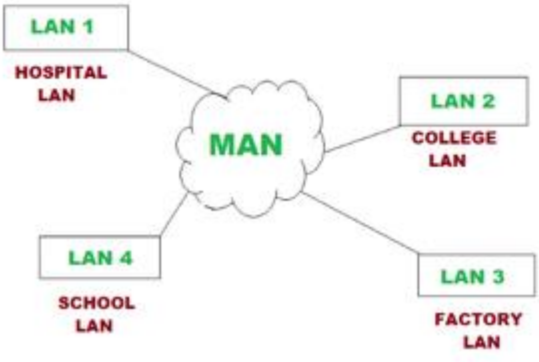
LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Early LANs had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN.

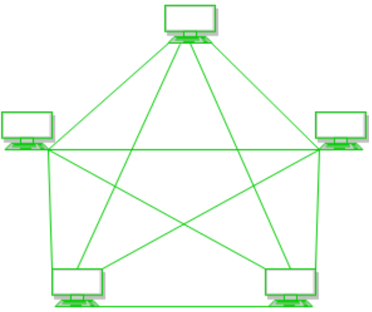
MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider).



WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LANs. There are two types of WAN: Switched WAN and Point-to-Point WAN.

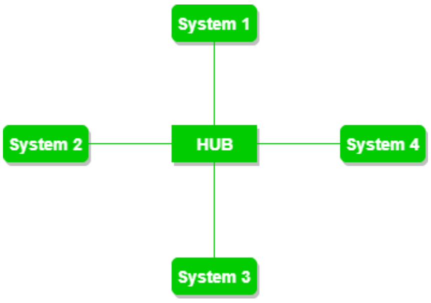
The arrangement of nodes in a network generally follows some pattern or organization. Each of these patterns have their set of advantages/disadvantages. Such arrangements are called collectively referred to as network topologies. Some of the popular network topologies are as follows:

Mesh



1. Robust & Easy fault-detection.
2. Installation is difficult & Expensive (fully-connected ~ lots of cable required = ${}^{n}C_2$).

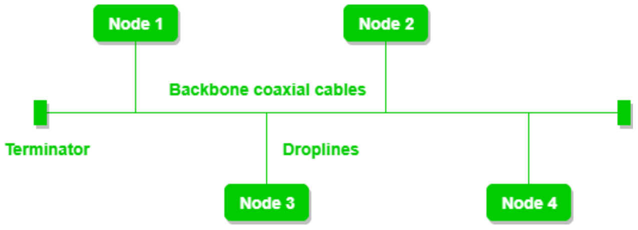
Star



1. Easy & Cheap Installation (n cables required). Also device needs to have only 1 port.

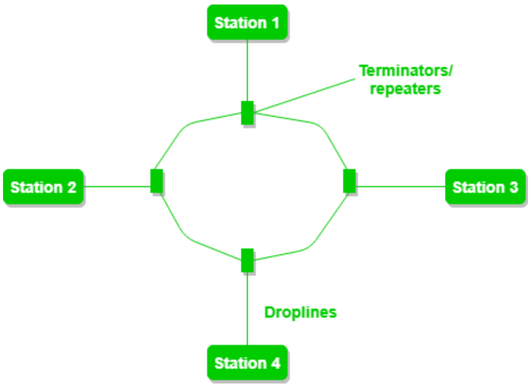
2. Single point-of-failure (central node).

Bus



1. Easy & Cheap Installation (n + 1(main-line) cables required).
2. Single line-of-failure (main-line).
3. Heavy Traffic causes collisions.

Ring



1. Easy & Cheap Installation (1 line).
2. Difficulty in Troubleshooting.
3. Addition/Removal of nodes disturbs the topology.

Hybrid

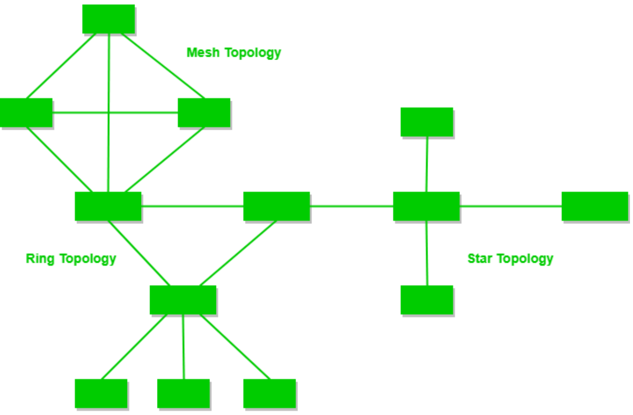
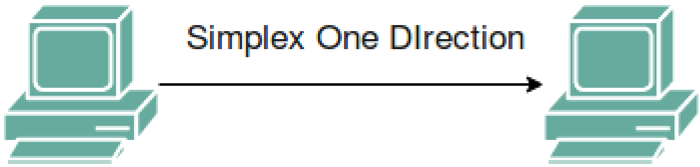


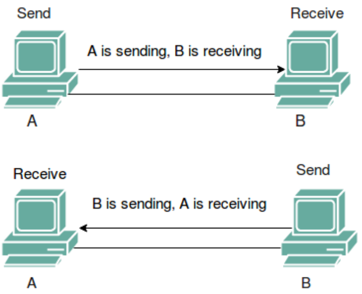
Figure - A Hybrid Topology

1. Combination of all topologies (according to requirement).
2. This kind of topology is scalable and can serve a variety of requirements
3. Due to intermixing of Ring, Bus, Star etc. topologies, it is difficult to develop. (As each of the individual topologies have their own rules and concepts ~ collision detection, protocols for data transfer etc.).

In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



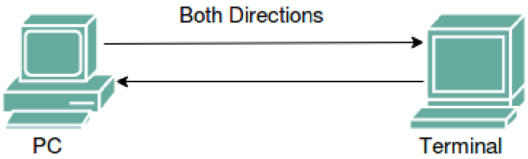
In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. Walkie-talkie in which message is sent one at a time and messages are sent in both directions. Channel capacity=Bandwidth *Propagation Delay

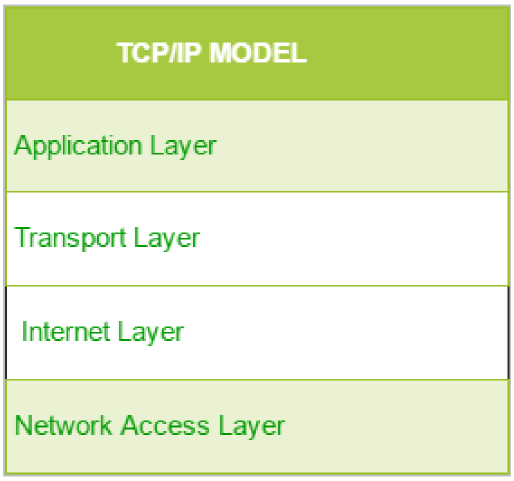


full-duplex mode, both stations can transmit and receive simultaneously. In full_duplex mode, signals going in one direction share the capacity of the link with signals going in another direction, this sharing can occur in two ways:

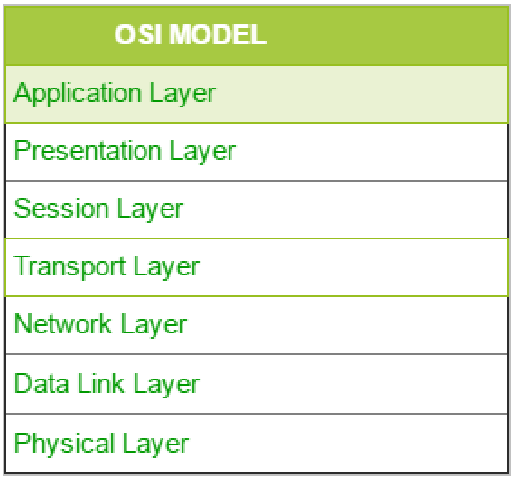
- Either the link must contain two physically separate transmission paths, one for sending and the other for receiving.
- Or the capacity is divided between signals traveling in both directions.

Channel Capacity=2* Bandwidth*propagation Delay





TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer



OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

OSI Model: Open Systems Interconnection.

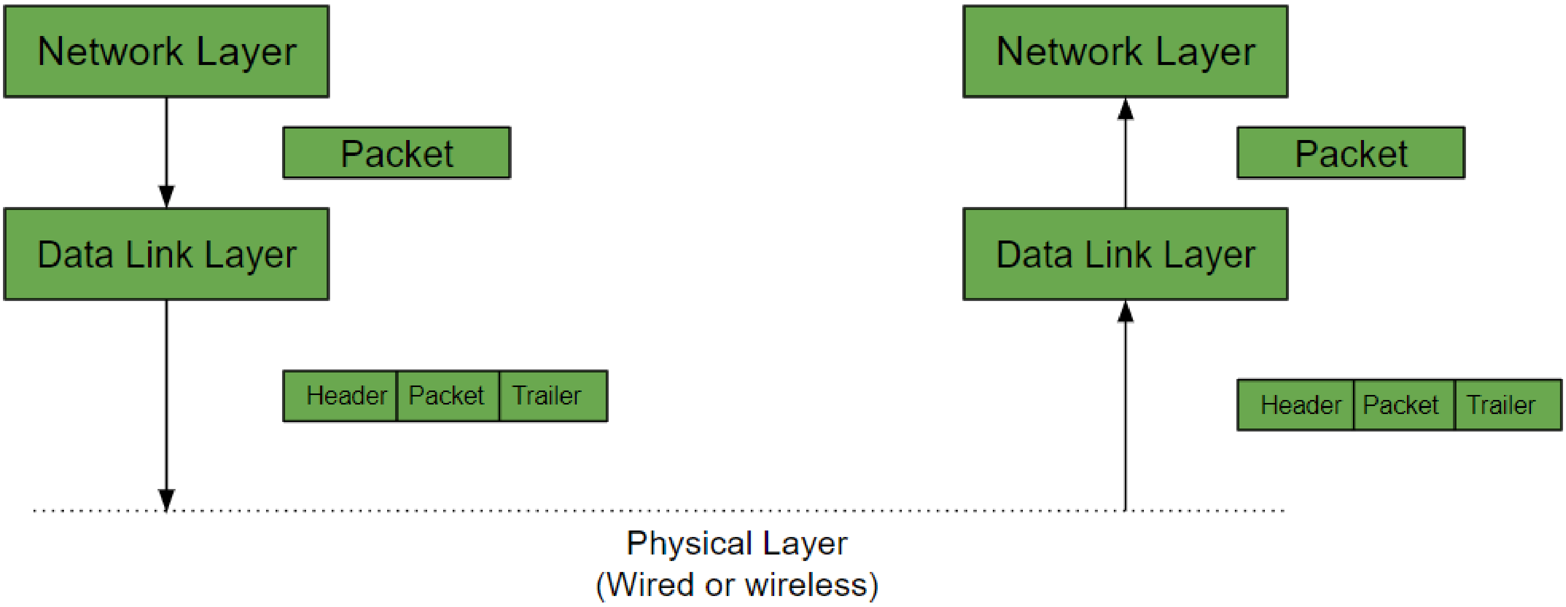
- Physical Layer: It receives/transmits signals and then converts it to physical bits (0 & 1). It handles bit-synchronization (using clock), bit-rate control (no.of bits/sec), physical topology and transmission mode (simplex, half-duplex, full-duplex).
- Data-link Layer: It is responsible for Node-to-Node delivery of packets, Framing, Error control, Flow control, Physical Addressing (MAC). Upon receiving packets from network layer, it encapsulates it within a frame with the hardware (MAC) address of the receiver (obtained via ARP ~ Address Resolution Protocol).
- Network Layer: It is responsible for Logical Addressing (IPv4/v6) and Routing. Various routing algorithms are implemented at this layer, which determines the IP for the next hop in routing.
- Transport Layer: It is responsible for End-to-end delivery of packets. It also does Segmentation & Reassembly of packets (done if packet-size exceeds MTU ~ Max. Transmission Unit). It also does multiplexing/de-multiplexing of packets according to the application (using port no.). TCP/UDP (Connection vs. Connection-less) protocol is implemented at this layer.
- Session Layer: It is responsible for Session Management (Establishment, Maintenance, Termination), Authentication, Security, Synchronization & Restoration (check-points are established, such that upon re-connection state is resumed from the last saved point) and Dialog Control (synchronization when multiple parties are interacting ~ conference).

- Presentation Layer: It is responsible for Translation (e.g. ASCII to EBCDIC), Encryption/Decryption and Compression.
- Application Layer: Implements application-specific protocols (HTTP, HTTPS, FTP, SMTP etc.) They produce the data, interacts with the user (input and display of data). e.g. Browsers, Skype, Messaging Apps.

TCP/IP Model
It comprises of 4 layers with the following responsibilities (starting from the lowest layer):

- L1 (Physical Layer): Deals with the physical aspects like electrical signals, cable types, and bit transmission.
- L2 (Data Link Layer): Manages data transfer between directly connected devices using MAC addresses, error detection, and framing.
- L3 (Network Layer): Routes packets across networks using IP addresses, responsible for logical addressing and path determination.
- L4 (Transport Layer): Provides reliable end-to-end data transfer by managing segmenting, flow control, and error checking using protocols like TCP and UDP.
- L5 (Application Layer): The user-facing layer that interacts with applications like email, web browsing, and file transfer protocols.

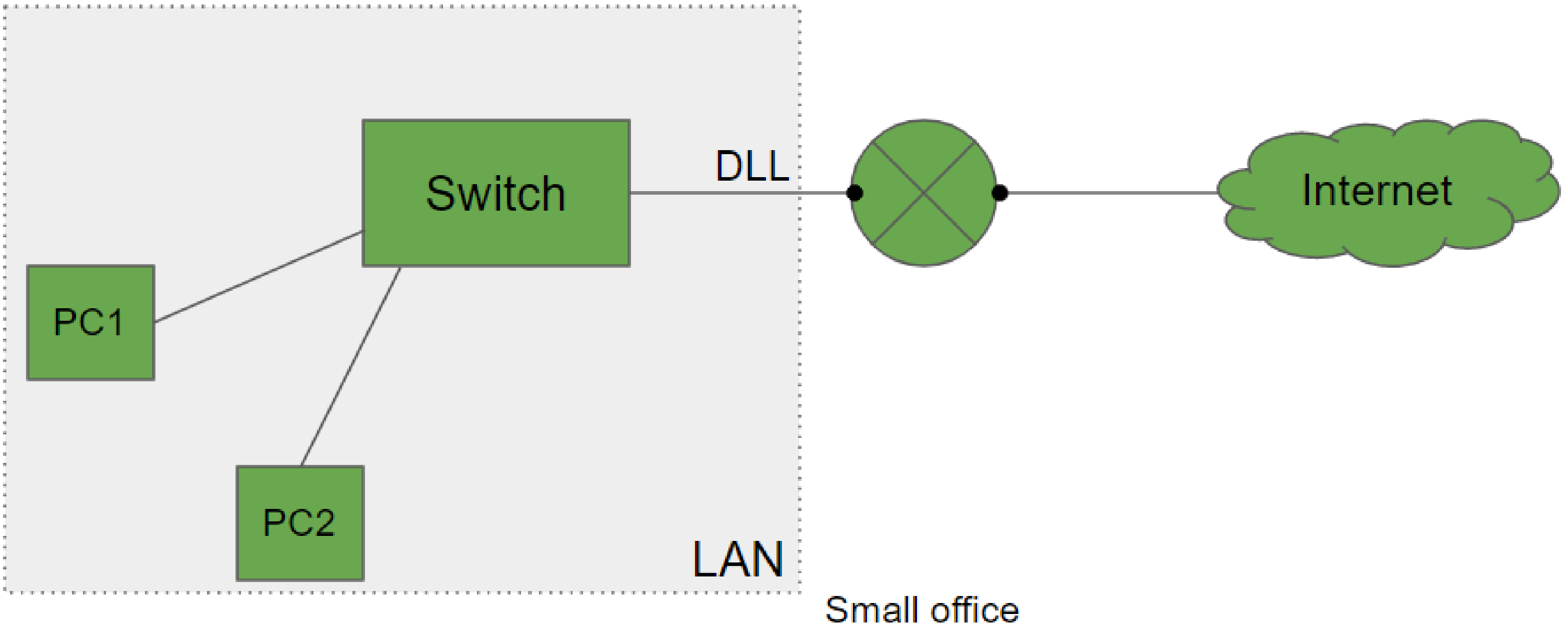
The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host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



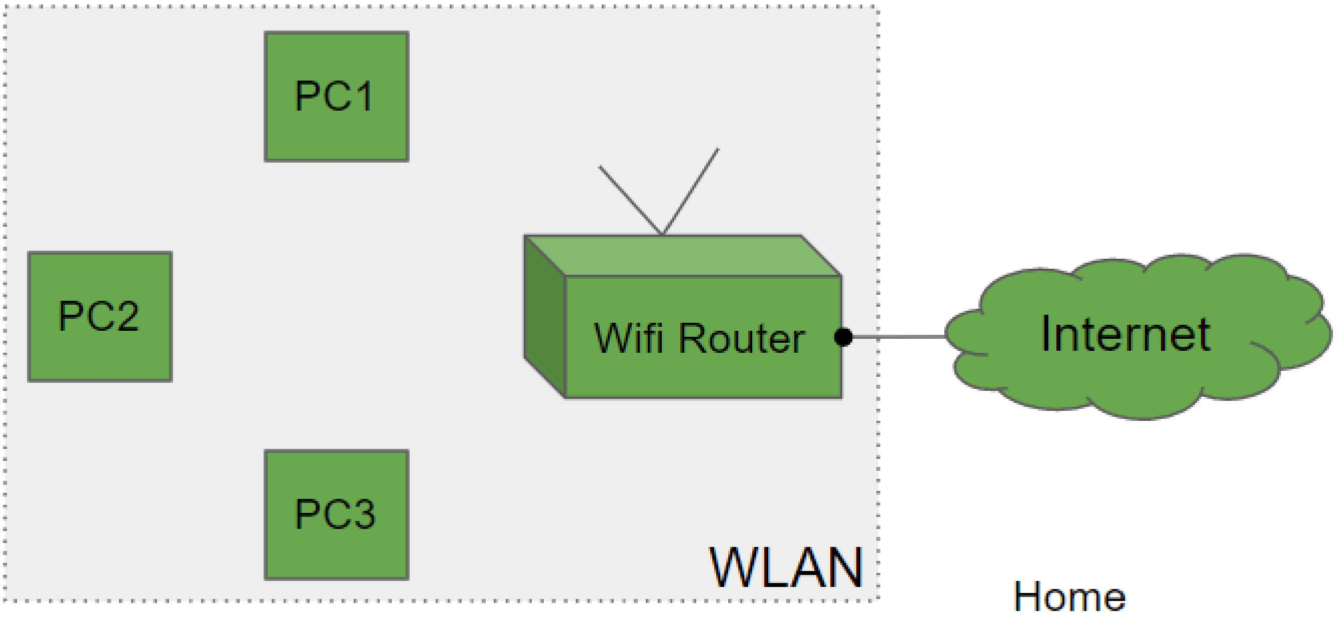
Data Link Layer is divided into two sub layers :

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

The packet received from the Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header. The Receiver’s MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.



The switch is used to connect multiple computers or laptops which in turn is connected to a router. This is then connected to the internet. All the 1-to-1 connection is done using DLL. The setup is called LAN as they are all connected in Local Area Network.



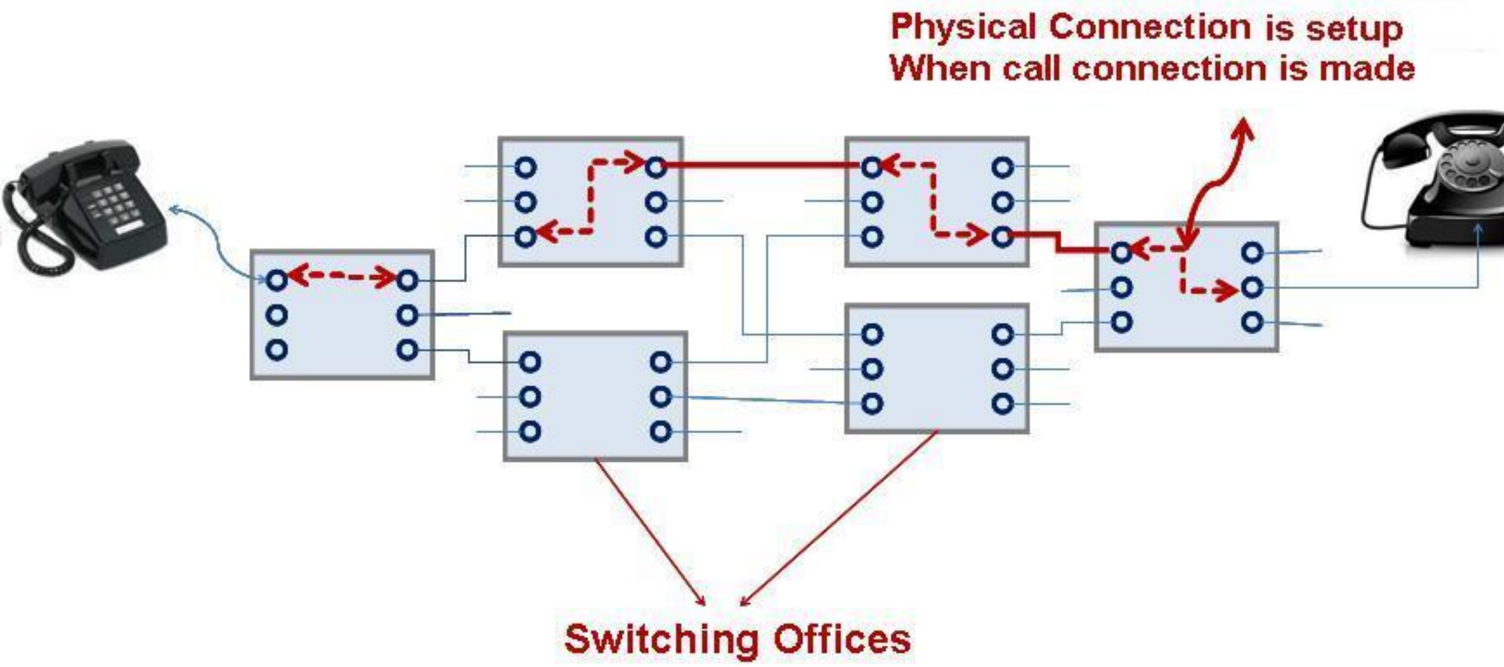
Here the router is used to convey the connection in wireless form. This is then connected to the internet. All the 1-to-1 connection is again done using DLL. The setup is called WLAN as they are all connected in Wireless Local Area Network. This network might have a collision. The functions of the Data Link layer are :

1. Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. Physical addressing: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. Error Detection: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. Error and Flow Control: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

- Packet in Data Link layer is referred as 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.

Stop and wait ARQ, Selective repeat protocol, Sliding window, Go back N etc. protocols are used in data link layer and transport layers.

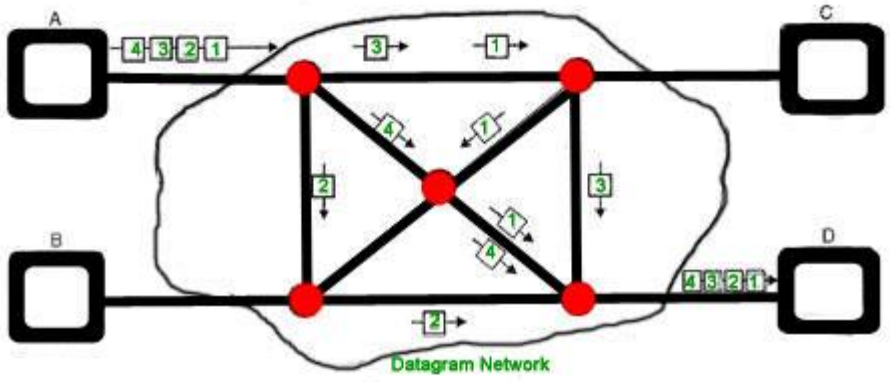
Circuit-Switching is a historically used scheme which has been currently replaced by Packet-Switching. In circuit-switching, network resources are dedicated to establish a connection between the end-devices. Thus, a dedicated fixed path is established where data is transmitted without delays (as there is no concept of network congestion). A telephone system works under this scheme.



Key points of circuit switching:

- suitable for continuous transmission (dedicated line)
- guaranteed data-rate
- Inefficient (no transmission even if line is free)
- Under-utilization of resources in most cases

Packet switching is a method of transferring the data to a network in the form of packets. In order to transfer the file fast and efficient manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called Packet. At the destination, all these small-parts (packets) has to be reassembled, belonging to the same file. A packet composes of payload and various control information. No pre-setup or reservation of resources is needed.
Packet Switching uses Store and Forward technique while switching the packets; while forwarding the packet each hop first store that packet than forward. This technique is very beneficial because packets may get discarded at any hop due to some reason. More than one path is possible between a pair of source and destination. Each packet contains Source and destination address using which they independently travel through the network.



Datagram Packet Switching

Some of the key points of packet switching are:

- Efficient utilisation of network resources
- out-of-order reception of packets

- Transmission delay (variable data-rate)

Advantage of Packet Switching over Circuit Switching :

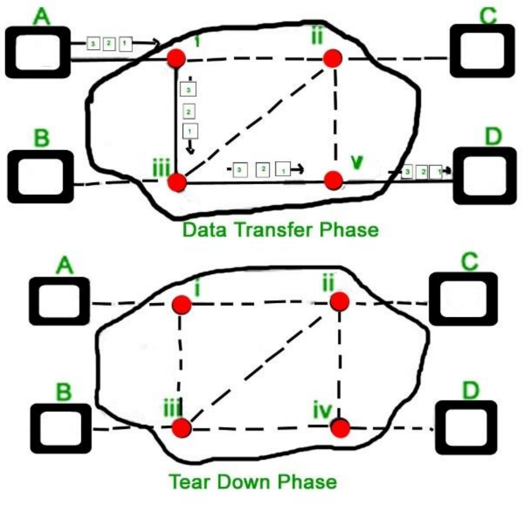
- More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
- Minimal transmission latency.
- More reliable as destination can detect the missing packet.
- More fault tolerant because packets may follow different path in case any link is down, Unlike Circuit Switching.
- Cost effective and comparatively cheaper to implement.

Disadvantage of Packet Switching over Circuit Switching :

- Packet Switching don't give packets in order, whereas Circuit Switching provides ordered delivery of packets because all the packets follow the same path.
- Since the packets are unordered, we need to provide sequence numbers to each packet.
- Complexity is more at each node because of the facility to follow multiple path.
- Transmission delay is more because of rerouting.
- Packet Switching is beneficial only for small messages, but for bursty data (large messages) Circuit Switching is better.

Modes of Packet Switching :

1. Connection-oriented Packet Switching (Virtual Circuit) :- Before starting the transmission, it establishes a logical path or virtual connection using signalling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended with help of sequence number. Overall, three phases takes place here- Setup, data transfer and tear down phase.

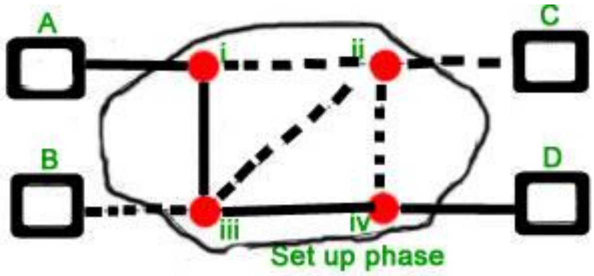


Data Transfer Phase

Tear Down Phase

Phases in virtual circuit packet switching

2.

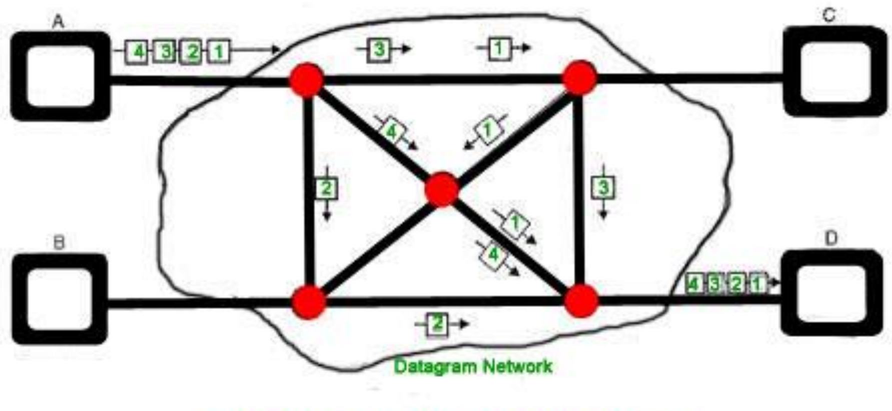


Set up phase

3.

4. All address information is only transferred during setup phase. Once the route to destination is discovered, entry is added to switching table of each intermediate node. During data transfer, packet header (local header) may contain information such as length, timestamp, sequence number etc. Connection-oriented switching is very useful in switched WAN. Some popular protocols which use Virtual Circuit Switching approach are X.25, Frame-Relay, ATM and MPLS(Multi-Protocol Label Switching).

5. Connectionless Packet Switching (Datagram) :- Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers etc. In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits. Packet delivery is not guaranteed in connectionless packet switching, so the reliable delivery must be provided by end systems using additional protocols.



Datagram Packet Switching

To send a packet from A to B there are delays since this is a Store and Forward network.

FPS फपस: Frame packet segment

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

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

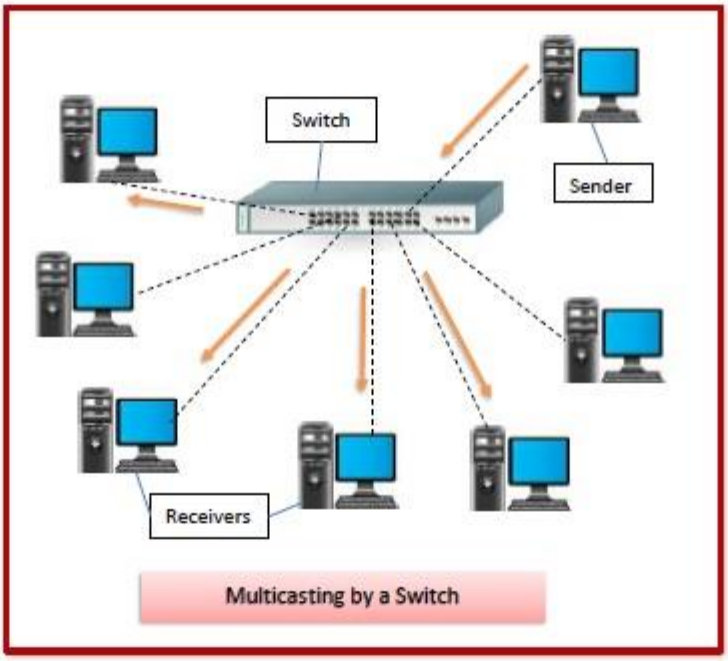
Segment in Network layer is referred as Packet.
Network layer is implemented by networking devices such as routers.

1. Internetworking: Made possible using Routers. This can be across various types like 802.11, 3G, Ethernet etc
2. Addressing: This involves processing of IP Adresses
3. Routing and Forwarding: A routing table is maintained by the routers to decide how a packet must be transmitted globally to its specific IP addresses. This process does the global connection is called routing. Forwarding is more of a local concept instead of global.
4. Scalability (Using hierarchy in Networks): This refers to the hierarchial organisation of packets.
5. Bandwidth Control: There must be a good utilisation of Bandwidth.
6. Fragmentation and Re-assembly: Division of bigger packets into multiple small packets and rearranging them to get the original packet is called Fragmentation and Re-assembly respectively.

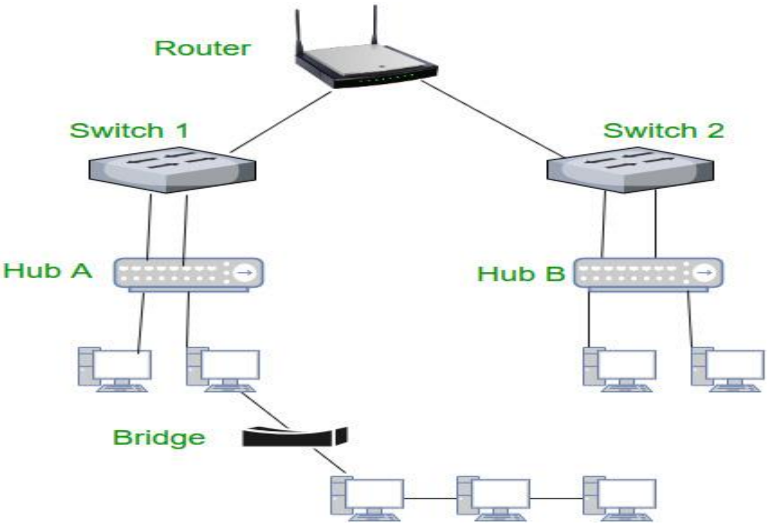
Before understanding the working at the Networking layer, let's get familiar with a few technical devices that has a great role to play in this system:

1. Switch - A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. The switch is a data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains the same. Switches

learn the Ethernet addresses of connected devices. When a data packet arrives at a switch port, the switch determines where it's going. The switch forwards the packet to the correct port for its destination. A network switch connects devices on a network, like computers, printers, and servers, so they can communicate with each other.



2. Routers - A router is a device like a switch that routes data packets based on their IP addresses. The 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.



3. Brouter - It is also known as the bridging router is a device which combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as a bridge, it is capable of filtering local area network traffic.

4. Repeater - A repeater 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. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

5. Hub - A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage. Types of Hub

   - Active Hub:- These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.

- Passive Hub:- These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

6. 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 protocol. It has a single input and single output port, thus making it a 2 port device. Types of Bridges

   - Transparent Bridges:- These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

   - Source Routing Bridges:- In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

7. Gateway - A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

8. Functions of Network Layer:
   1) It helps in the delivery of data in the form of packets.
   2) It helps in the delivery of packets from source host to the destination host.
   3) The network layer is basically used when we want to send data over a different network.
   4) In this logical addressing is used ie. when data is to be sent in the same network we need an only physical address but if we wish to send data outside network we need a logical address.
   5) It helps in routing ie. routers and switches are connected at this layer to route the packets to its final destination.

IPv4 and IPv6 are internet protocol version 4 and internet protocol version 6, IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Difference Between IPv4 and IPv6:

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end to end, connection integrity is Achievable
It can generate 4.29×10^9 address space	Address space of IPv6 is quite large it can produce 3.4×10^{38} address space
The Security feature is dependent on application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by the sender

IPv4	IPv6
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has header of 40 bytes fixed
IPv4 consist of 4 fields which are separated by dot (.)	IPv6 consist of 8 fields, which are separated by colon (:)
IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C , Class D , Class E.	IPv6 does not have any classes of IP address.
IPv4 supports VLSM(Variable Length subnet mask).	IPv6 does not support VLSM.
Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

Network Address and Mask

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.

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 B - 255.255.0.0

Class C - 255.255.255.0

Example : Given IP address 132.6.17.85 and default class B mask, find the beginning address (network address).

Solution : The default mask is 255.255.0.0, which means that the only the first 2 bytes are preserved and the other 2 bytes are set to 0. Therefore, the network address is 132.6.0.0.

Subnetting: Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different smaller networks is called subnetting. It is a practice that is widely used when classless addressing is done.

Classless Addressing

To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28. Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.

Some values calculated in subnetting :

1. Number of subnets : Given bits for mask - No. of bits in default mask

2. Subnet address : AND result of subnet mask and the given IP address

3. Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address

4. Number of hosts per subnet : $2^{(32\text{ - Given bits for mask})}$ - 2

5. First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)

6. Last Host ID : Subnet address + Number of Hosts

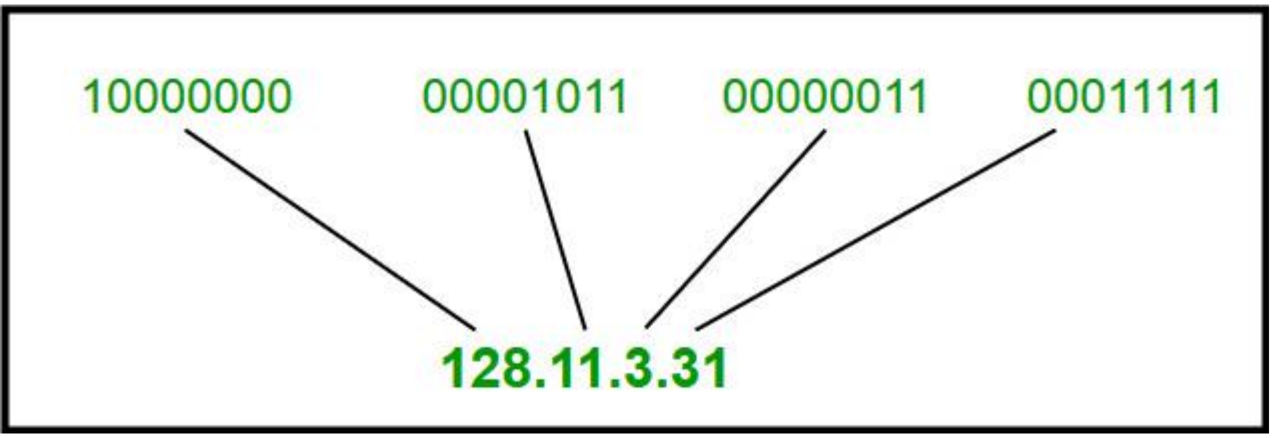
Example : Given IP Address - 172.16.0.0/25, find the number of subnets and the number of hosts per subnet. Also, for the first subnet block, find the subnet address, first host ID, last host ID and broadcast address.

Solution : This is a class B address. So, no. of subnets = $2^{(25-16)} = 2^9 = 512$.

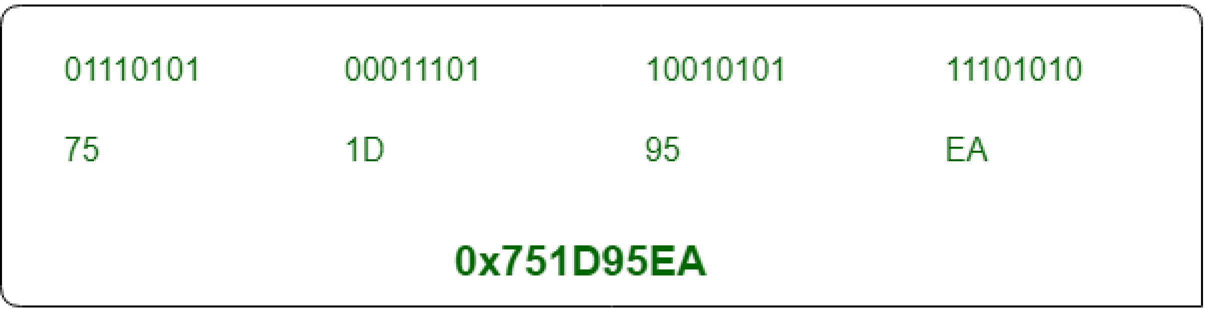
No. of hosts per subnet = $2^{(32-25)} - 2 = 2^7 - 2 = 128 - 2 = 126$

For the first subnet block, we have subnet address = 0.0, first host id = 0.1, last host id = 0.126 and broadcast address = 0.127

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 2^{32}. Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation. Dotted Decimal Notation:



Hexadecimal Notation:



Some points to be noted about dotted decimal notation:

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

Classful Addressing
The 32 bit IP address is divided into five sub-classes. These are:

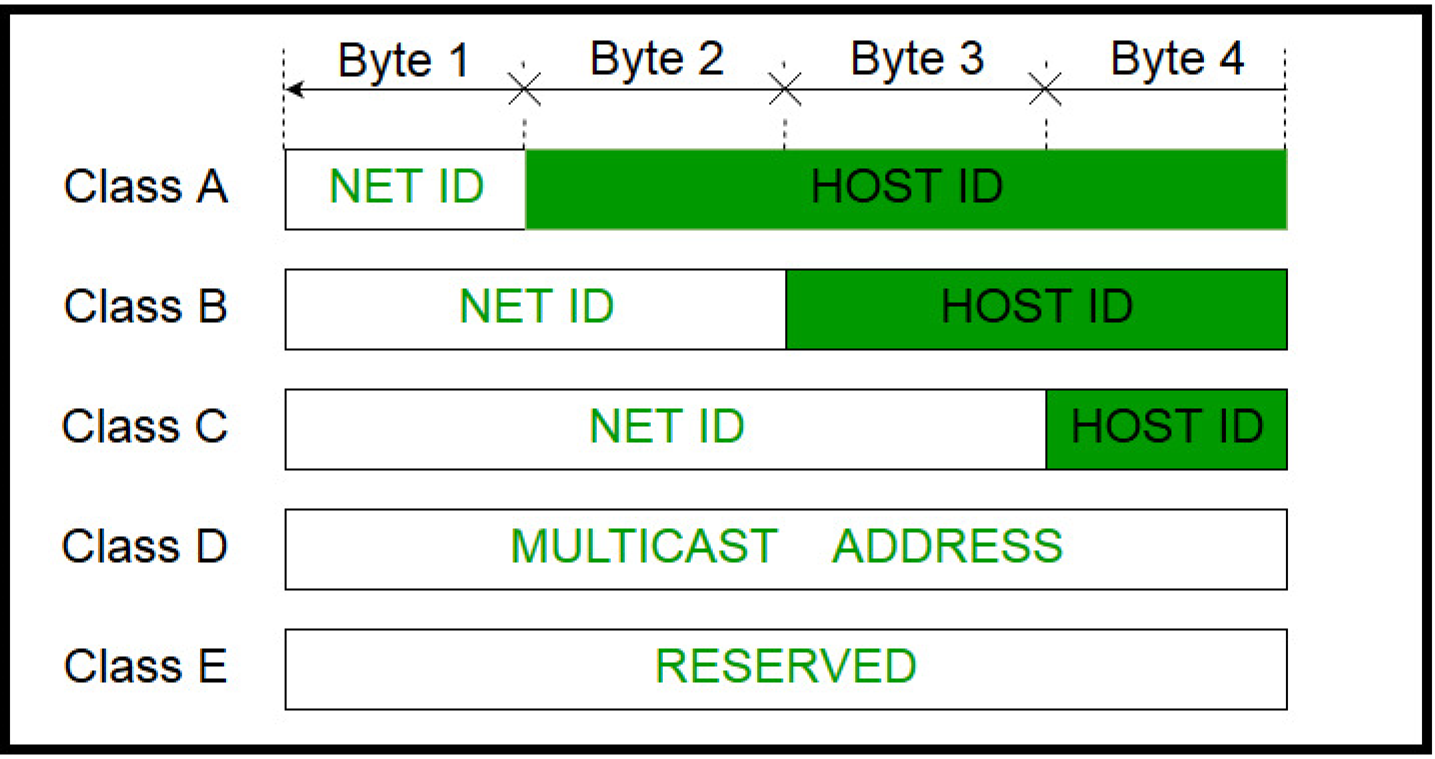
- Class A
- Class B

- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.
IPv4 address is divided into two parts:

- Network ID
- Host ID

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.
Class A:

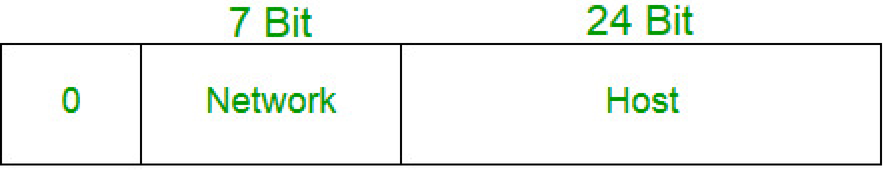
IP address belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

- 2^7-2= 126 network ID(Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address.)
- 2^24 - 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.x.x.x - 126.x.x.x



Class A

Class B:

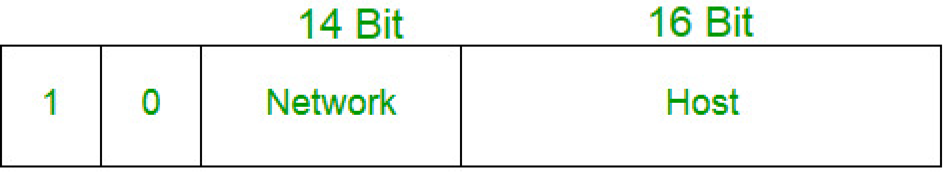
IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 - 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.x.x - 191.255.x.x.



Class B

Class C:

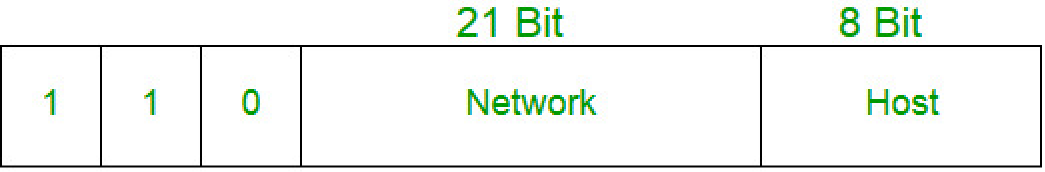
IP address belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address
- 2^8 - 2 = 254 host address

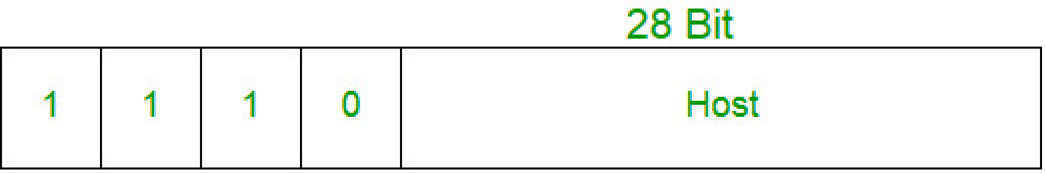
IP addresses belonging to class C ranges from 192.0.0.x - 223.255.255.x.



Class C

Class D:

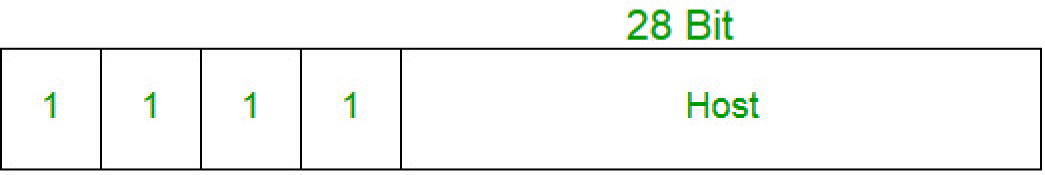
IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize. Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 - 239.255.255.255.



Class D

Class E:

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 - 255.255.255.254. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Class E

Range of special IP addresses:

169.254.0.0 - 169.254.0.16 : Link local addresses 127.0.0.0 - 127.0.0.8 : Loop-back addresses 0.0.0.0 - 0.0.0.8 : used to communicate within the current network.

Rules for assigning Host ID:

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

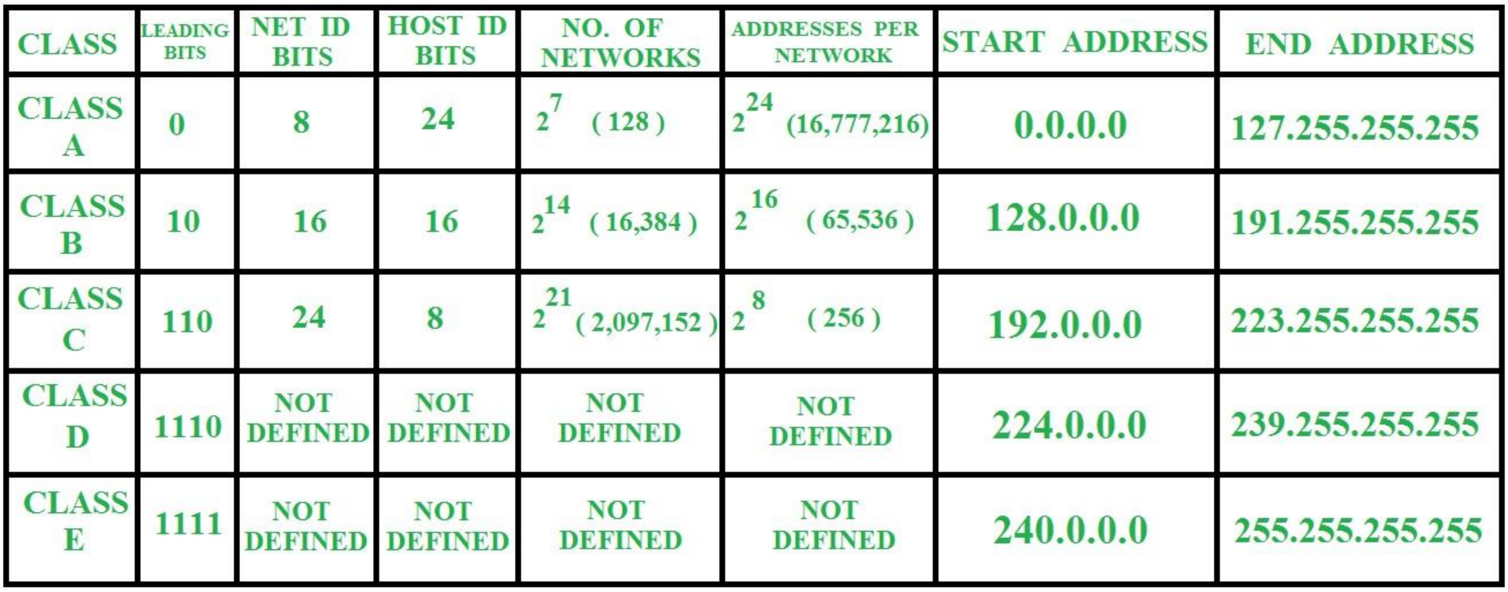
- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast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

Rules for assigning Network ID:

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Summary of Classful addressing :



CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^{7} (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^{8} (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Problems with Classful Addressing:

The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

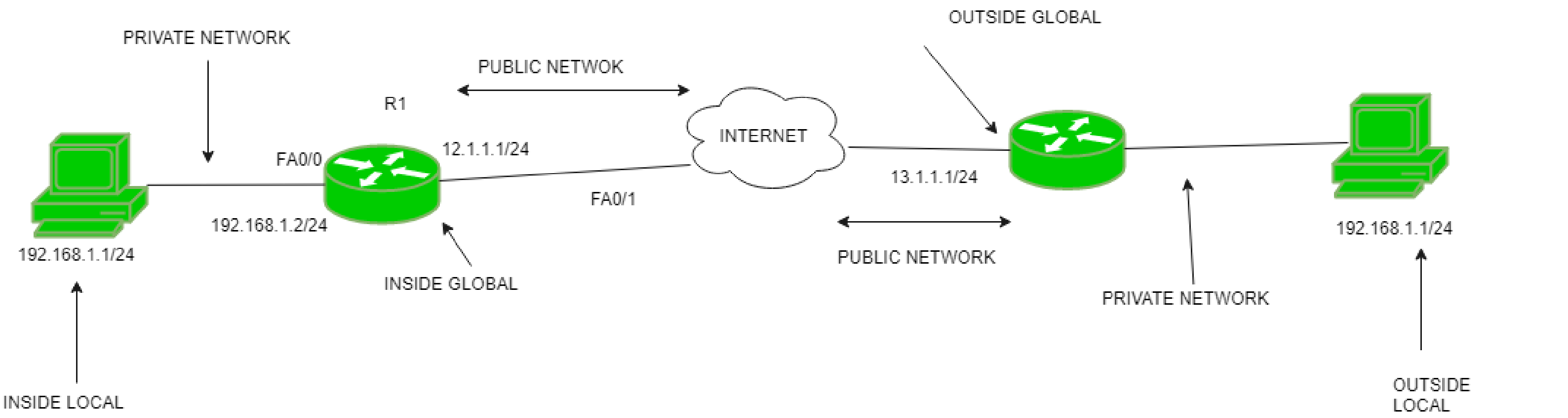
To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Network Address Translation (NAT) working -
Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that 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.

Why mask port numbers ?
Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies to the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are the same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

NAT inside and outside addresses -
Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.



- Inside local address - An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.

- Inside global address - IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.

- Outside local address - This is the actual IP address of the destination host in the local network after translation.

- Outside global address - This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types -
There are 3 ways to configure NAT:

1. Static NAT - In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed. Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

2. Dynamic NAT - In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses. Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

3. Port Address Translation (PAT) - This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT -

- NAT conserves legally registered IP addresses.

- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.

- Eliminates address renumbering when a network evolves.

Disadvantage of NAT -

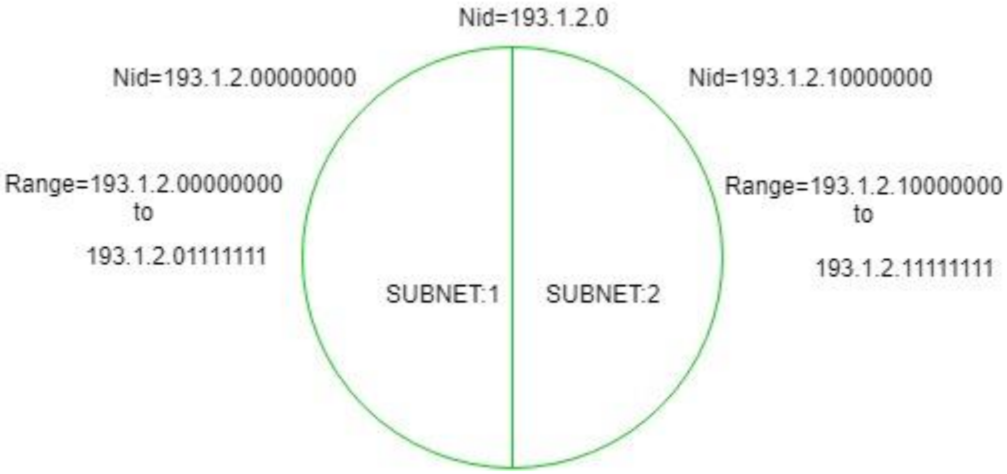
- Translation results in switching path delays.

- Certain applications will not function while NAT is enabled.

- Complicates tunnelling protocols such as IPsec.

- Also, the router being a network layer device, should not tamper with port numbers (transport layer) but it has to do so because of NAT.

When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks. For example, if we consider a class A address, the possible number of hosts is 2^{24} for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts. Now, let's talk about dividing a network into two parts: To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets. Note: It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part. Subnetting for a network should be done in such a way that it do not effect the network bits. In class C the first 3 octet's are network bits so it remains as it is.

- For Subnet-1: The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part and the . Thus, the range of subnet-1:

  193.1.2.0 to 193.1.2.127

  Subnet id of Subnet-1 is : 193.1.2.0

  Direct Broadcast id of Subnet-1 is : 193.1.2.127

  Total number of host possible is : 126 (Out of 128, 2 id's are used for Subnet id & Direct Broadcast id)

  Subnet mask of Subnet- 2 is : 255.255.255.128

- For Subnet-2: The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111). Thus, the range of subnet-2:

  193.1.2.128 to 193.1.2.255

  Subnet id of Subnet-2 is : 193.1.2.128

  Direct Broadcast id of Subnet-2 is : 193.1.2.255

  Total number of host possible is : 126 (Out of 128, 2 id's are used for Subnet id & Direct Broadcast id)

  Subnet mask of Subnet- 2 is : 255.255.255.192

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

Note:

1. To divide a network into four (2^2) parts you need to choose two bits from the host id part for each subnet i.e, (00, 01, 10, 11).
2. To divide a network into eight (2^3) parts you need to choose three bits from the host id part for each subnet i.e, (000, 001, 010, 011, 100, 101, 110, 111) and so on.
3. We can say that if the total number of subnets in a network increases the total number of usable hosts decreases.

Along with the advantage there is a small disadvantage for subnetting that is, before subnetting to find the IP address first network id is found then host id followed by process id, but after subnetting first network id is found then subnet id then host id and finally process id by this the computation increases.

Example1. An organization is assigned a class C network address of 201.35.2.0. It uses a netmask of 255.255.255.192 to divide this into sub-networks. Which of the following is/are valid host IP addresses?

A. 201.35.2.129

B. 201.35.2.191

C. 201.35.2.255

D. Both (A) and (C)

Solution:

Converting the last octet of the netmask into the binary form: 255.255.255.11000000

Converting the last octet of option A into the binary form: 201.35.2.10000001

Converting the last octet of option B into the binary form: 201.35.2.10111111

Converting the last octet of option C into the binary form: 201.35.2.11111111

From the above, we see that Option B and C is not a valid host IP address (as they are broadcast address of a subnetwork)

and OPTION A is not a broadcast address and it can be assigned to a host IP.

Example 2. An organization has a class C network address of 201.32.64.0. It uses a subnet mask of 255.255.255.248. Which of the following is NOT a valid broadcast address for any subnetworks?

A. 201.32.64.135

B. 201.32.64.240

C. 201.32.64.207

D. 201.32.64.231

Solution:

Converting the last octet of the netmask into the binary form: 255.255.255.11111000

Converting the last octet of option A into the binary form: 201.32.64.10000111

Converting the last octet of option B into the binary form: 201.32.64.11110000

Converting the last octet of option C into the binary form: 201.32.64.11001111

Converting the last octet of option D into the binary form: 201.32.64.11100111

From the above, we can see that, in OPTION A, C, and D all the host bits are 1 and give the valid broadcast address of subnetworks and OPTION B the last three bits of the Host address are not 1 therefore it's not a valid broadcast address.

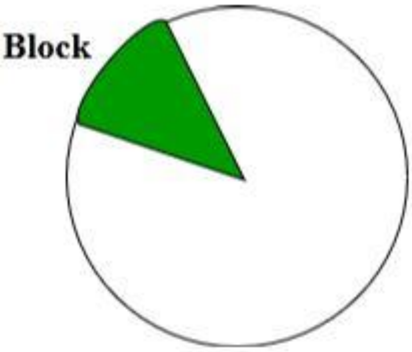
As we have already learned about Classful Addressing, so in this article, we are going to learn about Classless Inter-Domain Routing. which is also known as Classless addressing. In the Classful addressing the no of Hosts within a network always remains the same depending upon the class of the Network.

Class A network contains 2^{24} Hosts,

Class B network contains 2^{16} Hosts,

Class C network contains 2^{8} Hosts

Now, let's suppose an Organization requires 2^{14} hosts, then it must have to purchase a Class B network. In this case, 49152 Hosts will be wasted. This is the major drawback of Classful Addressing. In order to reduce the wastage of IP addresses a new concept of Classless Inter-Domain Routing is introduced. Now a days IANA is using this technique to provide the IP addresses. Whenever any user asks for IP addresses, IANA is going to assign that many IP addresses to the User.

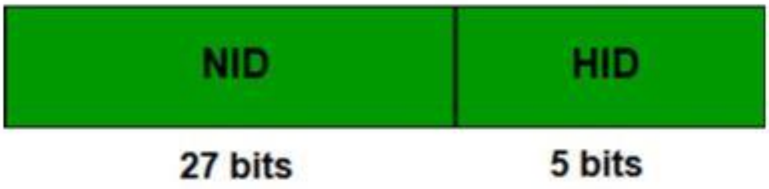


Representation: It is as also a 32-bit address, which includes a special number which represents the number of bits that are present in the Block Id.

a . b . c . d / n
Where, n is number of bits that are present in Block Id / Network Id.
Example:

20.10.50.100/20
Rules for forming CIDR Blocks:

1. All IP addresses must be contiguous.
2. Block size must be the power of 2 (2^n). If the size of the block is the power of 2, then it will be easy to divide the Network. Finding out the Block Id is very easy if the block size is of the power of 2. Example: If the Block size is 2^5 then, Host Id will contain 5 bits and Network will contain 32 - 5 = 27 bits.



3. First IP address of the Block must be evenly divisible by the size of the block. in simple words, the least significant part should always start with zeroes in Host Id. Since all the least significant bits of Host Id is zero, then we can use it as Block Id part.
   Example:
   Check whether 100.1.2.32 to 100.1.2.47 is a valid IP address block or not?

1. All the IP addresses are contiguous.
2. Total number of IP addresses in the Block = 16 = 2^4.
3. 1st IP address: 100.1.2.00100000 Since, Host Id will contains last 4 bits and all the least significant 4 bits are zero. Hence, first IP address is evenly divisible by the size of the block.

All the three rules are followed by this Block. Hence, it is a valid IP address block.

A distance-vector routing (DVR) protocol requires that a router inform its neighbours of topology changes periodically. Historically known as the old ARPANET routing 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 a chosen metric, are computed using information from the neighbors' distance vectors.
Information kept by DV router -

- Each router has an ID
- Associated with each link connected to a router,
- there is a link cost (static or dynamic).

- Intermediate hops

Distance Vector Table Initialization -

- Distance to itself = 0
- Distance to ALL other routers = infinity number.

Distance Vector Algorithm -

1. A router transmits its distance vector to each of its neighbours in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbours.
3. A router recalculates its distance vector when:
   - It receives a distance vector from a neighbour containing different information than before.
   - It discovers that a link to a neighbour has gone down.

The DV calculation is based on minimizing the cost to each destination

Dx(y) = Estimate of least cost from x to y

C(x,v) = Node x knows cost to each neighbor v

Dx = [Dx(y): y ∈ N] = Node x maintains distance vector

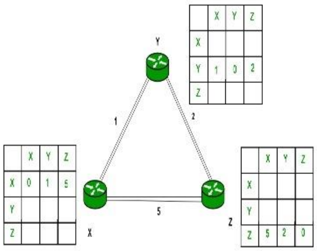
Node x also maintains its neighbors' distance vectors

– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N]

Note -

- From time-to-time, each node sends its own distance vector estimate to neighbors.
- When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it updates its own DV using B-F equation:
- Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ∈ N

Example - Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



	X	Y	Z
X			
Y	1	0	2
Z			

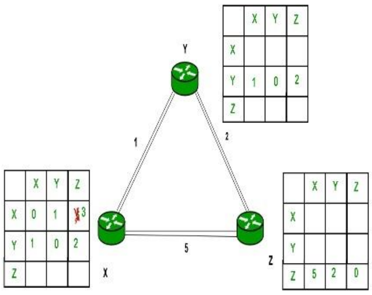
	X	Y	Z
X	0	1	5
Y			
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

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

As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.

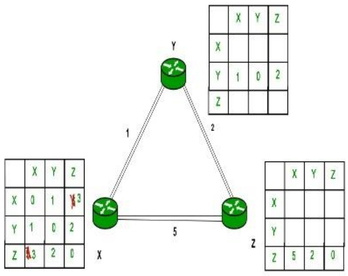


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~3
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Similarly for Z also –

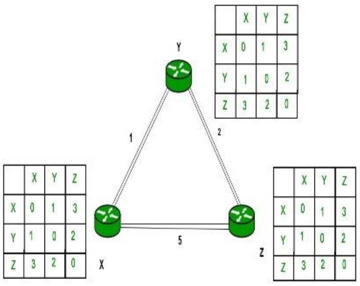


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~3
Y	1	0	2
Z	~~5~~3	2	0

	X	Y	Z
X			
Y			
Z	5	2	0

Finally the routing table for all –



	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

Advantages of Distance Vector routing -

- It is simpler to configure and maintain than link state routing.

Disadvantages of Distance Vector routing -

  - It is slower to converge than link state.
  - It is at risk from the count-to-infinity problem.
  - It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.
  - For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links.

Note - Distance Vector routing uses UDP(User datagram protocol) for transportation.

Unicast - Unicast means the transmission from a single sender to a single receiver. It is a point-to-point communication between sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

- TCP is the most commonly used unicast protocol. It is a connection-oriented protocol that relies on acknowledgement from the receiver side.
- HTTP stands for HyperText Transfer Protocol. It is an object-oriented protocol for communication.

There are three major protocols for unicast routing:

1. Distance Vector Routing
2. Link State Routing
3. Path-Vector Routing

Link State Routing - Link state routing is the second family of routing protocols. While distance-vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.

Features of link state routing protocols -

- Link state packet - A small packet that contains routing information.
- Link state database - A collection of information gathered from the link-state packet.
- Shortest path first algorithm (Dijkstra algorithm) - A calculation performed on the database results in the shortest path
- Routing table - A list of known paths and interfaces.

Calculation of shortest path -
To find the shortest path, each node needs to run the famous Dijkstra algorithm. This famous algorithm uses the following steps:

- Step-1: The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database
- Step-2: Now the node selects one node, among all the nodes not in the tree-like structure, which is nearest to the root, and adds this to the tree. The shape of the tree gets changed.
- Step-3: After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.
- Step-4: The node repeats Step 2. and Step 3. until all the nodes are added to the tree

Link State protocols in comparison to Distance Vector protocols have:

1. It requires a large amount of memory.
2. Shortest path computations require many CPU circles.
3. If a network uses little bandwidth; it quickly reacts to topology changes
4. All items in the database must be sent to neighbors to form link-state packets.
5. All neighbors must be trusted in the topology.
6. Authentication mechanisms can be used to avoid undesired adjacency and problems.
7. No split horizon techniques are possible in the link-state routing.
    - Open Shortest Path First (OSPF) is a unicast routing protocol developed by a working group of the Internet Engineering Task Force (IETF).
    - It is an intradomain routing protocol.
    - It is an open-source protocol.
    - It is similar to Routing Information Protocol (RIP)
    - OSPF is a classless routing protocol, which means that in its updates, it includes the subnet of each route it knows about, thus, enabling variable-length subnet masks. With variable-length subnet masks, an IP network can be broken into many subnets of various sizes. This provides network administrators with extra network configuration flexibility. These updates are multicasts at specific addresses (224.0.0.5 and 224.0.0.6).
    - OSPF is implemented as a program in the network layer using the services provided by the Internet Protocol

  - IP datagram that carries the messages from OSPF sets the value of the protocol field to 89
  - OSPF is based on the SPF algorithm, which sometimes is referred to as the Dijkstra algorithm
  - OSPF has two versions - version 1 and version 2. Version 2 is used mostly

OSPF Messages – OSPF is a very complex protocol. It uses five different types of messages. These are as follows:

1. Hello message (Type 1) - It is used by the routers to introduce themselves to the other routers.
2. Database description message (Type 2) - It is normally sent in response to the Hello message.
3. Link-state request message (Type 3) - It is used by the routers that need information about specific Link-State packets.
4. Link-state update message (Type 4) - It is the main OSPF message for building Link-State Database.
5. Link-state acknowledgement message (Type 5) - It is used to create reliability in the OSPF protocol.

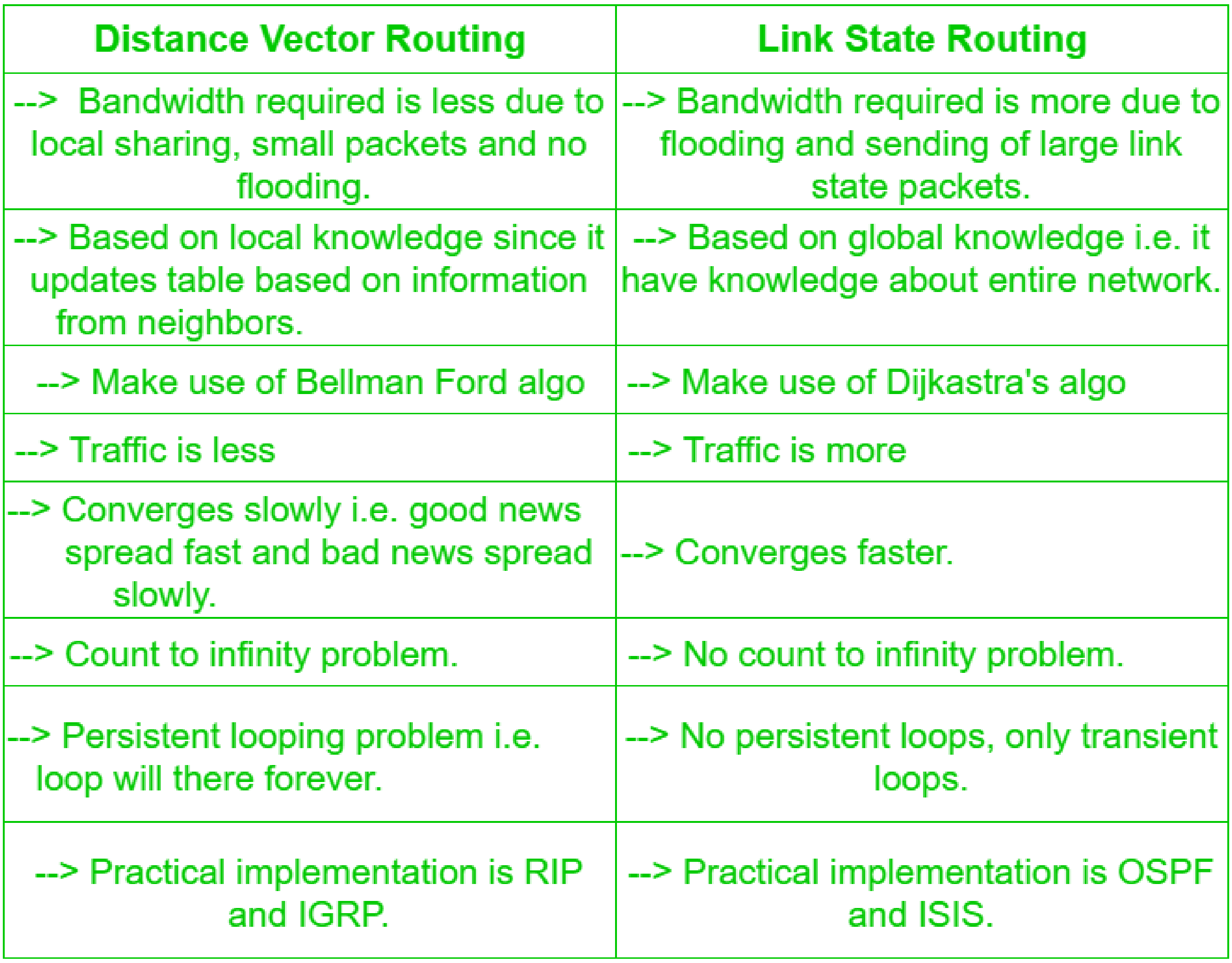
Distance Vector Routing -

- It is a dynamic routing algorithm in which each router computes a distance between itself and each possible destination i.e. its immediate neighbours.
- The router shares its knowledge about the whole network to its neighbours and accordingly updates the table based on its neighbours.
- The sharing of information with the neighbours takes place at regular intervals.
- It makes use of Bellman-Ford Algorithm for making routing tables.
- Problems - Count to infinity problem which can be solved by splitting horizon.
  - Good news spread fast and bad news spread slowly.
  - Persistent looping problem i.e. loop will be there forever.

Link State Routing -

- It is a dynamic routing algorithm in which each router shares knowledge of its neighbours with every other router in the network.
- A router sends its information about its neighbours only to all the routers through flooding.
- Information sharing takes place only whenever there is a change.
- It makes use of Dijkstra's Algorithm for making routing tables.
- Problems - Heavy traffic due to flooding of packets.
  - Flooding can result in infinite looping which can be solved by using the Time to live (TTL) field.

Comparison between Distance Vector Routing and Link State Routing:



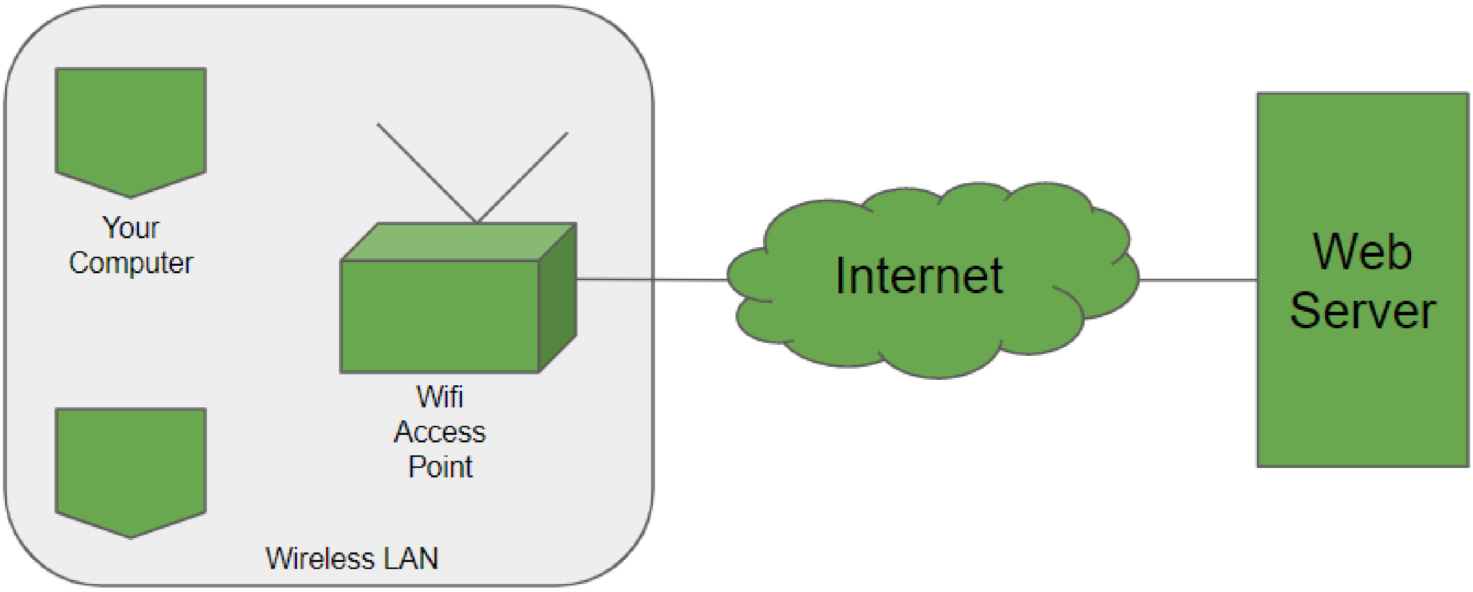
Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

Transport Layer is the layer which lies just above the Network layer and is responsible for end-to-end connectivity. It is so-called because it provides point-to-point rather than hop-to-hop. The unit of transmission at the transport layer is called segmentation.

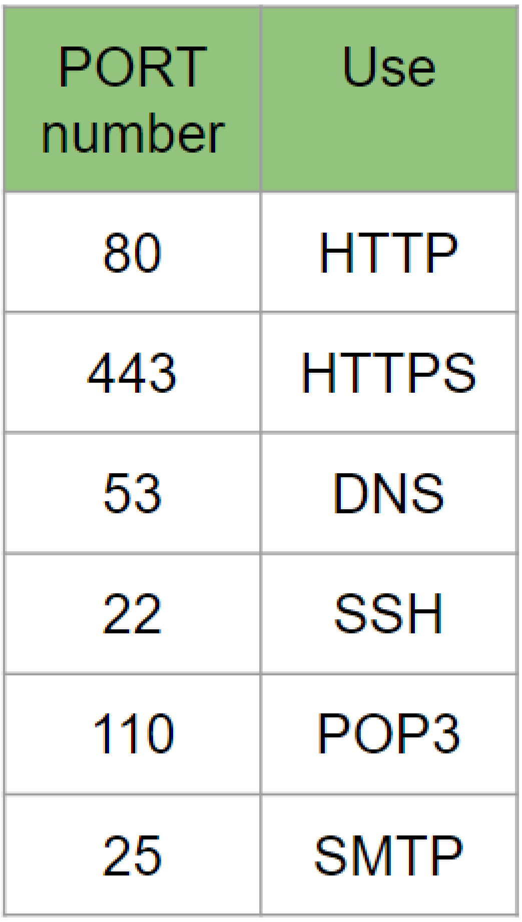
TCP (Transmission Control Protocol), UDP (User Datagram Protocol) and DCCP (Datagram Congestion Control Protocol) are some of the protocols running in the transport layer. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

At sender’s side:
Transport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.
Note: The sender needs to know the port number associated with the receiver’s application. Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

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 reassembling of the segmented data.



Here is a list of few important port numbers and there uses:



PORT number	Use
80	HTTP
443	HTTPS
53	DNS
22	SSH
110	POP3
25	SMTP

Transport Layer has the following responsibilities:

- Process to process delivery - While Data Link Layer requires the MAC address (48 bits address contained inside the Network Interface Card of every host machine) of source-destination hosts to correctly deliver a frame and Network layer requires the IP address for appropriate routing of packets , in a similar way 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.
- End-to-end Connection between hosts - The transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection- orientated protocol which uses a handshake protocol to establish a robust connection between two end- hosts. TCP ensures reliable delivery of messages and is used in various applications. UDP, on the other hand, is a stateless and unreliable protocol which ensures best-effort delivery. It is suitable for the applications which have little concern with flow or error control and requires to send the bulk of data like video conferencing. It is often used in multicasting protocols.

- Multiplexing and Demultiplexing - Multiplexing allows simultaneous use of different applications over a network which is running on a host. The transport layer provides this mechanism which enables us to send packet streams from various applications simultaneously over a network. The transport layer accepts these packets from different processes differentiated by their port numbers and passes them to the network layer after adding proper headers. Similarly, Demultiplexing is required at the receiver side to obtain the data coming from various processes. Transport receives the segments of data from the network layer and delivers it to the appropriate process running on the receiver's machine.
- 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 loss of packets occur. As a result, retransmission of packets from the sources increases the congestion further. In this situation, the Transport layer provides Congestion Control in different ways. It uses open loop congestion control to prevent the congestion and closed loop congestion control to remove the congestion in a network once it occurred. TCP provides AIMD- additive increase multiplicative decrease, leaky bucket technique for congestion control.
- Data integrity and Error correction - Transport layer checks for errors in the messages coming from application layer by using error detection codes, computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.
- Flow control - The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.

Basis	Transmission control protocol (TCP)	User datagram protocol (UDP)
Type of Service	TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn't support Broadcasting.	UDP supports Broadcasting.
Protocols	TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.
Stream Type	The TCP connection is a byte stream.	UDP connection is message stream.
Overhead	Low but higher than UDP.	Very low.

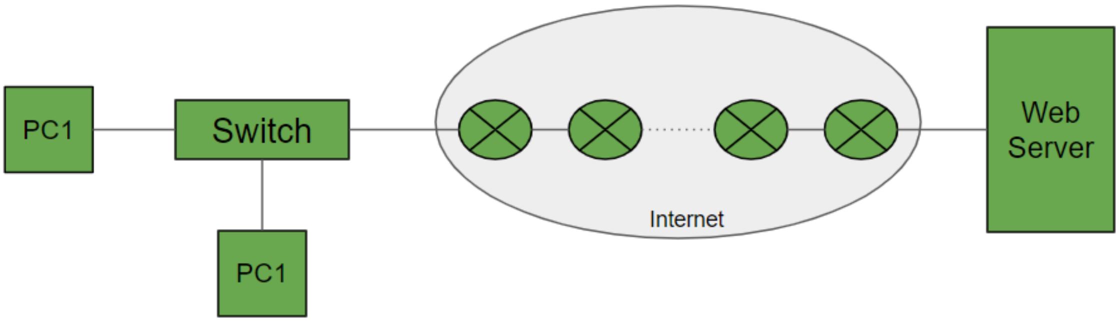
A short example to understand the differences clearly : Suppose there are two houses, H1 and H2 and a letter have to be sent from H1 to H2. But there is a river in between those two houses. Now how can we send the letter?

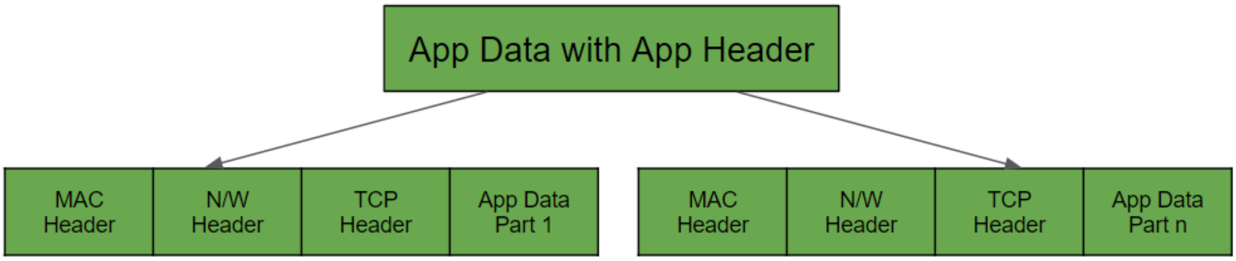
- Solution 1: Make a bridge over the river and then it can be delivered.
- Solution 2: Get it delivered through a pigeon.

Consider the first solution as TCP. A connection has to be made (bridge) to get the data (letter) delivered. The data is reliable because it will directly reach another end without loss in data or error.

And the second solution is UDP. No connection is required for sending the data. The process is fast as compared to TCP, where we need to set up a connection(bridge). But the data is not reliable: we don't know whether the pigeon will go in the right direction, or it will drop the letter on the way, or some issue is encountered in mid-travel.

The application layer is the topmost layer of the OSI Model. It is the layer in which user applications run. Various protocols run at this layer serving different requirements.





When someone browses the internet, then the browser generates Application Data with specific Header files. Following this, the transport layer breaks the Application data into various parts. To this TCP header is added to each part of the Application Data. Next comes the network layer, which adds the destination address in the network header. Then the link is made between the computer and the ISP routers. All the traffic is being sent to the routers. To send the data over the data link layer to any other routers, the computer uses MAC address where the routers MAC address is used to set the link. This MAC address is known using the ARP or Address Resolution Protocol. The switch reads the MAC header of the destination router. The routers laying on the Internet implements three layers namely network layer, DLL, and physical layer. Now finally when the data reached the webserver then using the TCP header, the webserver combines all the data.

- HTTP: Stands for Hyper Text Transfer Protocol. It is a request-response protocol that is used to receive web-pages on a client-server architecture. The client requests for a resource (HTML page, javascript file, images or any other file) to the server. The server returns a response accordingly. It uses TCP as the underlying Transport Layer protocol. HTTP supports the following methods (modes) of requests:

    1. GET - Retrieve information from the server (GET Requests is intended only for data fetching and should not have any side-effect).
    2. HEAD - Retrieve only header (meta-information) and no response-body.
    3. POST - Post/Send data back to the server. e.g. User-data, form-data.
    4. DELETE - Delete the specified resource.
    5. OPTIONS - Returns the list of HTTP methods supported by the server.

Port no. for HTTP: 80 (8080 occasionally)

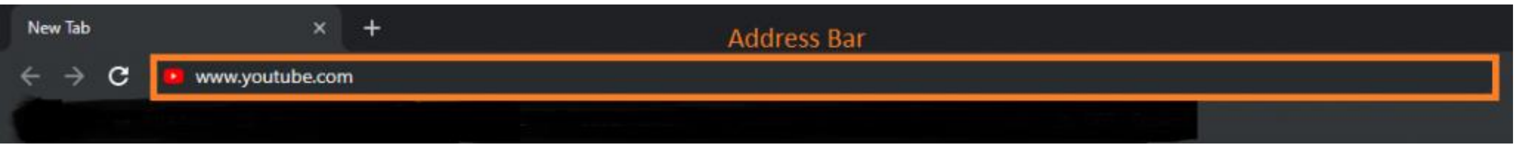
- HTTPS: It is a secured version of HTTP made possible by encrypting the data transferred using TLS (Transport-Layer-Security). Earlier, its predecessor ~ SSL was used. The use of HTTPs over HTTP increases security by preventing eavesdropping, tampering and man-in-the-middle attacks. Port used in HTTPs is the same as that of HTTP. While browsing, remember how website name and then port number etc. is passed?

- TELNET: Stands for TELecommunications NETwork. It is used in terminal emulation, which one can use to access a remote system. It is used for file-access and for the initial setup of switches. One may draw its similarities to SSH (Secure-Shell), but as the name suggests SSH is secure as it uses encryption in addition to normal terminal emulation. Telnet is thus no longer used thanks to SSH. Port no. for Telnet: 23 Port no. for SSH: 22
- FTP: Stands for File Transfer Protocol. It provides reliable and efficient file-transfer between two remote machines. Port no. for FTP Data: 20 Port no. for FTP Control: 21s. WinSCP uses SFTP, remember?
- SMTP: Stands for Simple Mail Transfer Protocol. Uses TCP under the hood. Using a process called "store and forward," SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. Port no. for SMTP: 25.
- DNS: Stands for Domain Name Service. DNS maps human-addressable English domain names to IP addresses. www.abc.com might translate to 198.105.232.4. We as humans are comfortable in dealing with named addresses of websites (facebook.com, google.com etc.). However, to uniquely identify the server hosting the application, numeric IP addresses are required by the machine. DNS servers contain this mapping of named addresses to IP addresses. Whenever we us a named address is used, client machine services a request to the DNS server to fetch the IP address. Port no. for DNS: 53
- DHCP: Stands for Dynamic Host Configuration Protocol. Used for dynamic addressing of devices in a network. DHCP server keeps a pool of available IP addresses. Whenever a new device joins the network, it provides it with an IP from the available pool with an expiration time. DHCP is required in place of static addresses because current requirements involve managing devices which are continuously leaving/joining a network. Thus, a pool of available addresses is required which can be leased to devices currently residing in the network. Port no. for DHCP: 67, 68

We shall cover the whole walkthrough of what happens step-by-step starting from entering an URL on the address bar of the browser till the loading of the actual webpage.

Entering the URL

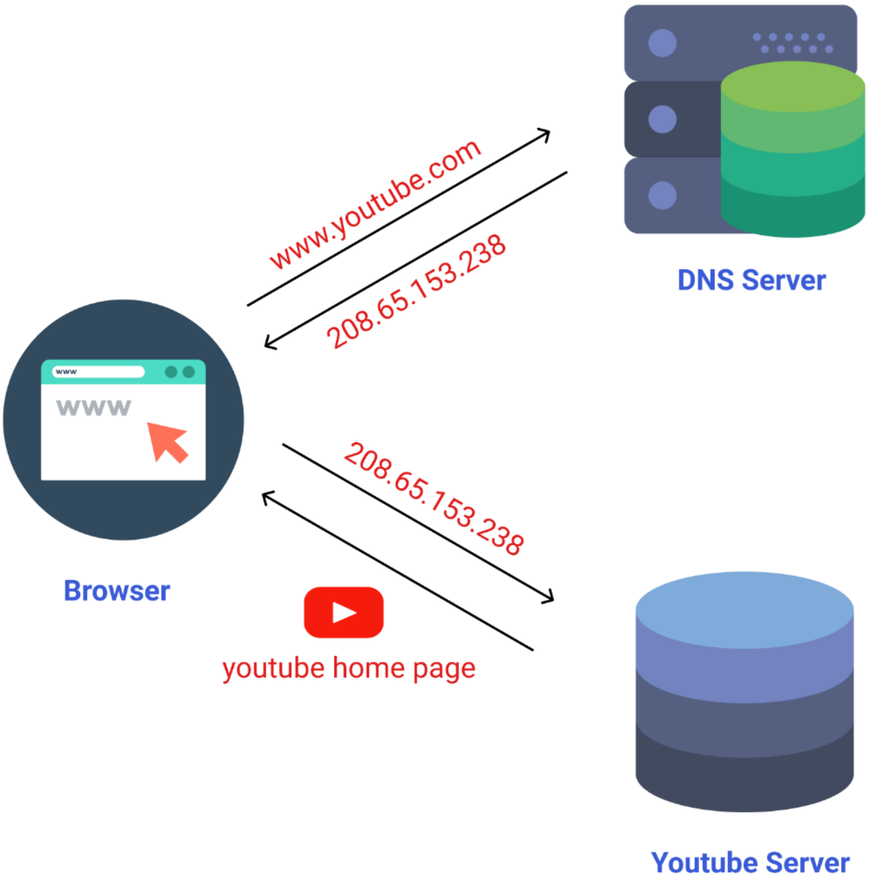
We use browsers to surf the internet (Chrome, Firefox, Edge, etc.). Each of them has an address-bar at the top where we provide the URL of the website we want to visit -



[redacted]

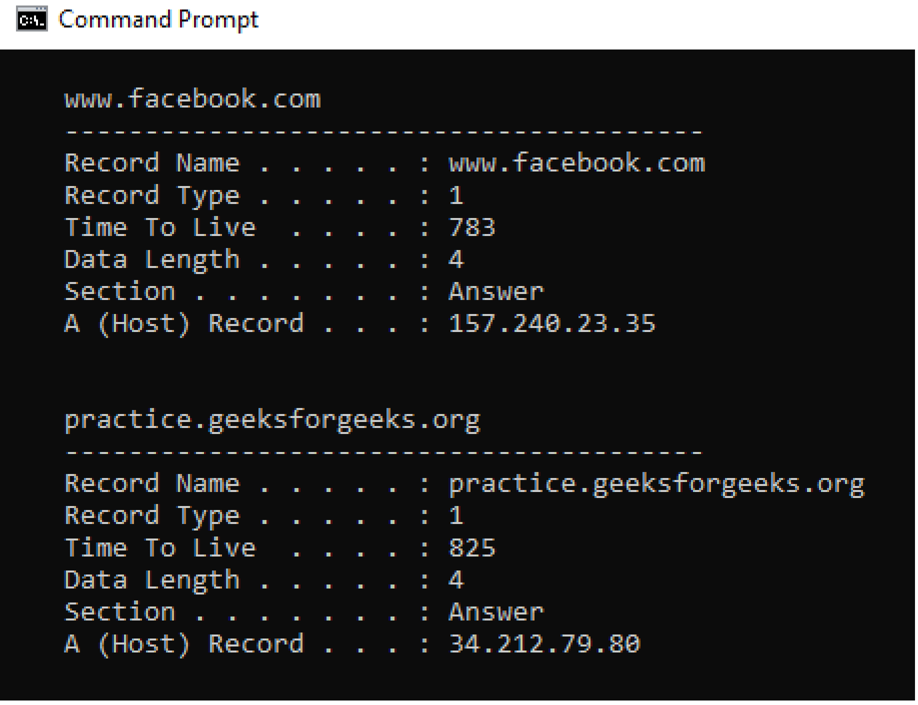
We enter some URL, say www.google.com or youtube.com as an example and press Enter. After waiting for a while, we are presented with the landing pages of the website. But we all know Computer Systems can't understand human-language addresses. Also, human-language addresses have many issues such as (uppercase/lowercase, etc.). We have IP addresses (IPv4/IPv6) as the numerical equivalent for addressing in the realm of computer networks. An IP address is unique to a particular system at a time. i.e. A system running currently can't have multiple IP addresses ~ providing us the best scheme for addressing systems present in the network.

However, humans are not good with memorizing numbers (IPs) for websites, so the usage of English-language addresses can't be eliminated. Thus, we require some mechanism to map the English-language addresses to numeric IP addresses. Here, comes the role of DNS, which we cover in the next section. As of now, all we need to know is whenever we type an English-language address, the system calls the DNS server with the URL to get the corresponding IP address. Only, after the browser receives the IP, it can request the actual server for the webpage. The process looks as -



DNS Lookup

DNS calls are an extra overhead which serves us no good in loading the actual website. Thus, it would be very beneficial if we can cache DNS IP values for frequently visited websites in the user-system itself. Thus, comes the concept of DNS caching. Before making a call to the actual DNS server, the browser looks up the DNS cache of the system. The DNS cache looks as –



```
    www.facebook.com
    ----------------------------------------
    Record Name . . . . . : www.facebook.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 783
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 157.240.23.35


    practice.geeksforgeeks.org
    ----------------------------------------
    Record Name . . . . . : practice.geeksforgeeks.org
    Record Type . . . . . : 1
    Time To Live  . . . . : 825
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 34.212.79.80
```

We can display the DNS cache information in Windows CMD as -

```bash
ipconfig /displaydns
```

If no entry in Cache is found, then we call the DNS server. DNS server IP is either provided by the ISP, or there are public DNS servers provided by Google (8.8.8.8/8.8.4.4) or OpenDNS (208.67.222.222/208.67.220.220). These settings can be set/adjusted in Network Settings of the system. The system performs a DNS call with the address provided. The type of packets used is generally UDP because we require a lot of DNS calls and UDP packets are smaller in size (max. 512 bytes) as compared to TCP. Also, DNS requests are done on a separate port no. ~ 53.

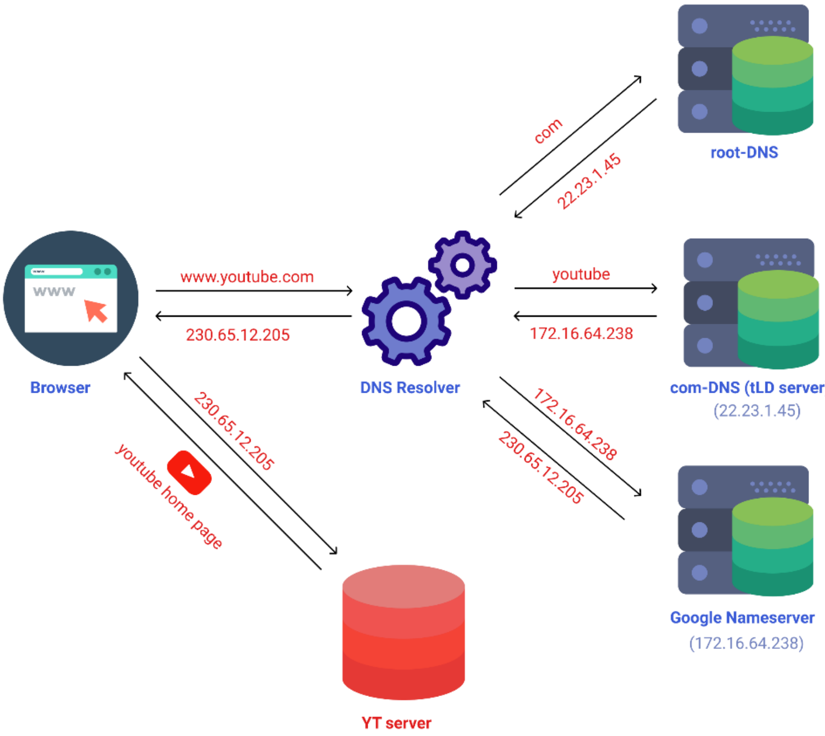
DNS Resolution

We shall understand this with an example. Say we search www.youtube.com. DNS resolution occurs from end to start of the address. i.e. for our query, com -> youtube -> www . THe DNS resolver first requests the root-DNS with com as the search query.

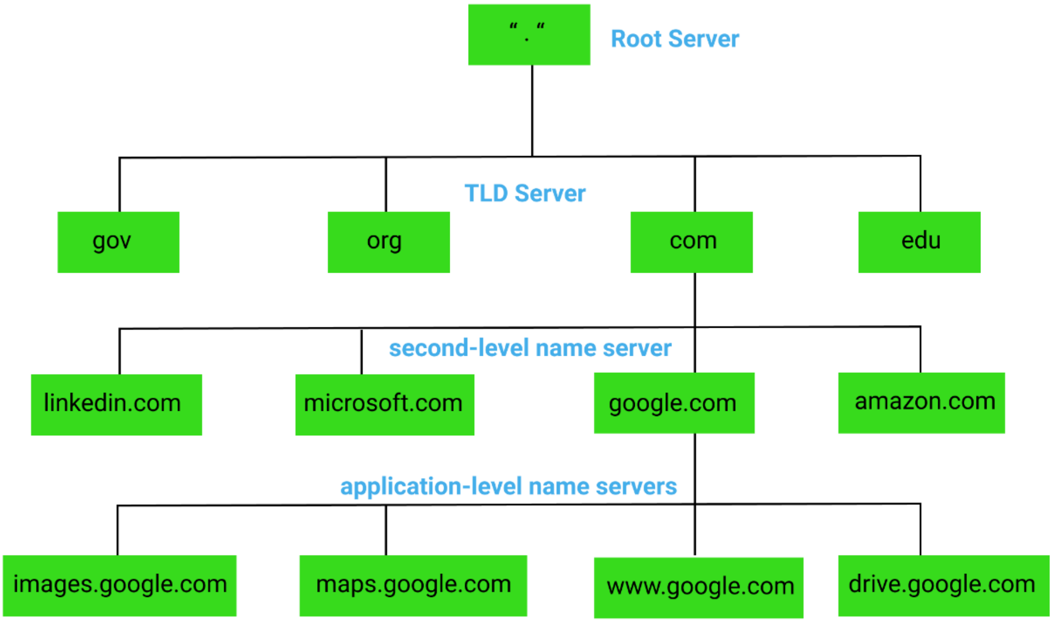
What is the root-DNS Server?
Root-DNS is the topmost level DNS server which contains the addresses of tLD (top-level-domain) name-servers such as com, org, gov. We have queried .com, so it returns the address of .com tLD server.

We thereafter query the .com-tLD server with the request for youtube. This name server looks up into its database and other similar tLDs and returns back the list of name servers matching youtube. Youtube is owned by Google, so we are returned name server list ns1.google.com-ns4.google.com.

We then query one of these Google name servers for youtube, and we get back the IP address for the website which is geographically closest to our location. (Nowadays, the same website is hosted in a distributed fashion over multiple regions). Diagrammatically -



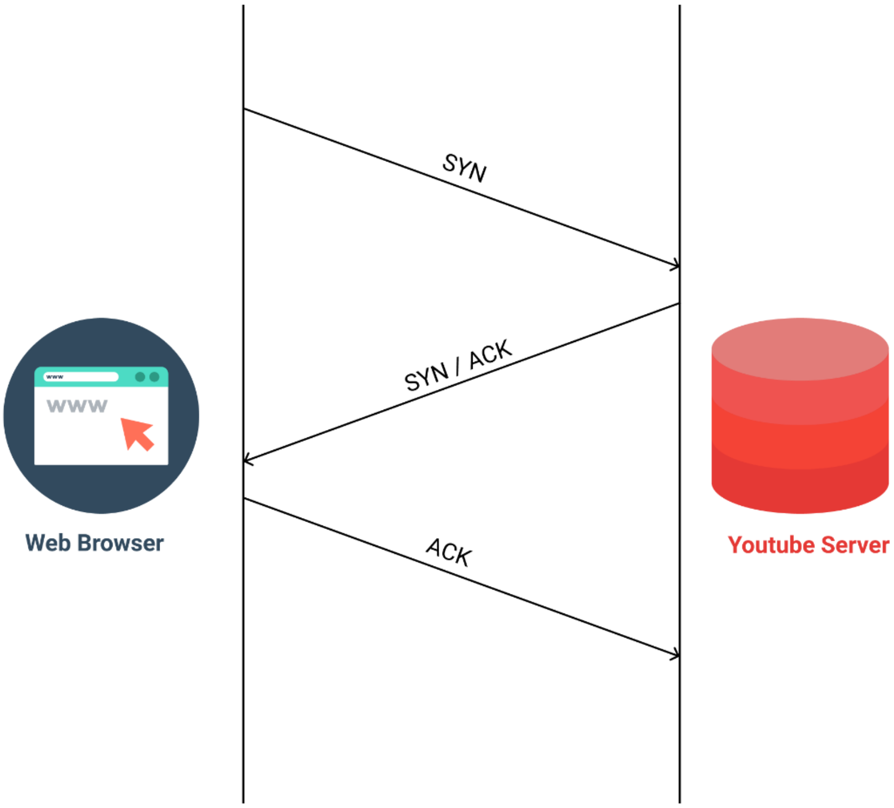
NOTE - All the IP addresses shown in the image is just for illustration. They are by no means accurate to the example discussed.



Above diagram shows the hierarchy of DNS servers and the various levels of resolution. After the browser receives the correct IP address for the requested website, it establishes a TCP connection which we describe below -

TCP Connection & HTTP Request

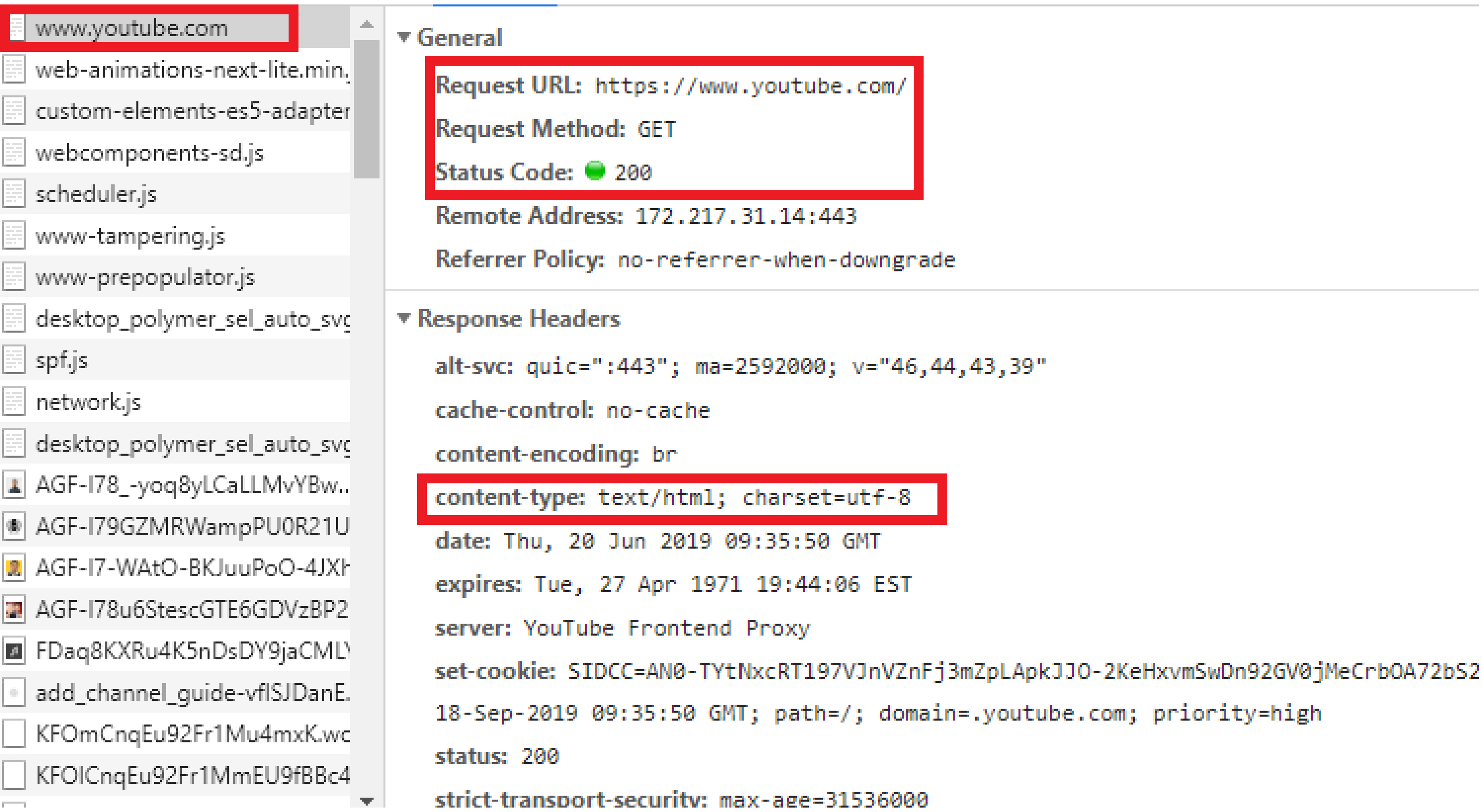
Establishing a TCP connection is a 3-way handshake process which is described in the figure shown below -



The client sends a SYN packet to the Youtube server to check whether it can accommodate any new connections or not. The server replies with a SYN/ACK (acknowledgment to the SYN request) back to the client. The client completes the 3-way handshake process by replying with its own acknowledgment (ACK).

Website & Resource Delivery

After client and server are successfully connected via a secure TCP connection, browser issues an HTTP Request to the server demanding it to serve the page requested by the user. The server responds with an HTTP Response (the HTML page containing images, links to videos and other relevant data ~ JSON data perhaps) back to the client. The browser application then renders the source files received onto the user screen as a webpage.



```
www.youtube.com
web-animations-next-lite.min.
custom-elements-es5-adapter
webcomponents-sd.js
scheduler.js
www-tampering.js
www-prepopulator.js
desktop_polymer_sel_auto_svg
spf.js
network.js
desktop_polymer_sel_auto_svg
AGF-I78_-yoq8yLCaLLMvYBw..
AGF-I79GZMRWampPU0R21U
AGF-I7-WAtO-BKJuuPoO-4JXH
AGF-I78u6StescGTE6GDVzBP2
FDaq8KXRu4K5nDsDY9jaCML
add_channel_guide-vflSJDanE.
KFOmCnqEu92Fr1Mu4mxK.wo
KFOlCnqEu92Fr1MmEU9fBBc4
```

```
▼ General
  Request URL: https://www.youtube.com/
  Request Method: GET
  Status Code: ● 200
  Remote Address: 172.217.31.14:443
  Referrer Policy: no-referrer-when-downgrade

▼ Response Headers
  alt-svc: quic=":443"; ma=2592000; v="46,44,43,39"
  cache-control: no-cache
  content-encoding: br
  content-type: text/html; charset=utf-8
  date: Thu, 20 Jun 2019 09:35:50 GMT
  expires: Tue, 27 Apr 1971 19:44:06 EST
  server: YouTube Frontend Proxy
  set-cookie: SIDCC=AN0-TYtNxcRT197VJnVZnFj3mZpLApkJJO-2KeHxvmSwDn92GV0jMeCrbOA72bS2
  18-Sep-2019 09:35:50 GMT; path=/; domain=.youtube.com; priority=high
  status: 200
  strict-transport-security: max-age=31536000
```

Sub-URL Resolution

What happens when we access, say geeksforgeeks.org/data-strucure-and-algorithms/ or geeksforgeeks.org/users/. i.e. The issue we are trying to tackle here is how the part after the main URL gets resolved once we hit the main server for the website. This issue has been handled in 2 different ways, the 1st one of which has gone obsolete (the reason we discuss why) -

1. Seperate HTML files - In both the implementations, we are required to have one root file named index.html. We should have to keep the name as same, as this is the 1st webpage which is required to be served once HTTP request hits the server. It is the root/landing page in case a sub-URL is not specified. i.e. say we access http://abc.com/, then index.html present in the abc server will get served. Instead, if we access say http://abc.com/feed.html, then the server looks for feed.html file present in the directory and serves that to the client browser. Similarly, http://abc.com/profile.html asks the server to look for profile.html and serve it back. This kind of system relies on the presence of separate HTML files along with other resources (images, js files, CSS files, etc.). Each of them gets served based on the page requested. It is obvious that this kind of system won't scale. Imagine having a profile of millions of users. Then we would have to keep separate files like abc.com/profile/levi.html, abc.com/profile/eren.html, abc.com/profile/erwin.html

2. Single Bundle File with API end-points - Modern systems have a single JS bundle file which contains the basic HTML structure to load in-case each URL is requested. Whenever we request a website, the whole bundle is downloaded into the user system. Accordingly, when we browse to different web-pages, API calls are made and the response data is injected into the HTML template (served by the bundle). Understanding this requires good knowledge of modern front-end frameworks (such as React, Angular, etc.) and REST-API backend frameworks (Nodejs, Django, etc.). Hence, it is out of the scope of this article to explain the overall mechanism in detail.

ICMP is L3 protocol which uses IPv4 and used for network diagnostic. DNS doesn't use ICMP.

In a computer network, we have 2 addresses associated with a device (physical & logical). Physical Address is permanent and fixed (although can be changed, but shouldn't be done ~ MAC spoofing) for a device and doesn't change if the device changes network.

Logical Addresses (IP) is transient and changes once device leaves current network and joins another. To finally transmit data from one device to another, however physical/MAC address is required (at Data-Link-layer). But, all a Network Layer knows is the logical address/IP of the next-hop-device.

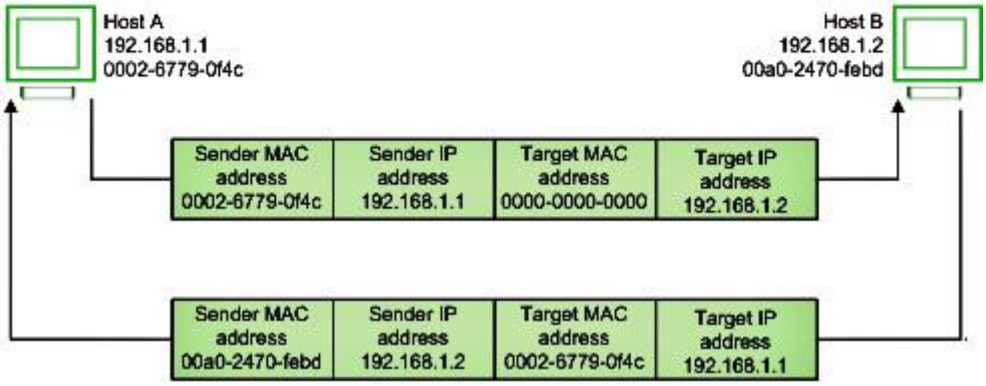
ARP (Address-Resolution-Protocol) is the de-facto method of acquiring the physical address of next-hop from its logical address. Similarly, Reverse-ARP is the process of getting the IP address from the device's physical address.

ARP

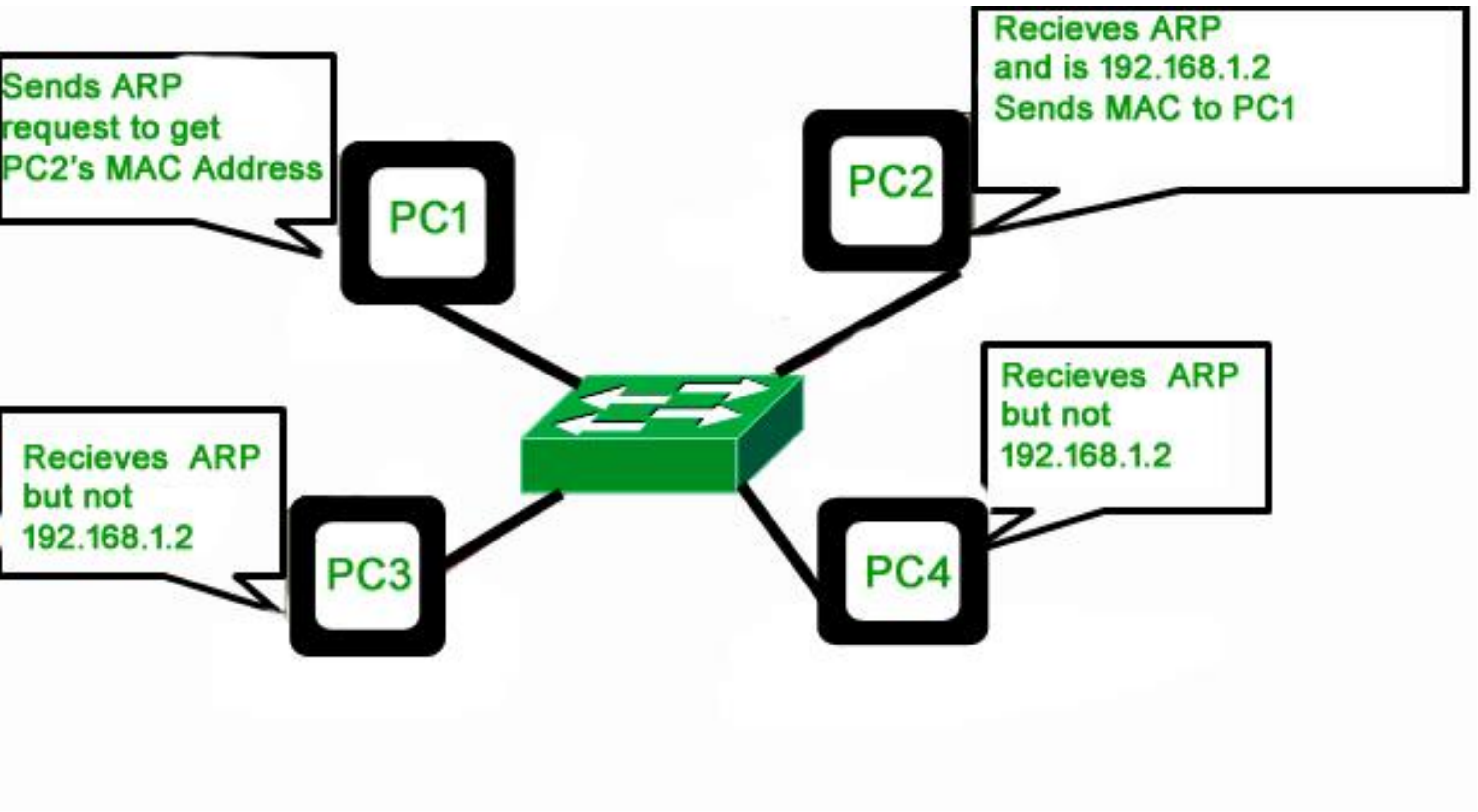
To get the MAC address of the target machine, the sender broadcasts a special ARP-message over it's immediate neighbors, requesting the MAC address. The contents of this message are:

- Sender IP address
- Sender MAC address
- Destinaton MAC address (filled as all 0s initially)
- Destination IP addresss

Upon reception of this ARP message, the device associated with the destination IP, fills it's MAC address into the destination MAC space (filled with 0s), and unicasts it to the sender (Sender MAC is provided for this purpose). All other machines simply ignore the request. Finally, the sender recieves the reply and gets to know the destination MAC address.



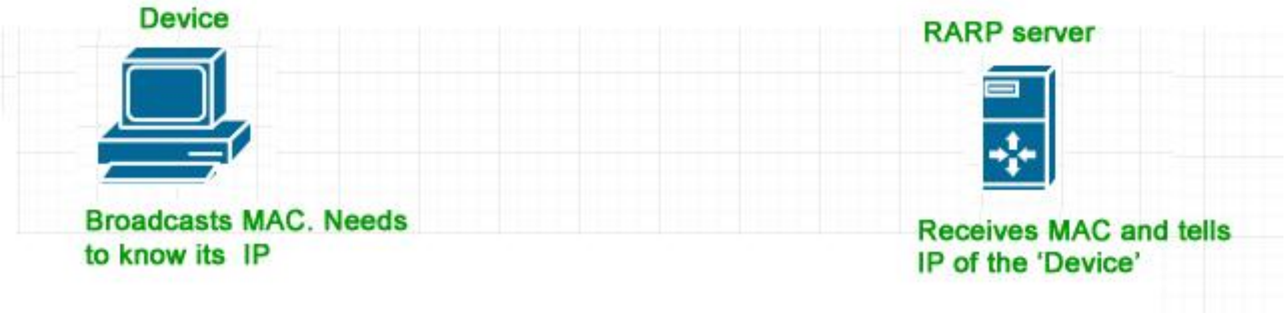
Sender MAC address	Sender IP address	Target MAC address	Target IP address
0002-6779-0f4c	192.168.1.1	0000-0000-0000	192.168.1.2
00a0-2470-febd	192.168.1.2	0002-6779-0f4c	192.168.1.1


Sends ARP request to get PC2's MAC Address
PC1
Recieves ARP and is 192.168.1.2 Sends MAC to PC1
PC2
Recieves ARP but not 192.168.1.2
PC3
Recieves ARP but not 192.168.1.2
PC4

Reverse ARP

Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.

When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.


Device
RARP server
Broadcasts MAC. Needs to know its IP
Receives MAC and tells IP of the 'Device'

A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.

Dynamic Host Configuration Protocol(DHCP) is an application layer protocol which is used to provide:

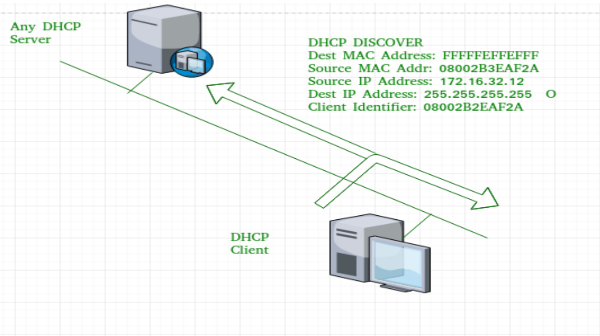
1. Subnet Mask (Option 1 - e.g., 255.255.255.0)
2. Router Address (Option 3 - e.g., 192.168.1.1)
3. DNS Address (Option 6 - e.g., 8.8.8.8)
4. Vendor Class Identifier (Option 43 - e.g., 'unifi' = 192.168.1.9 ##where unifi = controller)

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

DHCP port number for server is 67 and for the client is 68. It is a Client-server protocol which uses UDP services. IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process.

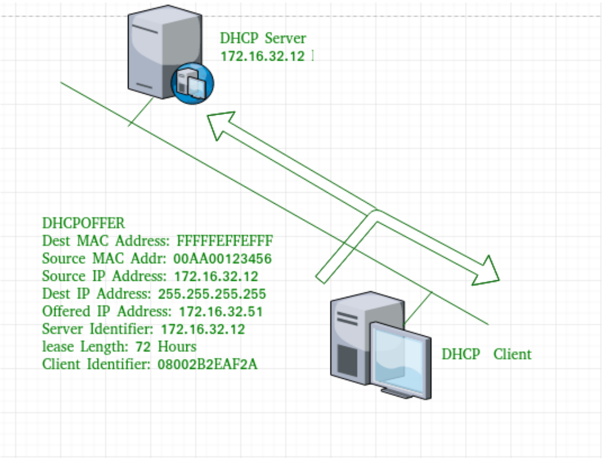
These messages are given as below:

1. DHCP discover message - This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long


Any DHCP Server
DHCP DISCOVER
Dest MAC Address: FFFFFEFFEFFF
Source MAC Addr: 08002B3EAF2A
Source IP Address: 172.16.32.12
Dest IP Address: 255.255.255.255 O
Client Identifier: 08002B2EAF2A
DHCP Client

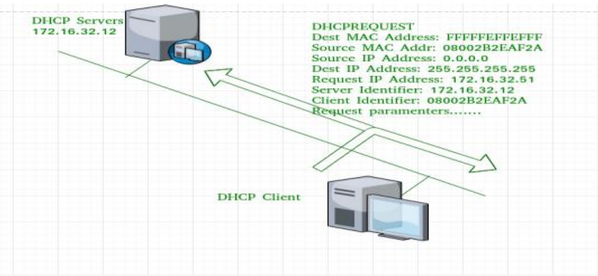
2. As shown in the figure, source MAC address (client PC) is 08002B2EAF2A, destination MAC address(server) is FFFFFFFFFFFF, source IP address is 0.0.0.0(because PC has no IP address till now) and destination IP address is 255.255.255.255 (IP address used for broadcasting). As the discover message is broadcast to find out the DHCP server or servers in the network, therefore, broadcast IP address and MAC address is used.
3. DHCP offer message - The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by the server. Size of the message is 342 bytes. If there are more than

one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also, a server ID is specified in the packet in order to identify the server.


DHCP Server
172.16.32.12
DHCPOFFER
Dest MAC Address: FFFFFEFFEFFF
Source MAC Addr: 00AA00123456
Source IP Address: 172.16.32.12
Dest IP Address: 255.255.255.255
Offered IP Address: 172.16.32.51
Server Identifier: 172.16.32.12
lease Length: 72 Hours
Client Identifier: 08002B2EAF2A
DHCP Client

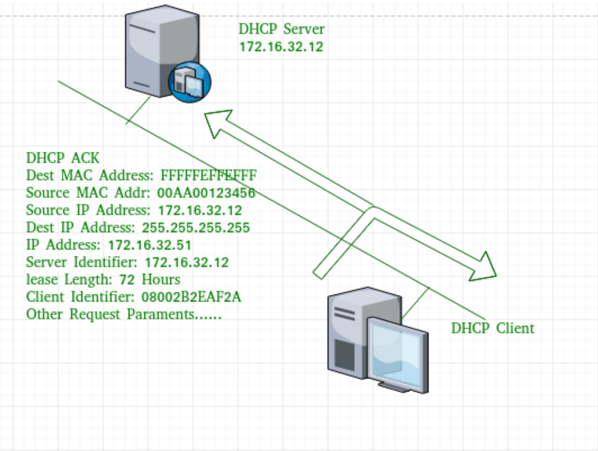
4. Now, for the offer message, source IP address is 172.16.32.12 (server's IP address in the example), destination IP address is 255.255.255.255 (broadcast IP address) ,source MAC address is 00AA00123456, destination MAC address is FFFFFFFFFFFF. Here, the offer message is broadcast by the DHCP server, therefore, destination IP address is broadcast IP address and destination MAC address is FFFFFFFFFFFF and the source IP address is the server IP address and MAC address is server MAC address. Also the server has provided the offered IP address 192.16.32.51 and lease time of 72 hours(after this time the entry of host will be erased from the server automatically) . Also the client identifier is PC MAC address (08002B2EAF2A) for all the messages.

5. DHCP request message - When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address .A Client ID is also added in this message.


DHCP Servers
172.16.32.12
DHCPREQUEST
Dest MAC Address: FFFFFEFFEFFF
Source MAC Addr: 08002B2EAF2A
Source IP Address: 0.0.0.0
Dest IP Address: 255.255.255.255
Request IP Address: 172.16.32.51
Server Identifier: 172.16.32.12
Client Identifier: 08002B2EAF2A
Request paramenters.......
DHCP Client

6. Now, the request message is broadcast by the client PC therefore source IP address is 0.0.0.0(as the client has no IP right now) and destination IP address is 255.255.255.255 (broadcast IP address) and source MAC address is 08002B2EAF2A (PC MAC address) and destination MAC address is FFFFFFFFFFFF. Note - This message is broadcast after the ARP request broadcast by the PC to find out whether any other host is not using that offered IP. If there is no reply, then the client host broadcast the DHCP request message for the server showing the acceptance of IP address and Other TCP/IP Configuration.

7. DHCP acknowledgement message - In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.


DHCP Server
172.16.32.12
DHCP ACK
Dest MAC Address: FFFFFEFFEFFF
Source MAC Addr: 00AA00123456
Source IP Address: 172.16.32.12
Dest IP Address: 255.255.255.255
IP Address: 172.16.32.51
Server Identifier: 172.16.32.12
lease Length: 72 Hours
Client Identifier: 08002B2EAF2A
Other Request Paraments......
DHCP Client

8. Now the server will make an entry of the client host with the offered IP address and lease time. This IP address will not be provided by server to any other host. The destination MAC address is FFFFFFFFFFFF and the destination IP address is

255.255.255.255 and the source IP address is 172.16.32.12 and the source MAC address is 00AA00123456 (server MAC address).

9. DHCP negative acknowledgement message - Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it send DHCP Nak message to client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.
10. DHCP decline - If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server .When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.
11. DHCP release - A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.
12. DHCP inform - If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the dhcp inform message, DHCP server generates DHCP ack message with local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

Note - All the messages can be unicast also by dhcp relay agent if the server is present in different network.
Advantages - The advantages of using DHCP include:

- centralized management of IP addresses
- ease of adding new clients to a network
- reuse of IP addresses reducing the total number of IP addresses that are required
- simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client

The DHCP protocol gives the network administrator a method to configure the network from a centralised area.
With the help of DHCP, easy handling of new users and reuse of IP address can be achieved.

Disadvantages - Disadvantage of using DHCP is:

- IP conflict can occur