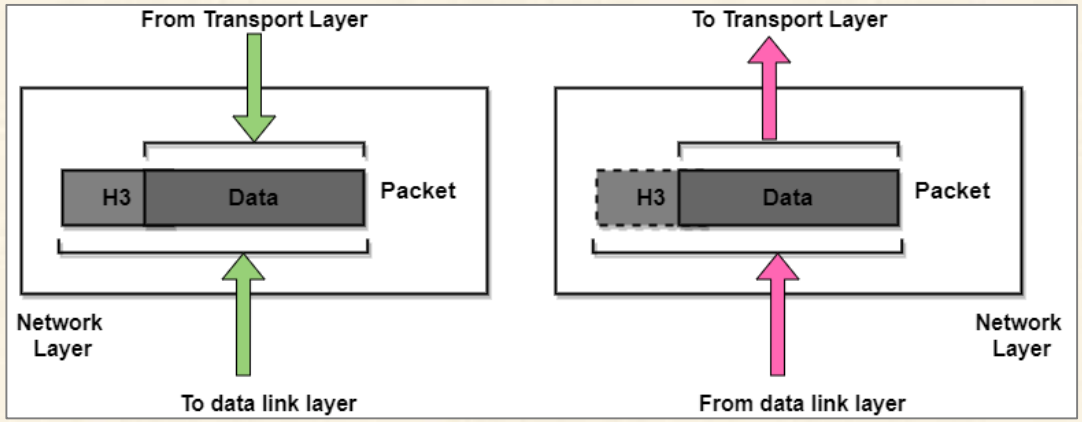
CN: UNIT-3 Network Layer

Prepared By,
M.Gouthamm, Asst.Prof, CSE, MRUH

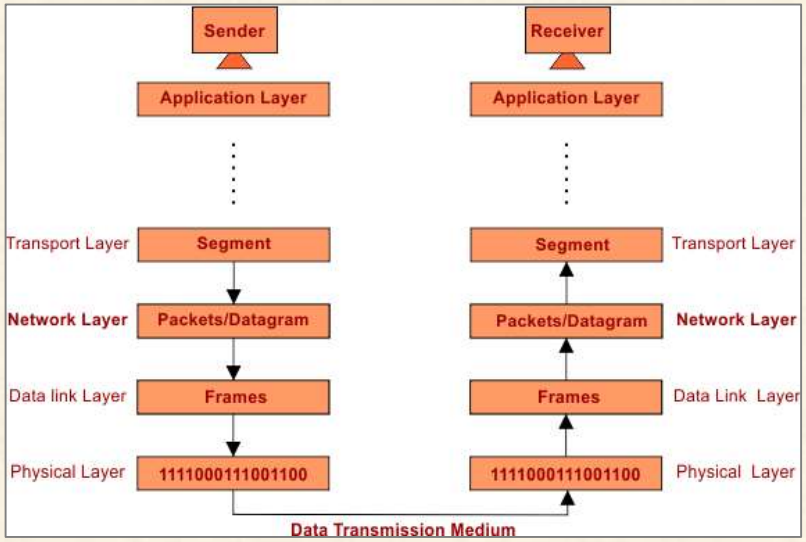
Network Layer

- Network Layer is layer 3 of the OSI reference model. The network layer controls the operation of the subnet. The main aim of this layer is to **deliver packets** from source to destination across multiple links (networks). It **routes the signal through different channels** to the other end and acts as a network controller.
- As the data link layer oversees the delivery of the packets between two systems **on the same network**; the network layer mainly ensures that each packet gets from its **point of origin to the final destination**.
- It also divides the outgoing messages into **packets and to assemble incoming packets into messages** for higher levels.
- If two computers (system) are connected on the **same link, then there is no need** for a network layer. But in case if two systems ate attached to **different networks(links)** with connecting devices between the networks(links), then there is a **need for the network layer** in order to accomplish the source-to-destination delivery.



Network Layer

- The network layer is responsible for converting **logical addresses into physical addresses.** It decides the path from the source to the destination and manages **issues such as switching, routing, and data packet congestion.**
- The network layer's primary function is to transport packets from the sending host to the receiving host.
- **At Sender Side,** Network layer receives **segments** from transport layer and convert these segments into packets/datagrams and transmit these packets/datagrams to data link layer.
- **At Receiver Side,** Network layer receives frames from data link layer and convert these frames to packets/datagrams and then transmit to transport layer.



Design Issues

Network Layer Design Issues

- A key design issue is **determining how packets are routed from source to destination**. Routes can be based on static tables that are wired into the network and rarely changed. They can also be highly dynamic, being determined anew for each packet, to reflect the current network load.
- If **too many packets** are present in the subnet at the same time, they will get into one another's way, forming **bottlenecks**. The **control of such congestion** also belongs to the network layer.
- Moreover, the **quality of service** provided(delay, transmit time, jitter, etc) is also a network layer issue.
- When a packet has to **travel from one network to another to get to its destination**, many problems can arise such as:
  - The addressing used by the second network may be different from the first one.
  - The second one may not accept the packet at all because it is too large.
  - The protocols may differ, and so on.
- It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

Design Issues

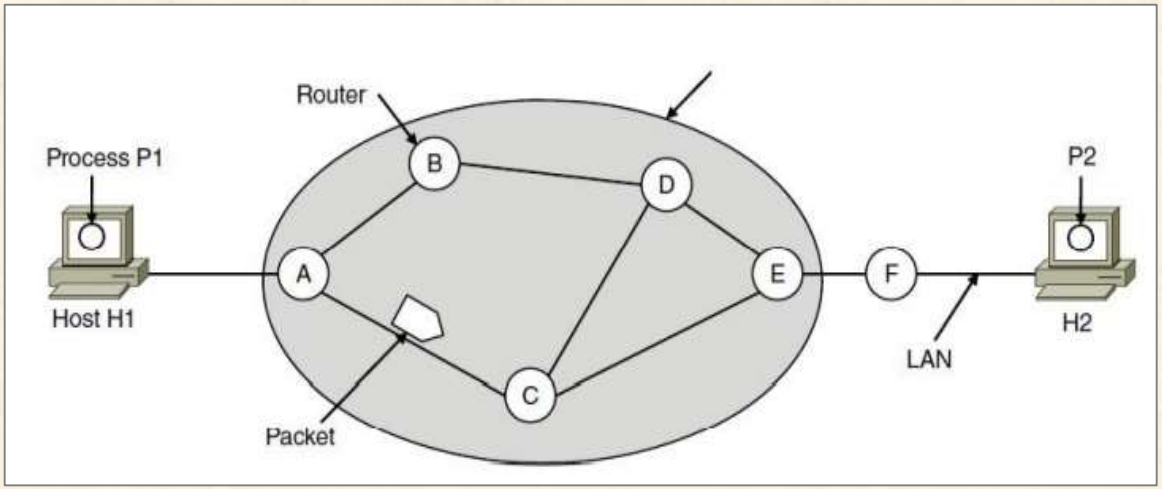
Network Layer Design Issues

1. Store-and-forward packet switching
2. Services provided to transport layer
3. Providing of connectionless service
4. Providing of connection-oriented service
5. Comparison of virtual-circuit and datagram networks

Design Issues

1. **Store-and-forward packet switching**

- A host with a packet to send **transmits it to the nearest router,** either on its own LAN or over a point-to-point link to the ISP.
- The packet is **stored there until it has fully arrived** and the link has finished its processing by verifying the checksum.
- Then it is **forwarded to the next router** along the path until it reaches the destination host, where it is delivered.
- This mechanism is **store-and-forward packet switching.**



Design Issues

2. Services provided to transport layer

- The network layer provides service its immediate upper layer, namely transport layer, through the network − transport layer interface.

The two types of services provided are −

i. Connection − Oriented Service − In this service, a **path is setup** between the source and the destination, and all the data packets belonging to a message are routed along this path.

ii. Connectionless Service − In this service, each packet of the message is considered as an **independent entity** and is **individually routed** from the source to the destination.

The objectives of the network layer while providing these services are −

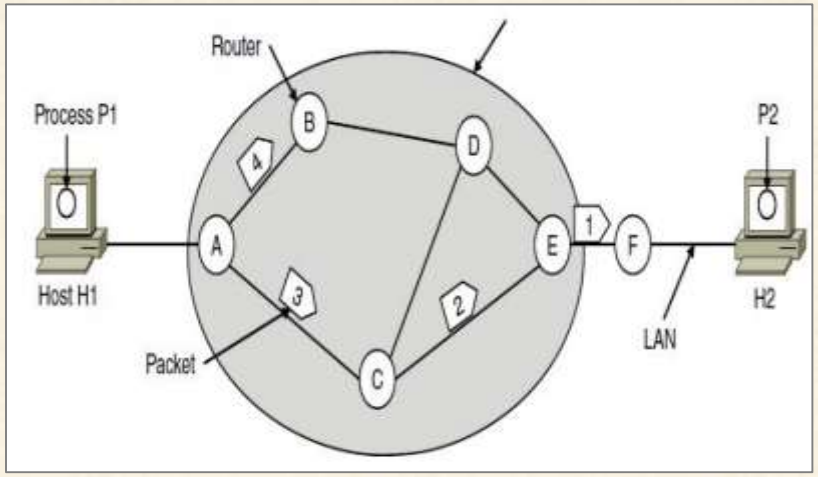
1. The services should **not be dependent** upon the router technology.
2. The router **configuration details should not** be of a concern to the transport layer.
3. A **uniform addressing** plan should be made available to the transport layer, whether the network is a **LAN, MAN or WAN.**

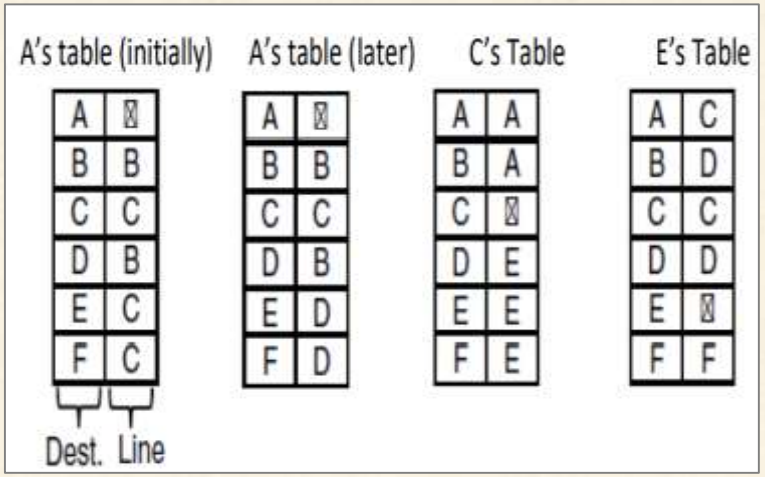
Design Issues

3. Providing of connectionless service

- If connectionless service is offered, packets are **injected** into the network **individually and routed independently** of each other.
- No advance setup is needed. In this context, the packets are frequently called **datagrams** (in analogy with telegrams) and the network is called a **datagram networks or datagram subnets.**
- An example of connectionless service is **Internet Protocol or IP.**

Let us assume for this example that the message is four times longer than the maximum packet size, so the network layer has to break it into four packets, 1, 2, 3, and 4, and send each of them in turn to router A.





Design Issues

- Every router has an internal table telling it where to send packets for each of the possible destinations. Each table entry is a pair(destination and the outgoing line). Only directly connected lines can be used.

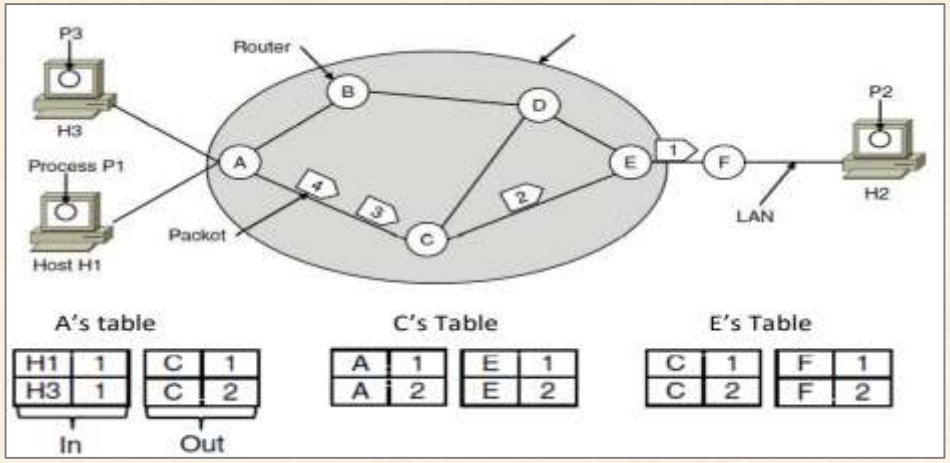
A's initial routing table is shown in the figure under the label "initially."

- At A, packets 1, 2, and 3 are stored briefly, having arrived on the incoming link. Then each packet is forwarded according to A's table, onto the outgoing link to C within a new frame. Packet 1 is then forwarded to E and then to F.
- However, something different happens to packet 4. When it gets to A it is sent to router B, even though it is also destined for F. For some reason (traffic jam along ACE path), A decided to send packet 4 via a different route than that of the first three packets. Router A updated its routing table, as shown under the label "later."
- The algorithm that manages the tables and makes the routing decisions is called the **routing algorithm.**

Design Issues

4. Providing of connection-oriented service

- If connection-oriented service is used, a **path** from the source router all the way to the destination router **must be established** before any data packets can be sent. This connection is called a **VC (virtual circuit)**, and the network is called a **virtual-circuit network.**
- When a connection is established, a route from the source machine to the destination machine is chosen as part of the **connection setup and stored in tables** inside the routers.
- That route is used for **all traffic flowing over the connection**, exactly the same way that the telephone system works. When the connection is released, the virtual circuit is also terminated.
- With connection-oriented service, each packet carries an identifier telling which virtual circuit it belongs to.



Design Issues

- Here, host H1 has established connection 1 with host H2. This connection is remembered as the first entry in each of the routing tables. The first line of A's table says that if a packet bearing connection identifier 1 comes in from H1, it is to be sent to router C and given connection identifier 1. Similarly, the first entry at C routes the packet to E, also with connection identifier 1.
- Now let us consider what happens if H3 also wants to establish a connection to H2. It chooses connection identifier 1 (because it is initiating the connection and this is its only connection) and tells the network to establish the virtual circuit. This leads to the second row in the tables. Note that we have a conflict here because although A can easily distinguish connection 1 packets from H1 from connection 1 packets from H3, C cannot do this. For this reason, A assigns a different connection identifier to the outgoing traffic for the second connection. Avoiding conflicts of this kind is why routers need the ability to replace connection identifiers in outgoing packets.
- In some contexts, this process is called **label switching.** An example of a connection-oriented network service is **MPLS (Multi Protocol Label Switching).**

Design Issues

5. Comparison of virtual-circuit and datagram networks

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Functionality

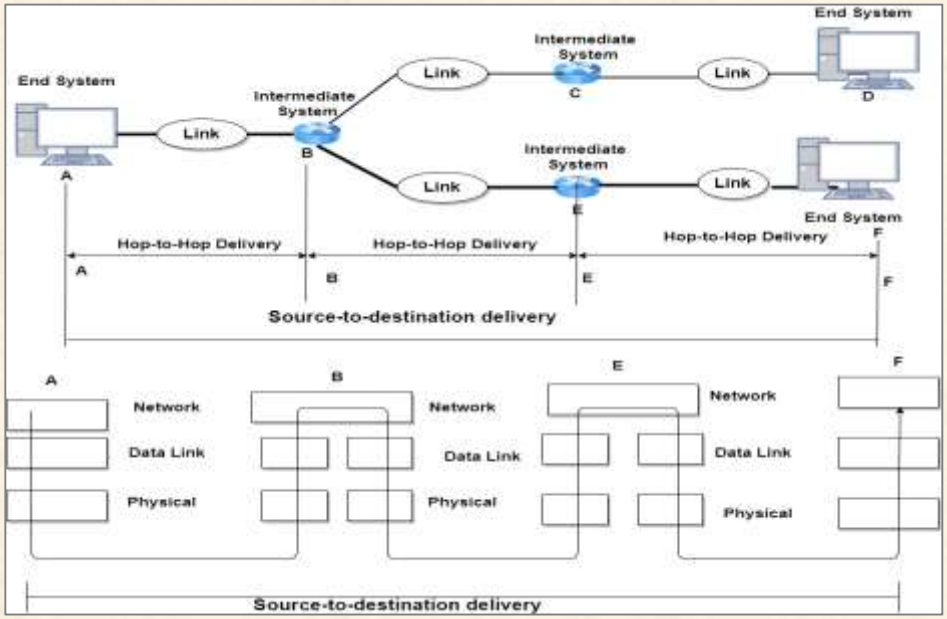
Functions of Network Layer:

1. **Source to Destination Delivery**
2. **Addressing**
3. **Routing**
4. **Internetworking**
5. **Fragmentation**
6. **Congestion Control**
7. **Flooding**

Functionality

1. **Source to Destination Delivery**

- Network layer provides Source to destination Delivery which also called HOST to HOST delivery. Following figure shows host to host delivery.



- In the above figure, the network layer at the A node sends the packet to the network layer at the B node. When the packet arrives at router B then the router makes the decision of the path based on the final destination that is the F node of the packet transmitted. Router B makes use of its routing table for finding the next hop that is router E. The Network layer at node B sends the packet to the network layer at E which then sends the packet to the network layer at F.

Functionality

2. Logical Addressing:

- The **physical addressing** is implemented by the data link layer, while the **logical addressing** is implemented by the network layer. The network layer appends a header to the packet that contains the logical addresses of the sender and recipient.
- Network layer is used when source to destination delivery is required in different networks or over the **internet**. Network layer use the **Logical (IP) Address to communicate** over the internet. IP address contains the **network ID and Host ID** of destination machine. Network layer use **IPV4 or IPV6 for addressing purpose.**

3. Routing: Networking layer uses the **Router device** to determine the best optimal path out of the multiple paths from source to the destination. Router uses **routing protocols (i.e. RIP, OSPF etc.)**

4. Internetworking: The network layer's primary function is to establish **logical connections between different** types of networks.

5.Fragmentation: Sometimes when a sender sends a packet to router then router may not have enough space to accommodate entire packet. So, it is required to **break these packets into fragmentations** (parts).

So, fragmentation of packets/datagram is also responsibility of network layer.

Functionality

6. Congestion Control:

- The case, when maximum nodes send the data at a time to same router even with fragmentations, then buffer of router may be out of capacity. In this case, traffic must be control. Controlling of traffic is called congestion control. So, in some cases congestion control is required which is also the responsibility of Network layer.

6. Flooding:

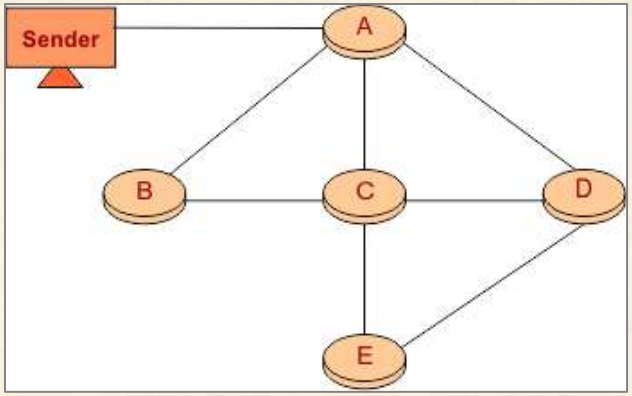
When a data packet arrives at a router, then router sent this data to all the outgoing links from router except the link from which the data arrived.

Example

- Suppose there are 5 routers (A, B, C, D and E) which are connected though transmission lines as given below.

By using flooding technique

1. An incoming data packet from sender will send to Router A.
2. Router A will forward the data packet to other routers B, C and D.
3. B will send the packet to C.
4. C will send the packet to B,D and E.
5. D will send the packet to C and E.
6. E will send the packet to D.



Note: Main advantage of flooding is that, the shortest path is always chosen by flooding because in flooding **each router holds the information's of their neighbours.**

Services

Forwarding and Routing:

- A router is used on the network layer to forward packets. A forwarding table is included on every router. A router passes a packet by **inspecting the header field and then indexing it into the forwarding table** using the header field value. The forwarding table value matching to the header field value specifies the router's outgoing interface connection to which the packet is to be forwarded.

Network Layer Services:

1. **Guaranteed delivery:** This layer offers a service that **ensures the packet arrives** at its destination.
2. **Guaranteed delivery with bounded delay:** It is another service provided by the network layer and it guarantees that the packet will surely be delivered within a specified **host-to-host delay bound.**
3. **In-Order packets:** This service assures that packets reach their destination in the **order they were delivered.**
4. **Guaranteed maximum jitter:** This service assures that the **time between two consecutive transmissions** at the sender **equals the time between** their receipt at the destination.
5. **Security services:** These are provided at the network layer through the use of a **session key between** the source and destination hosts. The payloads of datagrams transmitted to the destination host are **encrypted** by the network layer of the source host. The payload would subsequently be **decrypted** by the network layer at the target host. In this manner, the network layer ensures data integrity and source authentication services.

Pros & Cons

Advantages of Network Layer Services

Given below are some benefits of services provided by the network layer:

1. By forwarding service of the network layer, the data packets are transferred from one place to another in the network.
2. In order to reduce the traffic, the routers in the network layer **create collisions and broadcast the domains.**
3. Failure in the data communication system gets eliminated by **packetization.**

Disadvantages of Network layer Services

1. In the design of the network layer, there is a **lack of flow control.**
2. In the network layer, there is a **lack of proper error control** mechanisms; due to the **presence of fragmented** data packets the implementation of error control mechanism becomes difficult.
3. Due to the presence of **too many datagrams** there happens **occurrence of congestion.**

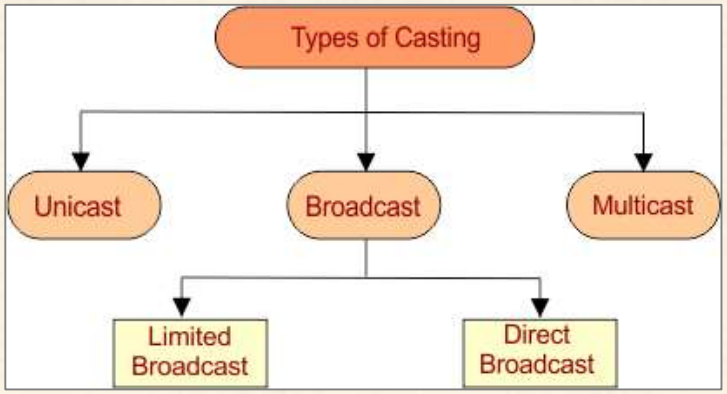
Network Layer in the Internet

Casting And Its Types

Casting is a method of transferring a packet to various hosts simultaneously by using an IP address.

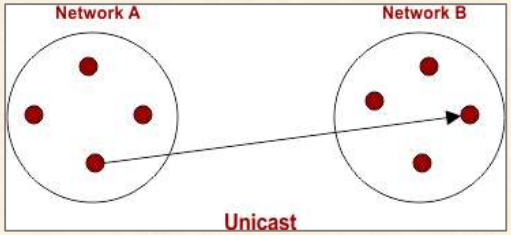
Types of Casting

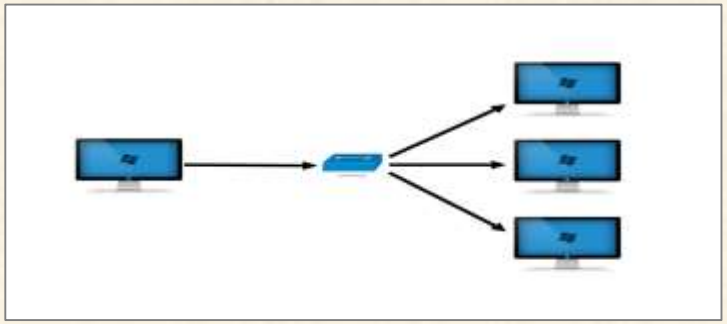
- There are three types of casting



1. Unicast

- Transmitting a packet from **one source node to one destination node** is called as unicast.
- We can say, it is a **one to one** transmission.





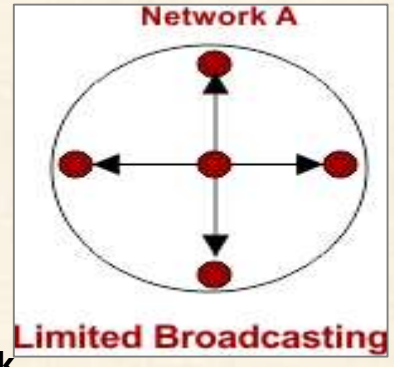
Example

- Consider a Node/Host "A" having IP Address 11.2.2.31 in one network is sending data to Node/Host "B" having IP Address 21.11.41.21 in another network.
- Then, Source IP Address of Host A = **11.2.2.31** Destination IP Address of Host B = **21.11.41.21.**

Casting And Its Types

2. Broadcast

- In Broadcasting, Packet is send to all residing host in the same or different network, depending on its types. It is a one to all transmission.



Broadcasting is of two types

1. **Limited Broadcast**
2. **Direct Broadcast**

1. Limited Broadcast

- According to Limited Broadcasting, Packet is send to **all residing host in the same network.**
- If a Host need to send a broadcast message with in the same network then All 32 bits of **IP address are set to 1.As**
- Limited Broadcast Address for any network = **11111111.11111111.11111111.11111111 = 255.255.255.255**
- This IP address cannot pass through router to go for another network.

Example

- Consider a Node/Host "A" having IP Address 11.2.2.31 is sending data to all other hosts residing in the same network.

Then,

- Source IP Address = **IP Address of host A = 11.2.2.31**
- Destination IP Address = **255.255.255.255**

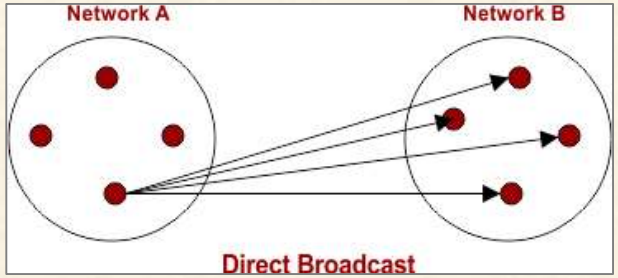
Casting And Its Types

2. Direct Broadcast

- According to Limited Broadcasting, Packet is send to **all residing host in the other network**
- If a Host in a network wants to send a broadcast message to other network then **all hosts bits of IP address are set to 1.**
- This IP address can pass through router to go for another network.

Example

- Host "A" in one Network having IP Address 11.11.121.13 sending data to all other hosts residing in the network having IP Address 21.0.0.0

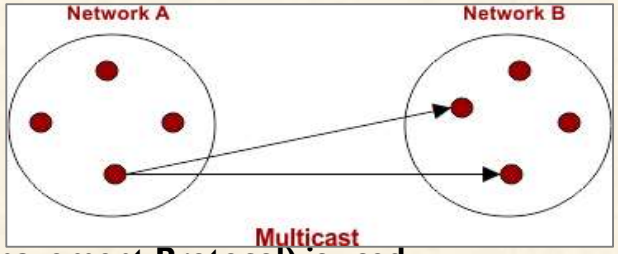


Then,

- Source IP Address of host A = **11.11.121.13**
- Destination Address = **21.255.255.255**

3. Multicast

- Transmitting data packet from one source Node to a **particular group of Nodes** is known as Multicast.
- It is also an example of **one to many** transmission.



Examples

- Sending a message to group of people on whatsapp.
- Video conference to a particular group of people

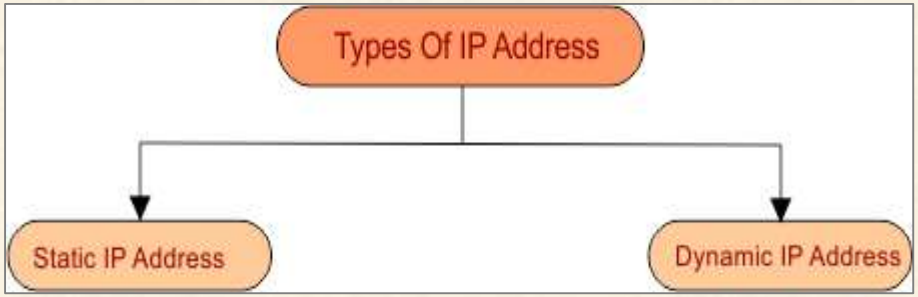
Note: To identify the group in multicast, **IGMP (Internet Group Management Protocol) is used.**

IP Address in Networking

- In computer networking IP addressing is used at network layer, IP stand for Internet Protocol.
- IP address is a **unique address which is assigned by ISP** to each device whenever it connected to internet.

Types Of IP Address

- There are two types of IP address



1. Static IP Address

- After assigning a Static IP Addresses to host, **it always remains** the They are configured manually.

Note: Some internet service providers (ISPs) do not provide static IP addresses. **Static IP are more costly** than dynamic IP Addresses.

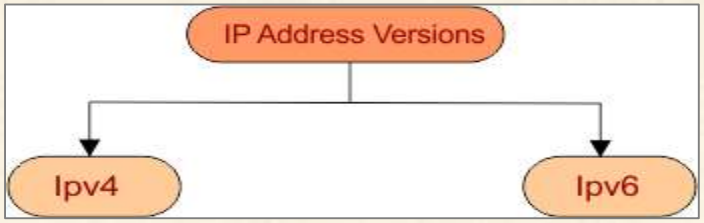
2. Dynamic IP Address

- Dynamic IP Address is a **temporarily assigned IP** Address to any host of a network. It can be assigned to a different device if it is available (not in use of any Host).
- **DHCP** (Dynamic Host Configuration Protocol) or **PPPoE** (point to point connection over Ethernet) **assigns** dynamic IP addresses.

IP Address Versions

IP Address Versions

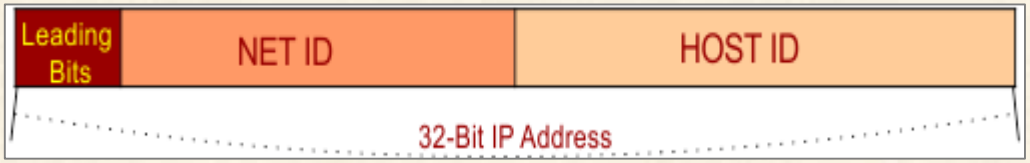
- IP address is classified into two versions



- IPv4 is mostly using now a days. However both **IPv4 and IPv6** are supported by mostly Operating systems and manufacturer of networking devices.

IPv4 Address Format

- IPv4 Address is a **32 bit binary address** which has 4 octet. Each octet (8-bits) and must be a decimal value between 0 and 255 are separated by dot (“.”).
- it supports **2^{32} or 4.3 billion IP addresses.** IPv4 addresses are not enough due to rapid growth of internet.
- In IPv4, Some octets are fixed for Net ID and rest of octet are reserve for Host ID.



NET ID: Net ID always contains the **some first octets** out of 4 octets. Net ID is used to **identify the network** in which Host/computer exists.

Host ID: Host section always contains the least octet of IP address. It **identifies the actual Host/computer** in the network.

So, IP address (Network ID and Host ID) represents the location of host in the network.

IP Address Versions

IPv4 Address Example

- Example of an IP Address in Binary = **00000011.10100001.00001011.11110001**
- Example of an IP Address in Binary Decimal Representation = **3.161.11.241**

IPv6 Address Format

- As the IPv4 are running out as with the growing of internet. And IPv6 comes into picture, it use **128 bits long, written as 8 sections of 16 bits each**. techniques as compared to 32-bit IPv4. IPv6 provides **(2^{128}) unique IP addresses.**

IPv6 Address Example

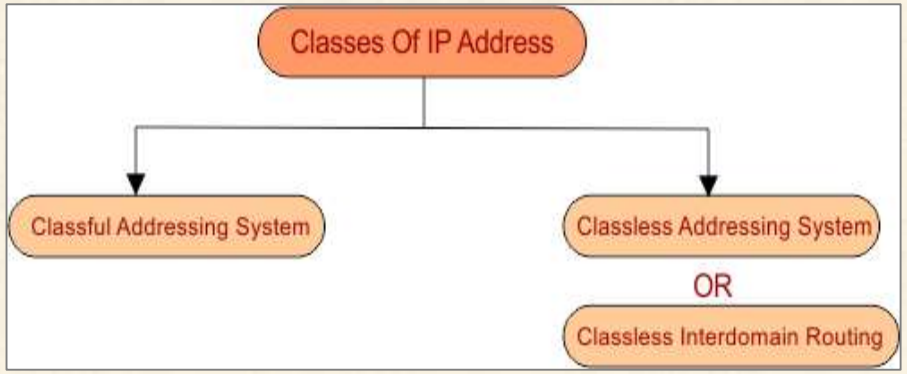
- An IPv6 (Normal) address has the following format: y : y : y : y : y : y : y : y where *y* is called a *segment* and can be any hexadecimal value between 0 and FFFF. The segments are separated by colons. An IPv6 normal address must have eight segments.
- It is **hexadecimal** instead of decimal, as given below

  6789:ABCD:1234:EF92:6789:ABCD:1234:EF92

- Each hexadecimal character is denoted by **4 binary bits**. IPv6 may also be **unicast, multicast or broadcast.**

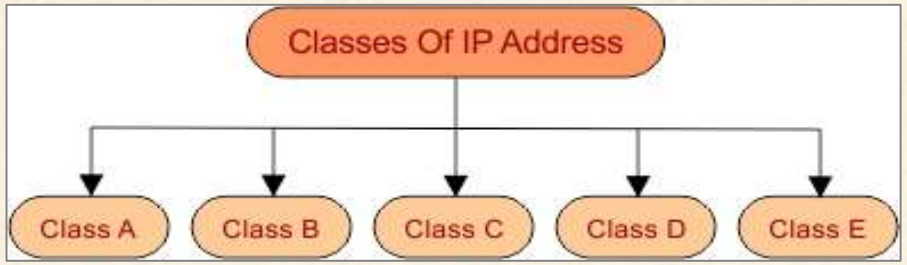
IP Addressing

- IP addressing is classified into two systems which are



Classful IP Addressing

- In classful IP addressing, there are five classes which are given below



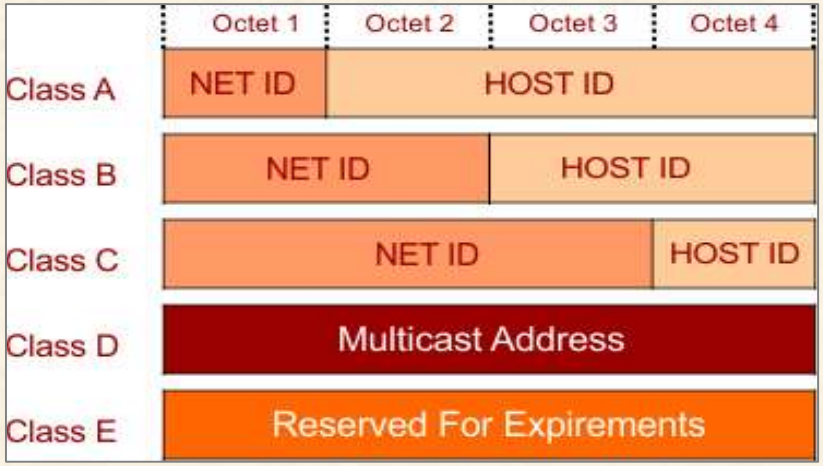
- **In each class, two hosts IP are reserved**
- **First host-IP** in the network which is zero (i.e. for **class A (0.0.0.0)** represents to that network and cannot be assign to any host in the network.
- **And last IP** in the network (i.e. for **class A (126.255.255.255)** used for broadcasting.

Classful IP Addressing

- **In each class, Some Leading Bits are reserved For Class Identification**
- For **class A,** The first one leading bit is always fix to "**0**"
- For **class B,** The first two leading bits are always fixed to **"10"**
- For **class C,** The first three leading bits are always fixed to **"110"**
- For **class D,** The first four leading bits are always fixed to **"1110"**
- For **class E,** The first four leading bits are always fixed to **"1111"**

Look at the following diagram for better understanding

Range of First Octet Values (decimal)
1 to 126
128 to 191
192 to 223
224 to 239
240 to 255



Classful IP Addressing

- Number of networks and number of hosts in each class can be calculated through the following formula

- ***Important To find Subnet mask of each class, Replace all Host octets to Zero and Network Octets to 255.***

Subnet Mask

- A subnet mask is a 32 bits address used to **distinguish between a network address and a host address** in IP address. A subnet mask identifies which part of an **IP address is the network address and the host address.** They are not shown inside the data packets traversing the Internet. They carry the destination IP address, which a router will match with a subnet.

Class	Default subnet mask	No. of networks	No. of host per network
A	255.0.0.0	128	16,777,214
B	255.255.0.0	65,536	65,534
C	255.255.255.0	16,777,216	126

Classful IP Addressing

Descriptive diagram of IP Classes

Class	Leading Bit	Bits For Network ID	No. of Networks	Bits For HOST ID	No. of HOSTS per Network	Total Addresses in the Class	First IP Address	First HOST Address	Last IP Address	Last HOST Address	Default Subnet Mask
Class A	0	7	2^7	24	$2^{24} - 2$	2^{31}	0.0.0.0	0.0.0.1	127.255.255.255	127.255.255.254	255.0.0.0
Class B	10	14	2^{14}	16	$2^{16} - 2$	2^{30}	128.0.0.0	128.0.0.1	191.255.255.255	191.255.255.254	255.255.0.0
Class C	110	21	2^{21}	8	$2^8 - 2$	2^{29}	192.0.0.0	192.0.0.1	223.255.255.255	223.255.255.254	255.255.255.0
Class D	1110	Not Defined	Not Defined	Not Defined	Not Defined	2^{28}	224.0.0.0	224.0.0.1	239.255.255.255	223.255.255.254	Not Defined
Class E	1111	Not Defined	Not Defined	Not Defined	Not Defined	2^{28}	240.0.0.0	240.0.0.1	255.255.255.255	223.255.255.254	Not Defined

Important Points

- In a **single network**, All hosts holds the **same network ID but different Host ID.**
- Two hosts in **different networks** having different network ID but may have the same host ID.
- Last Network ID (i.e. 255.255 in Class B) with Last IP Address of that class (i.e. 255.255 in class B) is always a limited broadcast address of that class. Limited broadcast address of any class will always = **255.255.255.255.**
- Any Network ID (i.e. 135.115 in class B) with its Last IP Address (i.e. 255.255 in class B) is always a direct broadcast address of that class. direct broadcast address of Network ID 135.115 is = **135.115.255.255.**

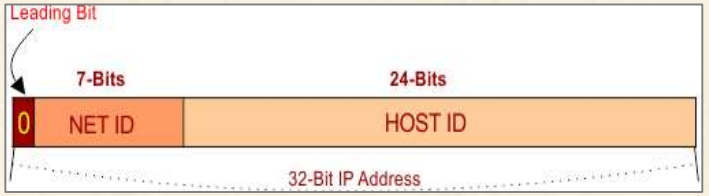
Classful IP Addressing

Class A

- First octet (8-bits) represent network ID and remaining 3-octet (24-bits) represents the host ID. The first 1 leading bit of network ID in Class A is always (0) and remaining 7-bits represent network ID.

  Format: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH (in binary)

- Start to End IP Address = **(0.0.0.0 to 127.255.255.255)**
- Value of first octet = **0 – 127**
- Possible network ID's = **(2^7) = 128**



Important Note: In class A, Network ID Zero **(i.e. 0.0.0.0) is reserved for default** network and Network ID 127 **(i.e. 127.0.0.0) is reserved for loopback** (used for software testing). So, the remaining 126 (1-126) networks ID's are used in class A.

- Possible Hosts = **(2^{24}-2) = 16777214**
- Total number of possible IP addresses = **(2^{31}) = 2,147,483,648** (because "1 out of 32" bit is leading bit)
- First IP address = **0.0.0.0** First Host address = **0.0.0.1**
- Last IP address = **127.255.255.255** Last Host address = **127.255.255.254**
- Subnet Mask = **255.0.0.0**

Note: *Class A Network is used for* ***large size companies*** *because it has large number of hosts.*

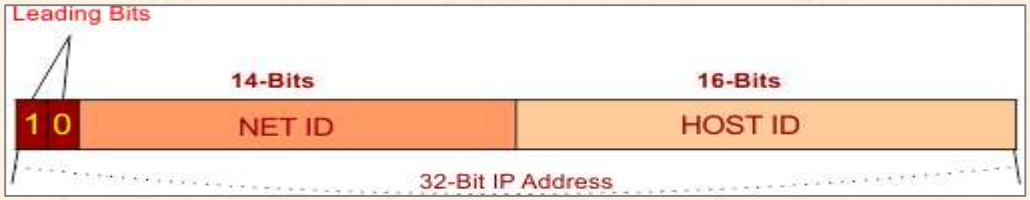
Class A Example

Classful IP Addressing

Class B

First two octets (16-bits) represent network ID and remaining 2-octets (16-bits) represents the host ID. The first two leading bit of network ID in Class B are always (10) and remaining 14-bits represent network ID.

Format: 10NNNNNN. NNNNNNNN.HHHHHHHH.HHHHHHHH (in binary)



- Start to End Address IP addresses = **(128.0.0.0 to 191.255.255.255)**
- Value of first octet = **(10000000 – 10111111) = 128 – 191**
- Possible network ID = **(2^{14}) = 16384**
- Possible Hosts = **(2^{16}-2) = 65534**
- Possible Total number of IP addresses = **(2^{30}) = (2 out of 32 bit is leading bit)**
- First IP address = **128.0.0.0** First Host address = **128.0.0.1**
- Last IP address = **191.255.255.255** Last Host address = **191.255.255.254**
- Subnet Mask = **255.255.0.0**

Class B Example

Note: *Class B Network is used for **medium size companies** because it has small number of hosts as compare to class A.*

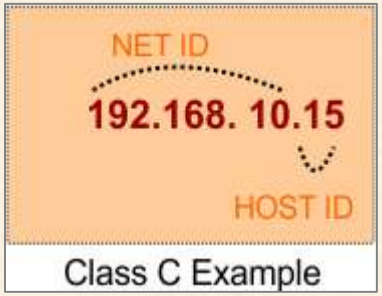
Classful IP Addressing

Class C

- First three octets (24-bits) represent network ID and remaining 1-octet (8-bits) represents the host ID. The first three leading bit of network ID in Class B are always (110) and remaining 21-bits represent network ID.

Format: 110NNNNN. NNNNNNNN. NNNNNNNN.HHHHHHHH (in binary)

- Start to End Address IP addresses = **(192.0.0.0 to 223.255.255.255) (in hexadecimal)**
- Value of first octet = **(11000000 – 11011111) = 192 – 223**
- Possible network ID = **(2^{21}) = 2097152**
- Possible Hosts = **(2^{8}-2) = 254**
- Possible Total number of IP addresses = **(2^{29}) = (3 out of 32 bit is leading bit)**
- First IP address =**192.0.0.0** First Host address = **192.0.0.1**
- Last IP address = **223.255.255.255** Last Host address = **223.255.255.254**
- Subnet Mask = **255.255.2555.0**



Class C Example

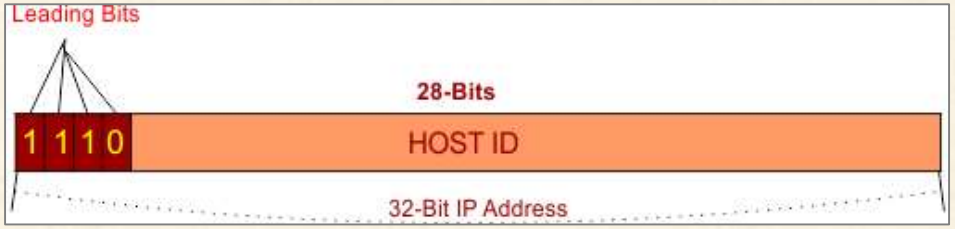
- **Note:** *Class C Network is used for **small size companies** because it has small number of hosts as compare to class A and B.*

Classful IP Addressing

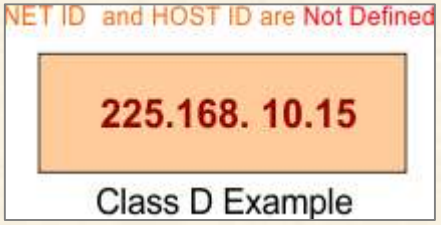
Class D

- Class D is used for **multicasts.** Multicasting is used to pass the copies of **datagram to selected groups of hosts** instead of individual host. Class D is slightly different class from first three classes.
- The first four leading bit of network ID in Class D are always **(1110)** and remaining 28-bits represent group of computers where the multicast message will be passed.

Format: 1110mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm (in binary)



- Start to End Address IP addresses = **(224.0.0.0 to 247.255.255.255) (in hexadecimal)**
- Value of first octet = **(11100000 – 11101111) = 224 – 247**
- Possible Total number of IP addresses = **(2^{28}) = (4 out of 32 bit is leading bit)**
- First IP address = **224.0.0.0** First Host address = **224.0.0.1**
- Last IP address = **239.255.255.255** Last Host address = **223.255.255.254**



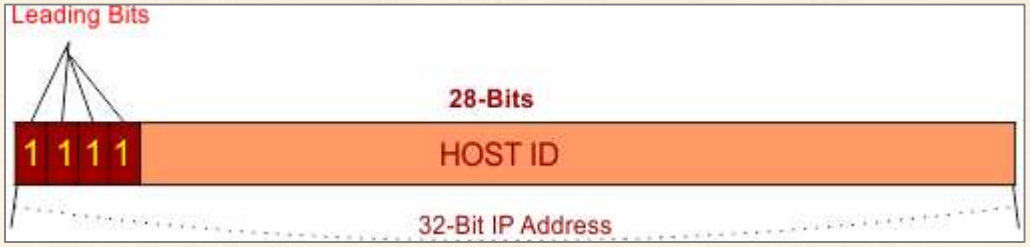
- ***Subnet Mask, Network ID and Host ID are not defined in Class D***

Classful IP Addressing

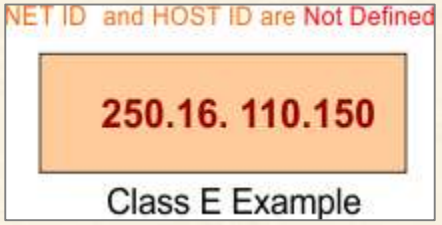
Class E

- Class E is used for **future Experimental** purpose only. It is mostly used in **research and development fields**. The first four leading bit of network ID in Class E are always (1111)

  Format: 1111rrrr. rrrrrrrr. rrrrrrrr. rrrrrrrr (in binary)



- Start to End Address IP addresses = **(248.0.0.0 to 255.255.255.255) (in hexadecimal)**
- Value of first octet = **(11110000 – 11111111) = 248 – 255)**
- Possible Total number of IP addresses = **(2^{28}) = (4 out of 32 bit is leading bit)**
- First IP address = **240.0.0.0** First Host address = **240.0.0.1**
- Last IP address = **255.255.255.255** Last Host address = **223.255.255.254**



- ***Subnet Mask, Network ID and Host ID are not defined in Class E***

Classful IP Addressing

Question is that if given IP address = 201.20.31.65 then find out the following parts

1: Find the Class of given IP?

2: Find the Subnet Mask of given IP?

3: Find the Network ID?

4: Find First and Last IP address of given Network IP?

5: Find first and Last Host ID of given Network IP?

6: Find the Limited broadcast IP addressing?

7: Find the Direct broadcast IP addressing?

Classful IP Addressing

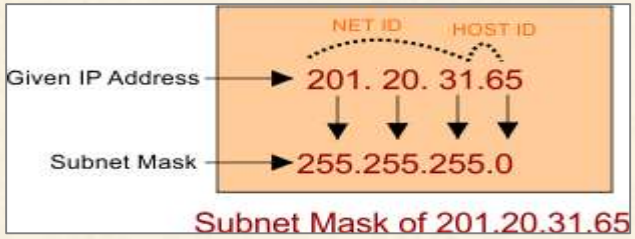
Question is that if given IP address = 201.20.31.65 then find out the following parts

Part 1: Find the Class of given IP?

- **Solution:** As the first Octet of given IP address exist in between the range of Class C (192 – 223). So, given IP belongs to class C.

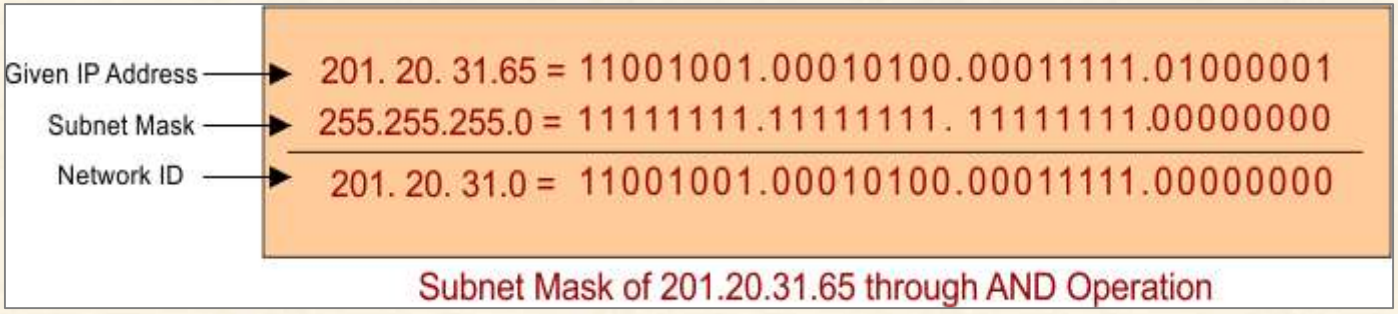
Part 2: Find the Subnet Mask of given IP?

- **Solution:** After checking the class of given IP. Subnet mask can be found by putting all octet-bits of network ID to "255" and Host bits to "0". So, Class C subnet mask is 255.255.255.0.



Part 3: Find the Network ID?

- **Solution:** To find network ID, Perform **AND operation of given IP with Subnet mask in binary**. It will provide the network ID where that particular IP exist. So network ID will be **201.20.31.0.**



Classful IP Addressing

Part 4: Find First and Last IP address of given Network IP?

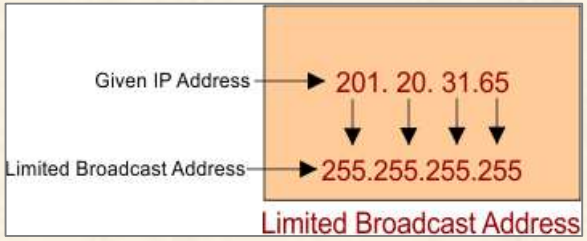
- **Solution:** We know that there are two IP's of each network are reserved. As the **Network ID is 201.20.31.0.** So, the first IP address will be 201.20.31.0 which is reserved for network identification. And **Last IP address is 201.20.31.255** which is reserved for direct broadcasting.

Part 5: Find first and Last Host ID of given Network IP?

- **Solution: Due to reservation of two Hosts,** of Network ID is 201.20.31.0. So, the first host IP address will be 201.20.31.1 and Last host IP address is 201.20.31.254.

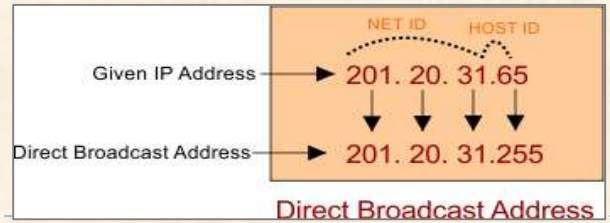
Part 6: Find the Limited broadcast IP addressing?

- **Solution:** By replacing all octets of IP address to 255 (decimal) is called Limited broadcast IP addressing. So, Limited broadcast address = 255.255.255.255.



Part 7: Find the Direct broadcast IP addressing?

- **Solution:** By replacing the Host-bits-octets to 255 of given IP is called direct broadcast IP addressing. So, direct broadcast IP addressing = 201.20.31.255.



Classful IP Addressing

PRACTICE PROBLEMS BASED ON IP ADDRESS IN NETWORKING

Problem-01:

For the following IP Addresses-

1. 1.2.3.4
2. 10.15.20.60
3. 130.1.2.3
4. 150.0.150.150
5. 200.1.10.100
6. 220.15.1.10
7. 250.0.1.2
8. 300.1.2.3

Identify the Class, Network IP Address, Direct broadcast address and Limited broadcast address of each IP Address.

Classful IP Addressing

Problem-02:

- A host with IP Address **200.100.1.1** wants to send a packet to all the hosts in the same network. What will be-

1. Source IP Address
2. Destination IP Address

Problem-03:

- A host with IP Address **10.100.100.100** wants to use loop back testing. What will be-

1. Source IP Address
2. Destination IP Address

Problem-04:

- How many bits are allocated for Network ID and Host ID in **23.192.157.234** address?

Problem-05:

Match the following-

	Column-I	Column-II
1.	200.10.192.100	Class A
2.	7.10.230.1	Limited Broadcast Address
3.	128.1.1.254	Direct Broadcast Address
4.	255.255.255.255	Class C
5.	100.255.255.255	Class B

Classless IP Addressing

- Classless IP addressing makes the **allocation of IP Addresses more flexible** which is also known as **Classless Inter Domain Routing (CIDR).**
- In Classless IP addressing, **CIDR block contains the required number of IP** Addresses as demanded by the user.

Note: CIRD BLOCK Contains required number of IP Addresses as demanded by the user. Whenever

Purpose of Classless Addressing

There were two major problems with Classful IP addressing

1. **Wastage of IP Addresses:** As there are almost **1-crore host IP** addresses in class A. But these are **too much hosts IP** addresses for a single organization. So, it is **wastage of IP** addresses.
2. **No Flexibility:** If any user required almost 1000 IP address then there is **no class of networking** which will provide exact **1000 IP address even after subnetting.** If Class A provides 1000 IP address after subneting to that organization then still a lot of **chances of wastage of remaining IP** addresses. So, it does not provide the flexibility.

Solution of Classful Problem

- **Subneting in Classless IP** addressing is used for network flexibility. It provides the **exact number of IP addresses** as one organization or network required.

Classless IP Addressing

CIDR Block

- When a user asks for specific number of IP Addresses,
- CIDR **dynamically assigns** a block of IP Addresses based on certain rules.
- This block contains the required number of **IP Addresses as demanded** by the user.
- This block of IP Addresses is called as a **CIDR block**.

Notation of CIDR

CIDR IP Addresses look like the following - **a.b.c.d / n**

- They end with a slash followed by a number called as **IP network prefix.**
- IP network prefix tells the **number of bits** used for the **identification of network.**
- Remaining bits are used for the **identification of hosts** in the network.

Example of Classless IP addressing

- An example of CIDR IP Address is given : **90.10.12.20 / 26**

Where,

- 26 bits represents the network.
- Remaining bits (**6 out of 32** in IPv4) are used for the identification of hosts in the network.

Classless IP Addressing

Rules For Creating CIDR Block

- **Rule-01:** All the IP Addresses in the classless Addressing **(CIDR Block)** must be **contiguous.**
- **Rule-02:** Number of IP addresses (for hosts) in a CIDR block must be in the **power of 2 (i.e. $2^1, 2^2, 2^3, 2^4$ and so on).**
- **Rule-03:** First IP Address of the block in CIDR, must be **divisible by the size of the block.**

Rule 3 Explanation:

Any binary pattern of IP is divisible by 2^n, if and only if its least "n" significant bits are 0.

Examples: Consider a binary pattern of an IP address **100.2.3.64**

01100100.00000010.00000011.01000000

- Above IP is divisible by either **$2^1, 2^2$ $2^3, 2^4$,2^5or 2^6** Because its least 6 significant bits are zero.
- It is divisible by 2^6 since its least significant 6 bits are zero.
- Above IP is not divisible by 2^7 because its least 7 significant bits are not zero.

So, if the size of CIDR Block is **$2^1, 2^2$ $2^3, 2^4$,2^5 and 2^6** then Rule 3 is valid for above IP otherwise if size of CIRD Block is greater than 2^7 then Rule 3 in not valid for above IP.

Classless IP Addressing

Example: Consider a classless IP address is **21.11.40.35 / 28.** Find out the range of IP Addresses in the CIDR block or classless block.

Solution

- 28 bits are used for **network identification**. Remaining 4 bits are used for **host's identification** in the classless
- Given CIDR IP Address may be represented as

  00010101.00001011.00101000.00100011 / 28

So,

- First IP Address = **00010101.00001011.00101000.00100000= 21.11.40.32**
- Last IP Address = **00010101.00001011.00101000.00101111= 21.11.40.47**
- Put all Host bits to zero for first IP, and put all host bits to "1" for Last IP of Network.

Note: Direct broadcast IP address of a network is always the last IP of that Network.

Thus, Range of IP Addresses = **[21.11.40.32 , 21.11.40.47]**

Now Check all Three rules of CIDR block

- **Rule 01:** As all IP's are contiguous **(21.11.40.32 to 21.11.40.47).** So Rule 1 is satisfied.
- **Rule 02:** Range (21.11.40.32 to 21.11.40.47) **contains 16 IP's which is the Power of 2.** So Rule 2 is satisfied.
- **Rule 03:** According to third rule, First IP must be **divisible by block size.** As the Network Size is 28 and last 4 bits of first IP are Zero. So, it is divisible. Hence, Rule 3 is also satisfied.
- As all 3 rules are valid, so, **Classless block with 16 IP's is Valid.**

Classless IP Addressing

PRACTICE PROBLEMS BASED ON CLASSLESS INTER DOMAIN ROUTING

Problem-01:

- Given the CIDR representation **20.10.30.35 / 27.** Find the range of IP Addresses in the CIDR block.

Problem-02:

- Given the CIDR representation **100.1.2.35 / 20.** Find the range of IP Addresses in the CIDR block.

Problem-03:

Consider a block of IP Addresses ranging from **100.1.2.32 to 100.1.2.47.**

- Is it a CIDR block?
- If yes, give the CIDR representation.

Problem-04:

Consider a block of IP Addresses ranging from **150.10.20.64 to 150.10.20.127.**

- Is it a CIDR block?
- If yes, give the CIDR representation.

Classless IP Addressing

Problem-04:

Consider a block of IP Addresses ranging from **150.10.20.64 to 150.10.20.127.**

- Is it a CIDR block?
- If yes, give the CIDR representation.

Solution-

For any given block to be a CIDR block, 3 rules must be satisfied-

Rule-01:

- According to Rule-01, all the IP Addresses must be contiguous.
- Clearly, all the given IP Addresses are contiguous. **So, Rule-01 is satisfied.**

Rule-02:

- According to Rule-02, size of the block must be presentable as 2^n.
- Number of IP Addresses in given block = 127 – 64 + 1 = 64.
- Size of the block = 64 which can be represented as 2^6. **So, Rule-02 is satisfied.**

Classless IP Addressing

Rule-03:

- According to Rule-03, first IP Address must be divisible by size of the block.
- So, 150.10.20.64 must be divisible by 2^6.
- 150.10.20.64 = **150.10.20.01000000 is divisible by 2^6** since its 6 least significant bits are zero.
- So, Rule-03 is satisfied.

Since all the rules are satisfied, therefore given block is a CIDR block.

CIDR Representation-

We have-

- Size of the block = Total number of IP Addresses = 2^6.
- To have 2^6 total number of IP Addresses, 6 bits are required in the Host ID part.
- So, Number of bits in the Network ID part = 32 – 6 = 26.

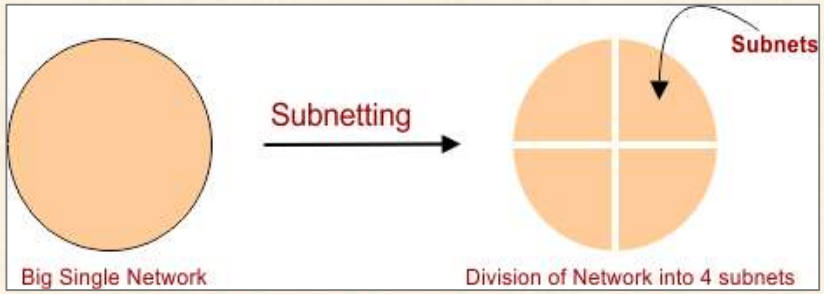
Thus, **CIDR Representation = 150.10.20.64 / 26**

Subnetting

- Subnetting is a process in which a single network is dividing into multiple sub-networks, also called as **subnets**.

Example

- Following figure shows the sub networks of a large single network into 4 smaller sub networks.

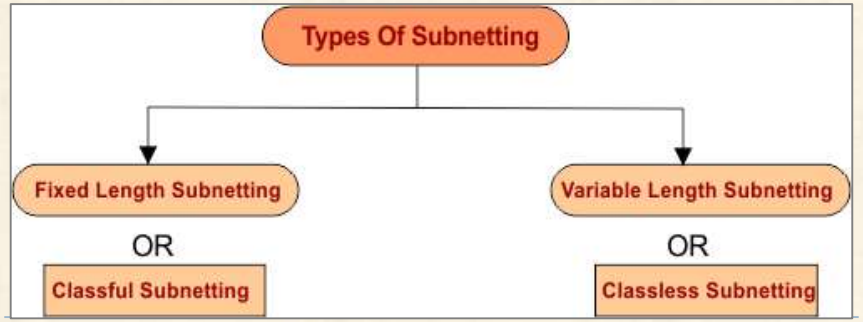


Subnet ID

- Each sub network has its unique network ID known as its **Subnet ID**.
- The subnet ID is created by borrowing some bits from the part of Host ID.
- The number of bits borrowed from hosts depends on the number of subnets created.

Types of Subnetting

- Subnetting of a network can be achieved through the following methods



Subnetting

1. Fixed Length Subnetting

- Fixed length subnetting also called as **classful subnetting.** Fixed length subnetting hold the following properties.
- Sizes of all sub networks and Subnets of all **sub networks are same.**
- All the sub networks have **equal number of hosts.**

2. Variable Length Subnetting

- Variable length subnetting also called as **classless subnetting**. Variable length subnetting hold the following properties.
- Sizes of all sub networks are not same and Subnets of all **sub networks are not same.**
- All the sub networks **do not have the equal number of hosts.**

Advantages of Subnetting

- Subnetting improves the security because the **administration and maintenance** of sub networks is easy.
- In simple words, management and maintenance of entire university is tough as compare to its different departments.

Subnetting

Disadvantages of Subnetting

Point-01:

- Subnetting leads towards the **loss of IP Addresses.**
- Two IP Addresses are always **wasted for every sub-network** (subnet).In subnetting, One IP Address is wasted for its network address and other for its direct broadcasting address.

Point-02:

- Subnetting leads toward more complicated communication process as compare to without subnetting communication.

After subnetting, the communication is done through the following 4 steps

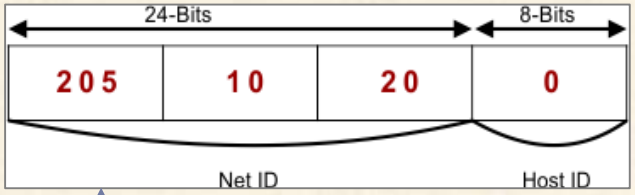
1. First Identifying the network
2. Second Identifying the sub network
3. Third Identifying the host
4. And in the last, Identifying the process

Subnetting in Classful

As we already know that, The classful subnetting is also called Fixed length subnetting. The Fixed length subnetting contain the following properties.

- Sizes of all sub networks and Subnets of all sub networks are same.
- All the sub networks have equal number of hosts.

Let understand with example,



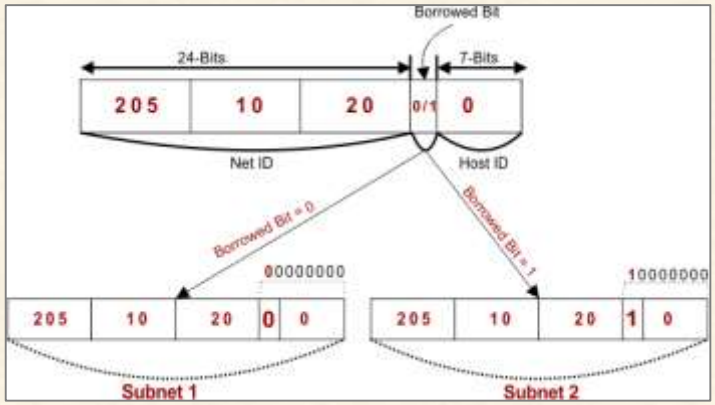
Example-01

Suppose,

- We have a big single big network having IP Address **205.10.20.0.**
- We want subnetting. So, divide this network into 2 subnets.
- As given IP belongs to Class C So, **24 bits are used for net ID and 8 bits are used for Host ID.**
- For creating two subnets (sub networks) and to represent their subnet IDs, we require **1 borrowed-bit from Host part.**

So,

- We **borrowed one bit** from the Host part.
- If borrowed **bit = 0**, then it will represent the first subnet.
- If borrowed **bit = 1**, then it will represent the second subnet.

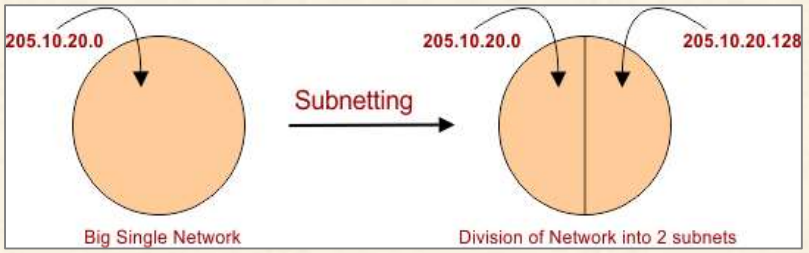


Note: After borrowing one bit, Host ID part remains with only 7 bits.

Subnetting in Classful

IP Address of the two subnets are

- 10.20.00000000 = **205.10.20.0**
- 10.20.10000000 = **205.10.20.128**



For First Subnet

- IP Address of the subnet = **205.10.20.0**
- Total number of IP Addresses = **2^7= 128**
- Total number of hosts = **128 – 2 = 126**
- Range of IP Addresses = **[205.10.20.00000000 to 205.10.20.01111111] = [205.10.20.0 to 205.10.20.127]**
- Direct Broadcast Address = **205.10.20.01111111 = 205.10.20.127**
- Limited Broadcast Address = **255.255.255.255**

For Second Subnet

- IP Address of the subnet = **205.10.20.128**
- Total number of IP Addresses = **2^7= 128**
- Total number of hosts = **128 – 2 = 126**
- Range of IP Addresses = **[205.10.20.10000000 to 205.10.20.11111111] = [205.10.20.128 to 205.10.20.255]**
- Direct Broadcast Address = **205.10.20.11111111 = 200.1.2.255**
- Limited Broadcast Address = **255.255.255.255**

Subnetting in Classful

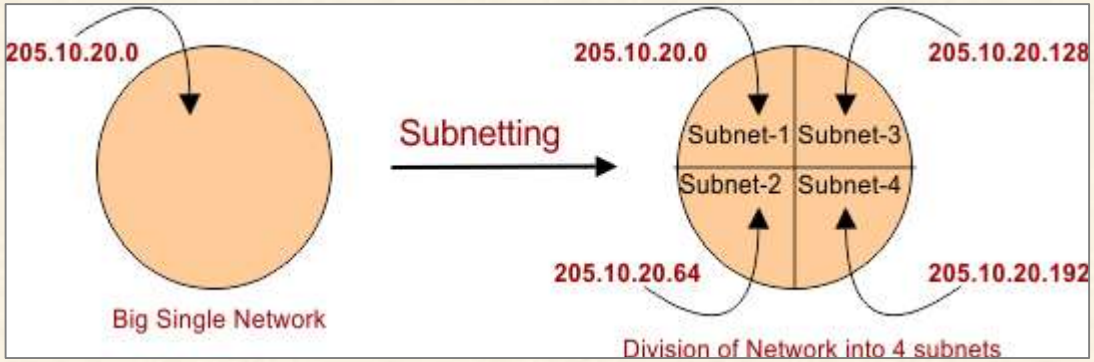
- **Important Note:** Number of subnets depends upon the number of borrowed bits. We can define this relation through the following formula.

Number of subnets = 2^n.

where "n" is number of borrowed bits. So, if number of borrowed bits are 2 then subnets will be $2^2 = 4$.

If given IP= 205.10.20.0. then first IP Address of each of four subnets are

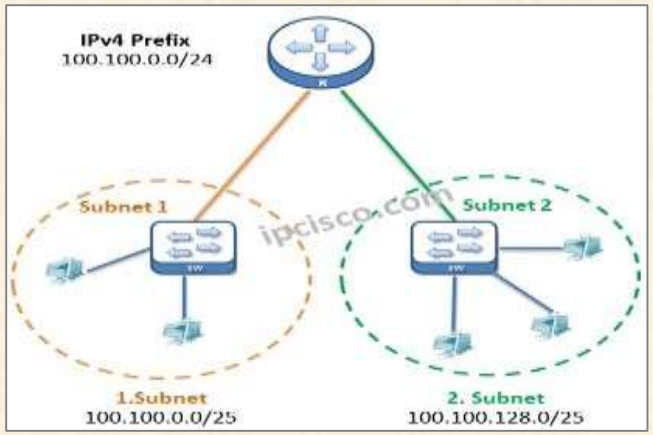
- 10.20.**00**000000 = **205.10.20.0**
- 10.20.**01**000000 = **205.10.20.64**
- 10.20.**10**000000 = **205.10.20.128**
- 10.20.**11**000000 = **20.10.20.192**



Subnetting in Classless

We have an IPv4 Prefix **100.100.0.0/24**. How can we divide this IPv4 prefix into two different subnet?

- As you can see below, we will use this **two subnets for different networks** that is connected to our router.



Firstly, lets write our IPv4 address in binary format.

- **Decimal :** 100.100.0.0/24
- **Binary :** 01100100.01100100.00000000.00000000 /24

- According to our prefix, our subnet **mask is /24.** This means that, our first **24 bits are network** and the remaining parts are host bits in this subnetting mask. Here, hosts bits are **32-24=8 bits.**
- So, to divide this network, we should **borrow some bits** from the host part. So, how many bits we will borrow? To determine this, we will check our subnet need. How many subnet do we need? For this question, we **need 2 subnets. So, we will borrow 1 bit** from host part. Why 1 bit?
- 2^0 = 1
- **2^1 = 2**

As you can see above, with **1 bit**, we can have **2 subnets** (**2^1=1**).

Subnetting in Classless

- After borrowing this address, our **network part will be 24+1=25 bits.**
- So, for these two new subnets, subnet mask will be **/25.** And **host parts will be 8-1= 7 bits.**
- To build these two subnets, we will change the borrowed bit only. We will use **0 and 1** for this borrowed bit.

As you can see below, it is the first bit of the last octet.

Original Prefix : 01100100.01100100.00000000.00000000

Original Prefix : 01100100.01100100.00000000.**0**0000000 **(Borrowed Bit)**

- **Subnet 0: 01100100.01100100.00000000.0**0000000
- **Subnet 1: 01100100.01100100.00000000.1**0000000

So, in decimal, our subnets will be like below:

- **Subnet 0 Decimal : 100.100.0.0/25**
- **Subnet 1 Decimal : 100.100.0.128/25**

Public Vs. Private IP Addresses

- Public and private IP addresses are two basic parts of your device's identity. In simple words, the **public IP address is your identity over internet and Private IP is your identity in local network** without internet.

Note: If your device is assigned private IP address, then your device will not be able to access the Internet.

Public IP address	Private IP address
1. Internet service provider (ISP) assigns and control the Public IP to any device connected with internet.	1. Private IP addresses are provided by network devices such as •Routers which using NAT (network address translation). •Mobile/EVO hotspot which using type 2 NAT
2. Public IP address also called External or Global IP.	2. Private IP address also called Internal or local IP.
3. It is required when needs to communicate outside your private network, over the internet	3. It is required when needs to communicate within your private network. Private network may involve your home or office network.
4. Public IP is a unique numeric code never reused by other devices over internet at the same time.	4. Private IP is a non-unique numeric code. It will be unique for any private network but may be reused by other devices in other private networks.
5. Finding of Public IP, Simply Type What is my IP address over Google. The desired public IP will be visible.	5. Finding of private IP is possible on your device's internal settings, by using the command of "ipconfig".
6. Public IP addresses are Not free	6. Private IP addresses are totally Free
7. Public IP addresses cannot fall within private IP address ranges.	7. Private IP addresses fall within private IP address ranges.
8. Other than reserved private IP address range are Public IP addresses **Example: 8.8.8.8.**	8. Private IP addresses Ranges Class A: **10.0.0.0 — 10.255.255.255**; Class B: **172.16.0.0 — 172.31.255.255**; Class C: **192.168.0.0 — 192.168.255.255** **Example: 10.11.12.15**

Public Vs. Private IP Addresses

Who Assigns a private IP address to our Laptops

- As we know a Private IP address may assigned to a device even it is not connected to router. Who assigns this private IP address to our device (i.e. Laptop, PC).
- Simple answer is, in such cases the **mobile acts as a router** which assigns private IP address to your connected device via WiFi.

Explain: When you enable Hotspot from mobile or EVO, it acts as a **wireless router with DHCP**. When you connect your devices (i.e. laptop) to your mobile's Hotspot, then your mobile assigns a Private IP address to your corresponding device (such as Tablet, PC, laptop's).

- DHCP of mobile hotspot has its own NAT, which is a **Type 2, B, Moderate one**. EVO WiFi also acts as **a mobile hotspot.**

NAT

Network Address Translation (NAT)

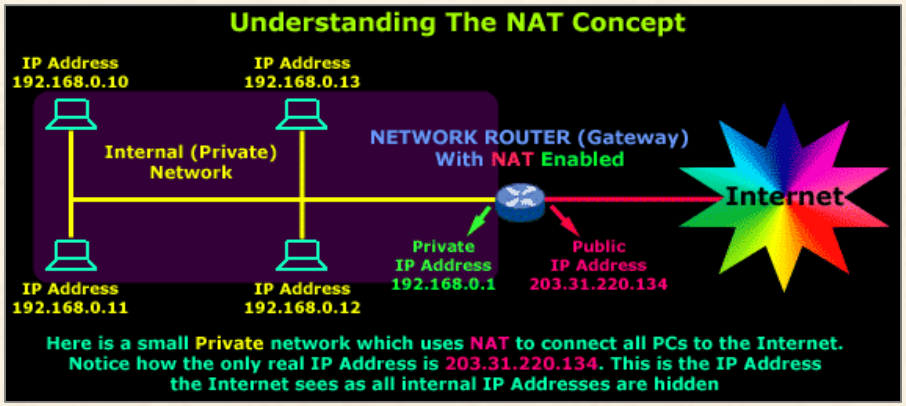
We generally have two types of IP address, which are as follows −

1. Private IP address
2. Public IP address

- **Private IP address normally used in the LAN** (Local area network) side of the Network.
- **Public IP address provided by the ISP** is configured in the WAN side of the network.
- Public IP addresses are always **paid**, while the private IP address is **free.**

Private IP addresses range as follows −

- **192.168.0.0 - 192.168.255.255 (65,536 IP addresses)**
- **172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses)**
- **10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses)**



NAT

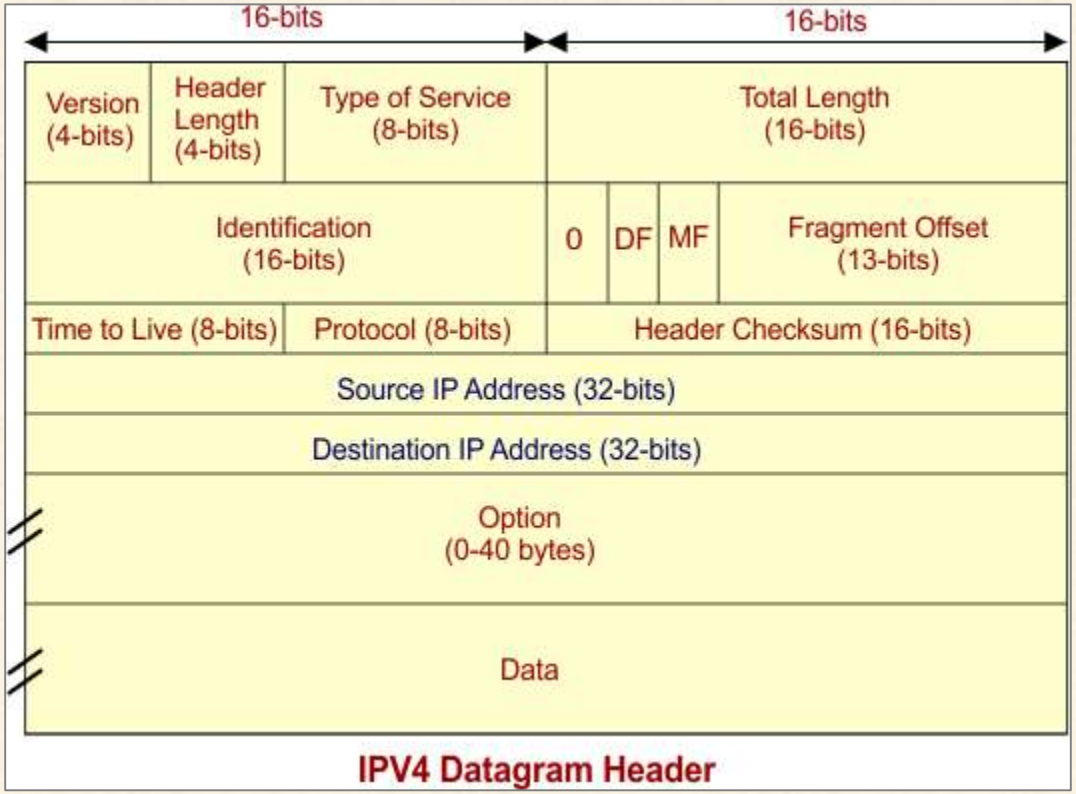
Now let us try to understand what Network Address Translation (NAT) is.

- **Step 1** − Consider you have internet provided by Internet Service Provider ABC.
- **Step 2** − So, they will give you connection to your Modem. That connection we used to call WAN.
- **Step 3** − This connection is always configured with a Public IP address.
- **Step 4** − Then, your LAN side of the MODEM is configured with a Private IP address.
- **Step 5** − That means your computer or laptop connected to the network receives a Private IP address.
- **Step 6** − As per the standard Private IP will not communicate with Public IP address at any Point of time.
- **Step 7** − To achieve this, Private IP addresses need to be translated to Public IP addresses with help of NAT.
- **Step 8** − In simple words, Network Address translation is used to translate Private IP address to Public IP address to communicate LAN side of the Device to Global Network. Network address translation can be processed in Router or Firewall.

NAT stands for network address translation. It's **a way to map multiple local private addresses to a public one before transferring the information**. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.

IPv4 Datagram Header

IPv4 Datagram Header diagram is given below



IPv4 Datagram Header

IPV4 Datagram Header Attributes

1. VERSION: Version of the IP protocol is of 4 bits. These 4 bits are always fixed as **0100 to represent 4 in decimal for IPv4.**

2. HLEN: IV4P header length is of 4 bits. The minimum value for this field is **5 and the maximum is 15 bytes.**

- header length can be calculated by the following formula

  Header length = Header length field value x 4 bits

Examples

- If header length field contains decimal value 11 (represented in binary 1011) then Header length = 11 x 4 = 44 bytes

IPv4 Datagram Header

3. Type Of Service: it is 8 bit field that is used for Quality of Service. The division of 8-bits are explained under

Precedence (3 bits)	Delay (1 bit)	Throughput (1 bit)	Reliability (1 bit)	Cost (1 bit)	Reserved (1 bit)

- **Precedence (3 bits):** First 3 bits define the precedence. Precedence means priority i.e. immediate, routine etc. If a router is congested and needs to discard a packets, it will discard packets having lowest priority first. Bits values will be 0 or 1.
- **Delay (1 bit):** if we want a minimum delay in data packets then this field will be 1 otherwise 0. It Mostly in video calling where needs no delay.
- **Throughput (1 bit):** if need highly output then its field bit will be 1 otherwise 0.
- **Reliability (1 bit):** if need highly reliability then its field bit will be 1 otherwise 0. It is used where no data loss is tolerated.
- **Cost (1 bit):** if need low cost then its field bit will be 1 otherwise 0. It requires when to select the shortest path to its destination.
- **Last bit:** is reserved for future purpose which mostly controls the congestion Notification. Congestion mean it inform to sender to minimize the speed of sending data.

IPv4 Datagram Header

4. Total Length: It is Total length of the datagram. it is a 16 bit field which can represent $2^{16} = 65536$ value . It has minimum size of 20 bytes and max value of 65535 bytes.

Total length = Header length + Payload length

5. Identification:

- It is a 16-bit field. It is helpful for the **identification of the fragments** of an original datagram.
- When an IP datagram is fragmented, each fragmented datagram is assigned the **same identification header number.**
- This header-number is useful during the **re-assembly of fragmented datagrams.**

6. Flag Bits: It use 3 flag bits

- First flag bit is **Reserved**
- Second Flag bit **(DF Bit).** DF bit stands for **Do Not Fragment bit.** DF value may be **0 or 1.**
  - When **DF value is 0** then It gives the permission to the **intermediate devices (i.e. routers) to fragment the datagram** if required.
  - When **DF value is 1** then It indicates the **intermediate devices (i.e. router) not to fragment the datagram** at any cost.
- Third flag bit is **MF.** MF bit stands for **More Fragments bit.** MF value may be 0 or 1.
  - When **MF bit value is 0** then It tells to the receiver that the **current datagram-fragment is the last fragment** and no more segment will appear of same datagram.
  - When **MF bit value is 1** then it tells more fragments are **still to come after this fragment.** MF bit is set to 1 for all the fragments except the last one.

IPv4 Datagram Header

7. Fragment Offset: Fragment Offset is a 13 bit field. It tells the **position of a fragmented datagram** in the original un-fragmented IP datagram.

Fragment offset for a given fragmented IP datagram = Number of data bytes ahead of it in the original un-fragmented IP datagram4. Hence, The 1st fragmented datagram has a fragment offset of zero.

8. Time to live: It is 8-bit field which **prevents the datagram to go to loop.** If a datagram go to loop then congestion can happens which cause the problem. So, Time to live **(TTL) avoids in such stations.**

- According to TTL, 8-bit can represent 256 nodes. Therefore, datagram is self-loop can goes to 256 nodes, when datagram goes to a node, it is decremented by 1 in values. As the value reaches 0, the datagram is terminated.

9. Protocol: it is **an 8-bit number that defines what protocol is used inside the IP packet**. TCP, UDP, ICMP or IGMP protocols can be filtered on, although they are most common**. Protocol number of ICMP is 1 (in binary 00000001), IGMP is 2 (in binary 00000010), TCP is 6 and UDP is 17.**

10. Header Checksum: it is a 16 bits field. It is used for **checking errors in the datagram header**. At receiving end, it is used to **know that receiving data is corrupted or not** because data can lose or corrupt while passing through the network.

11. Source IP address: 32 bits IP address of the sender

12. Destination IP address: 32 bits IP address of the receiver

13. Option: Due to options field, datagram-header-size can be of variable length (20 bytes to 60 bytes). Optional information include as source route etc.

IPv4 Datagram Header

- Here's a real life example of an IP packet in Wireshark where you can see how these fields are used:

```
Internet Protocol Version 4, Src: 192.168.82.147 (192.168.82.147), Dst: 192.243.232.2 (192.243.232.2)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
    Total Length: 1155
    Identification: 0x69de (27102)
  Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  Header checksum: 0xd064 [validation disabled]
      [Good: False]
      [Bad: False]
    Source: 192.168.82.147 (192.168.82.147)
    Destination: 192.243.232.2 (192.243.232.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
+ Transmission Control Protocol, Src Port: 57487 (57487), Dst Port: 80 (80), Seq: 1102, Ack: 883, Len: 1115
```

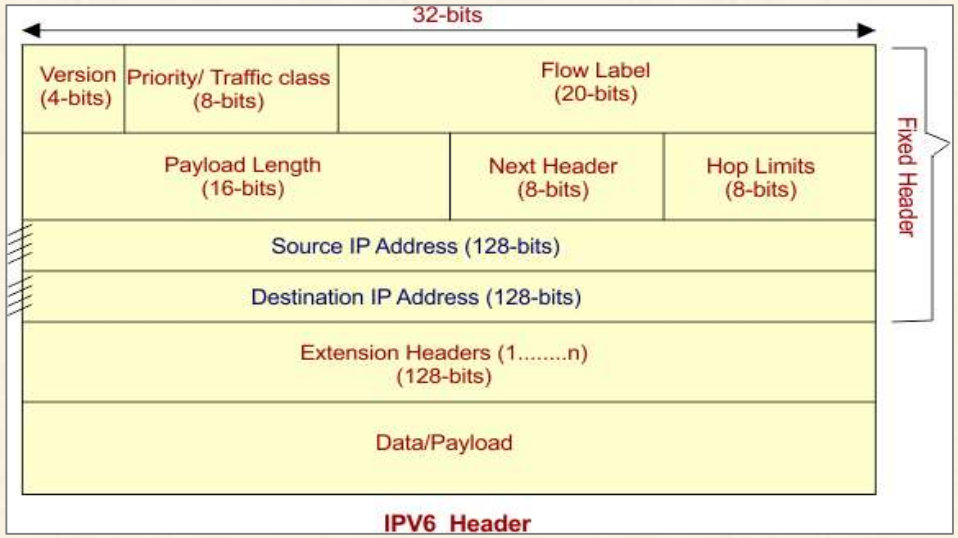
IPv6 Datagram Header

IPV6 is also a datagram and connectionless service like IPV4. But its **size and functionality** of working is a bit difference than IPV4.

IPv6 headers have **one Fixed Header and zero or more Optional** Headers.

- **Fixed header** is also called **base header**. It is the compulsory part of IPV6 header. All the **necessary information** which are compulsory for a router is kept in the Fixed Header. IPv6 fixed header is 40 bytes (320 bits) long.
- **Optional Headers** are also called **Extension Headers.** The optional Header holds some extra (optional) information that helps routers to understand how to **handle a packet or flow control**. With 40 bytes of fixed header, some extension headers can also be used which may increase the size of packet.

IPV6 Header contains the following information.



IPv6 Datagram Header

1. Version: **it is a** 4-bit field. It represents version IPV6 in binary **0110 (6).**

2. Traffic Class: **it is** 8-bits filed which also known as **priority**. These 8 bits are divided into two parts.

- The most significant **6 bits are used for Type of Service**. it replaces IPv4's 'type of service' field. It's basic purpose is to provide quality of service (QoS).
- The least significant **2 bits handles the packets in Congestion** (i.e. loop). Instead of dropping packets, last 2-bits use **Explicit Congestion Notification** (ECN) to handle the packets.

3. Flow Label: **it is** 20-bits field. It uses the **virtual circuit** for data transmission. In this way sequential flow of the packets is maintained belonging to a datagram. This field avoid to re-ordering of data packets because all data travel in a **single path**. It is designed for streaming/real-time media.

4. Payload Length: **It is** 16-bits field. It tells the routers about the size of payload which belongs to a particular packet. With 16 bits, up to 65535 bytes can be indicated of data.

IPv6 Datagram Header

5. Next Header: it is 8-bits field. It tells the type of **Extension Header** which are additionally used with base header to send more data or information's. Some extension headers are given below

Extension Header	Next Header Vaule	Description
Hop-by-Hop Options header	0	Read by all devices in transit network
Routing Header	43	Contains method to support making routing decision
Fragment Header	44	contains parameters of datagram fragmentations
Destination Options Header	60	Read by destination Device
Authentication Header	51	Information Regarding Security
Encapsulating security payload Header	50	encryption informations

- If extension header is used along with payload, then corresponding bits value is presented in this filed. It mean if **Routing header is used as extension header then 43(in bits)** is represented in Next header (8bit) field.

Note: Extension headers are optional, and are used if needed.

6. Hop Limit: it is 8-bits field. This field is used **to stop packet to loop** in the network infinitely. This is same as TTL in IPv4. The Hop-Limit field value is **decremented by 1 as it passes a link** (i.e. router). When the value of Hop-limit field reaches 0 the packet is discarded.

IPv6 Datagram Header

7. Source Address: (128-bits): This field indicates the address of originator of the packet.

8. Destination Address: (128-bits): This field provides the address of intended recipient of the packet.

9. This is the payload portion of the IPv6 packet.

Note: We can say that an IPv6 address (128 bits) is 4 times larger than IPv4 (32bit) address but base header (40bytes) of an IPv6 is only 2 times larger than that of IPv4 header (20bytes).

IPv6 Packet Contains

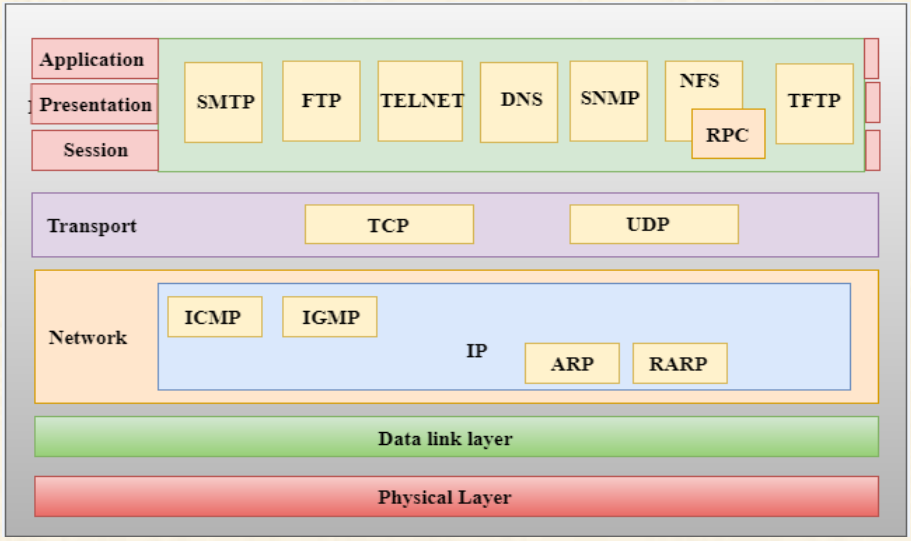
- base header
- may contains zero, one or more extension headers
- Data, needs to transfer

Network Layer/IP Protocols

What is IP?

- IP stands for **internet protocol**. It is a protocol defined in the TCP/IP model used for sending the packets from source to destination. The main task of IP is to **deliver the packets from source to the destination based on the IP addresses** available in the packet headers. IP defines the **packet structure that hides the data** which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.
- An IP protocol provides the connectionless service, which is accompanied by two transport protocols, i.e., TCP/IP
- **and UDP/IP,** so internet protocol is also known as TCP/IP or UDP/IP.
- The first version of **IP (Internet Protocol) was IPv4. After IPv4, IPv6 came into the market**, which has been increasingly used on the public internet since 2006.

TCP/IP supports the following protocols



Network Layer/IP Protocols

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as **IP addresses**. The IP addresses are used by the internet and higher layers to identify the device and to **provide internetwork routing.**
- **Host-to-host communication:** It **determines the path** through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it **encapsulates the data into message known as IP datagram.**
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as **Maximum Transmission unit (MTU)**. If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the **datagram into smaller units** so that they can travel over the local network. **Fragmentation can be done by the sender** or intermediate router. At the receiver side, all the **fragments are reassembled** to form an original message.
- **Routing:** When IP datagram is sent over the **same local network** such as LAN, MAN, WAN, it is known as **direct delivery.** When source and destination are on the distant network, then the IP datagram is **sent indirectly**. This can be accomplished by **routing the IP datagram** through various devices such as routers.

Address Resolution Protocol

ARP

ARP stands for **Address Resolution Protocol.**

- It is used to associate an **IP address with the MAC address.**
- Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the **MAC address for communication on a local area network**. MAC address can be changed easily.
- For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to **find the MAC address of the node when an internet address is known**.

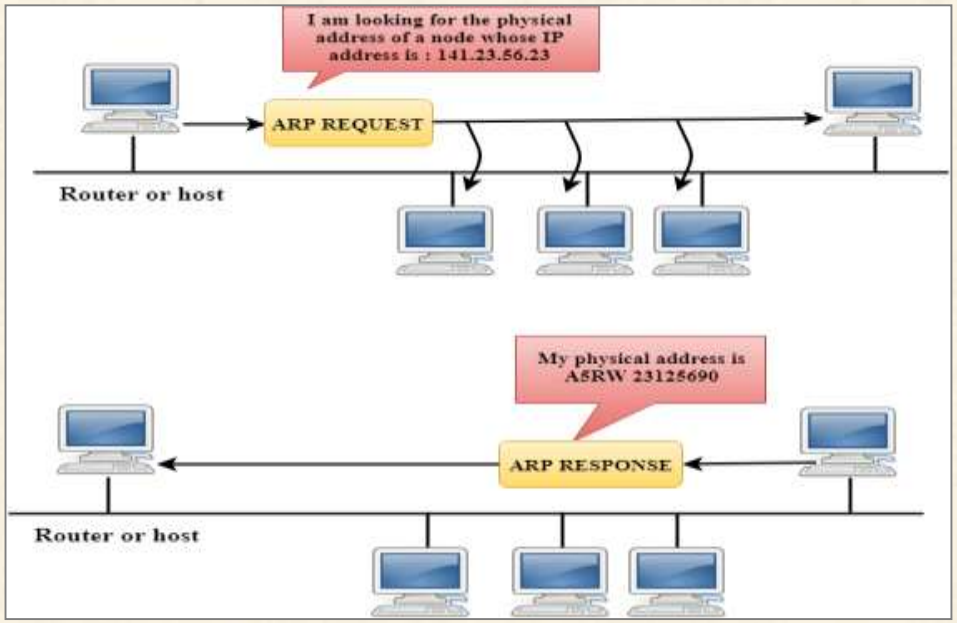
How ARP works

- If the host wants to know the physical address of another host on its network, then it sends an **ARP query packet** that includes the **IP address and broadcast it** over the network.
- Every host on the network receives and processes the ARP packet, but **only the intended recipient recognizes the IP address** and sends back the physical address.
- The host holding the datagram **adds the physical address to the cache memory and to the datagram header,** then sends back to the sender.

Address Resolution Protocol

How ARP works

- If the host wants to know the physical address of another host on its network, then it sends an **ARP query packet** that includes the **IP address and broadcast it** over the network.
- Every host on the network receives and processes the ARP packet, but **only the intended recipient recognizes the IP address** and sends back the physical address.
- The host holding the datagram **adds the physical address to the cache memory and to the datagram header,** then sends back to the sender.

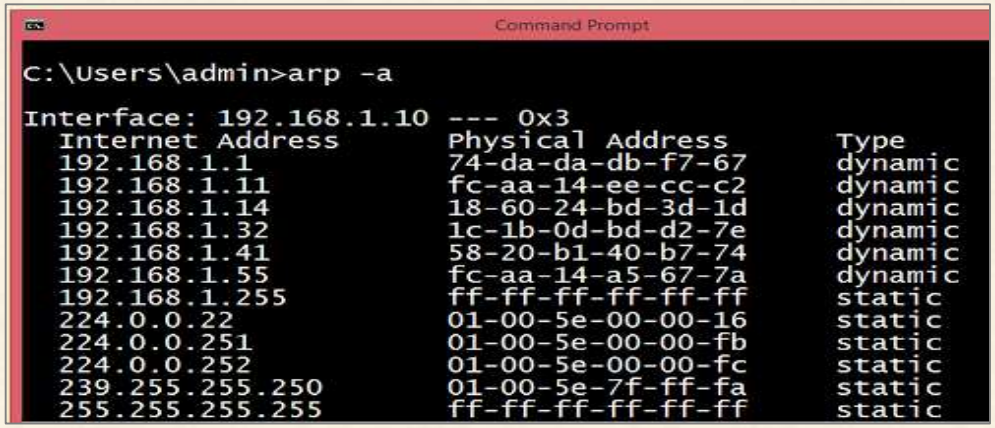


Address Resolution Protocol

Steps taken by ARP protocol

If a device wants to communicate with another device, the following steps are taken by the device:

- The device will first look at its **internet list, called the ARP cache** to check whether an IP address contains a matching MAC address or not. It will check the ARP cache in command prompt by using a command **arp -a**.
- If ARP cache is empty, then device **broadcast the message to the entire network** asking each device for a matching MAC address.
- The device that has the matching IP address **will then respond back** to the sender with its MAC address
- Once the MAC address is received by the device, then the **communication can take place** between two devices.
- If the device receives the MAC address, then the **MAC address gets stored in the ARP cache**. We can check the ARP cache in command prompt by using a command arp -a.



Address Resolution Protocol

There are two types of ARP entries:

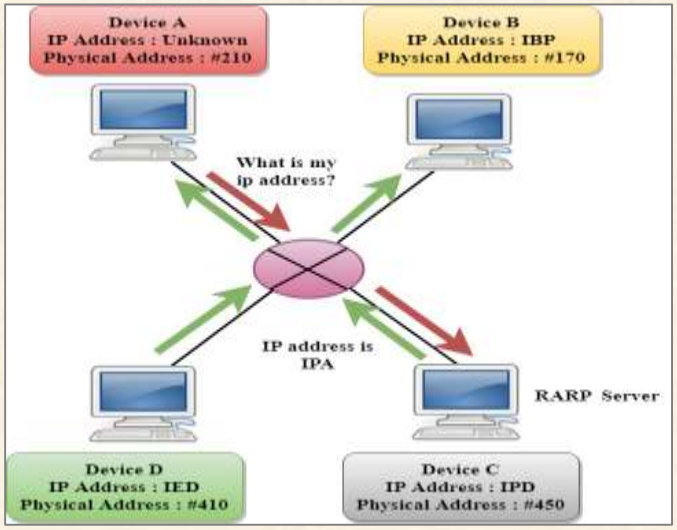
- **Dynamic entry:** It is an entry which is **created automatically when the sender broadcast its message** to the entire network. Dynamic entries are not permanent, and they are removed periodically.

- **Static entry:** It is an entry where someone **manually enters the IP to MAC address association** by using the ARP command utility.

Reverse Address Resolution Protocol

RARP

- RARP stands for **Reverse Address Resolution Protocol**.
- If the host wants to know its IP address, then it **broadcast the RARP query packet** that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and **responds back with the host IP address.**
- The protocol which is used to obtain the IP address from a server is known as **Reverse Address Resolution Protocol**.
- The message format of the RARP protocol is similar to the ARP protocol.
- Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

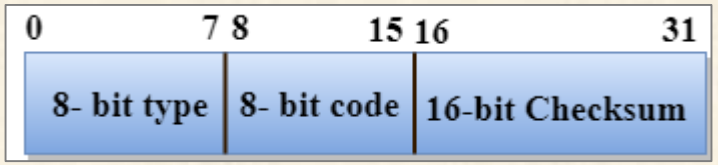


Internet Control Message Protocol

ICMP

- ICMP stands for **Internet Control Message Protocol.**
- The ICMP is a network layer protocol used by hosts and routers to send the **notifications of IP datagram problems back to the sender.**
- ICMP uses echo **test/reply** to check whether the destination is reachable and responding.
- ICMP handles both **control and error messages,** but its main function is to **report the error** but not to correct them.
- An IP datagram contains the addresses of both source and destination, but it **does not know the address of the previous router** through which it has been passed. Due to this reason, ICMP can only **send the messages to the source,** but not to the immediate routers.
- ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned back to the user processes.
- ICMP messages are transmitted within IP datagram.

The Format of an ICMP message.



- The first field specifies the type of the message.
- The second field specifies the reason for a particular message type.
- The checksum field covers the entire ICMP message.

Internet Control Message Protocol

Error Reporting

- ICMP protocol reports the error messages to the sender.

Five types of errors are handled by the ICMP protocol:

- **Destination unreachable:** The message of "Destination Unreachable" is sent **from receiver to the sender** when destination cannot be reached, or packet is discarded when the destination is not reachable.
- **Source Quench:** The purpose of the source quench message is **congestion control.** The message sent from the congested router to the source **host to reduce the transmission rate.** ICMP will take the IP of the discarded packet and then add the source quench message to the IP datagram to inform the source host to reduce its transmission rate. The source host will **reduce the transmission rate** so that the router will be free from congestion.
- **Time Exceeded:** Time Exceeded is also known as **"Time-To-Live".** It is a parameter that defines how **long a packet should live** before it would be discarded.
- **Parameter problems:** When a router or host discovers **any missing value in the IP datagram,** the router discards the datagram, and the "parameter problem" message is **sent back to the source host.**
- **Redirection:** Redirection message is generated when host consists of a **small routing table.** When the host consists of a **limited number of entries** due to which it sends the datagram to a wrong router. The router that receives a datagram will **forward a datagram to a correct** router and also sends the "Redirection message" to the host to update its routing table.

Internet Group Message Protocol

IGMP

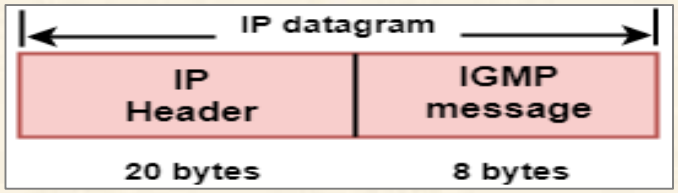
- IGMP stands for **Internet Group Message Protocol**.

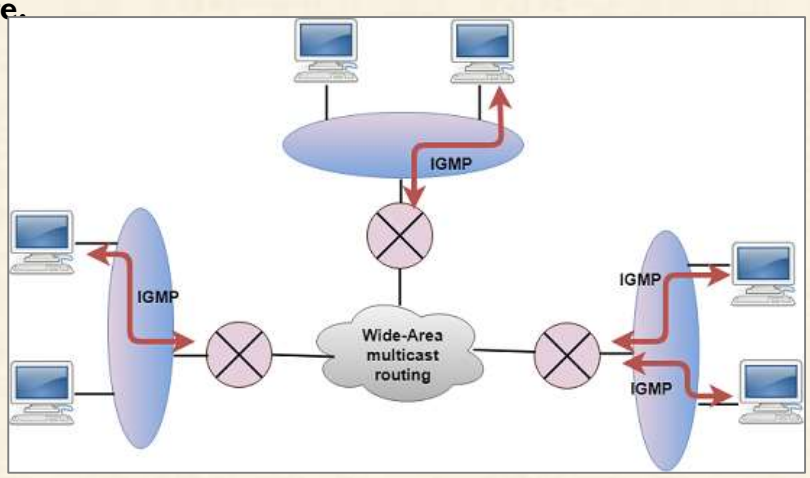
The IP protocol supports two types of communication:

- **Unicasting:** It is a communication between one sender and one receiver. Therefore, we can say that it is **one-to-one** communication.
- **Multicasting:** Sometimes the sender wants to send the same message to a large number of receivers simultaneously. This process is known as multicasting which has **one-to-many** communication.

- The IGMP protocol is used by the hosts and router **to support multicasting.**
- The IGMP protocol is used by the hosts and router to identify the **hosts in a LAN that are the members of a group.**

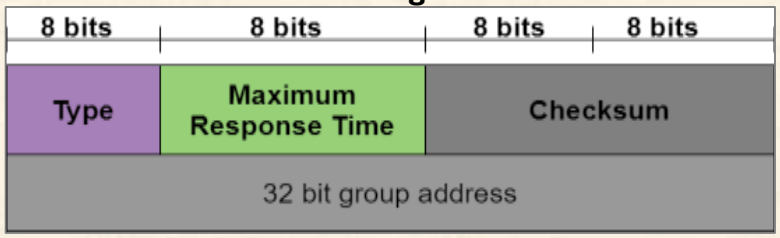
- IGMP is a part of the IP layer, and IGMP has a **fixed-size message**.
- The IGMP message is **encapsulated within** an IP datagram.





Internet Group Message Protocol

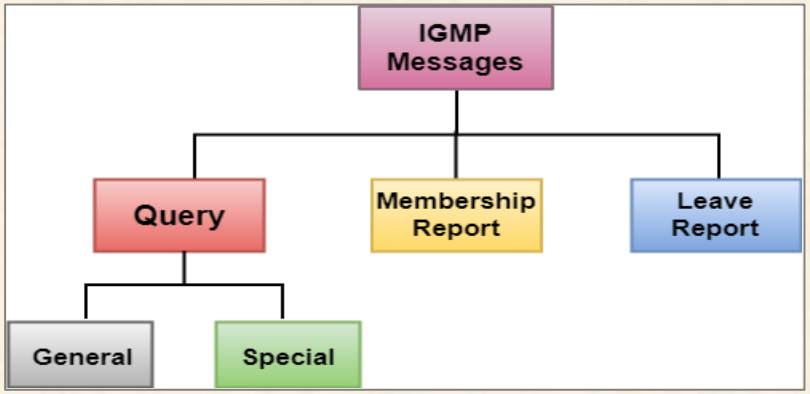
The Format of IGMP message



Type	Value
General or Special Query	0x11 or 00010001
Membership report	0x16 or 00010110
Leave Report	0x17 or 00010111

Where,

- **Type:** It determines the type of IGMP message. There are three types of IGMP message: **Membership Query, Membership Report and Leave Report.**
- **Maximum Response Time:** This field is used only by the Membership Query message. It determines the **maximum time the host can send the Membership Report message** in response to the Membership Query message.
- **Checksum:** It determines the **entire payload of the IP datagram** in which IGMP message is encapsulated.



Network Layer/IP Protocols

Membership Query message

- This message is sent by a **router to all hosts** on a local area network to determine the set of all the multicast groups that have been joined by the host.
- It also determines whether a specific **multicast group has been joined by the hosts** on a attached interface.

Membership Report message

- The host **responds to** the membership query message with a membership report message.
- Membership report messages can also be generated by the host when a **host wants to join the multicast group** without waiting for a membership query message from the router.
- Membership report messages are **received by a router as well as all the hosts** on an attached interface.

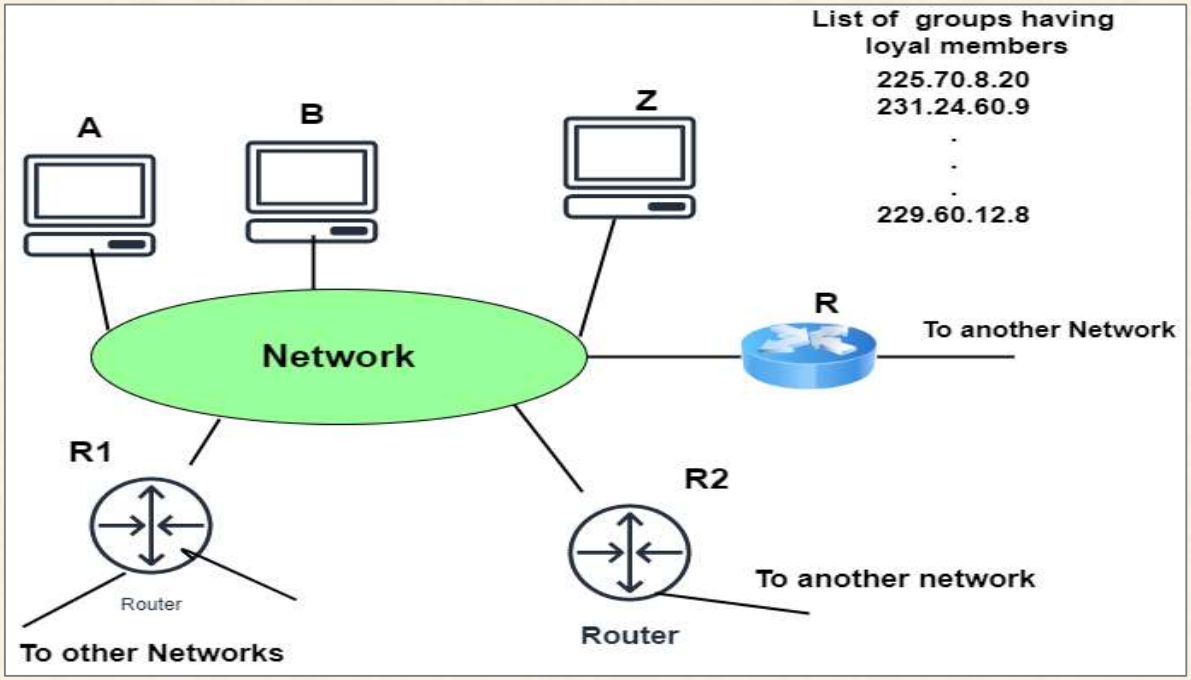
Leave Report

- When the host does not send the **"Membership Report message"**, it means that the **host has left the group.** The host knows that there are no members in the group, so even when it receives the next query, it would not report the group.

Internet Group Message Protocol

IGMP Operation

- The Internet Group Management Protocol operates locally. The Multicast router that is connected to the network mainly has a **list of multicast addresses of the group with at least one loyal member** in that network. And for each group, there is mainly one router that has the duty of distributing the multicast packets destined for that group.
- This simply indicates that in the case if there are three multicast routers connected to a network then their list of **groupids** are **mutually exclusive.**



Network Layer/IP Protocols

Given below are the operations of IGMP:

Joining a Group

- In this operation, both the host and the router can join a group. Whenever a process on the **host wants to join a group then it simply sends the request to the host**. After that, the host then adds the name of the process and the name of the group to its list.
- In case, if this is the first entry of that particular group, then the **host sends the membership report message** to the multicast router of the group.
- And if the entry is not the first entry then there is no need of sending such a message.

Leaving a group

- Whenever the host finds that there is **no process that is interested** in the group then it mainly leaves a report message.
- The membership is not disinfected by the multicast router of the group, rather than it immediately transmits the query packets repeatedly to see if anyone is still interested or not.
- And in case if it gets the response in the form of a membership report message then the membership of the host or network is preserved.

Monitoring Membership Mainly the general query message **does not define** a particular group.

Delayed Response In order to prevent unnecessary traffic, the IGMP mainly makes use of a **delayed response strategy.**

Routing Protocols/Algorithms

Routing

- A Routing is a process of **selecting path along which the data can be transferred** from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the **information available in the packet header and forwarding table.**
- The routing algorithms are used for routing the packets. The **routing algorithm** is nothing but a software responsible for **deciding the optimal path** through which packet can be transmitted.
- The **routing protocols** use the metric to **determine the best path** for the packet delivery. The metric is the standard of measurement such as **hop count, bandwidth, delay, current load on the path,** etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm **initializes and maintains the routing table** for the process of path determination.

Routing Metrics & Costs

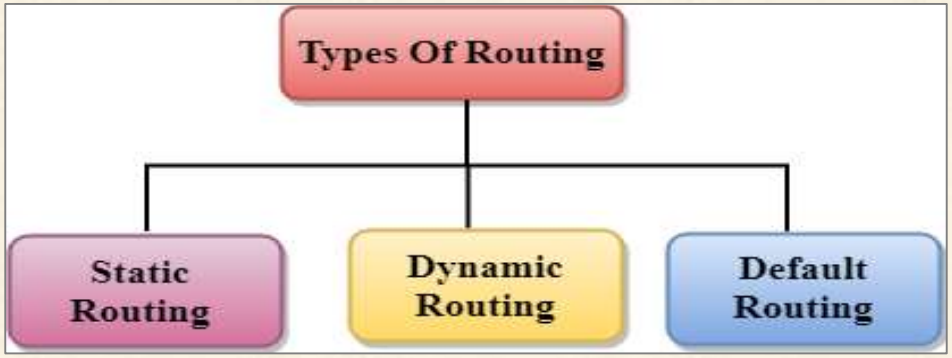
- Routing **metrics and costs** are used for determining the best route to the destination. The **factors** used by the protocols to **determine the shortest path,** these factors are known as a metric.
- Metrics are the network variables used to determine the best route to the destination. For some protocols use the **static metrics** means that their value cannot be changed and for some other routing protocols use the **dynamic metrics** means that their value can be assigned by the system administrator.

The most common metric values are given below:

1. **Hop count:** Hop count is defined as a metric that specifies the **number of passes through internetworking devices** such as a router, a packet must travel in a route to move from source to the destination.
2. **Delay:** It is a **time taken by the router** to process, queue and transmit a datagram to an interface.
3. **Bandwidth:** The **capacity of the link** is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a **higher transfer rate** like gigabit is preferred over the link
4. **Load:** Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as **CPU utilization, packets processed per second**. If the traffic increases, then the load value will also be increased.
5. **Reliability:** Reliability is a metric factor may be composed of a **fixed value.** It depends on the **network links, and its value** is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links.

Routing Types

Routing can be classified into three categories:



Static Routing

- Static Routing is also known as **Non-adaptive Routing.**
- It is a technique in which the **administrator manually adds** the routes in a routing table.
- A Router can send the packets for the destination along the **route defined by the administrator.**
- In this technique, **routing decisions are not made** based on the condition or topology of the networks

Routing Types

Default Routing

- Default Routing is a technique in which a router is **configured to send all the packets to the same hop device**, and it doesn't matter whether it belongs to a particular network or not. A **Packet is transmitted to the device for which it is configured** in default routing.
- Default Routing is used when networks deal with the **single exit point.**
- It is also useful when the bulk of transmission networks have to transmit the data to the **same hop device.**
- When a **specific route** is mentioned in the routing table, the router will choose the **specific route rather than the default route.** The default route is chosen only when a specific route is not mentioned in the routing table.

Dynamic Routing

- It is also known as **Adaptive Routing.**
- It is a technique in which a router **adds a new route in the routing table** for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to **discover the new routes** to reach the destination.
- In Dynamic Routing, **RIP and OSPF** are the protocols used to discover the new routes.
- If any route goes down, then the **automatic adjustment** will be made to reach the destination.

The Dynamic protocol should have the following features:

- All the routers must have the **same dynamic routing protocol** in order to exchange the routes.
- If the router discovers any change in the condition or topology, then **router broadcast this information** to all other routers.

Routing Algorithms

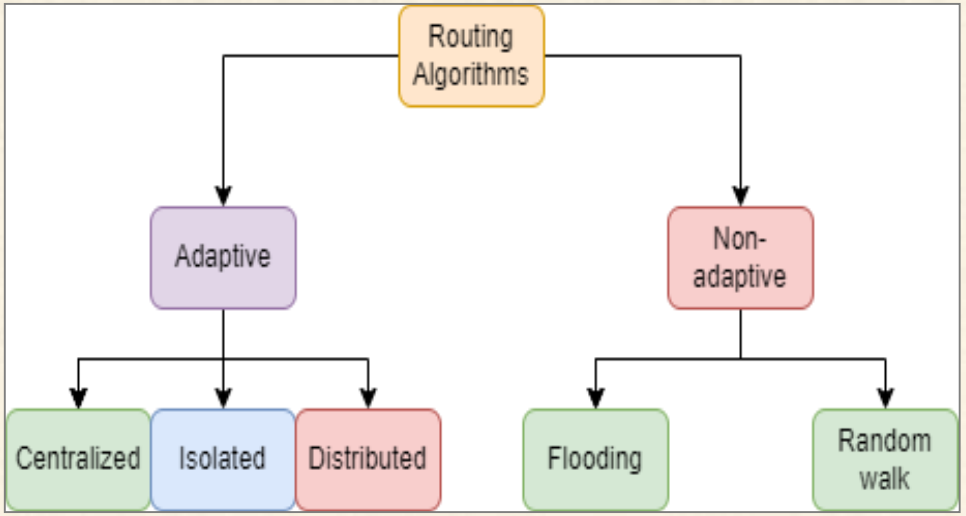
Routing algorithm

- In order to transfer the packets from source to the destination, the network layer must determine the **best route** through which packets can be transmitted.
- Whether the network layer provides **datagram service or virtual circuit service,** the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best **path from the source to the destination**. The best path is the path that has the **"least-cost path"** from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

1. **Adaptive Routing algorithm**
2. **Non-adaptive Routing algorithm**



Adaptive Routing Alg

Adaptive Routing algorithm

- An adaptive routing algorithm is also known as **Dynamic routing algorithm.**
- This algorithm makes the routing decisions based on the **topology and network traffic.**
- The main parameters related to this algorithm are **hop count, distance and estimated transit time.**

An adaptive routing algorithm can be classified into three parts:

1. **Centralized algorithm:** It is also known as global routing algorithm as it computes the **least-cost path** between source and destination by using **complete and global knowledge about the network.** This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. **Link state algorithm** is referred to as a centralized algorithm since it is aware of the cost of each link in the network.
2. **Isolation algorithm:** It is an algorithm that obtains the routing information by **using local information** rather than gathering information from other nodes.
3. **Distributed algorithm:** It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an **iterative and distributed manner.** In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an **iterative process of calculation computes the least-cost path** to the destination. A Distance vector algorithm is a decentralized algorithm as it **never knows the complete path** from source to the destination, instead it knows the **direction through which the packet is to be forwarded** along with the least cost path.

Non-Adaptive Routing Alg

Non-Adaptive Routing algorithm

- Non Adaptive routing algorithm is also known as a **static routing algorithm.**
- When **booting up** the network, the routing **information stores to the routers.**
- Non Adaptive routing algorithms **do not take the routing decision** based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

1. Flooding: In case of flooding, every **incoming packet is sent to all the outgoing links** except the one from it has been reached.

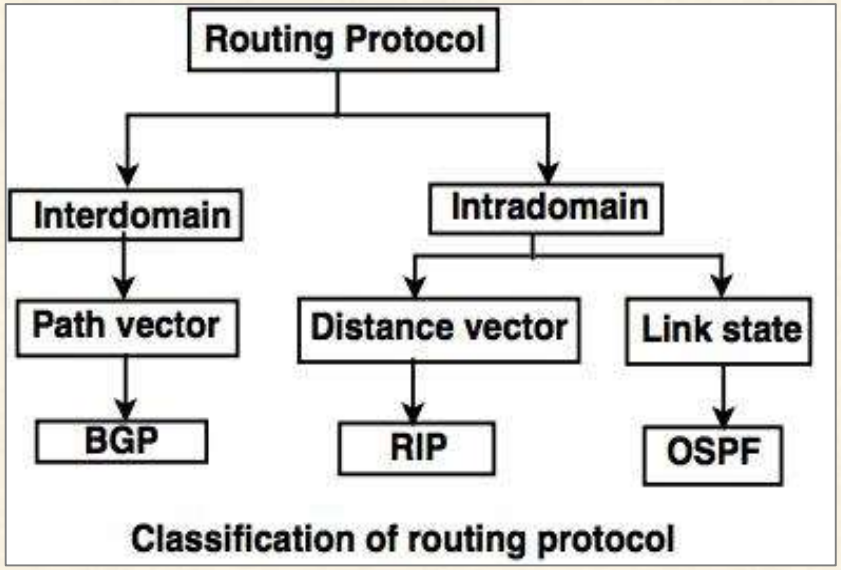
The disadvantage of flooding is that node may contain several copies of a particular packet.

2. Random walks: In case of random walks, a packet sent by the **node to one of its neighbour's randomly**.

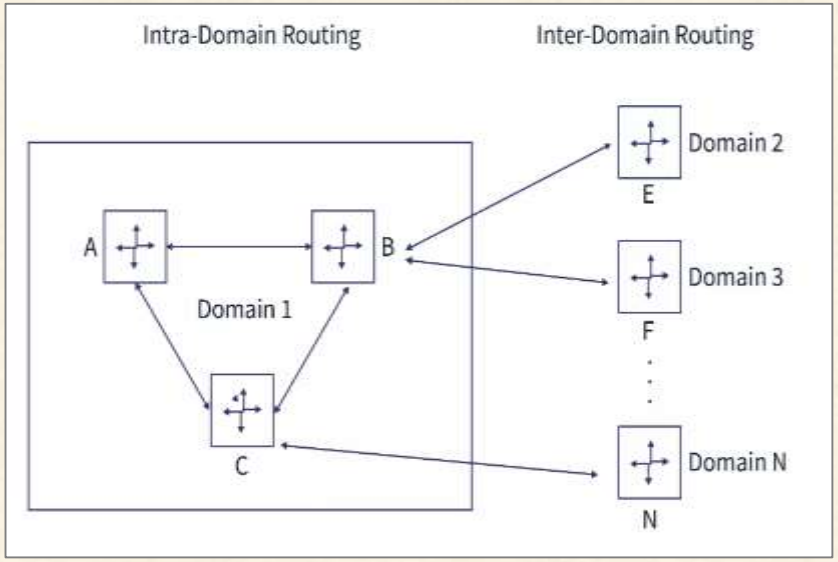
An advantage of using random walks is that it uses the alternative routes very efficiently.

Routing Protocols

- Routing is the process of choosing a **path for transferring data** from a source to a destination. Routing is performed using devices called routers.
- In order to send the packet by determining the **best route** from one network to another, routing is carried out at the network layer. The network layer primarily makes sure that each packet arrives at its intended destination from the point of origin.
- **Intra-domain** and **Inter-domain routing**, the basic difference between the two is that inter-domain **routing operates both within and across domains** (a domain is a set of devices in a network that communicate and share data among each other), whereas intra-domain **routing operates only within a domain.**



Classification of routing protocol



Inter Vs Intra Domain

Inter-domain Routing

- Inter-domain Routing is the protocol in which the routing algorithm works **both within and between domains**. Domains must be connected in some way, for hosts inside one domain to exchange data with hosts in other domains.
- This connection within domains is governed by the inter-domain routing protocols. This is often done using the ***Border Gateway Protocol (BGP).***
- It is used in ***Path Vector Routing*** using which inter-domain routing is performed. In path vector routing, the **routing depends on the analysis of the path** from the nodes in the current domain to the node in the other domain, and **not on the distance between nodes.**

Intra-domain Routing

- Intra-domain Routing is the routing protocol that **operates only within a domain.**
- In other words, intra-domain routing protocols are used to route packets within a specific domain, such as within an institutional network for e-mail or web browsing.
- Unlike inter-domain routing protocols, it doesn't communicate with other domains.

There are two types of protocols used for intra-domain routing:

1. **Distance Vector Routing (uses Routing Information Protocol or RIP)**
2. **Link State Routing (uses Open Shortest Path First or OSPF)**

Intra-Domain Routing

There are two types of protocols used for intra-domain routing:

1. Distance Vector Routing (uses Routing Information Protocol or RIP)

- In ***distance vector routing***, each node in a domain **stores information about its neighbouring nodes.**
- The information is stored in a table known as a **routing table,** which is maintained by each node in the domain.
- RIP is one of the earliest distance-vector routing protocols, and it **uses hop count as a routing statistic.** By placing a cap on the **maximum number of hops** that may be taken between a source and a destination, RIP avoids routing loops.

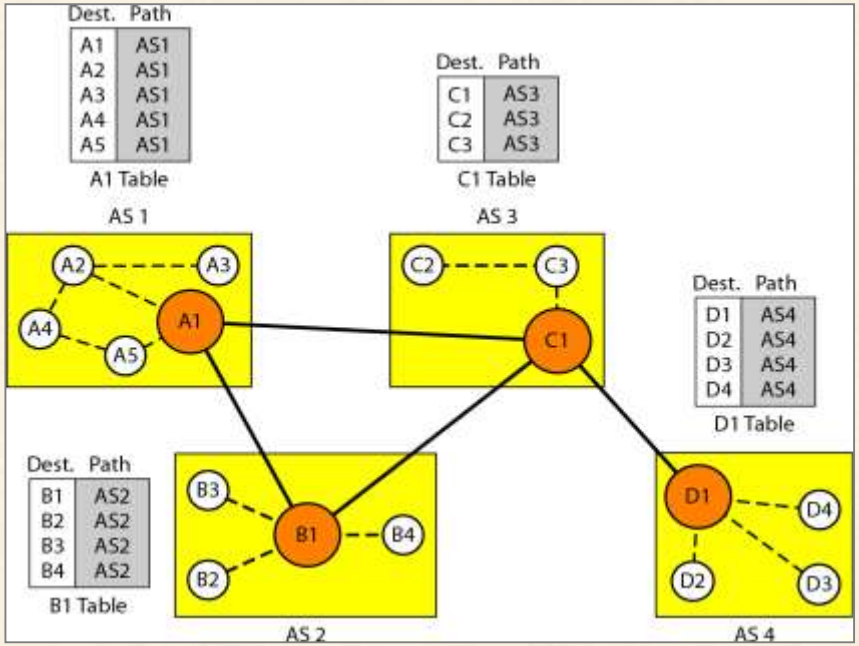
2. Link State Routing (uses Open Shortest Path First or OSPF)

- In ***link state routing,*** each node in a domain stores information about **all the other nodes in the domain,** in other words, the routing table of each node stores **information about the entire topology of the domain.**
- Since each node has all the information about the domain at its disposal, ***Dijkstra's algorithm*** is used to calculate the best routing path. This is possible due to OSPF, and this is also its advantage.

Inter Domain Routing

Path Vector Routing

1. Path Vector Routing is a routing algorithm of network layer, and it is useful for **inter-domain routing.**
2. The principle of path vector routing is similar to that of distance vector routing. It assumes that there is one node in each autonomous system that **acts on behalf of** the entire autonomous system is called **Speaker node.**
3. The speaker node in an AS **creates a routing cable and advertises** to the speaker node in the neighbouring ASs .
4. A speaker node **advertises the path**, not the metrics of the nodes, in its autonomous system or other autonomous systems.



Dest.	Path
A1	AS1
...	
A5	AS1
B1	AS1-AS2
...	...
B4	AS1-AS2
C1	AS1-AS3
...	...
C3	AS1-AS3
D1	AS1-AS2-AS4
...	...
D4	AS1-AS2-AS4

A1 Table

Dest.	Path
A1	AS2-AS1
...	
A5	AS2-AS1
B1	AS2
...	...
B4	AS2
C1	AS2-AS3
...	...
C3	AS2-AS3
D1	AS2-AS3-AS4
...	...
D4	AS2-AS3-AS4

B1 Table

Dest.	Path
A1	AS3-AS1
...	
A5	AS3-AS1
B1	AS3-AS2
...	...
B4	AS3-AS2
C1	AS3
...	...
C3	AS3
D1	AS3-AS4
...	...
D4	AS3-AS4

C1 Table

Dest.	Path
A1	AS4-AS3-AS1
...	
A5	AS4-AS3-AS1
B1	AS4-AS3-AS2
...	...
B4	AS4-AS3-AS2
C1	AS4-AS3
...	...
C3	AS4-AS3
D1	AS4
...	...
D4	AS4

D1 Table

Inter Domain Routing

- It is the initial table for each speaker node in a system made four ASs. Here **Node A1 is the speaker node for AS1, B1 for AS2, C1 for AS3 and D1 for AS4**, Node A1 creates an initial table that shows A1 to A5 and these are located in AS1, it can be reached through it.
- A speaker in an autonomous system **shares its table with** immediate neighbours, here Node **A1 share its table with nodes B1 and C1**, Node C1 share its table with nodes A1,B1 and D1, Node B1 share its table with nodes A1 and C1 , Node D1 share its table with node C1.
- If router A1 receives a packet for nodes A3 , it knows that the path is in AS1,but if it receives a packet for D1,it knows that the packet should go from AS1,to AS2 and then to AS3 ,then the routing table shows that path completely on the other hand **if the node D1 in AS4 receives a packet for node A2,it knows it should go through AS4,AS3,and AS1.**

FUNCTIONS

1. **Prevention Of Loop**
2. **Policy Routing**
3. **Optimum Path**

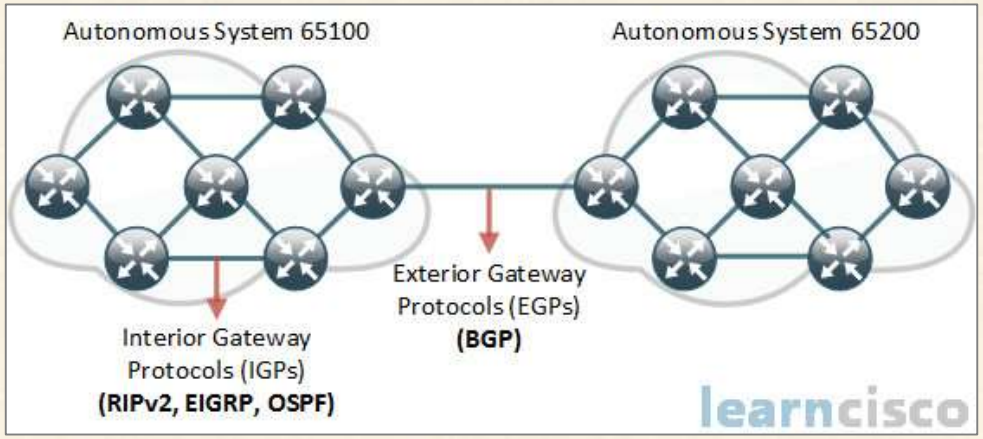
Inter Domain Routing

FUNCTIONS

1. **PREVENTION OF LOOP-** The creation of **loop can be avoided** in path vector routing .A router receives a message it checks to see if its autonomous system is in the path list to the destination if it is looping is involved and the message is ignored
2. **POLICY ROUTING-** When a router receives a messages it can check the path, if one of the **autonomous system listed in the path against its policy, it can ignore its path** and destination it does not update its routing table with this path or it does not send the messages to its neighbours.
3. **OPTIMUM PATH -** A path to a destination that is the **best for the organization** that runs the autonomous system

Border Gateway Protocol

- BGP stands for **Border Gateway Protocol**. It is a standardized gateway protocol that exchanges routing information across autonomous systems (AS). When one network **router is linked to other networks, it cannot decide which network is the best** network to share its data to by itself.
- Border Gateway Protocol considers all peering partners that a router has and **sends traffic to the router closest to the data's destination.** This communication is possible because, at boot, BGP allows peers to communicate their **routing information and then stores that information in a Routing Information Base (RIB).**
- The main goal of BGP is to find any path to the destination that is **loop-free.** This is different from intra-domain routing protocols' common goals: finding an optimal route to the destination based on a specific link metric.
- The routers that connect other ASs are called border gateways. The task of the border gateways is to forward packets between ASs. Each AS has at least one **BGP speaker**. BGP speakers exchange reachability information among ASs.



Border Gateway Protocol

The types of BGP are as follows –

Internal BGP

- Routes are exchanged, and traffic is transmitted over the Internet using external BGP or eBGP. Autonomous systems can also use an internal BGP version to **route through their internal networks**, known as internal BGP.
- It should be noted that using internal BGP is NOT a requirement for using external BGP. Autonomous systems can choose from several internal protocols to connect the routers on their internal network.

External BGP

- External BGP is like international shipping; some specific standards and guidelines need to be followed when shipping a piece of mail internationally. Once that piece of mail reaches its destination country, it has to go through its local mail service to reach its final destination.

Distance Vector Routing Alg.

The Distance vector algorithm is iterative, asynchronous and distributed.

- **Distributed:** It is distributed in that each node receives information from one or more of its directly attached neighbours, performs calculation and then **distributes the result back to its neighbours.**
- **Iterative:** It is iterative in that its process continues until **no more information is available to be exchanged** between neighbours.

- Each router maintains a distance table known as **Vector**. It is mainly used in **ARPANET, and RIP.**

3 Keys to understand the working of Distance Vector Routing Algorithm:

- **Knowledge about the whole network:** Each router **shares its knowledge** through the entire network. The Router sends its collected knowledge about the network to its neighbours.
- **Routing only to neighbours:** The router sends its knowledge about the network to only those **routers which have direct links.** The router sends whatever it has about the network through the ports. The information is received by the router and uses the information to update its own routing table.
- **Information sharing at regular intervals:** **Within 30 seconds**, the router sends the information to the neighbouring routers.

Distance Vector Routing Alg.

Let $d_x(y)$ be the cost of the least-cost path from node x to node y. The least costs are related by Bellman-Ford equation,

$$d_x(y) = \min_v\{c(x,v) + dv(y)\}$$

Where, the $\min_v$ is the equation taken for all x neighbours. After traveling from x to v, if we consider the least-cost path from v to y, the path cost will be $c(x,v)+d_v(y)$. The least cost from x to y is the minimum of $c(x,v)+d_v(y)$ taken over all neighbours.

With the Distance Vector Routing algorithm, the node x contains the following routing information:

1. For each neighbour v, the **cost c(x,v)** is the path cost from x to directly attached neighbour, v.
2. The distance vector x, i.e., $\mathbf{D_x = [\, D_x(y) : y \text{ in } N\,]}$, containing its cost to all destinations, y, in N.
3. The distance vector of each of its neighbours, i.e., $\mathbf{D_v = [\, D_v(y) : y \text{ in } N\,]}$ for each neighbour v of x.

- Distance vector routing is an asynchronous algorithm in which node x sends the copy of its distance vector to all its neighbours.
- When node x receives the new distance vector from one of its neighbouring vector, v, it saves the distance vector of v and uses the Bellman-Ford equation to update its own distance vector. The equation is given below:

$$d_x(y) = \min_v\{ c(x,v) + dv(y)\} \quad \text{for each node y in N}$$

- The node x has updated its own distance vector table by using the above equation and sends its updated table to all its neighbours so that they can update their own distance vectors.

Distance Vector Routing Alg.

At each node x,

Initialization

for all destinations y in N:

$D_x(y) = c(x,y)$ // If y is not a neighbour then $c(x,y) = \infty$

for each neighbour w

$D_w(y) = ?$ for all destination y in N.

for each neighbour w

send distance vector $D_x = [D_x(y) : y \text{ in } N]$ to w

loop

wait(until I receive any distance vector from some neighbour w)

for each y in N:

$D_x(y) = \min_v\{c(x,v)+Dv(y)\}$

If $D_x(y)$ is changed for any destination y

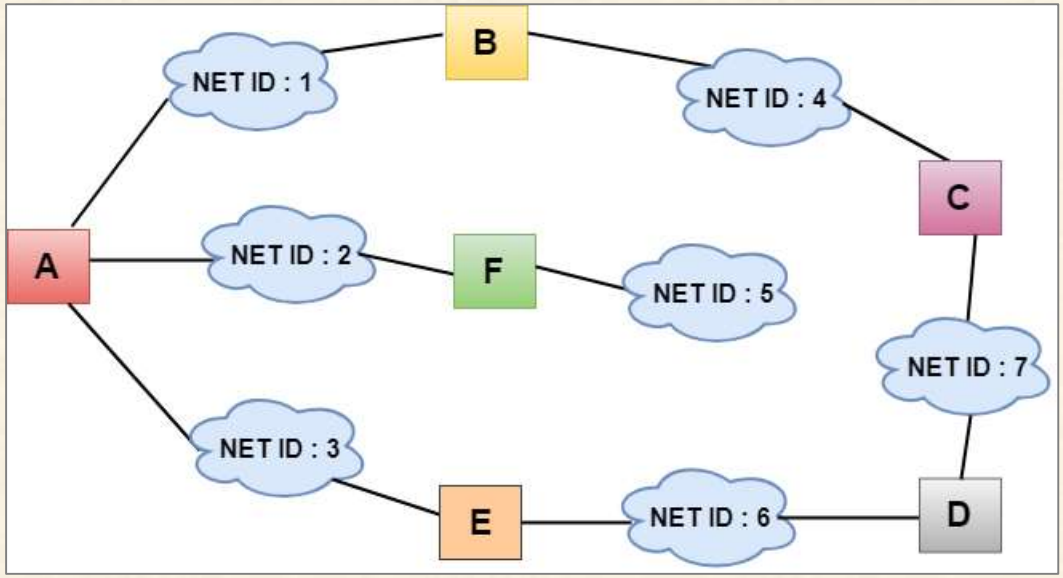
Send distance vector $D_x = [D_x(y) : y \text{ in } N]$ to all neighbours

forever

Distance Vector Routing Alg.

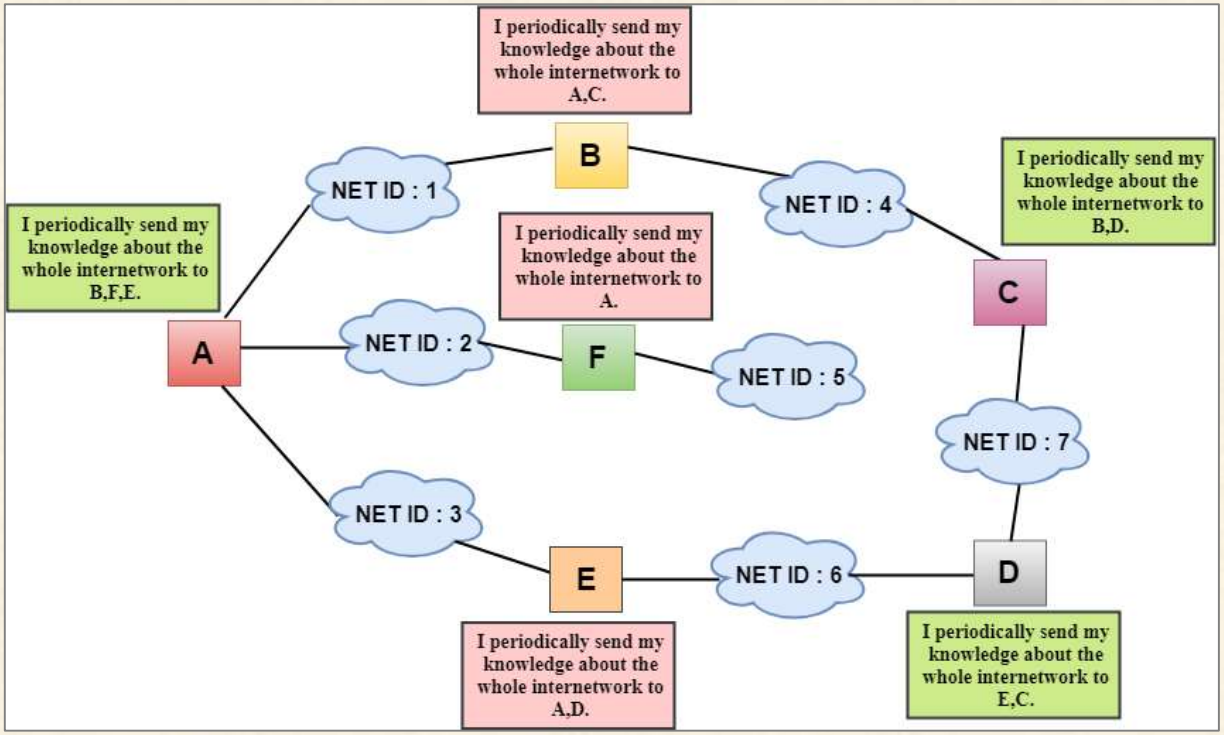
Let's understand through an example:

- Sharing Information



- In the above figure, **each cloud** represents the network, and the **number inside the cloud** represents the network ID.
- All the **LANs are connected by routers**, and they are represented in boxes labelled as A, B, C, D, E, F.
- Distance vector routing algorithm simplifies the routing process by **assuming the cost of every link is one unit.** Therefore, the efficiency of transmission can be measured by the **number of links to reach the destination.**
- In Distance vector routing, the **cost is based on hop count.**

Distance Vector Routing Alg.



- In the above figure, we observe that the router **sends the knowledge** to the immediate neighbours.
- The neighbours **add this knowledge to their own knowledge** and sends the updated table to their own neighbours.
- In this way, routers get its **own information plus the new information** about the neighbours.

Distance Vector Routing Alg.

Routing Table

Two process occurs:

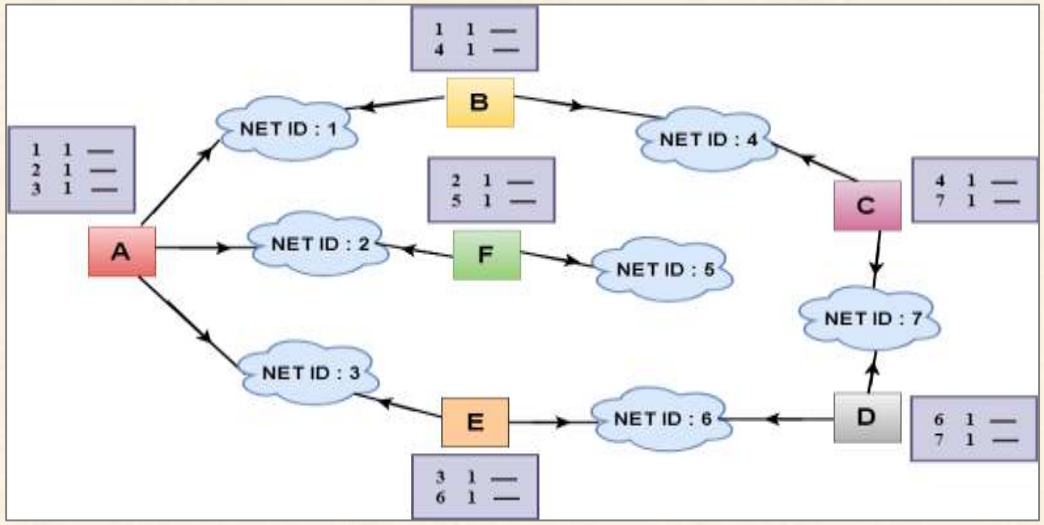
1. **Creating the Table**
2. **Updating the Table**

Creating the Table

- Initially, the routing table is created for each router that contains atleast three types of information such as Network ID, the cost and the next hop.
  - **NET ID:** The Network ID defines the final destination of the packet.
  - **Cost:** The cost is the number of hops that packet must take to get there.
  - **Next hop:** It is the router to which the packet must be delivered.

NET ID	Cost	Next Hop

Distance Vector Routing Alg.



- In the above figure, the original **routing tables are shown of all the routers.** In a routing table, the first column represents the **network ID**, the second column represents the **cost of the link**, and the third column is empty.
- These routing tables are sent to all the neighbours.

For Example:

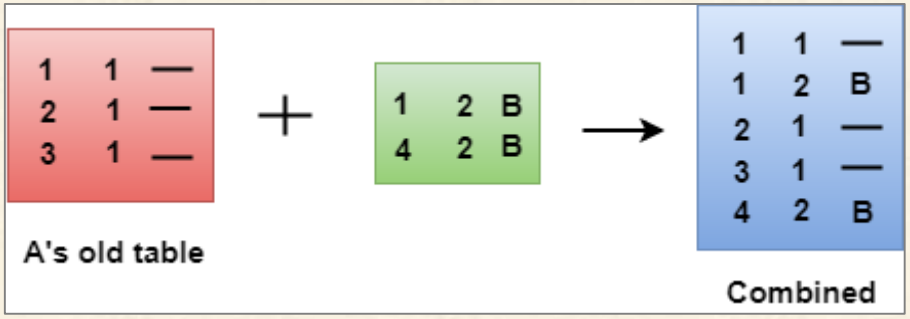
1. A sends its routing table to B, F & E.
2. B sends its routing table to A & C.
3. C sends its routing table to B & D.
4. D sends its routing table to E & C.
5. E sends its routing table to A & D.
6. F sends its routing table to A.

Distance Vector Routing Alg.

Updating the Table

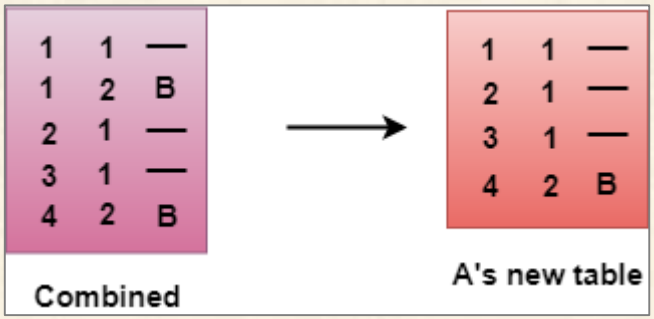
- When A receives a routing table **from B,** then it uses its **information to update the table.**
- The routing table of B shows how the packets can **move to the networks 1 and 4.**
- The B is a neighbour to the A router, the packets from A to B can **reach in one hop.** So, 1 is added to all the costs given in the B's table and the **sum will be the cost to reach** a particular network.

- After adjustment, A then combines this table with its own table to create a combined table.



Distance Vector Routing Alg.

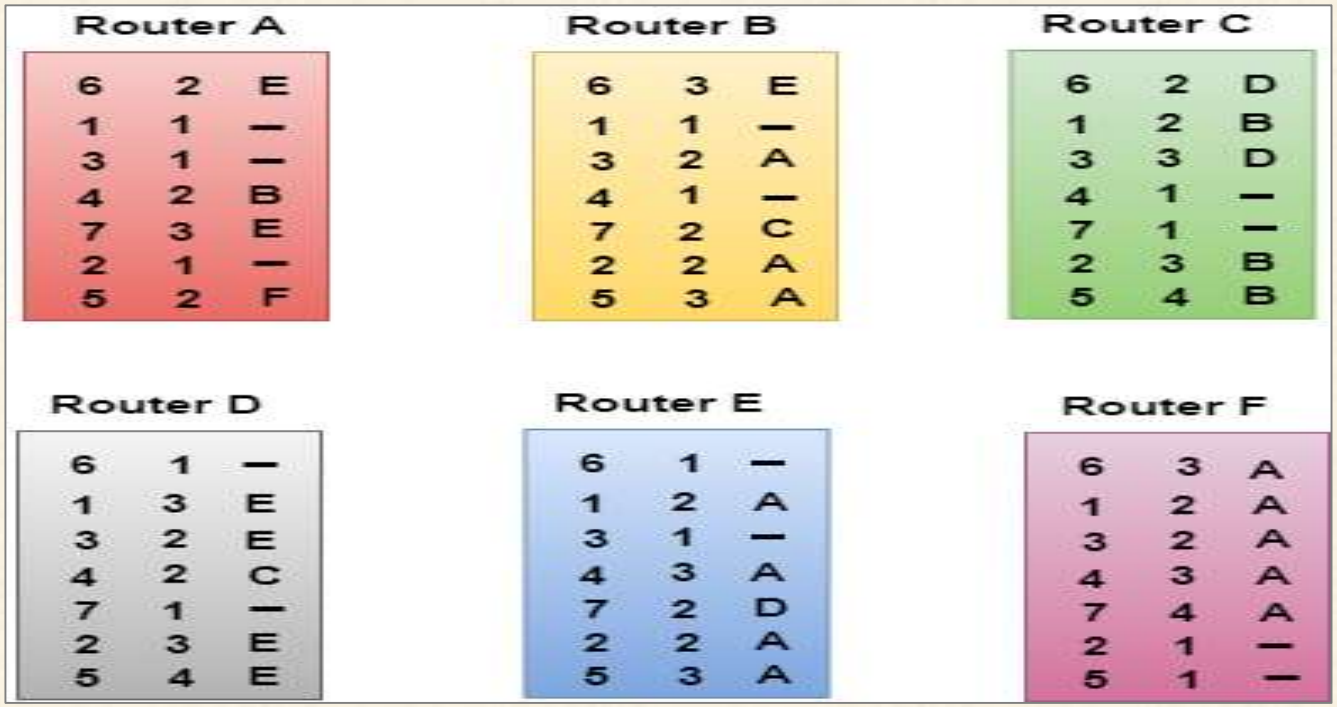
- The combined table may contain some duplicate data. The combined table of **router A contains the duplicate data**, so it **keeps only those data which has the lowest cost.**
- For example, A can send the data to network 1 in two ways. The first, which uses no **next router**, so it costs one hop. The second requires **two hops (A to B, then B to Network 1).**
- The first option has the lowest cost, therefore it is kept and the second one is dropped.



- The process of **creating the routing table continues** for all routers. Every router receives the information from the neighbours, and **update the routing table.**

Distance Vector Routing Alg.

Final routing tables of all the routers are given below:



Router A

6	2	E
1	1	—
3	1	—
4	2	B
7	3	E
2	1	—
5	2	F

Router B

6	3	E
1	1	—
3	2	A
4	1	—
7	2	C
2	2	A
5	3	A

Router C

6	2	D
1	2	B
3	3	D
4	1	—
7	1	—
2	3	B
5	4	B

Router D

6	1	—
1	3	E
3	2	E
4	2	C
7	1	—
2	3	E
5	4	E

Router E

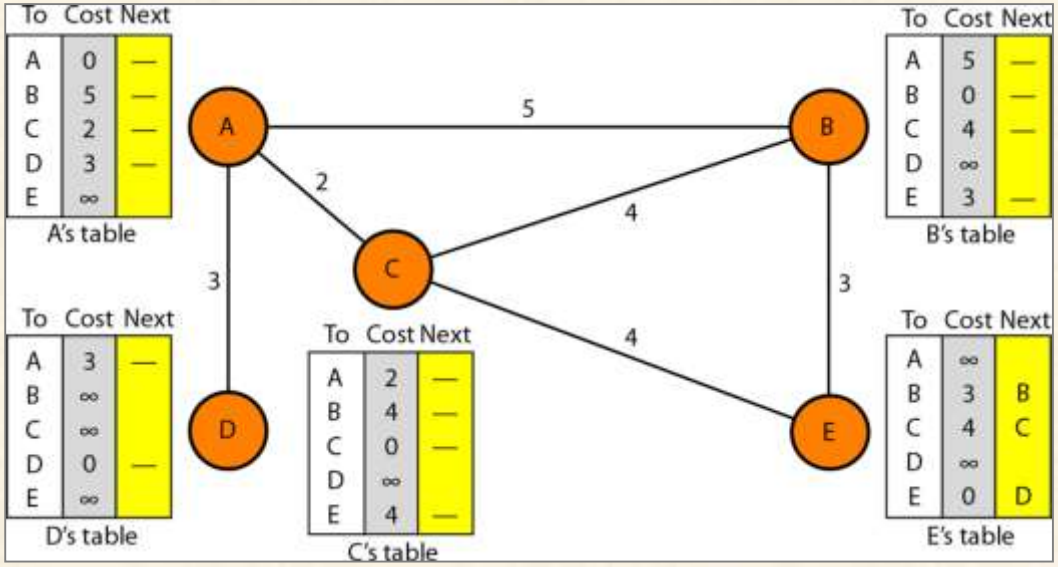
6	1	—
1	2	A
3	1	—
4	3	A
7	2	D
2	2	A
5	3	A

Router F

6	3	A
1	2	A
3	2	A
4	3	A
7	4	A
2	1	—
5	1	—

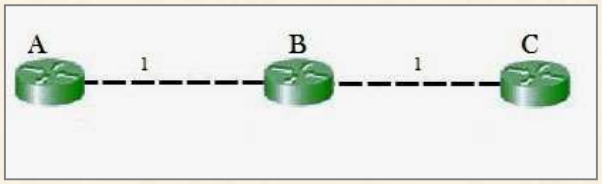
Distance Vector Routing Alg.

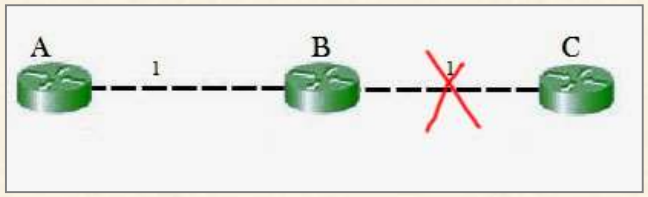
- Example



Count to infinity problem

- The main issue with **D**istance Vector **R**outing (DVR) protocols is Routing Loops since Bellman-Ford Algorithm cannot prevent loops.
- This routing loop in the DVR network causes the **Count to Infinity Problem**. Routing loops usually occur when an **interface goes down or two routers send updates** at the same time.





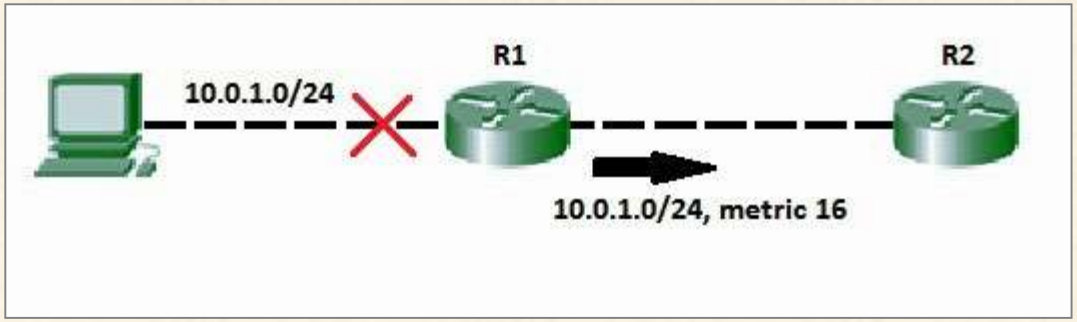
- So in this example, the **Bellman-Ford algorithm** will converge for each router, they will have entries for each other.
- B will know that it can get to **C at a cost of 1**, and A will know that it **can get to C via B at a cost of 2**.
- If the link between B and C is disconnected, then B will know that it can **no longer get to C via that link** and will remove it from its table.
- Before it can send any updates it's possible that it will receive an **update from A** which will be advertising that it can **get to C at a cost of 2.** B can get to A at a cost of 1, so it will update a **route to C via A at a cost of 3**. A will then receive updates from B later and update its cost to 4.
- They will then **go on feeding each** other bad information toward infinity which is called as **Count to Infinity problem**.

Route Poisoning

Solution for Count to Infinity problem

Route Poisoning:

- When a route fails, distance vector protocols spread the ***bad news*** **about a route failure** by poisoning the route. Route poisoning refers to the practice of advertising a route, but with a special metric value called **Infinity.**
- Routers consider routes advertised with an **infinite metric** to have failed. Each distance vector routing protocol uses the concept of an **actual metric** value that represents infinity. **RIP defines infinity as 16.**
- The main disadvantage of poison reverse is that it can significantly **increase the size of routing announcements** in certain fairly common network topologies.

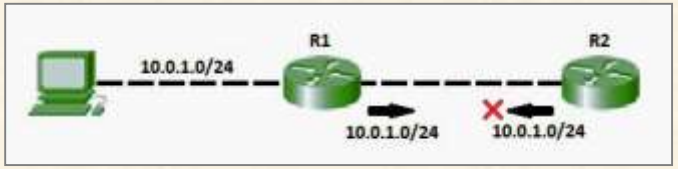


Route Poisoning

Split horizon:

- If the link between B and C goes down, and B had received a route from A, B could end up using that route via A. A would send the packet right back to B, creating a loop.
- But according to the **Split horizon Rule**, Node A does not advertise its route for C (namely A to B to C) back to B. On the surface, this seems redundant since B will never route via node A because the **route costs more than the direct route** from B to C.

Consider the following network topology showing Split horizon-



- In addition to these, we can also use **split horizon with route poisoning** were above both techniques will be used combined to achieve **efficiency and less increase the size** of routing announcements.
- Split horizon with Poison reverse technique is used by Routing Information Protocol (RIP) to **reduce routing loops**.
- Additionally, **Holddown timers** can be used to **avoid the formation of loops**. The hold-down timer immediately starts when the router is informed that the **attached link is down**.
- Till this time, the **router ignores all updates** of the down route unless it receives an update from the router of that downed link. During the timer, If the **s**, the routing table can be updated.

Link State Routing Alg.

Link state routing is a technique in which each router shares the knowledge of its neighbourhood with every other router in the internetwork.

The three keys to understand the Link State Routing algorithm:

- **Knowledge about the neighbourhood:** Instead of sending its routing table, a router sends the information about its neighbourhood only. A router ***broadcast its identities and cost of the directly attached links*** to other routers.
- **Flooding:** Each router sends the information to every other router on the internetwork ***except its neighbours.*** This process is known as Flooding. Every router that receives the ***packet sends the copies to all*** its neighbours. Finally, each and every router receives a copy of the same information.
- **Information sharing:** A router sends the information to every other router only when the ***change occurs*** in the information.

Link State Routing has two phases:

1. Reliable Flooding

- **Initial state:** Each node knows the ***cost of its neighbours.***
- **Final state:** Each node knows the ***entire graph.***

Link State Routing Alg.

Route Calculation

- Each node uses ***Dijkstra's algorithm*** on the graph to calculate the optimal routes to all nodes.
- The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.
- The Dijkstra's algorithm is an iterative, and it has the ***property that after k^{th} iteration*** of the algorithm, the least cost paths are well known for k destination nodes.

Let's describe some notations:

- **c(i , j):** Link cost from node i to node j. If i and j nodes are not directly linked, ***then c(i , j) = ∞.***
- **D(v):** It defines the cost of the ***path from source code to destination*** v that has the least cost currently.
- **P(v):** It defines the ***previous node (neighbour of v)*** along with current least cost path from source to v.
- **N:** It is the total ***number of nodes*** available in the network.

Link State Routing Alg.

Algorithm

Initialization:

N = {A} ***// A is a root node.***

for all nodes v

if v adjacent to A

then D(v) = c(A,v)

else D(v) = infinity

Loop

find w not in N such that D(w) is a minimum.

Add w to N

Update D(v) for all v adjacent to w and not in N:

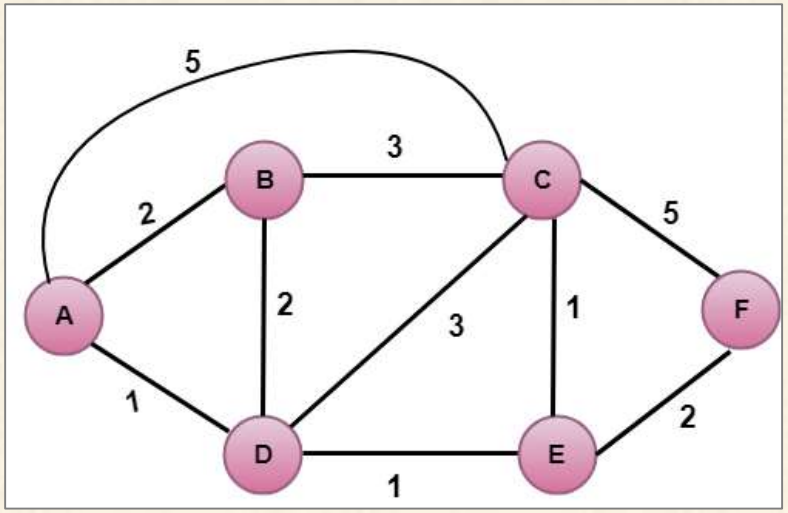
D(v) = min(D(v) , D(w) + c(w,v))

Until all nodes in N

In the above algorithm, an initialization step is followed by the loop. The number of times the loop is executed is equal to the total number of nodes available in the network.

Link State Routing Alg.

Let's understand through an example:



- **In the above figure, source vertex is A.**

Step 1:

- The first step is an initialization step. The currently known least cost path from A to its directly attached neighbours, B, C, D are 2,5,1 respectively. The cost from A to B is set to 2, from A to D is set to 1 and from A to C is set to 5. The cost from A to E and F are set to infinity as they are not directly linked to A.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞

Link State Routing Alg.

Step 2:

- In the above table, we observe that vertex D contains the least cost path in step 1. Therefore, it is added in N. Now, we need to determine a least-cost path through D vertex.

a) Calculating shortest path from A to B

- v = B, w = D
- D(B) = min(D(B) , D(D) + c(D,B))
- = min(2, 1+2)
- = min(2, 3)

The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

b) Calculating shortest path from A to C

- v = C, w = D
- D(B) = min(D(C) , D(D) + c(D,C))
- = min(5, 1+3)
- = min(5, 4)

The minimum value is 4. Therefore, the currently shortest path from A to C is 4.

Link State Routing Alg.

c) Calculating shortest path from A to E

- v = E, w = D
- D(B) = min(D(E) , D(D) + c(D,E))
- = min(∞, 1+1)
- = min(∞, 2)

The minimum value is 2. Therefore, the currently shortest path from A to E is 2.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞

Link State Routing Alg.

Step 3:

- In the above table, we observe that both E and B have the least cost path in step 2. Let's consider the E vertex. Now, we determine the least cost path of remaining vertices through E.

a) Calculating the shortest path from A to B.

- v = B, w = E
- D(B) = min(D(B) , D(E) + c(E,B))
- = min(2 , 2+ ∞)
- = min(2, ∞)

The minimum value is 2. Therefore, the currently shortest path from A to B is 2.

b) Calculating the shortest path from A to C.

- v = C, w = E
- D(B) = min(D(C) , D(E) + c(E,C))
- = min(5 , 2+1)
- = min(5,3)

The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

Link State Routing Alg.

c) Calculating the shortest path from A to F.

- v = F, w = E
- D(B) = min(D(F) , D(E) + c(E,F))
- = min(∞ , 2+2)
- = min(∞ ,4)

The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E

Link State Routing Alg.

Step 4:

- In the above table, we observe that B vertex has the least cost path in step 3. Therefore, it is added in N. Now, we determine the least cost path of remaining vertices through B.

a) Calculating the shortest path from A to C.

- v = C, w = B
- D(B) = min(D(C) , D(B) + c(B,C))
- = min(3 , 2+3)
- = min(3,5)

The minimum value is 3. Therefore, the currently shortest path from A to C is 3.

b) Calculating the shortest path from A to F.

- v = F, w = B
- D(B) = min(D(F) , D(B) + c(B,F))
- = min(4, ∞)
- = min(4, ∞)

Step	N	D(B), P(B)	D(C), P(C)	D(D), P(D)	D(E), P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E

The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Link State Routing Alg.

Step 5:

- In the above table, we observe that C vertex has the least cost path in step 4. Therefore, it is added in N. Now, we determine the least cost path of remaining vertices through C.

a) Calculating the shortest path from A to F.

- v = F, w = C
- D(B) = min(D(F) , D(C) + c(C,F))
- = min(4, 3+5)
- = min(4,8)

The minimum value is 4. Therefore, the currently shortest path from A to F is 4.

Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E

Link State Routing Alg.

Final table:

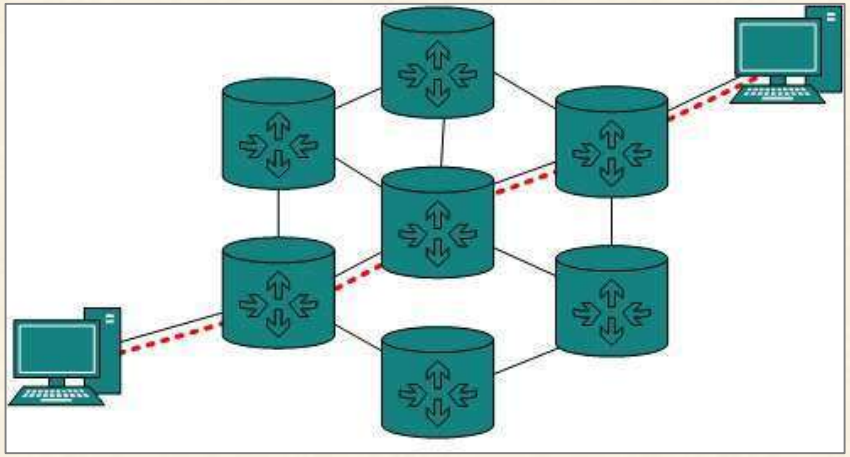
Step	N	D(B),P(B)	D(C),P(C)	D(D),P(D)	D(E),P(E)	D(F),P(F)
1	A	2,A	5,A	1,A	∞	∞
2	AD	2,A	4,D		2,D	∞
3	ADE	2,A	3,E			4,E
4	ADEB		3,E			4,E
5	ADEBC					4,E
6	ADEBCF					

Disadvantage:

- Heavy traffic is created in Line state routing due to Flooding. Flooding can cause an infinite looping, this problem can be solved by using Time-to-leave field

Internetworking

- There may exist requirement of **connecting two different networks of same kind** as well as of different kinds. Routing between two networks is called internetworking.
- Networks can be considered different based on various parameters such as, **Protocol, topology,** Layer-2 network and addressing scheme.
- In internetworking, routers have knowledge of each other's address and addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol.

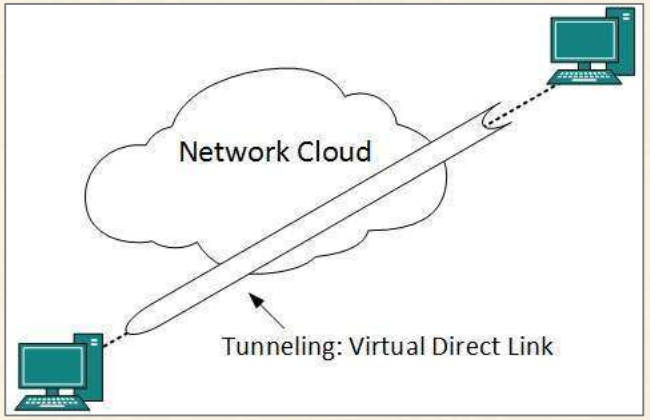


- Routing protocols which are used within an organization or administration are called **Interior Gateway Protocols or IGP. RIP, OSPF** are examples of IGP. Routing between different organizations or administrations may have Exterior Gateway Protocol, and there is only one EGP i.e. Border Gateway Protocol.

Internetworking

Tunneling

- If they are two geographically separate networks, which want to communicate with each other, they may deploy a dedicated line between or **they have to pass their data through intermediate networks.**
- Tunneling is a mechanism by which **two or more same networks communicate with each other,** by passing intermediate networking complexities. Tunneling is configured at both ends.



- When the data enters from one end of Tunnel, it is tagged. This tagged data is then **routed inside the intermediate or transit network to reach the other end** of Tunnel. When data exists the Tunnel its tag is removed and delivered to the other part of the network.
- Both ends seem as if they are directly connected and tagging makes data travel through transit network without any modifications.

Internetworking

Packet Fragmentation

- Most Ethernet segments have their **maximum transmission unit (MTU) fixed to 1500 bytes.** A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software capabilities which tell what amount of data that device can handle and what size of packet it can process.
- If the data packet size is **less than or equal to the size of packet** the transit network can handle, it is processed neutrally. If the packet is larger, it is **broken into smaller pieces** and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is assembled again.
- If a packet with **DF (don't fragment) bit set to 1** comes to a router which can not handle the packet because of its length, the packet is dropped.
- When a packet is received by a router has its **MF (more fragments) bit set to 1,** the router then knows that it is a fragmented packet and parts of the original packet is on the way.
- If packet is fragmented too small, the overhead is increases. If the packet is fragmented too large, intermediate router may not be able to process it and it might get dropped.

End Of UNIT-3