is related to the postal system, It does not include any connection establishment and connection termination. This service does not give the guarantee of reliability. In this service, packets do not follow same path to reach destination. Thus connection is preferred by bursty communication.

⊛. Basic Concept of Internet and ISP's:

Internet → Internet is the largest computer network in the world, connecting ~~more~~ billions of computer users. ~~The~~ Internet is ~~used~~ most often used for three main purposes:

- → Communication
- → Buying and selling (e-commerce).
- → Searching for information.

Internet is a self-publishing medium which means that no one is in charge of the content found on it. ~~Any~~ Anyone can publish anything on the internet, wheather the information is true or not.

ISPs → An Internet Service Provider (ISP) is a company that provides customers with internet access. ISPs use fiber-optics, satellite, copper wire and other forms to provide internet access to its customers. To connect to an ISP, we need a modem and an active account. The ISP verifies our account and assigns our modem an IP address. Once, we have IP address we are connected to internet. We can use a router to connect multiple devices to the internet.

ISPs act as hubs on the internet since they are often connected directly to the internet backbone. Because of the large amount of traffic ISPs ~~handle~~ require high bandwidth connections to the internet. In order to offer faster speed to customers, ISPs must add more bandwidth to their backbone connection.

⊛ **Backbone Networks:** Backbone network is a network containing a high capacity connectivity infrastructure to different part of the network.

❖ **Bus Backbone:-** In Bus backbone the topology used for the backbone is bus topology.

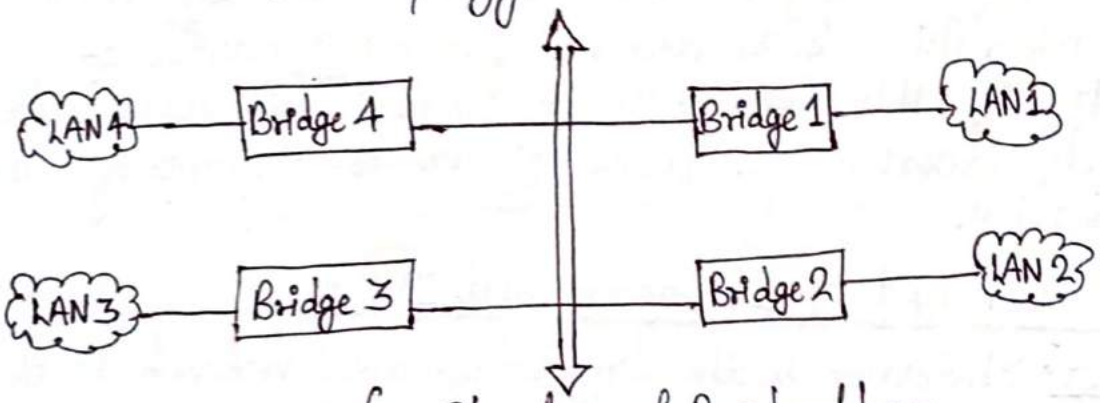


fig. Structure of Bus backbone.

The above Bus Backbone is a bridge based (bridge is the connecting device) backbone with four LANs. This type of backbone are basically used for connecting different buildings in an organization.

❖ **Star Backbone:-** The topology of this backbone is star topology.

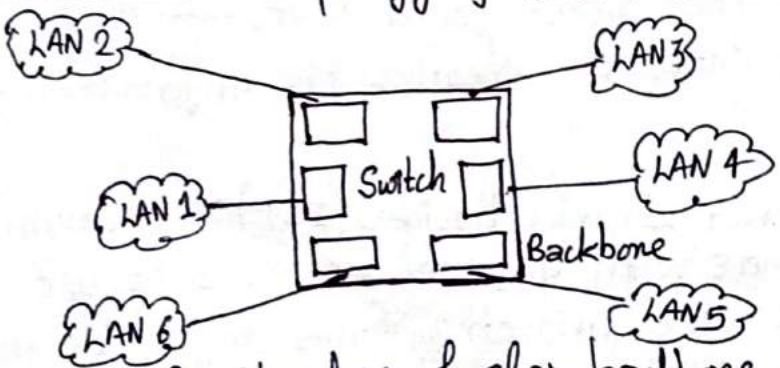


fig. Structure of star backbone

In above figure the switch does the job of backbone and connect the LANs. This type of backbone are basically used as distribution backbone inside a building.

⊛ Connecting remote LANs :-

Connecting remote LANs is one of the common application for a backbone network. This type of backbone network is useful when a company has several offices with LANs and needs to connect them. The connection can be done through bridges, sometimes called remote bridges. The bridges act as connecting devices connecting LANs and ~~point point~~ point-to-point networks such as leased telephone lines or ADSL lines. The following figure shows a backbone connecting remote LANs.

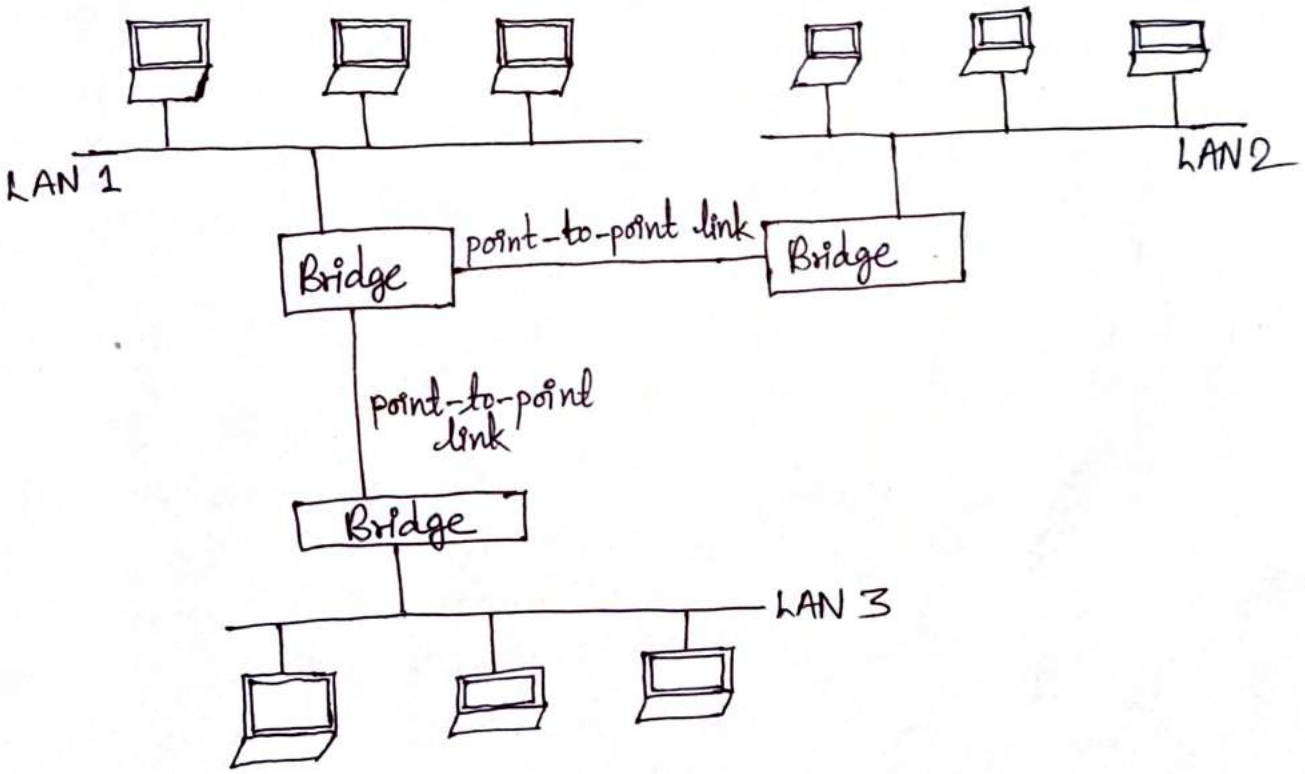


fig. Backbone connecting remote LANs.

Unit-2
Physical Layer and Networking Media

⊛Network Devices:

Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called network devices. These devices transfer data in a fast, secure and correct way over same or different networks. Network devices maybe inter-network or intra-network. Following are some of the key networking devices:

i) Repeater → A repeater is a networking device which operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. Repeaters do not amplify the signals. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a two port device.

ii) Hub → A hub is basically a multipoint repeater. A hub connects multiple wires comming from different branches. Hubs cannot filter data, so data packets are sent to all connected devices. There are two types of hub: active hub and passive hub.

Active hub have their own power supply and can clean, boost and ~~relu~~ relay the signal along with the network. Active hubs are used to extend maximum distance between nodes. Passive hubs have power supply from active hub and these hub can't clean, boost and relay the signals onto the network. Passive hubs can't be used to extend the distance between nodes.

iii) Switch → A switch is a multiport bridge with a buffer and a design that can boost its efficiency and performance. A switch is a data link layer device. The switch can perform error checking before foreworading data that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.

iv) Bridge → A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocal. It has a single input and single output port, thus making it a 2 port device.

There are two types of bridges: transparent bridges and source routing bridges. In transparent bridge the stations are completely ~~unaware~~ unaware whether a bridge is added or deleted from the network or not. In source routing bridge, routing operation is performed by source station and frame specifies which route to follow.

v) Routers → A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a network layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

⑧ Different Types of Transmission Medias:

Transmission media are the means by which a communication signal is carried from one system to another. Mainly there are two types of transmission medias: Wired and wireless.

ⓐ Wired transmission medias: It is also referred as guided media or bounded media. Signal being transmitted are directed and confined in a narrow pathway by using physical links. It has features like high speed and secure and used for comparatively shorter distances.

Types

i) Twisted pair cable: It consists of 2 seperately insulted conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted pair cable is futher of following two types:

Unshielded Twisted Pair (UTP):- This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications. Following are the advantages of UTP:

→ Least expensive
→ Easy to install
→ High speed capacity

Limitations:

→ lower capacity and performance in comparision to STP.
→ Short distance transmission due to attenuation.

Shielded Twisted Pair (STP):- This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

Advantages

→ Better performance at a higher data rate in comparision to UTP.
→ Eliminates crosstalk.
→ Comparatively faster.

Disadvantages

→ Bulky
→ Expensive
→ Comparatively difficult to install and manufacture.

9) Coaxial Cable:

It has an outer plastic covering containing 2 parallel conductors each having a seperate insulted protection cover. Coaxial cable transmits information in two modes: Baseband mode and Broadband ~~cable~~ mode. Cable TVs and analog television networks widely use Coaxial cables.

Advantages

→ High Bandwidth.
→ Better noise immunity.
→ Easy to install and expand.

Disadvantage

→ Single cable failure can disrupt the entire network.

iii) Optical Fibre Cable:- It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for transmission of large volume of data. The cable can be unidirectional or bidirectional.

Advantages

→ Increased capacity and bandwidth.
→ Light weight.
→ less signal attenuation.
→ Immunity to electromagnetic interference
→ Resistance to corrosive materials.

Disadvantages

→ Difficult to install and maintain
→ High cost
→ Fragile.

(b). Wireless / Unguided Media:

It is also referred to as wireless or unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Features:

→ Signal is broadcasted through air.
→ less Secure.
→ Used for larger distances.

There are three major types of unguided media:

i) Radiowaves → These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not to be aligned. Frequency range: 3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission.

ii) Microwaves → It is a line of sight transmission i.e, the sending and receiving antennas need to be properly aligned to each other. The distance covered by the signal is directly proportional to the height of the antena. Frequency Range: 1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

⊛. Circuit, Message & Packet Switching:-

Whenever we are dealing with a large network or say a very long-distance data transmission has to take place, this can't be done directly without any external hardware support. Hence, we must have a dedicated path for our data packets to traverse. Since there are so many choices for which path to take, so we have to select a particular path. This selecting of the path on which our data packets will be transmitted is known as Switching. We can categorize and sub-categorize the switching techniques as below:-

1). Circuit Switching:- The circuit switching technique establishes a dedicated path or channel between the sender and receiver for data transmission, and once a dedicated path is established then it does not terminate it until and unless the connection between the two data transmission point terminates.

We can say that it operates in a similar manner in which a telephonic network operates when we call someone, then a dedicated communication channel or path is established between we two, which remains open till we disconnect the phone call.

There are two methods through which we can perform multiplexing multiple signals into a single ~~or~~ channel or path.

- Frequency Division Multiplexing (FDM) → We use FDM when multiple data signals are combined for simultaneous data transmission through a shared communication channel. It divides total bandwidth into a series of non-overlapping frequency sub-bands, where each sub-band carries a different signal for data transmission. Radio transmission and optical fiber transmission to share multiple independent signals is its example.

- Time Division Multiplexing (TDM) → It divides the data transmission into time frames. It transmitts and receives independent signals over a common communication channel through synchronized switches at each end of the transmission line. This technique is widely used for long-distance communication links and also supports heavy data traffic loads from both the ends.

iii) Infrared → Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range: 300 GHz – 400 THz. It is used in TV remotes, wireless mouse, keyboard, printer etc.

Less imp ⑧ Ethernet Cable Standards: [Also called twisted pair cables]

ⓐ Ethernet copper twisted pair:- cables are broadly classified into two: Unshielded Twisted Pair (UTP) cable and Sheilded Twisted Pair (STP) cable. Thes cables are used for different shielding techniques to limit any signal from the cable or wire to escape and to reduce electromagnetic interface from outside environment.

i) UTP
ii) STP
} These two are already discussed.

ⓑ. Fiber Cable Standards:-

Fiber cable standards are mainly of two types: multimode and singlemode, which are as follows:-

	Multimode	Singlemode
IEC/ISO 11801	OM1, OM2, OM3, OM4	OS1, OS2
IEC 60793-2	-10 (A1b), -10 (A1a), -10 (A1a.2), -10 (A1a.3)	-50 (B1.1) -50 (B1.2)
ITU-T	G.651, G.651, G.651, G651	G.652 G.652.D
TIA-492	AAAA AAAB AAAC AAAD	CAAA CAAB.

Advantages:-
→ Establishment of a dedicated channel.
→ Improves data transmission rate.
→ Improves data loss.
→ Improves delay in the data flow.

Disadvantages:-
→ Establishing a dedicated channel sometimes takes a very long duration of time.
→ The amount of bandwidth required is more for establishing a dedicated channel.

2). Message Switching:- This technique was developed to act as an alternative to circuit switching. In this technique data is transmitted in form of messages which consist of entire data to be shared. Unlike circuit switching there's no dedicated path between the sender and the receiver, hence they are connected through several intermediate nodes which helps and ensures proper data transfer.

They have 2 important characteristics:-

i) Store & forward → Each node must have a storage capacity, because a message will only be delivered if the next node and the link between them are available to connect otherwise it will be stored indefinitely. A store and forward switch thus forwards a message only if sufficient resources are available and the next node is ready to accept the data. This was earlier used in telegraph message switching centres.

ii) Message delivery → The entire ~~information message~~ is compiled into a single message and then that message is transmitted from source to destination. To successfully reach its destination each message must contain the routing information in its header section.

Advantages:
→ Stores the message when the next node is not available.
→ Reduces traffic congestion.
→ Data channels are shared by network devices.
→ Manages traffic efficiently by assigning priorities.

Disadvantages:
→ Storing of message causes delays.
→ The whole network require a large storage capacity.

3). Packet Switching:

The packet switching technique transmits data through the network by breaking it down into several data packets for more efficient transfer and it also utilizes multiple vacant resources, these network devices direct or route the data packets to the destination where the receiving device then collects all of them and ressembles to get the proper orientation of message.

Types:

i) Connectionless Packet Switching:- This technique consists of multiple data packets, each data packet is individually routed, means every single data packet contains complete routing information in it's header section. This kind of packet switching technique is also known as Datagram switching.

ii) Connection-Oriented Packet Switching:- In this type of packet switching the data-packets are first assembled and then sequentially numbered. Now they are ready to travel across a predefined route sequentially. The information about the address is not required here, because all the data packets are sent in sequence. This technique is also known as Virtual Circuit switching.

Advantages:
→ Highly efficient
→ Faster
→ Cost-effective.
→ Digital
→ Reliable

⊛. ISDN [Interface & Standards]:

ISDN stands for Integrated Services Digital Network. It is a circuit-switched telephone network system, but it also provides access to packet switch networks that allows digital transmission of voice and data. This results in potentially better voice and data quality than an analog phone can provide.

It provides a packet-switched connection for data increments of 64 kilobits. It provided a maximum of 128 kilobits bandwidth in both upstream and downstream directions. A greater data rate was achieved through channel bonding.

ISDN Interfaces:-

1). Basic Rate Interface (BRI) → There are two data-bearing channels ('B' channels) and one signaling channel ('D' channel) in BRI to initiate connections. The B channels operate at a maximum of 64 kbps while the D channel operates at maximum of 16 kbps. The two channels are independent of eachother.

2). Primary Rate Interface (PRI) → Primary Rate Interface service consists of a D channel and either 23 or 30 B channels depending on the country you are in. PRI is not supported on the 7 Series. A digital pipe with 23 B channels and one 64 kbps D channel is present in PRI. PRI requires a digital pipe of 1.544 Mbps.

3). Broadband-ISDN (B-ISDN) → Narrowband ISDN has been designed to operate over the current communications infrastructure, which is heavily dependent on the copper cable however B-ISDN relies mainly on the evolution of fiber optics. According to CCITT, B-ISDN is best described as "a service requiring transmission channels capable of supporting rates greater than the primary rate."

ISDN Standard:

The ISDN works based on the standards defined by ITU-T (formally CCITT). The Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications on behalf of the International Telecommunication Union (ITU) and is based in Geneva, Switzerland. The various principles of ISDN as per ITU-T recommendation are:-

→ To support switched and non-switched applications.
→ To support voice and non-voice applications.
→ Reliance on 64-kbps connections.
→ Intelligence in the network.
→ Layered protocal architecture.
→ Variety of configurations.

Unit-3
Data Link Layer (DLL)

The data link layer (dll) transforms the physical layer, a raw transmission facility, to a link responsible for node-to-node communication. Specific responsibilities of the data link layer include framing, addressing, flow control, error control and media access control. The data link layer divides the stream of bits received from the network layer into managable data units called frames.

The data link layer adds a header to the frame to define the address of the sender and receiver of the frame. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

⊛ Functions:

i) **Framing** → The data link layer receives the stream of bits from the network layer divides into managable data units called frames.

ii) **Physical addressing** → If frames are to be distributed to different stations on the network. To define the physical address of the sender and/or receiver of the frame, the DDL adds a header to the frame.

iii) **Flow Control** → If the rate at which the data are consumed by the receiver is less than the rate produced by the sender, the data link layer deals with a flow control mechanism to prevent overrun the receiver.

iv) **Error Control** → The data link layer also deals with damaged or lost frames. By adding mechanisms to detect and retransmit lost frames increases reliability.

v) **Access Control** → When more than two or two devices are connected to the common link, data link layer protocals are necessary to determine which device has control over the link at any point of time.

The data link layer (dll) is divided into two sub layers as follows:

ⓐ Logical Link Control (LLC):- It is the upper sublayer of the data link layer of the open system interconnections (OSI) refrence model for data transmission. It acts as an interface between the network layer and the medium access control (MAC) sublayer of the data link layer. It is mainly used for its multiplexing property. It allows several network protocols to operate simultaneously within a multipoint network over the same network medium. LLC provides node-to-node flow and error control. Frame Sequence Numbers are assigned by LLC.

ⓑ Media Access Control (MAC):- It is the sublayer that controls the hardware responsible for interaction with the wired, optical or wireless transmission medium. It provides flow control and multiplexing for the transmission medium. It provides a control abstraction of the physical layer such that the complexities of physical link control are invisible to the LLC and upper layers of network stack. It encapsulates higher-level frames into frames appropriate for the transmission medium.

⊛ Framing and Flow Control Mechanisms:-

Framing → Frames are the units of digital transmission particularly in computer networks and telecommunications. Frame is continuously used in time division multiplexing process. Framing is the point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. framing is a function of the data link layer. Frames have headers that contain information such as error-checking codes. There are two types of framing:

i) Fixed size → The frame is of fixed size and there is no need to provide boundaries to the frame, length of the frame itself acts as delimiter.

ii) Variable size → In this there is need to define end of frame as well as beginning of next frame to distinguish.

Flow Control: It is a design issue at data link layer. It is technique that generally observes proper flow of data from sender to receiver. It is very essential because it is possible for sender to transmit data or information at very fast rate. and hence receiver can receive this information and process it.

Flow control is basically technique that gives permission to two of stations that are working and processing at different speeds to just communicate with one another. It is actually set of procedures that explains sender about how much data or frames it can transfer before data overwhelms receiver.

Flow Control Mechanisms:

1) **Stop-and-wait ARQ:** It is a method used in communication to send information between two connected devices. It ensures that information is not lost and received in the correct order. A stop-and-wait ARQ sends one frame at a time. After sending each frame, the sender doesn't send any frames until it receives an acknowledgement (ACK) signal. After receiving a good frame, the receiver sends an ACK. If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again.

In this case, the sender resends the same packet. The sender, waiting for a single ACK, receives two ACKs, which may cause problems if it assumes that the second ACK is for the next frame in the sequence. To avoid these problems, the most common solution is to define a 1 bit sequence number in the header of the frame. This sequence number alternates (from 0 to 1) in subsequent frames.

Stop-and-wait ARQ is inefficient compared to other ARQs, because the time between packets is twice the transit time. The throughput on the channel is a fraction of what it could be. To solve this problem, one can send more than one packet at a time. This is what is done in GO-BACK-N ARQ and the Selective Repeat mechanisms.

ii) Piggybacking → Piggybacking is a technique that controls the flow of information in both direction thereby improving the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B and vice-versa. Piggybacking combines the data frames and control info into the same frames.

Merit → It can save bandwidth since the data frame and ACK frame can be combined into just one frame.

Demerit → The algorithm is complicated because it needs to combine two arrival events into one.

iii) Go-Back-N ARQ → It is an specific technique of the ARQ protocol, in which the sending process continues to send a number of frames specified by a window size even without receiving an ACK packet from the receiver. The receiver process keeps track of the sequence number of the next frame it expects to receive, and sends that number with every ACK it sends. The receiver will discard any frame that does not have the exact sequence number it expects and will resend an ACK for the last correct in-order frame.

Once the sender has sent all of the frames in its window, it will detect that all of the frames since the first lost frame are outstanding and will go back to sequence number of the last ACK it received from the receiver process and fill its window starting with that frame and continue the process over again.

Go-Back-N ARQ is a more efficient use of a connection than stop and wait ARQ since unlike waiting for an acknowledgement for each packets, the connection is still being utilized as packets are being sent.

iii) Selective Repeat ARQ → In this mechanism unlike Go Back N ARQ, the receiving process will continue to accept and acknowledge frames sent after an initial error; this is the case of the sliding window protocal with both transmit and receive window sizes greater than 1.

The receiver process keeps track of the sequence number of the earliest frame it has not received, and sends that number with every ACK it sends. If a frame from the sender does not reach the receiver, the sender continues to send subsequent frames until it has emptied its window.

The receiver continues to fill its receiving window with the subsequent frames, replying each time with an ACK containing the sequence number of the earliest missing frames. Once the sender has sent all the frames in its window, it re-sends the frame number given by the ACKs, and then continues where it left off.

Maximum Window Size = Sequence Number Space / 2

⊛. Error Detection and Correlation Techniques:-

Data can be corrupted during transmission. Some applications require that errors be detected and corrected. Some applications can tolerate a small level of error. For example, random errors in audio or video transmissions may be tolerable, but when we transfer text, we expect a very high level of accuracy.

In a single-bit error, a 0 is changed 1 or a 1 to a 0. In a brust error, multiple bits are changed. For example, a 1100 s brust of impulse noise on a transmission with a data rate of 1200 bps might change all or some of the 12 bits of information. In a single-bit error, only 1 bit in the data unit has changed. A brust error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

Redundancy → The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver.

@. Error Detection:-

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver end fails, the bits are considered corrupted.

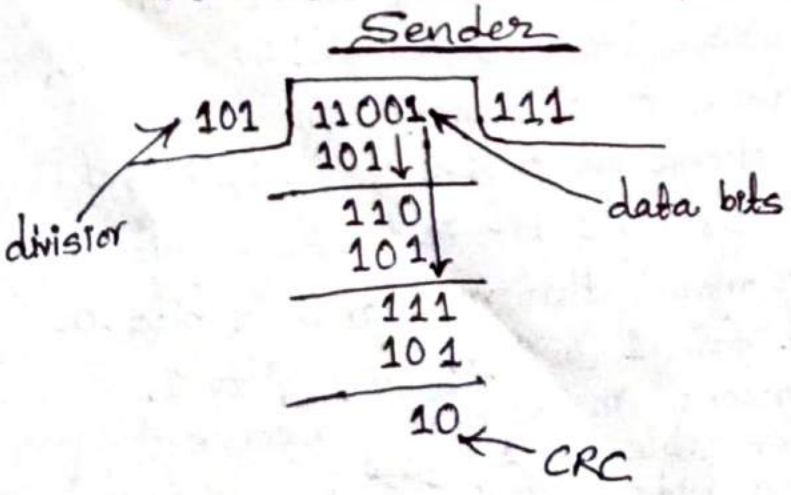
Parity Check: One extra bit is sent along with the original bits to make number of 1s either ever in case of even parity, or odd in case of odd parity.

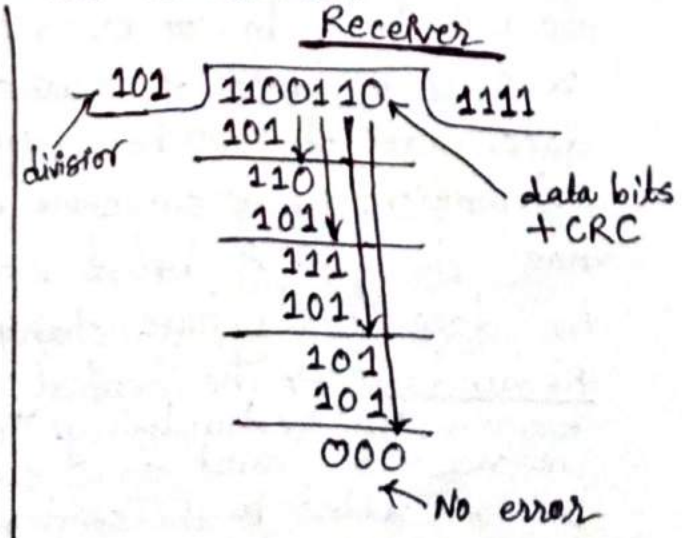
The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.

The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

Cyclic Redundancy Check (CRC):-

CRC technique involves binary division of the data being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.





At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occured in transit.

(b). Error Correction:-

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

→ Backward error correction: When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.

→ Forward error correction: When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

For correcting the errors, one has to know the exact position of the error. To achieve this, we have to add some additional redundant bits. Suppose r is the number of redundant bits and d is the total number of the data bits. The number of redundant bits r can be calculated by using formula: $2^r >= d+r+1$

For example:- If the value of d is 4, then the possible smallest value that satisfies the above relation would be 3.

Hamming Code:- To determine the position of the bit which is in error, a technique developed by R.W Haming is the Haming code which can be applied to any length of the data unit and uses the relationship between data units and redundant units.

Steps for Hamming code

→ An information of d bits are added to the redundant bits r to form d+r.

→ The location of each of the (d+r) digits is assigned a decimal value.

→ The r-bits are placed in the positions $2^0, 2^1, \ldots, 2^{k-1}$.

→ At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

For example:- Suppose the original data is 1010 which is to be sent. Then,

Total number of data bits 'd' = 4

Number of redundant bits $r = 2^r >= d+r+1$

i.e, $2^r >= 4+r+1$

Therefore, the value of r is 3 that satisfies the above relation.

Total number of bits = d+r = 4+3 = 7.

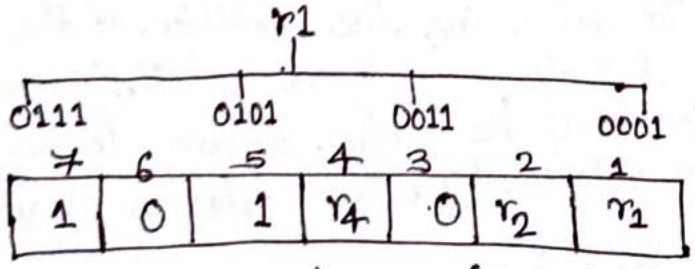
Determining the position of redundant bits:

The number of redundant bits is 3. The three bits are represented by r1, r2, r4. The position of the redundant bits are calculated with corresponds to the raised power of 2. Therefore, their corresponding positions are 2^0, 2^1 and 2^2.

The position of r1 = 1
The position of r2 = 2
The position of r4 = 4.

Determining the parity bits:

For r1 bit → The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.



We observe from above figure that the bit positions that includes 1 in the first position are 1,3,5,7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r1 is even, therefore the value of the r1 bit is 0.

⇒ Similarly for determining r2 bit we perform a parity check on the bit positions whose binary representation includes 1 in the second position. Similarly for r4 bit.

⊛ **Checksumming Method:** It is a error detection scheme, where data is divided into k segments each of m bits. In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum. The checksum segment is sent along with the data segments.

At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented. If the result is zero, the received data is accepted; otherwise discarded.

Example:

Original data

10011001	11100010	00100100	10000100
1	2	3	4

k=4, m=8

Sender

```
1→  10011001
2→  11100010
    ---------
   (1)01111011
      ↳      1
    ---------
    01111100
3→  00100100
    ---------
    10100000
4→  10000100
    ---------
   (1)00100100
      ↳      1
    ---------
Sum: 00100101
    ---------
CheckSum: 11011010
```

Receiver

```
1→  10011001
2→  11100010
    ---------
   (1)01111011
      ↳      1
    ---------
    01111100
3→  00100100
    ---------
    10100000
4→  10000100
    ---------
   (1)00100100
      ↳      1
    ---------
    00100101
    11011010
    ---------
Sum: 11111111
Complement: 00000000
```

Conclusion: Accept Data

⊛ **Channel Allocation Techniques:-**

Channel allocation is a process in which a single channel is divided and alloted to multiple users in order to carry user specific tasks. Channel allocation problem can be solved by two schemes: static channel allocation and dynamic channel allocation.

(a) Static Channel allocation in LANs and MANs:

It is the traditional approach of allocating a single channel among multiple competing users frequency division multiplexing (FDM). If there are N users, the bandwidth is divided into N equal sized ~~pro~~ portions each user being assigned one portion. Since each user has a private frequency band, there is no interface between users.

$$T = 1/(U*C-L)$$

$$T(FDM) = N*T(1/U(C/N)-L/N)$$

where, T = mean time delay,
C = capacity of channel,
L = arrival rate of frames,
1/U = bits/frame,
N = number of sub channels,
T(FDM) = Frequency Division Multiplexing Time.

(b) Dynamic ~~Chall~~ Channel Allocation:

Dynamic channel allocation is a strategy in which channels are not permanently allocated to the cells. When a user makes a call request then Base Station (BS) send that request to the Mobile Station Center (MSC) for the allocation of channels or voice channels. This way the likelihood of blocking calls is reduced. As traffic increases more channels are assigned and vice-versa.

(c) Multiple Access Protocol:

When nodes are connected and use a common link called a multipoint we need multiple access protocol to coordinate access to the link. It is of three types: Random access protocols, controlled access protocols and Channelization protocols.

1) Random Access Protocol:-

In this method no node is superior to another node and none is assigned the control over another. Any node can send data depending on medium's state (idle or busy). It has two features:-

→ There is no fixed time for sending data.
→ There is no fixed sequence of stations sending data.

The random access protocols are further subdivided as;

a) **ALOHA:-** The aloha protocol was designed as a part of a project at the University of Hawaii. It provided data transmission between computers on several of the Hawaiian Islands involving packet radio networks. Aloha is a multiple access protocol at the data link layer and proposes how multiple terminals access the medium without interference or collision. There are two different versions of ALOHA as follows:-

i) **Pure ALOHA →** Pure Aloha is an un-slotted, decentralized and simple to implement protocol. In pure ALOHA, the stations simply transmit frames whenever they want data to send. It does not check whether channel is busy or not before transmitting. In case, two or more stations transmit simultaneously, collision occurs and frames are destroyed.

Whenever any station transmits frame, it expects acknowledgement from the receiver. If it is not received within specified time, the station (i.e, node) assumes that frame has been destroyed. Then, the station waits for random amount of time and sends frame again. This randomness helps in avoiding more collisions. This scheme works well in small networks where the load is not much. But it is not suitable for largely loaded networks. This led to the development of Slotted Aloha.

Pure ALOHA vunerable Time = 2 × Frame Transmission Time (T_{fr}).

Throughput for pure ALOHA (S_{pure}) = $G \times e^{-2G}$

where G is no. of stations wants to transmit in T_{fr}.

Maximum throughput $(S_{pure})_{max} = 0.184$ for $G = 0.5$

Which means, in Pure ALOHA, only about 18.4% of time is used for successfull transmissions.

ii) **Slotted ALOHA →** In slotted ALOHA, the time of shared channel is divided into discrete intervals called slots. The stations are eligible to send a frame only at the beginning of the slot and only one frame per slot is sent. If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the beginning of the next time slot.

Slotted ALOHA vulnerable Time = Frame Transmission Time (T_{fr}).
Throughput for slotted ALOHA ($S_{slotted}$) = $G \times e^{-2G}$
where G is no. of stations wants to transmit in T_{fr} slot.
Maximum throughput $(S_{slotted})_{max} = 0.368$ for $G = 1$.
Which means, in slotted ALOHA, about 36.8% of the time is used for successful transmissions.

(b) Carrier Sense Multiple Access (CSMA):

It ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay.

CSMA access modes:-

i) 1-persistent → The node senses the channel, if idle sends the data, otherwise it continiously keeps on checking the medium for being idle and transmits unconditionally as soon as the channel gets idle.

ii) Non-persistent → The node senses the medium, if idle sends the data with p probability. If the data is not transmitted then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. It is used in WiFi and packet radio systems.

iii) O-persistent → Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

(c) Carrier Sense Multiple Access with Collision Detection (CSMA/CD):

This method adds on to the CSMA algorithm to deal with collision. In CSMA/CD, the size of a frame must be large enough so that collision can be detected by sender while sending the frame. So, the frame transmission delay must be at least two times the maximum propagation delay.

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

It was invented for wireless networks. The process of collission detection involves sender receiving acknowledgement signals. If there is just one signal then the data is successfully sent but if there are two signals then it means a collision has occured. To distinguish between these two cases, collision must have a lot of impact on received signal.

CSMA/CA avoids collision by:

i) Interframe space → Station waits for medium to become idle and if found idle does not immediately send data rather it waits for a period of time called interframe space or IFS. After this time it again checks medium for being idle.

ii) Contention Window → It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium not found idle.

iii) Acknowledgement → The sender re-transmits the data if acknowledgement is not received before time-out.

⑤ Ethernet Standards:

(802 denotes ethernet standard)

IEEE 802 specifies to a group of IEE standards. IEEE standards 802 are used for controlling the Local Area Network and Metropolitan Area Network. The user layer in IEEE 802 is serviced by the two layers: data link layer and physical layer. Generally used IEEE 802 specifications are as follows:-

IEEE 802.3	IEEE 802.4	IEEE 802.5
i) The IEEE 802.3 standard determines the CSMA/CD access control protocol.	i) IEEE 802.4 describes a token bus LAN standards.	i) IEEE 802.5 describes token ring standards.
ii) ~~Topoly~~ Topology used in IEEE 802.3 is Bus Topology.	ii) Topology used in IEEE 802.4 is Bus Topology.	ii) Topology used in IEEE 802.5 is Ring Topology.
iii) It has frame format size of 1572 bytes.	iii) It has frame format size of 8202 bytes.	iii) It has frame format size equal to variable size.

iv) Size of data field is 0 to 1500 bytes.	iv) Size of data field is 0 to 8182 bytes.	iv) No limit is of the size of the data field.
v) Minimum frame required is 64 bytes.	v) It can handle short minimum frames.	v) It supports both short and large frames.
vi) Modems are not required.	vi) Modems are required.	vi) Modems are required.
vii) Protocol is very simple.	vii) Protocol is extremely complex.	vii) Protocol is moderately complex.

⊛. Wireless LAN:

ⓐ **Spread Spectrum** → Spread Spectrum techniques are methods by which a signal (e.g. electrical, electromagnetic etc.) are generated with a particular bandwidth which spread in frequency domain resulting a signal with wider bandwidth. These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise, and jamming, to prevent detection and to enable multiple-access communications.

ⓑ **Bluetooth** → It is a wireless technology standard for exchanging data over short distances. It can connect several devices overcomming problems of synchronization. Bluetooth was standardized as IEEE 802.15.1 but the standard is no longer maintained. It is managed by the Bluetooth Special Interest Group (SIG), which has more than 35,000 member companies in the areas of telecommunication, computing, networking and consumer electronics.

ⓒ **Wi-Fi** → Wireless-Fidelity (Wi-Fi) is a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access, allowing nearby devices to exchange data by radio waves. These are the most widely used computer networks in the world used globally in laptop, tablets, mobiles, smart TVs etc.

⊛. Overview of Virtual Circuit Switching, Frame Relay & ATM:

Virtual Circuit Switching → It is a packet switching method where a path is established between the source and destination through which all packets will be routed during a call. The path is called virtual circuit because the connection appears to be a dedicated physical circuit.

Before the data transfer begins, the source and destination identify a suitable path for the virtual circuit. Additional parameters such as maximum packet size are also exchanged between the source and destination during call setup. The virtual circuit is cleared after the data transfer is completed.

Frame Relay → It is also a packet switching method that uses virtual circuits. These virtual circuits can be set up for each session or can be set up permanently. Frame Relay is designed for fiber optic cables with a very low bit error rate. Frame Relay has no error recovery and no flow control.

It is extensively used today in large corporations to interconnect the LANs between buildings. Frame relay operates at high speed (1.544 Mbps to 44.376 Mbps). It has large frame size of 9000 bytes. The damaged frame is simply dropped, there is no retransmission.

Asychronous Transfer Mode (ATM) → It is a switching technique used by telecommunication networks that ~~used~~ uses asychronous time-division multiplexing to encode data into small, fixed-sized cells. This is different from Ethernet or internet which use variables packet sizes for data or frames.

The ATM provides data link layer services that run on the OSI's Layer 1 physical links. It functions much like small-packet switched and circuit-switched networks, which makes it idle. ATM services have four different bit rate choices:

- → Available bit rate
- → Constant bit rate
- → Unspecified bit rate
- → Variable bit rate.

⊛. DLL Protocol: HDLC, PPP

(read comparing each points of both as differences, so will be easier to read)

(HDLC) High-Level Data Link Control → HLDC stands for high-level data link control. HDLC is a bit oriented protocol. HDLC is implemented by point-to-point configuration and also multi-point configurations. Dynamic addressing is not offered by HDLC. HDLC is used in synchronous media. HDLC is not compatible with non-Cisco devices. HDLC does not provide link authentication. HDLC is more costly comparatively.

8	8	8	>=0	16	8
Flag	Address	Control	Data	Checksum	Flag

Frame Format for HDLC Protocol.

(PPP) Point-to-Point Protocol → PPP stands for Point-to-Point Protocol. PPP is a byte oriented protocol. PPP is implemented by Point-to Point configuration only. Dynamic addressing is offered by PPP. PPP is used in synchronous media as well as asynchronous media. PPP is compatible with non-Cisco devices. PPP provides link authentication using various protocols. PPP is comparatively less costly.

1	1	1	1 or 2	Variable	2 or 4	1
Flag	Address	Control	Protocol	Payload	Checksum	Flag

Frame Format for PPP Protocol.

UNIT-4
Network Layer

⊛. Introduction & Functions:

Network layer selects and manages the best logical path for data transfer between nodes. It manages device addressing, tracks the location of devices on the network and determines the best way to move data. This layer contains hardware devices such as routers, bridges, firewalls and switches. Internet Protocol and Netware IPX/SPX are the most common protocols associated with the network layer.

Functions:

→ It translates logical network address into physical address, concerned with circuit, message or packet switching.
→ Routers and gateways operate in this layer.
→ Breaks larger packets into small packets.
→ Connection services are provided including network layer flow control, network layer error control and packet sequence control.

⊛. IPv4 Addressing:

IPv4 addresses are unique. They are unique in the sense that each address defines one and only one connection to the Internet. Two devices on the Internet can never have the same address at the same time. The 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 addresses are 32-bit numbers that are typically displayed in dotted decimal notation. A 32-bit address contains two primary parts: the network prefix and the host number. IP addresses are assigned by a central numbering authority called the Internet Assigned Numbers Authority (IANA). The IPv4 contains the following sections:

1) IPv4 Classfull Addressing:

In classful addressing the address space is divided into five classes: A, B, C, D and E. Each ~~part~~ class occupies some part of the address space. We can find the class of an address when address is given in binary notation or dotted-decimal notation. If the address is

given in binary notation, the first few bits can immediately tell us the class of address. If the address is given in decimal-dotted notation, the first byte defines the class.

<u>Class A</u> → Addresses use only the first byte (octet) to specify the network prefix, leaving 3 bytes to define individual host numbers.

<u>Class B</u> → Addresses use the first 2 bytes to specify the network prefix, leaving 2 bytes to define host address.

<u>Class C</u> → Addresses use the first 3 bytes to specify the network prefix, leaving only the last byte to identify hosts.

In binary format, with an x (can have 0 or 1 value) representing each bit in the host number, the three address classes can be represented as follows:-

first byte — second byte — and so on

```
00000000  xxxxxxxx  xxxxxxxx  xxxxxxxx  (Class A)
00000000  00000000  xxxxxxxx  xxxxxxxx  (Class B)
00000000  00000000  00000000  xxxxxxxx  (Class C)
```

Each bit x represents a power of 2 indicating how many host numbers can be created for a particular network prefix. Class A have 2^{24} possible host numbers, class B have 2^{16} and class C have 2^{8}.

⊛ <u>Finding the classes in binary and dotted decimal notation.</u>

Classes	Binary notation (first byte)	Dotted-decimal notation (first byte)	Range.
class A	0	0–127	0.0.0.0–172.255.255.255
class B	10	1128–19111	128.0.0.0–191.:
class C	110	1192–22311	192.,"–223.:
class D	1110	1224–23911	224."–239.:
class E	1111	1240–25511	240."–255.:

⊛ <u>Examples</u>: Find the class of each address.

a). 00000001 00001011 00001011 11101111
→ The first bit is 0. This is a class A address.

b). 11000001 100000011 00011011 11111111
→ The first 2 bits are 1 & 3rd bit is 0, This is class C address.

c). 14.23.120.8
→ The first byte is 14 (between 0 and 127); the class is A.

d) 252.5.15.111
→ The first byte is 252 (between 240 and 255); the class is E.

⊛. Rules for assigning Host ID:

Host ID's are used to identify a host within a network. The host ID are assigned based on following rules:

→ The Host ID must be unique.
→ Host ID in which all bits are set to 0 cannot be assigned because it is used to represent network ID of the IP address.
→ Host ID in which all bits are set to 1 cannot be assigned because it is used for broadcasting address to all hosts.

⊛ Rules for assigning Network ID:

The network ID is assigned based on following rules;-

→ Network ID cannot start with 127, because it is reserved for internal loop-back functions.
→ Network ID with all bits set to 0 cannot be assigned because it is used to denote specific host on local network.
→ Network ID with all bits set to 1 cannot be assigned because it is ~~used~~ reserved for an IP broadcast address.

⊛ Table (Representing host ID & Network ID):

Class	Network ID bit	Host ID bit
Class A	8	24
Class B	16	16
Class C	24	8
Class D	Not Defined	Not Defined.
Class E	Not Defined	Not Defined.

⊛ IPv4 Subnetting / Supernetting:

Subnetting → Subnetting is the procedure to divide the network into sub-networks. In subnetting, Network addresses bits are increased and the mask bits are moved towards right. It is implemented via variable length subnet masking. In subnetting, address depletion is reduced or removed. Each of the subnets has its own specific address.

A subnet address is created by borrowing bits from the host field and designating them as subnet field. The number of bits borrowed ~~from~~ varies and is specified by the subnet mask.

Why use subnetting?

When a network becomes too big with too much traffic, performance can begin to suffer. Breaking the network into smaller parts can help to increase network performance upto its original performance. A subnet allows routers to choose the right destination for packets. Subnetting can also improve network security.

How to create subnets?

To create a subnet, ~~net~~ we will start by fulfilling following three steps:

i) Determine the number of required network IDs.
   - → One for each LAN subnet.
   - → One for each wide area network connection.

ii) Determine the number of required host IDs per subnet.
   - → One for each TCP/IP host.
   - → One for each router interface.

iii) Finally create the following:
   - → A unique subnet mask for entire network.
   - → A unique subnet ID for each physical segment.
   - → A range of host IDs for each subnet.

Subnet Mask

A subnet mask is a 32-bit value that allows the device that is receiving IP packets to distinguish the network IP portion of the IP address. The 32-bit subnet mask is composed of 1s and 0s, where 1s represent positions that refer to the network subnet addresses.

Class	Format	Default Subnet Mask
A	network.host.host.host	255.0.0.0
B	network.network.host.host	255.255.0.0
C	network.network.network.host	255.255.255.0

Table: Default Subnet Mask

Q. If 200.100.10.66/26 is IPv4 address then answer the following questions:

a) Is this a host, network or broadcast address?
b) What is the subnet mask in dotted decimal?
c) What is the network address?
d) What is the broadcast address?
e) What is the first usuable host address?
f) What is the last usable host address?
g) How many usable hosts are in the network?
h) What is the next available network address?

Solution :-

IP address: 200.100.10.66/26

Subnet Mask: 11111111 11111111 11111111 11000000

= 255.255.255.192

Total subnets = $2^2 = 4$

Total hosts = $2^6 = 64$

Usable hosts = $2^6 - 2 = 64 - 2 = 62$

Valid Subnets (4^{th} octet) = 256 - 192 = 64.

Subnet (Network IP)	Usable IP Pool (first host to last host)		Broadcast IP
	First host	Last host	
200.100.10.0	200.100.10.1	200.100.10.62	200.100.10.63
200.100.10.64	200.100.10.65	200.100.10.126	200.100.10.127
200.100.10.128	200.100.10.129	200.100.10.190	200.100.10.191
200.100.10.192	200.100.10.193	200.100.10.254	200.100.10.255

aAns: It is host address

bAns: 255.255.255.192

cAns: 200.100.10.64/26

dAns: 200.100.10.127/26

eAns: 200.100.10.65/26.

fAns: 200.100.10.126/26

gAns: 62

hAns: 200.100.10.128/26

Classless Inter-Domain Routing (CIDR):-

It is basically the method that Internet service providers (ISPs) use to allocate a number of addresses. They provide address in a certain block size. We will receive a block of address from ISP like this: 192.168.10.32/28. This is telling us what our subnet mask is. The slash notation (/) means how many bits are turned on (1s). The maximum could only be /32 because a byte is 8 bits and there are 4 bytes in an IP address: (4×8 = 32). But we have to keep at least 2 bits for host bits so the largest subnet mask available relevent to the Cisco exams objectives can only be a /30.

Class A → /8 to /15
Class B → /16 to /23
Class C → /24 to /30.

@ Subnetting Class C Addressing:

Binary	Decimal Dotted	CIDR
00000000	255.255.255.0	/24
10000000	255.255.255.128	/25
11000000	255.255.255.192	/26
11100000	255.255.255.224	/27
11110000	255.255.255.240	/28
11111000	255.255.255.248	/29
11111100	255.255.255.252	/30

Table: Class C subnet masks.

i) No. of subnets → 2^x, where x is the number of masked bits (1s).

ii) No. of hosts per subnet → $2^y - 2$, where y is the number of unmasked bits (0s). [No. of usable hosts $2^y - 2$ & No. of hosts = 2^y]

iii) **Block size = 256 − subnet mask**

iv) Broadcast address → The number right before the next subnet.

v) Valid hosts → Numbers between the subnets, omitting the all-0s and all-1s. For example: If 64 is the subnet number and 127 is the broadcast address, then 65–126 is the valid host range. It is group of numbers between the subnet address and the broadcast address.

(b) Subnetting Class B Addresses:

Binary (3rd and 4th octet)	Decimal Dotted	CIDR
00000000 00000000	255.255.0.0	/16
10000000 00000000	255.255.128.0	/17
⋮	⋮	⋮
11111111 00000000	255.255.255.0	/24
11111111 10000000	255.255.255.128	/25
⋮	⋮	⋮
11111111 11111100	255.255.255.252	/30

Table: Class B subnet masks.

The process of subnetting a class B is pretty much the same as it is for a class C, except that we have more host bits and we start in the third octet. Use the same subnet numbers for the third octet with class B that we used for the fourth octet with class C, but add zero to the network portion and a 255 to the broadcast section in the fourth octet.

Example: Let we take same example of subnetting class C which we discussed before and now here we only discuss differ ones only neglecting same ones.

Solution:

Subnet Mask: 11111111 11111111 10

Q. If 172.16.0.0/17 is IPv4 address then answer the following questions:
(Same questions as in before question a to h).

Solution:-

IP address: 172.16.0.0/17

Subnet Mask: 11111111 11111111 10000000 00000000
= 255.255.128.0

Total Subnets = $2^1 = 2$

Total hosts = $2^{15} = 32768$

Usable hosts = $2^{15} - 2 = 32768 - 2 = 32766$

Valid Subnets (3rd octet) = 256 − 128 = 128

Valid Subnets (4th octet) = 256 − 0 = 256

Subnet (Network IP)	Usable IP Pool (First host to last host)		Broadcast IP
	First host	Last host	
172.16.0.0	172.16.0.1	172.16.127.254	172.16.127.255
172.16.128.0	172.16.128.1	172.16.255.254	172.16.255.255

aAns:- It is network address

bAns:- 255.255.128.0

cAns:- 172.16.0.0/17

dAns:- 172.16.127.255/17

eAns:- ~~172.16.127.254/17~~ 172.16.0.1/17

fAns:- 172.16.127.254/17

gAns:- 32766

hAns:- 172.16.128.0/17

ⓒ Subnetting Class A Address:-

Binary (2nd, 3rd and 4th octet)	Subnet Mask	CIDR value
00000000 00000000 00000000	255.0.0.0	/8
10000000 00000000 00000000	255.128.0.0	/9
⋮	⋮	⋮
11111111 11111111 10000000	255.255.255.128	/25
⋮	⋮	⋮
11111111 11111111 11111100	255.255.255.252	/30

Table: Class A subnet mask

Subnetting class A is also similar as class B or class C subnet. We must leave at least 2 bits for defining hosts. Again we have more host bits and we just use the same subnet numbers we used with class B and class C but we start using these numbers in the second octet.

Q. If 10.1.0.0/9 is IPv4 address then find all network address, broadcast address, usable host, Total subnets, total hosts, valid subnets.

Solution:- IP address: 10.1.0.0/9

Subnet Mask: 11111111 10000000 00000000 00000000
= 255.128.0.0

Total Subnets = $2^1 = 2$

Total hosts = $2^{23} = 8388608$

Usable hosts = $2^{23} - 2 = 8388606$

Valid Subnets (2nd octet) = 256 − 128 = 128

Valid Subnets (3rd octet) = 256 − 0 = 256

Valid Subnets (4th octet) = 256 − 0 = 256

Subnet (Network IP)	Usable IP Pool (first host to last host)		Broadcast IP
	First host	Last host	
10.0.0.0	10.0.0.1	10.127.255.254	10.127.255.255
10.128.0.0	10.128.0.1	10.255.255.254	10.255.255.255

Supernetting:

Supernetting is the procedure to combine the small networks into larger space. In subnetting, Network addresses' bits are increased, but in supernetting, Host addresses bits are increased. It is implemented via variable-length subnet masking.

Why supernetting?

The routing table contains the entry of a subnet mask for every network. If there are lots of small networks then size of the routing table increases. When the router has a big routing table then it takes a lot of time for the router to process the routing table. Supernetting is used to reduce the size of the IP routing table to improve network routing efficiency.

How does supernetting work?

All the networks are not suitable for supernetting. For any network to be supernetted it should follow three rules:

i) Contiguous → All the networks should be contiguous.

ii) Same size → All the networks should be of the same size and also a power of 2 i.e, 2^n.

iii) Divisibility → The first network ID should be divisible by the size of the block.

Note: If a binary number is divided by 2^n then last n bits are the remainder.

(Not more imp)

Example: Suppose we have four small networks with network ID as 201.1.0.0, 201.1.1.0, 201.1.2.0, 201.1.3.0. Check if this can be supernetted (or aggregated) or not.

Solution:

i) Contiguous → As we can see that all the four networks are class C networks. The range of the first network is from 201.1.0.0 to 201.1.0.255. The range of the second network start from 201.1.1.0. If we add 1 to the last IP address of the first network we get the starting IP address of the second network. Similarly we can check that all the networks are contiguous.

ii) Same Size → All the networks are of class C. Each network has 2^8 i.e, 256 hosts.

iii) Divisibility → The first IP address should be divisible by the total size of the networks. The total size of the network is 4×2^8 i.e, 2^{10}. The last 10 bits are the remainder if we divide the first IP address by 2^{10}. In order that they are divisible, the last ten bits should be 0.

First IP address binary representation: 11001001.00000001.00000000.
00000000

The last 10 bits are zero. Hence it is divisible by the size of the network. Hence all three conditions are satisfied.

2. Classless Addressing:

Classless addressing is a concept of addressing the IPv4 addresses which was adopted after the failure of classful addressing. The classful addressing leads to wastage of addresses as it assigns a fixed-size block of addresses to the customer. But, the classless addressing assigns a block of addresses to the customer according to its requirement which prevents the wastage of addresses. The classless IPv4 addressing does not divide the address space into classes like classful addressing. It provides a variable-length of blocks which have a range of addresses according to the need of users.

CIDR Notation:

Like in classful addressing, the address was divided into two parts Network ID and Host ID. Network ID define the address of the network and host id defines the host address in the corresponding network. The Network ID and Host ID part would vary with the classes.

The classless addressing also divides the IPv4 addresses into two parts referred to as 'prefix' and 'suffix'. Prefix defines the Network ID whereas suffix defines the host address in the corresponding network. The length of prefix(n) is added to the last of address separated by a slash. It is known as CIDR notation.

Properties: (OR restrictions on classless address blocks).

→ Addresses in a block must be in contiguous form.
→ The number of address in a block must be the power of 2. i.e, 2, 4, 8, 16, ...
→ The first address must be evenly divisible by the number of addresses.

Representation:

Let IP address be 192.168.10.1/28. (no. of mask bit)

Here we have 28 bits. So, we need to put 28 bits out of 32 bits as 1 and rest of bits as 0. will give us the mask for the Ip address block.

11111111.11111111.11111111.11100000
255. 255. 255. 240

Mask is: 255.255.255.240

Q. If 205.16.37.39/28 be the address. Now, find the first address, last address and the number of addresses.

Solution:-

Address (In Binary): 11001101 00010000 00100101 00100111
Mask of given address: 11111111 11111111 11111111 11110000

Now, The first address can be found by AND operation of given address with the mask.

Address: 11001101 00010000 00100101 00100111
Mask : 11111111 11111111 11111111 11110000

First Address: 11001101 00010000 00100101 00100000

The last address can be found by OR operation of given address with complement of the mask. Complement of number can be found by changing each 1 to 0 and each 0 to 1.

Address: 11001101 00010000 00100101 00100111
Mask complement: 00000000 00000000 00000000 00001111
Last Address: 11001101 00010000 00100101 00101111.

The number of addresses can be found by complementing the mask, interpreting it as a decimal number, and adding 1 to it.

Mask complement: 00000000 00000000 00000000 00001111
Number of addresses: 15+1 = 16

⊛ IPv6 Addressing and Its Features:

Internet protocol version 6 is a new addressing protocol designed to incorporate all the possible requirements of future Internet known to us as Internet version 2. This protocol works on Network Layer (ie, layer-3). It is a 128-bit alphanumeric string that identifies an endpoint device in the Internet Protocol Version 6 (IPv6) addressing scheme. It is arranged in eight groups, each of which is 16 bits. Each group is expressed as four hexadecimal digits and the groups are seperated by colours.

Example: FE80:CD00:0000:0CDE:1257:0000:211E:729C

The address can be shortened, because the addressing scheme allows the omission of any leading zero, as well as sequences consisting only of zeros. Here's the short version:

FE80:CD00:0:CDE:1257:0:211E:729C.

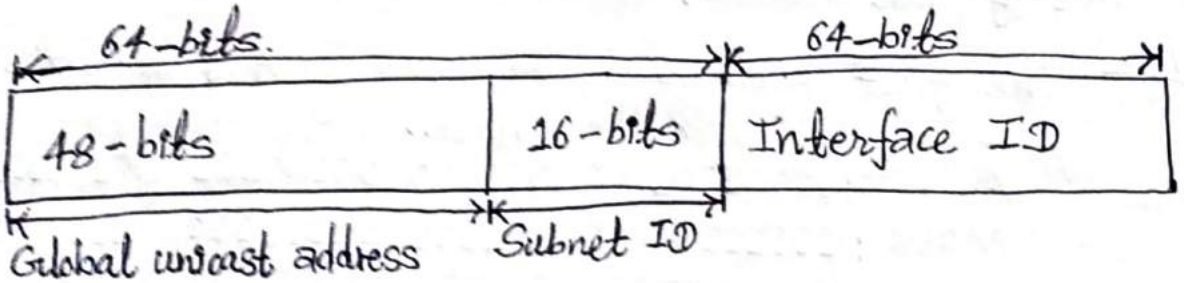


Fig. IPv6 address structure.

Features:

i) **Larger Address Space:-** In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×1034 different combination of addresses. According to an estimate, 1564 addresses can be allocated to every square meter of this earth.

ii) **Simplified Header:-** IPv6's header has been simplified by moving all unnecessary information and options to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 provided the fact that IPv6 address is four times longer.

iii) **End-to-end Connectivity:-** Every system has now unique IP address and can traverse through the Internet without using any translating components.

iv) **Auto-configuration:-** IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way, absence of a DHCP server does not put a halt on inter segment communication.

v) **Mobility:-** IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address.

vi) **No Broadcast:-** IPv6 does not have any broadcast support any more. It uses multicast to communicate with multiple hosts.

(*). IPv4 and IPv6 Datagram Formats:

IPv4 Datagram Formats:- Packets in the network (internet) layer are called datagrams. A datagram is a variable-length packet consisting of two parts: header and data. The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

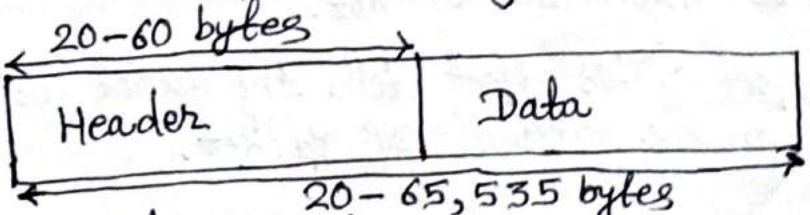


fig. IP Datagram for IPv4

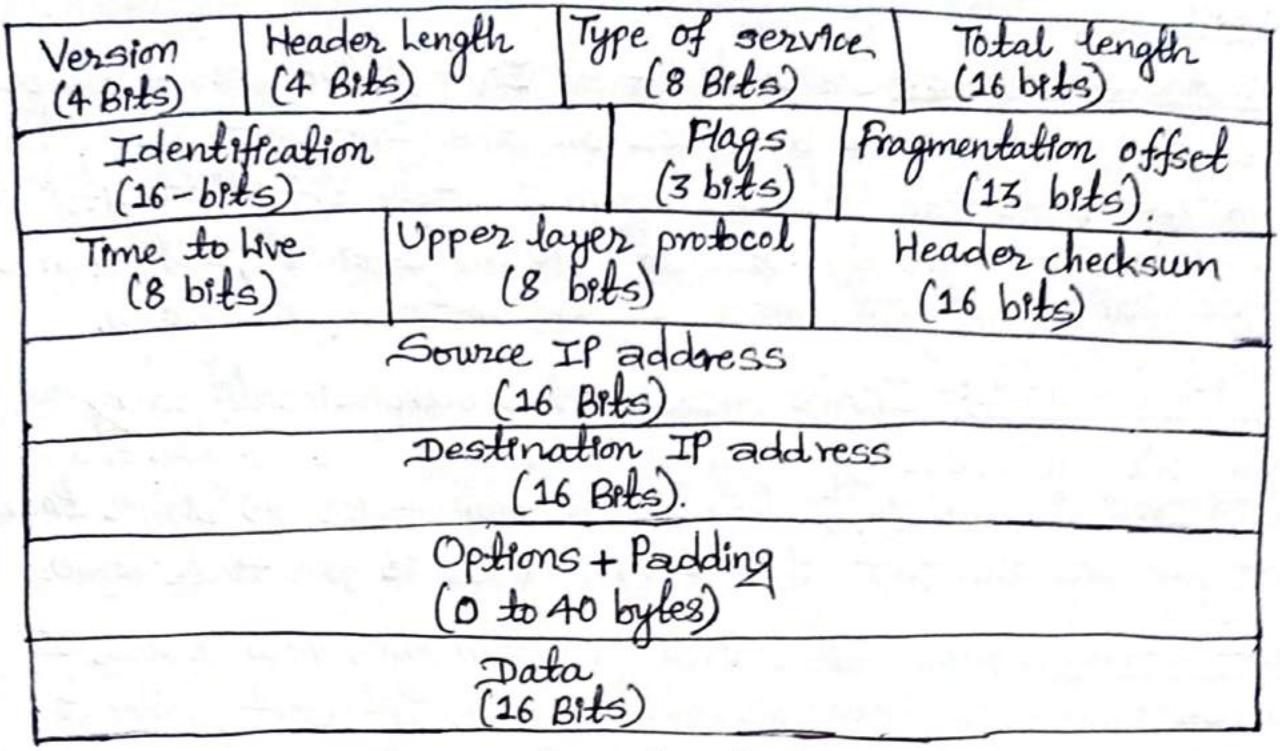


Fig. Header format of IPv4.

Version Number → It specifies the IP protocol version of the datagram. By looking at the version number the router can determine how to interpret the remainder of the IP diagram.

Header Length → It determines where in the IP datagram the data actually begins. Most IP datagrams do not contain options, so the typical IP datagram has a 20-byte header.

Type of service → The type of service bits were included in the IPv4 header to allow different types of IP datagrams to be distinguished from each other.

Datagram Length (Total Length) → Since this field is 16-bits long, the theoretical maximum size of the IP datagram is 65,535 bytes. However, datagrams are rarely larger than 15,00 bytes.

Length of data = total length - header length.

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

Flags → If IP Packet is too large to handle, these flags tells if they can be fragmented or not.

Fragmentation offset → This offset tells the exact position of the fragment in the original IP Packet.

Time-to-live → To avoid looping in the network, every packet is sent with some TTL value set, which tells network how many routers this packet can cross.

Protocol → This field value indicates the specific transport-layer protocol to which the data portion of this IP datagram should be passed.

Header checksum → This field is used to keep checksum value of entire header.

Source address → This 32-bit field define the address of the sender (or source) of the packet.

Destination address → This 32-bit field define the address of the receiver (or destination) of the packet.

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

Data → It contains the transport layer segment (TCP or UDP) to be delivered to destination.

IPv6 Datagram Formats:

IPv6 Datagram format has a much ~~larger~~ simpler packet header compared with IPv4, by including only the information needed for forwarding the IP datagram. IPv6 header allows the routers to process the IPv6 datagram packets more efficiently.

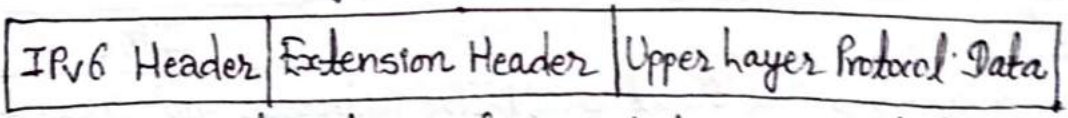


Fig. Structure of IPv6 datagram packet.

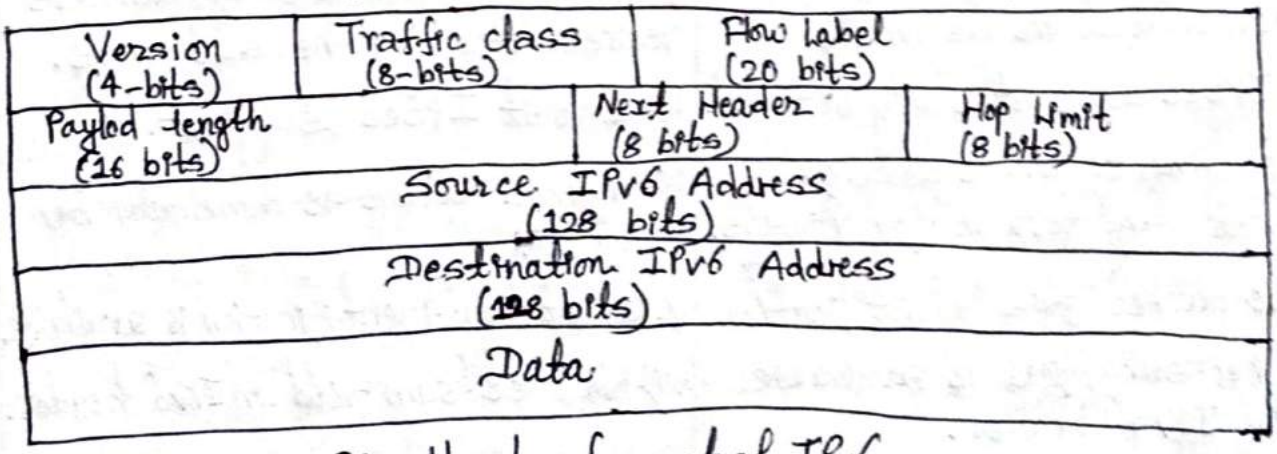


Fig. Header format of IPv6.

Version → It represents the version of Internet Protocol i.e, 0110.

Traffic Class → Among 8 bits, the most significant 6 bits are used for type of service and least significant 2 bits are used for Explicit Congestion Notification (ECN).

Flow label → This label is used to maintain the sequential flow of the packets belonging to a communication. This field also helps to avoid re-ordering of data packets.

Payload length → This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper layer data.

Next header → This field identifies the protocol to which the contents of this datagram will be delivered.

Hop limit → This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4.

Source Address → The field indicates the address of originator of the packet.

Destination Address → It provides the address of intended recipient of the packet.

Data → This is payload portion which will be removed from the IP datagram and passed on to the protocol specified in the next header field when the datagram reaches its destination.

Comparision of IPv4 and IPv6 Addressing:-

IPv4	IPv6
i) IPv4 addresses are 32-bit length.	i) IPv6 addresses are 128-bit length.
ii) IPv4 addresses are binary numbers represented in decimals.	ii) IPv6 addresses are binary numbers represented in hexadecimals.
iii) IPSec support is only optional.	iii) Inbuit IPSec support.
iv) Fragmentation is done by sender and forwarding routers.	iv) Fragmentation is done only by sender.
v) No packet flow identification.	v) Packet flow identification is available.
vi) Checksum field is available in IPv4 header.	vi) No checksum field in IPv6 header.
vii) It can generate 4.29 X 109 addresses.	vii) It can generate 3.4 X 1038 addresses.

Network Address Translation (NAT):

The number of home users and small businesses that want to use the internet in the past were connected to the Internet with a dial-up line. Which means that connection was for specific period of time. But the situation is different today. Home users and small businesses can be connected by an ADSL line or cable modem. Many are not happy with one address. With the shortage of addresses, this is a serious problem.

A quick solution to this problem is called network address translation (NAT). NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally. The traffic inside can use the large set: the traffic outside can use the small set.

To seperate the addresses used inside the home or business and the ones used for the Internet, the internet authorities have reserved three sets of addresses as below:

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

Any organization can use an address out of this set without permission from the Internet authorities. They are unique inside the organization, but they are not unique globally.

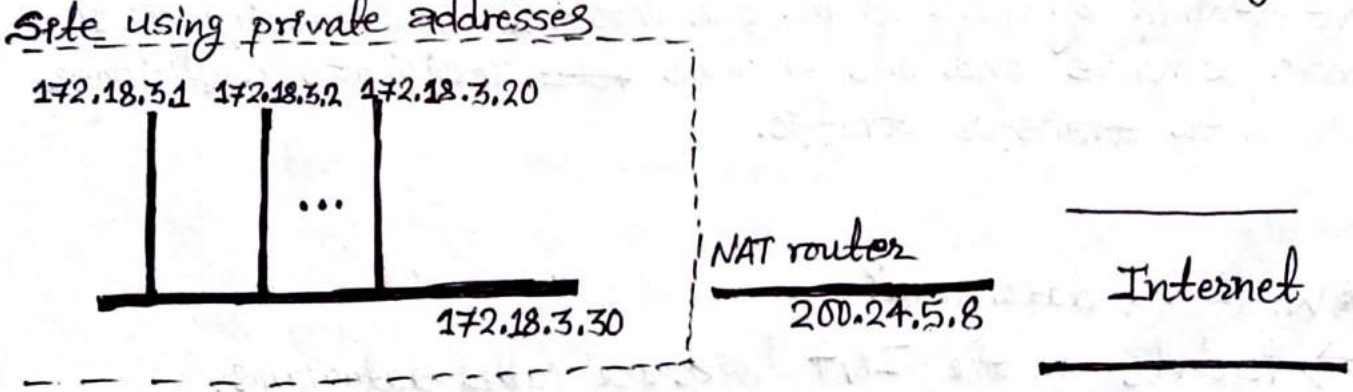


Fig: A NAT Implementation.

⊛. Example Addresses: Unicast, Multicast and Broadcast

Unicast Addressing Mode:- In this mode, data is sent only to one destined host. The destination field contains 32-bit IP address of the destination host. Here the client sends data to the targeted server. This type of information transfer is useful when there is a participation of single sender and single recipient. It is one-to-one transmission.

(one to all transmission)

Broadcast Addressing Mode:- It is classified into two types:

1) **Limited Broadcasting** → This method is used when we have to send stream of packets to all the devices over the network. It will append 255.255.255.255 (all the 32 bits of IP address set to 1) called as limited broadcast address in the destination address of the datagram header.

2) **Direct Broadcasting** → This is useful when a device in one network wants to transfer packet stream to all the devices over the other network. This is achieved by translating all the Host ID part bits of the destination address to 1, referred as Direct Broadcast Address in the datagram header for information transfer.

Multicast Addressing Mode:-

This mode is the mix of unicast and broadcast addressing mode. In this packet, the destination address contains a special address which starts with 224.x.x.x and can be entertained by more than one host. In multicasting, one or more senders and one or more recipients participate in data transfer traffic.

⊛ What is datagram?

⇒ Packets in the IPv4 layer are called datagrams.

Packets → Small segment of a larger message are packets. Data sent over computer networks such as internet is divided into packets.

* Routing

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Routing is broadly performed in many types of networks, such as the public switched telephone network (PSTN) and computer networks, such as the Internet. Routing is the path that network data or a packet takes to reach it's destination on a network. The routing process usually directs forwarding on the basis of routing tables. Routing tables maintain a record of the routes to various network destinations.

⊛. Types of Routing:-

@ Static vs Dynamic:

Static Routing → Static routing is a process in which we have to manually add routes in routing table. Static routing is used when we have very few devices to configure and when we know the routes which probably never change. Static routing does not handle failures in external networks well because any route configured manually must be updated or reconfigured manually to fix or repair lost connectivity.

Advantages:

→ Easily implemented in a small network.
→ No ~~other~~ overheads are produced on router CPU.
→ Secure because the routes are managed statically.
→ Bandwidth usage is not required between routers.

Disadvantages:

→ Unsuitable for large networks.
→ Large networks increase configuration complexity and time consumption.
→ Link failure can hinder traffic rerouting.
→ The administrator must be extra careful while configuring the routes.

Dynamic Routing → Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and routes to reach it. Automatic adjustment will be made to reach the network destination if one route goes down.

Advantages:
→ Suitable for all topologies.
→ Network size doesn't affect the router operations.
→ Topologies are adapted automatically to reroute the traffic.

Disadvantages:
→ Initially it could be complicated to implement.
→ Routes rely on current topologies.
→ The broadcasting and multicasting of routing updates makes it less secure.

(b) Unicast vs. Multicast:

Unicast → It is the simplest form of routing because destination is already known. In unicast there is only one sender and only one receiver. When we want to send data to multiple people then unicast will waste lots of bandwith. It does not perform well while streaming medias. An example of unicast is surfing web.

Multicast → In multicast routing data is sent only nodes which wants to receive the packets. In multicast there is only one sender but multiple receivers. When we want to send data to multiple people then multicast will utilize the bandwidth more efficiently. It does not perform well across large networks. An example of multicast is stock exchange.

(c) Link State vs Distance vector:

→ In link state, bandwidth required is more due to flooding and sending of large state packets. But in distance vector, bandwidth required is less due to local sharing, no flooding and sending of small state packets.

→ Link state make use of Dijkstra's algorithm while distance vector make use of Bellman Ford algorithm.
→ Link state routing has more traffic while distance vector routing has less.
→ Link state routing has faster coverages while distance vector routing has ~~too~~ slower.
→ Link state routing has difficult configuration while distance vector routing has easy configuration.
→ Link state routing has hierarchical structure while distance vector routing doesn't have hierarchical structure.

d) Interior vs Exterior:-

Interior routing protocols are designed for use within a contained network of limited size ~~whee~~ whereas exterior routing protocols are designed to link multiple networks together. Nearly all routing protocols are interior routing protocols. Only BGP is commonly used as an exterior routing protocol. Interior gateway protocol (IGP) used to refer to ~~inter ro~~ interior routing protocols and exterior gateway protocol (EGP) used to refer to exterier routing protocols.

⊛ Path Computation Algorithms:

Path computation algorithms are algorithms that helps to compute shorted path from a source to destination among several paths. Bellman Ford and Dijkstra algorithm are two main path computation algorithms.

a) Bellman Ford Algorithm:-

The Bellman-Ford algorithm is an algorithm that computes shortest paths from a single source vertex to all of the other vertices in a weighted graph. It is slower than Dijkstra's algorithm but more versatile, as it is capable of handling graphs in which some of the edge weights are negative numbers.

Similar to Dijkstra's algorithm this algorithm also initializes the source node to 0 and other nodes to infinity.

Then we go on relaxing all the edges repeatedly for n-1 times. Where n is the number of vertices.

What is Relaxation?

Ans:- If (u,v) is an edge between two vertices. then,

$$if(d[u] + w(u,v) < d[v])$$

then,

$$d[v] = d[u] + w(u,v)$$

min cost weight recently calculated

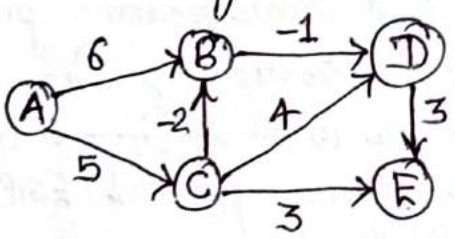
where,

d[u] = weight at source vertex

d[v] = weight at destination vertex.

w(u,v) = weight of edge from source to destination.

Example:- Find the shortest path of following graph by using Bellman Ford algorithm.



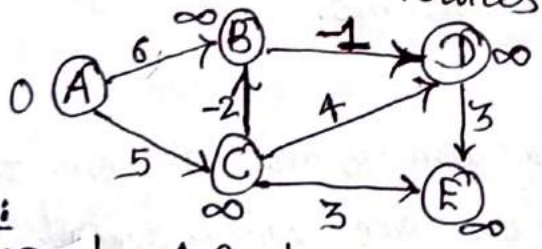
Solution:-

Let source vertex be A then we write all the edges in any order as: (A,B), (A,C), (C,B), (C,D), (C,E), (B,D), (D,E).

not compulsory for calculation

Since there are 5 vertices i.e, n=5, so no. of iterations for solving problem is (n-1) = (5-1) = 4.

Now we initialize the vertices and redraw the figure as;



i.e,

A	B	C	D	E
0	∞	∞	∞	∞

Iteration-1:

Now For edge AB: $d[A] + w(A,B) < d[B]$

or, $0 + 6 < \infty$ [True]

Then, $d[B] = d[A] + w(A,B)$

$= 0 + 6$

$= 6$

formula if(source + edge < destination) then destination = source + edge

Similarly for edge AC:

$d[A] + w(A,C) < d[C]$ i.e, $0 + 5 < \infty$ [True]

So, $d[C] = d[A] + w(A,C)$ or $d(C) = 0 + 5 = 5$

For edge CB:

always put recently calculated value

$d[C] + w(C,B) < d[B]$
$= 5 + (-2) < 6$ [True]
So, $d[B] = d[C] + w(C,B)$
$= 5 + (-2)$
$= 3$

For edge CD

$d[C] + w(C,D) < d[D]$
$= 5 + 4 < \infty$ [True]
So, $d[D] = 9$

For edge CE

$d[C] + w(C,E) < d[E]$
$= 5 + 3 < \infty$ [True]
So, $d[E] = 8$

For edge BD

$d[B] + w(B,D) < d[D]$
$= 3 + (-1) < 9$ [True]
$= 2 < 9$
So $d[D] = 2$

For edge DE

$d[D] + w(D,E) < d[E]$
$= 2 + 3 < \infty$ [True]
So, $d[E] = 5$

Now, we continue other iterations using table as follows:-

Iterations.	A	B	C	D	E
Initialization	0	∞	∞	∞	∞
1st Iteration		3	5	2	5
2nd Iteration		3	5	2	5
3rd Iteration		3	5	2	5
4th Iteration		3	5	2	5

since 0+6 < 3 [False], not true so, we copy same previous value

lowest values from calculated values are put here.

Here we get all values same as above so we can stop calculation here, but computer algorithm will go upto n-1 iterations.

We may get same values like this in any iteration according to question, Maybe 3rd iteration or, 4th or any other last iteration. Not necessary to get in second iteration.

Hence, shortest distances for respective vertices are as follows:-

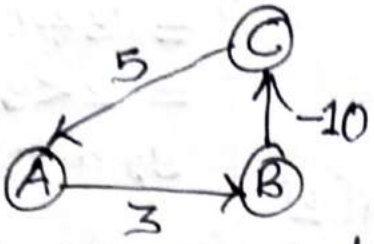
A = 0
B = 3
C = 5
D = 2
E = 5

Time Complexity of Bellman ford Algorithm: If E is the no. of edges then time complexity is $O(E(V-1))$. Since we iterate V-1 times. Or we can write it as $O(E.V)$. If we take E and V both as n we can write it as $O(n^2)$. In case of complete graph we have $\frac{n(n-1)}{2}$ no of edges. So, in this case time complexity will be $O[\frac{n(n-1)}{2}(n-1)]$.

Drawback of Bellman Ford Algorithm:

The main drawback of Bellman Ford algorithm is that, if we have negative weight cycle in graph then we can not get the correct solution.

For example:



Here, $5+3-10=-2$ (which is negative weight cycle).

b) Dijkstra's Algorithm:-

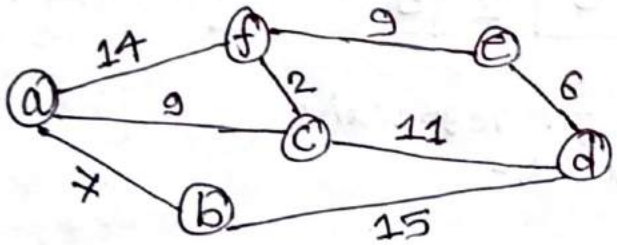
This is another approach of getting single source shortest paths. In this algorithm it is assumed that there is no negative weighted edge. This algorithm also starts with initializing source vertex to 0 and remaning other vertex to infinity. Then we start finding shortest path for each vertex using formula as;

if $(d[u]+w(u,v)<d[v])$ then,

$$d[v]=d[u]+w(u,v).$$

where, u = source vertex.
v = destination vertex.

Example:- Find the shortest paths from source node to all other vertices using Dijkstra's algorithm.



Solution:- Let source vertex be a, so we initialize initially source vertex 'a' with weight 0 and ∞ to all other remaining vertices. Now, we construct table for faster calculations. Calculations are same as Bellman Ford Algorithm only difference is that we use n-1 iterations there but no. of iterations are not fixed in this method.

once the vertex is selected no need to relax next time

Vertex Selected ↓	a	b	c	d	e	f
a	[0]	∞	∞	∞	∞	∞
b		[7] ←	9	∞	∞	14
c			[9]	22	∞	14
f				20	∞	[11]
d				[20]	20	
e					[20]	

[ ] → shows selected vertex. which is min in row.

calculations done in rough as;

~~d[b]+d~~

d[a]+w(a,b) < d[b]

0+7 < ∞ [True]

∴ d[b]=7.

Similarly for others.

Hence, the shortest paths with weights for different vertex are as follows;

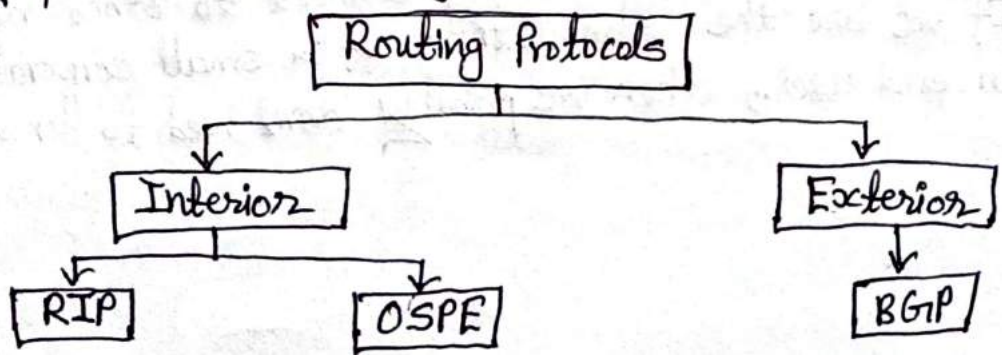
Shortest path from a to b = {a, b} with weight 7.
" " " a to c = {a, c} with weight 9.
" " " a to d = {a, c, d} with weight 20.
" " " a to e = {a, c, f, e} with weight 20.
" " " a to f = {a, c, f} with weight 11.

Disadvantage:- This algorithm may not work for negative weighted edge having graph.

Time complexity:- $O(V^2)$ where, V is no. of vertices in the graph.

✱ Routing Protocols:-

The routing protocol specifies how routers communicate to select the routes for data transfer. Different types of routing protocols are as follows:-



a) Routing Information Protocol (RIP):

In RIP distance vector routing protocol is used for data transmission. The maximum number of Hop in RIP is 15. Mechanism like split horizon, holdown etc. are used to prevent from incorrect or wrong routing information. RIP is a dynamic protocol used to find the best route from source to destination over a network. Compared to other routing protocols RIP is poor and limited sized network. RIP v1 (version 1), RIP v2 (version 2). and RIPng (next generation) are the types of routing information protocol (RIP).

~~b) Border Gateway Protocol (BGP):~~

b) Open Shortest Path First (OSPE):

It is the link-state routing protocol which is used to find the best path between the source and the destination. OSPE is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP). It is a network layer protocol which works on the protocol number 89 and used AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router.

c) Border Gateway Protocol (BGP):

BGP are the core routing protocol of the internet and responsible to maintain a table of Internet protocol networks which authorize network reaching capability between AS. BGP is expressed as path vector protocol. BGP is relevant to network administrators of large organizations which connect to two or more ISPs, as well as to ISPs who connect to other network providers. If we are the administrator of a small corporate network, or an end user, then we probably dont need to know about BGP.

Comparision of OSPF and BGP

OSPF	BGP
i) OSPF is an internal gateway protocol.	i) BGP is an external gateway protocol.
ii) OSPF is comparatively easy to implement.	ii) BGP is comparatively complex to implement.
iii) Port number 89 is used.	iii) Port number 179 is used.
iv) IP protocol is used.	iv) TCP protocol is used.
v) OSPF is mainly used on smaller scale networks that are centrally administered.	v) The BGP protocol is mainly used on very large-scale networks, like the internet.
vi) Dijkstra's algorithm is suitable to implement OSPF routing protocal.	vi) Best path algorithm is suitable to implement BGP routing protocol.

⊛ Overview of IPv4 to IPv6 Transition Mechanisms:-

In modern devices both versions IPv4 and IPv6 exist today simultaneously. Following are the some methods that can be used when transitioning a network from IPv4 to IPv6.

a) Dual Stack:- The process of running both IPv4 and IPv6 on the same devices is called dual stack. It is the simplest method to run IPv6 on all of the devices that are currently running IPv4. It is easy to implement, however IPv6 is not supported on all of the IPv4 devices, in these situations other methods must be considered.

b) Tunneling:- The process of transporting IPv6 traffic through an IPv4 network transparently is called tunneling. In this method a packet is encapsulated into a wrapper then enables its transport from a source to destination where it is decapsulated and retransmitted. The following list shows the different available tunneling methods:-

i) Manual IPv6 tunnels
ii) 6 to 4 tunnels
iii) IPv6 rapid deployment

iv) IPv4 compatible tunnels.
v) Generic Routing Encapsulation (GRE) IPv6 tunnels.

c) Translation:- The process of converting IPv6 traffic to IPv4 traffic for transport and vice versa is called translation. When using translation, the traffic is not encapsulated but is converted to the destination type. There are two methods of translation:

i) Network Address Translation → This method enables the ability to either statically or dynamically configure a translation of a IPv4 network address into an IPv6 network address and vice versa.

ii) NAT 64 → NAT 64 offers both stateless and stateful option when deploying.

⊛ Overview of ICMP/ICMP v6:-

ICMP stands for Internet Control Message Protocol which depends on internet to provide an error control. Since IP does not have a inbuilt mechanism for sending error and control messages. ICMP is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending the error messages and operations information.

e.g: The requested service is not available.

ICMP v6 is the version 6 of ICMP which plays far more important role in the operation of IPv6. ICMP v6 is used for several purposes beyond simple error reporting and signaling. It is used for:

→ Neighbour Discovery
→ Router Discovery
→ Managing hand-offs in Mobile IPv6.

⊛ Security Concepts: Firewall & Router Access Control

Firewall → A Firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between our internal network and incomming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic comming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry points called ports where information is exchanged with external devices.

Firewalls can either be software or hardware, though it's best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between network and gateway.

Firewalls can be divided into several different categories based on their general structure and method of operation. Following are some types:

- → Packet filtering firewalls
- → Circuit-level gateways
- → Stateful inspection firewalls
- → Application level gateways
- → Software firewalls
- → Hardware firewalls etc.

UNIT-5

Transport Layer

The transport layer is a 4th layer from the top. It works for the transmission of data from one host to the other located in different networks. It also takes care of selection of shortest path to transmit the packet from the number of routes available. Segment in network layer is referred as packet. The transport layer protocols are implemented in the end systems but not in the network routers. A computer network provides more than one protocol to the network applications. For example, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.

Functions of Transport Layer

i) Segmentation and Reassembly → This layer accepts the message from the (session) layer, breaks into smaller units. The transport layer at the destination station resembles the message.

ii) Service Point Addressing → This layer includes service point address which makes sure that the message is delivered to the correct process.

iii) Flow Control → In this layer, flow control is performed end to end.

iv) Error Control → Error control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error correction is done through retransmission.

v) Connection Control → It includes Connectionless Transport layer and Connection Oriented Transport layer. In connectionless transport layer each segment is considered as an independent packet and delivered to the transport layer at the destination machine. In connection oriented transport layer before delivering packets, connection is made with transport layer at the destination machine.

Services/Responsibilites of Transport Layer:

i) **Process to Process Delivery** → Transport layer requires a port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host. A port number is a 16 bit address used to identify any client-server program uniquely.

ii) **End-to-end Connection between Hosts** → Transport layer is also responsible for creating the end-to-end connection between hosts for which it mainly uses TCP and UDP.

iii) **Multiplexing and De-multiplexing** → Multiplexing allows simultaneous use of different applications over networks which are running on a host. De-multiplexing is required at the receiver side to obtain the data comming from various processes.

iv) **Congestion Control** → Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which lots of packets occur. In this situation Transport Layer provides Congestion Control in different ways like open loop, closed loop etc to prevent congestion.

v) **Data Integrity and Error Correction** → Transport layer checks for errors in the messages comming from application layer by using error detection codes and uses the ACK and NACK services to inform the sender if the data is arrived or not and checks for the integrity of data.

⊛. Transport Protocols:

The transport protocols provide services to their upper layers at well-defined interface points, which are also referred as ports. The IP address and the port are an important combination to set up a transport connection. TCP and UDP are the main transport layer protocols that provide different set of services to the network layer.

Transmission control protocol (TCP)	User datagram protocol (UDP)
i) TCP is a connection-oriented protocol.	i) UDP is the Datagram oriented protocol.
ii) TCP is reliable as it guarantees the delivery of data to the destination router.	ii) The delivery of data to the destination cannot be guaranteed in UDP.
iii) TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgement of data.	iii) UDP has only the basic error checking mechanism using checksums.
iv) TCP doesn't support Broadcasting.	iv) UDP supports Broadcasting.
v) TCP is comparatively slower than UDP.	v) UDP is faster, simpler and more efficient than TCP.
vi) TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	vi) UDP is used by DNS, DHCP, TFTP, SNMP, RIP and VoIP.

⊛. Connection Oriented and Connectionless Services:

Comparision Parameter	Connection-oriented service	Connection-less service
Definition	The service used to create an end to end connection betwn the senders to the receiver before transmitting the data over the network is called Connection-oriented service.	The service used to transfer the data packets betwn senders to the receiver without creating any connection is called connectionless service.
Virtual path	It creates a virtual path between the sender and receiver.	It does not create any virtual path between the sender and receiver.
Authentication	It requires authentication before transmitting the data packets to the receiver.	It does not require authentication before transferring data packets.

Data Packets Path.	All data packets are received in the same order as those sent by the sender.	Not all data packets are received in the same order as those sent by the sender.
Bandwidth Requirement	It requires a higher bandwidth to transfer the data packets.	It requires low bandwidth to transfer the data packets.
Examples	TCP is an example of a connection-oriented service.	UDP is an example of connectionless service.

⊛ Congestion Control:

An important issue in a packet-switched network is congestion. Congestion in a network may occur if the load on the network is greater than the capacity of network. Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity. Congestion happens in any system that involves waiting. In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control and closed-loop congestion control.

1) **Open-Loop Congestion Control:** In open-loop congestion control, policies are applied to prevent congestion before it happens. Following are the policies used to prevent congestion in open-loop.

Retransmission Policy → If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in network. However, a good retransmission policy can prevent congestion.

Window Policy → The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control. The Selective Repeat window tries to send the specific packets that have been lost or corrupted.

Acknowledgement Policy → The acknowledgement policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge

every packet it receives, it may slow down the sender and help prevent congestion. Sending fewer acknowledgments means imposing less load on the network.

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

Admission Policy → It also can prevent congestion in virtual-circuit networks. A router can deny establishing a virtual-circuit connection if there is congestion in the network or if there is a possibility of future congestion.

2. Closed-Loop Congestion Control: In closed-loop congestion control, polices are applied to prevent congestion after it happens. Following are the policies used to prevent congestion in closed-loop.

Backpressure → It is a mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This technique can be only applied to virtual circuit networks.

Choke Packet → It is a packet sent by a node to the source to inform it congestion. In backpressure the warning is from one node to it's upstream node but in choke packet method, the warning is from the router, which has encountered congestion.

Implicit Signaling → In implicit signaling, there is no communication between the congested node(s) and the source. The source gusses that there is a congestion somewhere in the network from other symptoms.

Explicit Signaling → In explicit signaling, the signal is included in the packets that carry data.

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

Forward Signaling → A bit can be set in a packet moving in the direction to the congestion. This bit can warn the destination that there is congestion.

TCP Congestion Control:

TCP's general policy for handling congestion consists of following three phases:

i) **Slow Start Phase** → It helps to avoid sending more data than the network is capable of forwarding. Initially sender sets Congestion window size = Maximum Segment Size (1MSS). After receiving each acknowledgment, sender increases the congestion window size by 1MSS. In this phase, the size of congestion window increases exponentially. The Formula is;

Congestion Window Size = Congestion Window Size + Maximum Segment Size

In this phase after every RTT the congestion window size increments exponentially.

Initially cwnd = 1 (cwnd: congestion window)

After,
1RTT, cwnd = $2^1 = 2$
2RTT, cwnd = $2^2 = 4$
3RTT, cwnd = $2^3 = 8$ (RTT: Round-Trip Time)

ii) **Congestion Avoidance Phase** → It is also called additive increment. This phase starts after the threshold value also denoted as ssthresh. The size of congestion window increases additive. After each RTT cwnd = cwnd+1.

Initially cwnd = i
After,
1RTT, cwnd = i+1
2RTT, cwnd = i+2
3RTT, cwnd = i+3.

iii) **Congestion detection** → It is also called multiplicative decrement. Retransmission is needed to recover a missing packet which is assumed to have been dropped by a router due to congestion. Retransmission can occur in one of two cases: when the RTO timer times out or when three duplicate ACKs are received.

⊛. Traffic Shaping Algorithms:

Traffic Shaping is a mechanism to control the amount and the rate of the traffic sent to the network. Approach of congestion management is called Traffic Shaping. Traffic Shaping helps to regulate rate of data transmission and reduces congestion. There are two types of traffic shaping algorithms: Leaky Bucket and Token Buket.

Leaky bucket → The leaky Bucket algorithm is used to control rate in a network. It is implemented as a single server queue with constant service time. If the bucket overflows then packets are discarded. In this algorithm the input rate can vary but the output rate remains constant. This algorithm saves busty traffic into fixed rate traffic by averaging the data rate.

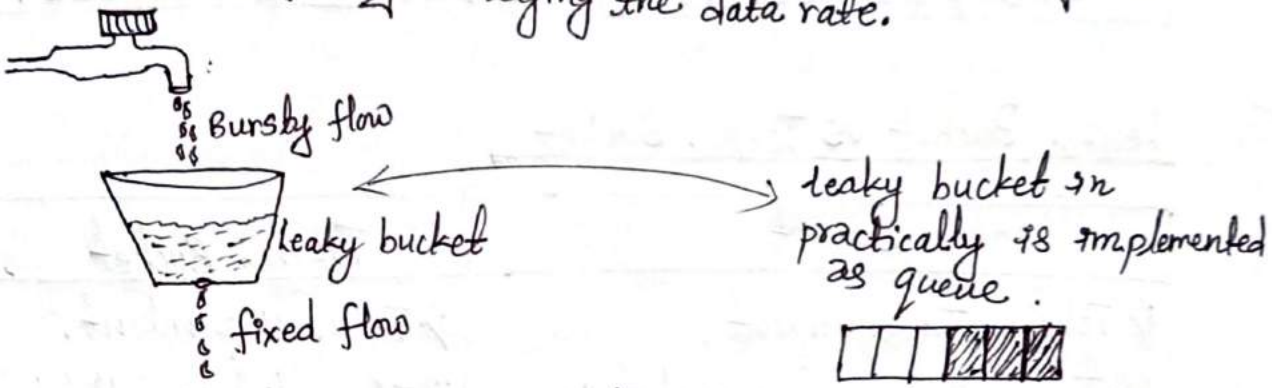


Fig. Demonstrating leaky bucket concept.

Algorithm:

Step1: Initialize the counter to 'n' at every tick of clock.
Step2: If n is greater than the size of packet in the front of queue send the packet into the network and decrement the counter by size of packet. Repeat the step until n is less than the size of packet.
Step3: Reset the counter and go to step-1.

Token bucket → The token bucket algorithm allow to vary the output rate depending on the size of brust. In this algorithm the bucket holds token to transmit a packet, the host must capture and destroy one token. Token are generated by a clock at the rate of one token every second.

Algorithm:

Step1: A token is added at every Δt time.
Step2: The bucket can hold b-token. If a token arrive when bucket is full, it is discarded.

Step 3: When a packet of m bytes arrived m tokens are removed from the bucket and the packet is sent to the network.

Step 4: If less than n tokens are available no tokens are removed from the buckets and the packet is considered to be non conformant.

If not understood refer example from kec book page no. 206

> **Note:** May be these formulas important if numericals asked:
>
> i) Brust Length = $\frac{\text{Capacity of bucket (In kb)}}{(\text{Output rate} - \text{Arrival rate}) * 1000}$ = ... msec (unit)
>
> (Output rate, Arrival rate: In mbps)
>
> ii) For another 500 kb the time taken will be, (let capicity of bucket considered 500 kb)
>
> $\frac{\text{Capacity of bucket}}{\text{Arrival rate} * 1000}$ = let we get 250 msec.
>
> ∴ Output time = Brust length + 250 = ... msec.

Leaky Bucket vs Token Bucket

Leaky Bucket	Token Bucket
i) Token Independent	i) Token Dependent.
ii) If bucket is full packet is discarded.	ii) If bucket is full token are discarded but not the packet.
iii) Bucket leaks at constant rate.	iii) Bucket has maximum capacity.
iv) Packets are transmitted continiously.	iv) Packets can only be transmitted when there are enough token.
v) It does not save token	v) It saves token to send large bursts.

⊛. Techniques to Improve QOS:

i) **Scheduling** → A good scheduling technique treats the different flows of packets in a fair and appropriate manner. Several scheduling techniques are designed to improve the quality of service. FIFO queuing, priority queuing and weighted fair queuing are some of those techniques.

i) FIFO Queuing → In FIFO queuing, packets wait in a queue until the node is ready to process them. If the average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded.

ii) Priority Queuing → In priority queuing, packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest-priority queue are processed first. Packets in the lowest-priority queue are processed last.

iii) Weighted Fair Queuing → It is a better scheduling technique. In which the packets are assigned to different classes and admitted to different queues. The queues are weighted based on the priority of queues; higher priority means a higher weight. The system processes packets in each queue in a round-robin fashion.

2) Traffic Shaping → Already Discussed.

3) Resource Reservation:

A flow of data needs resources such as a buffer, bandwidth, CPU time, and so on. The quality of service is improved if these resources are reserved beforehand. This section consist of QoS model called Integrated Services, which depends heavily on resource reservation to improve the quality of service.

4) Admission Control:

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

⊛ Queuing Techniques for Scheduling:-

FIFO queuing, Priority queuing & Weighted fair queuing discussed above are queuing techinques for scheduling.

[already discussed]

⊛ Introduction to Ports and Sockets:

Port → A port is a logical construct assigned to network processes so that they can be identified within the system. The word "Port" is the number used by the particular software. The same port number can be used in different computer running on same software. A port is a communication endpoint.

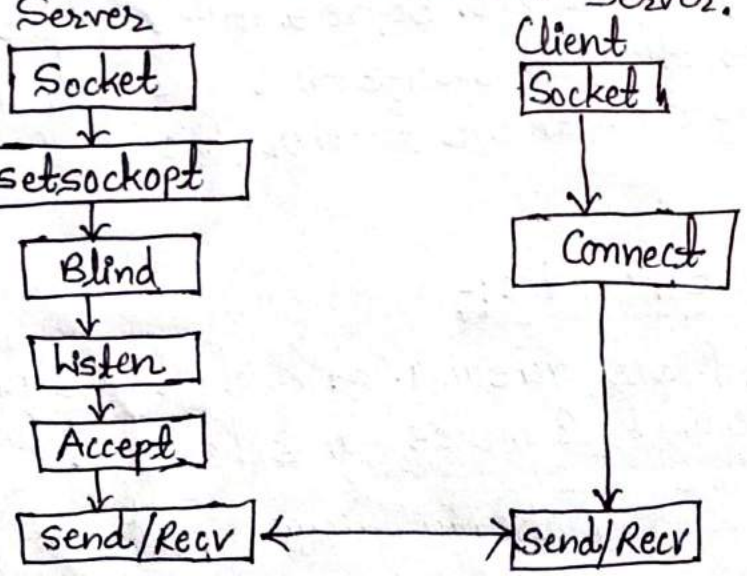
A port number is a 16-bit unsigned integer thus ranging from 0 to 65535. For TCP, port number 0 is reserved and cannot be used while the source port is optional and a value of zero means no port for UDP.

Socket → A socket is a combination of port and IP address. The word "socket" is the combination of port and IP address. It is used to identify both a machine and a service within the machine. A socket is one endpoint of a two-way communication link between two programs running on the network.

In networking, a socket is used to allow many processes within a single or different host to use TCP communication simultaneously. The socket is formed by including the IP address with the port number to uniquely identify seperate data stream.

⊛. Socket Programming:

Socket Programming is a way of connecting two nodes on a network to communicate with eachother. One socket (node) listens on a particular port at an IP, while other socket reaches out to the other to form a connection. Server forms the listener socket while client reaches out to the server.



This is a state diagram for server and client model.

UNIT-6

Application Layer

The application layer is the highest abstraction layer of the TCP/IP model that provides the interfaces and protocols needed by the users. This layer is implemented by network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Examples: Applications, Browsers, Skype, Messenger etc.

Functions of Application Layer:

File transfer → It allows user to access, retrive and manage files in a remote computer.

Mail Services → It provides the basis for email forwarding and storage facilities.

Directory services → It provides ~~database sources~~ access for global information about various services.

⊛ Web & HTTP:

The World Wide Web (WWW), or simply Web, is a global network of servers linked by a common protocol allowing access to all connected hypertext resources. When a client host requests an object, a Web server responds by sending the requested object through browsing tools. The WWW has unique combination of flexibility, portability and user friendly features that distinguish it from other services provided by the Internet. The WWW today is a distributed client-server service, in which a client using a browser can access a service using the server. However, the service provided is distributed over many locations called websites.

HTTP stands for Hyper Text Transfer Protocol that transfers the page browsed by user at the application layer. HTTP uses TCP rather than UDP, since reliability of delivery is important for Web pages with text. In a hypertext environment, information is stored in a set of documents that are linked

together using the concept of pointers. The reader who is browsing through document can move to other documents by clicking the items that are linked to other documents. To use WWW, we need three components: a browser, a web server and a protocal called HTTP.

⑧. HTTP Message Format:

HTTP Message is used to show how data is exchanged between the client and the server. It is based on client-server architecture. HTTP message consists of an initial request line and an initial response line.

Format:

HTTP-Message = Request | Response ; HTTP/1.1 messages

i) Initial Request Line → The initial line is different for the request and the response. A request-line consist of three parts: a method name, requested resource's local path, and the HTTP version being used. All these parts are separated by spaces.

Syntax:

GET /path/to/file/index.html HTTP/1.0

uniform resource identifies

Here,
- → GET is the most common HTTP method.
- → The **path** shows the part of the URL after the host name. It is also called a request URI.
- → The **version** of HTTP always takes the form "HTTP/x.x".

ii) Initial Response Line → The initial response line is also known as the status line. It also has three parts: the HTTP version, a response status code that gives the result of the request and the English reason phrase describing the status code.

Example

HTTP/1.0 200 OK OR HTTP/1.0 404 Not Found.

Here, the HTTP version of the response line and the request line are same as "HTTP/x.x".

⊛ Persistent Versus Nonpersistent Connection:

Persistent Connection → HTTP version 1.1 specifies a persistent connection by default. In a persistent connection, the server leaves the connection open for more requests after sending a response. The server can close the connection at the request of a client or if a time-out has been reached. The sender usually sends the length of the data with each response. However, there are some occasions when the sender does not know the length of the data. This is the case when a document is created dynamically or actively. In these cases, the server informs the client that the length is not known and closes the connection after sending the data so the client knows that the end of the data has been reached.

Nonpersistent Connection → HTTP prior to version 1.1 specifies a non-persistent connection. In a nonpersistent connection, one TCP connection is made for each request/response. The following lists the steps in this strategy:

1. The client opens a TCP connection and sends a request.
2. The server sends the response and closes the connection.
3. The client reads the data until it encounters an end-of-file marker; it then closes the connection.

In this strategy, for N different pictures in different files, the connection must be opend and closed N times. The nonpersistent strategy imposes high overhead on the server because the server needs N different buffers and requires a slow start procedure each time a connection is opened.

⊛ DNS and Query Types:

The Domain Name System (DNS) is a supporting program that is used by the other programs such as e-mail. It is a global system for translating IP addresses to human-readable domain names. When a user tries to access a web address like "example.com", their web browser or application performs a DNS

Query against a DNS server, supplying the host name. The DNS server takes the hostname and resolves it into a numeric IP address, which the web browser can connect to.

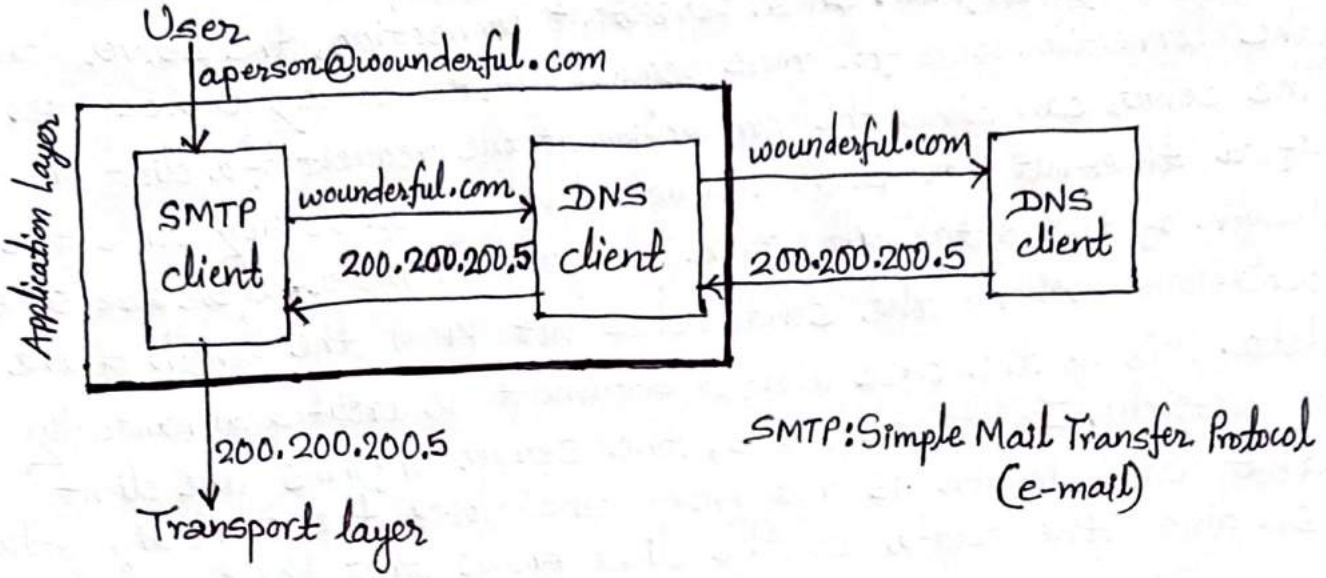


Fig: Example of using DNS service.

Query Types in DNS System:

There are three types of queries in the DNS system:

i) Recursive Query → In a recursive query, a DNS client provides a hostname, and the DNS Resolver must provide an answer. DNS Resolver responds with either a relevant resource record, or an error message if it can't be found. The resolver starts a recursive query process, starting from the DNS Root Server, until it finds the Authoritative Name Server that holds the IP address and other information for the requested hostname.

ii) Iterative Query → In an iterative query, a DNS client provides a hostname, and the DNS Resolver returns the best answer it can. If the DNS resolver has the relevant DNS records in its cache, it returns them. If not, it refers the DNS client to the Root Server or another Authoritative Name Server which is nearest to the required DNS zone.

iii) Non-Recursive Query → In non-recursive query, the DNS Resolver already knows the answer. It either immediately returns a DNS record or queries a DNS Name Server which is authoritative for the record. In both cases, there is no need for additional rounds of queries, rather a response is immediately returned to the client.

Services provided by DNS:

i) Host Aliasing → A host with a complicated hostname can have one or more alias names. DNS can be invoked by an application to obtain the canonical hostname for a supplied alias hostname as well as the IP address of the host. For example, a hostname such as relay1.west-coast.enterprise.com could have, say, two aliases such as enterprise.com and www.enterprise.com. In this case, the hostname relay1.west-coast.enterprise.com is said to be canonical hostname.

ii) Mail Server Aliasing → It is highly desirable that e-mail address be easy to remember. For example, if Bob has an account with Gmail, Bob's e-mail address might be as simple as bob@gmail.com. DNS can be invoked by a mail application to obtain the canonical hostname for a supplied alias hostname as well as the IP address of the host.

iii) Load Distribution → DNS is used to perform load distribution among replicated servers, such as replicated web servers. Busy sites such as cnn.com, are replicated over multiple servers, with each running on a different end system and having a different IP address. For replicated web servers, a set of IP addresses is thus associated with one cannonical hostname.

Overview of How DNS Works:

DNS is a client/server network communication protocol. DNS clients send requests to the server while DNS servers send responses to the client. Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as a reverse DNS lookups. DNS implements a distributed database to store the name of all the hosts available on the internet.

If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS Resolver sends a request to the DNS server to obtain the

IP address of a hostname. If the DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

DNS Records:

DNS records are mainly used to convert domain names into servers IP that host website. The main purpose is that people and applications don't have to remember big numbers to navigate to a domain. For example, www.helloprogrammers.com has an IP of 93.184.220.42, so it is easier to remember a friendly name. Following are the different types of DNS records that are used for a webpage, depending on the functions that we need to publish.

A Record → Connects an IP Address to a host name.

CNAME Record → Allows more than one DNS name for a host.

MX Record → Ensures email is delivered to the right location.

NS Record → Contains the name server info.

SRV Record → Finds computers that host specific services.

SPF Record → Used to help prevent against spam.

DNS Messages:

DNS has two types of messages query and response. Both types have the same format. The query message consists of a header and question records. The response message consist of a header, question records, answer records, authoritative records and additional records.

Header → Both query and response messages have the same header format with some fields set to zero for the query messages. The header is 12 bytes.

Question section → This is a section consisting of one or more question records. It is present on both query and response messages.

Answer section → This is a section consisting of one or more resource records. It is present only on response messages. This section includes the answer from the server to the client.

Authoritive Section → This is a section consisting of one or more resource records. It is also present only on response messages. This section gives information (domain name) about one or more authoritative servers for query.

Additional Information Section → This section provides additional information that may help the resolver. For example, a server may give the domain name of an authoritative server to the resolver in the authoritative section and include the IP address of the same authoritative server in the additional information section.

⊛. File Transfer and Email Protocols:-

FTP → File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections. FTP is a client-server protocol that relies on two communication channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content.

FTP differs from other client-server applications in that sense it establishes two connections between the hosts. One connection is used for data transfer and other for control information. Separation of commands and data transfer makes FTP more efficient.

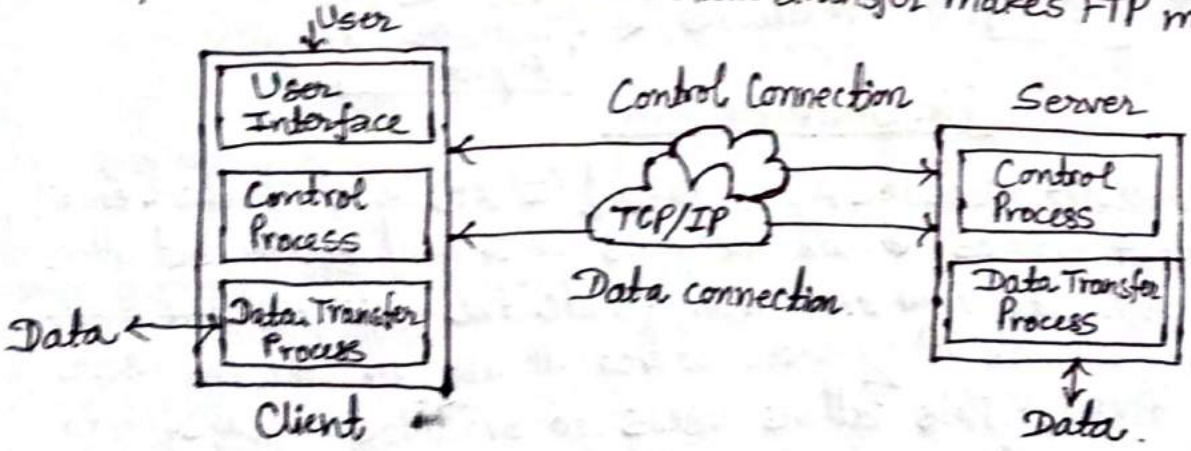


Fig: Control and data connection in FTP.

2) SFTP → SSH File Transfer Protocol (SFTP) is a secure file transfer protocol. It runs over the SSH protocol. It supports the full security and authentication functionality. SFTP also protects against password sniffing and it protects the integrity of the data using encryption and cryptographic hash functions. It also authenticates both the server and the user.

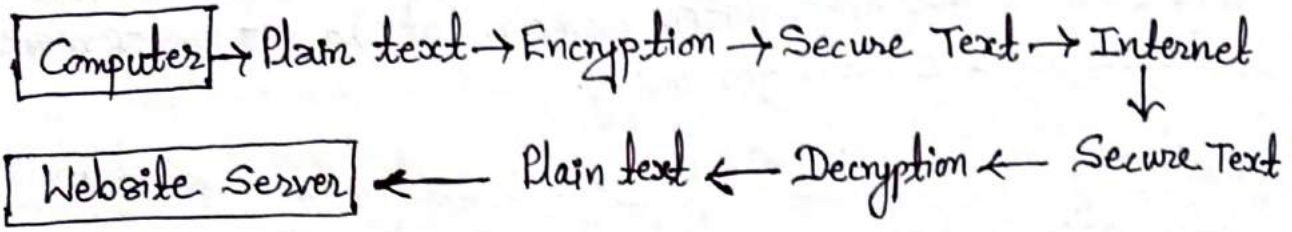


Fig: Process of SFTP

3) SMTP → SMTP stands for "Simple Mail Transfer Protocol". It contains rules for correct communication between computers in a network. SMTP is responsible for feeding and forwarding e-mails from sender to recipient. The SMTP model is of two types: end-to-end method and store-and-forward method.

The end-to-end model is used to communicate between different organizations whereas the store and forward method is used within an organization.

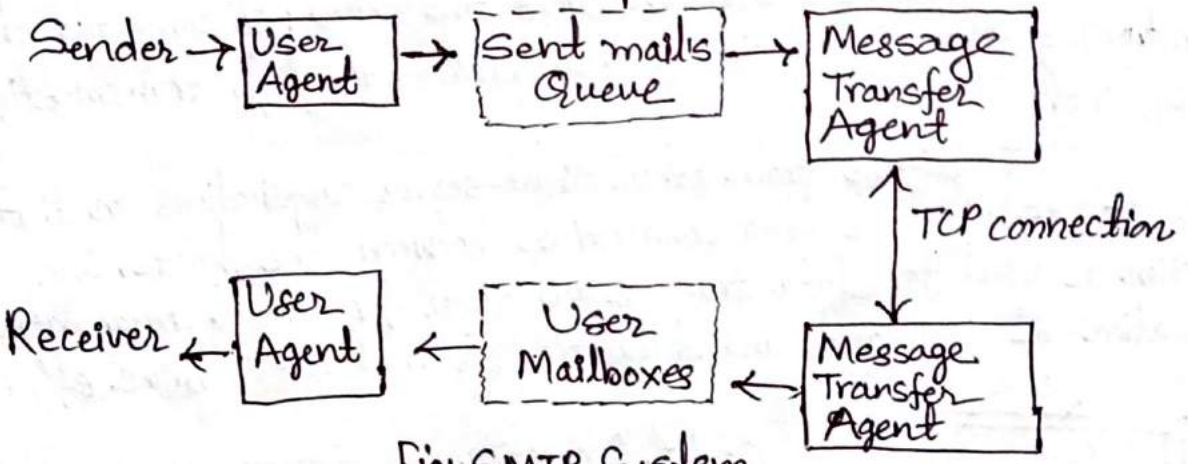


Fig: SMTP System

4) IMAP → Internet Message Access Protocol (IMAP) is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages ~~have been read~~ as though they were stored locally on the end user's computing device. This allows users to organize messages into folders, have multiple client applications know which messages have been read, flag messages for urgency or follow-up and save draft messages on the server.

IMAP supports both on-line and off-line modes of operation. E-mail clients using IMAP generally leave messages on the server until the user explicitly deletes them. To use IMAP, the mail server runs an IMAP server that listenes to port 143.

5). POP(3) → Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows us to download email messages on our local computer and read them even when we are offline. By default, the POP3 protocol works on two ports:

Port 110: this is a default POP3 non-encrypted port.

Port 995: this is the port we need to use if we want to connect using POP3 securely.

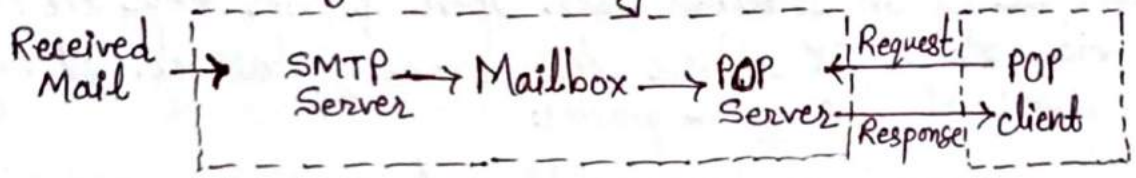


Fig: POP 3

⊛. Overview of Application Server Concepts:

An application server is a component-based product that resides in the middle-tier of a server centric architecture. It provides middleware services for security and state maintenance, along with data access and persistence.

The application server is frequently viewed as a part of three-tier application, consisting of graphical user interface (GUI) server, an application server and a database and transaction server. An application server is a server program in a computer network that provides the business logic for an application program.

1. Proxy Application Server → A proxy server is any machine that translates traffic between networks or protocols. It's an intermediary server separating end-user clients from the destinations that they browse. Proxy servers provide varying levels of functionality, security and privacy depending on use, needs, or company policy.

Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests. Proxy servers can provide a high level of privacy.

Types of Proxy Servers:

i) Forward Proxies → A forward proxy server sits between the client and an external network. It evaluates the outbound requests and takes action on them before relaying that request to the external resource.

Most proxy services that we are likely to encounter are forward proxies. Virtual Private Networks (VPN) and Web content filters are both examples of forward proxies.

ii) Open Proxies → An open proxy is a proxy server that is accessible by an Internet user. Open proxies helps the clients to hide their IP address while browsing the web. Following are some of the open proxies:

http://www.stayinvisible.com/
http://www.multiproxy.org/
http://www.openproxies.com/

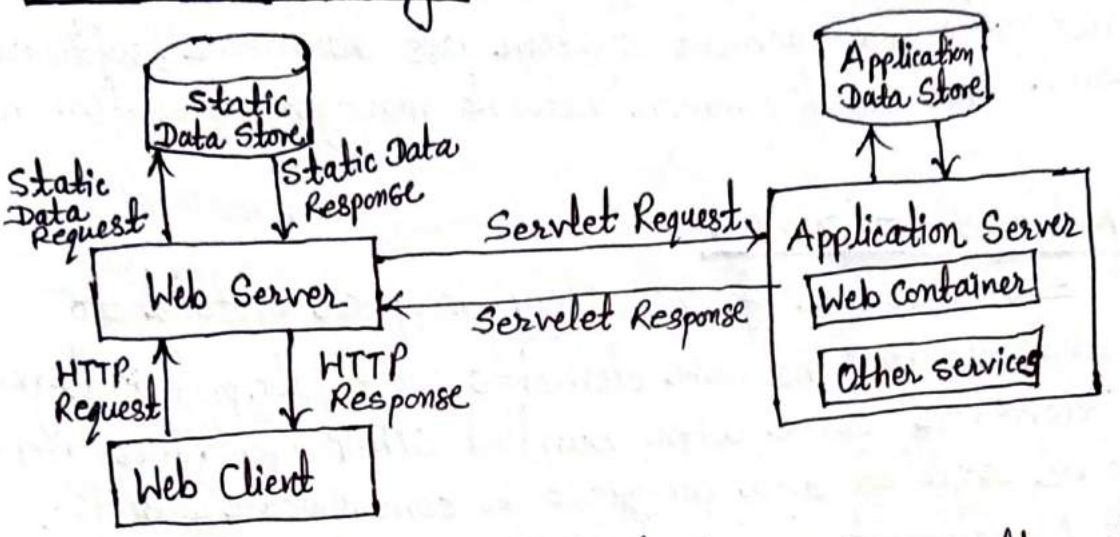
iii) Reverse Proxies → A reverse proxy server sits between a network and multiple other internal resources. A large website might have dozens of servers that collectively serve requests from a single domain. To accomplish that, client requests would resolve to a machine that would act as a load balancer. The load balancer would then proxy that traffic back to the individual servers. Varnish and Squid are some popular open source proxies.

⊛. Why should we use a proxy server?

→ To control internet usage of employees and children.
→ For bandwidth savings and improved speeds.
→ For Privacy benfits.
→ For Improved security.
→ To get access to blocked resources.

2). Web Application Servers: Web server is a computer where the web content is stored. Basically web server is used to host the websites but there exists other web servers also such as gaming, storage, FTP, email etc. Website is collection of web pages while web server is a software that respond to the request for web resources.

Web Server Working:



→ When client sends request for a web page, the web server search for the requested page. If requested page is found then it will send it to client with an HTTP response.

→ If the requested web page is not found, web server will send an HTTP response: Error 404 Not found.

→ If client has requested for some other resources then the web server will contact to the application server and data store to construct the HTTP response.

3) Mail Application Server:

A mail server also known as a mail transfer agent or MTA is an application that receives incoming e-mail from local users and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is called a mail server. Microsoft Exchange, Sendmail, gmail etc. are some common mail server programs.

Mail servers can be broken down into two main categories; outgoing mail servers and incoming mail servers. Outgoing mail servers are known as SMTP servers. Incomming mail servers come in two main varieties. POP3 servers are best known for storing sent and received messages. IMAP servers always store copies of messages on servers.

⊛. Network Management:

We define network management as monitoring, testing, configuring, and troubleshooting network components to meet a set of requirements defined by an organization. These requirements include the smooth, efficient operation of the network that provides the predefined quality of services for users. To accomplish this task, a network management system uses hardware, software and humans. The most common network management system is SNMP.

Network Management: SNMP

SNMP is one of the widely accepted protocol to manage and monitor network elements. Most of the professional-grade network elements come with bundled SNMP agent. These agents have to be enabled and configured to communicate with the Network Management System (NMS).

SNMP is a set of protocols for network management and monitoring. These protocols are supported by many typical network devices such as routers, hubs, bridges, switches, servers, workstations, printers etc. SNMP is simple and powerful and has the ability to manage network by providing read/write abilities, collecting information on how much bandwidth is being used, Emailing an alert when computer server is low on disk space and many more.

SNMP Components and their functionalities:

1) SNMP Manager → A manager is a seperate unit that's accountable to communicate with the SNMP agent on network devices. This is usually a software installed on a PC or a server to operate one or more network management systems.

Functions:
- → Queries agents
- → Gets responses from agents
- → Locates variables in agents
- → Accept no synchronous events from agents.

ii) Managed Devices → A managed device is a part of the network that needs some type of monitoring and management. For example, switches, routers, servers, printers etc.

iii) SNMP Agent → The agent is an application packaged inside the network element. The agent gathers the management information database from the device locally and makes it accessible to the SNMP manager, when its asked for. These agents could be specific or standard to a manufacturer.

Functions:
- → Collects management information about its local environment.
- → Stores and retrives management information.
- → Signals an event to the manager.
- → Acts as proxy for some non-SNMP managable network node.

iv) Management Information Base (MIB): MIB files are the set of parameters that an SNMP Manager can request the agent. Agent assembles these data locally and stores them as described in the Management Information Base. MIB contains standard set of statistical and control values defined for hardware nodes on a network. The SNMP Manager should be aware of these standard and private questions for every type of agent.

UNIT-7

Multimedia & Future Networking:

⊛. Multimedia Streaming Protocols:

We use term multimedia to refer to data that contains audio or video, and may include text. The phrase real-time multimedia refers to multimedia data that must be reproduced at exactly the same rate that it was captured. For example: a television news program that includes audio and video of an actual event.

Stream Control Transmission Protocol (SCTP):

SCTP is a connection-oriented protocol in computer networks which provides a full-duplex association i.e, transmitting multiple streams of data between two end points at the same time that have established a connection in network. SCTP provides some of the features of both UDP and TCP: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages like TCP. SCTP is also intended to make it easier to establish connection over wireless network and managing transmission of multimedia data.

Features/Characteristics of SCTP:

i) Unicast with Multiple properties → It is a point-to-point protocol which can use different paths to reach end host.

ii) Reliable Transmission → It uses SACK and checksums to detect damaged, corrupted, discarded, duplicate and reordered data. It is similar to TCP but SCTP is more efficient when it comes to reordering of data.

iii) Message oriented → Each message can be framed and we can keep order of data stream and tabs on structure. For this, In TCP, we need a different layer of abstraction.

iv) Multi-homing → It can establish multiple connection paths between two end points and does not need to rely on IP layer for resilience.

⊛. Software-defined networking (SDN):

In order to understand SDN, we need to understand data plane and Control plane firstly.

Data plane: All the activities involving as well as resulting from data packets sent by the end user belong to this plane. This plane includes:

→ Forwarding of packets.
→ Segmentation and reassembly of data.
→ Replication of packets for multicasting.

Control plane: All activities necessary to perform data plane activities but do not involve end user data packets belong to this plane. In other words, this is the brain of the network. The activities of the control plane include:

→ Making routing tables.
→ Setting packet handling policies.

In traditional network, each switch has its own data plane as well as a control plane. The control plane of various switches exchange topology information and hence construct a forwarding table which decides where an incoming ~~packet~~ data packet has to be forwarded via the data plane.

SDN: It is an approach via which we can take the control plane away from the switch and assign it to a centralised unit called the SDN controller. Hence, a network administrator can shape traffic via a centralised console without having to touch the individual switches. The data plane still resides in the switch and when a packet enters a switch, its forwarding activity is decided based on the entries of flow tables, which are pre-assigned by the controller. A flow table consists of match fields and instructions. The packet is first matched against the match fields of the flow table entries.

Then the instructions of the corresponding flow are executed. If a packet doesn't find a corresponding match in the flow table, the switch queries the controller which sends a new flow entry to the switch. The switch forwards or drops the packet based on this flow entry.

SDN Architecture: A typical SDN architecture consists of three layers.

i) **Application Layer** → It contains the typical network applications like intrusion detection, firewall and load balancing.

ii) **Control Layer** → It consists of the SDN controller which acts as the brain of the network. It also allows hardware abstraction to the applications written on top of it.

iii) **Infrastructure Layer** → This consists of physical switches which forms the data plane and carries out actual movement of data packets.

The layers communicate via a set of interfaces called the northbound APIs (between application and control layer) and southbound APIs (between control and infrastructure layer).

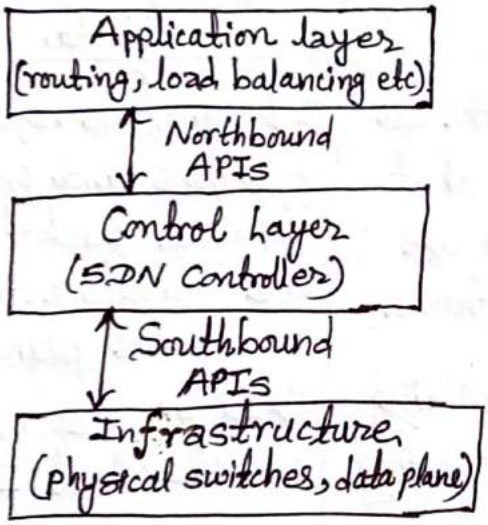


fig: SDN Architecture

Features of SDN:

i) **Directly programmable** → Network control is directly programmable because it is decoupled from forwarding functions.

ii) **AGILE** → Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.

iii) **Centrally managed** → Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch.

iv) Programmatically configured → SDN lets network managers configure, manage, ~~and~~ secure and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.

v) Open Standards-Based and Vendor-Neutral → When implemented through open standards, SDN simplifies network design and operation because ~~instru~~ instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.

⊛. Differences between Control Plane and Data Plane:

Control Plane	Data Plane.
i) Control plane refers to the all functions and processes that determine which path to use to send the packet or frame.	i) Data plane refers to all the functions and processes that forward packets/frames from one interface to another based on control plane logic.
ii) It is responsible for building and maintaining the IP routing table.	ii) It is responsible for forwarding ~~actu~~ actual IP packet.
iii) It takes care of how packets should be forwarded.	iii) It takes care for moving packets from source to destination.
iv) Control plane performs its task independently.	iv) Data plane performs its ~~tak~~ task on data plane.
v) It includes STP, ARP, RIP, DHCP etc.	v) It includes TTL, IP header, checksum etc.

⊛ Network Function Virtualization (NFV):

NFV is a network architecture which aims to accelerate service deployment for network operators and reduce the cost by separating functions like firewall. It is a way to virtualize network services, such as routers, firewalls, and load balances, that have traditionally been run on computer hardware whose interface is controlled by proprieter and allows network services to be hosted on virtual machines. NFV allows various network operators to implement network policy without being taken care of where to place functions in network and how to route traffic through these functions.

NFV provides a new way to create, distribute and operate networking ~~devices~~ services. It allows network operators to manage and expand their network capabilities on demand using virtual software based applications. NFV is designed to combine and deliver the networking components needed to support an infrastructure totally independent from hardware.

Benefits of NFV:

→ Reduce costs in purchasing network equipment via migration to software on standard servers.
→ Efficiencies in space, power and cooling.
→ Faster time to deployment.
→ Flexibility — ~~scale~~ elastic scale up and scale down capacity.
→ Access to broad independent software community, including open source.

⊛ Next Generation Network (NGN):

NGN refers to a packet-based network and it can be used for both telecommunication services as well as data and it supports mobility. It is able to make use of multiple broadband capabilities, especially Quality of Services (QoS) enabled transport technologies where the service-related functions are independent of the underlying transport-related technologies.

The main goal of NGN is to work as an replacement of Public Switched Telephone Network (PSTN) and Integrated ~~Digital~~ Services Digital Network (ISDN). The concept of this network will not only bring wide range of possibilities to introduce new and existing technologies in the field of information transmission and processing, but also many possibilities especially in the branch of network services.

Features of NGN:

→ NGN works on Packet based transferring.
→ It supports a wide range of services, applications and mechanisms based on service building blocks.
→ It provide the advantage of general mobility.
→ It provides unrestricted access by users to different service providers.
→ It has Broadband capabilities with end-to-end QoS and transparency.

Applications of NGN:

→ Voice Telephone services
→ Multimedia services.
→ Data services.
→ Push to talk over NGN
→ Content delivery services
→ Global mobility services.

Advantages of NGN:

→ It generates additional revenue streams for new IP/Ethernet services.
→ It fulfills customers demand for high bandwidth, Ethernet/IP solutions.
→ It diminishes expertise in legacy.
→ It gives End of life/End of Service vendor notification.