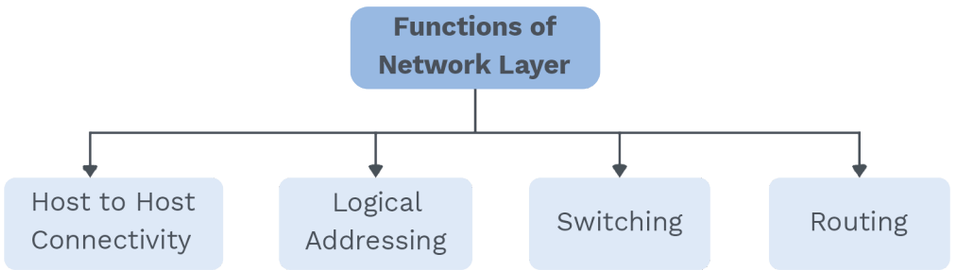
# 4 Network Layer

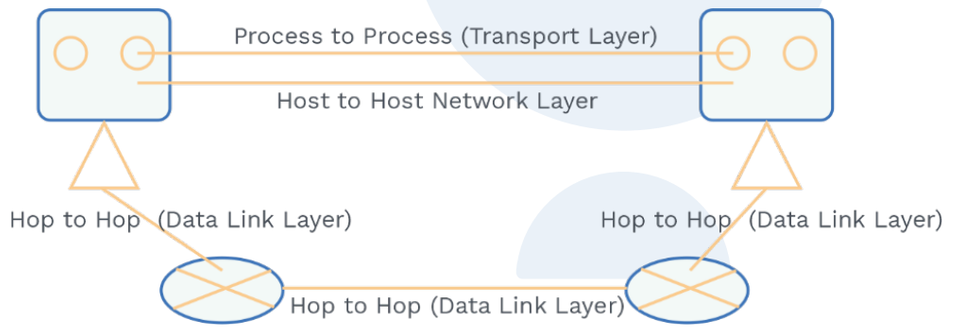


## 4.1 NETWORK LAYER

Across multiple links, the network layer is responsible for source to destination delivery. Is the data link layer not enough? No, as it works on the same links.




**Host to Host Connectivity**




**Logical addressing:**

Now for implementation, logical address is IP addresses having 32 bit number which is globally unique, and physical address are MAC address having 48 bit which is also globally unique.

**Let's talk about IPV4 address:**

It is 32 bit long and unique

What do you understand by unique here!

This means two devices on the internet can never have the same address at the same time.

**Rack Your Brain**

**a)** Can IP be used as Physical Address?
**b)** Can MAC be used as Logical Address?

**Note:**

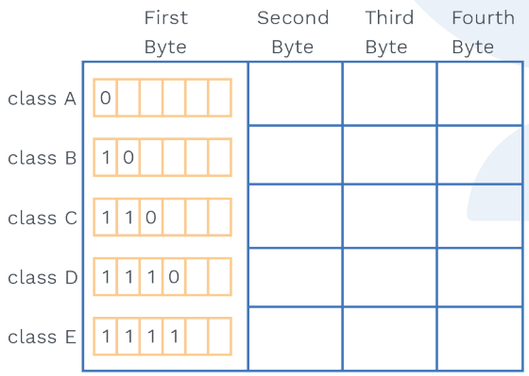
For N bit, there can be $2^N$ values.

For 32 bit address, we have $2^{32}$ address space (4,294,967,296).

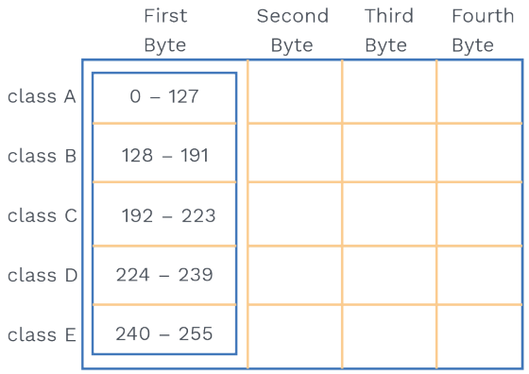
**Notation:**
**Binary notation** – 10000001.10000011.10000010.00000010
**Dotted decimal notation** – 129 . 131 . 130 . 2

**Classful addressing:**
In classful addressing, the address space is divided into five classes: A, B, C, D and E.

**a)** How each class is distributed when it is represented in Binary?
When the address is given in binary notation, the first few bits can signify the class of the address.
Let's say if the starting bits are 110... then it is of class C, and if the address starts from 1110... then it is of class D.
Have a deep look at the below diagram:




**b)** How each class distributed when it is represented in dotted decimal?
When the address is given in decimal–dotted notation, the first byte defines the class.




**Rack Your Brain**

**a)** Change the following binary notation into dotted decimal. 0000 0001.00000011.00001011.10101101
**b)** Change the following dotted decimal into binary notation. 1.3.11.173

**Rack Your Brain**

Identify, below IP address is of which class? 00000001.00000011.00001011.10101101

**Rack Your Brain**

The IP address below is of which class? 25.27.129.15

Now we will see what Net ID and Host ID are!
In IP address, each of 4 bytes is called octets, where each octet has 8 bits. The octets are divided into 2 components – Net ID and Host ID.

Class A, B and C have Net ID and Host ID, class D, and; class E does not have Net ID and Host ID.

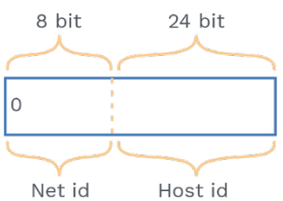
**Note:**

**Net ID:** Network IDs are IP addresses of the network and are used to identify the network.

**Host ID:** Host IDs are the IP address of the host and is used to identify the host within the network.

In Class A, 1 byte denotes Net ID and remaining 3 bytes are Host IDs.
In Class B, 2 bytes denote Net ID and remaining 2 bytes are Host IDs.
In Class C, 3 bytes denote Net ID and remaining 1 bytes are Host IDs.
In Class D, there is no Net ID and Host ID.
In Class E, there is no Net ID and Host ID.
Let's take a look at individual class.

**Class A:**




**Rack Your Brain**

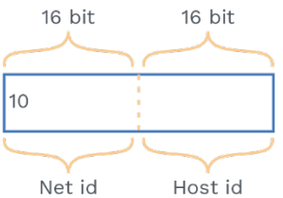
Why 31 bit is taken, why not 32 bit?

- Total number of possible IP addresses available in this class is number of networks * possible number of address in single network.
  $126 * (2^{24}) = 2113929216$
- Total number of networks available in this class is $2^7-2$.
- Total number of hosts available in each network in this class is $2^{24}-2$.

**Why did we subtract 2 from $2^7$?**

IP address 0.0.0.0 is reserved for broadcasting requirements and IP address 127.0.0.1 is reserved for loopback address used for software testing.

**Class B:**

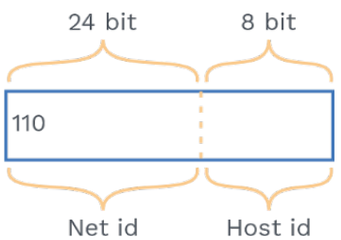



**Rack Your Brain**

Why 30 bit is taken, why not 32 bit?

- Total number of possible IP addresses available in this class is $2^{30}$.
- Total number of networks available in this class is $2^{14}$.
- Total number of hosts available in each network in this class is $2^{16}-2$.

**Class C:**




- Total number of possible IP addresses available in this class is $2^{29}$.
- Total number of networks available in this class is $2^{21}$.
- Total number of hosts available in each network in this class is $2^{8}-2$.

**Class D:**


- Total number of possible IP addresses available in this class is $2^{28}$.
- Class D is reserved for multicasting and there is no need to extract the host address from the IP address in multicasting.

**Class E:**


- Total number of possible IP addresses available in this class is $2^{28}$.
- Class E is reserved for future purposes.

**Mask:**
It is a 32 bit number made of contiguous 1 followed by contiguous 0. It will help to find the Net ID and Host ID.

Let's say the mask for a class A address has eight 1's, which means the first 8 bits of any address in class A define the Net ID, and the next 24 bits define the Host ID.

Default masks for classes A, B and C are given in table.

Summary of what we have read till now is given in table below:

| Class of IP Address | Total Number of IP Addresses | Number of Networks Available | Host Per Network | Default Subnet Mask |
|---|---|---|---|---|
| Class A | 126 * ($2^{24}$) | $2^7$–2 | $2^{24}$–2 | 255.0.0.0 |
| Class B | $2^{30}$ | $2^{14}$ | $2^{16}$–2 | 255.255.0.0 |
| Class C | $2^{29}$ | $2^{21}$ | $2^8$–2 | 255.255.255.0 |
| Class D | $2^{28}$ | | | |
| Class E | $2^{28}$ | | | |

**Note:**
Blank spaces are not defined.

**Concept Building Exercise**

**Q.1** Why are we subtracting 2 in Hosts per network?
**Sol:** The reason is when all Host ID bits are 0, it represents the Network ID for the network, and when all Host ID bits are 1, it represents the broadcast address.

**Q.2** How can we obtain the IP address of the network?
**Sol:** For any IP address, its network ID can be obtained by making all the Host bit 0.

**Q.3** For any Given IP address, How can we obtain Direct broadcast address and Limited broadcast address?
**Sol:** Direct Broadcast address -> make all the Host bit 1
Limited broadcast address -> make all the bit (Net ID and Host ID) as 1

**Q.4** For the given IP address 4.5.6.7, what will be the Class, Network IP address, DBA and LBA?
**Sol:** Class is A because it is in the range (1–126)
Network IP address is 4.0.0.0
Direct Broadcast address is 4.255.255.255
Limited Broadcast address is 255.255.255.255

### Concept Building Exercise

**Q.5** In performing a Loopback address, if the given Ip address is 4.5.6.7, then what will be the source and destination IP?

**Sol:** Source address 4.5.6.7
Destination address 127.0.0.1

**Q.6** What is the default mask for 171.10.55.10?

**Sol:** Given IP address belongs to B, hence default subnet mask is 255.255.0.0.

**Q.7** Which of the following can be used as both Source as well as destination IP?

**a)** 191.2.255.255 **b)** 127.0.0.1
**c)** 255.255.255.255 **d)** 18.18.18.18

**Ans. d)**

**Sol:** **a)** 191.2.255.255 is DBA
**b)** 127.0.0.1 is Loopback address
**c)** 255.255.255.255 is Limited broadcast address
**d)** 18.18.18.18 can be used as Source as well as destination IP

**Note:**
In classful addressing, class A, B and C are used for reserved addresses, class D is used for multicast, and class E is used for future purpose addresses.

**Limitation of classful addressing:**
In classful addressing, we are using fixed classes for special purposes which is not efficient in today's scenario like Class C is used for the midsize organization, but it is not effective as the only Host available per network is $2^8$.

**Rack Your Brain**

For the given IP address 191.5.26.7 what will be the Class, Network IP address, Direct broadcast address and Limited broadcast address?

**Classless addressing:**

- Classless addressing is used now, and classful has become obsolete.
- In classless addressing, ISP (Internet service provider) grants IP addresses based on requirement on the number of customers needed.
- It is an improved version of classful addressing and is also known as CIDR (classless interdomain routing).

**How ISP grants IP addresses?**
There are 3 rules for CIDR block creation:
Rule 1: All the IP addresses must be contiguous in a block.
Rule 2: A block must be in power of 2 ( 1,2,4,8....).
Rule 3: The first address is evenly divisible with number of address.

## PRACTICE QUESTIONS

**Q1** **Block of 4 addresses can be assigned to an organisation having an IP 205.26.24.8 Is it possible?**

**Sol:** According to CIDR,
Rule 1: All the IP addresses must be contiguous in a block.

205.26.24.8, 205.26.24.9, 205.26.24.10, 205.26.24.11

Rule 2: A block must be in the power of 2.
Yes, 4 is power of 2
Rule 3: The first address is evenly divisible by a number of address.
First address is 205.26.24.8 which is divisible by 4 (block size).

**Q2** **What does a CIDR IP address look like?**

**Sol:** p.q.r.s/t
t is used as identifier for network bits.
32-t bits used as identifier for Host bits.

**Rack Your Brain**

**Q)** What is the block address of 2.2.3.4/5?

**Q3** **What do you understand by 192.4.5.6/16?**

**Sol:** Let's first write it in binary.

11000000. 00000100. 00000101. 00000110/16

First 16 bits represents network id.
11000000. 00000100. 0. 0 (Network ID)
As you see, we got the network address by keeping 16 bits as it is and making 32 - 16 bits 0.
Remaining 16 bits are used for the identification of the Host id, in which one of the host is given IP address i.e 192.4.5.6.

**Q4** **Given a CIDR representation 122.10.5.8 / 29. Find the range of an IP addresses in CIDR representation?**

**Sol:** Range means the block which is provided in CIDR.
Octet having decimal value, in binary address will be 122.10.5.00001000 / 29.
Make 29 bits as network address 122.10.5.00001000 (First address of block).
Make remaining bits 32-29 as 1.122.10.5.00001111 (Last address of block).

**Q5** **Following IP addresses are given, can you apply CIDR aggregation?**
**188.67.4.0/24, 188.67.5.0/24, 188.67.6.0/24, 188.67.7.0/24**

**Sol:** 188.67.00000100.0 / 24
188.67.4.0 Number of hosts possible in one network is $2^8$
Rule 1: Is the given block contiguous ! Yes.
Rule 2: Is the size of the block is in power of 2 !! yes.
Total number of host possible is $2^8 + 2^8 + 2^8 + 2^8 = 2^{10}$
Which is in the power of 10
Rule 3: The address of the first block is evenly divisible by the size of the block !!!
188 .67.00000100.0 when divided by $2^{10}$ last 10 significant bits are 0.
Hence yes given block can follow CIDR aggregation.

**Rack Your Brain**

**Q)** Is the following range of IP addresses following CIDR rules 188.67.3.0/24, 188.67.5.0/24, 188.67.6.0/24, 188.67.7.0/24?

**Note:**
The first address in a block is normally not assigned to any device, it is used as the network address that represents the organization to the rest of the world.

**Subnetting:**
An organisation that is generated a large block of address may need to break into small networks (Subnets) On a higher level i.e. from outside the organisation, it works as a signal network, but internally, it may have many networks.


Subnetting is the process of dividing a network into multiple sub networks.

We can divide subnetting into two parts:

Classful Subnetting (Fixed length subnetting)

Classless Subnetting (Variable length subnetting)

Lets see the difference between Classful subnetting and classless subnetting.

**Rack Your Brain**

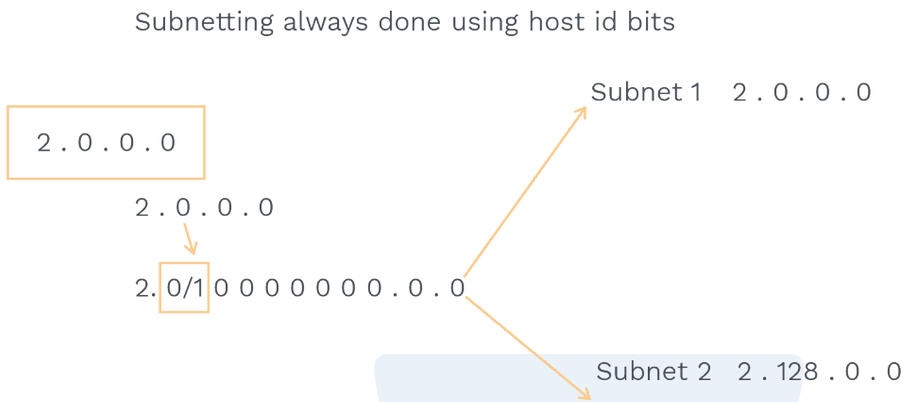
**Q)** Can you guess the advantages of subnetting.

| Classful Subnetting | Classless Subnetting |
|---|---|
| Same size subnets | Different size subnet |
| Subnets have equal number of host | Unequal number of host |
| All the subnet have same mask | Each subnet have different mask |

**Table 4.1 Classful Subnetting vs Classless Subnetting**

Lets say we have a single big network having IP 2.0.0.0.

**We have to make 2 subnet?**
Take one bit from the host id, from one bit we can make two subnet.




- Lets see inside First Subnet i.e Subnet 1.
  Subnet Id of Subnet 1 = 2.0.0.0, this is the Net ID of the Big network also.
  DBA of subnet 1 = 2.127.255.255
  LBA of subnet 1 = 255.255.255.255
- Total number of IP addresses possible in Subnet 1 = $2^{23}$. Why have we taken 23 not 24 bits? one bit is used for subnetting from host part.
- Total number of hosts that can be configured = $2^{23} - 2$.
- Subnet Mask of this subnet = 255.128.0.0
- Range of subnet 1 = 2.0.0.0 to 2.127.255.255 !! Why have we stopped at 127 not 255.
- Since subnet 1 as taken 0 bit on MSB see binary notation of last octet.
  00000010.0000000.0000000.0000000 to 00000010.01111111.11111111.11111111

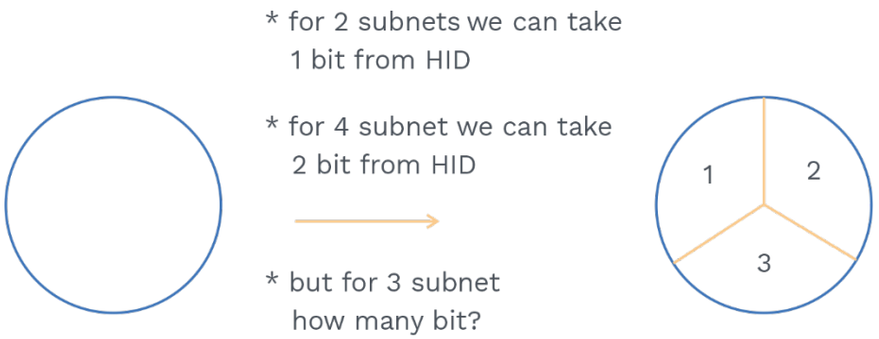
**Lets see inside Subnet 2.**

- Subnet Id of Subnet 2 = 2.128.0.0
- DBA of subnet 2 = 2.255.255.255. this is the DBA of entire network also.
  LBA of subnet 2 = 255.255.255.255
- Total number of IP addresses possible in Subnet 2 = $2^{23}$. Why have we taken 23 not 24 bits? One bit is used for subnetting from host part.
- Total number of hosts that can be configured = $2^{23}$ - 2.
- Subnet Mask of this subnet = 255.128.0.0
- Range of subnet 2 = 2.128.0.0 to 2.255.255.255.
- Since subnet 2 as taken 1 bit on MSB see binary notation of last octet.
  00000010.1000000.0000000.0000000 to 0000010.1111111.11111111.11111111

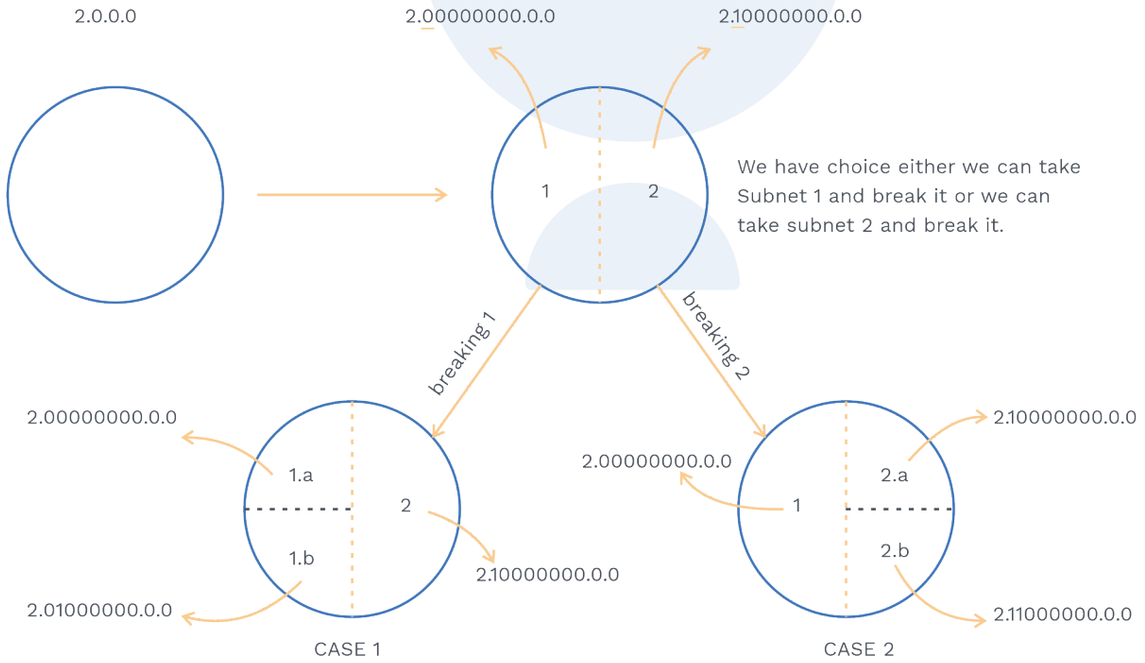
**Rack Your Brain**

Can you divide the network having IP address 2.0.0.0 into 4 Subnet?

We want, to divide this big network having IP address into 3 small networks!
Lets see




For 3 subnet also we have to take 2 bits; see the figure below




3 Subnet having Possible IP address using,

**Case 1:**

2.0.0.0

2.64.0.0

2.128.0.0

**Case 2:**

2.0.0.0

2.128.0.0

2.192.0.0

**Previous Years' Question**

**Q)** An organization requires a range of IP address to assign one to each of its 1500 computers. The organization has approached an Internet Service Provider (ISP) for this task. The ISP uses CIDR and serves the requests from the available IP address space 202.61.0.0/17. The ISP wants to assign an address space to the organization, which will minimize the number of routing entries in the ISP's router using route aggregation. Which of the following address spaces are potential candidates from which the ISP can allot any one of the organization?

**i)** 202.61.84.0/21 **ii)** (202.61.104.0/21

**iii)** 202.61.64.0/21 **iv)** 202.61.144.0/21

**a)** I and II only **b)** II and III only

**c)** III and IV only **d)** I and IV only

**Sol: b)** **(GATE-2020)**

**Let's see how address allocation is done?**

Responsibility of address allocation is taken care by ICANA (Internet Corporation for Assigned Names and Addresses). ICANA gives a block of addresses to ISP; Now it is the responsibility of ISP to divide the block of address into sub-blocks;

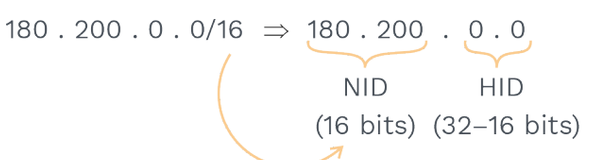
Standard example of subnetting in CIDR

**Example 1:** Suppose ISP grants a block of address starting with 180.200.0.0/16 to Unacademy. Now Unacademy wants to distribute this address into two teams, the names of the teams are NEET. GATE.

**I)** NEET has 32 teams and each team needs 128 address.

**II)** GATE has 64 teams and each team needs 64 address.

**Sol:**



**Q6** **How many possible Host addresses does the Unacademy block have?**

**Sol:** 16 bits are available for address; therefore, $2^{16}$ addresses are possible but first and the last IP should not be assigned to any host therefore $2^{16}$ - 2 Hosts can be configured.

Since the NEET team wants $2^{12}$ and the GATE team wants $2^{12}$.

combinedly need $2^{13}$ address. i.e 8192 address.

Total Available address are $2^{16}$

S0, Available can satisfy the Needs of two teams.

given,

180.200.0.0/16

make, two subnets by borrowing a single bit from HID part 16 bits.

180.200.0/1 0000000.00000000

Suppose NEET team

180.200.00000000.00000000/17 → start

180.200.01111111.11111111/17 → end

it has 32 teams each with 128 address requirements.

for 32 teams take 5 bits.

180.200.0xxxxx00.00000000/22

180.200.00000000.00000000/22 -starts

180.200.01111100.00000000/22 -End

suppose GATE team.

180.200.10000000.00000000/17 -- start

180.200.11111111.11111111/17 --end

it has 64 teams with each 64-address requirement.

for 64 teams take 6 bits.

180.200.1xxxxxx0.00000000/23

180.200.10000000.00000000/23 –starts

180.200.11111110.00000000/23 --ends

**Rack Your Brain**

How many total addresses are present in the NEET team?

**Example 2:** A subnet mask 255.255.192.0.0 belongs to class B.
How to find the number of subnets in this subnet mask.

NID

11111111 . 11111111 . 11 000000 . 00000000

SID

No. of bits in Subnet = 2

Total number of subnet possible = $2^2 = 4$

How to find the number of hosts in each Subnet?

NID

11111111 . 11111111 . 11 000000 . 00000000

SID HID

14 Host id bits → $2^{14}$ address for each subnet

Since 1st and last address are not used

$\therefore 2^{14} - 2$ address possible

**Example 3:** A subnet mask 255.255.0.0 belongs to class A.
How to find number of subnets in this subnet mask.
Class A net id has 8 bits.
Given Subnet mask has 16 nits.
Number of subnet bit = 16 - 8 = 8 bits (see below figure for more information).

11111111 . 11111111 . 00000000 . 00000000

for class A → 11111111 . 00000000 . 00000000 . 00000000 (NID)

No. of subnet bit = $16 - 8 \Rightarrow 8$

Possible no. of subnet $\Rightarrow 2^8 \Rightarrow 256$

How to find the number of subnets if subnet mask 255.255.0.0 belongs to class B.

for class B → 11111111 . 11111111 . 00000000 . 00000000

No. of subnet bit = $16 - 16 \Rightarrow 0$

Possible no. of subnet $\Rightarrow 2^0 \Rightarrow 1$

How to find the number of subnets if subnet mask 255.255.0.0 belongs to class C.

for class C ⟶ 11111111 . 11111111 . 00000000 . 00000000

No. of subnet bit = Not possible

**Why is the subnet not possible in the above case!!**
For Subnet Mask for class C (255.255.255.0), all 1's cover the given subnet mask (255.255.0.0). Hence there are no extra 1's which can be used in subnetting therefore, subnet is not possible.

**Supernetting:**
Combination of multiple networks into one single network by following some rules is Supernetting.
Rules for Supernetting:
Rule 1: All the IP addresses must be contiguous in a block.
Rule 2: A block must be in power of 2 (1,2,4,8....)
Rule 3: The first address is evenly divisible with number of address.

**Concept Building Exercise**

**Q.8** Can we come up with a bigger network of given sub networks?
200.100.10.0
200.100.12.0
200.100.15.0
200.100.17.0

**Sol:** In this Even first rule is not followed, therefore we cannot perform supernetting.

**Q.9** Let's make above subnetworks contiguous.
200.100.10.0
200.100.11.0
200.100.12.0
200.100.13.0

**Sol:** In this first and second rule is followed but third rule is not followed.
First address i.e 11001000.01100100.00001010.00000000.
Block size is $2^{10}$
But first address is not divisible by $2^{10}$; therefore cannot perform supernetting.

**Network address translation:**

**a)** With a shortage of available IP, there is a need for translation of addresses. NAT comes as a solution for this problem.

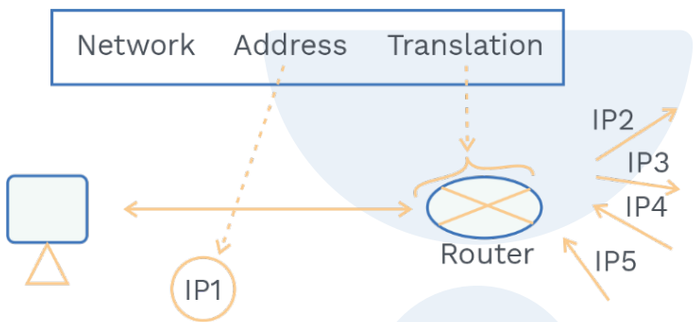
**b)** In the given diagram, $IP_1$ is used inside the organisation, while outside the organization it can be treated as $IP_2$, $IP_3$ depending upon the situation.

**c)** Inside the organization, $IP_1$ is called as Private IP.

**d)** Outside the organization, $IP_2$, $IP_3$, $IP_4$ and $IP_5$ are called public IP.

**Rack Your Brain**

Can prepladder distribute IP addresses to UPSC groups, in this UPSC group there are 511 teams, and each team needs 512 addresses.




**How does a host get to know that a particular IP coming from the internet is it's or not?**

**Answer:** It is the NAT table. A NAT table is responsible for mapping each private IP to its corresponding public IP.

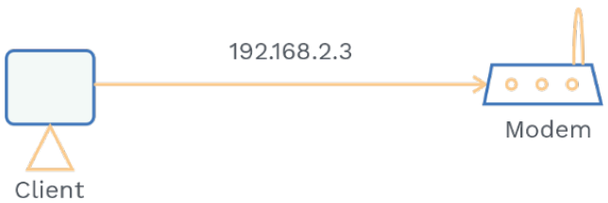
The Internet authorities have reserved three sets of addresses as private addresses.

| Range | Total |
|---|---|
| 10.0.0.0 to 10.255.255.255 | $2^{24}$ |
| 172.16.0.0 to 172.31.255.255 | $2^{20}$ |
| 192.168.0.0 to 192.168.255.255 | $2^{16}$ |

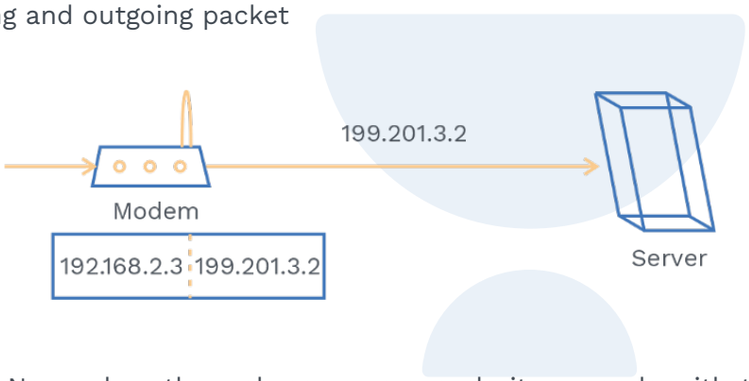
**Table 4.2 Range of Private IP Addresses**

Lets understand the NAT working:

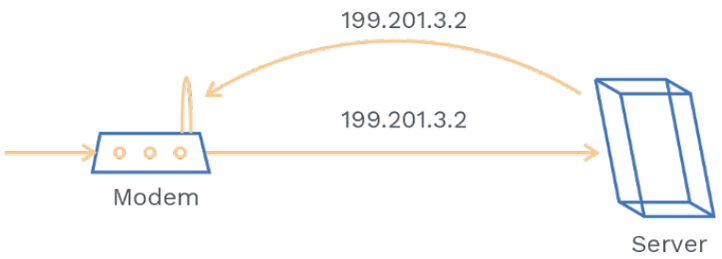
**Step 1:** Client send an IP packet to access point:



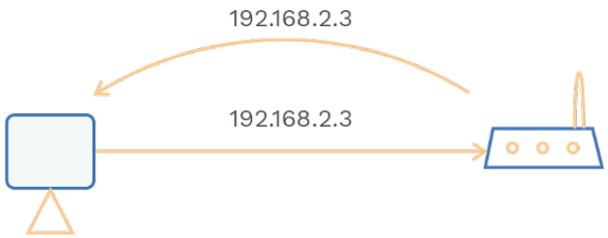

**Step 2:** Now the modem or access point sends the IP packet with a different IP address to the server. In addition to this, it records the mapping of the incoming and outgoing packet




**Step 3**: Now, when the web server responds it responds with the same public IP address.




**Step 4**: Access point gives back packet to the client.



### Concept Building Exercise

**Q.10** How will NAT use this mapping when the packet has source IP 192.168.22.1 returns from the server?
**NAT Table:**

| Source IP | Destination IP | Source Port | Destination Port | NAT Port |
|---|---|---|---|---|
| 192.168.22.1 | 200.200.1.1 | 2456 | 80 | 4000 |
| 192.168.11.2 | 201.102.1.1 | 1245 | 21 | 5000 |

**Sol:** It will look like this.
Source IP 200.200.1.1
Destination IP 192.168.22.1

**Q.11** What types of devices can do NATing?
**Sol:** It can be Routers, Switch, even some servers also.

**Note:**

Despite having NAT, the depletion of IP address is not yet solved.
IPv4 does not provide better security features on its own.
By maintaining the basic functionality of IP addressing, IPV6 comes into the picture.
Let's discuss IPv6 addressing.

**Points:**

**1)** It is 128 bit long, hence a larger address space (IPV4 is 32 bit long).
**2)** IPv6 can be written in hexadecimal and binary notation.

### Rack Your Brain

**Q)** Is NATing always preferable? If yes, then What will happen if some protocol changes the position of the IP address inside the IP packet? Do you still think it's always good!!

**a)** In Binary we denote IPv6 something like this

$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8\ b_9\ b_{10}\ b_{11}\ b_{12}\ b_{13}\ b_{14}\ b_{15}\ b_{16}.$
$b_{17}\ b_{18}$ ..... $b_{32}$ .
$b_{33}\ b_{34}$ ..... $b_{48}$ .
$b_{49}\ b_{50}$ ..... $b_{64}$ .
$b_{65}\ b_{66}$ ..... $b_{80}$ .
$b_{81}\ b_{82}$ ..... $b_{96}$ .
$b_{97}\ b_{98}$ ..... $b_{112}$ .
$b_{113}\ b_{114}$ ..... $b_{128}$ .

Now if write IPv6 in binary every time, it would be long, hence we can use hexadecimal notation also.

**b)** In hexagonal notation, IPv6 looks like:

$h_1\ h_2\ h_3\ h_4 : h_5\ h_6\ h_7\ h_8 : h_9\ h_{10}\ h_{11}\ h_{12} : h_{13}\ h_{14}\ h_{15}\ h_{16} :$
$h_{17}\ h_{18}\ h_{19}\ h_{20} : h_{21}\ h_{22}\ h_{23}\ h_{24} : h_{25}\ h_{26}\ h_{27}\ h_{28} : h_{29}\ h_{30}\ h_{31}\ h_{32}$

There are 8 octets in hexadecimal notation, each octets is having 2 byte in length

**1) Abbreviations in IPv6:**

The need for abbreviations in IPv6 is that if we write in hexadecimals, then also there are some zeros which can be shortened. Hence we come up with rules which can reduce the size of hexadecimal notation illustrated below.

FDAB : 0017 : 000F : 0000 : 0000 : 0000 : A123 : 4567

Refined → FDAB : 17 : F : 0 : 0 : 0 : A123 : 4567

More Refined → FDAB : 17 : F : : A123 : 4567

**Points from above illustration:**

**a)** Leading zeros can be eliminated.
**b)** Lets say 0017 can be written as 17.
**c)** If there are consecutive zeros that can be replaced by a double colon.
**d)** Only leading zeros can be removed not the trailing zeros like 4120 cannot be written as 412.

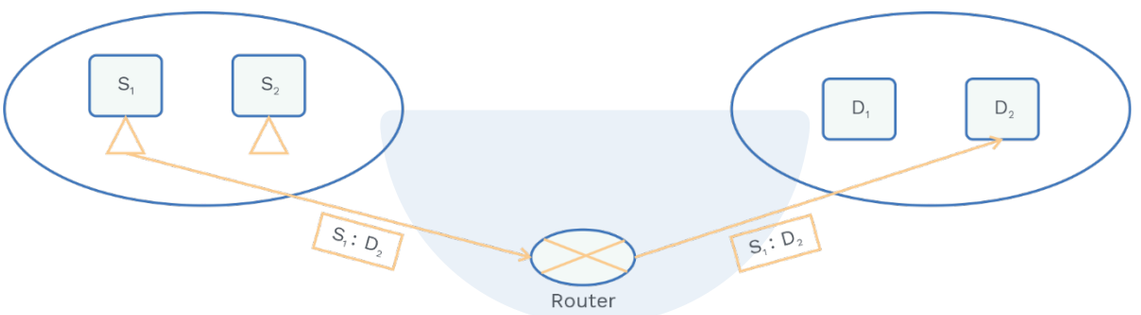
**Rack Your Brain**

Expand: 13:: 123: FFFF: ABCD: 1AC0

**e)** With a larger number of IP addresses, end to end connectivity can be easily done.
**f)** No broadcasting in IPv6, though multicast is there to communicate multiple host.
**g)** IPv6 has different types of addressing modes UNICAST, MULTICAST and ANYCAST.

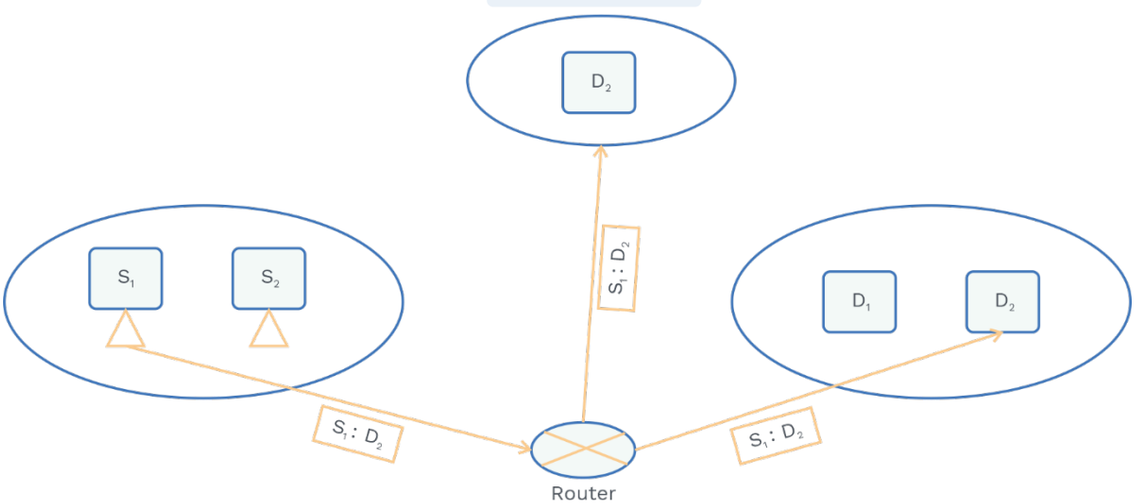
**UNICAST:**

- It is based on one source and one destination.
- In unicasting, the router forwards the received packet through only one of its interfaces.
- Forwarding a packet is done only one of its interfaces.
- Its a type of one one communication.



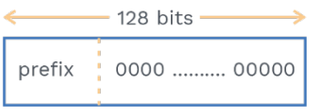

**MULTICAST:**

- There is one source and one group of destinations.
- In this source is unicast, but the group of destinations is multicast.




A multicast packet starts from S1 and sends it to groups D2 at all interfaces.
In multicasting, the router may forward the received packet through several of its interfaces.

**ANYCAST:**
Standard point from cisco: Assigning a unicast address to more than one interface makes a unicast address an anycast address.
Host which is closest to the Sender will receive the unicast message.




**Concept Building Exercise:**

**Q.12** 01000011.... patterns come as IPv4 packets, Can you tell if it is a valid pattern?
**Sol:** NO,
First 4 bit are version 0100
Next four bit are header length i.e 0011 it comes out as 3 * 4 = 12
Header length at least should be 20.

**Q.13** Hogwarts has the block 15.0.0.0/8. Albus Dumbledore wants to create 400 fixed-length subnets.
**a)** Find the subnet mask.
**b)** Find the number of addresses in each subnet that can be assigned.
**c)** Find the first and last addresses in subnet.

**Sol:** **a)** Subnet mask:
Albus Dumbledore wants fixed length Subnet.
He needs 9 bits for 400 fixed length subnets.
Subnet mask will have 8+9 = 17 bits
It will look like 15.0.0.0/17
**b)** Number of possible address in each subnet that can be assigned.
$2^{32-17}$ - 2 addresses will be assigned as a host in each subnet
**c)** First and last possible addresses in subnet 1 that can be assigned.
Assuming 15.0.0.0 is subnet 1
Now first possible address would be 15.0.0.1
Last possible address would be 15.0.127.254

**Note:**

**1)** In order to find the Subnet ID or number of Subnet, We have to know class ID or NID.
**2)** Even without knowing the class of network, we can find HID.

**Example 1:** Subnet mask = 255.255.255.128 and it is from class A.

**Sol:**
We know NID + SID = Total number of 1
HID = No of Zeros

Number of 1's is 25
NID in class A = 8 bits
SID = 17
Number of Subnet = $2^{17}$

Number of 0's = 6
IP address = $2^6$
Possible Host = $2^6$ - 2

**Example 2:** What should be the value of n in a.b.c.d/n, when we want a block size as $2^{15}$?

**Sol:** It should be 32 - 15 = 17
NID = 17 bits

**Example 3:** Can you mention all the IP addresses present in 10.1.5.0/30 block ?

**Sol:** It has 4 IP addresses

10.1.5.0/30

10.1.5.1/30

10.1.5.2/30

10.1.5.3/30

**Note:**
In above solution only 2 IP can be used as Host ID.

**Previous Years' Question**

**Q)** Every host in an IPv4 network has a 1–second resolution real–time clock with battery backup. Each host needs to generate up to 1000 unique identifiers per second. Assume that each host has a globally unique IPv4 address. Design a 50–bit globally unique ID for this purpose. After what period (in seconds) will the identifiers generated by a host wrap around?

**Sol: 256** **(GATE-2014)**

Special IP address chart and their meaning:

| NID | HID | Description |
|---|---|---|
| ✓ | ✓ | Valid IP Address |
| ✓ | 0'S | Network IP |
| ✓ | 1'S | Directed Broadcast |
| 1'S | 1'S | LImited Broadcast |
| 1'S | 0'S | Subnet Mask |
| 0'S | ✓ | Host within N/w |
| 0'S | 0'S | Host dont know IP |
| 127 | ✓ | Loop Back address |

**Need for network layer:**
Since the data link layer was responsible for Hop to Hop delivery, there needs a mechanism which will take care of host to host delivery through routers.

You may think Host to Host delivery can also be done through a data link layer! yes, possible only when these two hosts share a single network. What if they share a different network? Network layer takes care of this situation.

**Note:**
Internet uses datagram approach in packet switching.

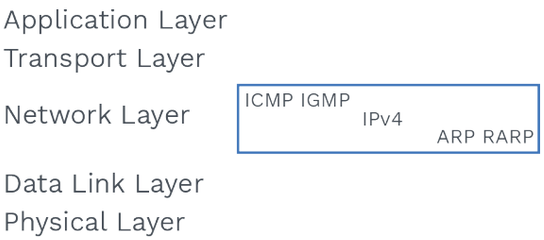
Internet protocol version 4 is used by TCP/IP model.
Look where IPv4 is placed at TCP/IP suite.

**Grey Matter Alert!**

Internet uses datagram approach, ATM and frame relay uses virtual circuit approach.

**Rack Your Brain**

Is the Internet connection-oriented or connectionless since we know it uses datagram services?




IPv4 has no error control and no flow control, IP relies on TCP in order to take care of error and flow control.

**What are we called packets at IPv4?** Datagram packets.
**IPv4 datagram format:**

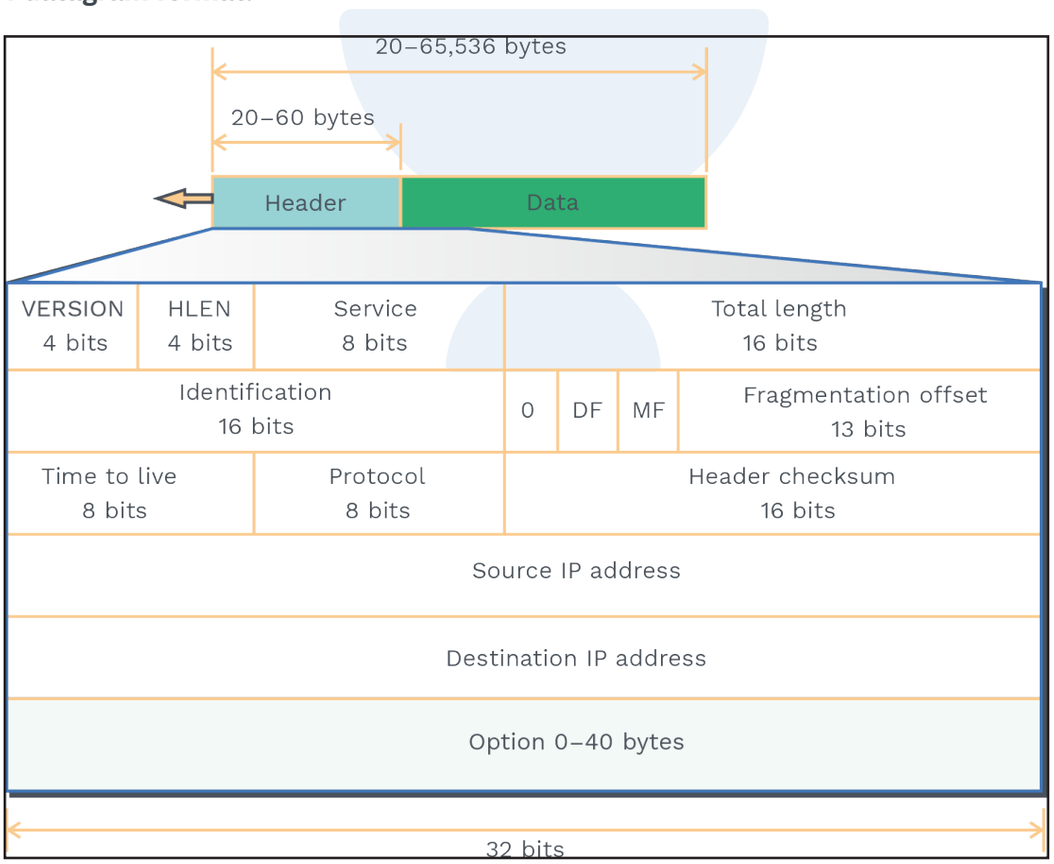



**Fig. 4.1 IPV4 Header Format**

**Version:** It has 4 bit,

- IPv4 uses version 4 whereas IPv6 uses version 6.

- Binary 0100 can be written in this field.

**Header length:**
- It has 4 bit.
- It defines length of IP header.

**Note:**
What is the minimum and maximum length of the IP header?
Minimum length = 20 Bytes, How? number of essential rows * size of each rows i.e 5 * 4 bytes.
Maximum length = 60 bytes, How? Maximum size of options are 40 bytes
20 + 40 = 60 bytes.

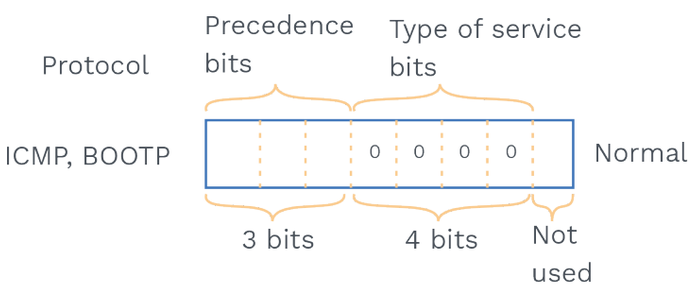
**Example:** If IPv4 has a binary pattern starting with 0100010.. What does this mean?
This means packet has version 4 and header length is 2 * 4 = 8 bytes.

**Example:** If IPv4 has a binary pattern starting with 01001111.. What does this mean?
This means packet has version 4 and header length is 15 * 4 = 60 bytes.

**Grey Matter Alert!**

- We have minimum and maximum length as 20 and 60 bytes respectively.
- But at header length we have only 4 bits i.e using 4 bits maximum we can go upto 15 bytes.
- It leads to the concept of scaling factor in this case it is 4 bytes.
- Header length = Header length field value * 4 bytes. If header length field contains decimal value 6 (represented as 0110), then-Header length = 6 x 4 = 24 bytes.

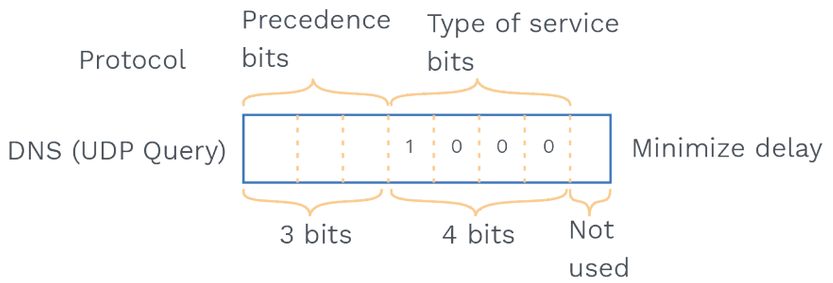
**Service:** It has 8 bit fields.




- Precedence bits are never used.
- Types of bits are used for various purposes depending on the protocol for ICMP and BOOTP it uses 0000 bits at Type of services.

**Rack Your Brain**

What is the range of Header length and Header length field?




**Total length:** It has 16 bit fields.
What is the minimum and maximum total length?
Minimum total length = Header length + Payload length

$$20 + 0 = 20 \text{ bytes}$$

Maximum total length = > with 16 bits we can go upto $(2^{16} - 1)$ bytes = 65535 bytes.

**Example:** In IPV4 packet HLEN is 7, value of total length field is 0x0033, How many
bytes of data are being carried?
HLEN = 7, number of bytes in header = 28 bytes (1 byte from the option)
Total length = 51 bytes
Packet carrying data = 51 - 28 = 23 bytes

**Identification:** It has a 16 bit field.

- From datagram packets, this field is responsible for the identification of fragments.
- Let's say there are n fragments; then each fragment are assigned the same identification number.
- Why is the identification number given to each fragment? So that during reassembly router can identify which IP datagram the fragments belong to.

**Flags:**
There are 3 bits, one bit uses do not fragment bit; one bit uses more fragment bits, and one bit is reserved.

**Do not fragment bit:** The value of this field can be 0 (do fragment if required) or 1 (do not fragment).
**More fragment bit:** It may be 0 (last fragment or only fragment) or 1 (more fragments are present behind this packet).

**Fragment offset:** It is has 13 bit.
It is equal to number of bytes ahead of it.

**Note:**
total length field = 16 bits = > 65535 Bytes.
Fragment offset = > 13 bits which will give $2^{13}$ - 1 bytes = 8191 Bytes.
Scaling is done because fragment offset cannot represent sequence of bytes greater than 8191.
Scaling factor in fragment offset = $2^{16}$ / $2^{13}$ = $2^{3}$
Fragment offset field value = fragment offset/8

**Time to live:** It is a 8 bit field.

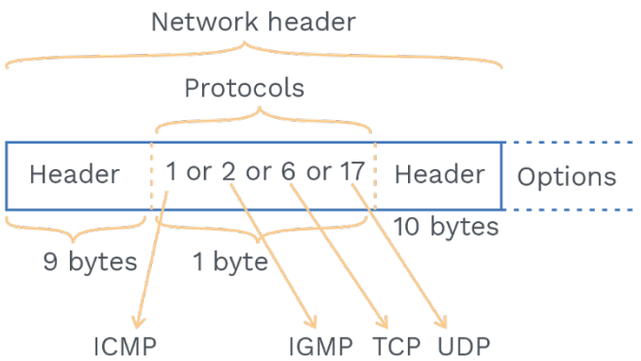
- Purpose of TTL is to prevent from looping.
- Devices which is having network layer decreases TTL by 1.
- At destination, value of TTL must be 0 or greater than 0 then the datagram packet will be accepted.
- At, the intermediate the value of TTL must be greater than 0; otherwise packet will be discarded.

**Protocol:** It is a 8 bit field.

**Protocol values**

| Value | Protocol |
|---|---|
| 1 | ICMP |
| 2 | IGMP |
| 6 | TCP |
| 17 | UDP |
| 89 | OSPF |

Which protocol IP datagram belongs depending on the value inside the protocol field.




These numbers will eventually decide the router when the traffic becomes heavy which packet to discard.

The sequence of discarding the packet at routers is ICMP > IGMP > UDP >TCP

Means, TCP is the least discarded.

**Header checksum:** It is a 16 bit field
Checksum value stored in this field

At every router, checksum is calculated if it is not matched with the value present in the header, then the packet is discarded.

What are the fields that may be modified at every router?
TTL, Fragment offset, Header length, Datagram length, Options

**Rack Your Brain**

Why is checksum used at the Network layer?

**Source IP address:**
- It is a 32 bit fields.
- It is having IPv4 address of the source.

**Note:**
IPv4 address must not change until packet reaches destination.

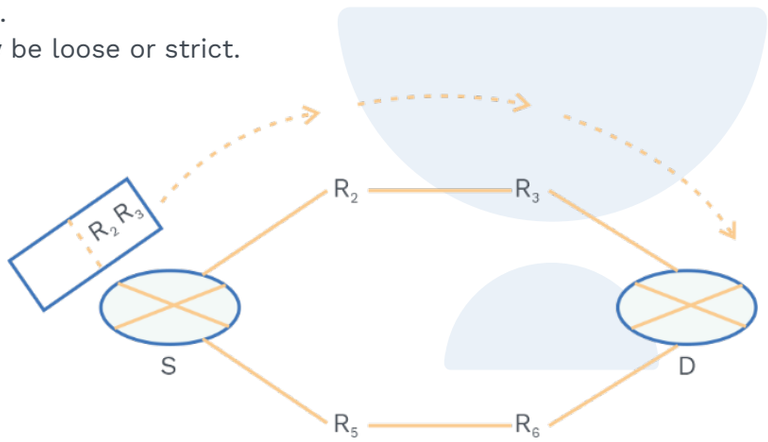
**Destination IP address:**
- It is a 32 bit fields.
- It is having IPv4 address of the destination.

**Note:**
IPv4 address must not change until packet reaches source.

**Options:** It has 0 to 40 bytes
- They are not mandatory but can be used for testing.
- Mainly it is used for source routing, record route and padding.

**Record route:**
When this option is set in the options field, the IP address of the router gets recorded in the options field.

**Source routing:** This field is used in order to check if the path is working or not.
It may be loose or strict.




**Padding:** Addition of dummy data to fill up space and make it a standard size is called padding, usually done through options only.
Options are actually used for testing and debugging.
Let us understand fragmentation through example.

**Example:** A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Give your view about fragmented packets?

**Sol:** Since M bit = 0,
This may be the last fragment but since we don't know about the fragmentation offset, we cannot say about the fragmented packet is the first, last or middle.

| MF | Fragment Offset | Description |
|---|---|---|
| 0 | 0 | Invalid |
| 0 | !0 | Last packet |
| 1 | 0 | First packet |
| 1 | !0 | Intermediate packet |

**Previous Years' Question**

**Q.** In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400, and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively, are:

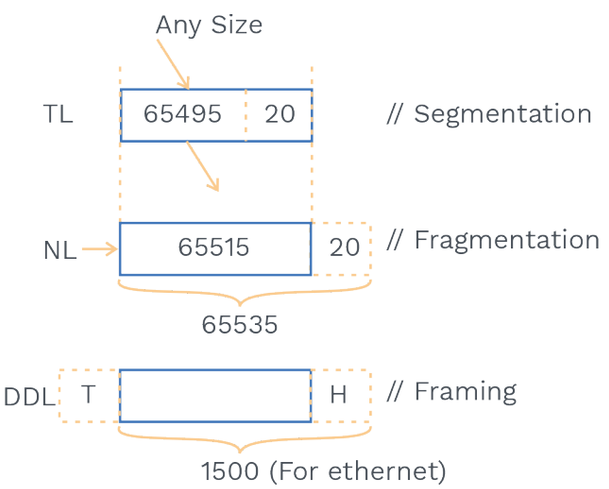
**a)** Last fragment, 2400 and 2789
**b)** First fragment, 2400 and 2759
**c)** Last fragment 2400 and 2750
**d)** Middle fragment 300 and 689

**Sol: c)** **(GATE - 2013)**

**Fragmentation:**

When the datagram is divided inorder to pass through other networks, this is called fragmentation.

Let us see the below scenario,



How we can limit fragmentation at the sender side!!

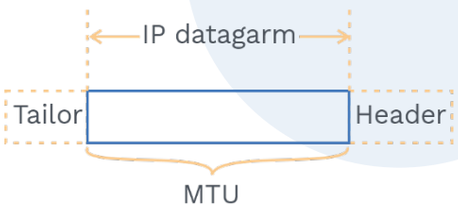
When TL segments the data in such way, that size of data can easily be taken by the network layer as well as in the data link layer.

Now, who will do fragmentation?

Sender and router, but keep in mind sender can limit the fragmentation by proper implementation.

**Note:**

MTU (Maximum Transmission Unit) is the maximum length that can be encapsulated in a frame.




**Points for fragmentation:**
It increases the datagram overhead because after fragmentation, IP header needs to be attached at every packet.
**1)** Total overhead = (Total number of fragmented datagram -1 ) * size of IP header.
**2)** Efficiency = Useful Bytes transferred / Total Byte transferred.
**3)** Bandwidth utilization or throughput = Efficiency * Bandwidth.
Understand Fragmentation using Example.

**There are two networks, A and B. Network A has MTU 1020 Bytes and Network B has MTU 500 Bytes.**
**Host P wants to send the message to Host Q.**
See the figure below,

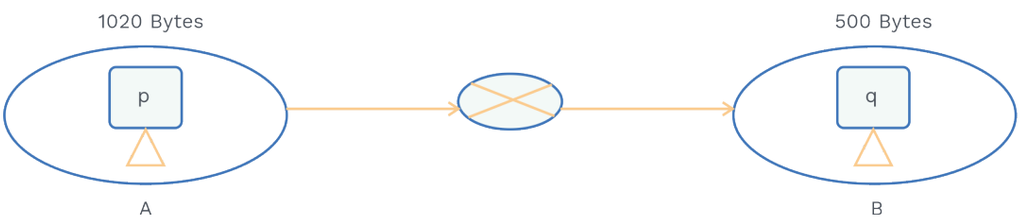



**Fig. 4.2 Diagrammatic Representation of the Process of Fragmentation**

Explanation how fragmentation will occur at router:

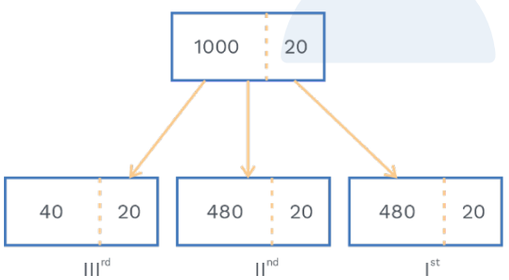
**Step 1:**
When Router receives the datagram packet having a Total size = 1020B, and if the DF flag is 0, now it can do fragmentation.

**Step 2:**
It will check if the network B MTU can accommodate the packet or not!
If not, then it will start fragmentation according to the MTU size of network B.

**Step 3:**
Here, MTU network B is 500 Bytes.
Out of 500 Bytes 20 Bytes will be the header, and 480 Bytes will be payload.
Maximum amount of data that can be sent at each fragment = 480.

**Note:**
Payload at each fragment must be multiple of 8 except the last fragment i.e. last packet may or may not have a multiple of 8 data byte.

See diagram below,




Lets see the header information of I$^{st}$ fragment.
Total length = 500
Fragment offset = 0
Header checksum will be calculated again.
MF bit = 1
Identification number = same to all fragments.

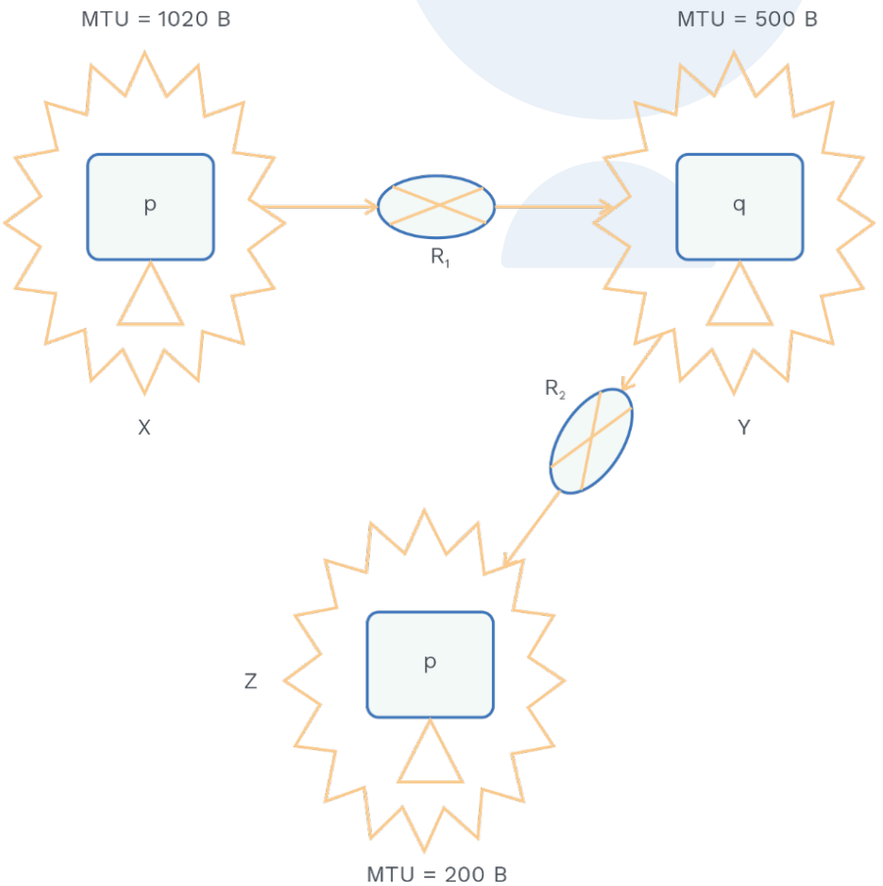
Information for II$^{nd}$ fragment.
Total length = 500
Fragment offset = 480/8 = 60

Header checksum will be calculated again.
MF bit = 1

Identification number = same to all fragments.
Information for III$^{rd}$ fragment.
Total length = 500
Fragment offset = (480 + 480)/8 = 120
Header checksum will be calculated again.
MF bit = 0
Identification number = same to all fragments.

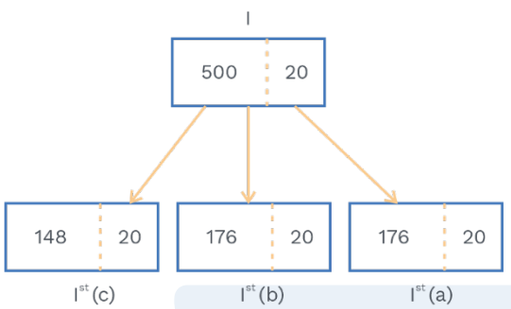
Receiver will take all the three segments and reassembly algorithms applied to get the original datagram.

Let's take the second scenario of the above example.

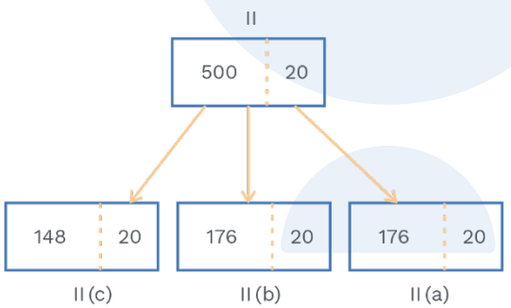


Router 2 will receive a datagram of 500B, but it can't forward directly, because MTU of next network Z is 200B.

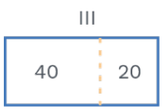
Router 2 will perform fragmentation for the I$^{st}$ datagram.




Router 2 will perform fragmentation for II$^{nd}$ datagram.




Router 2 will not perform any fragmentation for III$^{rd}$ datagram.




**Note:**
We have taken 176 byte in I.a,I.b, II.a and II.b because datagram byte must be divisible by 8.

**Reassembly algorithm:**
Receiver applies the following steps:

**I)** Identifies whether datagram fragmented or not using MF bits and fragments offset bits.

**II)** Using Identification fields, it identifies all the fragments belonging to the same packet or not.

**III)** Fragment with offset field 0 is first fragment.
**IV)** identifies subsequent fragments using total length, header length and fragment offset.
**V)** Repeats step IV until MF = 0

**IPv6 header:**

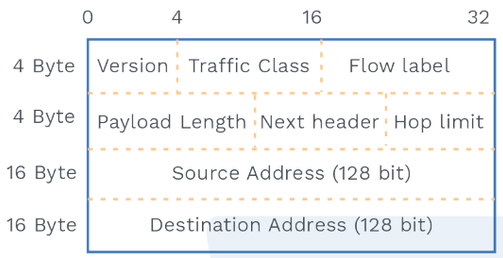



**Fig. 4.3 IPV4 Header**

**Version:** It will tell version of IP i.e 0110

**Traffic class:** It has 8 bits.
- The Most Significant 6 bits are used for Type of Service.
- The Last 2 bits are used for Explicit Congestion Notification.

**Flow label:** It has 20 bits.
- It is used for sequential flow of packet.
- It will help to avoid in re-ordering of packet.
- It is used for real time service.

**Payload length:** It has 16 bits.
- It tells how much information is present in the payload.

**Next header:** It has 8 bits.
- It is used for extension Header, if Extension Header is not present than it will inform Upper layer PDU.

**Hop limit:** It has 8 bits.
- It stop packets Loop to infinity.
- The value of Hop limit field decreases every time it crosses router.

**Source address:** It has 128 Bits.
- It indicates the address of originator.

**Destination address:** It has 128 bits.
- It indicates the address of indented destination.

**Q7** **An IPv4 datagram carries 512 bytes of data; what is the value of the header length? What is the value of the total length field? Assume option is not given.**

**Sol:** Since the option is not given header length is 20 bytes,
Total length field is Header length + Data bytes
512 + 20 = 532 bytes

**Q8** **The size of the option field of an IPv4 datagram is 28 bytes. What is the value of HLEN in binary?**

**Sol:** Total length of header is 28 + 20 = 48 Bytes.
HLEN should be the value after scaling.

48/4 = 12

In binary 1100

**Q9** **Consider a datagram packet of length 7000 and fields are shown in the figure.**

**Sol:**

| length | MF | ID | offset |
|---|---|---|---|
| 7000 | 0 | @ | 875 |

**Q10** **It goes into a network where MTU is 1500 Byte, now how will the router do fragmentation?**

**Sol:** Since MTU is 1500 Byte it will be,

| 20 | 1480 |
|---|---|

After fragmentation packet will look like see below.

**Let's see 1st fragment:**

- Length field has 1500 bytes which include 20 bytes of header and 1480 bytes of payload.
- MF field is 1 because more fragments are followed.
- Identification number will be the same for all the fragments.
- Offset field store scaled value, here it is 0 as before this fragment no data bytes are there.

**Let's see 2nd fragment:**

- Length field has 1500 bytes which include 20 bytes of header and 1480 bytes of payload.
- MF field is 1 because more fragments are followed.
- Identification number will be the same for all the fragments.
- Offset field store scaled value, here it is 185 as before this fragment fragment 1 is present which is having 1480 byte of data, scaled value of 1480/8 = 185.

**Let's see 3rd fragment:**

- Length field has 1500 bytes which include 20 bytes of header and 1480 bytes of payload.
- MF field is 1 because more fragments are followed.
- Identification number will be the same for all the fragments.
- Offset field store scaled value, here it is 370 as before this fragment 1 and fragment 2 is present which is having 1480 + 1480 byte of data, scaled value of 1480 *2/8 = 370.

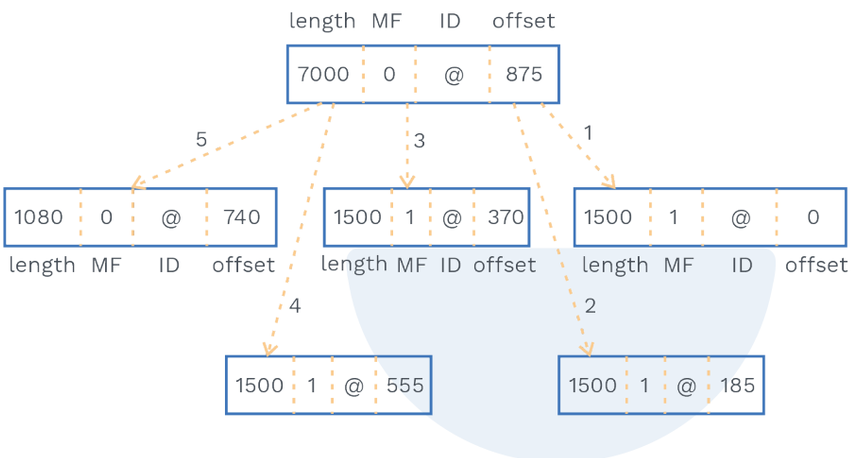
**Let's see 4th fragment:**

- Length field has 1500 bytes which include 20 bytes of header and 1480 bytes of payload.
- MF field is 1 because more fragments are followed.
- Identification number will be the same for all the fragments.
- Offset field store scaled value, here it is 555 as before this fragment fragment 1, fragment 2 and fragment 3 is present which is having 1480 + 1480 + 1480 byte of data, scaled value of 1480 *3/8 = 555.

**Let's see 5th fragment:**

- Length field has 1080 bytes which include 20 bytes of header and 1060 bytes of payload, Why 1040? 7000 - 4 * 1480.
- MF field is 0 because no more fragments are followed.

- Identification number will be the same for all the fragments.
- Offset field store scaled value, here it is 740 as before this fragment fragment 1, fragment 2, fragment 3 and fragment 4 is present which is having 1480 + 1480 + 1480 + 1480 byte of data, the scaled value of 1480 *4/8 = 740.




**Previous Years' Question**

**Q.** Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of the UDP header is 8 bytes, and the size of the IP header is 20 bytes. There is no option field in IP header. How many total number of IP fragments will be transmitted and what will be the contents of the offset field in the last fragment?

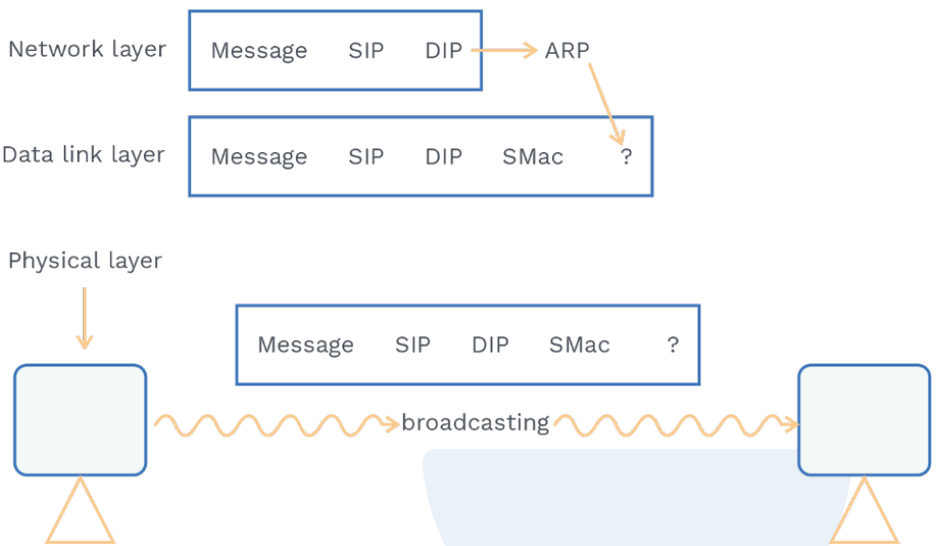
**a)** 6 and 925 **b)** 6 and 7400

**c)** 7 and 1110 **d)** 7 and 8880

**Sol: c)** **(GATE - 2015)**

**ARP protocol:**

- It is used for finding MAC addresses of corresponding IP address.
- ARP request is broadcast.
- ARP reply is unicast.
- It is used for finding MAC address of another Host or router.
- Even Router uses ARP, inorder to find MAC address of another Router or Host.




Lets understand working of ARP.

**Step 1:** Sender knows the target IP address.

**Step 2**: ARP request message is created and broadcast it which looks like.


**SIP:** Sender IP address.

**DIP:** Destination IP address.

**SMac:** Sender Mac Address or Sender Hardware address.

**DMac = ?:** Destination Mac Address which is unknown.

**Step 3:** The target Host or Router will Take the ARP request and reply its physical address and this reply will be unicast.

**Step 4:** Sender receives the reply and now it knows the target address of the machine.

**Step 5:** Now sender will do unicast to the destination IP address.
Let's understand better by taking example:

A host with IP address **a.b.c.d** and physical address **op:qr:st:uv:wx:yz** has a packet to send to another host with IP address **e.f.g.h** and physical address **zy:wx:uv:st:qr:op** (which is unknown to the first host). The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

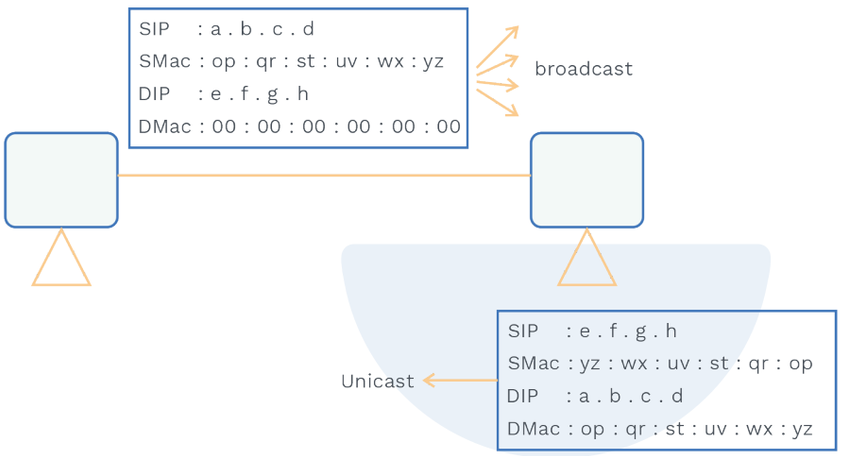



**Fig. 4.4 Diagram Showing ARP Request and Reply Packet**

Now we will see the Mapping of Physical to Logical address.
The possibilities when there is a need to convert from Physical to logical address are:

**Case 1:** While booting of diskless Node, it may find its hardware address but not an IP address.

**Case 2:** When IP address needs to assigned on demand, then the Host sends its MAC address and asks for short time lease.
For that, we use RARP, BOOTP and DHCP.

**RARP:** It will find an IP address (logical address) for given physical address.

- Machine gets its physical address by reading its NIC, By using Physical address Host can know the logical address using RARP protocol.
- RARP request is broadcast, and RARP reply is unicast, which is done by RARP Server.

MAC ⟶ RARP ⟶ IP

- Broadcasting is done at the data link layer. The MAC broadcast address does not pass the boundaries of a network.
- For this problem, the administrator has to assign a RARP server to each network, which is an overhead.

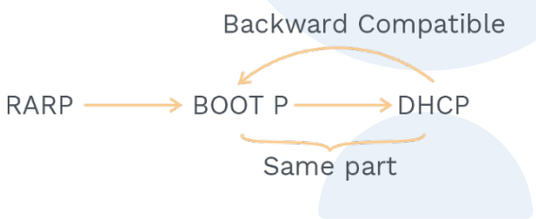
**Note:**
This RARP is now obsolete.

**BOOTP:** It is also designed such that it will convert the physical address into a logical address.

- It is similar to RARP, except it works at the application layer.
- Network, which does not have BOOTP server, has a relay agent.
- Because of the Relay agent, there is a need for only one BOOTP server.
- Disadvantage of BOOTP is that it maintains the static table.

**DHCP:** It will also maintain a table which helps in finding the Physical address for corresponding logical address.

- Only one DHCP server is enough in the network.
- No need for a relay agent.
- How do RARP, BOOTP and DHCP evolve?




**Note:**
DHCP provides static and dynamic address allocation that can be manual or automatic.

**ICMP:** Internet Control Message Protocol is a network layer protocol which is used by network devices to diagnose network communication issues.

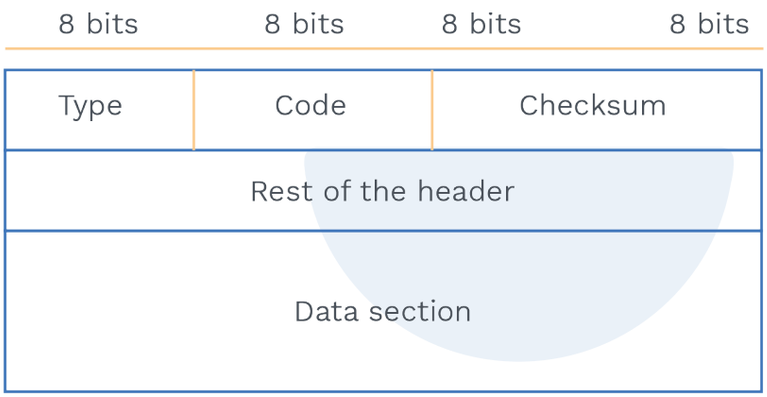
IP was designed for efficient use; It is an unreliable and connectionless datagram service which has its own advantages and disadvantages.

The two major shortcomings of IP are
**I)** Lack of error control and
**II)** Lack of providing assistance mechanism

Internet Control Message Protocol has been designed for this purpose.

**Points:**
ICMP has divided into two categories:
**1)** Error reporting message
**2)** Query message

**Message format of ICMP:**
It has 8 byte.
It has variable size data section.




- The first field defines the type of error message.
- The code field defines the reason for the particular message type.
- For each type of message there is the Header field section.
- Data Section contains information for finding the original packet in error message.
- Data Section contains information based on the type of query in query message.

**Note:**
ICMP always reports error messages to the original source.

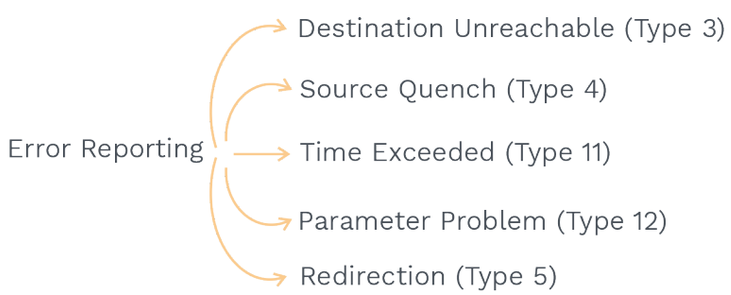
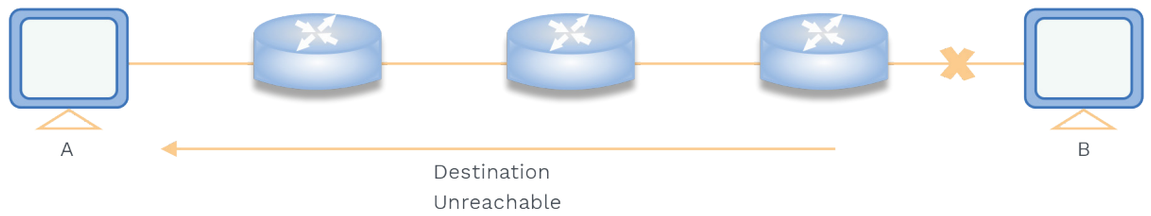



**Fig. 4.5 Diagram Showing ARP Request and Reply Packet**

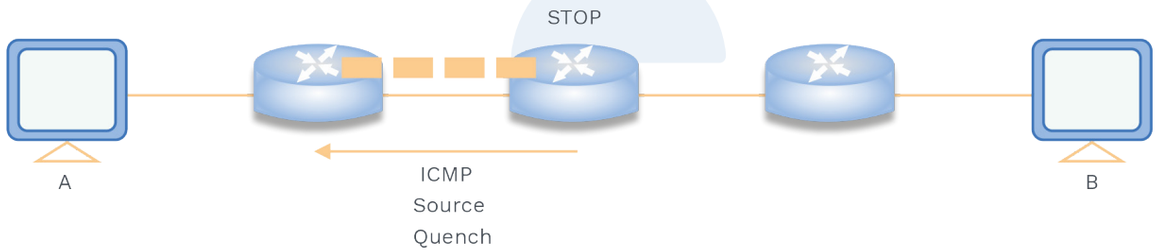
**Destination unreachable:** This problem occurs when the datagram does not reach to destination, the router and Host discard the packet and sends destination unreachable to the original sender.




**Note:**
Destination unreachable message can only be created either by destination host or router.

**Source quench:** The lack of flow control causes congestion in the router or destination Host.

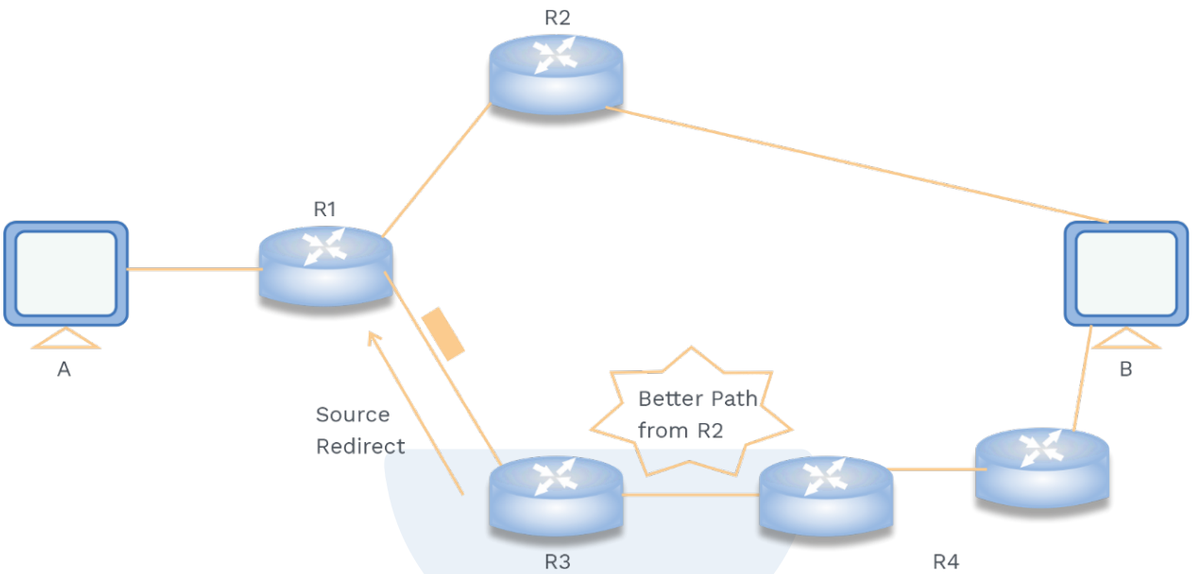
When the datagram is reached at a much higher rate so that router is not able to forward it, then it will discard the packet sending the source quench message to the source.




**Time exceed message:** When all fragments do not reach the destination at a certain time than Time exceed message is sends to source.

**Parameter problem:** If the router or the destination Host discovers the missing value or any error in the datagram packet, then it will send the Parameter problem.

**Redirection:** It is not an error message but just a warning message from a router to a Host that there is a better path which should be used.




**Important points about ICMP error message:**

- No ICMP error message will be generated in response to a datagram carrying an ICMP error message, multicast address and special address.
- No ICMP error message will be generated for a fragmented datagram that is not the first fragment.

**Query messages:**

Query Message
- Echo Request and Reply (Type 8 and 0)
- Timestamp Request and Reply (Type 13 and 14)
- Router Solicitation and Advertisement (Type 10 and 9)
- Address Mask Request and Reply (Type 17 and 18)

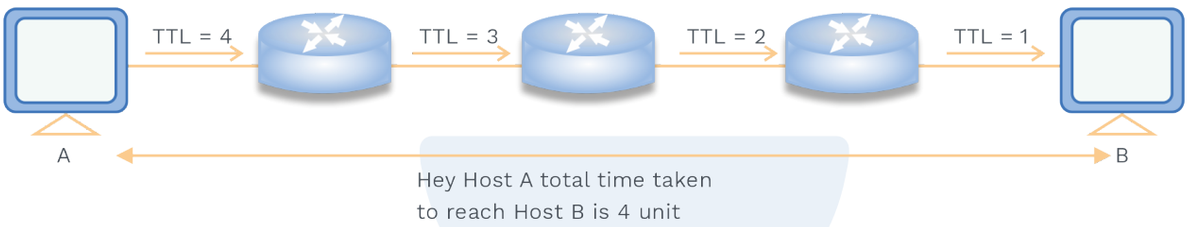
**In order to solve network problems, query messages are used**

**Echo request and reply:** The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other.

It is used to check if the destination is working or not, and all the routers comes along the path is working.

**Note:**
Nowadays Ping command is used for echo request and echo reply.

**Time stamp request and reply:** hosts or routers can use the timestamp request and timestamp reply messages to determine the total time needed for an IP datagram to travel between them.




**Address mask request and reply:** How does Host obtain its network mask? To obtain its network mask, a host sends an address-mask-request message to a router.

Now two cases arise if the Host knows the address of the router or not!

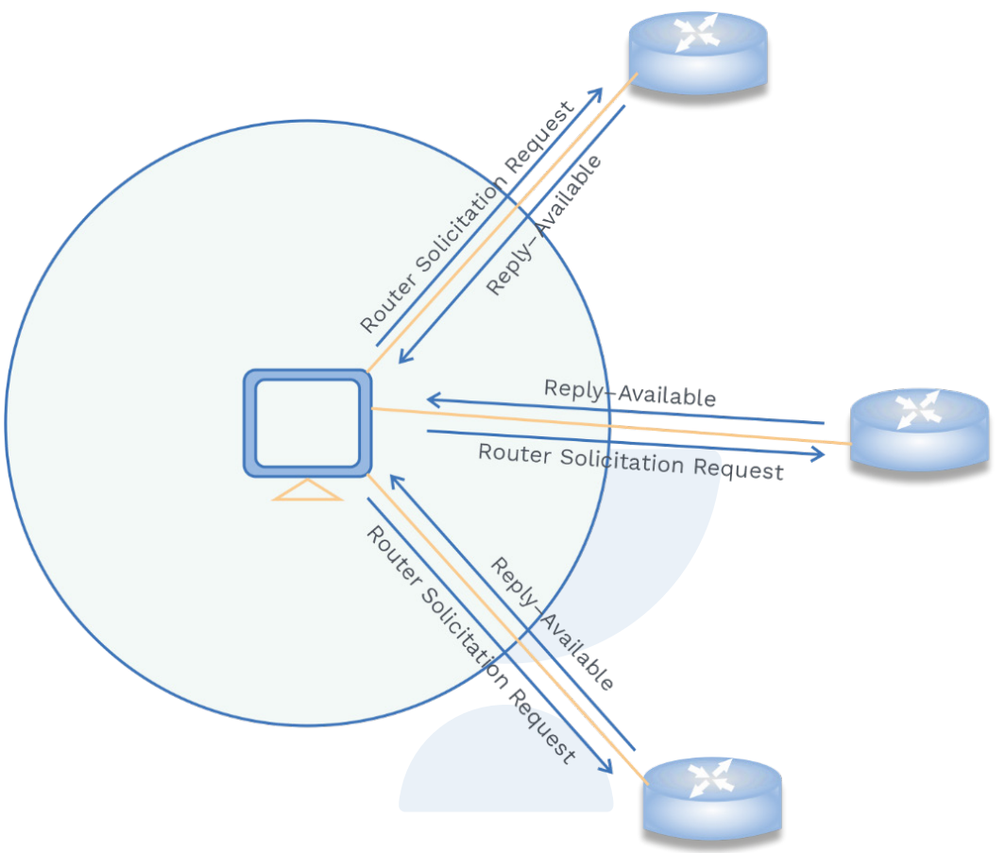
- If it knows, then it will directly send the router.
- if it does not know, then Host will broadcast the message.

Now Router will do address-mask-reply message, providing the necessary mask for the host.

**Router solicitation and advertisement:**

- For giving Router information, Router advertisement message is used via broadcasting.
- For finding a router Router solicitation message is used via broadcasting or multicasting.

**Note:**
When a router sends out an advertisement, it tells all the information of known routers also.




**Now we will see the routing of an IP packet:**
**Flooding:**
Sending packets through every possible path is flooding.

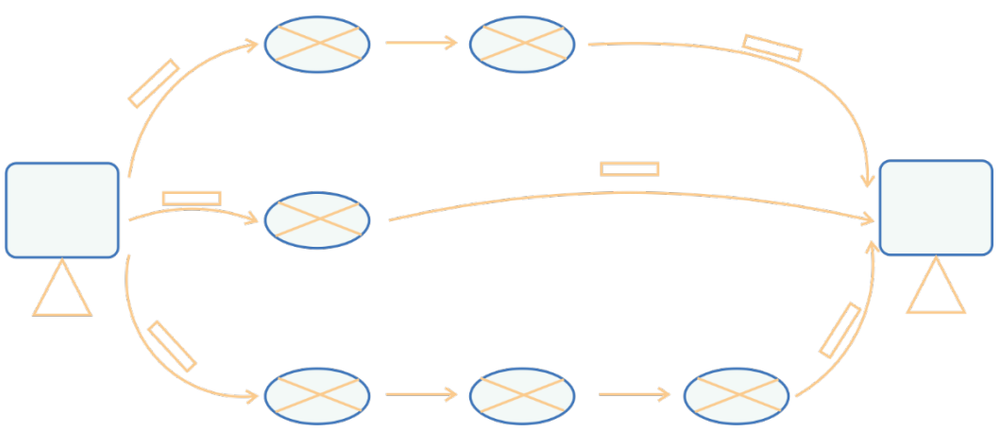


**Fig. 4.5 Diagrammatic Representation of Flooding**

**Advantage of flooding:**
- Reliability is more.
- Shortest path finding is guaranteed.

**Disadvantage:**
- Traffic is more.
- Duplicates packet will be more.

**Routing:**
Deciding the packet which path to follow by making a Routing Table is called Routing.

**Note:**
Putting a packet from one side and taking it to the other side is called switching.

**Advantage of Routing:**
- Traffic is less.
- No duplicate packet.

**Disadvantage of Routing:**
- Reliability is less.
- Shortest path finding is not guaranteed.

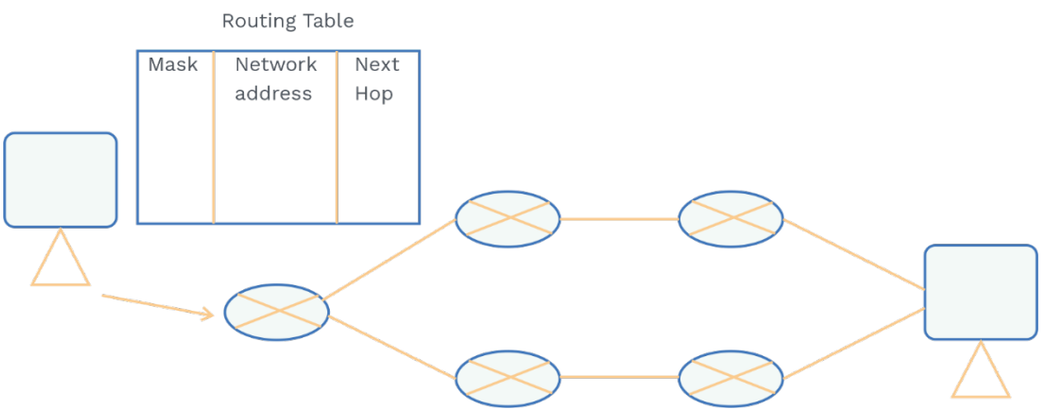



**Fig. 4.6 Diagrammatic Representation of Routing**

**Types of Routing Algorithm:**
**1)** Static Routing
**2)** Dynamic Routing
  **a)** DVR (Distance Vector Routing)
  **b)** LSR (Link state Routing)

**Static Routing:**

**a)** They don't change based on topology and traffic.
**b)** In static routing user-defined routes are used in the routing table.
**c)** Static Routing may not follow any specific protocol.
**d)** They are used in smaller networks.

**Dynamic Routing:**

**a)** They don't change based on topology and traffic.
**b)** In dynamic routing, routes will be updated as per changes are done in network.
**c)** They are used in larger networks.
**d)** Dynamic Routing follow protocol.

**Distance vector Routing:**

It is a dynamic routing algorithm.

**Step 1:** Each router makes its routing table.
Each router knows.

- All the router present in the network.
- Distance to its neighbour router.

**Step 2:** Each router exchanges its distant vector to its neighbour routers and prepare a new routing table.

**Step 3**: Repeat step 2 (n-1)times if there are n routers.

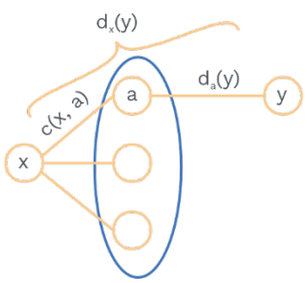
**Step 4:** After this routing table converge i.e. it become stable.

**Note:**

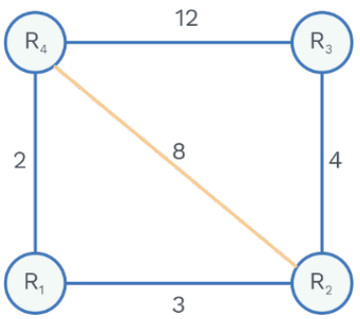
Distance vector routing uses Bellman Ford algorithm at each router.

Bellman–Ford equation

- $d_x(y) = \min_a\{c(x, a) + d_a(y)\}$
- $d_x(y)$ – least cost path from node x to y
- $\min_a$ – apply above eq. over all of x's neighbors



Let us understand using example




There are 4 routers in a network and delays or cost are mentioned on the edges.

**Step 1:**

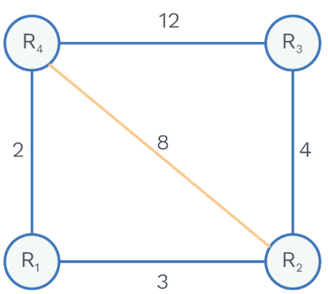
Each router will maintain a Routing table using its local knowledge.
Here we have taken Destination, Distance and next hope for building a routing table, but there may be many more fields.

for $R_4$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 2 | $R_1$ |
| $R_2$ | 8 | $R_2$ |
| $R_3$ | 12 | $R_3$ |
| $R_4$ | 0 | $R_4$ |

for $R_3$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | ∞ | – |
| $R_2$ | 4 | $R_2$ |
| $R_3$ | 0 | $R_3$ |
| $R_4$ | 12 | $R_4$ |




for $R_1$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 0 | $R_1$ |
| $R_2$ | 3 | $R_2$ |
| $R_3$ | ∞ | – |
| $R_4$ | 2 | $R_4$ |

for $R_2$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 3 | $R_1$ |
| $R_2$ | 0 | $R_2$ |
| $R_3$ | 4 | $R_3$ |
| $R_4$ | 8 | $R_4$ |

**Step 2:**
Each router will exchange its distant vector and build the new routing table.

**For router R1:**
Router R1 will receive distance vectors from its neighbour R2 and R4.
Now router R1 will prepare a new table as,

for $R_2$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 3 | $R_1$ |
| $R_2$ | 0 | $R_2$ |
| $R_3$ | 4 | $R_3$ |
| $R_4$ | 8 | $R_4$ |

for $R_4$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 2 | $R_1$ |
| $R_2$ | 8 | $R_2$ |
| $R_3$ | 12 | $R_3$ |
| $R_4$ | 0 | $R_4$ |

New routing table for R1 using R2 and R4

| $R_2$ | $R_4$ | Destination | Distance | Next hop |
|---|---|---|---|---|
| | | $R_1$ | 0 | $R_1$ |
| Min (3+0, | 2+8) = 3 | $R_2$ | 3 | $R_2$ |
| Min (3+4, | 2+12) = 7 | $R_3$ | 7 | $R_2$ |
| Min (3+8, | 2+0) = 2 | $R_4$ | 2 | $R_4$ |

**For router R2:**
Router R2 will receive distance vectors from its neighbour R3, R1 and R4.
Now router R2 will prepare, new table as,

for $R_1$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 0 | $R_1$ |
| $R_2$ | 3 | $R_2$ |
| $R_3$ | ∞ | – |
| $R_4$ | 2 | $R_4$ |

for $R_3$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | ∞ | – |
| $R_2$ | 4 | $R_2$ |
| $R_3$ | 0 | $R_3$ |
| $R_4$ | 12 | $R_4$ |

for $R_4$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 2 | $R_1$ |
| $R_2$ | 8 | $R_2$ |
| $R_3$ | 12 | $R_3$ |
| $R_4$ | 0 | $R_4$ |

New routing table for R2 using R1, R3 and R4

$R_1$ $R_4$ $R_3$
Min (3+0, 8+2, 4+∞)

$R_3$ $R_4$ $R_1$
Min (4+0, 8+12, 3+∞)

$R_1$ $R_4$ $R_3$
Min (3+2, 8+0, 4+12)

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 3 | $R_1$ |
| $R_2$ | 0 | $R_2$ |
| $R_3$ | 4 | $R_3$ |
| $R_4$ | 5 | $R_1$ |

**For Router R3:**

Router R3 will receive distant vectors from its neighbour R2 and R4. Now router R3 will prepare new table as,

for $R_2$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 3 | $R_1$ |
| $R_2$ | 0 | $R_2$ |
| $R_3$ | 4 | $R_3$ |
| $R_4$ | 8 | $R_4$ |

for $R_4$

| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 2 | $R_1$ |
| $R_2$ | 8 | $R_2$ |
| $R_3$ | 12 | $R_3$ |
| $R_4$ | 0 | $R_4$ |

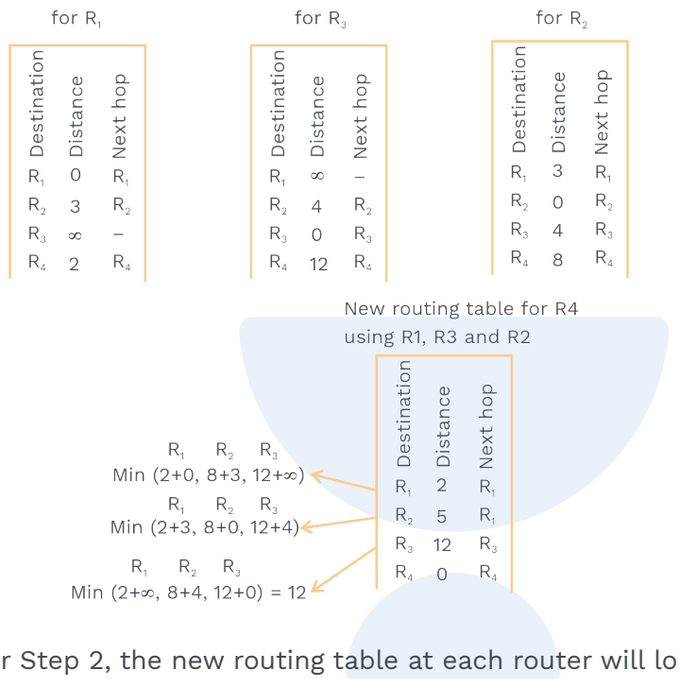
New routing table for R3 using R2 and R4

$R_2$ $R_4$
Min (4+3, 12+2) = 7
Min (4+0, 12+8) = 4
Min (4+8, 12+0) = 12

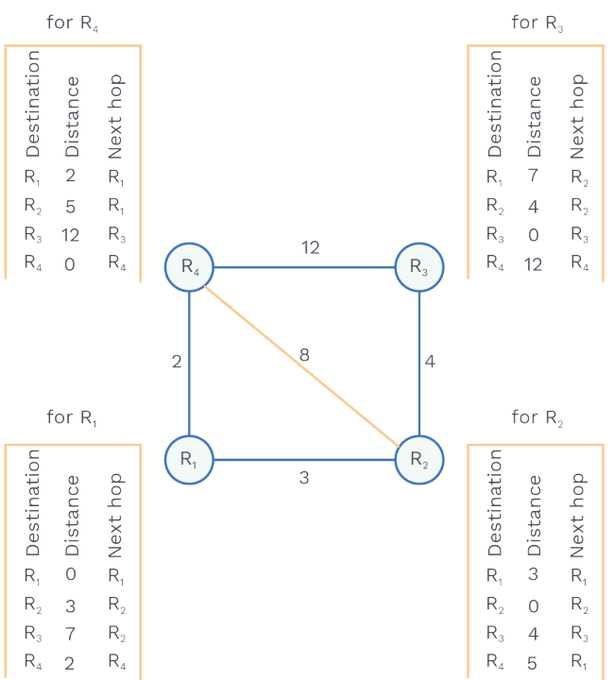
| Destination | Distance | Next hop |
|---|---|---|
| $R_1$ | 7 | $R_2$ |
| $R_2$ | 4 | $R_2$ |
| $R_3$ | 0 | $R_3$ |
| $R_4$ | 12 | $R_4$ |

**For Router R4:**

Router R4 will receive distant vectors from its neighbour R2, R3 and R1. Now router R4 will prepare new table as,



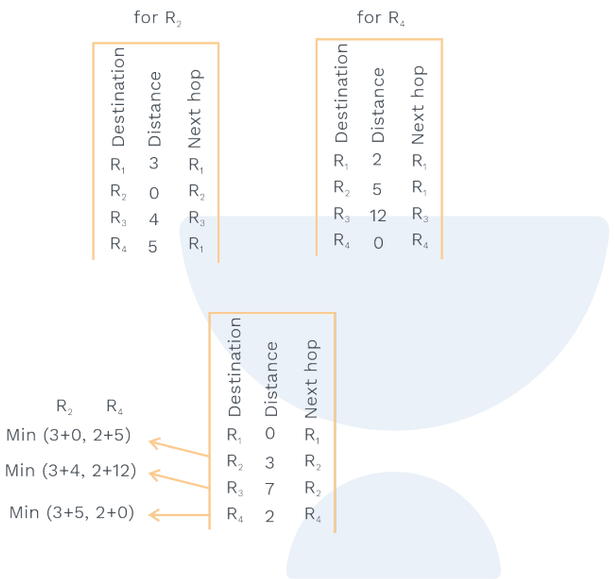

Finally after Step 2, the new routing table at each router will look like,



**Step 3:** Each router exchanges its distant vector obtained in step 2. After exchanging, each router will have a new routing table.

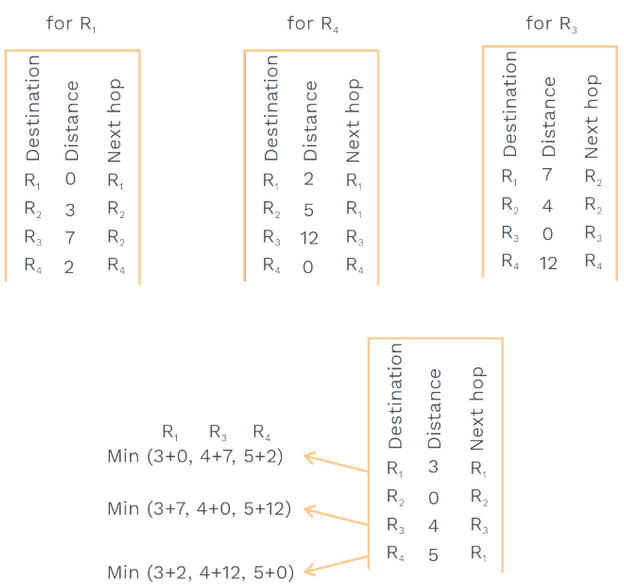
**For Router R1:**

Router R1 will receive distant vectors from its neighbour R2 and R4. Now router R1 will prepare new table as,



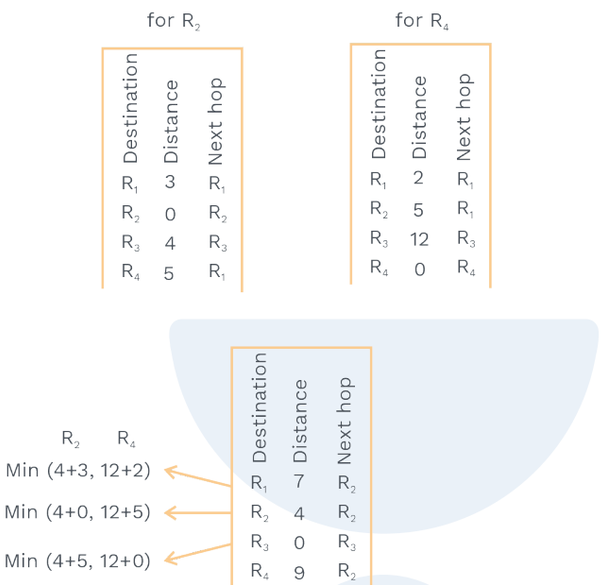

**For Router R2:**

Router R2 will receive distant vectors from its neighbours R1, R3 and R4. Now router R2 will prepare a new table as,



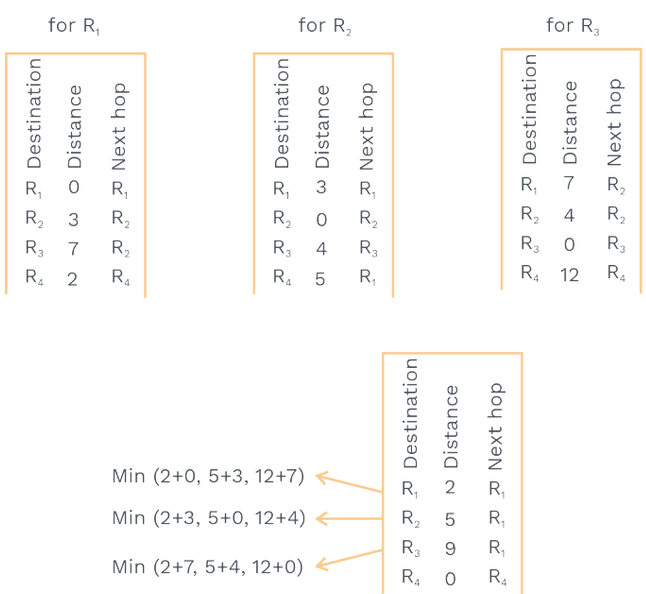
**For Router R3:**

Router R3 will receive distant vectors from its neighbour R2 and R4.
Now router R3 will prepare new table as,

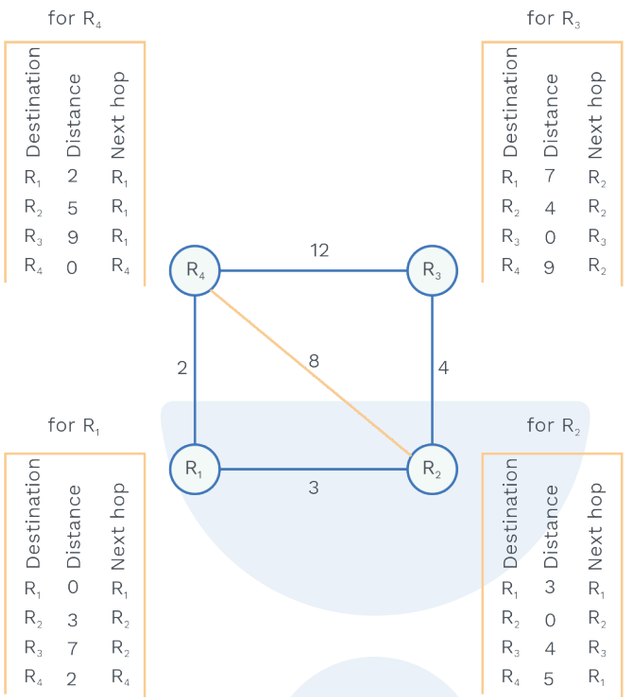



**For Router R4:**

Router R4 will receive distant vectors from its neighbours R2, R3 and R1.
Now router R4 will prepare a new table as

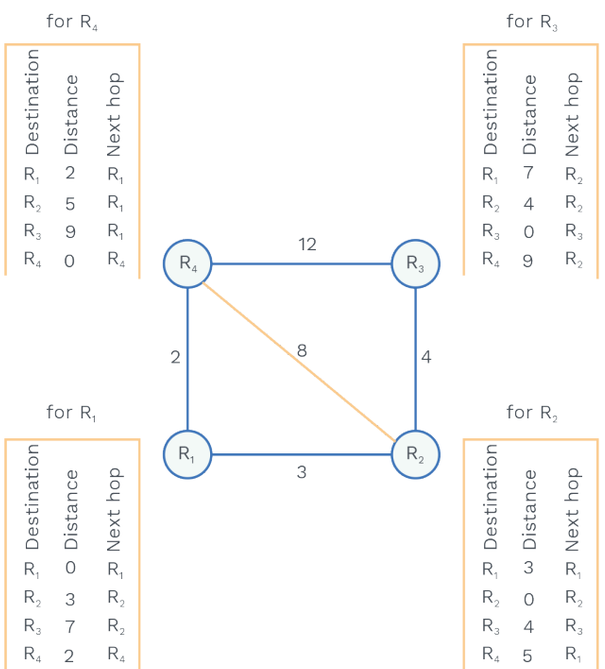


Now the routing table will be like,




**Step 4:**

Since there are 4 routers and 2 exchanges have been done now router will look like.



**Common field of Routing table:**
Till now we have seen the destination, distance and next hop in routing table but there are many other fields also.

| Mask | Network address | Next–hop address | Interlace | | Reference count | Use |
|---|---|---|---|---|---|---|
| | | | | | | |

**Mask:** It defines mask for a particular entry.

**Network address:** It defines the network of destination Host.

**Next hop address:** It defines the network where router will route next.

**Interface:** This shows the name of the interface.

**Use:** This field defines the number of packets transmitted through this router.

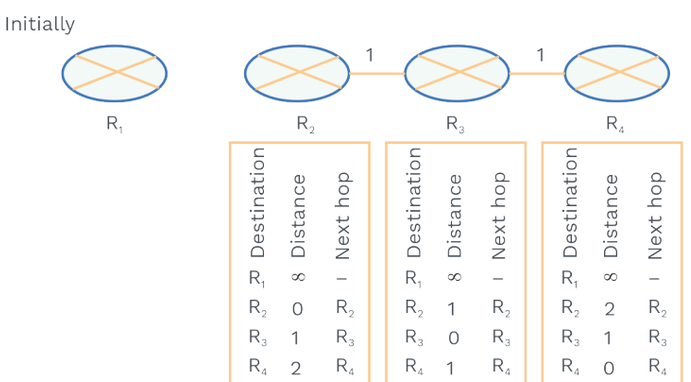
**Reference count:** Number of the user connected to this router at the same time, is defined by this field.

**Problem with Distance Vector Routing:**

- It has a count to infinity problem.

Trick to remember Count to infinity problem:
Bad News spreads slow and good news spread fast.

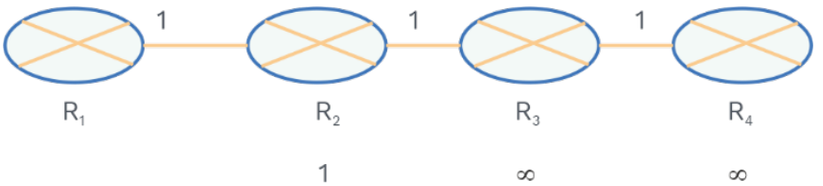
Let's understand How this problem occurs in DVR.
There is Router R1 which is not connected initially, so it looks like,



Now we will see what happens if Router R1 gets connected to the networks.

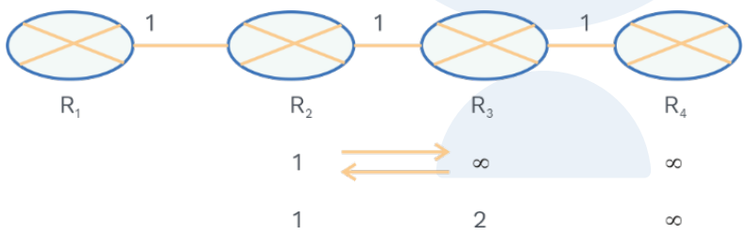
When R1 get connected to the R2, How do other router update their entry at R1 position given in diagram.

* Please Note We have taken R1 row value at every diagram.



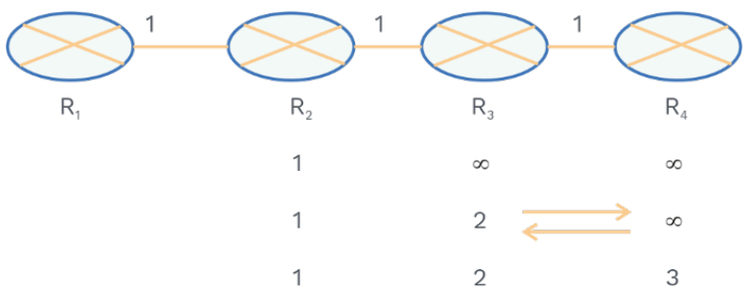

Now exchange of vectors will take place,

R3 will think R2 distance vector is showing 1 unit distant from R2 to R1, and since R2 is 1 unit to R3, So R3 will reach to R1 in 2 unit distance,




Now again exchange of vectors will take place,

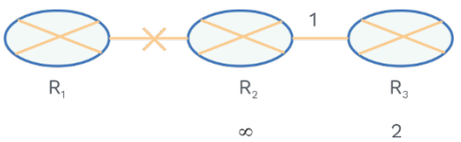
- R4 will think R3 Distance vector is showing 2 unit distant from R3 to R1, and since R3 is 1 unit to R4, So R4 will reach to R1 in 3 unit distance.



This means when R1 is added (Good news) router get to know each other soon.

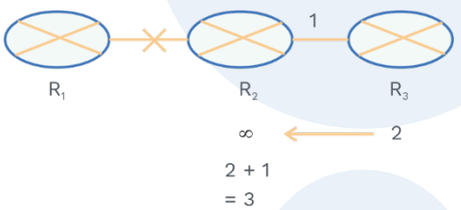
Now lets see what will happen if router get disconnected.

- R2 get to know that R1 is not there, but R3 will slowly get to know.



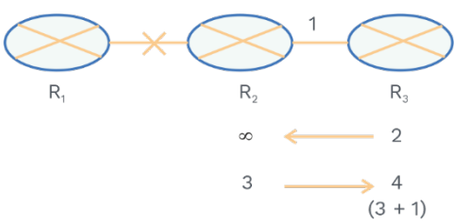

**Why will R2 get updated to 3?**

Now the exchange of Distance vectors takes place, R3 is saying to R2 that for reaching R1 it will take 2 units, and R3 distance is 1 unit from R2, So R2 will update 3 units.




**Why will R3 get updated to 4?**

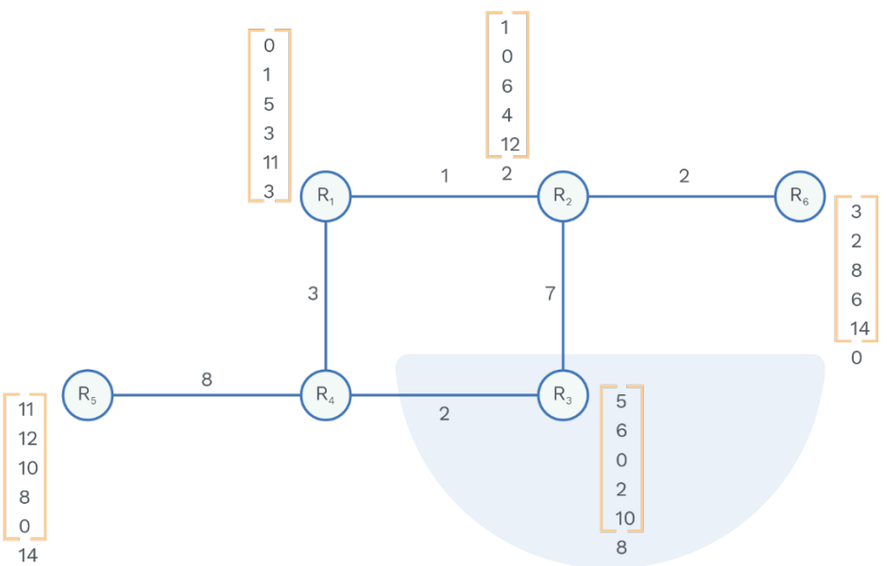
After R2 updated to 3, it will exchange its distance vector to R3, now R3 will think R2 can reach R1 in 3 unit and R2 is 1 unit distant, So R3 will update to 4.




Similarly, same exchange of routing table exchange and slowly it will lead to update.

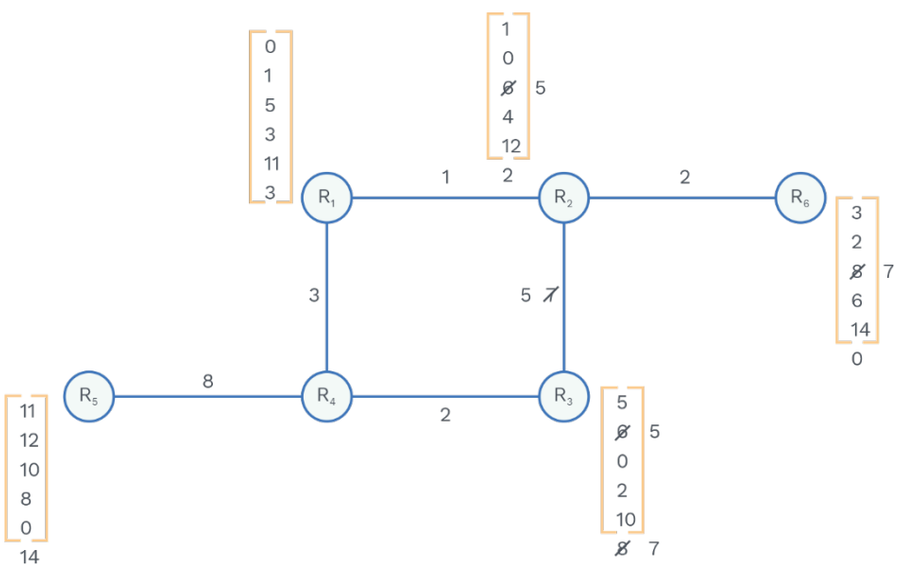
This is how Bad problem travels slow.

**Let's understand, through example, How DVR works when any Routes gets changes.**




Initially every router gets to know about each other through changing their distant vector.

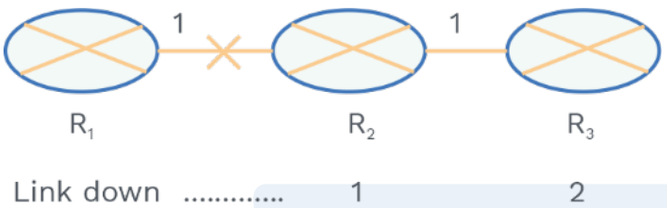
**Case 1:** Which link is unused!
R2 - R3 Link
**Case 2:** If R2 - R3 link changes to 5, What would be the distance vector of R3?



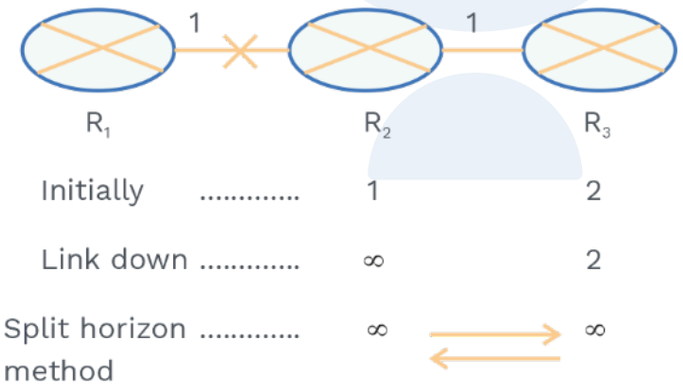
**Solution to count to infinity problem is to use Split horizon method:**
Split horizon is a method which prevents a router from advertising a route back on the same interface.

**Rack Your Brain**

What would be the distance vector of R4 before and after Link changes?




Split horizon says that in a given situation if R3 is depending on R2 inorder to Reach R1, it should not advertise its distance to R2 , it will always advertise infinity.



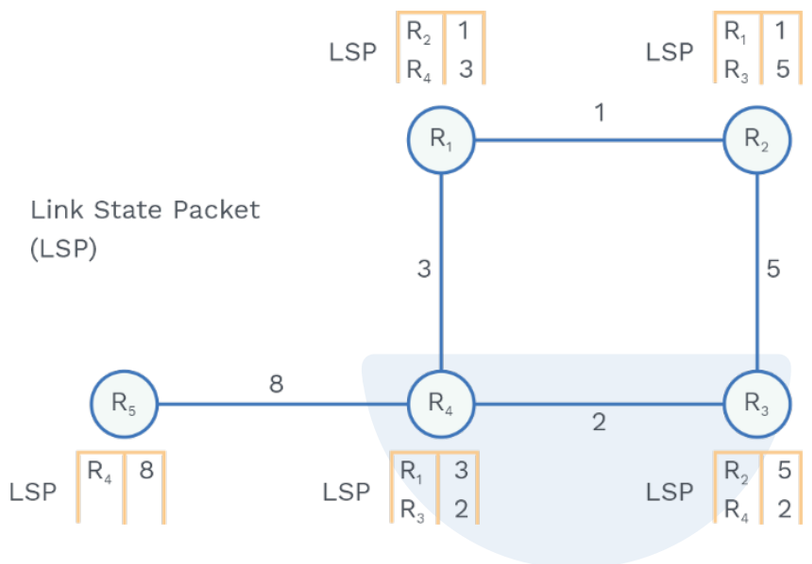

**Link state router:**
There are 4 steps for making routing using Link State protocol,
**Step 1:** Creation of states of the link by each node, those states are called Link state Packet.
**Step2:** Flooding Of LSP to every Router.
**Step 3:** Formation of the Shortest Path Tree for each node.

**Note:**
For creating the shortest path tree, Dijkstra algorithm is used.

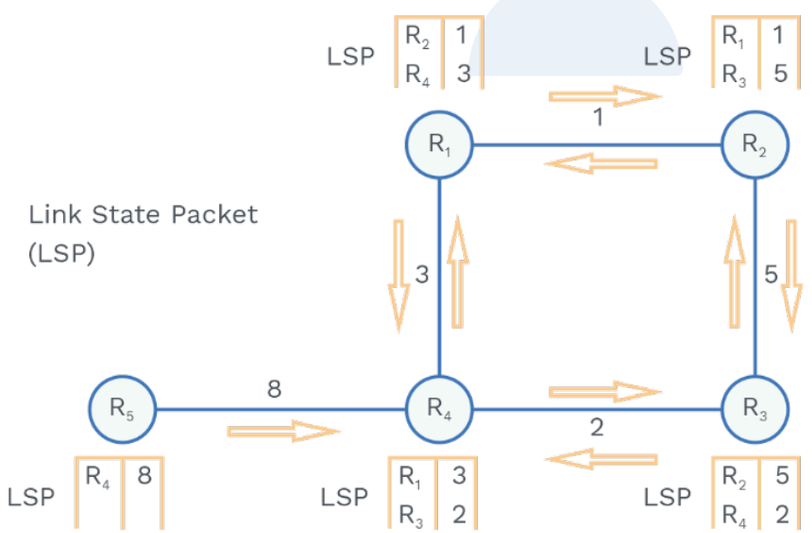
**Step 4:** Calculation of Routing Table based on the shortest Path tree.

**Lets understand using example:**

**Step 1:** Making Link State Packet (LSP), by knowing its neighbour.

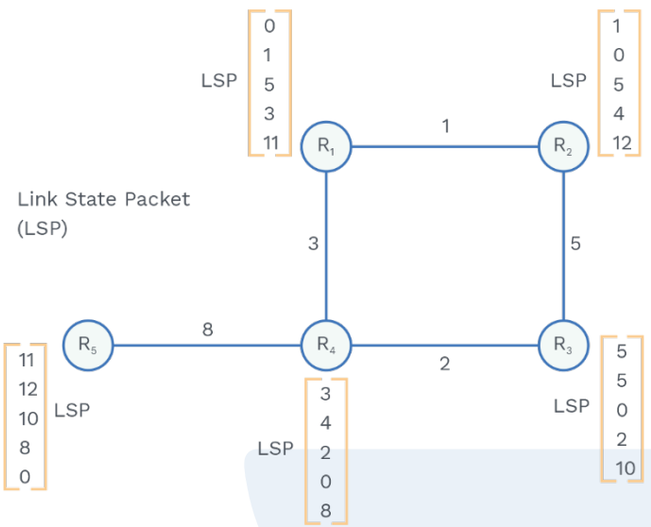



**Step 2:** Flood the LSP packet at every router.




**Step 3 and Step 4:**

At each router using Dijkstra shortest tree is made, and Routing table is computed.




**Problem In Link State:**

**1)** Router is facing heavy traffic,
Now because of heavy traffic, How routers get to know that Which Packet is latest!!
Every router will maintain a record of incoming packet and their sequence number.

**2)** Transient problem
(This problem occur for a short problem)
**a)** Black Hole problem

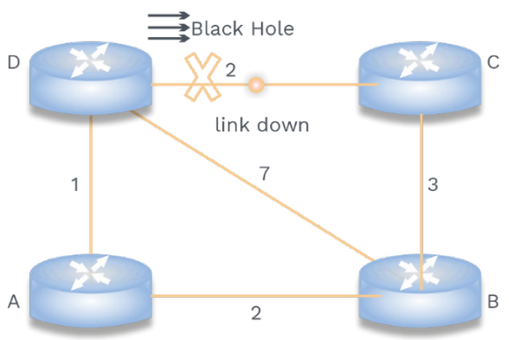



**Fig. 4.7 Diagram Representing Black Hole Problem in Link State Routing**

This says that if a link is down all the packet transmitted through this link will get lost, and this is called Black Hole problem.
But after some time, the Router will configure correctly, this means Black Hole problem only creates delays for some time.

**b)** Looping problem also arises when a link is down, it is also a transient problem.
compare DVR and Link State Routing:

| Basis for Comparison | Distance Vecotr Routing | Link State Routing |
|---|---|---|
| Algorithm | Bellman Ford | Dijsktra |
| Network view | Topology information from the neighbour point of view | Complete information on the network topology |
| Best path calculation | Based on the least number of hops | Based on the cost |
| CPU and memory | Low utilisation | Intensive |
| Convergence time | Moderate | Fast |

**Fig. 4.8 Comparison Between DVR and LSR**

**Note**

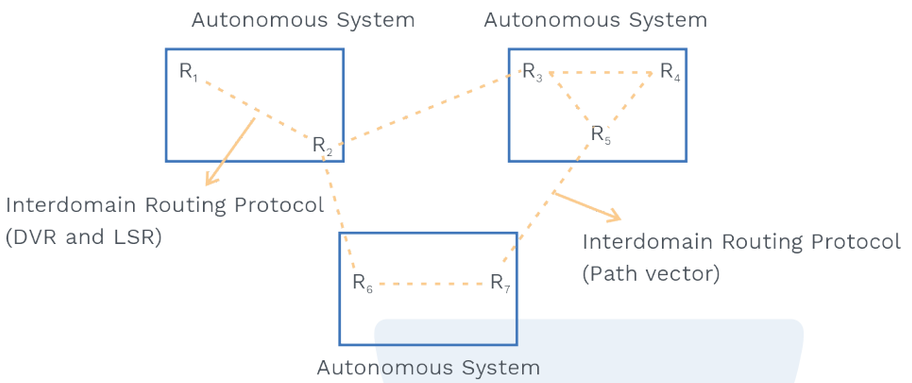
- Routing Information Protocol (RIP) is an implementation of Distance vector routing.
- Open Shortest Path First (OSPF) is an implementation of Link State Routing.
- Border Gateway Protocol (BGP) is an implementation of Path vector Routing.

**Intradomain and Interdomain Routing:**
Internet is divided into the autonomous system, because internet is large enough that it can't handle the records of all the router.

**Note**
Autonomous System (AS): It is a group of routers under guidance of single administration.

When Routing is done inside autonomous system it is considered as

intradomain Routing.
When Routing is done between autonomous system it is considered as interdomain Routing.




Till now we have discussed DVR and LSR, lets see How Path vector works, which is an Intradomain Routing.
Path vector is similar to Distance vector only except that only Speaker node can communicate with each other.

**Note:**
Speaker node is a node which can act as administrator of all the nodes present inside an autonomous system.

BGP is an implementation of Path vector, BGP can also be used in two ways Exterior BGP and Interior BGP.

**Exterior BGP:** This is used When two-speaker node used to communicate with each other.

**Interior BGP:** This is used when the speaker wants to collect information from other router inside an Autonomous System.

## Chapter Summary

- IPv4 is 32 bit long and used to define any host universally on the Internet.
- In classful addressing, IP address can be divided into NID (network identifier used to identify network) and HID (Host identifier used to identify the Host).
- Addresses in classes A, B, or C are mostly used for unicast communication and addresses in class D are used for multicast communication.
- Dividing of the large networks into smaller ones is called Subnetting, and Supernetting combines several networks into the larger one.
- Address space is divided into variable-length blocks in Classful addressing.
- Basically 3 rules in classless addressing given below:
  **1)** Block must have contiguous addresses.
  **2)** Size of Block must be written in the power of 2.
  **3)** First address of the block must be divisible by the size of the block.
- IPv6 addresses use hexadecimal colon notation with abbreviation methods available.
- Unicast, multicast and anycast is used in IPv6, there is no concept of broadcast in IPv6.
- IPV4 is an unreliable connectionless protocol for source to destination delivery.
- Minimum and the maximum length of IP header are 20 and 60 bytes, respectively.
- The maximum number of bytes that a data link protocol can encapsulate is called MTU (maximum transfer unit).
- Division of packets into the smaller packets so that it can accommodate in MTU is called fragmentation.
- Mapping of a logical address to a physical address can be static or dynamic.
- At every router, checksum is calculated if it is not matched with the value present in the header, then the packet is discarded.
- Options provide Source routing, padding and record route.
- The address resolution protocol (ARP) is a dynamic mapping method that is used to find a physical address when logical address is given.
- The Reverse address resolution protocol (RARP) is used to find a logical address when the physical address is given.
- Packet Internet Groper (ping) is an application program that uses the services of ICMP to test the reachability of a host.
- A static routing entries are updated manually by an administrator and dynamic routing entries are updated automatically by a routing protocol.
- An autonomous system (AS) is a group of networks, and routers under the authority of a single administrator.
- Routing Information Protocol (RIP) is an implementation of Distance vector routing.
- Open Shortest Path First (OSPF) is an implementation of Link State Routing.
- Border Gateway Protocol (BGP) is an implementation of Path vector Routing.