Chapter-4

Network Layer Protocol and Addressing

Introduction

- The main job of this layer is to inject packet into the network and have them travel independently to the destination.

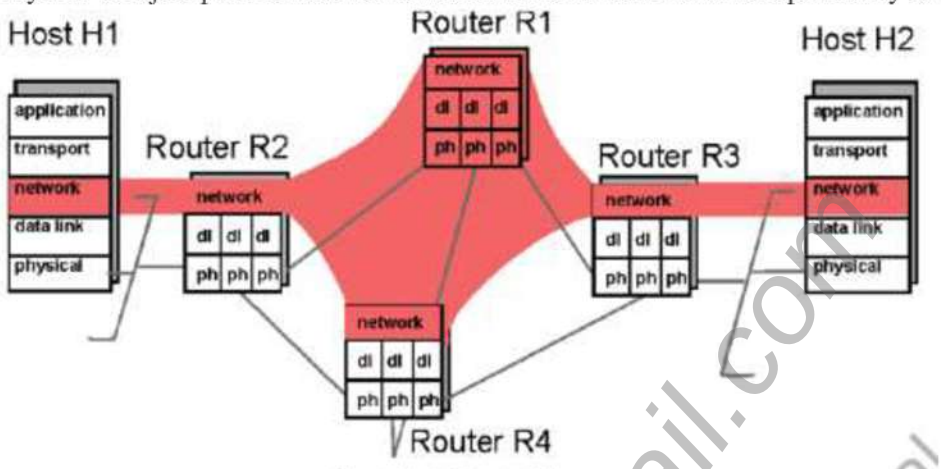


Figure 4.1-1: The network layer

- Above figure shows a simple network with two hosts (H1 and H2) and four routers (R1, R2, R3 and R4). The role of the network layer in a sending host is to begin the packet on its journey to the receiving host. For example, if H1 is sending to H2, the network layer in host H1 transfers these packets to it nearby router, R2. At the receiving host (e.g., H2), the network layer receives the packet from its nearby router (in this case, R3) and delivers the packet up to the transport layer at H2. The primary role of the routers is to "switch" packets from **input links** to **output links**.
- To do so, two important network functions are identified.
    1. Forwarding: Forwarding is the process of moving the packet arriving in the router input link to the appropriate output link.
    2. Routing: Routing is the process of determining the path or route taken by packets as they flow from sender to receiver.
- The main protocol that function at this layer is IP.

Router

- A router is a computer with components like CPU, RAM, IOS etc. whose primary functions is to connect two or more than two network and forward the packet from one network to another.
- A router has multiple interfaces that is belong to different IP network.

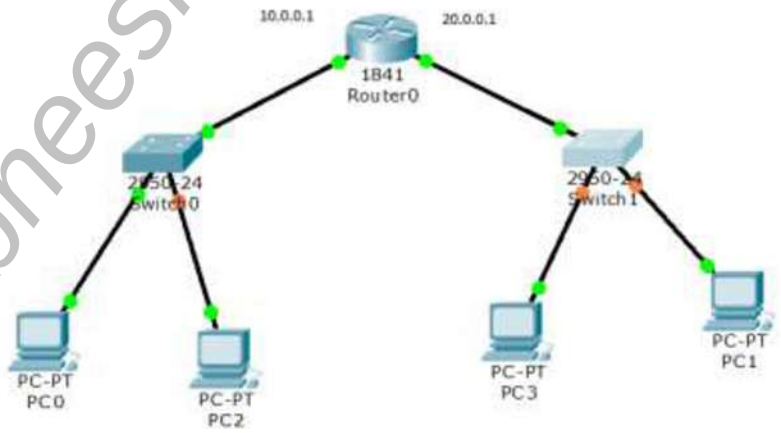


Fig: Router connection two different network

- A router uses IP to forward packet from source network to destination network.

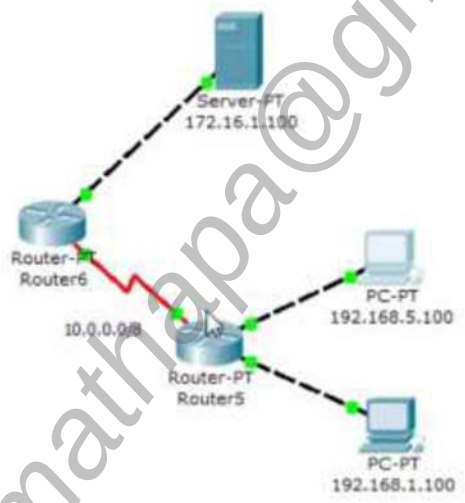
Routing Table

- In computer networking a routing table, or routing information base (RIB), is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes.
- Router keep track of following information in their tables.
  i. the network id: i.e. the destination subnet
  ii. cost/metric: i.e. the cost or metric of the path through which the packet is to be sent
  iii. next hop: The next hop, or gateway, is the address of the next station to which the packet is to be sent on the way to its final destination

Network id	Cost	Next hop
……	……	……
……	……	……

Example:

Let us consider following network



Routing table for Router6: Using CLI: show ip router

```
C    10.0.0.0/8 is directly connected, Serial2/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
```

Routing table for router5:

```
C    10.0.0.0/8 is directly connected, Serial2/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.5.0/24 is directly connected, FastEthernet1/0
```

Question: Can we ping server from pc-pt?
Answer: No, because Router 5 has no routing information on how to reach serve-pt from pc-pt.

Logical address and physical address

- An IP address is most commonly assigned to a piece of hardware by a router, using automation called **DHCP.** Or it can be assigned manually, by you typing a Static IP into the adapter properties, or various other way.
- An IP address can change many times in the "life" of a device. Hence it is also called as logical address.
- IP addresses are 4byte (32-bits) in length. This will be discussed in detail shortly.

- A MAC address is hard-coded into the hardware, and doesn't (normally) change. No matter where the device is, or what network it is connected to, the MAC remains the same. Hence it is also called as physical address.
- MAC addresses are 6-byte (48-bits) in length, and are written in MM:MM:MM:SS:SS:SS format. The first 3-bytes are ID number of the manufacturer, which is assigned by an Internet standards body. The second 3-bytes are serial number assigned by the manufacturer.
  Example of MAC address: *00:0a: 95:9d: 68:16*.

IP Address

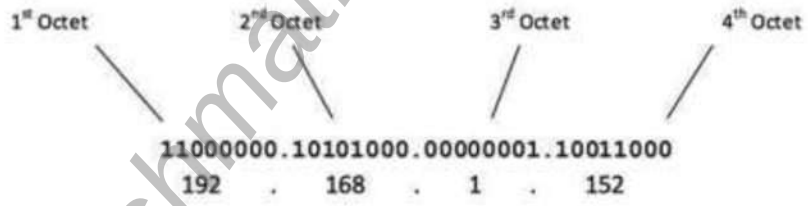
- An IP address is an identifier for a computer or a device on a TCP/IP network. To identify a host on the internet, each host is assigned an address called IP address.
- Router uses the IP address to route packet to correct network segment.
- It encodes its network number and host number.
  i.e. IP address = <Network Number><Host Number> where the network number identifies the network on the internet and the host number identifies the individual host in that network.
- Two types of IP address are currently in use
  1. IPV4 (32 bit)
  2. IPV6 (128 bit)

Example:

i. 197. 223. 57. 33
ii. 2001:0db8:85a3:0000:0000:8a2e: 0370:7334

IPV4 address Classes: Classful addressing

IPV4 address are 32 bit which are divided into four octets, separated by dot(.), each of 8 bit long. Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. So, in classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of address space. All the five classes are identified by the first octet of IP Address.



1. Class A
   - The general form of class A ipv4 address is N.H.H.H.H
   - The First bit of class A ipv4 address is always 0
     oNNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH
   - Range of IP = 0.0.0.0 to 127.255.255.255
   - Default Subnet Mask= 255.0.0.0 i.e. 11111111.00000000.00000000.00000000 (dotted notation) i.e. /8 (slash notation)
   - 7 network bit so 2^7 network addresses are available
   - 24 host bit so 2^{24} host address are available

0	Network	Host
	7 bit	24 bit

   - A class A address block was designed to support extremely large networks with more than 16 million host addresses.

2. Class B
   - The general form of class B ipv4 address is N.N.H.H
   - First two bit is 10

     10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH
   - Range of IP = 128.0.0.0 to 191.255.255.255
   - Default subnet mask = 255.255.0.0 i.e. 11111111.11111111.00000000.00000000 i.e. / 16 in slash notation
   - 14 network bit so 2^{14} network addresses are available
   - 16 host bit so 2^{16} host addresses are available

10	Network	Host
	14 bit	16 bit

   - Class B address space was designed to support the needs of moderate to large size networks with more than 65,000 hosts.

3. Class C
   - The general form of class C ipv4 address is N.N.N.H
   - First 3 bit is 110

     110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH
   - Range of IP = 192.0.0.0 to 223.255.255.255
   - Default Subnet Mask = 255.255.255.0 i.e. 11111111.11111111.11111111.00000000 i.e. /24 in slash notation

110	Network	Host
	21 bit	8 bit

   - 8 host bit so 2^8 host address are available
   - 21 network bit so 2^{21} network address are available.
   - This address space was intended to provide addresses for small networks with a maximum of 254 hosts.

4. Class D
   - 4 digits are fixed i.e. 1110
     The general form is 1110MMMM.MMMMMMMM.MMMMMMMM.MMMMMMMM
   - 2^{28} multicast addresses.
   - Range of IP = 224.0.0.0 to 239.255.255.255
   - There is no network and host bit as in previous case.
   - Every IP datagram whose destination address starts with "1110" is an IP Multicast datagram.
   - The remaining 28 bits identify the multicast "group" the datagram is sent to.
   - These addresses are reserved for multicasting(one to many communication like group sms) i.e. a kind of broadcasting but in limited area and only to host using the same class D address, example video conference

1110	Multicast address(group id)

   - In case of multicast communication, the server sends data on a particular multicast IP address and clients who intend to receive that data need to listen on the same multicast address. These clients can be various different networks. A group of clients listening to same multicast address is known as host group.
   - Also, they do not have subnet mask.
   - As with the case of ports (where we have well known ports ie 0-1024), there are some reserved multicast IP addresses or well known IP addresses.

224.0.0.0	**224.0.0.255**	Reserved for special "well-known" multicast addresses.

   - For example, an Open Shortest Path First (OSPF) router sends a "hello" packet to other OSPF routers on the network. The OSPF router must send this "hello" packet to an assigned multicast address, which is **224.0.0.5**, and the other routers will respond.

5. Class E
   - First four bit is 1111
     The general form is 1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX
   - Reserved for future use
   - Range of IP = 240.0.0.0 to 255.255.255.255

Summary:

Class	Start IP range	End IP range	Subnet Mask
A	0.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	undefined

Note:

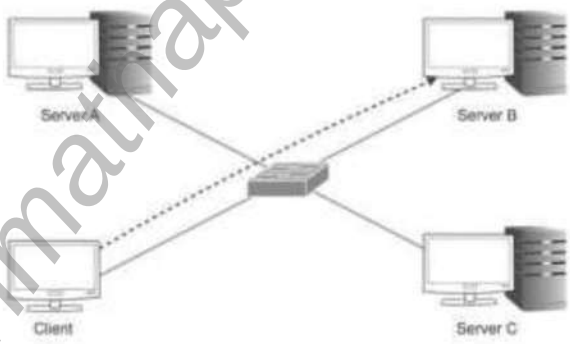
- Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

Addressing Mode

IPV4 support there types of addressing

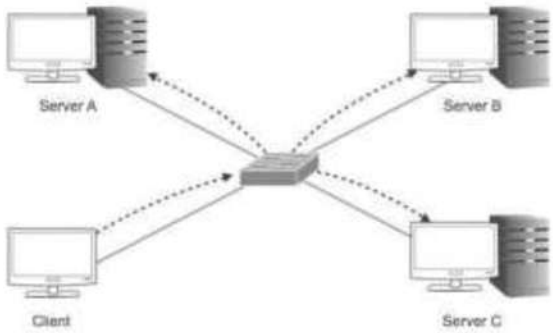
i. Unicasting

In this mode, data is sent only to one destined host. The Destination Address field contains 32- bit IP address of the destination host. Here the client sends data to the targeted server.



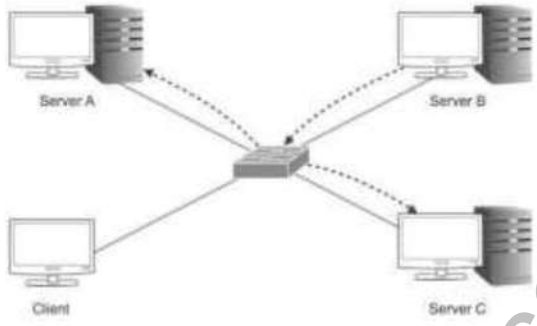
ii. Broadcasting

In this mode, the packet is addressed to all the hosts in a network segment. The Destination Address field contains a special All broadcast address, i.e. 255.255.255.255 or subnet broadcast i.e. X.X.X.255. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers.



iii. Multicasting

This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.



Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

Numerical examples

1. Given IP 192.168.0.0 /23 find
   a. Subnet mask in decimal/dotted notation.
   b. Network address
   c. Broadcast address
   d. Total no of host and usable host address
   e. Usable IP range

Solution:

a. Subnet mask:
   /23 = 11111111.11111111.11111110.00000000
   In decimal, 255.255.254.0

b. Network address:
   Note: Network address is calculated by logical anding the IP address with the subnet mask.
   So given IP address = 192. 168. 0. 0 = 11000000. 10101000. 00000000. 00000000
   Subnet Mask= 11111111. 11111111. 11111110. 00000000
   Performing logical anding, we get 11000000. 10101000. 00000000. 00000000
   i.e. 192. 168. 0. 0

c. Broadcast address:
   Note: O host bit in IP are changed to 1 for corresponding 0 in the subnet mask to get broadcast address.
   Given, Subnet Mask = 11111111. 11111111. 11111110. 00000000
   IP= 11000000. 10101000. 00000000. 00000000
   Broadcast Address= 11000000. 10101000. 00000001. 11111111
   = 192. 168. 1. 255

d. Total number of host and usable IP address range
   Total number of host = 2^9 = 512 hosts
   Total number of usable host address = total host -2
   = 512 – 2
   = 510
   Note: two addresses are used as network address and broadcast address

e. Useable IP range = 192. 168. 0 .1 to 192. 168. 1. 254

2. For given IP 10.10.2.3 and subnet mask 255.0.0.0. find
   i. Subnet mask in slash notation
   ii. Total number host and usable host
   iii. Network address
   iv. Broadcast address
   v. Usable Host range

Solution:

i. Given Subnet Mask = 11111111.00000000.00000000.00000000
   i.e. /8

ii. Total number of bits for host portion = 24
   total host = 2^{24} = 16777216
   Total usable host = 2^{24} -2 = 16777214

iii. network address
   IP = 00001010.00001010.00000010.00000011
   Subnet Mask= 11111111.00000000.00000000.00000000
   Logical anding = 00001010.00000000.00000000.00000000
   i.e. N/W address = 10.0.0.0

iv. Broad cast address
   IP = 00001010.00001010.00000010.00000011
   Subnet Mask = 11111111.00000000.00000000.00000000
   Broadcast Address=00001010.11111111.11111111.11111111
   i.e. 10.255.255.255

v. Host range
   10.0.0.1 to 10.255.255.254

Public IP and Private IP

- A public IP address is an IP address that can be accessed over the Internet
- Private IP address on the other hand is used to assign computers within your private space without letting them directly expose to the Internet
- For example, we can assign private IP address to multiple computers within our home or organization.
- In this case, our router get the public IP address, and each of the computers, tablets and smartphones connected to your router (via wired or wifi) get a private IP address from your router via DHCP protocol.
- When a computer is assigned a private IP address, the local devices sees this computer via it's private IP address. However, the devices residing outside of your local network cannot directly communicate via the private IP address, but uses your router's public IP address to communicate.
- To allow direct access to a local device which is assigned a private IP address, a Network Address Translator (NAT) should be used.
- *Network Address Translation* (NAT) is the process where a network device, assigns a public address to a computer (or group of computers) inside a private network.
- The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.
- Routers inside the private network can route traffic between private addresses with no trouble. However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them. This is where NAT comes into play.
- When NAT is used in this way, all users inside the private network access the Internet have the same public IP address when they use the Internet. That means only one public addresses is needed for hundreds or even thousands of users.
- The following IP blocks are reserved for private IP addresses and allows organizations to create their own private network.

Class	Starting IP Address	Ending IP Address	# of Hosts
A	10.0.0.0	10.255.255.255	16,777,216
B	172.16.0.0	172.31.255.255	1,048,576
C	192.168.0.0	192.168.255.255	65,536

i.e. For A /8 subnet mask
B /12 subnet mask
C /16 subnet mask

Subnetting and Subnet Mask

Generally, when an organization network need to connect to the internet, the ISP provides an IP address and subnet mask. Now the client can split this IP address into a number of independent networks, each network with fixed number of host. Each of the networks generated out of network is called subnet.

A subnet mask is a number that split an IP address into network portion and host portion. Thus a number of network can be generated out of a single network by varying the subnet mask. The subnet mask can be represented either in dotted format or in slash(/) notation. In dotted format, the region of binary 1 denote the network address where in slash notation, the number of bits counted from left to right equal to slash value represent the network portion.

Example:

1.Suppose you are given a IP address 172.30.0.0 and subnet mask /24. If the college need different networks for its different departments with at most 62 host. Calculate the subnet mask, subnets and their corresponding network address, broadcast address and their host range and number of usable host.

Solution:

Given IP = 172.30.0.0

Subnet Mask= /24 = 255.255.255.0

Maximum Host to be connected = 62, so we need 6 host bit because $2^6 = 64$.

Borrowing 2 bits from the host bit we get subnet mask of /26

172 . 30 . 00000000 . 00000000
/24 /26

1st subnet = 172. 30. 0.0/26

2nd subnet = 172.30.0.64/26

3rd subnet = 172.30.0.128/26

4rth subnet= 172.30.0.192/26

The below table shows the network address, broadcast address, their host range and number of host for each subnet

Subnet	Network Address	Broadcast Address	IP Range	No of host =(2^N -2)
1	172.30.0.0/26	172.30.0.63/26	172.30.0.1/26 to 172.30.0.62/26	2^6-2 = 62
2	172.30.0.64/26	172.30.0.127/26	172.30.0.65/26 to 172.30.0.126/26	62
3	172.30.0.128/26	172.30.0.191/26	172.30.0.129/26 to 172.30.0.190/26	62
4	172.30.0.192/26	172.30.0.255/26	172.30.0.1/193 to 172.30.0.254/26	62

So we can create at most four different subnets as given in above table each with maximum of 62 host.

2 In a 192.168.1.0/24, if 4 networks are required, calculate the subnet mask, their corresponding network address, broadcast address, host range and number of host.

Solution:

Given IP = 192.168.1.0

Subnet Mask= /24 = 255.255.255.0

Total Number of network = 4, so we need 2 bits because $2^2 = 4$.

Borrowing 2 bits from the host bit we get subnet mask of /26

192. 168. 00000001. 00 000000

/24 /26

1st subnet = 192.168.1.0/26

2nd subnet= 192.168.1.64/26

3rd subnet = 192.168.1.128/26

4rth subnet = 192.168.1.192/26

The below table shows the network address, broadcast address, host range and number of hosts per subnet.

Subnet	Network Address	Broadcast Address	IP Range	No of host =(2^N -2)
1	192.168.1.0/26	192.168.1.63/26	192.168.1.1/26 to 192.168.1.62/26	2^6-2 = 62
2	192.168.1.64/26	192.168.1.127/26	192.168.1.65/26 to 192.168.1.126/26	62
3	192.168.1.128/26	192.168.1.191/26	192.168.1.129/26 to 192.168.1.190/26	62
4	192.168.1.192/26	192.168.1.255/26	192.168.1.1/193 to 192.168.1.254/26	62

3. 2 In a 192.168.1.0/24, if 6 networks are required, calculate the subnet mask, their corresponding network address, broadcast address, host range and number of host.

Solution:

Given IP = 192.168.1.0

Subnet Mask= /24 = 255.255.255.0

Total Number of network = 6, so we need 3 bits because $2^3 = 8$.

Borrowing 2 bits from the host bit we get subnet mask of /26

192. 168. 00000001. 000 00000

/24 /27

1st subnet = 192.168.1.0/27

2nd subnet= 192.168.1.32/27

3rd subnet = 192.168.1.64/27

4th subnet = 192.168.1.96/27

5th subnet = 192.168.1.128/27

6th subnet = 192.168.1.160/27

7th subnet = 192.168.1.192/27

8th subnet = 192.168.1.224/27

The below table shows the network address, broadcast address, host range and number of hosts per subnet.

Subnet	Network Address	Broadcast Address	IP Range	No of host =(2^N -2)
1	192.168.1.0/27	192.168.1.31/27	192.168.1.1/27 to 192.168.1.30/27	2^5-2 = 30
2	192.168.1.32/27	192.168.1.63/27	192.168.1.33/27 to 192.168.1.62/27	30
3	192.168.1.64/27	192.168.1.95/27	192.168.1.65/27 to 192.168.1.94/27	30
4	192.168.1.96/27	192.168.1.127/27	192.168.1.97/27 to 192.168.1.126/27	30
5	192.168.1.128/27	192.168.1.159/27	192.168.1.129/27 to 192.168.1.158/27	30
6	192.168.1.160/27	192.168.1.191/27	192.168.1.129/27 to 192.168.1.190/27	30

So we can use the above subnets for creating 6 network that can have at most 30 usable host. Subnet 7 and subnet 8 remains unused.

Classless Addressing: CIDR (Class less Inter-Domain Routing)

- In case of classful addressing, class A was much too large and class C was much too small. Even a class B address was too large for many networks but was used because it was better than the alternatives.
- A new, flexible way of defining addresses is needed.

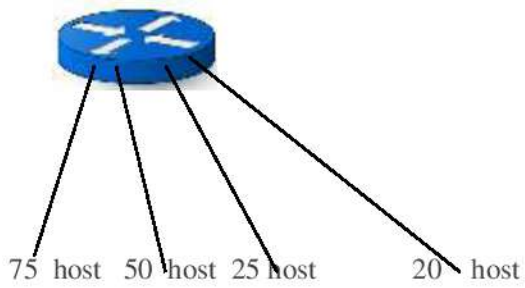
- Evaluating addresses according to the **class rules** discussed above limits the length of network numbers to 8, 16, or 24 bits - 1, 2, or 3 bytes.
- A more flexible way to interpret the network and host portions of an address is with a **bit mask**.
- An address bit mask works in this way: if a bit is on i.e. 1 in the mask, that equivalent bit in the address is interpreted as a network bit; if a bit in the mask is off i.e. 0, the bit belongs to the host part of the address.
- For example, if address 195.4.12.0 is interpreted as a class C address, the first 24 bits are the network number and the last 8 bits are the host address.
- The network mask that represents this is 255.255.255.0, 24 bits on and 8 bits off.
- The bit mask that is derived from the traditional class structure is called the default subnet mask or the natural subnet mask. A subnet mask is used to distinguish between network portion and host portion in a given IP address scheme.
- However, with bit masks we are no longer limited by the address class structure.
- A mask of 255.255.0.0 can be applied to network address 195.4.0.0. This mask includes all addresses from 195.4.0.0 to 195.4.255.255 in a single network number. In effect, it creates a network number as large as a class B network in the class C address space.
- The use of a mask instead of the address class to determine the destination network and host is called Classless Inter-Domain Routing (CIDR). Classless inter-domain routing (CIDR) is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks and individual devices
- Instead of writing network 172.16.26.32 with a mask of 255.255.255.224, we can write 172.16.26.32/27 in CIDR notation.

VLSM (Variable length subnet mask)

- CIDR is based on the variable-length subnet masking (VLSM) technique with effective qualities of specifying arbitrary-length prefixes.
- A subnet mask defines the size of the subnet (the number of host addresses in the subnet).
- VLSM is a process of dividing an IP network into the subnets of different sizes without wasting IP addresses.
- When we perform Subnetting, if all subnets have the same number of hosts, then, this is known as FLSM (Fixed length subnet mask).
- In FLSM all subnets use same subnet mask, this lead to inefficiencies.
- But where some subnets will have many hosts and some have few, FLSM results in some subnets having many orphaned addresses, or some sets of hosts being too big to fit into a subnet.
- When VLSM is used, a large subnet can be divided into a set of smaller sub-subnets, which can be used to handle smaller sets of hosts.

Example:

- Consider a Class C address space 192.168.1.0/24 and an organization with four groups of computers on different network
  - i. the data center with 75 hosts;
  - ii. the call center with 50 host;
  - iii. the operations floor with 25 host;
  - iv. and the executive floor with 20 host.



Calculate the subnet mask, subnets and their corresponding n/w address, broadcast address and host range.

Solution:

Under fixed length subnetting,

Given IP = 192.168.1.0

Subnet Mask= /24 = 255.255.255.0

Total Number of network = 4, so we need 2 bits because $2^2 = 4$.

Borrowing 2 bits from the host bit we get subnet mask of /26

192. 168. 00000001 | 00 | 000000

/24 /26

1st subnet = 192.168.1.0/26

2nd subnet= 192.168.1.64/26

3rd subnet = 192.168.1.128/26

4rth subnet = 192.168.1.192/26

The below table shows the network address, broadcast address, host range and number of hosts per subnet.

Subnet	Network Address	Broadcast Address	IP Range	No of Uhost =(2^N -2)
1	192.168.1.0/26	192.168.1.63/26	192.168.1.1/26 to 192.168.1.62/26	2^6-2 = 62
2	192.168.1.64/26	192.168.1.127/26	192.168.1.65/26 to 192.168.1.126/26	62
3	192.168.1.128/26	192.168.1.191/26	192.168.1.129/26 to 192.168.1.190/26	62
4	192.168.1.192/26	192.168.1.255/26	192.168.1.1/193 to 192.168.1.254/26	62

So, dividing the 255 host addresses available into four subnets would support only 62 hosts each, not meeting the needs of the data center and vastly oversupplying addresses for operations and the executive floor.

So using the concept of VLSM,

Given

IP = 192.168.1.0

Subnet Mask= /24 = 255.255.255.0

Maximum Host to be connected = 75, so we need 7 host bit because $2^7 = 128$.

Borrowing 1 bit from the host bit we get subnet mask of /26/25

192 . 168. 00000001 | 0 | 0000000

/24 /25

1st subnet = 192. 168. 1.0/25

2nd subnet = 192.168. 1.128/25

The below table shows the network address, broadcast address, their host range and number of host for 1st subnet

Subnet	Network Address	Broadcast Address	IP Range	No of Uhost =(2^N -2)
1	192.168.1.0/25	192.168.1.127/25	192.168.1.1/25 to 192.168.1.126/25	2^7-2 = 126

So, 1st subnet can be used to connect the datacentre.

Again subnetting subnet2.

2nd subnet = 192.168.0.128/25

192 . 168. 00000001 . 1 | 0000000

/25

Now second maximum number of host to be connected=50, so we need 6 host bits i.e. $2^6 = 64$ host

Borrowing 1 bit from the host bit of subnet2 we get subnet mask of /26

192 . 168. 00000000 . 10 | 000000

/25 /26

3rd subnet = 192.168.1.128/26

4th subnet = 192.168.1.192/26

The below table shows the network address, broadcast address, their host range and number of host for 3rd subnet.

Subnet	Network Address	Broadcast Address	IP Range	No of Uhost =(2^N -2)
3	192.168.1.128/26	192.168.1.191/26	192.168.1.129/26 to 192.168.1.190/26	2^6-2 = 62

So, 3rd subnet can be used to connect call center

Finally, subnetting 4th subnet.

4th subnet = 192.168.1.192/26

192. 168. 00000001. 11|000000

/26

Third maximum number of host to be connected = 25, so we need 5 host bit ie. $2^5 = 32$ host

Borrowing 1 bits from the host bit in subnet4, we get subnet mask of /27

192. 168. 00000001. 11|0|00000

/26 /27

5th subnet = 192.168.1.192/27

6th subnet = 192.168.1.224/27

The below table shows the network address, broadcast address, their host range and number of host for 5th and 6th subnet.

Subnet	Network Address	Broadcast Address	IP Range	No of Uhost =(2^N -2)
5	192.168.1.192/27	192.168.1.223/27	192.168.1.193/27 to 192.168.1.222/27	2^5-2 = 30
6	192.168.1.224/24/27	192.168.1.255/27	192.168.1.225/27 to 192.168.1.254/27	30

So 5th subnet can be used to connect operational floor and 6th subnet can be used to connect executive floor.

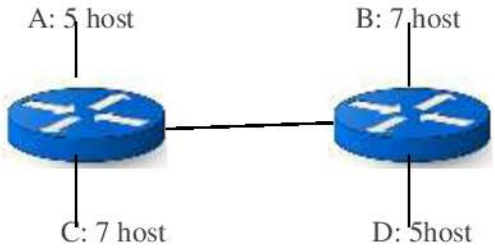
Note: In FLSM we start with checking the number of network requires and divide the network to get required subnets each with same subnet mask. But in VLSM we start with checking the host number create network depending upon it. In this case different subnet will have different subnet mask.

Steps for VLSM Subnetting

- Find the largest segment. Segment which need largest number of hosts address.
- Do Subnetting to fulfill the requirement of largest segment.
- Assign the appropriate subnet mask for the largest segment.
- For second largest segments, take one of these newly created subnets and apply a different, more appropriate, subnet mask to it.
- Assign the appropriate subnet mask for the second largest segment.
- Repeat this process until the last network.

Subnetting Numericals

1. The class C N/w of 204. 15. 5. 0/24 is given. Subnet the network in order to create the network in the given figure with the host requirement shown.



Solution:

Given IP Address = 204.15.5.0

Subnet Mask= 255.255.255.0

Here Maximum host = 7 (for B or C) so 4 bits are required i.e. 2^4 =16 because we need (7 +2) addresses: two addresses are required for network and broadcast. Borrowing 4 bits from the host bit we get subnet mask of /28

204 . 15. 0000101.|0000|0000

/24 /28

Subnet1 = 204. 15. 5. 0 /28 ……0000

Subnet2 = 204.15. 5. 16/28……....0001

Subnet 3 = 204. 15. 5. 32 / 28……0010

Subnet 4 = 204. 15. 5. 48 /28……0011

……5 – 16 subnets are unused

The below table shows the network address, broadcast address, their host range and number of host for 1st subnet and 2nd subnet

Subnet	Network Address	Broadcast Address	IP Range	No of U.host =(2^N -2)
1	204.15.5.0/28	204.15.5.15/28	204.15.5.1/28 to 204.15.5.14/28	2^4-2 = 14
2	204.15.5.16/28	204.15.5.31/28	204.15.5.17/28 to 204.15.5.30/28	14

So subnet1 can be used to connect Network B and subnet 2 can be used to connect network C.

Now for 5 host, we can use only 3 bit i.e. 2^3 =8, which is sufficient for 5 host+ 1 network + 1 broadcast address.

Again subnetting 3rd subnet with borrowing 1 bits from host we get new subnet mask of /29

204 . 15. 0000101.0010|0000

/28 /29

Subnet 5 = 204.15.5.32 /29

Subnet6 = 205. 15. 5. 40 /29

The below table shows the network address, broadcast address, their host range and number of host for 5th subnet and 6th subnet

Subnet	Network Address	Broadcast Address	IP Range	No of Uhost =(2^N -2)
5	204.15.5.32/29	204.15.5.39/29	204.15.5.33/29 to 204.15.5.38/29	2^3-2 = 6
6	204.15.5.40/29	204.15.5.47/29	204.15.5.41/29 to 204.15.5.46/29	6

So subnet5 can be allocated to network A and subnet 6 can be allocated to network D

Finally, two IP are required for route1 and router 2 serial interface. For this we need two bits i.e. 2^2 =4. So subnetting subnet4 with borrowing 2 bits from host we get subnet mask of /30

204 . 15. 0000101.0011|0000

/28 /30

Subnet 7= 204. 15. 5. 48/30……00

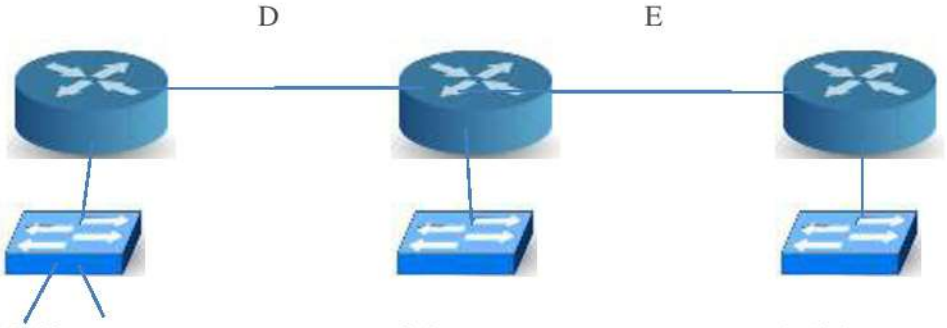
Other subnet remains unused

The below table shows the network address, broadcast address, their host range and number of host for 7th subnet

Subnet	Network Address	Broadcast Address	IP Range	No of Uhost =(2^N -2)
7	204.15.5.48/30	204.15.5.51/30	204.15.5.49/30 to 204.15.5.50/30	2^4-2 = 2

So subnet 7 can be used for router interface with router1 interface IP address 204.15.5.49/30 and router2 IP interface IP address 204.15.5.50/30.

2. The class C network of 192.168.1.0/24 is given. Subnet the network in order to create the network in given figure with the host requirement shown.



Solution: Given IP address = 192. 168. 1. 0
Subnet Mask= 255. 255. 255. 0

Here Maximum host = 123 (for A) so 7 bits are required i.e. 2^7 =128 so Borrowing 1 bit from the host bit we get subnet mask of /26 we get subnet mask of /25

192. 168.00000001.00000000
/24 /25

Subnet1: 192. 168. 1. 0/25 ……0
Subnet2: 192. 168. 1. 128/25……1
The below table shows the network address, broadcast address, their host range and number of host for 1st subnet

Subnet	Network Address	Broadcast Address	IP Range	No of Uhost =(2^N -2)
1	192.168.1.0/25	192.168.1.127/25	192. 168. 1. 1/25 to 192. 168. 126/26	2^7-2 =126

So subnet1 can be allocated to network A.

Now for 50 host, we can use only 6 bit i.e. 2^6 =64, which is sufficient for 50 host+ 1 network + 1 broadcast address.
Again subnetting 2nd subnet with borrowing 1 bit from host we get new subnet mask of /26

192. 168. 00000001.10000000
/25 /26

Subnet 3=192. 168. 1. 128/26
Subnet 4 = 192. 168.1. 192/26
The below table shows the network address, broadcast address, their host range and number of host for 1st subnet

Subnet	Network Address	Broadcast Address	IP Range	No of Uhost =(2^N -2)
3	192.168.1.128/26	192.168.1.191/26	192.168.1.129/26 to 192. 168. 1. 190/26	2^6-2 =62

So subnet 3 can be allocated to network B

Now for 6 computers, we can use only 3 bits i.e. 2^3 =8, which is sufficient for 6host + 1 nw + 1 broadcast. So again subnetting 4th subnet with borrowing 3 bits from host we get new subnet mask of /29
192. 168. 00000001.11000000
/26 /29
Subnet5 = 192. 168. 1. 192/29……..000
Subnet6 = 192. 168. 1. 200/29 …….001
Note we will get 8 subnets with subnet mask of /29
The below table shows the network address, broadcast address, their host range and number of host for 5th subnet

Subnet	Network Address	Broadcast Address	IP Range	No of Uhost =(2^N -2)
5	192. 168. 1. 192/29	192. 168. 1. 199/29	192. 168. 1. 193/29 to 192. 168. 1. 198/29	2^3-2 =6

Subnet 5 can be allocated to network C.

For D, i.e router interface, No of host = 2, i.e. so need to use 2 bits i.e $2^2 = 4$, which is sufficient for 2 host + 1nw + 1 host. So again subnetting 6th subnet with borrowing 2 bits from host we get new subnet mask of /30

192. 168. 00000000.11001000
/29 /30

Subnet 7 = 192. 168. 1. 200 /30

Subnet 8= 192. 168. 1. 204/30

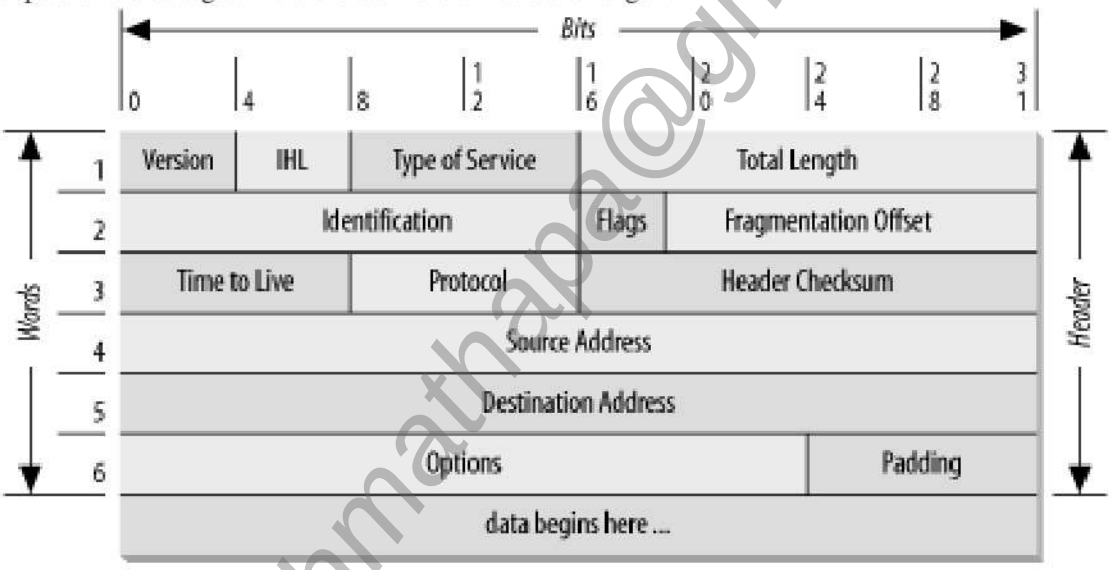
The below table shows the network address, broadcast address, their usable host range and number of host for 7th subnet and 8th subnet

Subnet	Network Address	Broadcast Address	IP Range	No of Uhost =(2^N -2)
7	192. 168. 1. 200 /30	192. 168. 1. 203 /30	192. 168. 1. 201 /30 to 192. 168. 1. 202 /30	2^2-2 =2
8	192.168.1.204/30	192.168.1.207/30	192.168.1.205/30 to 192.168.1.206/30	2

So subnet 7 can be allocated for router interfaces at network D and subnet 8 can be used for router interfaces at network at network E.

IPV4 Datagram / Header Format

- Packets in IP layer are called datagrams.
- An IP datagram consists of two part namely header and data.
- Header is 20 to 60 bytes which carry information essential for routing and delivery.
- The other part of the datagram is the data field of variable length.



- The different field in the IPv4datagram are

1. Version: Define Version of IP address i.e. IPV4 or IPV6.
2. Header Length: These four bits in the header length are used to determine where in the IP datagram the data actually begins.
3. Types of service: This 8-bit field used to describe the quality of service such as delay, throughput, priority and reliability that the router use in processing. When the network is overloaded, for example, it would be useful to be able to distinguish network control datagrams from datagrams carrying data (e.g., HTTP messages). It would also be useful to distinguish real-time datagrams (e.g., used by an IP telephony application) from non-real-time traffic (e.g., FTP).
4. Total length: It determine total length of the data including the header. It is of 16 bit.
1. Identification: It is a sequence number used to reassemble the fragments into packets. It is an integer that identifies the current datagram fragments.

   Note: IP fragmentation is an Internet Protocol (IP) process that breaks datagrams into smaller pieces (fragments), so that packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size. The fragments are reassembled by the receiving host.
2. Flag: This is 3-bit field.

X	DF	MF
Unused	Don't fragment	More Fragment

First bit is reserved and is zero.
The second bit is called don't fragment bit. If DF bit =1, machine shouldn't fragment the datagram, but if DF=0, machine can fragment the datagram if necessary.
The third bit is more fragment bit. If MF bit = 1, then datagram is not the last fragment but if MF=0, then this fragment is the last fragment.

3. Fragmentation offset: This is the 13 bit filed which shows the relative portion of the fragments with respect to the whole fragments.
4. TTL: This is 8-bit long field. It is a counter which limits the packet life time i.e. max number of router visited by the packet before it is considered as undeliverable.
5. Protocol: This field determines the higher level protocol which uses the service of IP layer. This field specify the final destination protocol i.e. TCP, UDP etc. to which the IP datagram should be delivered.
6. Header Checksum: It is used to detect error in the header.
7. Source Address: This 32 field defines the IP address of source.
8. Destination Address: This 32-bit field defines the IP address of destination.
9. Option and padding: Option are not required for every datagram. They are used to support various option such as allowing packets sender to set requirement on the path it take through network, recording route, labelling packets with security features. Padding ensures that headers ends on 32-bit boundary.
10. Data: It is the upper layer information to be delivered to the destination.

IPV6:

- IPv6 is short for "Internet Protocol Version 6".
- IPv6 is the Internet's next-generation protocol, designed to replace the current Internet Protocol, IP Version 4.
- IPv4 addresses are 32 bit whereas IPv6 addresses are 128 bits, which allow for approximately three hundred and forty trillion, trillion unique IP addresses.
- IPv4 general address format is

X:X:X:X:X:X:X:X
where X = 0000 ... FFFF (hex)

- Example:

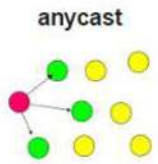
2001:db8:ffff:1:201:02ff:fe03:0405

- IPv6 offers following features
  - **Larger Address Space**
    In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet.

  - **Simpler header:**
    IPV4 header size is variable which can be 20 bytes +, but IPv6 header size is fixed i.e. 40 byte. IPv6's header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4

  - **End-to-end Connectivity**
    Every system now has unique IP address and can traverse through the Internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.

  - **Anycasting i.e one to nearest**
    This is another characteristic of IPv6 which is not found in IPv4. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Then, the routers, while routing, send the packet to the nearest destination.



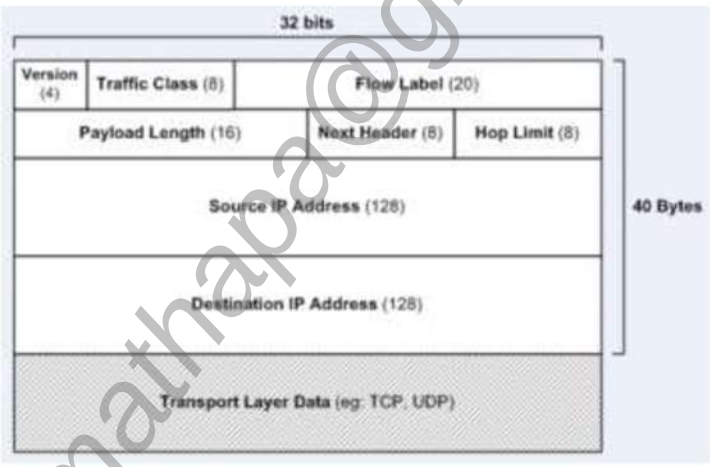
- **No Broadcast**
  IPv6 does not have any broadcast support any more. It uses multicast to communicate with multiple hosts.

- **Mobility**
  IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.

- **Support for more security**
  The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

- **Allowance for extension**
  IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

IPv6 header format



The different field in the IP datagram are

- Version – 4-bit version number of Internet Protocol
- Traffic class – 8-bit traffic class field. It is similar to TOS in IPv4
- Flow label – 20-bit field. It provides additional support for real time datagram delivery and QOS features. A unique flow label is used to identify all the datagram in a particular flow, so each router between source and destination treats in same way so as to ensure uniformity how the datagrams in the flows are delivered.
- Payload length – 16-bit unsigned integer, which is the rest of the packet that follows the IPv6 header, in octets. Total length in IPv4 is replaced by payload length in ipv6.
- Next header – 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. Uses the same values as the IPv4 protocol field.
- Hop limit – 8-bit unsigned integer. Decremented by one by each node that forwards the packet. The packet is discarded if the hop limit is decremented to zero. TTL filed of IPV4 header is replaced by Hop limit field.
- Source address – 128 bits. The address of the initial sender of the packet.
- Destination address – 128 bits. The address of the intended recipient of the packet. The intended recipient is not necessarily the recipient if an optional routing header is present.

- **Ipv4 vs ipv6**

IPV4	IPV6
1. source and destination addresses are 32 bits.)	1. Source and destination addresses are 128 bits.
2. ipv4 support small address space.	2. Supports a very large address space sufficient for each and every people on earth.
3. ipv4 header includes checksum.	3. ipv6 header doesn't includes the checksum. (the upper-layer protocol or security extension header handles data integrity)
4. addresses are represented in dotted decimal format. (Eg. 192.168.5.1)	4. Addresses are represented in 16-bit segments Each segment is written in Hexadecimal separated by colons. (Eg. 2001:0050:020c:0235:0ab4:3456:456b:e560
5. Header includes options.	All optional data is moved to IPV6 extension header..
6.Broadcast address are used to send traffic to all nodes on a subnet.	6. There is no IPV6 broadcast address. Here multicast addresses are used.
7. No identification of packet flow for QOS handling by router is present within the ipv4 header.	7. Packet flow identification for QOS handling by routers is present within the IPV6 header using the flow label field.

ICMP (Internet control message protocol)

- ICMP is a protocol which is used by hosts, routers, and gateways to communicate network layer information to each other.
- The most typical use of ICMP is for error reporting. For example, when running a HTTP session, you may have encountered an error message such as "Destination network unreachable." This message had its origins in ICMP. At some point, an IP router was unable to find a path to the host specified in your HTTP application. That router created and sent a type-3 ICMP message to your host indicating the error. Your host received the ICMP message and returned the error code to the TCP code that was attempting to connect to the remote host. TCP in turn returned the error code to your application.
- ICMP messages are carried inside IP packets i.e. ICMP messages are carried as IP payload, just as TCP or UDP packets are carried at IP payload. Similarly, when an host receives an IP packet with ICMP specified as the **upper layer protocol,** it de-multiplexes the packet to ICMP, just as it would de-multiplex a packet to TCP or UDP.
- ICMP messages have a type and a code field, and also contain the first 8 bytes of the IP packet that caused the IP message to be generated in the first place (so that the sender can determine which packet is sent that caused the error).
- Selected ICMP messages are shown below.
- Note that ICMP messages are used not only for signalling error conditions. The well-known ping program uses ICMP. ping sends an ICMP type 8 code 0 message to the specified host. The destination host, seeing the echo request sends back an type 0 code 0 ICMP echo reply.

ICMP type	code	description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

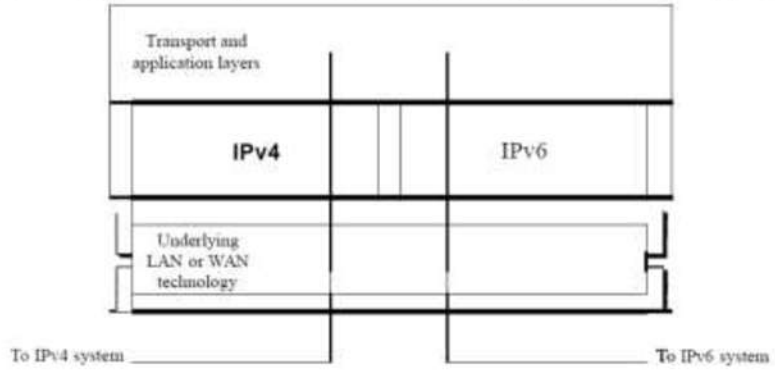
Table 4.4-10: Selected ICMP messages

ICMPv6

- As we know that ICMP protocol is used by IP nodes to report error conditions and provide limited information (e.g., the echo reply to a ping message) to an end system.
- A new version of ICMP has been defined for IPv6 called as ICMPv6 in which in addition to reorganizing the existing ICMP type and code definitions, ICMPv6 also added new types and codes required by the new IPv6 functionality.
- These include the "Packet Too Big" type, and an "unrecognized IPv6 options" error code.
- In addition, ICMPv6 subsumes the functionality of the Internet Group Management Protocol (IGMP) which is used to manage a host's joining and leaving of so called multicast groups, was previously a separate protocol from ICMP in IPv4.

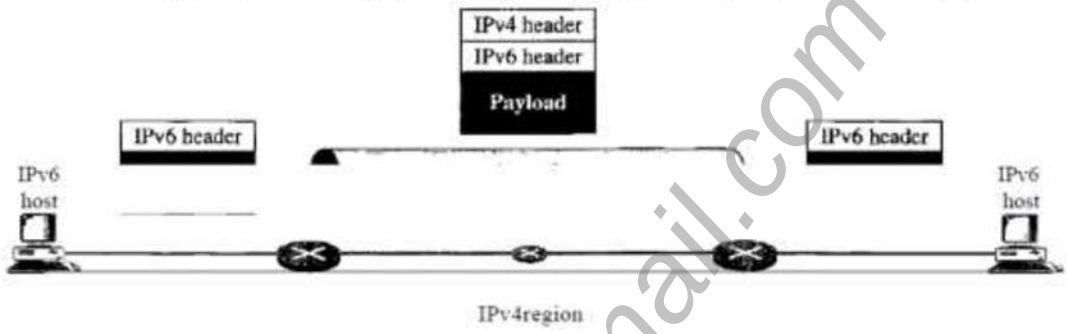
Transitioning from IPv4 to IPv6

- Not all routers can be upgraded simultaneous.
- So the question is how will the public Internet, which is based on IPv4, be transitioned to IPv6? And, How will the network operate with mixed IPv4 and IPv6 routers?
- Three approaches for transition from IPv4 to IPv4
  1. Duel Stack
     - It is recommended that all hosts, before migrating completely to version 6, have a **dual** stack of protocols.
     - In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6

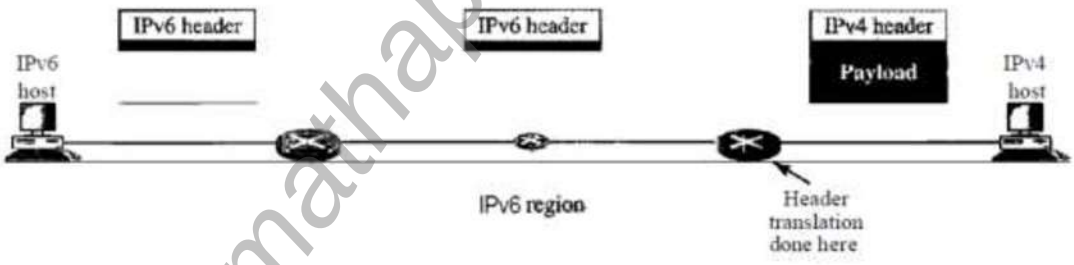


- To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

2. Tunnelling
   - Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4.
   - To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region.
     It seems as if the IPv6 packet goes through a tunnel at one end and emerges at the other end. To make it clear that the IPv4 packet is carrying an IPv6 packet as data, the protocol value is set to 41



3. Header translation
   - Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4.
   - The sender wants to use IPv6, but the receiver does not understand IPv6.
   - Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver.
   - In this case, the header format must be totally changed through header translation.
   - The header of the IPv6 packet is converted to an IPv4 header



Routing Algorithms

- The main function of the network layer is routing packets from the source machine to the destination machine.
- In most networks, packets will require multiple hops to make the journey.
- A hop is the trip a data packet takes from one router or intermediate point to another in the network
- The routing algorithm is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.
- If the network uses datagrams internally, this decision must be made a new for every arriving data packet since the best route may have changed since last time.
- If the network uses virtual circuits internally, routing decisions are made only when a new virtual circuit is being set up. Thereafter, data packets just follow the already established route.
- Routing is the process of making the decision which routes to use, and forwarding, which is what happens when a packet arrives.
- A router provides following two functionalities.
  1. Forwarding: It is the process of moving the packet arriving in the router input link to the appropriate output link.
  2. Routing: It is the process of determining the path or route taken by packet as they flow from sender to receiver.

Classification of Routing Algorithm

1. **Centralized/Global vs Decentralized Routing Algorithm**
   - In Centralize routing algorithm/ Global routing algorithm computes least cost path between source and destination using global knowledge about the network. i.e. it uses connections between all nodes and all link cost as input. In global routing algorithms, every router has complete information about all other routers in the network and the traffic status of the network. Example of such routing algorithm is **Link state algorithm.**

   - Decentralized routing algorithm computes least cost path between the source and destination using iterative distributive manner. No node has complete information about the cost of all network link i.e. has information about those **links that are directly connected**(it doesn't know about every router in the network). So using iterative process of calculation and exchange of information with its neighbour nodes, a node gradually calculates least cost path to destination. Example of such routing algorithm is **distance vector routing algorithm.**

2. **Adaptive vas Non Adaptive Routing Algorithm**
   - In non-adaptive or static routing, the routers forwarding table are configured manually i.e. the network administrator must add and delete the routing information to reflect the network topology change.
   - Static routing is preferred only when the network consists of few routers and when the network is to be connected to the internet only though single ISP.
   - In adaptive or dynamic routing, the routing path changes with change in the topology or network traffic load. So the routing table are build and sustained dynamically. Distance vector, link state routing algorithms are dynamic routing algorithms.

Routing Algorithms

Shortest Path algorithm

- Link between the routers have a cost associated with them.
- The cost can be a function of distance, bandwidth, traffic, communication cost etc.
- The shortest path algorithm finds the least expensive path through the network, based on the cost function.
- Every node in the network computes its routes to every other node in the network.
- Dijkstra's algorithm is used to find the shortest path.
    1. Mark all the nodes as unknown.
    2. For each node V, keep a distance d_v from source node to node V. (d_v = cost of the least cost path from source node to destination node V)
    3. Initially set d_v to ∞ for all node except starting node i.e. $d_v = 0$ for staring node.
    4. Repeat 5 to 7 until all vertex are known.
    5. Select a node V, which has smallest d_v among all the unknown node.
    6. Mark V as known.
    7. For each node W adjacent to V

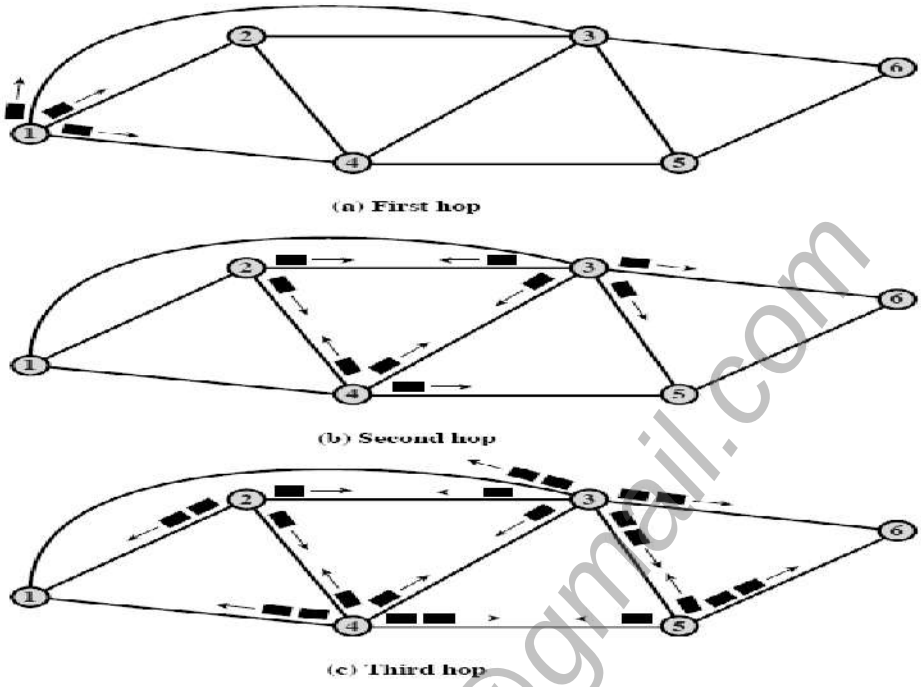
       If w is unknown and $d_v + cost(V,W) < d_W$ update $d_W = d_v + cost(V, W)$
- So upon termination, the algorithm will have calculated the shortest path form source node to every node in the network.

Example: See class note……

Flooding (Static Routing)

- In this algorithm, every incoming packet is sent out on every other link by a router i.e. packet sent by a node to every neighbour.
- It is very simple algorithm but generates a lots of redundant packets hence named flooding algorithm.
- So traffic grows very quickly when every node floods the packet so eventually multiple copies arrive in the destination.
- Duplicate nodes are discarded because each packet is uniquely numbered.
- It is robust algorithm because all possible routes are tried, so could be used to send emergency message.

- It can be used to set up route for virtual circuit because at least one copy of packet will arrive at the destination using a minimum hop route.
- A variant of flooding called **selective flooding** partially addresses these issues not by sending ever incoming packets out on every link, but only on those lines that are going approximately in the right direction.



(a) First hop

(b) Second hop

(c) Third hop

Link State Routing Algorithm

- Also called as shorts path routing algorithm.
- Information about the state of the link is called as link state. Example: Information about neighbour router, cost of that link.
- Link state routing algorithm advertise information about a network topology (directly connected links, neighboring routers…), so that in the end all routers running a link state protocol have the same topology database.
- In link state routing algorithm, each router must do the following.
    - Discover its neighbour and learn their network address.
    - Measure the cost to each of its neighbour.
    - Each router builds a Link-State Packet (LSP) containing the state of each directly connected link.
    - Each router then sends this LSP to all other routers using flooding who then store all received LSPs in their local database
    - Each router then computes the shortest path to every other router using Dijkstras shortest path algorithm by using their **local database information.**
    - The result of this algorithm is kept in routing table.

Example: see class notes……

Note:
Hop count: Hop count is the number of routers that a packet must travel through before reaching destination. Each router is equal to one hop. A hop count of five indicates that data would have to pass through five routers to reach destination. If multiple paths are available to a destination, the path with least number of hops is preferred.

Distance Vector Routing

- As the name implies, distance vector means that routes are advertised as vectors of distance and direction.
- The distance is usually the number of hops (routers) to the destination network (directly or indirectly reachable) and direction is simply the next-hop router or exit interface.
- DV routing algorithm is iterative, distributed and asynchronous algorithm.

- A DV routing algorithm requires a router to exchange information to or from directly attached neighbour for performing calculation and distributing the result of calculation back to its neighbour.
- It has less computational complexity and message overhead than link state routing algorithm because link state require to require to inform all nodes in the network.
- Distance vector uses **Bellman –Ford algorithm** to calculate shortest path as given below

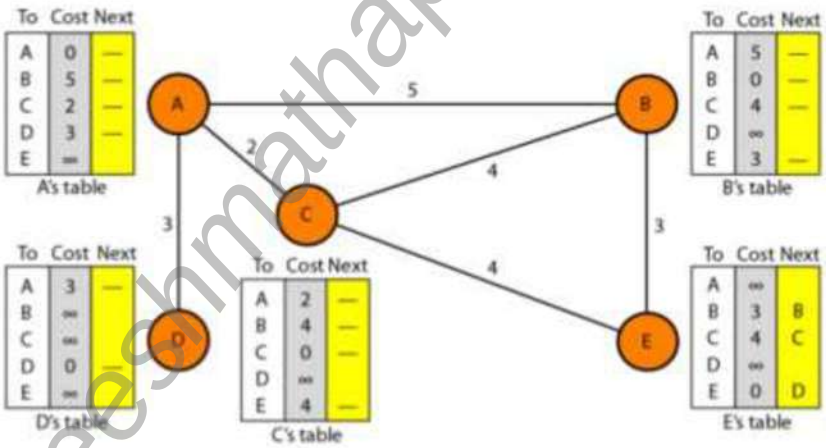
  $D_x(y) = \text{Min } \{C(x,v) + D_v(y)\}$ where $d_x(y)$ = least cost path from vertex x to y, and V are all neighbour vertex V of X.
- Compared with link state routing protocols, distance vector protocols are simpler to configure and require little management, but are susceptible to routing loops (count to infinity) and converge slower than link state routing protocols.
- Distance vector protocols also use more bandwidth because they send complete routing table, while link state protocols sends specific updates only when topology changes occur.
- The basic idea behind DV algorithm is
  - From time to time, each node sends its own distance vector estimates to its neighbour.
  - When node X receive a new Distance vector estimates from neighbour, it updates its own Distance vector using Bellman-Ford equation.
  - The estimated $d_x(y)$ is the actual least cost path.

Example:1

Router1 Router 2 Router 3

In this case, let the Routing metric be delay. The delay from Router 1 to Router2 is X and from router 2 to router 3 is y. Router2 has routing information required for router1 since router2 has routing information of y. hence router1 also knows the estimate of delay to reach from A to C.

Example2:



Let A, B, C, D and E are different routers, and cost represent the delay to reach from one router to next.

Step1:

- Initially each node knows the cost of itself and its immediate neighbour by sending some control message.
- The distance of an entry that is not neighbour is marked as infinite i.e. unreachable.

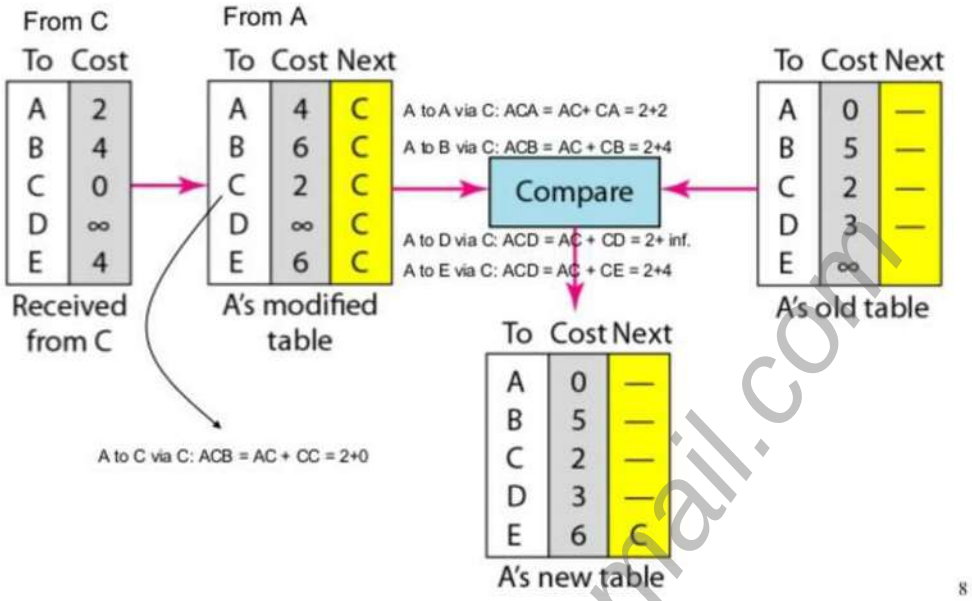
Step2:

- Here there is case like, Node A doesn't have information about E but C does, so if node C share its routing table with node A Then A also can know how to reach to E. so similar concept of **sharing is implemented** between each neighbours periodically and when there is a change in network topology.

Step3:

- When any node receives routing table information from its neighbour then it updates it routing table if better path is inferred then previously calculated.

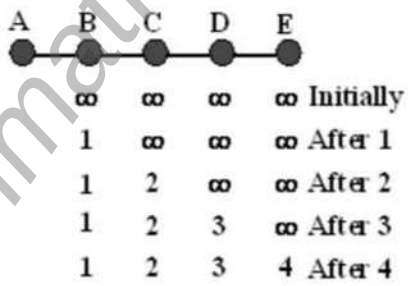
- The update can be done in two ways: first, periodic, in which a node sends its table to its neighbour nodes normally at period of 30 second, and second triggered, in which a node sends its routing table to its neighbour nodes whenever there is change in its routing table.
- Example: Updating the routing table: C to A



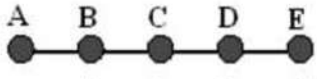
8

Count to infinity problem in Distance vector algorithm

- One of the important issue in Distance Vector Routing is **County of Infinity Problem**.
- Counting to infinity is just another name for a routing loop.
- In distance vector routing, routing loops usually occur when an interface goes down.
- It can also occur when two routers send updates to each other at the same time.
- Consider the following network segment having 5 nodes and all are up



  - Initially delay to A is infinite for all nodes.
  - In first exchange, B knows A is just 1 hop away.
  - In second exchange, C knows A is 2 hop away through B.
  - In third exchange, D knows A is 3 hop away through C.
  - In fourth exchange, E knows A is 4 hop away through E.
- Now consider the link between A and B is broken



1	2	3	4	Initially
3	2	3	4	After 1
3	4	3	4	After 2
5	4	5	4	After 3
5	6	5	6	After 4
7	6	7	6	After 5
.	.	.	.	
∞	∞	∞	∞	

- As seen in the above graph, there in only one link between A and the other parts of the network.
- Initially, When A is up, B, C, D, E have distance 1, 2, 3 and 4 respectively.
- When node A is down then, after first exchange, B notice it and updates its table but when it gets routing information from node C, C says that it has a link to A with the weight of 2 (1 for C to B, and 1 for B to A -- it doesn't know B has no link to A). so B updates its table to 3 via C i.e. B to C=1 and C to A=2
- After second exchange, when C receives B's routing table, it sees that B has changed the weight of its link to A from 1 to 3, so C updates its table and changes the weight of the link to A to 4 (1 for C to B, and 3 for B to A, as B said).
- Then, this process continues for infinite time. This process loops until all nodes find out that the weight of link to A is infinity.
- Hence all routers work their way up to infinity. So called count to infinity problem.

Link State Vs Distance Vector

- Distance vector views the network topology from the perspective of neighbour routers. LS get common view of entire network topology.
- DV add distance vector from router to router. LS calculates the shortest path to all other routers.
- DV sends entire routing table to neighbourhood nodes but Link state sends only link state information on entire net
- DV has less computational complexity and message overhead than link state routing algorithm because link state requires to require to inform all nodes in the network.
- DV is easy to implement than LS.
- DV is more bandwidth intensive than LS.
- DV has frequent and periodic updates but LS has event triggered updates.
- DV is susceptible to routing loops but LS is not.
- DV doesn't knows the entire topology but Link state knows the entire network topology.
- DV converges slower than Link state algorithm.
- DV require less memory and processing power than that of LS.

- **Hierarchical Routing: Interior and Exterior Routing protocols (Routing in internet)**
  - A routing protocol specifies how routers communicate with each other, spreading information that enables them to select routes between any two nodes on a computer network.
  - Although there are many types of routing protocols, three major classes are in widespread use on IP networks:
    i. Interior routing protocols
       - Provide intra-autonomous routing that maintain the routing tables within an autonomous system (AS).
       - Modern TCP/IP routing architecture groups routers into autonomous system(AS) that are independently controlled by different organization.
       - The routing protocols used to facilitate the exchange of routing information between routers within an AS ae called interior routing protocols or interior gateway protocols.
       - As a network administrator for an AS, we are free to choose any routing protocols that best suite our network.

- Example**: RIP (Routing Information Protocol), OSPF (Open Shortest Path First),**

ii. Exterior Routing protocols

- As an inter-autonomous system routing protocol, it provides for routing between autonomous systems.
- The routing information passed between AS is called reachability information.
- Reachability information is simply an information about which network can be reached through a specific autonomous system.
- The routing protocols used to facilitate the exchange of routing information between routers between AS is called Exterior routing protocols or exterior gateway protocols(EGP).
- Example: **BGP (Boarder gateway protocol)**
-

Let us consider the following network segment

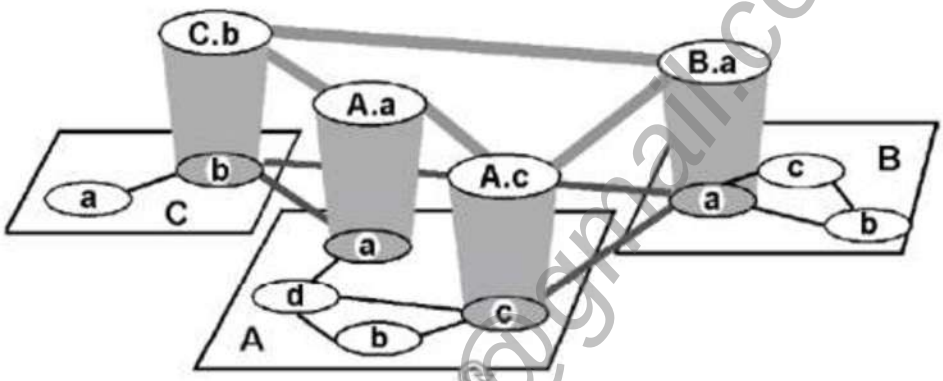


Figure 4.3-1: Intra-AS and Inter-AS routing.

Figure 4.3-1 illustrates this scenario. Here, there are three routing ASs, A, B and C. Autonomous system A has four routers, A.a, A.b, A.c and A.d, which run the intra-AS routing protocol used within autonomous system A. These four routers have complete information about routing paths within autonomous system A. Similarly, autonomous systems B and C have three and two routers, respectively. Note that the intra-AS routing protocols running in A, B and C need not be the same. The gateway routers are A.a, A.c, B.a and C.b. In addition to running theintra-AS routing protocol in conjunction with other routers in their ASs, these four routers run an inter-AS routing protocol among themselves. The topological view they use for their inter-AS routing protocol is shown at the higher level, with "links" shown in light gray. Note that a "link" at the higher layer may be an actual physical link, e.g., the link connection A.c and B.a, or a logical link, such as the link connecting A.c and A.a. Figure 4.3-2 illustrates that the gateway router A.c must run an intra-AS routing protocol with its neighbors A.b and A.d, as well as an inter-AS protocol with gateway router B.a.

RIP

- The Routing Information Protocol (RIP) defines a way for routers, which connect networks using the Internet Protocol (IP), to share information about how to route traffic among networks.
- RIP is classified by the Internet Engineering Task Force (IETF) as an Interior Gateway Protocol (IGP), one of several protocols for routers moving traffic around within a larger autonomous system network -- e.g., a single enterprise's network that may be comprised of many separate local area networks (LANs) linked through routers.
- Each RIP router maintains a routing table, which is a list of all the destinations (networks) it knows how to reach, along with the distance to that destination.
- RIP uses a **distance vector algorithm** to decide which path to put a packet on to get to its destination.
- It stores in its routing table the distance for each network it knows how to reach, along with the address of the "next hop" router -- another router that is on one of the same networks -- through which a packet has to travel to get to that destination.

- If it receives an update on a route, and the new path is shorter, it will update its table entry with the length and next-hop address of the shorter path.
- Using RIP, each router sends its entire routing table to its closest neighbours every 30 seconds. (The neighbours are the other routers to which this router is connected directly -- that is, the other routers on the same network segments this router is on.)
- The neighbours in turn will pass the information on to their nearest neighbours, and so on, until all RIP hosts within the network have the same knowledge of routing paths, a state known as convergence.

OSPF

- It stands for open shortest path first and is used as link state or shortest path first routing algorithm.
- OSPF uses a **link state to** decide which path to put a packet on to get to its destination.
- Routers connect networks using the Internet Protocol (IP), and OSPF (Open Shortest Path First) is a router protocol used to find the best path for packets as they pass through a set of connected networks.
- OSPF is designated by the Internet Engineering Task Force (IETF) as one of several Interior Gateway Protocols (IGPs) -- that is, protocols aimed at traffic moving around within a larger autonomous system network like a single enterprise's network, which may in turn be made up of many separate local area networks linked through routers.
- OSPF **replaced RIP** as distance vector protocol has count to infinite problem and slow convergence.
- Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information.
- Unlike RIP, which requires routers to send the entire routing table to neighbours every 30 seconds, OSPF sends only the part that has changed and only when a change has taken place.
- When routes change -- sometimes due to equipment failure -- the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time.
- So it speeds up convergence, confines network instability to an area and improves performance

Advantage

1. Changes in OSPF network are propagated quickly.
2. It is link state.
3. OSPF support VLSM
4. OSPF uses multicasting within areas.
5. OSPF only sends update packets on routing table which have been changed but it doesn't send the entire routing table.
6. OSPF is an open standard

Disadvantages

1. OSPF is processor intensive
2. OSPF is memory inefficient.
3. OSPF is not easy to learn.

BGP

- It provides inter-autonomous system routing.
- BGP (Border Gateway Protocol) is protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers.
- BGP directs packets between autonomous systems (AS) -- networks managed by a single enterprise or service provider. Traffic that is routed within a single network AS is referred to as **internal BGP, or iBGP**.
- More often, BGP is used to connect one AS to other autonomous systems, and it is then referred to as an external BGP, or eBGP.
- BGP makes routing decisions based on paths, rules or network policies configured by a network administrator.
- Each BGP router maintains a standard routing table used to direct packets in transit.

- This table is used in conjunction with a separate routing table, known as the **routing information base (RIB)**, which is a data table stored on a server on the BGP router.
- The RIB contains route information both from directly connected external peers, as well as internal peers, and continually updates the routing table as changes occur.
- In BGP, instead of advertising networks in terms of a destination and the distance to that destination, BGP devices advertise networks as destination addresses and path descriptions to reach those destinations.
- This means BGP uses, instead of a distance-vector algorithm, a path-vector algorithm.
- Example: customer network such as college, usually employee IGP such as RIP, OSPF are used for exchanging information within their own network but as they connect to ISPs, ISPs use BGP to exchange the customer and ISP routes.

Assignment:

1. **Explain multicast routing.**