UNIT IV

Network layer: Internet Protocol

Network Layer Introduction

Layer-3 in the OSI model is called Network layer. Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking.

Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

Layer-3 Functionalities

Devices which work on Network Layer mainly focus on routing. Routing may include various tasks aimed to achieve a single goal. These can be:

- Addressing devices and networks.
- Populating routing tables or static routes.
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- Internetworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provides connection oriented and connection less mechanism.

Network Layer Features

With its standard functionalities, Layer 3 can provide various features as:

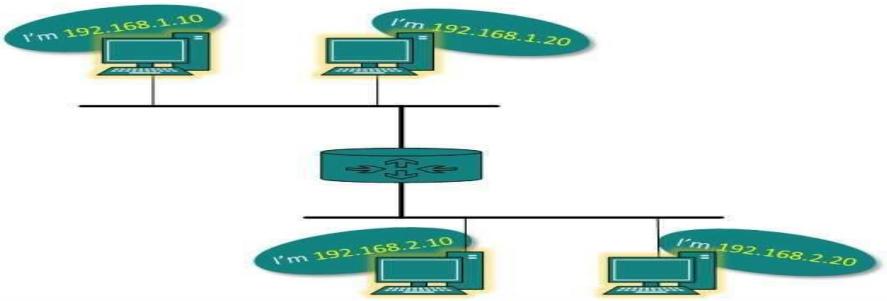
- Quality of service management
- Load balancing and link management
- Security
- Interrelation of different protocols and subnets with different schema.
- Different logical network design over the physical network design.
- L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

A network address always points to host / node / server or it can represent a whole network. Network address is always configured on network interface card and is generally mapped by system with the MAC address (hardware address or layer-2 address) of the machine for Layer-2 communication.

There are different kinds of network addresses in existence:

- IP
- IPX
- AppleTalk

We are discussing IP here as it is the only one we use in practice these days.



IP addressing provides mechanism to differentiate between hosts and network. Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network. The host which needs to communicate outside its subnet, needs to know destination network address, where the packet/data is to be sent.

Every computer in a network has an IP address by which it can be uniquely identified and addressed. An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time and another IP at some different time.

THE INTERNET PROTOCOL (IP)

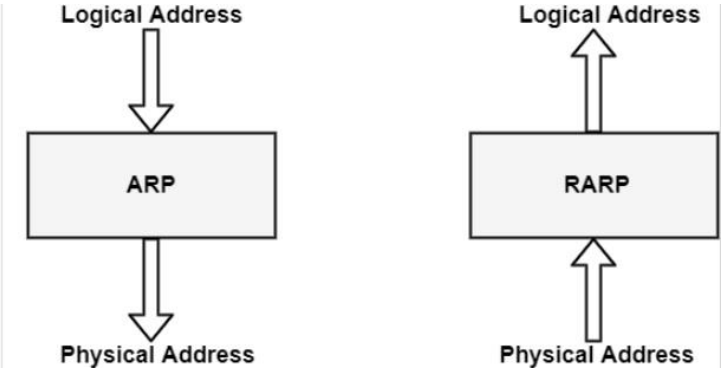
The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.
Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP. The most common transport protocols are TCP and UDP.

ADDRESS RESOLUTION PROTOCOL(ARP)

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.

Address Resolution Protocol (ARP) is a network-specific standard protocol. The Address Resolution Protocol is important for changing the higher-level protocol address (IP addresses) to physical network addresses. It is described in RFC 826.



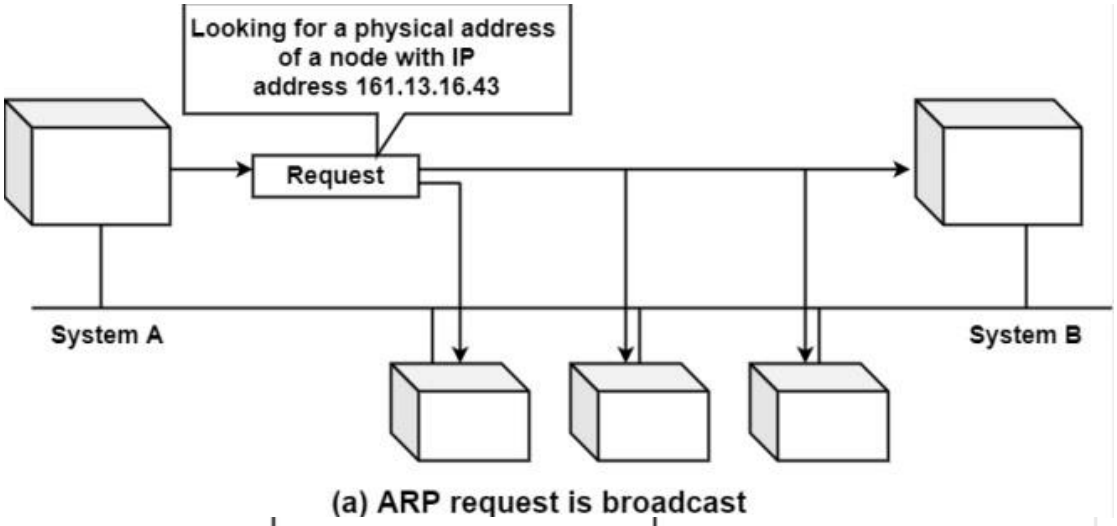
ARP relates an IP address with the physical address. On a typical physical network such as LAN, each device on a link is identified by a physical address, usually printed on the network interface card (NIC). A physical address can be changed easily when NIC on a particular machine fails.

The IP Address cannot be changed. ARP can find the physical address of the node when its internet address is known. ARP provides a dynamic mapping from an IP address to the corresponding hardware address.

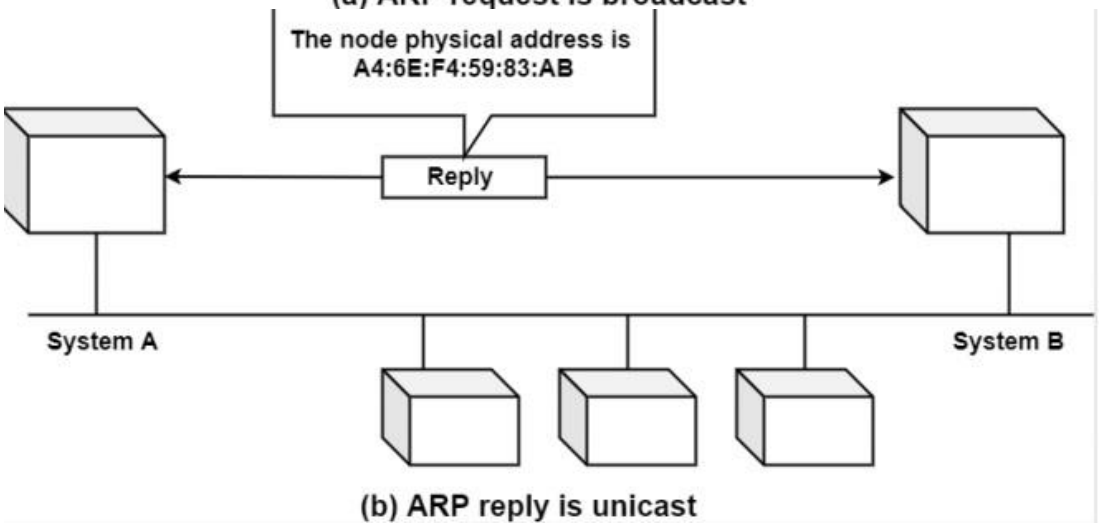
When one host wants to communicate with another host on the network, it needs to resolve the IP address of each host to the host's hardware address.

This process is as follows−

- When a host tries to interact with another host, an ARP request is initiated. If the IP address is for the local network, the source host checks its ARP cache to find out the hardware address of the destination computer.
- If the correspondence hardware address is not found, ARP broadcasts the request to all the local hosts.
- All hosts receive the broadcast and check their own IP address. If no match is discovered, the request is ignored.
- The destination host that finds the matching IP address sends an ARP reply to the source host along with its hardware address, thus establishing the communication. The ARP cache is then updated with the hardware address of the destination host.

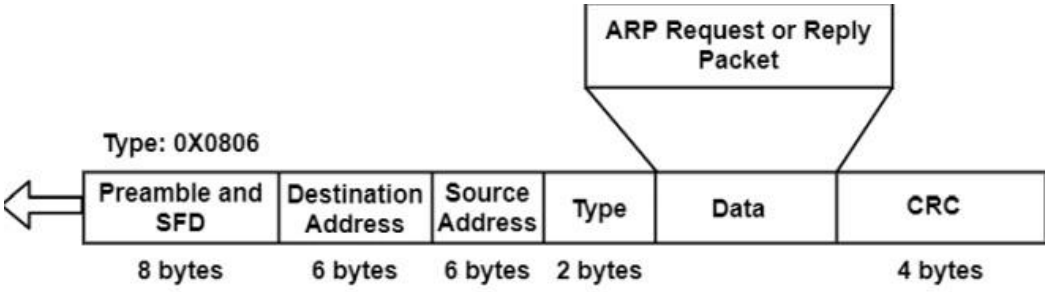


(a) ARP request is broadcast



(b) ARP reply is unicast

.



Encapsulation of ARP Packet

ARP Packet Generation

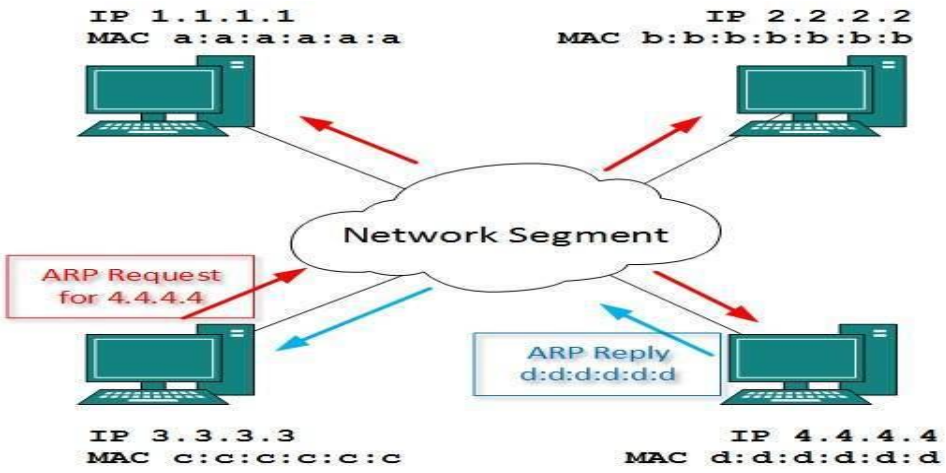
If an application needs to send information to a specific IP destination address, the IP routing structure first determines the IP address of the next-hop of the packet (it should be the destination host itself or a router) and the hardware tool on which it should be transmitted.

If it is an IEEE 802.3/4/5 network, the ARP structure should be considered to design the <protocol type target protocol address> to a physical address.

The ARP module attempts to find the address in this ARP cache. If it is to find the connecting pair, it provides the equivalent 48-bit physical location back to the caller (the device driver), which then shares the packet.

If it does not discover the pair in its table, it removes the packet (the assumption is that a higher-level protocol will resend) and creates a network broadcast of an ARP request.

- **Hardware address space:** It specifies the type of hardware such as Ethernet or Packet Radio net.
- **Protocol address space:** It specifies the type of protocol, same as the Ether type field in the IEEE 802 header (IP or ARP).
- **Hardware Address Length:** It determines the length (in bytes) of the hardware addresses in this packet. For IEEE 802.3 and IEEE 802.5, this is 6.
- **Protocol Address Length:** It specifies the length (in bytes) of the protocol addresses in this packet. For IP, this is 4 byte.
- **Operation Code:** It specifies whether this is an ARP request (1) or reply (2).
- **Source/target hardware address:** It contains the physical network hardware addresses. For IEEE 802.3, these are 48-bit addresses.
- For the ARP request packet, the target hardware address is the only undefined field in the packet.



To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, “Who has this IP address?” Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP. ICMP contains dozens of diagnostic and error reporting messages.

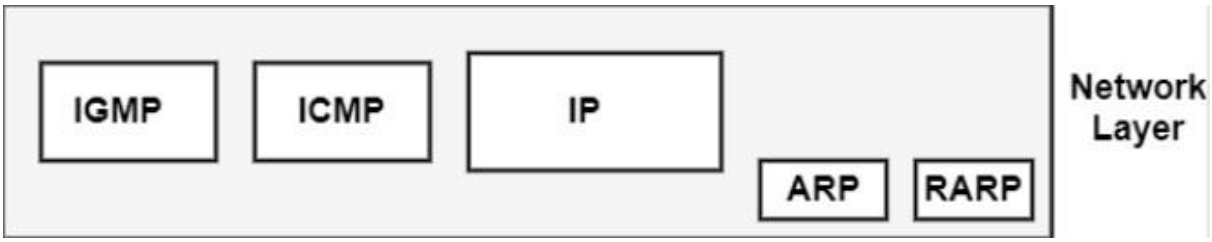
ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.

The ICMP represents Internet Control Message Protocol. It is a network layer protocol. It can be used for error handling in the network layer, and it is generally used on network devices, including routers. IP Protocol is a best-effect delivery service that delivers a datagram from its original source to its final destination. It has two deficiencies−

- Lack of Error Control
- Lack of assistance mechanisms

IP protocol also lacks a structure for host and management queries. A host needs to resolve if a router or another host is alive, and sometimes a network manager needs information from another host or router.

ICMP has been created to compensate for these deficiencies. It is a partner to the IP protocol.



ICMP is a network layer protocol. But, its messages are not passed directly to the data link layer. Instead, the messages are first encapsulated inside the IP datagrams before going to the lower layer.

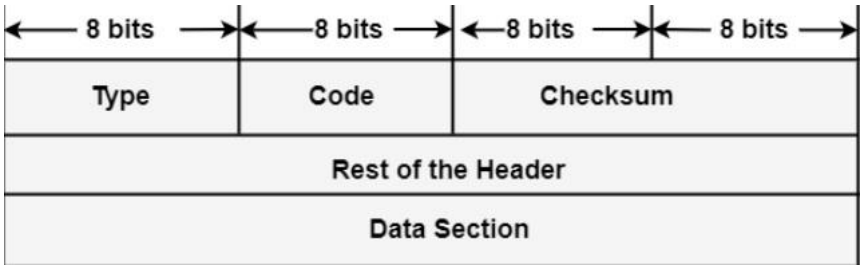
The cost of the protocol field in the IP datagram is I, to indicate that IP data is an ICMP message.

The error reporting messages report issues that a router or a host (destination) may encounter when it phases an IP packet.

The query messages, which appear in pairs, help a host or a network manager to get specific data from a router or another host.

ICMP Message Format

AN ICMP message includes an 8-byte header and a variable size data format.



- **Type:** It is an 8-bit field. It represents the ICMP message type. The values area from 0 to 127 are described for ICMPv6, and the values from 128 to 255 are the data messages.
- **Code:** It is an 8-bit field that represents the subtype of the ICMP message.
- **Checksum:** It is a 16-bit field to recognize whether the error exists in the message or not.

INTERNET PROTOCOL VERSION 4 (IPV4)

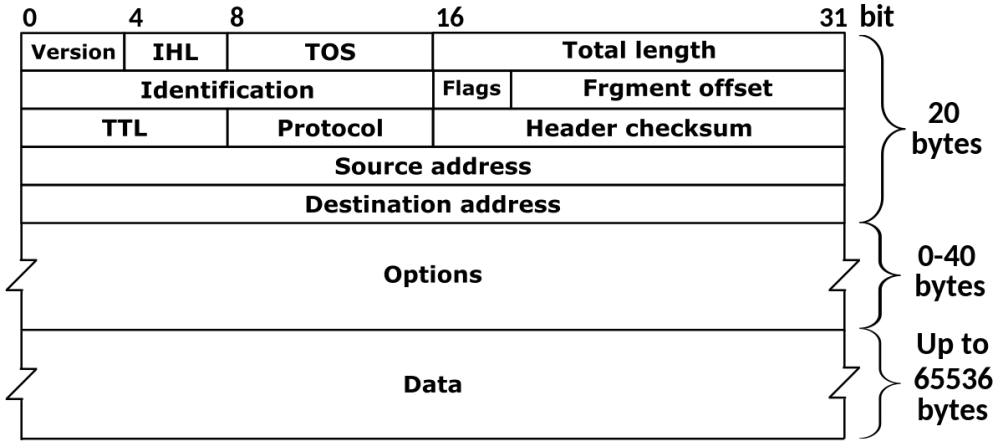
IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A** - it uses first octet for network addresses and last three octets for host addressing
- **Class B** - it uses first two octets for network addresses and last two for host addressing
- **Class C** - it uses first three octets for network addresses and last one for host addressing
- **Class D** - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E** - It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.



Parts of IPv4

- **Network part:**
  The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
- **Host Part:**
  The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.
- For each host on the network, the network part is the same, however, the host half must vary.
- **Subnet number:**
  This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields is twelve and the length of the header field is twenty.
- It has Unicast, broadcast, and multicast style of addresses.

- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

Advantages of IPv4

- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.
- IPV4 addresses are redefined and permit flawless encoding.
- Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
- Data communication across the network becomes a lot of specific in multicast organizations.
    - Limits net growth for existing users and hinders the use of the net for brand new users.
    - Internet Routing is inefficient in IPv4.
    - IPv4 has high System Management prices and it's labor-intensive, complex, slow & frequent to errors.
    - Security features are nonobligatory.
    - Difficult to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.

INTERNET PROTOCOL VERSION 6 (IPV6)

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

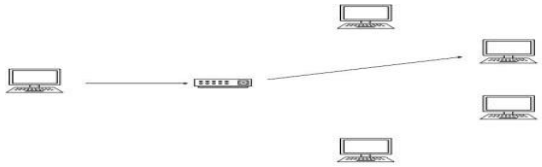
IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4.

- Dual stack implementation
- Tunneling
- NAT-PT

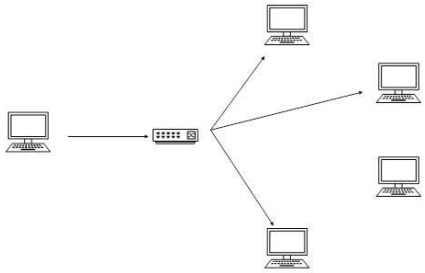
Unicast

In unicast mode of addressing, an IPv6 interface (host) is uniquely identified in a network segment. The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment.When a network switch or a router receives a unicast IP packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host.



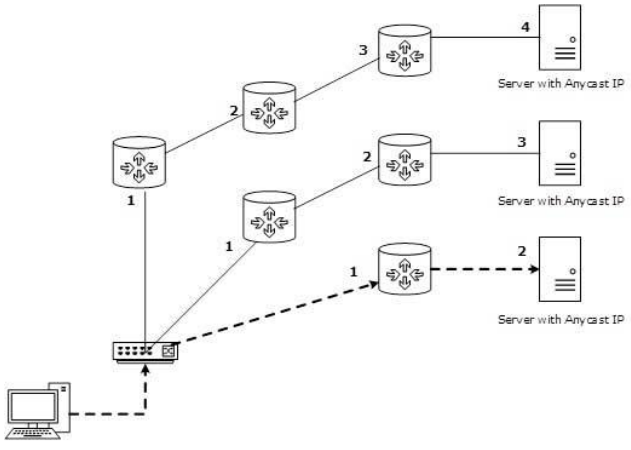
Multicast

The IPv6 multicast mode is same as that of IPv4. The packet destined to multiple hosts is sent on a special multicast address. All the hosts interested in that multicast information, need to join that multicast group first. All the interfaces that joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.



Anycast

IPv6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message. With the help of complex routing mechanism, that Unicast message is delivered to the host closest to the Sender in terms of Routing cost.



Let’s take an example of TutorialPoints.com Web Servers, located in all continents. Assume that all the Web Servers are assigned a single IPv6 Anycast IP Address. Now when a user from Europe wants to reach TutorialsPoint.com the DNS points to the server that is physically located in Europe itself. If a user from India tries to reach Tutorialspoint.com, the DNS will then point to the Web Server physically located in Asia. Nearest or Closest terms are used in terms of Routing Cost.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP. DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices. DHCP can be implemented on small local networks, as well as large enterprise networks.

DHCP will assign new IP addresses in each location when devices are moved from place to place, which means network administrators do not have to manually configure each device with a valid IP address or reconfigure the device with a new IP address if it moves to a new location on the network. Versions of DHCP are available for use in IP version 4 (IPv4) and IP version 6 (IPv6).

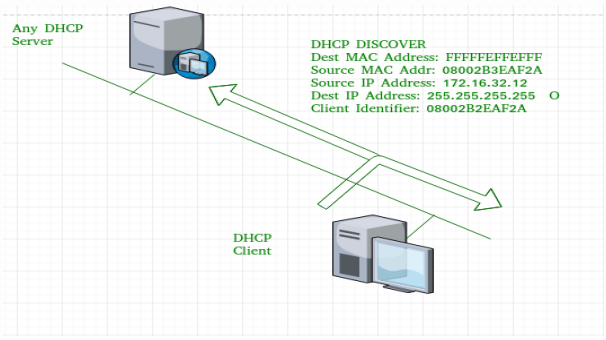
Dynamic Host Configuration Protocol(DHCP) is an application layer protocol which is used to provide:

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.

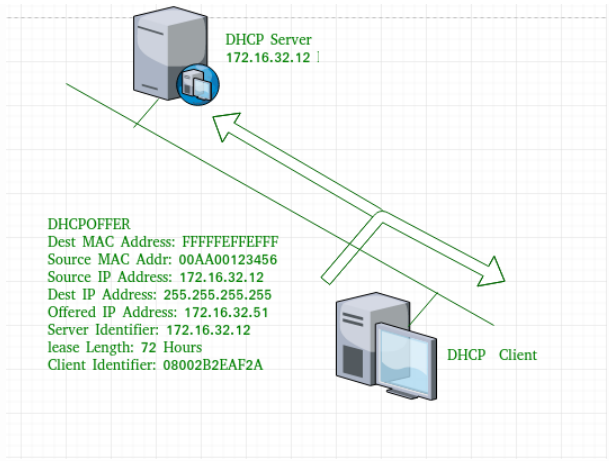
DHCP **port number** for server is 67 and for the client is 68. It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there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



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.

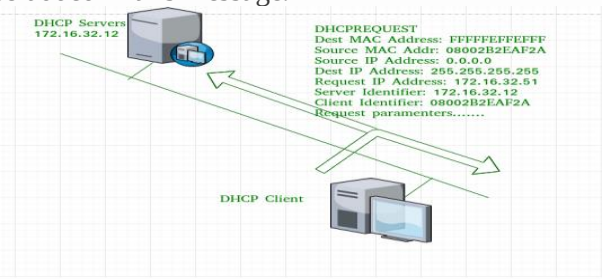
1. **DHCP offer message –**
   The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also a server ID is specified in the packet in order to identify the server.



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 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.

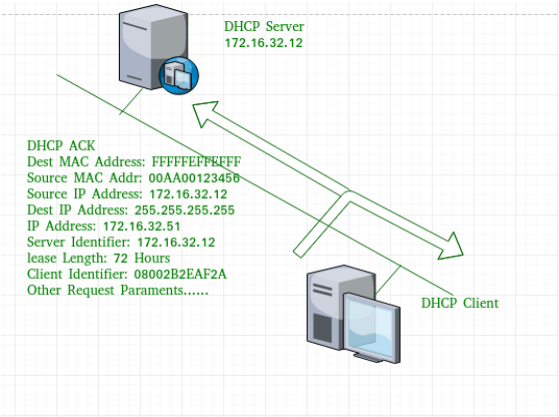
2. **DHCP request message –**
When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratitutous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is 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.



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.

3. **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.



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).

4. **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.
5. **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.
6. **DHCP release –**
   A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.
7. **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.

Advantages

- 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

Disadvantages

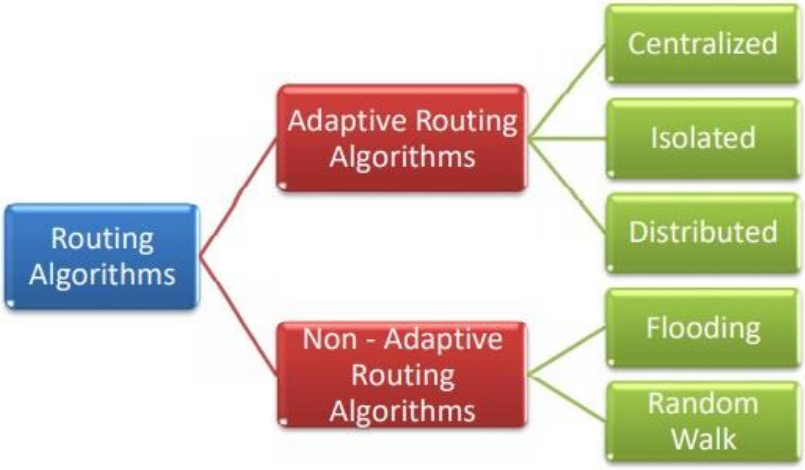
- IP conflict can occur

ROUTING ALGORITHM

A routing algorithm is a procedure that lays down the route or path to transfer data packets from source to the destination. They help in directing Internet traffic efficiently. After a data packet leaves its source, it can choose among the many different paths to reach its destination. Routing algorithm mathematically computes the best path, i.e. “least – cost path” that the packet can be routed through.

Types of Routing Algorithms

Routing algorithms can be broadly categorized into two types, adaptive and nonadaptive routing algorithms. They can be further categorized as shown in the following diagram −



Adaptive Routing Algorithms

Adaptive routing algorithms, also known as dynamic routing algorithms, makes routing decisions dynamically depending on the network conditions. It constructs the routing table depending upon the network traffic and topology. They try to compute the optimized route depending upon the hop count, transit time and distance.

The three popular types of adaptive routing algorithms are −

- **Centralized algorithm** − It finds the least-cost path between source and destination nodes by using global knowledge about the network. So, it is also known as global routing algorithm.
- **Isolated algorithm** − This algorithm procures the routing information by using local information instead of gathering information from other nodes.
- **Distributed algorithm** − This is a decentralized algorithm that computes the least-cost path between source and destination iteratively in a distributed manner.

Non – Adaptive Routing Algorithms

Non-adaptive Routing algorithms, also known as static routing algorithms, construct a static routing table to determine the path through which packets are to be sent. The static routing table is constructed based upon the routing information stored in the routers when the network is booted up.

The two types of non – adaptive routing algorithms are −

- **Flooding** − In flooding, when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on. Flooding may be uncontrolled, controlled or selective flooding.
- **Random walks** − This is a probabilistic algorithm where a data packet is sent by the router to any one of its neighbours randomly.

DISTANCE VECTOR ROUTING

A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors 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 neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
   - It receives a distance vector from a neighbor containing different information than before.
   - It discovers that a link to a neighbor 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

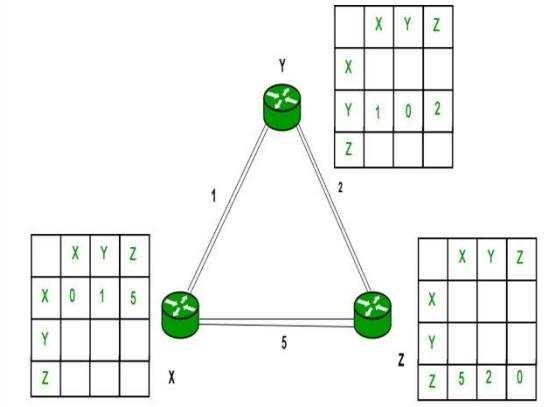
Node x also maintains its neighbors' distance vectors

– 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)} for each node y ∈ N

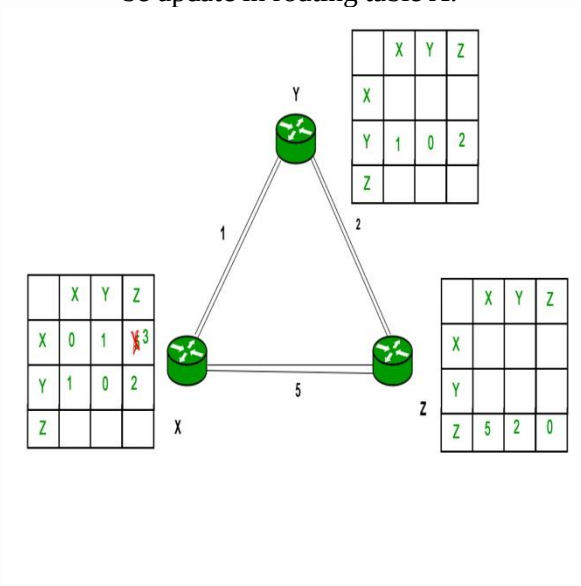
Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



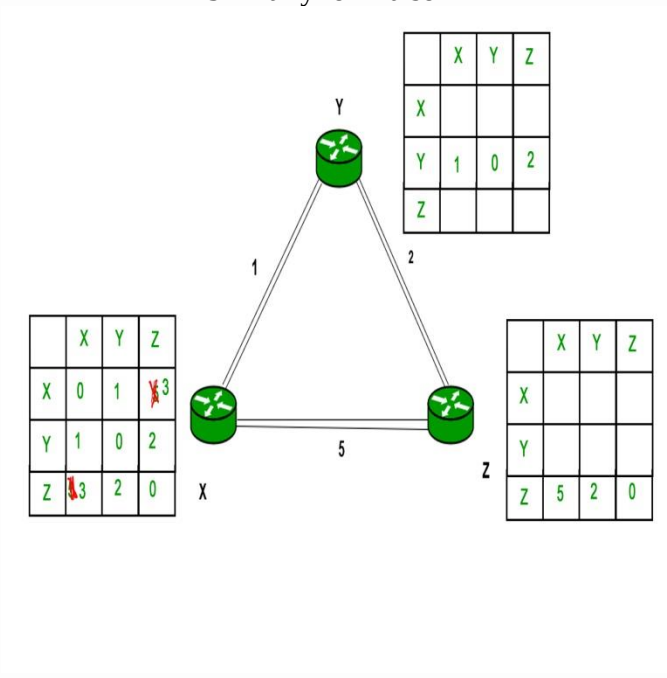
Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

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

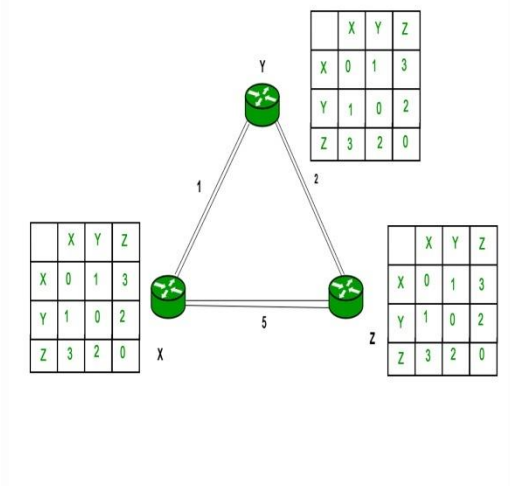
As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.



Similarly for Z also –



Finally the routing table for all –



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.

LINK-STATE ALGORITHM

It is **a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network**. A router sends its information about its neighbors only to all the routers through flooding. Information sharing takes place only whenever there is a change.

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.

Link State Routing –

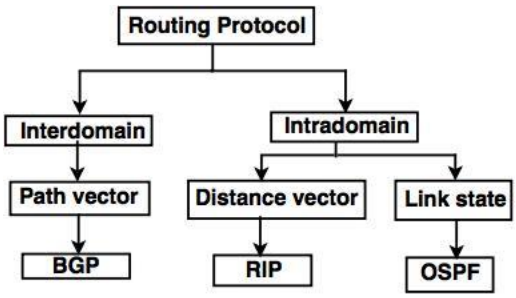
Link state routing is the second family of routing protocols. While distance-vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, 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.

INTER-DOMAIN ROUTING PROTOCOL

Classless inter domain routing (CIDR) is **a way to categorize Internet Protocol (IP) addresses for allocation to hosts and more efficient routing**. CIDR represents the IP address and its subnet mask with a single number.



Classification of routing protocol

THE CONCEPT OF SUBNETTING AND SUPERNETTING

Computer networks can be broken into many networks or small networks can be combined to form large networks depending upon our needs. This is done by **IP subnetting and supernetting**. In this blog, we will learn about these concepts in detail. So, let's get started.

The process of dividing a network into subnetwork is called as subnetting, and the process of combining small networks into a large network is called supernetting. In subnetting, the numbers of bits of network addresses are increased, and in supernetting the number of bits of host addresses is increased. Supernetting is designed to make the routing process more convenient. It reduces the size of routing table information; therefore, it consumes less space in the router's memory. FLSM and VLSM methods are used for subnetting, and for supernetting, CIDR is used.

Subnetting

- Subnetting is a technique that is used to divide the individual physical network into a smaller size called sub-networks. These sub-networks are called a subnet. An internal address is made up of a combination of the small networks segment and host segment. A subnetwork is designed by accepting the bits from the IP address host portion; then, they are uses to assign a number of small-sized sub-networks in the original network.
- In the subnetting process, network bits are converted into host bits. Subnetting process is performed to slow down the depletion of the IP addresses. It allows the administrator to divide the single class A, class B and class C into small segments. Subnetting makes use of VLSM (Variable Length Subnet Mask) and FLSM (Fixed Length Subnet Mask). The process of partitioning the IP address space into a subnet of different size is called a Variable Length

Subnet Mask. VLSM reduces the wastage of memory. The process of partitioning the IP address space into a subnet of the same size is called a Fixed Length Subnet Mask.

Advantages and Disadvantages of Subnetting:

Below are some advantages and disadvantage of subnetting:

Advantages:

- Subnetting increases the number of allowed hosts in the local area network.
- Subnetting decreases the volume of broadcast, hence minimize the number of network traffic.
- Sub networks are easy to maintain and manage.
- Subnetting increases the flexibility of address.
- Network security can be readily employed between sub networks rather than employing it in the whole network.

Disadvantages:

- The process of subnetting is quite expensive.
- To perform subnetting process, we need a trained administrator.

Supernetting

Supernetting is the process that is used to combine several sub networks into a single network. Its process is inverse of the subnetting process. In supernetting, mask bits are moved towards the left of the default mask; network bits are converted into hosts bits. Supernetting is also called router summarization and aggregation. It creates a more number of host addresses at the expense of network addresses. The Internet service provider performs the supernetting process to achieve the most efficient IP address allocation.

It uses the CIDR method, i.e. Classless inter-domain routing method, to route the network traffic across the internet. CIDR combines several sub networks and combined them together for routing network traffic. In other words, we can say that CIDR organizes the IP Addresses in the sub networks independent of the value of the Addresses.

Advantages and Disadvantages of Supernetting:

Below are some advantages and disadvantage of supernetting:

Advantages:

- Supernetting reduces the traffic of the network over the internet.
- Supernetting increases the speed of routing table lookup.
- As it is summarized the number of routing information entries into a single entry, the size of the router's memory table decreased, hence saving the memory space.
- Provision for the router to isolate the topology changes from the other routers.

Disadvantages:

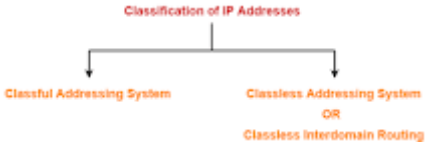
- The combination of blocks should be made in power 2 alternatively; if the three blocks are required, then there must be assigned four blocks.
- While merging several entries into one, it lacks covering different areas.
- The whole network must exist in the same class.

Difference Between Subnetting and Supernetting

- Subnetting divides the whole network into sub networks while supernetting. combines the sub network and merge it as a whole network.
- Subnetting converts the bits of a host to bits of network hence increase the number of network bits, while supernetting converts the bits of a network to bits of the host, hence increase the number of host bits.
- Subnetting reduces the depletion of address, while supernetting increases the routing process.
- Subnetting uses VLSM and FL techniques, while supernetting uses CIDR.
- In subnetting, mask bits are moved towards the right of the default mask, whereas in supernetting, the mask bits are moved towards the left of the default mask.

CLASSLESS ADDRESSING

CIDR or Classless Inter Domain Routing provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.



Classless Addressing is **an improved IP Addressing system**. It makes the allocation of IP Addresses more efficient. It replaces the older classful addressing system based on classes. It is also known as Classless Inter Domain Routing (CIDR).

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

NETWORK ADDRESS TRANSLATION (NAT)

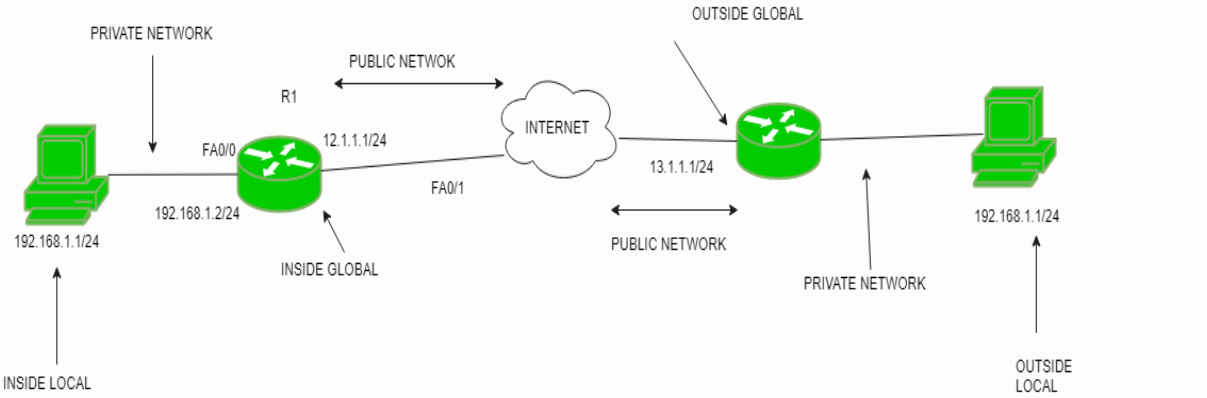
To access Internet, one public IP address is needed but as you use private IP address in our private network, translation of private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global 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 destination. It then makes the corresponding entries of ip address and port number in the NAT table. NAT generally operates on router or firewall.

Network Address Translation (NAT) working –
Generally, the border router is configured for NAT i.e the router which have one interface in local (inside) network and one interface in 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 local (private) IP address.
If NAT run 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 send.

Whymaskportnumbers?
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 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 on the public ip address of the router. Thus, on receiving 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 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 organisation. 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 a IP address assigned by the service provider i.e., these are private IP address. 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 form the outside network. It is the IP address of the outside destination host before translation.

NetworkAddressTranslation(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 address. This is generally used for Web hosting. These are not used in organisations as there are many devices who will need Internet access and to provide Internet access, public IP address is needed.

   Suppose, if there are 3000 devices who needs access to Internet, the organisation have 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 address. If the IP address of pool are not free, then the packet will be dropped as only fixed number of private IP address can be translated to public addresses.

   Suppose, if there is 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 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 wants to access the Internet are fixed. This is also very costly as the organisation have 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 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 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 tunneling protocols such as IPsec.
- Also, router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.