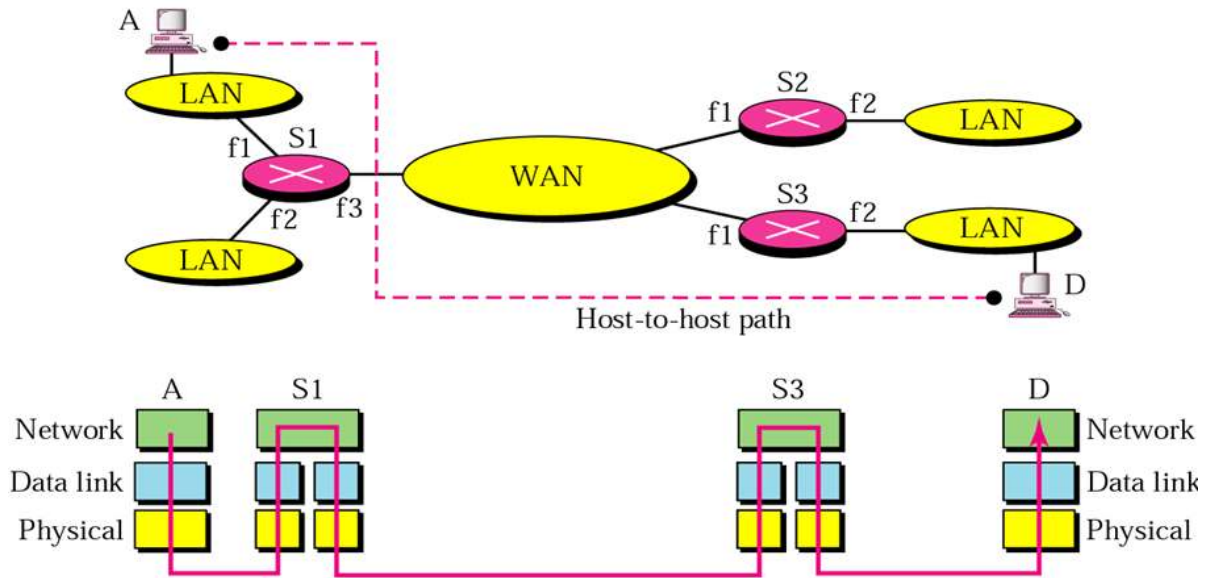


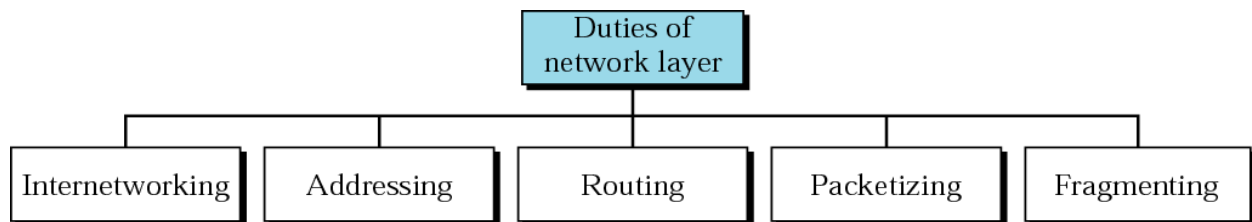
**CNS Model answers**  
**Unit 3 Network layer**

**Functions of Network layer.**

**Main function of Network layer :** “The delivery of individual packets from the **source** host(node) to the **destination** host(node) connected in **different** networks”



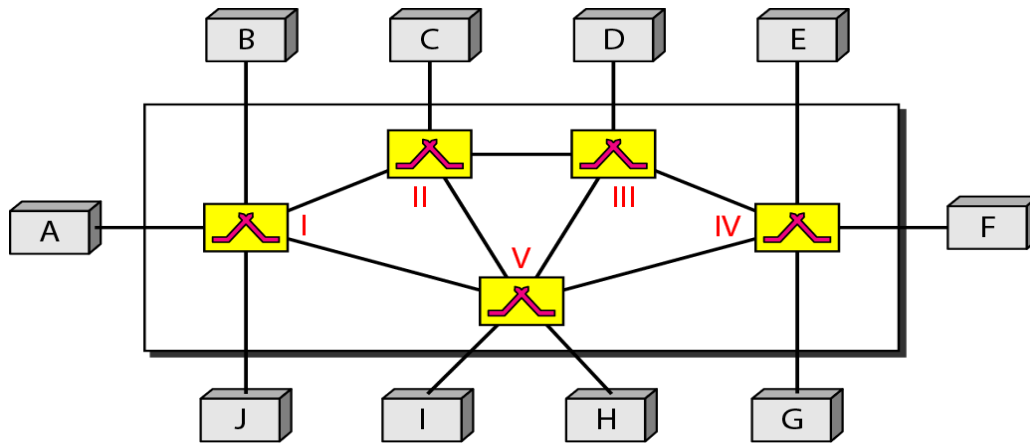
To carry out this function , the network layer need s following functions




- **Internetworking** : connecting the hosts which are in different networks
- **Packetizing** : dividing the message which is received from transport layer into packets
- **Logical addressing**: across different networks a logical address is required which is called Internet Protocol (IP) address
- **Routing**: protocols to decide to which path a packet has to be sent so that it reaches destination
- **Connection model**: connection-oriented and connectionless communication
- **Fragmenting** : dividing packets into fragments , if in between network does not allow big packets

What is a switched network ?

A switched network consists of interlinked nodes called switches. switches can create a **temporary** connection between two or more devices connected to it.

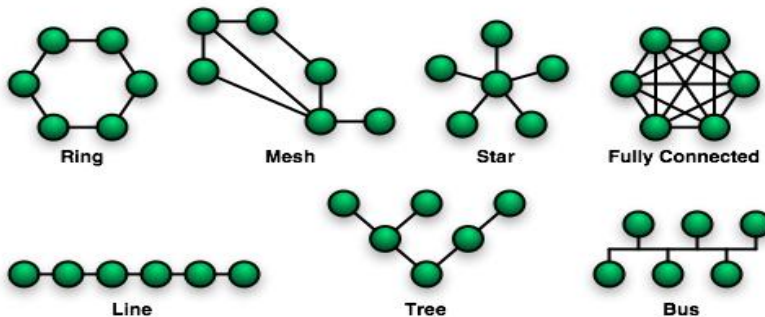


 is a switch

 is end device eg. PC.

What is the advantage of switched network over various topologies used in LAN?

Following topologies of LAN are **not practical** for **big** networks such as telephone network & Internet.



Because :

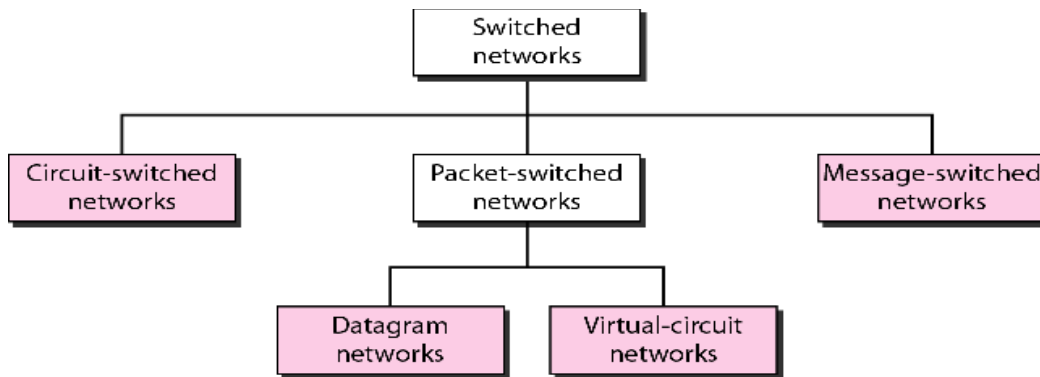
**mesh** or **star** are impractical for large no of devices due to too many links and their length.

**Bus** : length and no of devices are beyond capacity of media and equipment.

\*majority of links/devices would be idle most of the time\*

Eg . even if our phone is connected to all other phones , how much time we will be talking to all phones!

Give the taxonomy of switched networks:



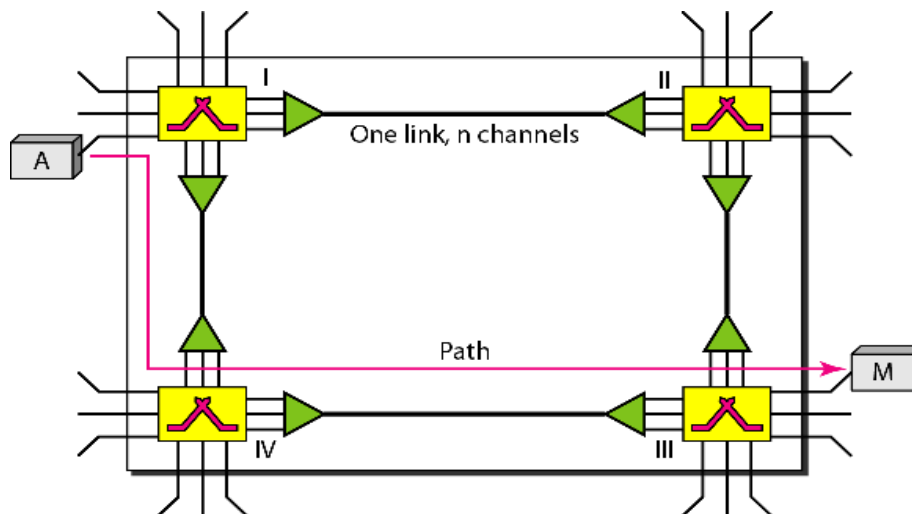
### Explain Circuit switching,

A circuit-switched network consists of a set of switches connected by physical links. A connection between any two stations is **dedicated/reserved** for that pair **only till they** are communicating.

There is only one link between one pair of switches. Link is divided into  $n$  channels (i.e. by multiplexing by using FDM or TDM)

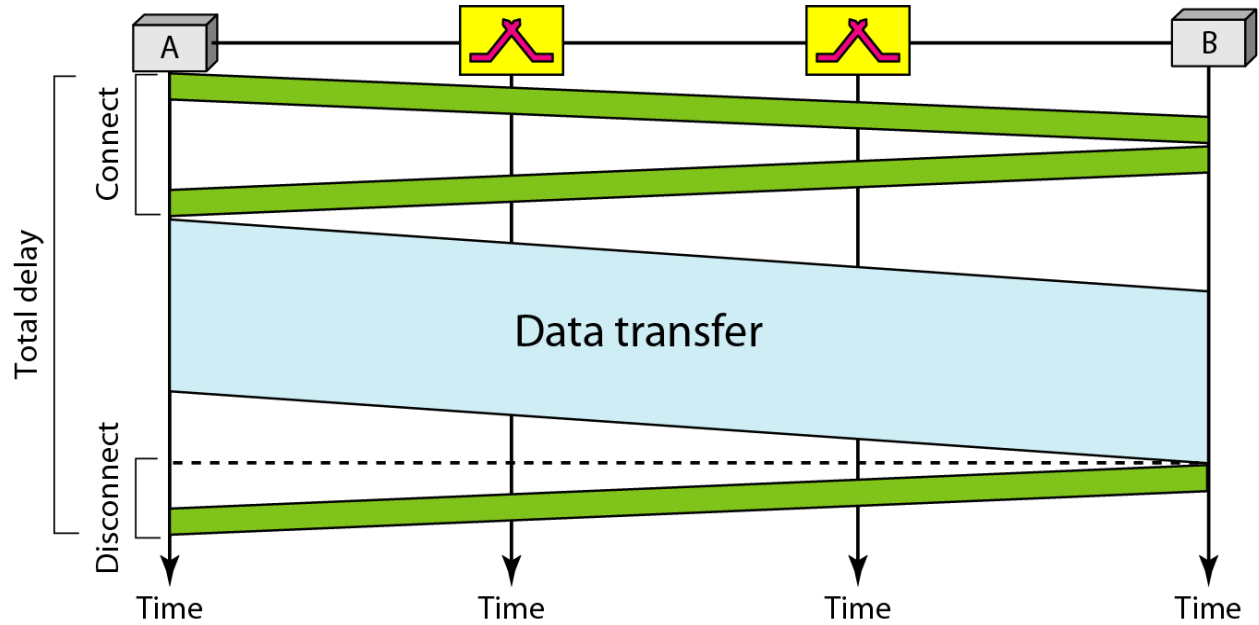
Here if Station A wants to communicate with Station M, it has to go through three phases:

1. Setup phase
2. Data transfer phase
3. Teardown phase

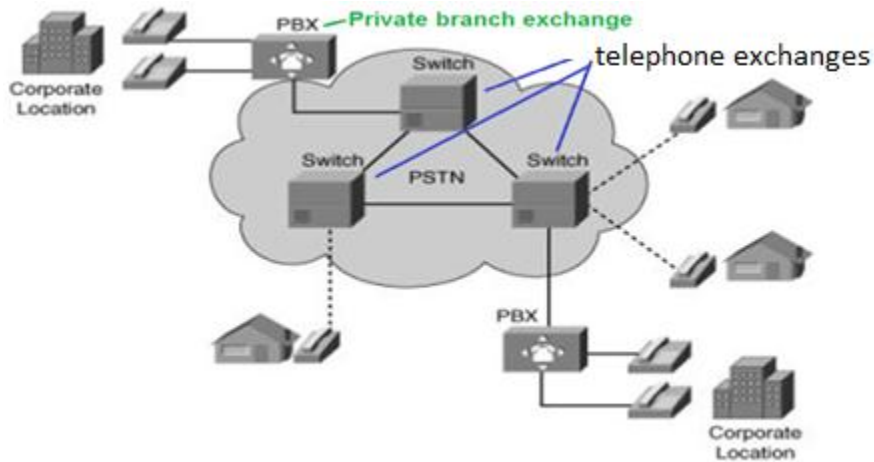


- Request of station A must be accepted by all switches in the path as well as M itself
- In circuit switching, the resources need to be reserved during the setup phase such as switches in the path, channel between each switch, switch ports etc;
- The resources remain dedicated for the entire duration of data transfer until the teardown phase.
- Data transfer is not packetized but is continuous flow with some periods of silence (eg human conversation).
- addressing is required only in the beginning i.e. during setup phase. No addressing required during data transfer & tear down.
- **Efficiency:** less than packet switched. Resources allocated & reserved for a pair & cannot be shared by multiple pairs

- **Delay** : It takes time for setup . but data transfer is fastest ( as resources are reserved during setup)

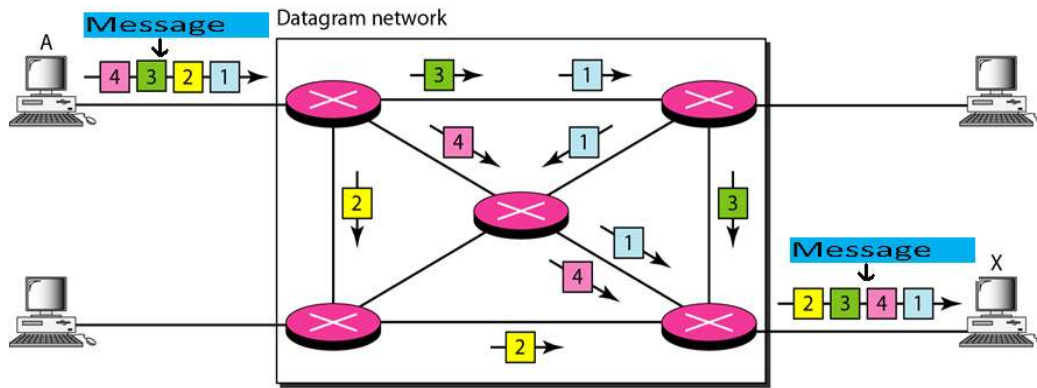


Eg public switched telephone network ( PSTN).

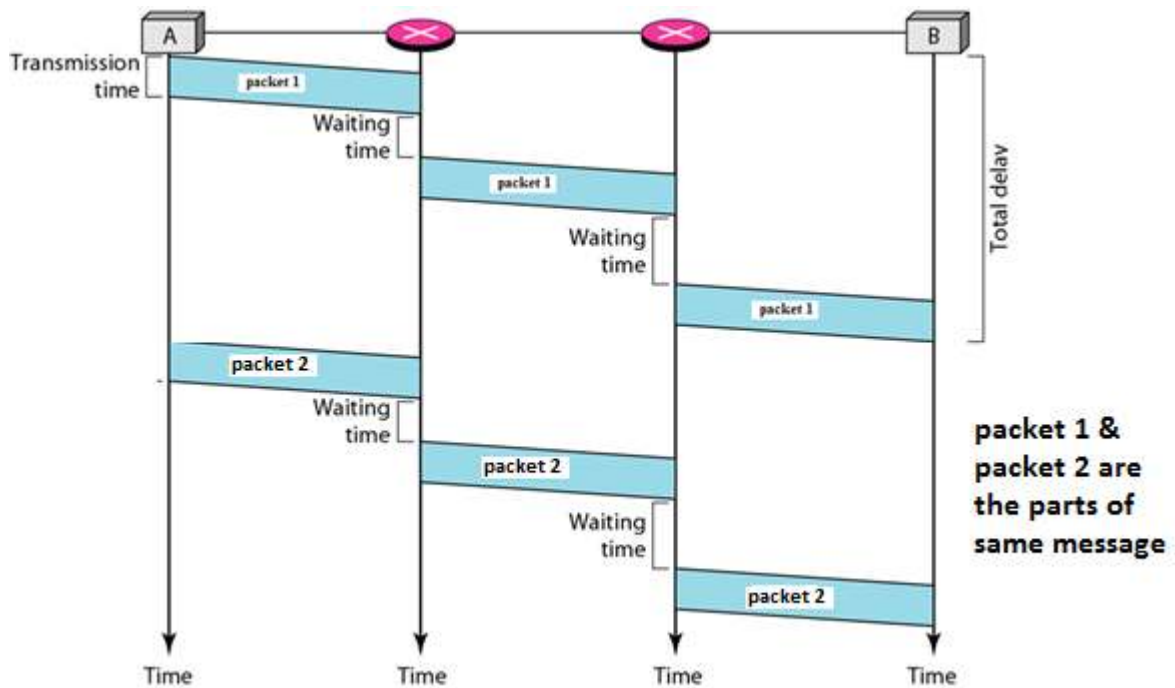


### Explain packet Switching,

In this, a Message (Data) is divided in to packets and packets can take different paths to reach the destination.

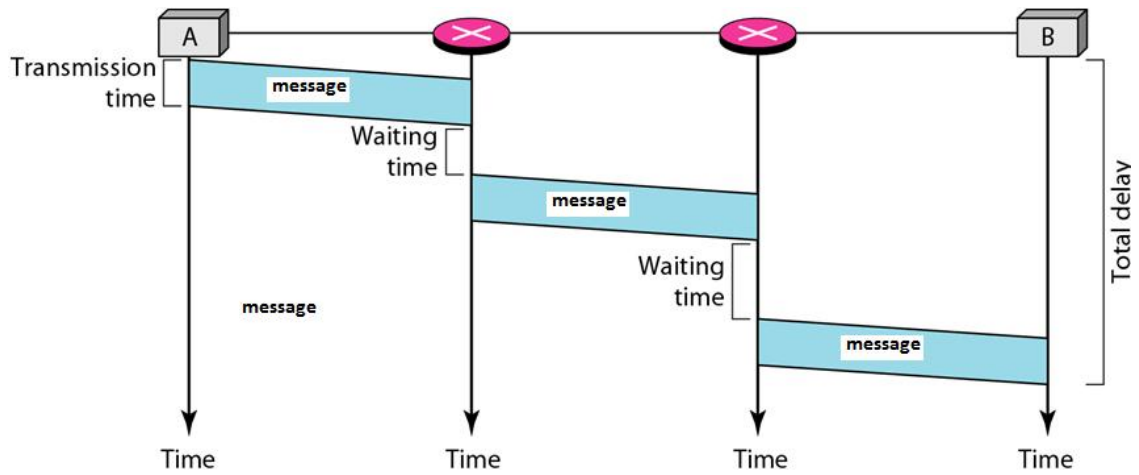


- In a packet-switched network, there is no resource reservation for communicating pairs. i.e. resources are allocated as available .
- Each packet is treated independently even if it is a part of the same Message. so each packet of the same message has same source and destination address.
- Packets may get lost , duplicated, damaged, or out of order. It is duty of layers in end stations to take action accordingly
- **Efficiency**: better than circuit switched . Resources allocated only when there are packets to be Transmitted. & can be shared by multiple pairs
- **Delay** : Delay is greater than circuit switched network. there is no delay of setup and teardown phase , but at each switch , the packet has to wait in queue because of processing delay. Delay is not same for all packets of a Message.



### Explain message Switching

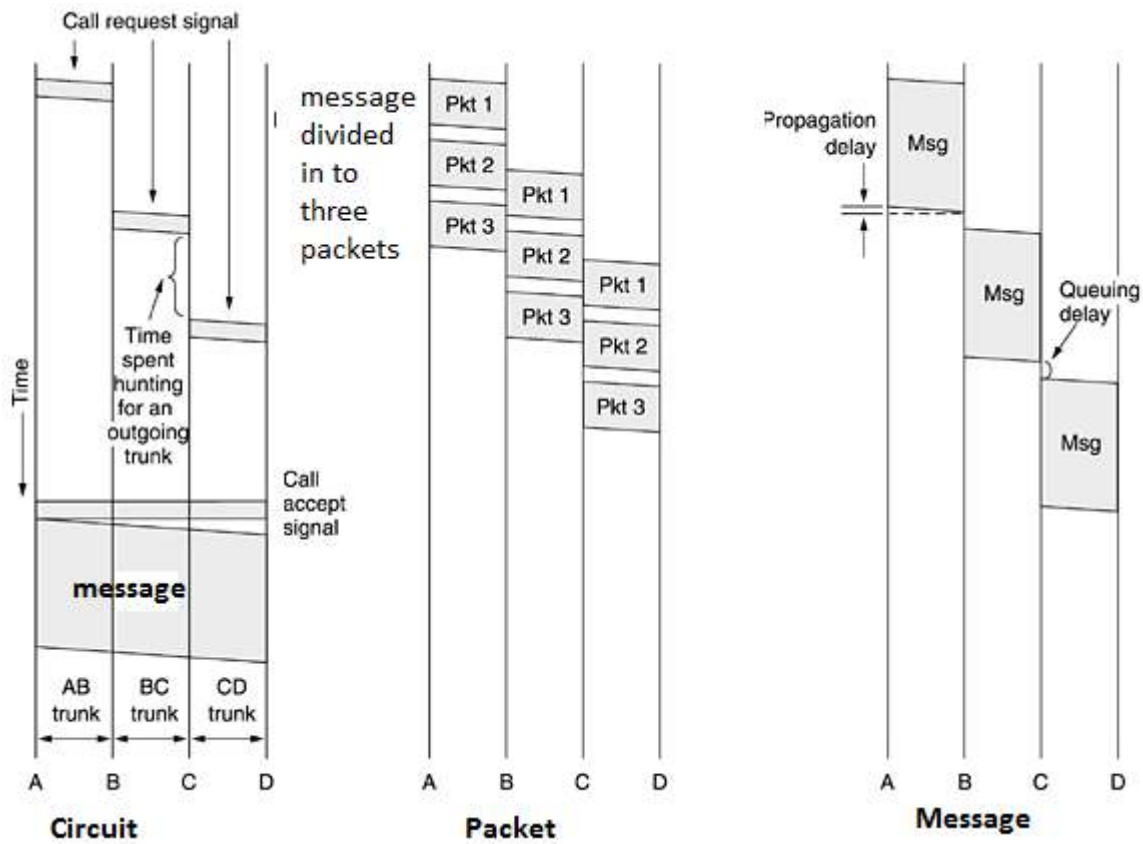
- In message switching, each switch stores the whole message and forwards it to the next switch



- In message switching no physical path is established in advance between sender and receiver.
- Instead, when the sender has a message to be sent, it is stored in the first switching office (i.e., router) and then forwarded later, one hop at a time.
- Each message is received completely then it is inspected for errors, and then retransmitted to next switch.
- **Application** : . it is still used in some applications like electronic mail (e-mail)

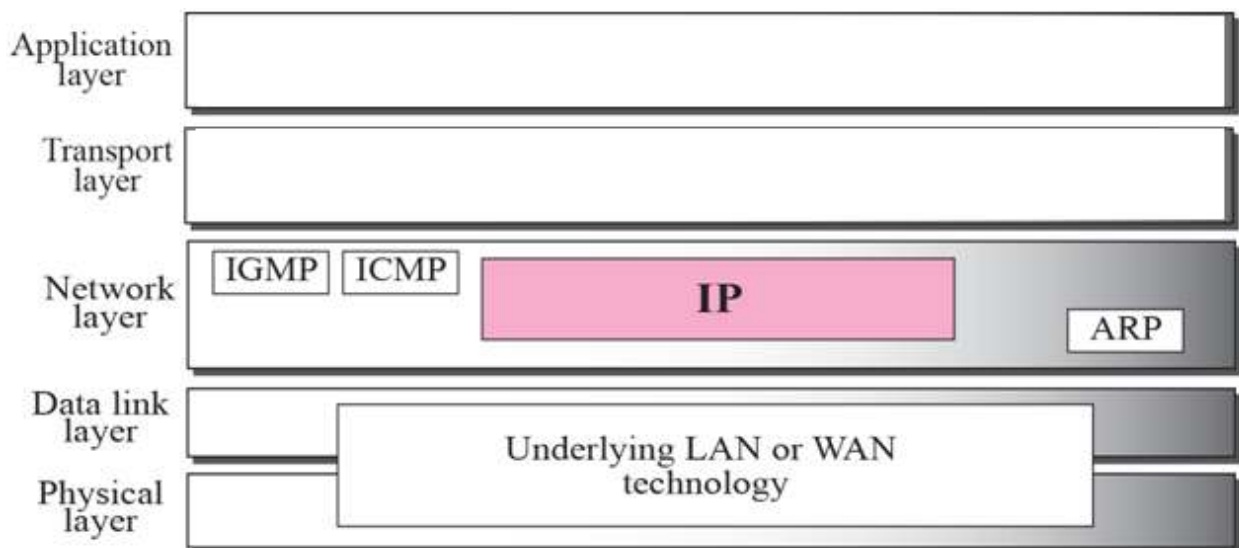
### Compare circuit , packet & message switching

	<b>Circuit switching</b>	<b>Packet switching</b>	<b>Message switching</b>
	Entire message is transmitted	Message is divided in to packets	Entire message is transmitted
Resource reservation	Resources ( path) is reserved for a particular pair	No resources are reserved	No resources are reserved
phases	Three phases : setup , data transfer, tear down	Only data transfer phase	Only data transfer phase
efficiency	Least . Since resources are locked for a pair . & can't be used by other pairs.	High : as resources are available for all pairs , subject to availability	High : as resources are available for all pairs , subject to availability
delay	Fastest data transfer	More delay than Circuit.	More delay than Circuit.
Addressing	Required only during setup phase	Each packet of same message requires address of source & destination	message requires address of source & destination
Application	Telephone network	Internet	Email application

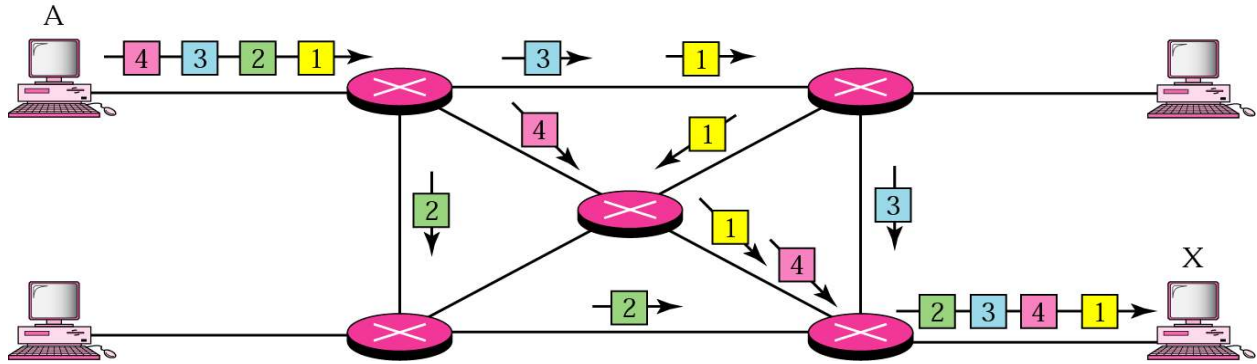


### Explain IP protocol

It is the **Internet Protocol (IP)** used at network layer of TCP / IP suite i.e. internet. It is used for routing of packets from source to destination. It is accompanied by other protocols such as IGMP, ICMP & ARP



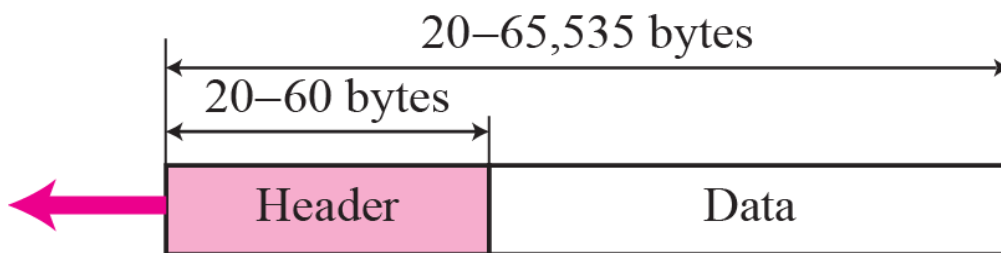
The message is divided into packets and packets of the same message can travel by different paths to the destination.



- IP is **connectionless** service, means it treats each packet independently, with each packet having no relationship to any other packet. Each packet has address of source & destination
- IP is **unreliable** . means that IP packets can be corrupted, lost, arrive out of order, or delayed and may create congestion for the network. If reliability is important, IP must be paired with a reliable protocol such as TCP.
- IP has two versions based on address length.
  1. IPv4 has 32 bit IP addresses for hosts & routers
  2. IPv6 has 128 bit IP addresses for hosts & routers
- IPv6 can communicate with IPv4 hosts using techniques such as tunneling & header translation.

### Explain IPv4 packet format

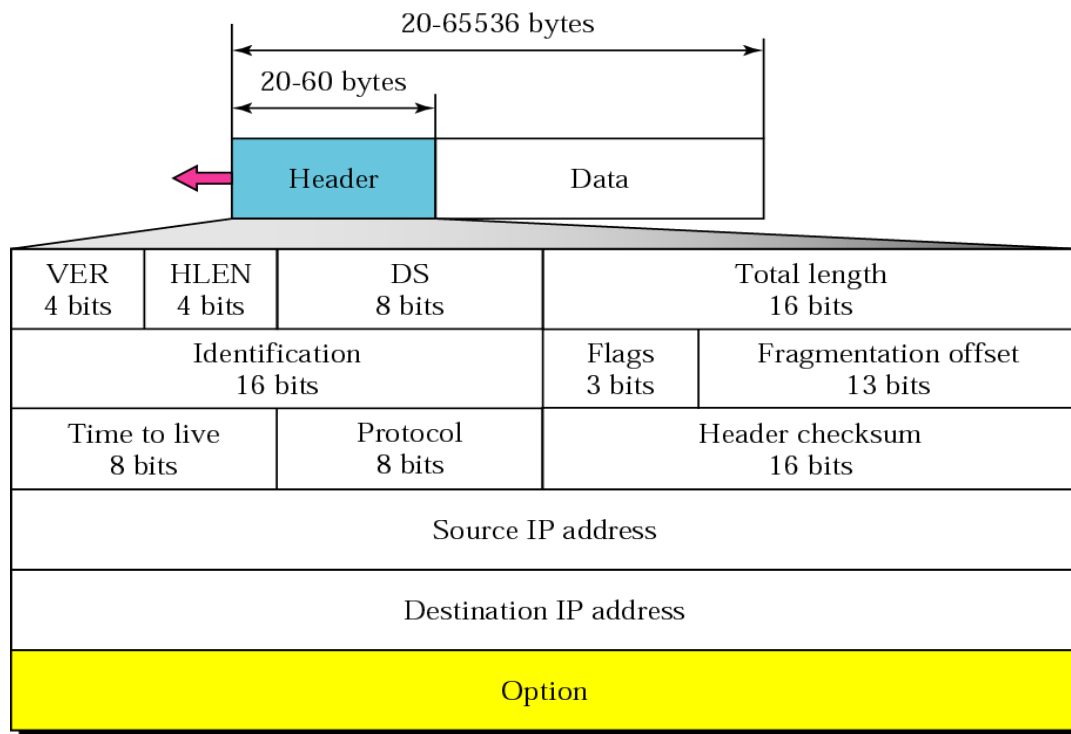
It has size from 20 to 65535 bytes. Header can be 20 to 40 bytes.



a. IP datagram

Header contains following fields





**Version (VER).** This 4-bit field defines the version of the IP protocol. It can be IPv4 or IPv6

**Header length (HLEN).** This 4-bit field defines the total length of the datagram **header** in 4-byte words. Which can between 20 and 60 bytes.

**DS :** a set of differentiated services. Used to give priority to packets of important message.

**Total length.** This is a 16-bit field that defines the total length (header plus data) of the IP datagram in bytes

**Identification.** This field is used in fragmentation . A packet may need to be fragmented if a network in between source & destination does not allow packet of big size.

**Flags.** This field is used in fragmentation

**Fragmentation offset.** This field is used in fragmentation

**Time to live.** is used to set the maximum number of hops (routers) visited by the packet. So as to avoid it getting circulated in the internet infinitely.

**Protocol.** Informs the destination , which higher-level protocol (such as TCP, UDP, ICMP, and IGMP) using the services of the IP layer.

**Checksum.**for detection of error in header only

**Source address.** This 32-bit field defines the IP address of the source.

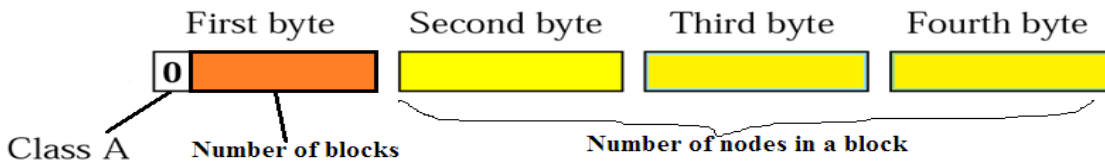
**Destination address.** This 32-bit field defines the IP address of the destination.

### Explain classful addressing

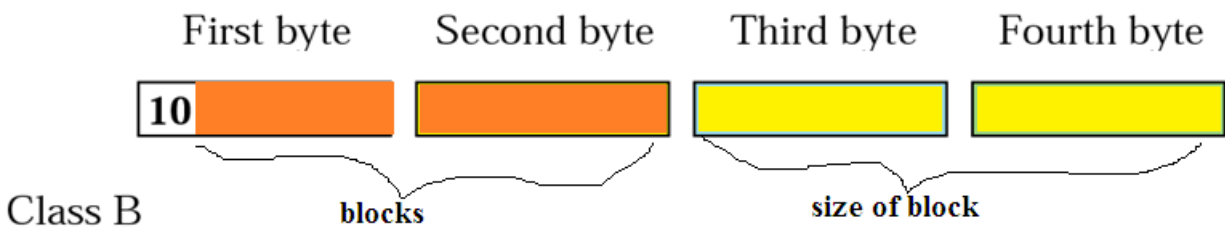
In classful addressing, the addresses are divided into five classes: A, B, C, D, and E.

Out of these, the classes A , B & C are used for networks, class D for groups messaging & class E for future applications.

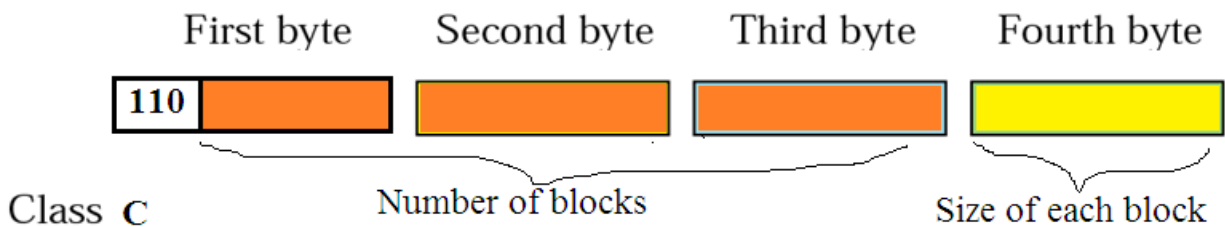
When first bit of the IP address is '0' , then it is class A address . total number of class A networks /blocks are 127. Each class A network can have 16777216 addresses.



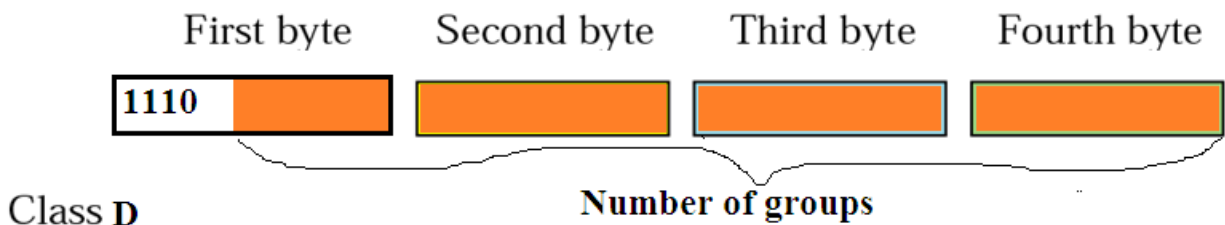
When first two bits of the address are '10' , then it is class B address . total number of class B networks /blocks are 16384. Each class B network can have 65536 addresses.



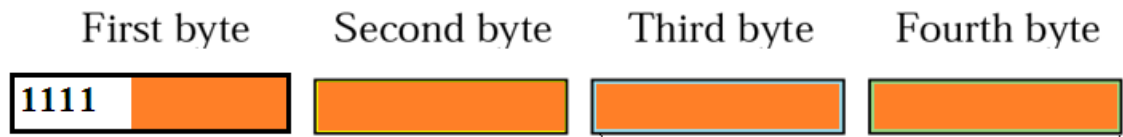
When first three bits of the address are '110' , then it is class C address . total number of class C networks /blocks are 2097152. Each class C network can have 256 addresses.



In class D there is only one block &  $2^{28} = 268,435,456$  groups . Used for multicasting



Class E addresses are reserved for future purposes



Class E

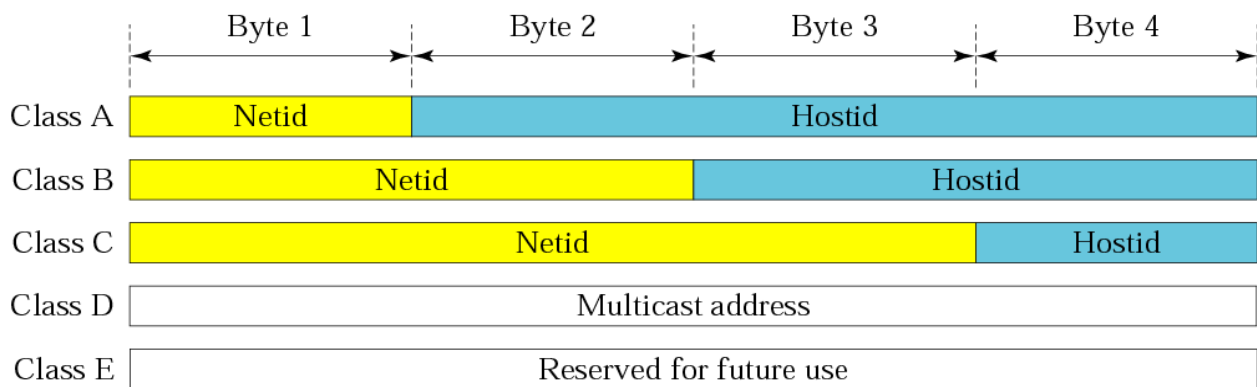
Not defined -

summary

<i>Class</i>	Number of networks /blocks	size of network	<i>Application</i>
A	128	16,777,216 hosts	Unicast
B	16,384	65,536 hosts	Unicast
C	2,097,152	256 hosts	Unicast
D	1	268,435,456 groups	Multicast
E	1	268,435,456	Reserved

In classful addressing, an IP address in class A, B, or C is divided into netid and hostid. These parts are of varying lengths, depending on the class of the address.

Note that the concept does not apply to classes D and E



**Disadvantage of classful : Many addresses are wasted.**

In class A , each network can have 1.67 crore hosts . No organization can have such number of hosts.

In class B , each network can have 65thousand hosts . Many organization cannot have such number of hosts

In class C , each network can have 256 hosts . Many organization have hosts **more** than this .

Class D has 27 crore groups, which is not required.

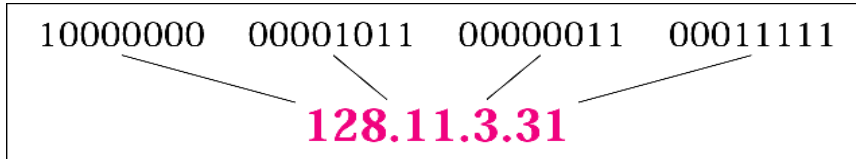
Class E reserved for future , only few used & most are wasted.

### Explain IPv4 address format

It is 32 bit address given to each node( hosts , routers ) .

Represented in decimal form with a decimal point (dot) separating the bytes. because each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255.

Eg



### Given the network address 220.34.76.0, find the class, the block, and the range of the addresses.

The class is C because the first byte is between 192 and 223.

The block has a netid of 220.34.76.

The addresses range from 220.34.76.0 to 220.34.76.255

### Given the address 132.6.17.85, find the beginning address (network address).

it is class B because the first byte is between 128 & 191 , The default mask for class B is 255.255.0.0, which means that the first 2 bytes are preserved and the other 2 bytes are set to 0s. The network address is 132.6.0.0.

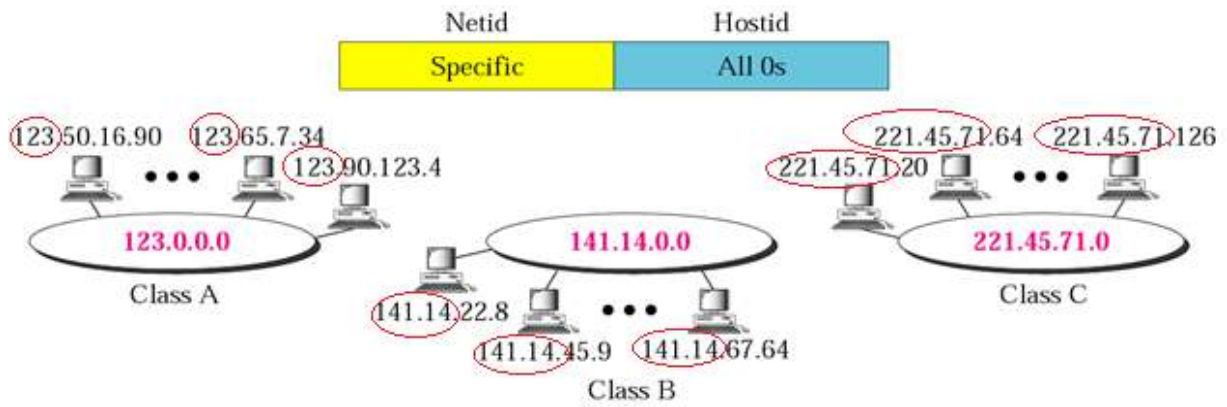
### list & explain the special addresses used in IPv4

These Are Reserved for particular functions

<i>Special Address</i>	<i>Netid</i>	<i>Hostid</i>	<i>Source or Destination</i>
Network address	Specific	All 0s	None
Direct broadcast address	Specific	All 1s	Destination
<b>Limited broadcast address</b>	All 1s	All 1s	Destination
<b>This host on this network</b>	All 0s	All 0s	Source
<b>Specific host on this network</b>	All 0s	Specific	Destination
Loopback address	127	Any	Destination

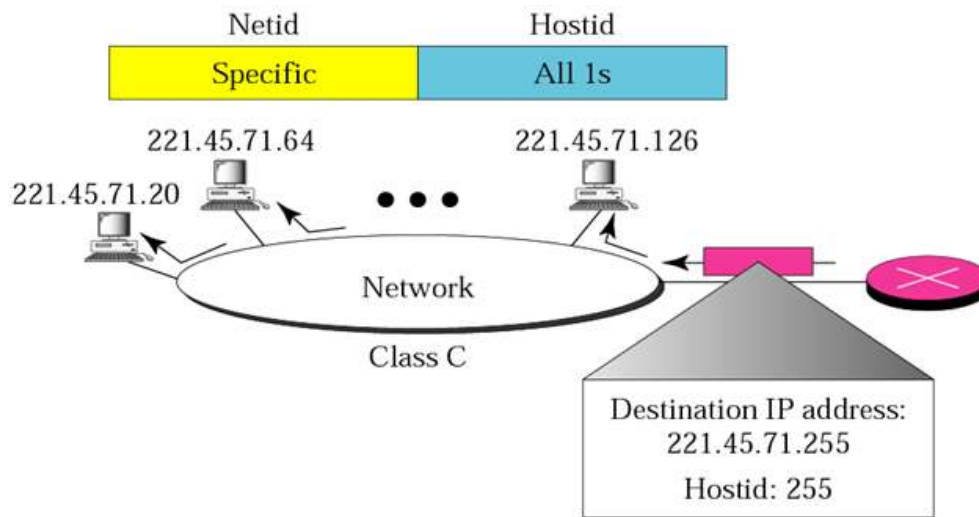
### Network address

All hosts in same network have same network address



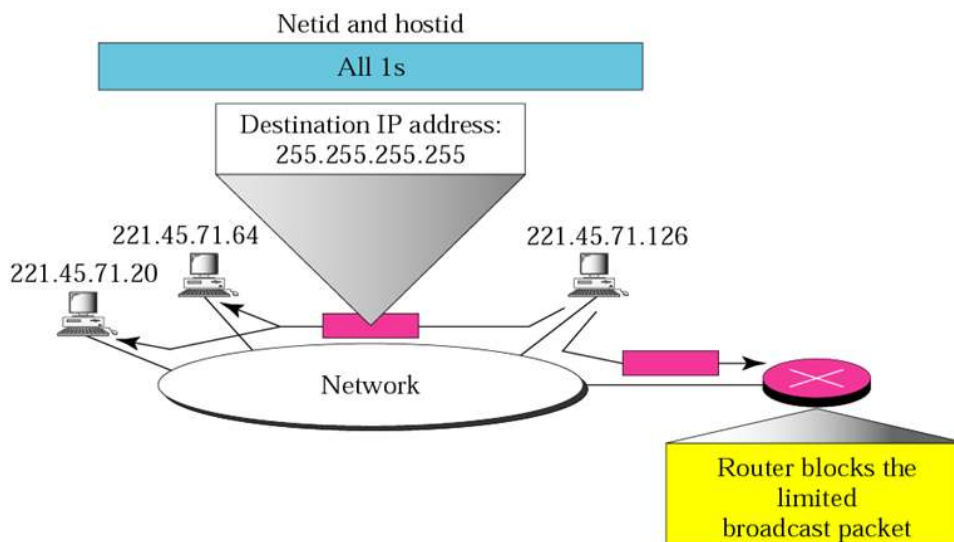
### Direct broadcast addr.

Used by router to send a packet to all hosts in the network ( i.e. broadcast)



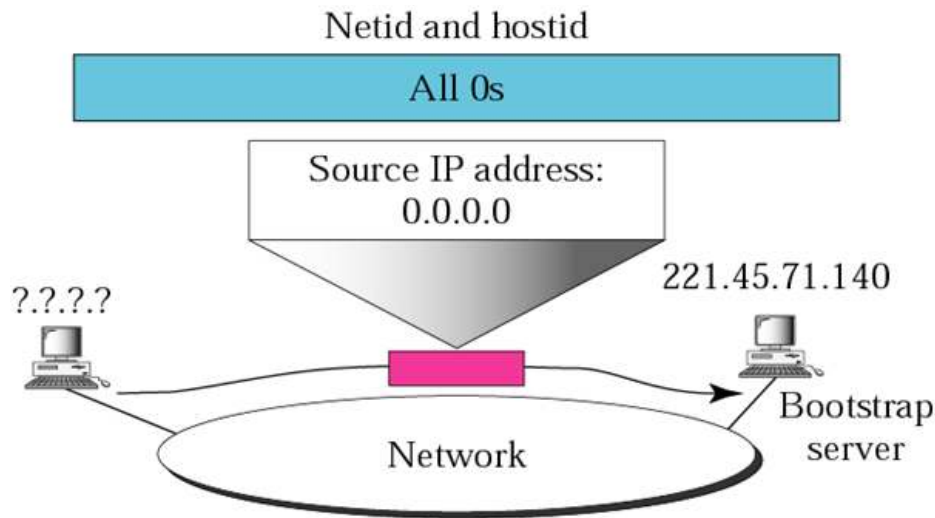
### limited broadcast address

Used by a host in a network to send a packet to all hosts in the same network ( broadcast) . But it is blocked by router so it does not go outside of network.



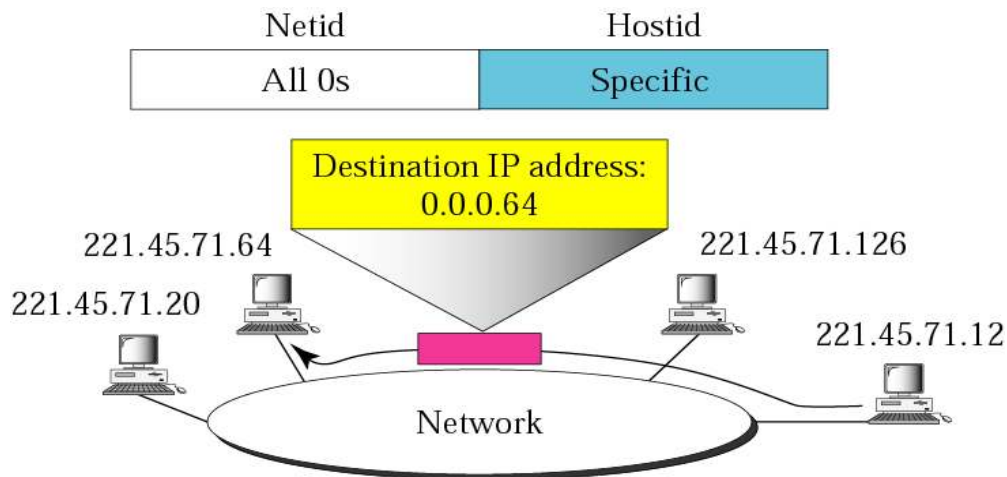
### this host on this network

Used by DHCP server to assign IP to a host



A host that does not know its IP address uses the IP address 0.0.0.0 as the source address and 255.255.255.255 as the destination address to send a message to a bootstrap server.

### specific host on this network

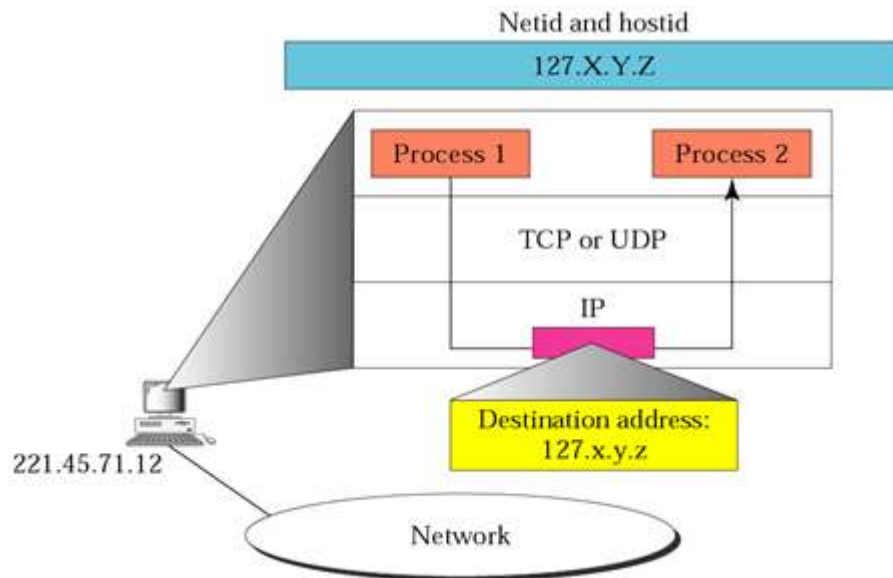


This address is used by a router or host to send a message to a specific host on the same network.

### loopback address

when two processes are in the same host . eg client & server program in same machine . ie. Localhost

This packet is not sent in the network by the host , but circulated in the same machine from client to server process.



**Compare classful addressing with classless addressing**

<b>classful addressing</b>	<b>classless addressing</b>
In this IP addresses are divided in to 5 classes	There are no classes
Each class has fixed number of networks And each network can have fixed number of hosts.	No fixed number of networks . And each network can have any number of hosts.
Many addresses are wasted in this	No addresses are wasted in this
This was initial scheme	This is later scheme. It is also called classless interdomain routing ( CIDR)
The masks are fixed Class A it is /8 Class B it is /16 Class C it is /24	Masks are not fixed It can be anything based on the size of network eg /7 /20 /29 etc

**Why is NAT required ?**

NAT means network address translation.

When connecting to internet , a host requires unique IP address. So if a home or office has many hosts, each will require a unique IP address.

Solution :NAT , which enables a organization to have a large set of addresses for internal hosts and one address to connect to external network ( Internet)

To separate the addresses used inside the home or business and the ones used for the Internet, the Internet authorities have reserved three sets of addresses as private addresses ,as shown

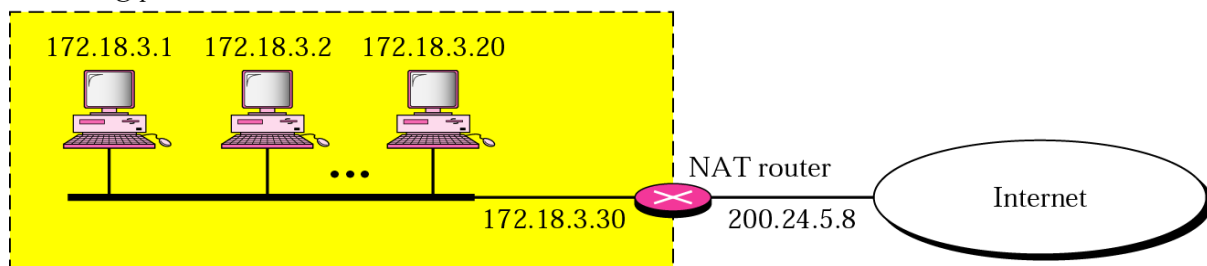
## Addresses for private networks

<i>Range</i>	<i>Total</i>
<b>10.0.0.0 to 10.255.255.255</b>	<b><math>2^{24} = 16777216</math></b>
<b>172.16.0.0 to 172.31.255.255</b>	<b><math>2^{20} = 1048576</math></b>
<b>192.168.0.0 to 192.168.255.255</b>	<b><math>2^{16} = 65536</math></b>

Any organization can use an address out of this set without permission from the Internet authorities. Since many organizations can use these addresses, they are not unique, so can't be used as public IP.

The site must have only one single connection to the global Internet through a router that runs the NAT software, as shown. The whole network has only one public IP address 200.24.5.8 which is the IP address of the NAT router.

Site using private addresses

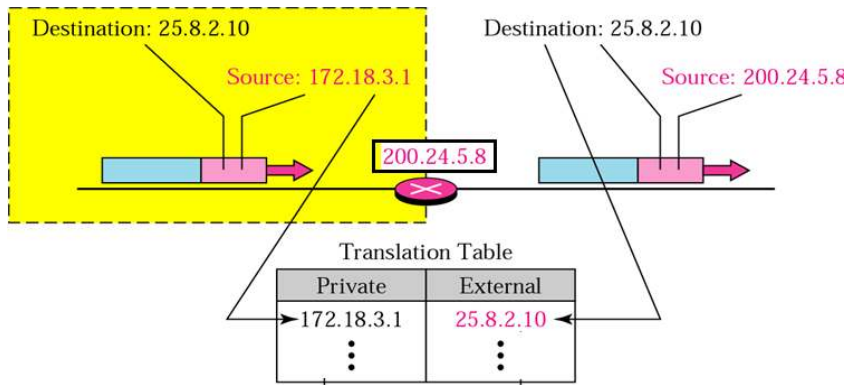


## Explain NATing

When an organization uses private IP addresses, it is required to be converted to public (global) IP address. It is done by NAT router in the organization which connects to the internet. All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global IP(NAT) address. All incoming packets also pass through the NAT router, which replaces the destination address (which is IP of the NAT router) in the packet with the appropriate private address of a host to which it is to be forwarded.

Eg. If a source host with private address 172.18.3.1 sends a packet to destination host in the internet with public address 25.8.2.10. The NAT router will replace (translate) the source IP which is private IP address 172.18.3.1 with its own public IP address 200.24.5.8.





Similarly when The destination host 25.8.2.10 sends packet to a host in this network , the NAT router will replace the destination IP address with the private IP of host 172.18.3.1.

## What is Sub-netting?

Sub-netting means Dividing (logically) a large network into small networks

Purposes:

1. To reduce network congestion( the packets send by one host to another host in the same subnet is not passed to other subnets)
2. Security between different small networks of an organization .

Eg . Consider class C network .

Each class C network has net id of 24 bits & host id of 8 bits . It can have 256 addresses . and now we want to make smaller networks( i.e. subnets) in the same network. Some of the MSB bits of host id part can be used to create subnets. The number of bits used will decide how many subnets can be there and how many hosts in each subnet )

If one bit from host part is used for subnets , there will be two subnets with subnet id 0 & 1.

So network id will have  $24 + 1 = 25$  bits .And each subnet will have 128 addresses

If two bits from host part is used for subnets , there will be four subnets with subnet id 00,01,10 & 11. So network id will have  $24 + 2 = 26$  bits .And each subnet will have 64 addresses

&so on.

Following table shows for different number of subnets ( for class c network), how many addresses can be there in each subnet and what is corresponding subnet mask.

<b>Subnets</b>	<b>1</b>	<b>2</b>	<b>4</b>	<b>8</b>	<b>16</b>	<b>32</b>	<b>64</b>	<b>128</b>	<b>256</b>
<b>Hosts</b>	<b>256</b>	<b>128</b>	<b>64</b>	<b>32</b>	<b>16</b>	<b>8</b>	<b>4</b>	<b>2</b>	<b>1</b>
<b>Subnet Mask</b>	<b>/24</b>	<b>/25</b>	<b>/26</b>	<b>/27</b>	<b>/28</b>	<b>/29</b>	<b>/30</b>	<b>/31</b>	<b>/32</b>

A company has class c network address: 192.168.4.0 / 24 . It wants to make three subnets , one for programmers , one for accounts office , one for guests/customers . design the subnets

company wants 3 subnets , so we choose column with 4 subnets , ( one subnet will be wasted)

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Each subnet will have 64 addresses , out of which two are reserved , so each subnet will have max 62 hosts.

Table shows all details of each subnet. ( company can use any three subnets out of four )

Network ID	Subnet Mask	Host ID Range	# of Usable Host	Broadcast ID
192.168.4.0	/26	192.168.4.1-192.168.4.62	62	192.168.4.63
192.168.4.64	/26	192.168.4.65-192.168.4.126	62	192.168.4.127
192.168.4.128	/26	192.168.4.129-192.168.4.190	62	192.168.4.191
192.168.4.192	/26	192.168.4.193-192.168.4.254	62	192.168.4.255

A company has class C network address: 192.168.4.0 / 24 . It wants to make subnets , each having no more than 50 hosts . design the subnets

Looking at the table , we see that using 4 subnets having 64 addresses in each , can be used

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Following Table shows all details of each subnet.

Network ID	Subnet Mask	Host ID Range	# of Usable Host	Broadcast ID
192.168.4.0	/26	192.168.4.1-192.168.4.62	62	192.168.4.63
192.168.4.64	/26	192.168.4.65-192.168.4.126	62	192.168.4.127
192.168.4.128	/26	192.168.4.129-192.168.4.190	62	192.168.4.191
192.168.4.192	/26	192.168.4.193-192.168.4.254	62	192.168.4.255

### What is CIDR?

It is Classless Interdomain Routing (CIDR) notation. The notation is used in classless addressing. it can also be applied to classful addressing , because classful addressing is a special case of classless addressing.

In classless addressing , an organization is given a block of addresses of any size as per their requirement. To identify what is network address & size of the network ( number of addresses assigned) , CIDR notation or slash notation is used.

Eg X. Y. Z.T / n ( where n is mask).

The address X. Y. Z.T and the /n notation can completely define the whole block (the first address, the last address, and the number of addresses).

What is the first address, last address & total number of addresses in the block if one of the addresses is 205.16.37.39/28?

The IP address 205.16.37.39 in binary, is

11001101 00010000 00100101 0010 0111.

&the mask is 28

1) first address :

$32 - 28 = 4$

So set 4 rightmost bits to 0, we get 11001101 00010000 00100101 0010 0000

or 205.16.37.32

2) last address :

$32 - 28 = 4$

So set 4 rightmost bits to 1, we get 11001101 00010000 00100101 00101111

Or

205.16.37.47

3) total number of addresses in the block

$n = 28$

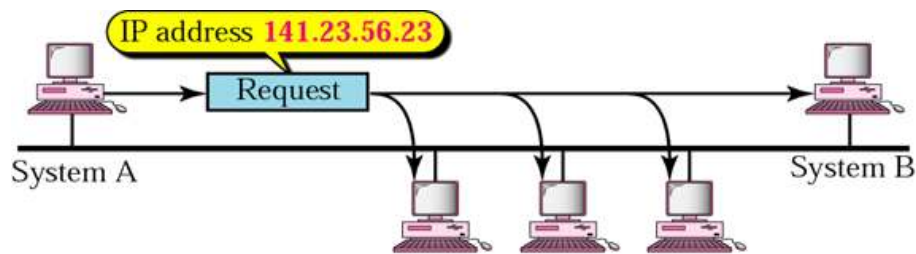
$32 - 28 = 4$

So  $2^4 = 16$

i.e. Total addresses in the block are 16

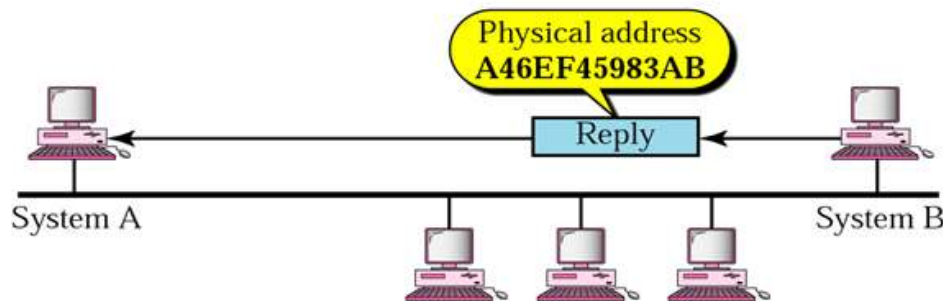
### Explain ARP

It is a protocol for obtaining the physical address of a node when its IP address is known. When a sender needs the physical address of the receiver, the host or the router uses ARP, which sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver, the query is broadcast over the network.



a. ARP request is broadcast

This packet is received by every system on the physical network, but only system B will answer it, as shown in Figure. System B sends an ARP reply packet that includes its physical address. Now system A can send all the packets it has for this destination by using the physical address it received.



b. ARP reply is unicast

*An ARP request is broadcast; an ARP reply is unicast*

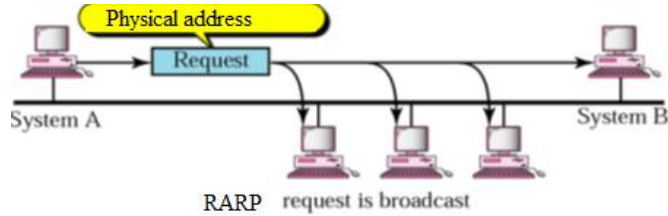
### Explain RARP

Reverse Address Resolution Protocol.

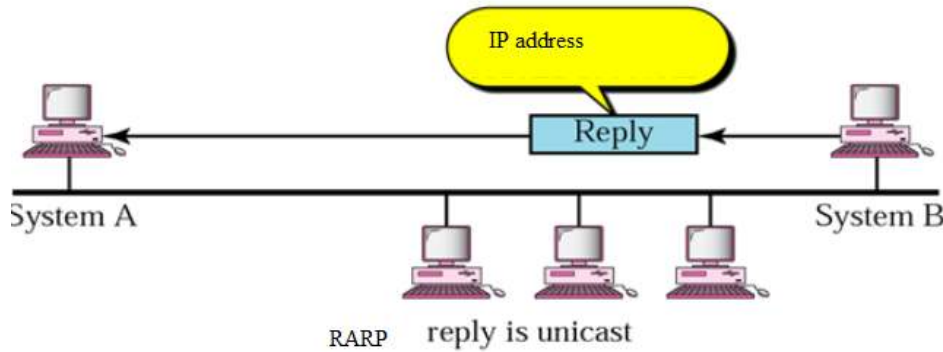
It finds the logical address for a machine that knows only its physical address.

It is required when a machine is not given static (manual) IP address but given dynamic IP address when it is booted.

The machine uses RARP to get IP address .A RARP request is created and broadcast on the local network.



Another machine on the local network that knows all the IP addresses ( i.e. a server) will respond with a RARP reply containing IP address to be assigned to the requesting machine.



RARP was replaced by BOOTP , which is then replaced by DHCP

## Explain ICMP

The Internet Control Message Protocol

It is a companion to the IP protocol.

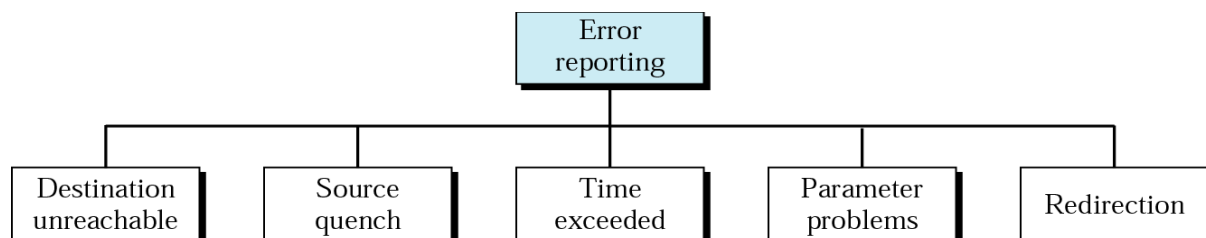
It has been designed to compensate for the two deficiencies of IP protocol.

IP provides unreliable and connectionless. So the IP protocol has no error-reporting or error-correcting mechanism. So if something goes wrong, ICMP can report it.

ICMP can send two Types of Messages: error-reporting messages and query messages.

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

The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.

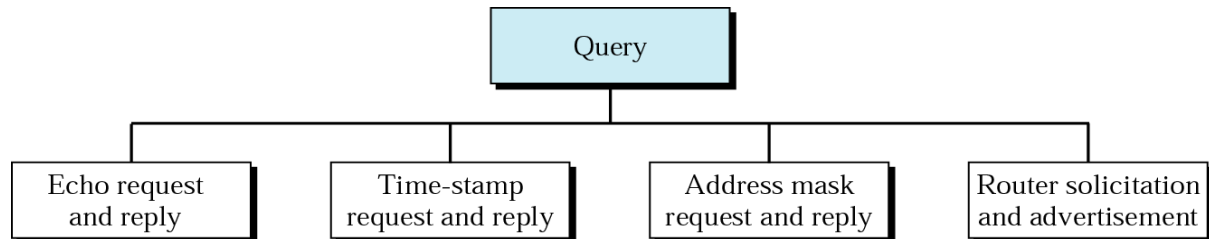


- *Destination Unreachable*  
When a router cannot route a datagram/packet
- *Source Quench*

If the datagrams are received much faster than they can be forwarded or processed, the queue (buffer memory where packets are stored in router) may overflow.

This message is sent by that router to inform source to slow down

- *Time Exceeded*  
Due to some error in routing, the packets pass through more than required routers, & when 'time to live' field in the packet reaches zero at a router, then that router informs the source through this ICMP message
- *Parameter Problem*  
when there is ambiguity in the header part of a datagram
- 



- The combination of echo-request and echo-reply messages determines whether two systems (hosts or routers) can communicate with each other at IP level. It is proof that the intermediate routers are receiving, processing, and forwarding IP datagrams. **Ping** command uses this
- *Timestamp Request and Reply*  
Two machines (hosts or routers) use these messages to determine the round-trip time needed for an IP datagram to travel between them. It can also be used to synchronize the clocks in two machines.
- *Address-Mask Request and Reply*  
A host may know its IP address, but it may not know the corresponding mask. To obtain its mask, a host sends an address-mask-request message to a router on the LAN
- *Router Solicitation and Advertisement*  
A host that wants to send data to a host on another network needs to know the address of routers connected to its own network. Also, the host must know if the routers are alive and functioning. A host can broadcast (or multicast) a router-solicitation message. The router or routers that receive the solicitation message broadcast their routing information using the router-advertisement message

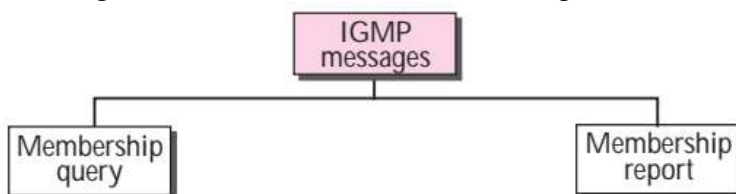
## Explain IGMP

### Internet Group Management Protocol

It is a protocol that manages group membership which can be used for multicasting by multicast routers.

In any network, there are one or more **multicast routers** that distribute multicast packets to hosts or other routers. The IGMP protocol informs the multicast routers about the membership status of hosts (routers) connected to the network.

- Eg video on demand, distance learning, stocks info to all agents etc



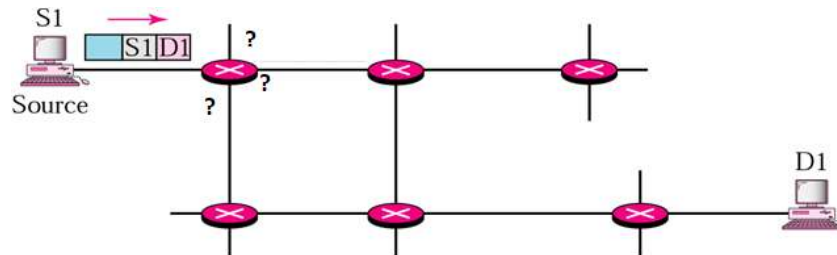
A membership query message is sent by a router to find active group members in the network.

The router periodically (by default, every 125 s) sends a general query message. When a host or router receives the general query message, it responds with a membership report message, if it is interested in a group.

## What is routing ?

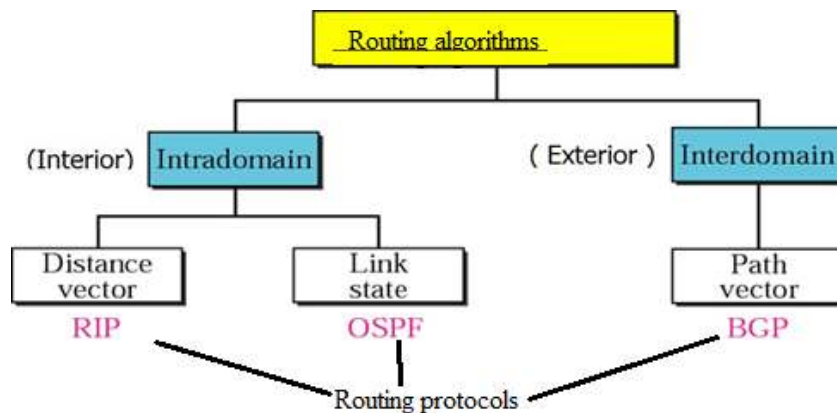
It is a function of network layer.

It is to find optimal path ( route) between a source node & destination node. It is done by the routers.



The optimal path is found based on a chosen metric such as delay or throughput or number of hops.

There are various routing algorithms & protocols based on these algorithms



the internet is divided into autonomous systems.

An **autonomous system (AS)** is a group of networks and routers under the authority of a single administration.

*intra domain routing is within same autonomous system;*

*inter domain routing is among different autonomous system.*

## Static Routing

In this there is a fix route between hosts. Routers use static routing table  
In which , the routing Information is entered manually .



The administrator enters the route for each destination into the table. When a table is created, it cannot update automatically when there is a change in the Internet. The table must be manually altered by the administrator every time there is change in network

A static routing table can be used in a small internet that does not change very often, or in an experimental internet for troubleshooting.

static routing table can't be used in a big internet .

there Dynamic Routing is used.

## Dynamic Routing

In this there is no fix route between hosts. Routers use dynamic routing table, one that is updated automatically by routers by using one of the dynamic routing protocols such as RIP, OSPF, or BGP when there is a change somewhere in the internet.

Egrouting table need to be updated when a link is down, or a new route is found through new network.

Routers in Internet use dynamic routing tables.

## Compare static & Dynamic Routing,

	static Routing,	Dynamic Routing,
	In this there is a fix route between hosts	In this there is no fix route between hosts
	Routers use static routing table	Routers use dynamic routing table
	In static routing table , the routing Information is entered manually by network administrator	dynamic routing table is updated automatically by routers by using one of the dynamic routing protocols such as RIP, OSPF, or BGP when there is a change somewhere in the internet.
	A static routing can be used in a small internet that does not change very often, or in an experimental internet for troubleshooting	A Dynamic routing can be used in internet

## Distance Vector Routing

**Principle :** *In this protocol each node maintains a vector (table) of minimum distances (minimum cost/metric) to every node*

Here distance mean any chosen metric. ( i.e. number of hops or delay or throughput etc)

It is based on algorithm called Bellman-Ford to find the shortest path between routers in a graph, given the distance between routers.

It was the routing algorithm used in first internet “ ARPANET”



Each router keeps a table ( called a vector) mentioning distance( cost) to all other routers & output port ( interface or next node ) to reach to all other routers. Then least distances ( cost of the chosen metric ), are computed using information from the neighbors' distance vectors.

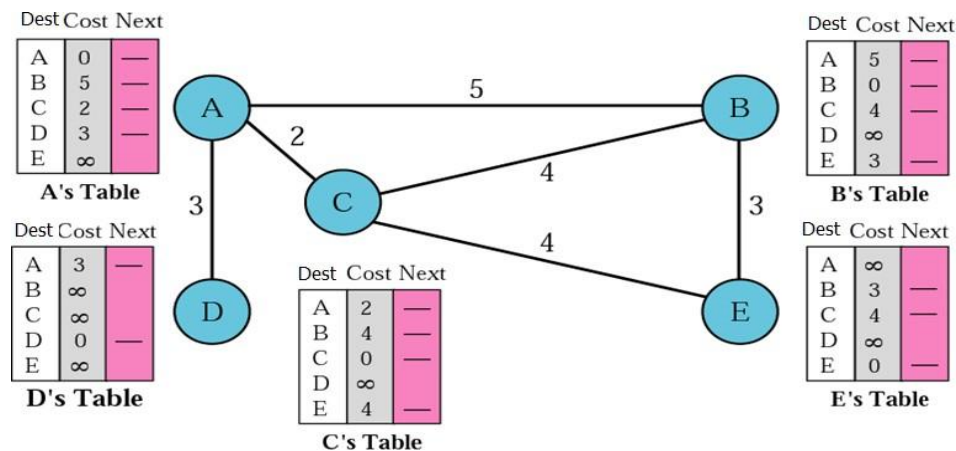
It has three stages 1) **Initialization** 2) **Sharing** 3) **Updating**

**Initialization** each router starts creating its own routing table when it is booted. After booting ,each node sends a Hello message to the immediate neighbors and find the distance between itself and these neighbors.

Distance Vector Table Initialization -

- Distance to itself = 0
- Distance to neighboring routers = distance ( cost of metric ) as seen from graph
- Distance to ALL other routers = infinity number , but for practical purpose it is set to 99

Initial tables of routers



∞ = 99

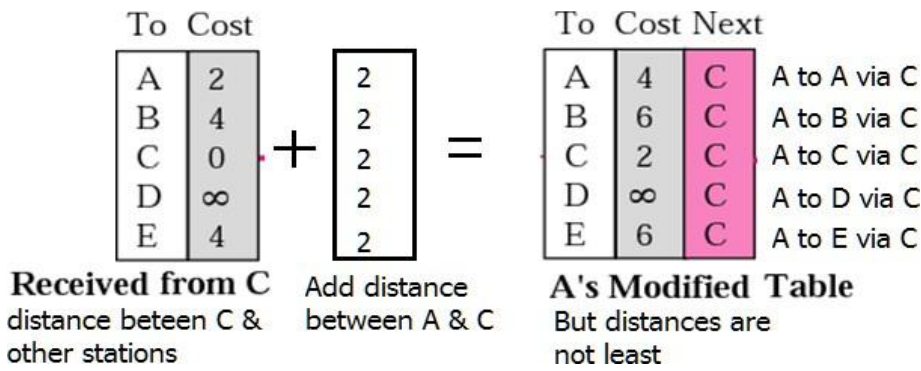
### Sharing

After initialization nodes share their tables with neighbors to improve their routing tables periodically and when there is a change in network (such as a failure in a link or in a node)

### Updating

Whenever a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

- 1) The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear . If node C claims that its distance to destination is x, and the distance between A and C is y, then the Distance between A and that destination, via C, is x+y. This is Bellman-Ford algorithm
- 2) The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.

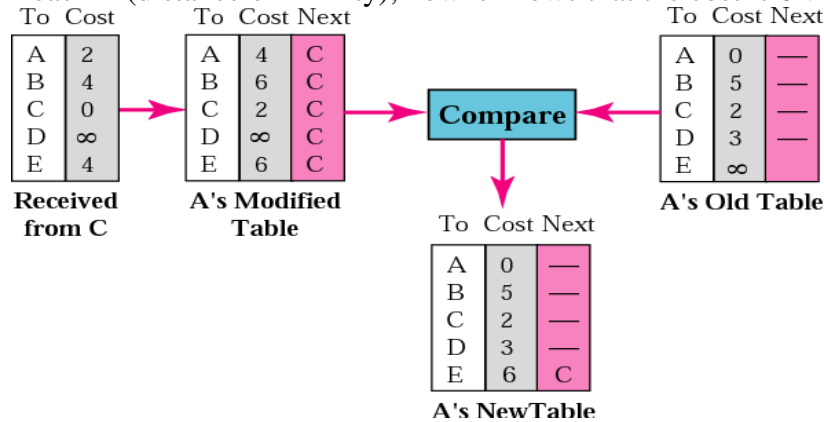


Example of new table of A after modifying its table after receiving table from C.

Whichever is entry is less, is copied in new table, with corresponding next hop.

Previously, node A did not know how to

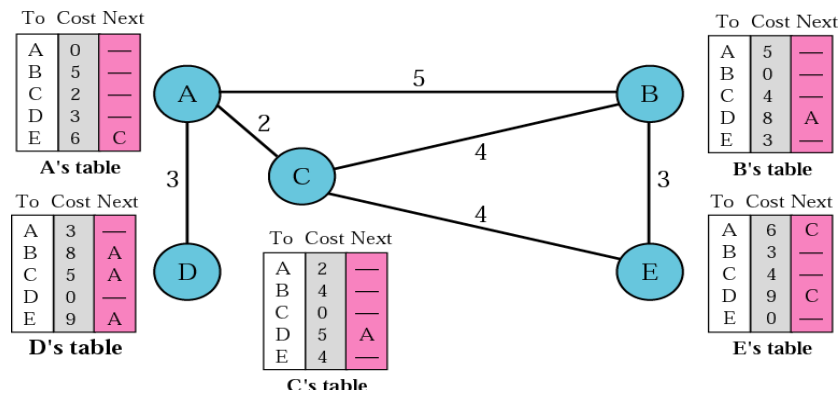
Reach E (distance of infinity); now it knows that the cost is 6 via C



Similarly Each node can update its table by using the tables received from other nodes.

In a short time, Node reaches a stable condition in which the contents of its table remains the same.

Final tables of all routers



Sharing of tables is done both periodically and when there is a change in the table.

Problem with DVR

1. Two node instability
  2. Three node instability
- Eg. Of protocol using DVR is RIP.

## Explain RIP

It is an intradomain routing protocol used inside an autonomous system.

It is a protocol based on distance vector routing algorithm.

Routers update by using Requests and Responses messages

**Requests** : A request message is sent by a router in case 1) it has just turned ON 2) It has some entries whose time is over. A request can ask about specific entries or all entries

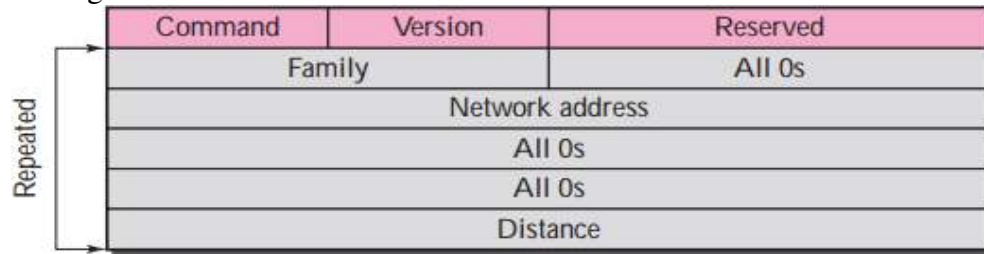


### Response

A response can be either solicited or unsolicited.

A solicited response is sent only in answer to a request. It contains information about the destination specified in the corresponding request.

An unsolicited response, is sent periodically, every 30 seconds or when there is a change in the routing table



### Timers in RIP

RIP uses three timers to support its operation. The periodic timer controls the sending of update messages, the expiration timer governs the validity of a route, and the garbage collection timer advertises the failure of a route.

## Link State Routing,

It is intradomain routing algorithm.

Each node builds whole topology upon receiving the info from **all** nodes.

topology means (the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down) ,

then the nodes can use Dijkstra's algorithm to find shortest path to every other node which is written in its routing table.

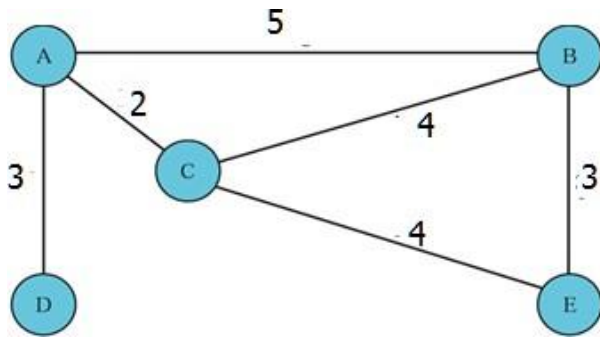
### Building Routing Tables in each router

requires four steps

1. Creation of the states of the links by each node, called the link state packet (LSP).(LSP is info of its neighbors with distances)
3. Distribution of LSPs to **every** other router, called **flooding**,
4. Formation of a shortest path tree for each node using Dijkstra's algorithm
5. Calculation of a routing table based on the shortest path tree.

Eg

For a given network of routers



Step 1. Each router creates its own LSP

eg LSP of router 'A' will be

<b>Node id</b>	<b>A</b>	
<b>sequence No.</b>		
<b>Age</b>		
<b>link states</b>	<b>B</b>	<b>5</b>
	<b>C</b>	<b>2</b>
	<b>D</b>	<b>3</b>

Step 2. Flooding of LSPs

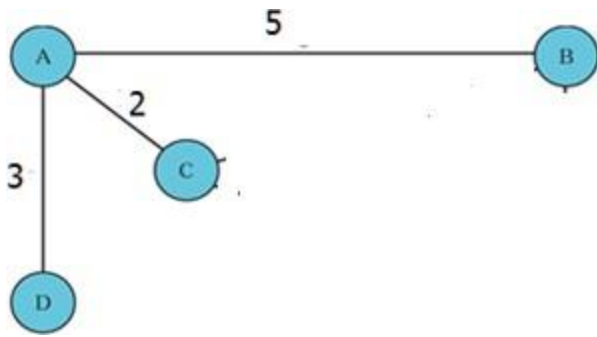
Each node sends it to all other neighbors. Then neighbors use it for building topology and also forward to their neighbors.

Step 3 :All Nodes find topology

Once Nodes get LSP from all other nodes , then All Nodes find topology

Eg below, how node A finds topology (Node A has three neighbors with given distances )

<b>A</b>	
<b>B</b>	<b>5</b>
<b>C</b>	<b>2</b>
<b>D</b>	<b>3</b>



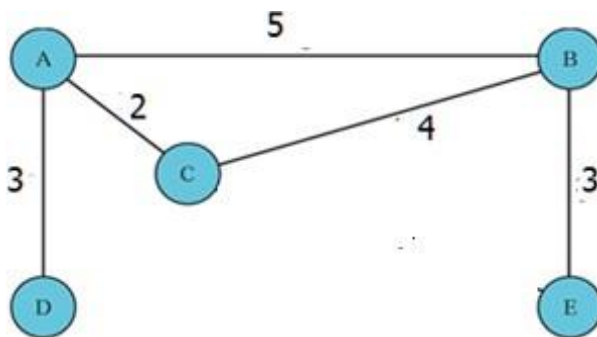
When it gets LSP from node 'B'

<b>B</b>	
<b>A</b>	<b>5</b>
<b>C</b>	<b>4</b>
<b>E</b>	<b>3</b>

Node A further updates its knowledge about topology as below

- From B's LSP, node A finds that B is connected to A, which is already in Node A's LSP
- There is link between B & C with distance 4.
- There is link between B & E with distance 3

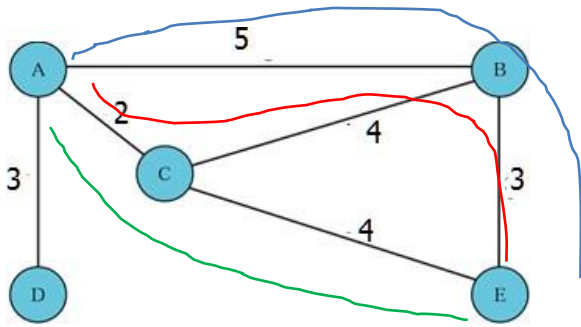
So node A modifies its knowledge about topology as shown below



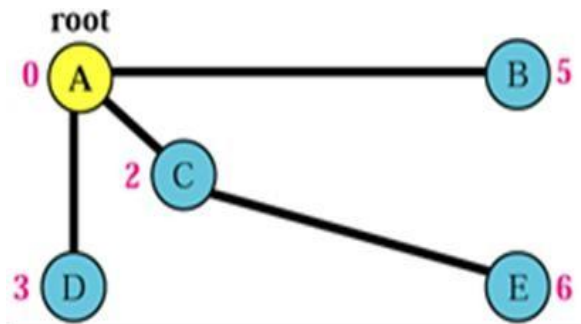
Similarly as & when it gets LSP from other nodes, it goes on building the topology. All other nodes B C D E also do the same to get complete topology.

### Step 3. Formation of Shortest Path Tree using Dijkstra Algorithm

By this the whole topology is converted in to tree. There is one tree for each node, with that node as root. All other nodes can be reached from the root through only one single shortest route.



Node E can be reached from A via ABE (with distance 8), ACE (with distance 6), ACBE (with distance 9) but shortest is ACE (with distance 6)  
 So the tree with root A is

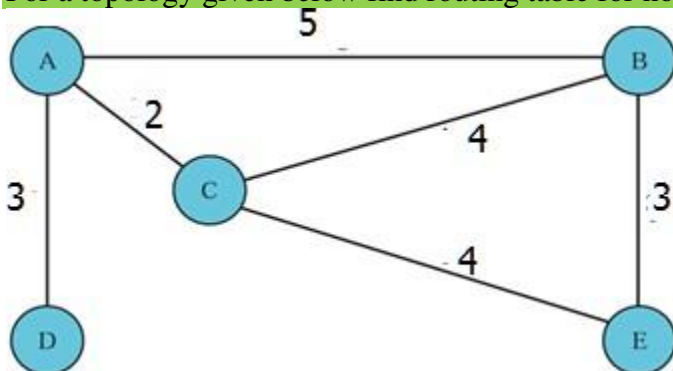


Step 4 Routing table for node  
 Routing table for node A using shortest tree path

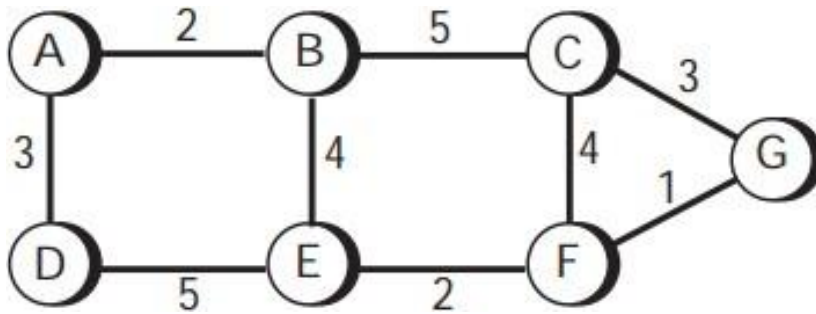
Node	Cost	Next Router
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

Similarly Routing table for other nodes can be build

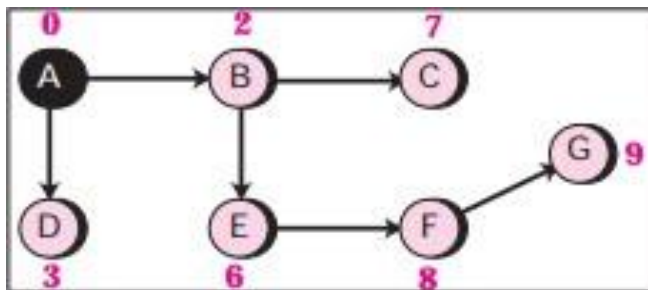
For a topology given below find routing table for node B using link state routing



For given topology , find routing table for node A , using link state routing . ( show step by step, the building of shortest path tree using Dijkstra algorithm )



Final Answer



<i>Destination</i>	<i>Cost</i>	<i>Next Router</i>
A	0	—
B	2	—
C	7	B
D	3	—
E	6	B
F	8	B
G	9	B

Compare DVR & LSR

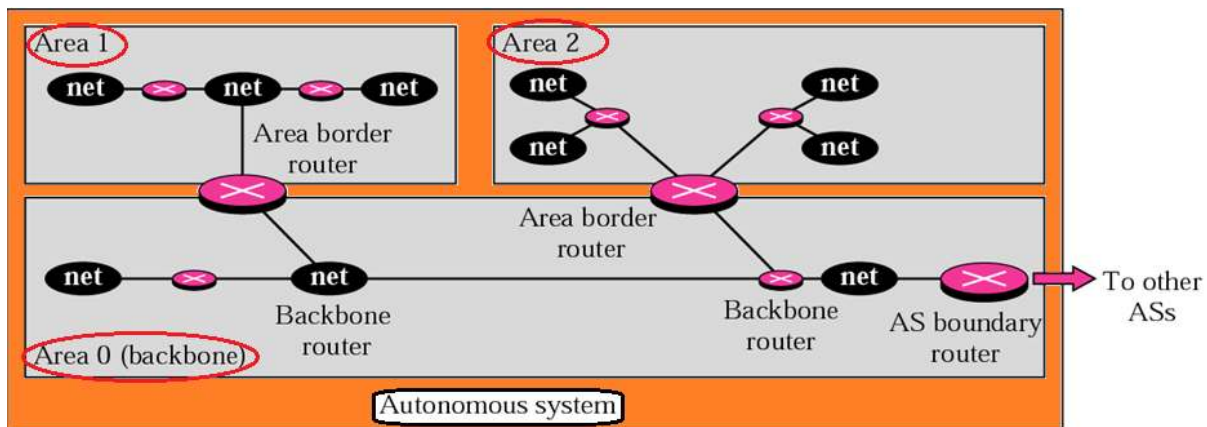
DVR	LSR
It is intradomain routing algorithm	It is also intradomain routing algorithm
Every node has only partial knowledge about whole topology	Every node has complete knowledge about whole topology
Each nodes sends info about its neighbours with respective distances to only its neighbours	Each nodes sends info about its neighbours with respective distances to its neighbours, &then neighbours send this to their neighbours. i.e. flooding
So Traffic for sending this info is less	So Traffic for sending this info is more
It generates routing tables slowly	It generates routing tables faster

Each router Uses Bellman -ford algorithm to find shortest paths to all other routers	Each router Uses Dijkshtra algorithm to find shortest paths to all other routers
It has problems of two & three node instability ( or count to infinity problem)	It does not have this problem
Implemented in RIP protocol	Implemented in OSPF protocol

## Explain OSPF

Open Shortest Path First (OSPF) protocol is an intradomain routing protocol based on link state routing.

To handle routing efficiently and in a timely manner, OSPF divides an autonomous system into **areas**. An area is a collection of networks, hosts, and routers all contained within an autonomous system (AS) . An autonomous system can be divided into many different areas.



Among the areas inside an autonomous system is a special area called the *backbone*; all the areas inside an autonomous system must be connected to the backbone. In other words, the backbone serves as a primary area and the other areas as secondary areas.

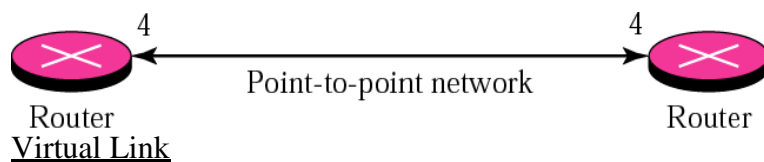
Each area has an area identification. The area identification of the backbone is zero.

Routers inside an area flood the area with routing information. At the border of an area, special routers called **area border routers** summarize the information about the area and send it to other areas.

### link.

Four types of links have been defined: point-to-point, transient, stub, and virtual

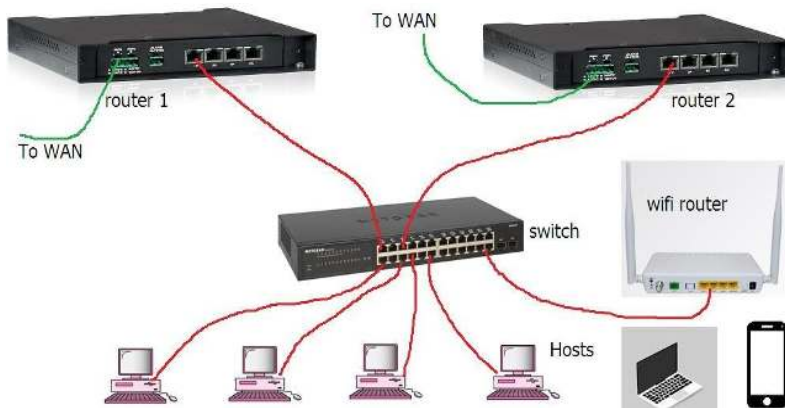
A point-to-point link connects two routers without any other host or router in between.



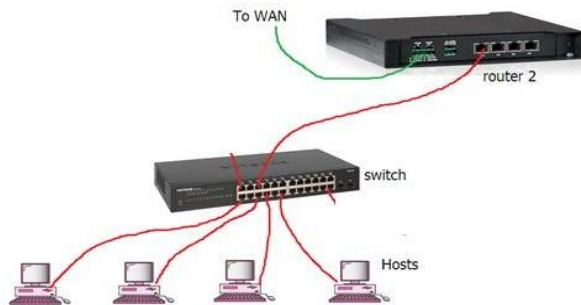
When the link between two routers is broken, the administration may create a **virtual link** between them using a longer path that probably goes through several routers.

A transient link is a network with several routers attached to it. The data can enter through any of the routers and leave through any router.

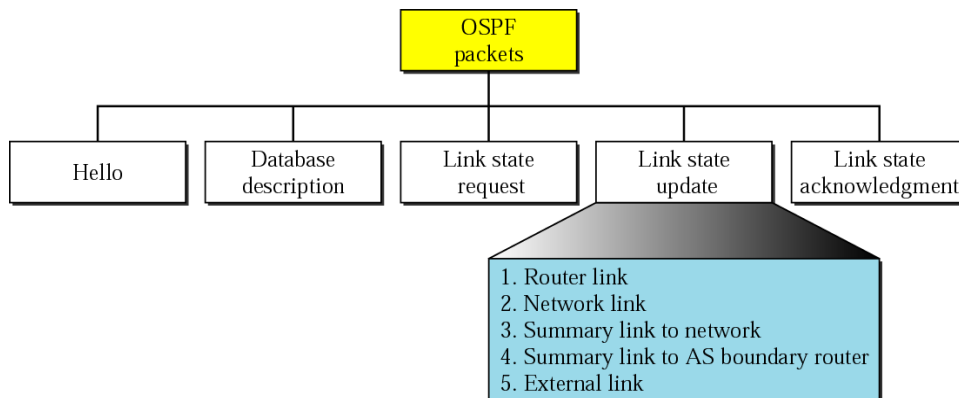




A stub link is a network that is connected to only one router. The data packets enter the network through this single router and leave the network through this same router.



OSPF uses five different types of packets for sharing info with other routers :



### Hello Message

Used to find neighbors and to test the reachability of neighbors. This is the first step in link state routing

### Database Description Message

after a router is connected to the system, it sends hello packets to greet its neighbors. If this is the first time that the neighbors hear from the router, they send a database description message ( which is their own routing table in summary form)

### Link State Request Packet

This is a packet that is sent by a router that needs information about a specific route or routes.

### Link State Acknowledgment Packet

every router must acknowledge the receipt of every link state update packet .

### Link State Update Packet

It is the heart of the OSPF operation. It is used by a router to advertise the states of its links

## Path Vector routing

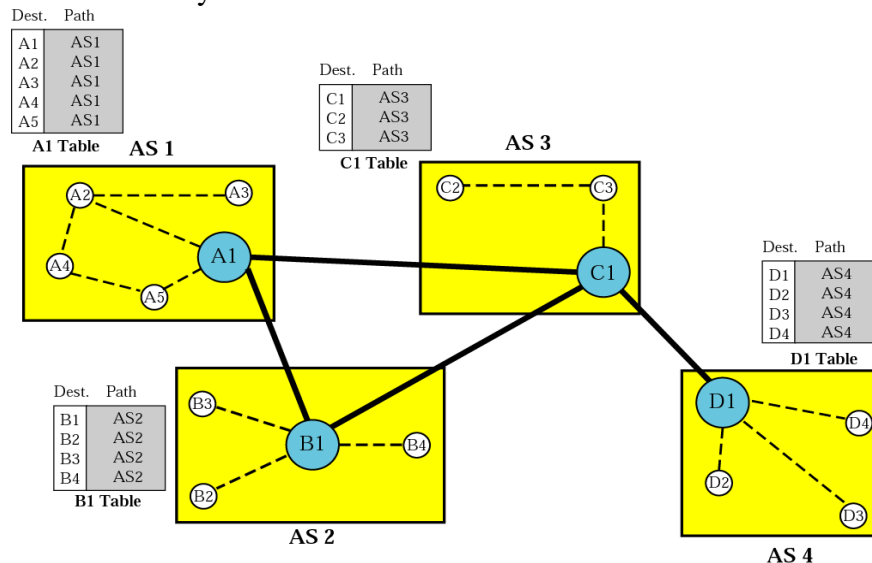
- Used for interdomain routing
- The principle of PVR is similar to that of DVR.
- IN PVR there is one node in each autonomous system (AS) that acts on behalf of the entire autonomous system, Called as speaker node. The speaker node in an AS creates a routing table and advertises it to speaker nodes in the neighboring ASs. The idea is the same as for DVR except that only speaker nodes in each AS can communicate with each other. However, what is advertised is different. A speaker node Advertises the path, not the metric of the nodes in its autonomous system.
- **Analogy** :The difference between the DVR and PVR can be compared to the difference between a national map and an international map. A national map can tell us the road to each city and the distance to be travelled if we choose a particular route; an international map can tell us which cities exist in each country and which countries should be passed before reaching that city

Eg

For given network of AS

### Initialization

At the beginning, each speaker node can know only the reachability of nodes inside its Autonomous system. As shown in tables of each AS



A1 ,B1 , C1 & D1 are speaker routers

A1..A5, B1..B4 ,C1..C3 , D1..D3 are networks

### Sharing

Just as in DVR , in PVR, a speaker in an Autonomous system shares its table with immediate neighbors. In Figure,node A1 shares its table with nodes B1 andC1. Node C1 shares its table with nodes D1,B1,And A1.Node B1 shares its table with C1 andA1. Node D1 shares its table with C1.

### Updating

When a speaker node receives a two-column table from a neighbor, it Updates its own table by adding the nodes that are not in its routing table.

After each speaker node gets tables from all neighbors, the system is stabilized.

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

**A1 Table**
**B1 Table**
**C1 Table**
**D1 Table**

## BGP

### Border Gateway Protocol (BGP)

is an interdomain routing protocol based on path vector routing algorithm.

It first developed in 1989 and has gone through four versions.

the Internet is divided into hierarchical domains called autonomous systems (ASs).

For example,

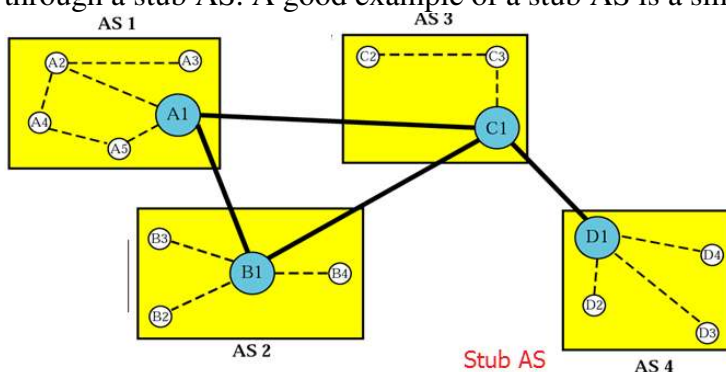
1. A large corporation that manages its own network and has full control over it, is an autonomous system.
2. A local ISP that provides services to local customers, is an autonomous system

Types of Autonomous Systems( domains)

We can divide autonomous systems into three categories: stub, multihomed, and transit.

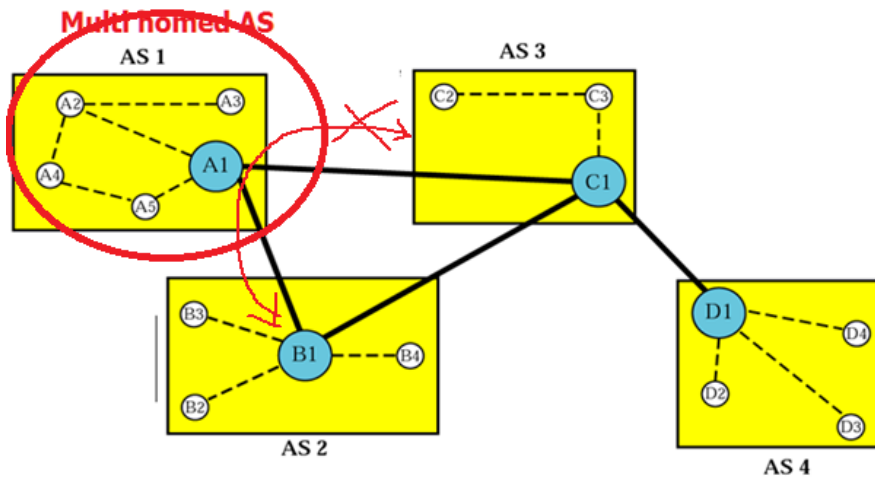
#### Stub AS

It is connected to only one AS .stub AS can send or receive data . But Data traffic, cannot pass through a stub AS. A good example of a stub AS is a small corporation or a small local ISP.



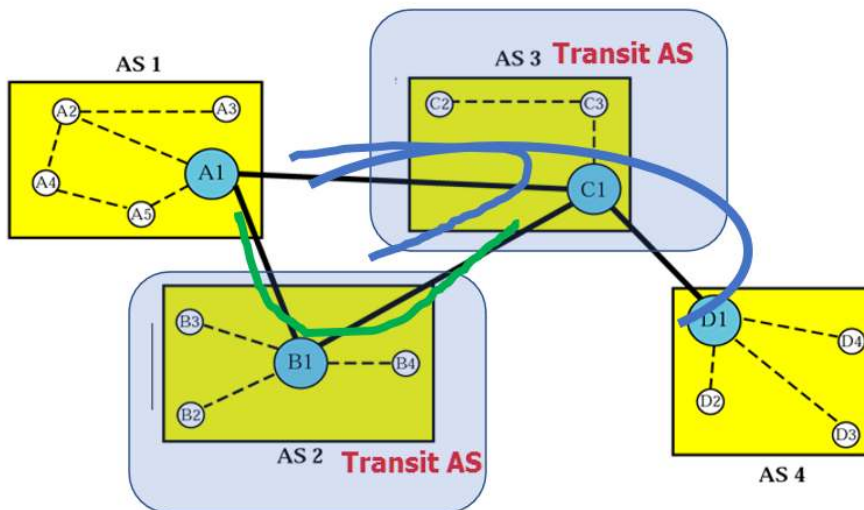
#### Multihomed AS

It is connected to more than one AS .It can receive data traffic from more than one AS. It does not allow data coming from one AS and going to another AS to pass through. A good example of a multihomed AS is a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.



### Transit AS

A transit AS is a multihomed AS that also allows transient traffic. Good examples of transit ASs are national and international ISPs (Internet backbones).



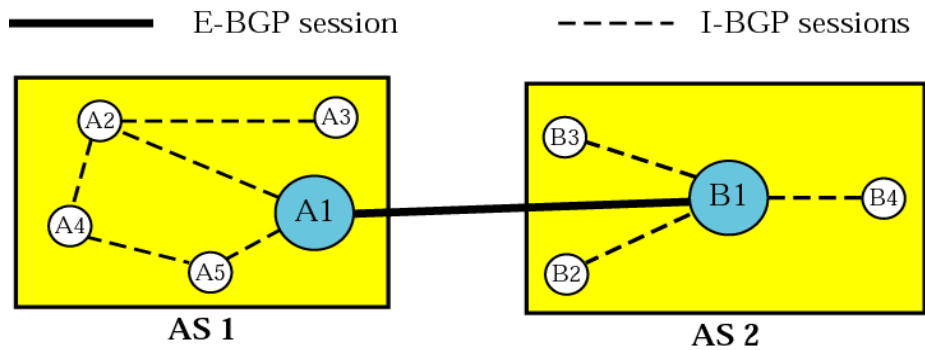
The path is a list of autonomous systems along with a list of attributes. Each attribute gives some information about the path. The list of attributes helps the receiving router make a better decision for routing.

Attributes are divided into two broad categories: well-known and optional.

### BGP Sessions

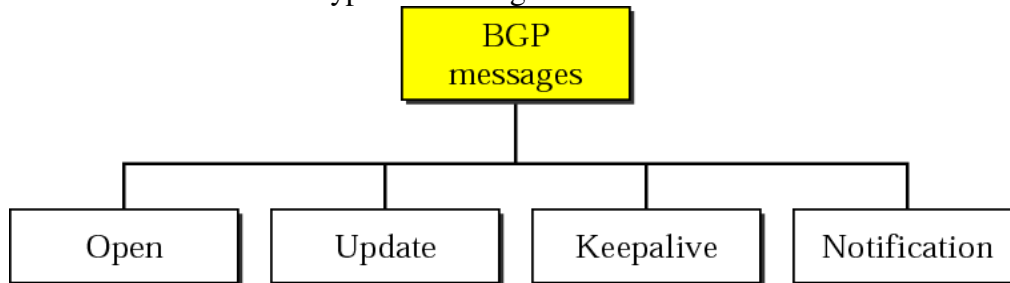
The exchange of routing information between two routers using BGP takes place in a session. A session is a connection that is established between two BGP routers only for the sake of exchanging routing information ( & not for sending data packets) . For reliable session, BGP uses the services of TCP.

BGP can have two types of sessions: external BGP (E-BGP) and internal BGP (I-BGP) sessions. The E-BGP session is used to exchange information between two speaker nodes belonging to two different autonomous systems. The IBGP session, is used to exchange routing information between two routers inside an autonomous system.



### Types of BGP messages

BGP uses four different types of messages:



- Open Message

To create a connection with its neighbors.

- Update Message

It is used by a router to update neighbors about new destinations, delete destinations or new paths to destinations.

- Keepalive Message

The routers send keepalive messages regularly to tell each other that they are alive

- Notification Message

A notification message is sent by a router whenever an error condition is detected or a router wants to close the connection

## MPLS

Multi-Protocol Label Switching .

It is Forwarding of IP packets Based on Label

IP is connectionless in which a router forwards a packet based on the destination address in the header of packet.

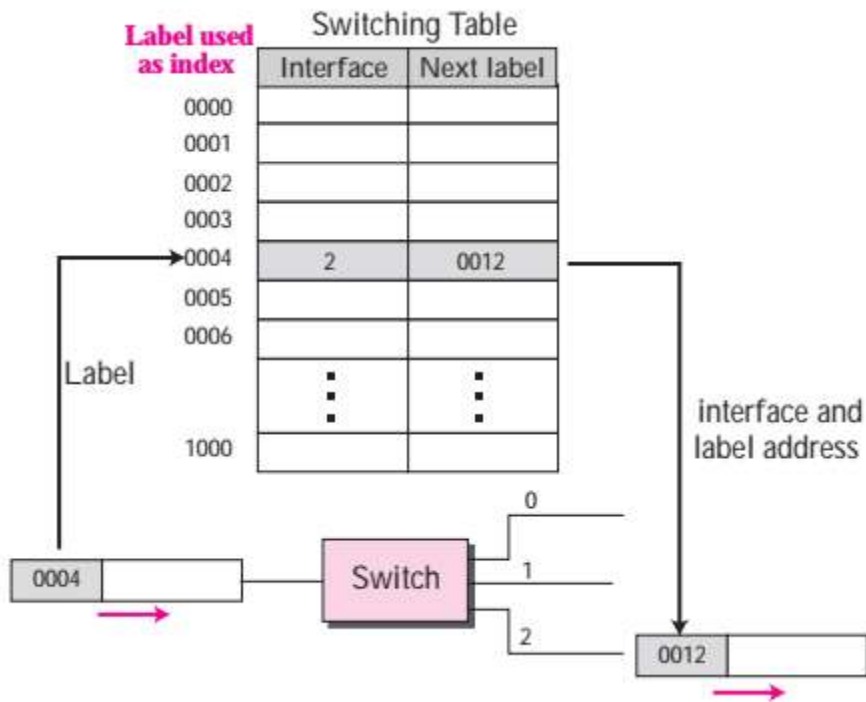
On the other hand, in a connection-oriented network (virtual-circuit approach), a switch forwards a packet based on the label attached to a packet.

In 1980s, an effort started to somehow change IP to behave like a connection-oriented protocol in which the routing is replaced by switching.

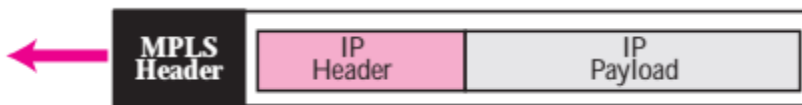
Routing is normally based on searching the contents of a table; switching can be done by accessing a table using an index.

In other words, routing involves searching; switching involves accessing

Conventional routers in the Internet can be replaced by MPLS routers that can behave like a router and a switch. When behaving like a router, MPLS can forward the packet based on the destination address; when behaving like a switch, it can forward a packet based on the label.

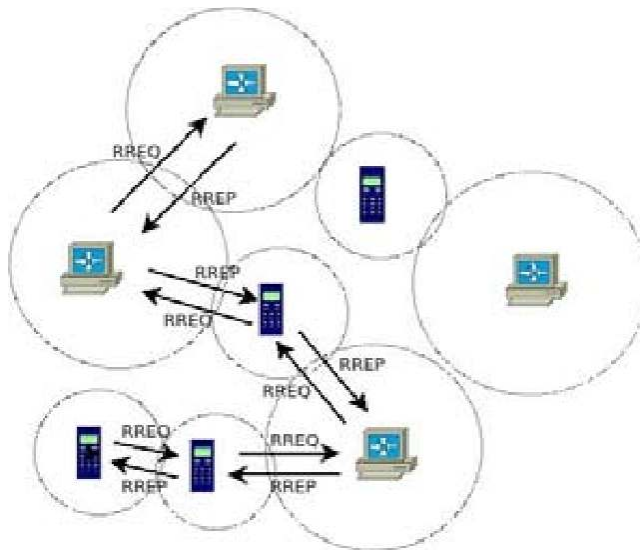


To simulate connection-oriented switching using a protocol like IP, the IPv4 packet is encapsulated in an MPLS packet & MPLS header is added.



## MANET

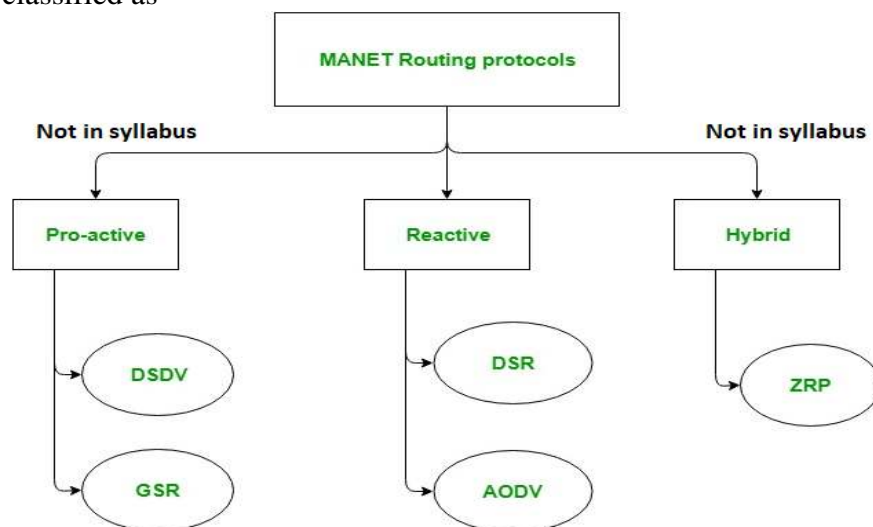
- MANET stands for Mobile Ad-Hoc Network.
- It is an **infrastructure-less** network of mobile nodes that can arbitrarily change their geographic locations. So these networks have dynamic topologies.
- MANET nodes are supplied with wireless transmitters and receivers.
- Those nodes have a limited transmission range and so, each node seeks the assistance of its neighboring nodes in forwarding packets and hence the nodes in an Ad hoc network can act as both router & hosts.
- The current **applications of MANETs** are in defense services, emergency search and rescue services, meetings and conventions, and other scenarios where quick sharing of information is acquired when no fixed infrastructure is available.



- Conventional routing protocols such as on DVR, LSR cannot be used here, because the amount of routing associated traffic would waste a huge part of the wireless bandwidth, and such discovered routes would soon become obsolete because of the mobility of nodes.

So different routing algorithms are used.

MANETs are classified as



**Proactive mode ( table-driven routing protocols ).** Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes. these routing tables are updated periodically as and when the network topology changes

**In reactive mode (on-demand routing protocol) :** the route is discovered only when it is required/needed by a node to send data to another node

## DSR

### Dynamic Source Routing protocol (DSR):

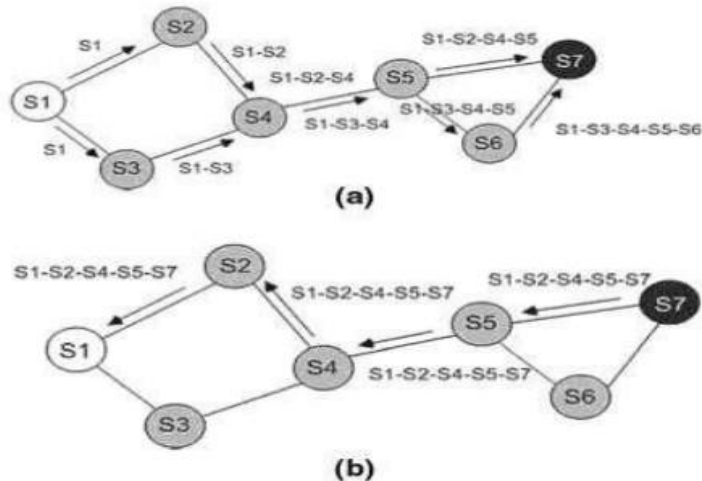
It is a reactive/on-demand routing protocol.

In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network. It consists of two phases:

1. **Route Discovery:** This phase determines the most optimal path for the transmission of data packets between the source and the destination mobile nodes.
2. **Route Maintenance:** This phase performs the maintenance work of the route as the topology in the mobile ad-hoc network is dynamic in nature and hence, there are many cases of link breakage resulting in the network failure between the mobile nodes.

### 1) Route Discovery

- It finds out the route from a source node to a destination node.
- When a source node wants to send a message to some destination node, then it first searches for its **route cache** to find whether there is a route to the destination is already exists or not.
- If there is no route to the destination, then the source node will initiate a Route Discovery and send out Route Request Message which is broadcasted to all the nodes within its transmission range.
- The Route Request Message contains the destination address, the source address, and a unique identification number.
- Each node that receives the Route Request Message checks whether it has a route to the destination or not. If it does not, it adds its address to the route record of the message and then rebroadcasts the Route Request Message on its outgoing nodes.
- When a message reaches the destination node, it will send a Route Reply Message towards the source node and this message contains the source route record list which is collected when the Route Request message is forwarded along its way to the destination.
- When the source node receives the Route Reply message, it stores returned route into its route cache. From then onwards all the messages destined to the same destination will use this route.



(a) Route Discovery (b) Using route record to send the route reply

### 2) Route maintenance

- The ad hoc network is dynamic in nature and the topology of the network changes frequently therefore, existing routes in route cache are broken frequently. Hence, route maintenance is very important.
- After forwarding a message, a node must need to confirm the reachability of the next-hop node.
- If the node does not receive any confirmation from the next hop during a certain period, it will retransmit the packet. If after few number of retransmission still does not receive any



confirmation, it will think the link to the next hop is broken and will send a Route Error message to the source node.

The protocol can also function with cellular telephone systems and mobile networks with up to about 200 nodes

### Advantages of DSR

- Reduces overhead ( additional work) on route maintenance because routes maintain only between nodes involved in communication.
- Route cache also reduces overhead during route discovery time.
- Single route discovery generates numerous routes because intermediate nodes provide replies from their local caches.

### Disadvantages of DSR

- Packet header size grows with route length due to source routing.
- A Flood of route requests may reach all nodes in the network.
- Potential collisions between route requests broadcasted by neighboring nodes
- Increased contention because too many route replies come back due to nodes replying using their local cache.
- Stale( not updated) caches will cause increased overhead

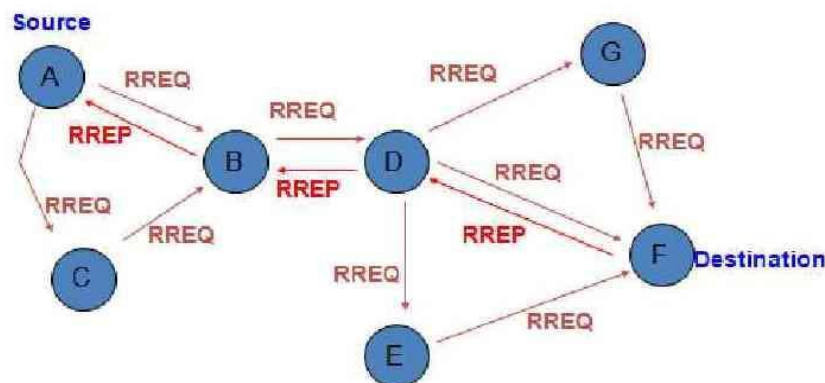
## AODV

Ad-Hoc On Demand Vector Routing protocol

- is a type of reactive /on demand protocol.
- It also operates in two phases in the similar fashion: Route discovery and Route maintenance
- supports both unicast and multicast routing. The AODV protocol was jointly developed by Nokia Research Center, the University of California, Santa Barbara and the University of Cincinnati in 1991.
- The AODV protocol builds routes between nodes only if they are requested by source nodes. AODV is therefore considered an on-demand algorithm and does not create any extra traffic for communication along links. The routes are maintained as long as they are required by the sources.

Three types of messages

- Route Request (RREQ)
- Route Reply (RREP)
- Route error ( RERR)



- node that need connections , broadcast a request ( RREQ) for connection. The remaining AODV nodes forward the message and record the node that requested a connection. Thus, they create a series of temporary routes back to the requesting node.
- A node that receives such messages and knows a route to a desired node sends a backward message (RREP) through temporary routes to the requesting node. The node that initiated the request uses the route containing the least number of hops through other nodes.
- If a link fails, the routing error (RERR) is passed back to the transmitting node and the process is repeated.

It is an extension of dynamic source routing protocol (DSR) and it helps to remove the disadvantage of dynamic source routing protocol.

- In DSR, after route discovery, when the source mobile node sends the data packet to the destination mobile node, it also contains the complete path in its header. Hence, as the nodes number increases, the length of the complete path also increases and the data packet's header size also increases which makes the whole network slow.
- Hence, AODV came as solution to it.

The main difference lies in the way of storing the path, AODV stores the path in the routing table whereas DSR stores it in the data packet's header itself

### Compare AODV & DSR

	<b>AODV</b>	<b>DSR</b>
Route discovery	Ad hoc / on demand	Ad hoc / on demand
	Nodes between source & destination decide route using routing table	Source routing ( source puts the route sequence to be used in each packet)
Number of Paths discovered	single	Multiple
Routes stored in	Routing table	Routing cache
Performance	Better in high mobility of nodes	Poor in high mobility of nodes
Route discovery	more number of times	Less number of times
Routing	Complex	simple

### Mobile IP

A Mobile IP enables a node / host to roam freely on the Internet or an organization's network while still keeping the same home address. Thus, computing activities are not disturbed when the user changes the node's point of attachment to the Internet or an organization's network. Instead, the network is updated with the new location of the mobile node.

## Stationary Hosts

The original IP addressing was designed for host which are stationary, i.e. attached to one specific network . The address is valid only when the host is attached to the network. If the network changes, the address is no longer valid.

## Mobile hosts

In Mobile IP scheme , a mobile host has two addresses : one **home address** and one **care-of address**.

- The home address is permanent;
- the care-of address changes as the mobile host moves from one network to another.

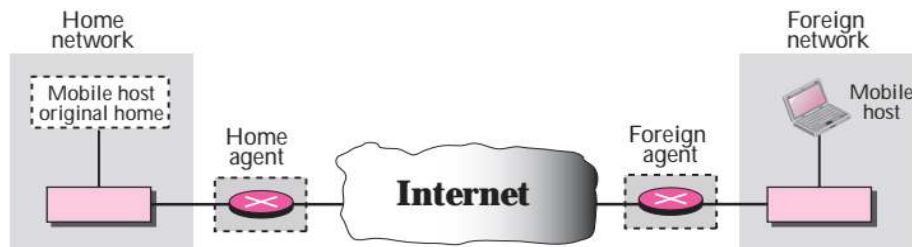
To make the change of address transparent (not visible) to the rest of the Internet requires a home agent and a foreign agent.

## Home Agent

The home agent is a router attached to the home network of the mobile host. The home agent acts on behalf of the mobile host when a remote host sends a packet to the mobile host. The home agent receives the packet and sends it to the foreign agent

## Foreign Agent

The foreign agent is a router attached to the foreign network. The foreign agent receives and delivers packets sent by the home agent to the mobile host



The Mobile IP process has three phases:

1. **Agent Discovery:** A mobile host must discover (learn the address of) a home agent before it leaves its home network. A mobile host must also discover a foreign agent after it has moved to a foreign network. This discovery consists of learning the care-of address as well as the foreign agent's address
2. **Registration:** The mobile node registers its current location with the foreign agent and home agent during registration.
3. **Data transfer :**
  1. the remote host sends a packet as if the mobile host is at its home network.
  2. the home agent sends the packet to the foreign agent using the tunneling. The home agent encapsulates the whole IP packet inside another IP packet using its address as the source and the foreign agent's address as the destination
  3. The foreign agent forwards this IP packet to the mobile host which is currently in its network

4. when mobile host wants to send packet to remote host . The mobile host prepares a packet with its home address as the source address, and the address of the remote host as the destination address. It sends this packet to foreign agent
5. The foreign agent sends it to remote host . ( here no tunneling is required as remote host is in its own home network)

