2 Data Link Layer

Multiple Access Protocols:

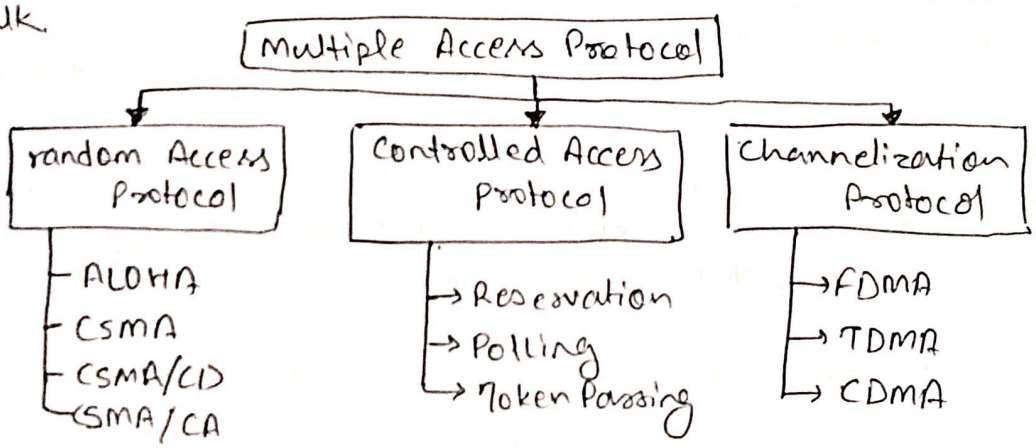
→ The Data Link Layer is responsible for transmission of data between two nodes. its main functions are:-
(i) Data Link Control
(ii) Multiple Access Control.

[1] Data Link Control:

→ The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control
→ DLC used to provide reliable data transfer over physical medium. Data link layer provides the coordination among the devices so that no collision occurs.

[2] Multiple Access Control:

→ If there is a dedicated link between the sender and the receiver then data link control layer is insufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously Hence multiple Access protocols are required to decrease collision and crosstalk.



(1) Random Access Protocol: All stations have same priority. Any station can send data depending upon medium's state.

(2) Controlled Access Protocol: The data is send by that station which is approved by other stations.

(3) Channelization: In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

NOTE: MAC addresses are used in this sublayer of DLL (i.e. Multiple Access Control)

Peer-to-Peer (P2P) File Sharing

→ P2P is a file sharing technology, allowing the users to access mainly the multimedia files like videos, music, games etc. The individual users in this network are referred to as peers. The peers request files from other peers by the establishing a TCP or UDP connection.

How P2P works :-

→ A P2P networks allows computer hardware and software to communicate without the need for a server. Unlike client-server architecture.

→ The peers directly interact with one another without the requirement of a central server.

→ Now, when one peer makes a request, it is possible that multiple peers have a copy of that requested object. Now the problem is how to get the ip address of all those peers. This is decided by the underlying Architecture supported by the P2P systems.
By means of one of these method client-peer can get to know about all other peers which have the requested object/file and the file transfer take place directly between these two peers.

→ Three such architectures are :-
1. Centralized Directory
2. Query Flooding
3. Exploiting Heterogeneity.

1 Centralized Directory :-

→ It is similar to client-server architecture as it also maintains a huge central server to provide directory service.

→ All the peers inform this central server of their IP address and files they have for sharing.

→ The server queries the peers at regular interval to make sure that peers are still connected or not.

→ So basically this server maintains a huge database regarding which file is present at which IP address.

WORKING :-

- Whenever a request peer comes in, it sends its query to server.
- Since the server have all the information of its peer, so it returns the IP address of all peers having requested file to the client peer.
- Now file transfer takes place between two peers.

Problem :-

- The main problem with this architecture is that there is a single point of failure. If the server crashes, the whole P2P network also crashes.
Also since all the processing is to be done by single server so a huge amount of database has to be maintained and regularly updated.

[2] Query Flooding :-

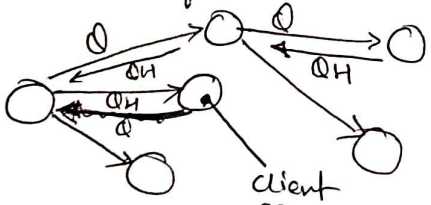
→ Unlike centralized approach, this method makes use of distributed systems.
→ In this, the peers are supposed to be connected to an overlay network. It means if a connection/path exist from one peer to another it is a part of this overlay network.
→ In this overlay network, peers are called nodes, and connection between peers is called an edge between the nodes. Thus resulting in graph like structure.

WORKING :-

- when client peer request for some file. This request is sent to all the neighbouring nodes i.e. to all nodes which are connected to this node. If those nodes dont have the required file they passes the query their neighbours and so on. This is called Query Flooding.
- when the peer with the requested file is found (referred to as query hit) the query flooding stops and it sends back the file name and file size to the client, thus following the reverse path.
- If there are multiple query hits, the client selects from one of these peers.

Disadvantage :-

→ The query has to be sent to all the neighbouring peers unless a match is found. This increase the traffic in the network.



Q = Query
QH = Query Hit.

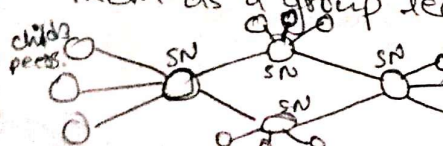
[3] Exploiting Heterogeneity :-

→ This P2P architecture uses of both the above-discussed system.
→ It resembles with Gnutella (distributed system like Gnutella because there is no central server for query processing.
→ But unlike Gnutella, it does not treat all its peer equally. The peer with higher bandwidth and network connectivity are at higher priority and are called group leaders / supernodes. The rest of the peers are assigned to these supernodes.
→ These supernodes are interconnected and the peers under these inform their respective leaders about their connectivity, IP address, and files available for sharing.

WORKING :-

- This structure can process the queries in two ways :-

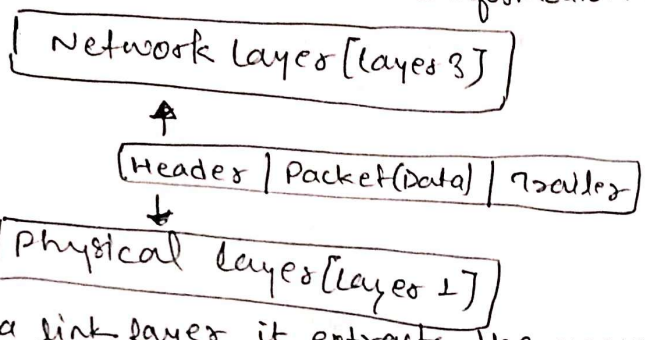
(i) the supernodes could contact other super nodes and merge their database with their own database. Thus this supernodes now has information of a large numbers of peers.
(ii) Another approach is that when a query comes in, it is forwarded to the neighbouring super nodes unit a match is found, just like in Gnutella. Thus query flooding exist with limited scope as each supernodes has many child peers. Hence such a system exploits the heterogeneity of the peers by designating some of them as a group leader and other as their child peer.



SN = Supernodes.

Framing in Data Link layer

- Frames are the Protocol Data Unit (PDU) in Data Link layer
- Framing is a point-to-point connection between two computers consists of a wire in which data is transmitted as a stream of bits. However these bits must be framed into discernible blocks of information.
- It provides a way for a sender to transmit a set of bits that are meaningful to the receiver.
- Frames have headers that contains information such as error-checking codes.



- At the data link layer, it extracts the message from the sender and provides it to the receiver by providing the sender's and receiver's addresses. The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption.

Types of framing :- (two types):

① Fixed size ② Variable size.

Ethernet:

- Ethernet is the most widely used LAN Technology, which defined under IEEE standards 802.3. The reason behind its wide usability is Ethernet is easy to understand, implement, maintain, and allows low-cost network implementation.
- Ethernet generally uses Bus topology
- Ethernet operates in two layers of OSI model, Physical layer, and Data link layer. For ethernet protocol data unit is frame since we mainly deal with DLL.
- In order to control collision, the access control mechanism used in ethernet is CSMA/CD
- Manchester encoding used in Ethernet

Carrier Sense Multiple Access (CSMA)

- This method was developed to decrease the ~~collision~~ chances of collision when two or more stations start sending their signals over DLL. CSMA requires that each station first check the state of medium befor sending

Error Detection

Error:

A condition when the receiver's information does not ~~math~~ match with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or 1 bit may change to 0.

Error Detecting Code (implemented in DLL or Transport Layer)

→ When a msg is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this we uses error detection code.

→ Basis approach used for error detection is the use of redundancy bits. where addition bits are added to facilitate detection of errors.

→ Some popular techniques are :

1. Simple Parity Check
2. Two-dimensional Parity Check
3. Checksum
4. Cyclic Redundancy check

Introduction of MAC Address

→ Media Access Control Address is a physical address which works at Data Link Layer.

MAC Address : MAC Address are unique 48 bits hardware number of a computer, which is embedded into NIC during the time of manufacturing. MAC address is also known as physical address of a network device.

MAC address is used in ~~M~~ Med. multiple Access control (sublayer of DLL)
MAC address is worldwide unique, since millions of network devices exists.

Format of MAC Address :

→ MAC address is a 12 digit hexadecimal number (6-Byte Binary number) which is mostly represented by Colon-Hexadecimal notation.

→ First 6-digit of MAC address identifies the manufacturer. called as OUI (i.e. Organizational Unique Identifier), IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.

Ex : 3C:5A:B4 ⟶ Google, Inc.
CC:46:D6 ⟶ Cisco

→ The rightmost six digit represents the Network Interface controller which is assign by manufacturer.

→ Representation (3 ways) :-

1. 00-0a-83-b1-c0-8e
2. 00:0a:83:b1:c0:8e
3. 000.a83.b1c.08e

Types of MAC Address

1) Unicast
2) Multicast
3) Broadcast.

Types of Switches :-

→ Switches are connectivity points of an Ethernet network. These are small devices that can receive data from multiple input ports and send it to the specific output port that takes data to its intended destination in the network.

Types of switches :-

1 Unmanged Switches :-

→ These are the switches that are mostly used in home networks and small businesses as they plug in and instantly start doing their job and such switches do not need to be watched or configured.
These requires only small cable connections.
It allows devices on a network to connect with each other such as computer to a computer or a computer to a printer.
They are least expensive switches.

2 Managed Switches :-

→ These type of switches have many features like the highest level of ~~secu~~ security precision control, full mangement of the network. These are used in organizations containing a large network and can be customized to enhance the functionality of certain network.
These are costly options but their scalability makes them an ideal option for a network that is growing.
They are achieved by setting Simple Network Management Protocal (SNMP)
They are of two types :-

(i) Smart switches
- → offers basic management features with ability to create some level of security
- → also called as partial managed switches.
- → mostly used in fast & constant LAN

(ii) Enterprise Managed Switches
- → features like ability to fix, copy, transfer and display diff. network configuration along with wed interface SNMP and command line interface
- → fully manged switches, more expensive.
- → used in organization with large number of ports, switches and nodes.

3 LAN Switches :-

→ These are also known as ethernet switches or data switches and are used to reduce network congestion or bottleneck by ~~disturbing~~ distributing a package of data only to its intended recipient. These are used to connect points on LANs.

4 PoE switches

→ These switches used in PoE technology which stands for Power over Ethernet that is a technology that integrates data and power on the same cable allowing power devices to receive data in parallel to power. Thus these switches provide greater flexibility by simplifying the cabling process.

3. Network Layer

Introduction :

→ Network layer is the 3rd layer of OSI model.
→ The network layer is concerned with the delivery of packets across multiple network.
It selects and manages the best logical path for data transfer between nodes.
→ This layer contains hardware devices such as routers, bridges, firewall and switches but it actually creates a logical image of the most efficient communication route and implements it with a physical medium.
→ Network layer protocols exist in every host or router. The router examine the header fields of all the IP packets that pass through it.
Internet protocol and netware IPX/SPX are most common # Protocals in network layer.
→ The network layer responds to requests from the layer above it (transport layer) and issues requests to the layer below it (data link layer).

■ Responsibilities of Network layer :-

Packet forwarding / Routing of packets : Relaying of data packets from one network segment to another by nodes in computer network.

Connectionless Communication (IP) : A data transmission method used in packet-switched networks in which each data unit is separately addressed and routed based on information carried by it.

Fragmentation of Data : Splitting of data packets that are too longe to be transmitted on the network.

Difference between Internet, Intranet and Extranet :-

[1] Internet

→ The network formed by the co-operative interconnection of millions of computers, linked together is called Internet.

[2] Intranet

→ It is an internal private network built within an organization using Internet and world wide web standards and products that allows employees of an organization to gain access to corporate information.

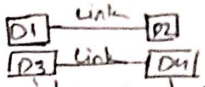
[3] Extranet

→ It is the type of network that allows users from outside to access the ~~Intranet~~ intranet of an organization.
It's a network of internetwork that's restricted in scope to one organization or entity bigger than intranet.

Line Configuration in Computer Network

→ A network is a two or more devices connected through a link. A link is a communication pathway that transfer data from one device to another. Devices can be computer, printer etc. or any other devices that is capable of receiving and sending of data.
For communication occurs, two devices must be connected in some ways to the same link at the same time, There are two possible ways of connections:-
① Point-to-point connection
② Multiple point Connection OR Multipoint connection.

1 Point-to-Point connection:



- A point-to-point connection provides a dedicated link between two devices.
- The entire capacity of the link is reserved for transmission between those two devices.
- Most point-to-point connection use an actual length of wire or cable to connect two ends, but other options like microwave or satellite links also possible.
- Point to Point network topology is considered to be one of the easiest and conventional network topology.
- It is also simplest to establish and understand.

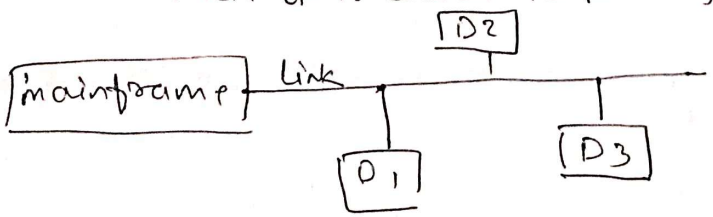
Ex Remote control and T.V. is ex. of P2P connection.

2 Multipoint Connection:

- Also called as multidrop connection. In this connection two or more devices share a single link.
- More than two devices share the link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a multipoint Line Configuration.

i) Spatial sharing: If several devices can share the link simultaneously its called Spatial shared Line Configuration

ii) Temporal (Time) Sharing: If users must take turns using the link, then it is called Temporally shared or Time shared Line Configu



Difference Between Unicast, Multicast, and Broadcast

Unicast : One-to-One transmission

Broadcast : One-to-all transmission

Multicast : One/more Sender to One/more Recipients.

** Already Covered **

Collision Domain and Broadcast Domain in Computer Network

1 Collision Domain

→ A Collision Domain is a Scenario in which when a device sends out a message to the network, all other devices which are included in its collision Domain have to pay attention to it, no matter if it was designed them or not.
This causes the problem because, in a situation where two devices send out their messages simultaneously, a collision will occur leading them to wait and re-transmit their respective messages one at a time.
** Remember, it happens only in the case of a half-duplex mode.

2 Broadcast Domain

→ A Broadcast Domain is a ~~seen~~ Scenario in which when a device sends out a broadcast message, all the devices present in broadcast domain have to pay attention to it.
This creates alot of congestion in network. (commonly called LAN congestion) which affects the bandwidth of the users present in that network.
From this we can realize that the more the number of collision domains and the more the number of broadcast domains, the more efficient is the network providing better bandwidth to all its users.

So which devices break CollisionDomain and which breaks BroadcastDomain

(i) HUB :-

- It neighter breaks the collisionDomain nor a Broadcast Domain i.e. a Hub is neither a collision domain separator nor a Broadcast Domain Separator. All devices connected to a hub are in a single collision and single broadcast domain. ~~Remain~~
Remember Hubs do not segments a network, they just connect network segments.

(ii) Switches :-

- Every port on a switch is in a different collision domain, i.e. a switch is a collision domain separator. So msg that comes from a devices connected to different port never experience a collision.
This helps us during designing networks but there is still a problem with switches
- They never breaks a broadcast domain, it means it is not a broadcast domain Separator
- All the ports on the switches are still in a single broadcast domain. If a device sends a broadcast message it will still cause congestion

iii) Routers :-

- Routers not only breaks collision domain but also breaks broadcast domain which means it is both broadcast as well as collision domain separator
- A router creates a connection between two networks
  A broadcast message from one network will never reach the other one as the router will never let it pass.

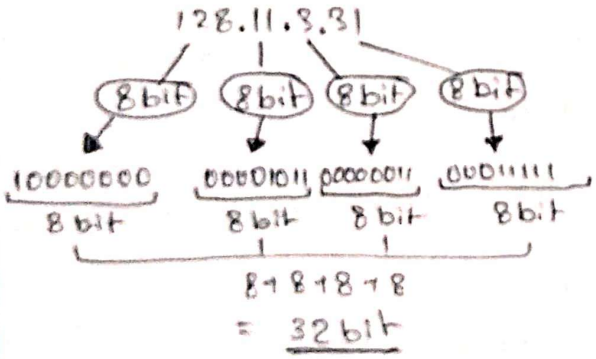
Also as repeaters and bridges differ from hubs and switches only in terms of the number of ports. a repeater does not breaks collision and broadcast domain while a bridge breaks only collision domain.

Introduction of IP Addressing

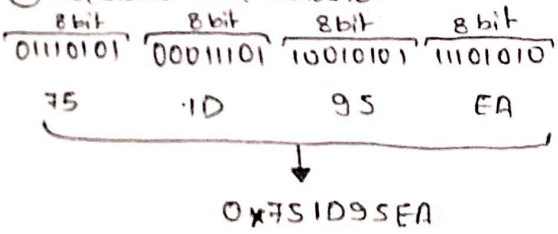
Introduction :-

→ To communicate with each other within a network IP Addresses are used.
→ The participants in a network have their own unique addresses.
→ The Internet Protocol is responsible for allowing the IP address and subnet mask
→ The allocation of IP addresses is regulated by an international Organization i.e. Internet Corporation for Assigned Names and Numbers (ICANN).
• ICANN is also responsible for allocation of DNS.
→ Certain IP address ranges are reserved for special purpose like range from 127.0.0.0 to 127.255.255.255. There is no reliable information on why that range was chosen.
→ IPv4 is a 32 bit (having 4 parts) unique address having an address space of 2^{32}.
→ Two notation in which IP address can be written.

① Dotted Decimal Notation :



② Hexadecimal Notation



Some points to be noted about Dotted Notation.

① The value of any segment (byte) is between 0 to 255 (both included)
② There are no zeroes preceding the value in any segment (i.e. 054 is wrong 54 is correct)

Types of IP address :-

1 IPv4 Address :-

→ 32 bit number with 4 words, each having 8-bit with value upto 255.
OR we can say IPv4 address has 4 octets of 8-bit with each number with a value upto 255.
→ IPv4 classes are differentiated based on the number of host it supports on the network.
→ Types of classes :-

IPv4 Class	IPv4 Start Address	IPv4 End Address	Usage.
A	0.0.0.0	127.255.255.255	Used for Large Networks
B	128.0.0.0	191.255.255.255	Used for Medium Size Network
C	192.0.0.0	223.255.255.255	Used for Local Area Network
D	224.0.0.0	239.255.255.255	Reserved for Multicasting
E	240.0.0.0	255.255.255.255	Study & R&D

→ IPv4 uses a 32-bit address scheme to store 2^{32} address which is more than 4 billion address.
→ It is considered the Primary Internet Protocol and carries 94% of Internet Traffic.

2 IPv6 Address

→ IPv6 is the most recent version of Internet Protocol.
→ This new IP address version is being deployed to fulfil the need of for more Internet address.
→ IPv6 is a 128 bit, allowing 340 undecillion ($2^{128} \approx 3.4 \times 10^{38}$) unique address.

Features of IPv6 :
- Hierarchical addressing and routing configuration infrastructure.
- Stateful and stateless configuration.
- Support for Quality of Services (QoS).
- An ideal protocol for neighbouring node interaction.

Network transmission techniques :-

Circuit Switches vs Packet-Switch :-

→ In circuit switched network, a sig. single path is designated for transmission of all the data packets whereas in case of packet Switched network, each packet may be sent through a different path to reach the destination.
In circuit switched network, the data packets are received in orders whereas in a packet switched network the data packet may be received out of order.
Packet-Switching is further divided into Virtual Circuit & Datagram.

■ IPv4 : IPv4 is a connectionless protocol used for packet-Switched networks.

■ IPv4 Datagram Header : Size of the header is 20 to 60 bytes.

IPv4 Datagram fragmentation & Delay

Why IPv4 Datagram fragmentation required?

→ Different networks may have different Maximum Transmission Unit (MTU) for example due to difference in LAN technology. When one network wants to transmit datagrams to a network with smaller MTU, the router on path may fragment and reassemble datagrams.

How is fragmentation done?

→ When a packet is received at router, destination address and MTU is determined. If size of packet is bigger than MTU, and the 'Do not fragment' (DF) bit is set to 0 in header, then the packet is fragmented into parts and sent one by one. The maximum size of each fragment is the MTU minus the IP header size (IP Header size: min 20byte to max 60 byte)

Each fragment is converted into a packet and the following changes happens in the datagram header.

(1.) The total length field is changed to the size of the fragmet.
(2.) The more fragment bit (MF bit) is set for all the fragment packets except the last one.
(3.) The fragment offset field is set, based on the number of fragment that is being set and the MTU.
(4.) Header Checksum is re-calculated.

Delays :-

4 types of Delays happens :-

(1). Processing Delay : Time taken by the routers to process the data Packt head

(2). Queuing Delay : Time taken by the data packet in routing queues.

(3). Transmission Delay : Time taken to load a data packet onto the transmission channel.

(4). Propagation Delay :- Time taken by the data packet to reach from source to destination.

Fragmentation at Network Layer

Fragmentation:

→ Fragmentation is done by the network layer when the maximum size of datagram is greater than the maximum size of data that can be held in a frame. i.e. MTU. The network layer divides the Datagram received from the Transport Layer into fragments so that data flow is not disrupted.

- Since there are 16 bits for total length in IP header, so max. size of IP datagram = $2^{16}-1 = 65535$ bytes
- It is done by network layer at the destination side and done at routers.
- Source side does not require fragmentation due to good segmentation by transport layer. i.e. instead of doing segmentation at transport layer and fragmentation at network layer, the transport layer looks at datagram data limit and frame data limit and does segmentation in such a way that resulting data can easily fit in a frame without need of fragmentation.
- Receiver identifies the frames with the identification (16 bits) field in the IP header. Each fragments of frame has the same identification number
- Receiver identifies the sequence of frame by fragment offset field in the IP header.
- Overhead at the network layer is present due to extra header introduced due to fragmentation.

Fields in IP header for fragmentation

① Identification (16 bits) - use to identify fragments of the same frame

② fragment offset (13 bits) - use to identify sequence of the fragments in frame.

③ More Fragment (MF = 1 bit) - tells if more fragments are ahead of this
i.e. if MF = 1, more fragments are ahead of this fragment
if MF = 0, it is the last fragment.

④ Don't fragment (DF = 1 bit) :- if we don't want the packet to be fragmented then DF is set i.e. DF = 1.

Reassembly of fragments:

→ It takes place only at the destination and not at routers since packets take an independented path (datagram packet switching), so all may not meet at a router and hence a need of fragmentation arise again. The fragments may arrive out of order also.

Rules for Assigning Host ID & Network ID

1 Rules for Assigning Host ID :

→ ~~Host ID's are assigned within a network~~

→ Host ID's are used to identify a Host within a network. The following are the rules for Assigning Host ID.

- Within a network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this Host ID is now reserved as Broadcast address to send packets to all the Host present on that particular network.

2 Rules for Assigning Network ID :

→ Hosts that are located on the same ~~network~~ physical network are identified by network ID's, as all the Host on the same physical network are assigned the same network ID. The network ID is assigned on the basis of :-

- The network ID cannot starts with 127 because 127 ~~is reserved~~ belongs to class A address and is reserved for internal loop-back function.
- All bits of network ID set to 1 are reserved for IP Broadcasting therefore it cannot be used.

II IP Addressing / Classless Addressing :-

1 Network Address : It identifies a network on internet. Using this, we can find range of addresses in the network and total possible number of hosts in the network.

2 mask : It is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are :-

Class A – 255.0.0.0 Class C – 255.255.255.0

Class B – 255.255.0.0

3 Subnetting : Dividing a large block of address into several contiguous ~~sub-blo~~ sub-blocks and assigning these sub-blocks to different smaller netwo is called Subnetting

4 Subnet mask : It is a 32 bit number used to differentiate the network component of an IP address by dividing the IP address into a network address and host address.

5 Classless Addressing

→ We use host ID-bits as net ID bits of a classful IP address. We give the IP address and define the no. of bits for mask along with it (followed by "/" symbol) like, 192.168.1.1/28. Here subnet mask is found by putting the given number of bits ~~of~~ out of 32 as 1

6 Default Gateway: It serves as an Access point or IP router that a networked computer used to send information to a computer in another network or over the internet.
The default simply means that it is used by default until an address an application specifies another gateway. ~~with~~
without it, a network is isolated from outside.

7 Supernetting

→ It is the opposite of Subnetting. In subnetting a big network is divided into multiple smaller subnetworks. In subnetting multiple networks are combined into a bigger network termed as Supernetwork, or Supesnet.

Longest Prefix Matching in Routers :-

1 Forwarding: Forwarding is moving incoming packets to the appropriate interface. Routes uses a forwarding to decide which incoming packets should be forwarded for the next hop.

2 IP Prefix: IP Prefix is ~~an~~ a prefix of IP address. All computers on one network have the same IP prefix. For ex. 192.24.0.0/18, 18 is the length of the prefix and the prefix is the first 18 bits of the address.

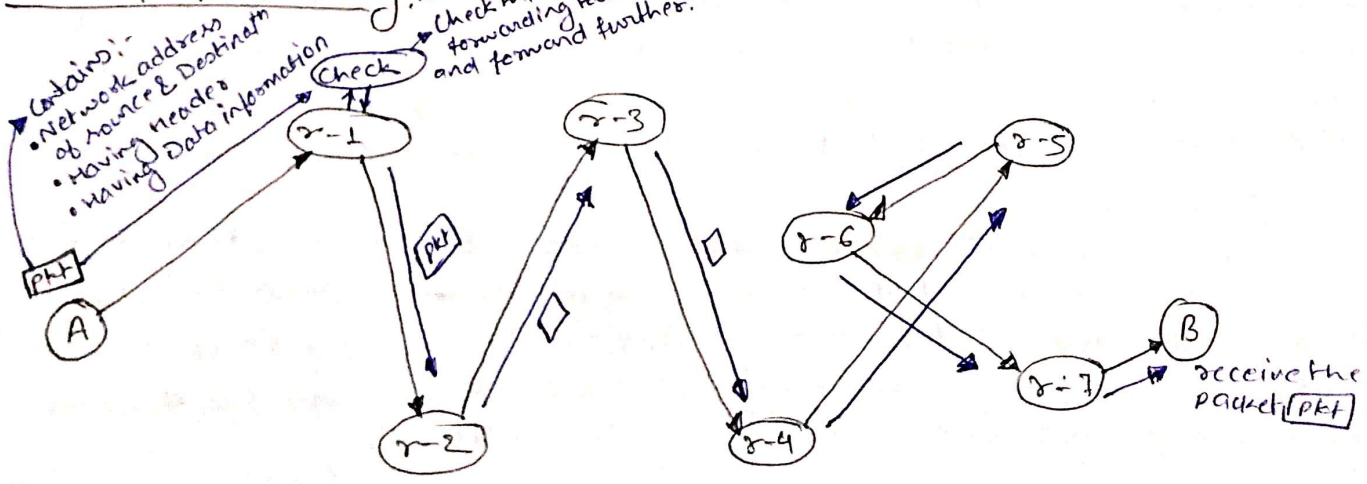
3 How does forwarding works?

→ Routers basically look at the destination address's IP prefix, searches the forwarding table for a match, and forward the packets to the corresponding next hop in the forwarding table.

4 What Happens if the Prefix Overlaps?

→ Since prefix might overlap (this is possible as classless Addressing is used everywhere) an incoming IP's prefix may match multiple IP entries in a table.

5 HOP-By-Hop Forwarding :-



Now what if someone adds a new routes in between this router network would that new router also be included in this or what really happends. Answer of this is that that new router also included in this routers networks. Now another question came up that is about forwarding table, How this new routes will know about other Routers and destination.

Answer → Control Plane.

→ This Routes network can be visualize as a graph.

where,

Routers ⟶ Nodes

Links ⟶ Edges.

Types of Routing :-

→ Routing is a process that is performed by Network layer devices in order to deliver the packet by choosing an optimal path from one network to another.

There are 3 types of Routing :-

1. Static Routing
2. Default Routing
3. Dynamic Routing.

1 Static Routing :-

→ Static Routing is a process in which we have to manually add routes to the routing table.

Advantages :-

- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because only the administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

Disadvantages :-

- For large Network it is a hectic task for the administrator to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have a very good knowledge of the routes of the topology.

2 Default Routing :-

→ This is a method where router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packets belongs to, it is forwarded out to the router which is configured for default routing. It is generally used with Stub router. A Stub router is a router that has only one route to reach all other networks.

3 Dynamic Routing :-

→ Dynamic Routing makes adjustments of the routes according to the current state of the route in the routing table. Dynamic Routing uses protocols to discover network destinations and the routes to reach them. RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) are the protocols used in Dynamic Routing

Features :-

- The routers should have the same dynamic protocol running in order to exchange routes.
- When a router finds a change in the topology then the router advertises it all to all other routers.

Advantages :-

- Easy to configure.
- More effective at selecting the best route to the destination remote network and also for ~~discovering~~ discovering remote network.

Disadvantages

- Consumes more bandwidth for communicating with other neighbours.
- Less secure than static Routing.

Middle Box

1 NAT (Network Address Translation)

→ Network Address Tsonslation is a process in which one or more local IP address is translated to one or more global IP address and vice versa in order to provide Internet access to local host. Also it does the translation of port numbers. i.e. masks the port number of host with another port number, in the packet ~~that~~ that will be routed to the destination. It then makes the ~~corresponding~~ corresponding entries of IP address and port number in the NAT table. NAT generally ~~root~~ operates on a router or Firewall.

To access the Internet, one public IP address is needed, we can only use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the internet through a single public address. To achieve this, the translation of a private IP address to a Public IP address is requir. which can be done by NAT.

Working :-

→ Generally, the border router is configured for NAT i.e. the router which has one interface in local (inside) network and one interface in the global (outside) network when a packet traverse outside the local (inside) Network, then NAT converts the the ~~local (inside)~~ local (Private) IP address to a global (public) IP address. when a packet enters the local network, the global (Public) IP address is converted to a local (private) IP address.

If NAT runs out of addresses. i.e. no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

Types of NAT

1. Static NAT: In this, single private IP address is mapped with a single public IP address. It used in web hosting.
2. Dynamic NAT: In this, multiple private IP addresses are mapped to a pool of public IP address. It is used when we know the number of fixed users who want to access the internet at a given point of time.
3. Port Address Translation (PAT): In this, many local (Private) IP address are mapped or translated to a single Public IP address. Port numbers are used to distinguish the traffic. This is the most frequently used one.

How NAT protects us

- It hides the IP address of any device on your network from the outside world giving them all a single address.
- It requires every incoming packet of information to have been asked by a device. If a malicious data packet isn't on the list of expected communications it gets rejected.
- Some firewalls can be whitelisting to block unauthorized outgoing traffic so that if you do contract a piece of malware your firewall may prevent it from communicating with your device.

2) Firewall

- The firewall is a network security system that is used to monitor the incoming and outgoing traffic and blocks the same based on the firewall securities policies.
  It acts as a wall between the internet (public network) and the networking devices (a private network). It is either a hardware device, software programs or a combination of both, It adds a layer of security to the network.

#Internet Control Message Protocol (ICMP)

- Since IP does not have an built-in mechanism for sending errors and control message. It depends on ICMP to provide an error control.
  It is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending errors messages and operations information, e.g. the requested service is not available or that a host or router could not be reached.

Hot Standby Router Protocol (HSRP)

- It is a CISCO proprietary protocol, which provides redundancy for a local subnet. In HSRP, two or more routers gives an illusion of a virtual Router. HSRP allows you to configure two or more routers as standby routers and only a single act as an active router at a time. All the routers in single HSRP group shares a single MAC address and IP address, which acts as a default gateway to the local network. The active router is responsible for forwarding the traffic. If it fails, the standby router takes up all the responsibilities of the active router and forwards the traffic.

Distance Vector Routing (DVR) Protocol:

→ A Distance vector Routing (DVR) protocol requires that a router inform its neighbours of topology changes periodically. Historically known as old ARPANET routing ~~protocol~~ algorithm (or known as Bellman-ford algorithm)

■ Bellman-Ford Basics: Each router maintains a Distance vector table containing the distance between itself and all possible destination nodes. Distances based on chosen matrix. are computed using information from the neighbours distance vector.

Open Shortest Path First (OSPF) Protocol

→ OSPF Protocol is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First (SPF) algorithm.

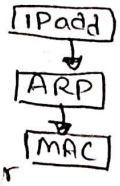
A link-State-Routing Protocol is a protocol that uses the concept of triggered updates i.e. If there is a changes observed in the learned routing table then the updates are triggered only. not like the distance-vector routing protocol where the routing table is exchanged at a period of time.

ARP and how it works

■ Address Resolution Protocol: ARP is a communication protocol used for discovering physical address associated with given network address. Typically. ARP is a network layer to data link layer mapped process, which is used to discover MAC address for given Internet Protocol Address

■ Working:

Most of the computer application/Programs uses IPaddress. to send/receive messages, however, the actual communication happens over the physical add. (MAC Address). So. our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes in to picture, its functionality is to translate IP address to MAC address.



Now,

Imagine ~~that~~ a device wants to communicate ~~over~~ with other device over the internet what ARP does?

The devices of the network peel the header of the data link layer from the PDU also called as frame and trasfer the packet to network layer. where the network ID of packet is validated with destination IP's network ID of the packet and if it is equals then it responds to the source with the MAC address of the destination, else, the packet reaches the gateway of the network and broadcasts the packet to the devices it is connected with and validates their network ID.

The above process continues till the second last network device in the path reaches the destination where it gets validated and ARP, in turn, responds with the MAC address of destination.

Packet flow in the Same Network :-

→ To transfer a packet from source to destination, both the IP address and MAC address of destination should be known. If the destination MAC address is not present then ARP will resolve this issue first then the packet will be delivered to the destination host.

There are simple rules for packet flow in a Network :

① If the destination host is present in the same network as the source host then the packet will be delivered directly to the destination host using MAC address.

② Within a network the packet will be delivered on the basis of MAC address

③ MAC address never crosses its broadcast domain.

Packet Flows in Different Network :-

→ To deliver the packet to destination host the source IP, destination IP, source MAC address, destination MAC address should be known,

Some basic rules for packet to flow :-

① If the destination host is present in same network, packet will be directly delivered.

② If the destination host is present in different network then the packet is delivered to the default gateway first which in turn delivers the packet to the destination host.

③ If ARP is not resolve then ARP will Resolve first.

④ MAC address never crosses its broadcast domain.

Layer-2 Switches v/s Layer-3 Switches

Switch :- A switch is a device which sends a data packet in a local Network

Now, what its advantage over Hub?

→ A Hub floods the network with the packets and only destination system receives that packet while others just drop, due to which the traffic increases a lot. To solve this problem switches come into picture.

A Switches first learns, by flooding network just like hub to fill MAC-address table, on which port a particular device is connected. After learning it sends packet to that particular host only.

Layer-2 switches works on Layer-2 (Data Link layer) and sends 'frames' to destination ports using MAC address table which stores the MAC address of a device associated with that port.

Layer-3 switches works on Layer-3 (network layer) where it route packet by using IP address, used widely on VLANs

Difference between Ping and Traceroute.

Need ?

→ In computer networks, data is sent as packets (PDU). Each packet is transmitted individually and may also follow a different route to reach the destination. Once all packets of original ~~packets are~~ message reaches the destination they are re-assembled to form the original message But sometimes, it may happen that the web server is down, network congestion, or some other technical glich is these, that may prevent the message from reaching the destination. To diagnose such congestions and network failure, we use two programs that are Ping & Traceroute.

1 Ping :-

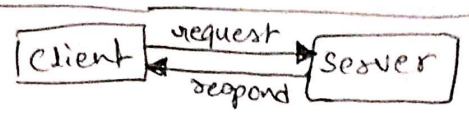
→ Ping is a utility that helps one to check if a particular IP address is accessable or not. Ping works by sending a packet to the specified address and waits for the reply.
It also measures round trip time and reports errors.
Ping is also used in checking if the computers on a local network are active For this, In cmd, type : ping 127.0.0.1.
The IP address 127.0.0.1 is the address of the localhost and would receive a ping reply even if the sender is not connected to the internet.

2 Traceroute :-

→ It is a utility that traces a packet from your computer to the host, and will also show the number of steps (hops) required to reach there, along with the time by each step.
Traceroute works by sending the packets of data with low survival time (Time to Live - TTL) which specifies how many steps (hops) can a packet survive before it is returned. when a packet can't reach the final destination and expire at intermediate step, that node returns a packet id and identifies itself. So by increasing the TTL gradually, Traceroute is able to identify the intermediate nodes. If any of the hops came back with request "Request Timed Out", it denotes network congestion and a reason for slow loading web pages. and dropped connections.

The main difference between & Ping and Traceroute is that, Ping is a quick and easy utility to tell if a specified server is reachable and how long will it take to send and receive data from the server whereas Traceroute finds the exact route taken to reach the server and time taken by each step (hop)

Servers in Computer Network :



→ A server is a computer program or a device that provides functionality for clients which are other programs or devices. This architecture is called the client-server model.
→ A single overall computation is distributed across multiple process or devices.
→ Servers can provide various functionalities called services like, sharing data or resources among among among multiple devices/clients or performing computation for clients.
→ Multiple clients can served by a single server, and a single client can use multiple servers.
→ A client process may run on the same device, It can also connect over a network to a server to run on a different device.

Ex: Web servers, mail servers, game servers, database servers, file servers, Application servers etc.

Types of Servers and their Applications :-

1 Application Server :

→ These servers hosts web apps (computer programs that run inside a web browser) allowing the users in the network to run and use them preventing the installing a copy of on their own computers.
→ These servers need not be part of the World Wide Web
→ Their clients are computers with web browser

2 Catalog Server :

→ These servers maintains an index or table of contents of information that can be found across a large distributed network. Distributed Network may include computers, users, files shared on file servers and web apps. Example of Catalog Servers are Directory servers and names servers.
• Their clients are any computer program that needs to find something on the network. Example can be domain member attempting to log in, an email client looking for an email address, or a user looking for a file.

3 Communication Servers :

→ These servers maintains an environment needed for one communication endpoint to find other endpoints and then communicates with them. These servers may or maynot include a directory of communication endpoints and a presence of detection service, depending on the openness and security parameters of the network. Their clients are communication endpoints.

4 Computing Servers :

→ These servers share vast amounts of computing resources which included CPU and RAM over a network. Any computer program that needs more CPU power and RAM than a personal computer can probably afford and can use these type of servers.
• The client must now be a networked computer to implement the client-server model which is necessity.

5. Database Server :
→ These servers maintains and shares any form of database over a network. A database is a organized collection of data with predefined properties that may be displayed in a table. • Clients of these servers are Spreadsheets; accounting software, asset management software or virtually any computer program that consumes well-organized data, especially in large volumes.

6. Fax server :
→ These servers share one or more fax machines over a network which eliminates the hassle of physical access. ~~Any~~
• Any fax sender or recipient are the clients of these servers.

7. File Server :
→ Shares files and folders, storage space to hold files and folders, or both over a network
• Networked computers are the intended clients, even though local programs can be clients.

8. Game Servers :
→ These servers enables several computers or gaming devices to play multiplayer games.
• Personal computer or gaming consoles are their clients.

9. Mail Servers :
→ These servers makes email communication possible in the same way as a post office makes snail mail communication possible.
• Clients of these servers are sender & receiver of mails (e-mails)

10. Print Servers :
→ These servers shares one or more printers over a network which eliminates the hassle of physical access.
• Clients are computers in need of printing something.

11. Proxy Servers :
→ This acts as an intermediary between clients and a server accepting incoming traffic from the client and send it to the server
Reason to use proxy server includes content control and filtering, improving traffic performance, preventing unauthorized network access or simply routing the traffic over a large and complex network.
• These clients are any networked computer

12. Web-Servers :
→ These servers hosts webpages. A web servers is responsible for making the world wide web possible. Each website has one or more web servers.
• These clients are computers with Web browser.