

# Computer Networks

BE Computer

Er. Anuj Sherchan  
Assistant Professor

# Unit 9 : The Network Layer in the Internet

- Outline
- 9.1 IP Protocol IPv4
- 9.2 IP Addresses
- 9.3 Subnets
- 9.4 Supernet
- 9.5 VLSM(Variable length Subnet Masking), CIDR(Classless Inter-Domain Routing) and NAT (Network Address Translator)
- 9.6 Overview of Internet Control Protocols
- 9.6.1 ICMP,IGMP
- 9.7 Routing Protocols
- 9.7.1 Interior Routing Protocol: OSPF
- 9.7.2 Exterior Routing Protocol: BGP
- 9.8 Introduction to IPv6

# Network Layer in the Internet

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).
- It ensures that each packet gets from its point of origin to its final destination.
- The network layer is considered the backbone of the OSI Model.
- It selects and manages the best logical path for data transfer between nodes.
- The routing information contained within a packet includes the source of the sending host and the eventual destination of the remote host.
- This information is contained within the network layer header that encapsulates network frames at the data link layer.

# Network Layer in the Internet

- The primary function of the network layer is to permit different networks to be interconnected.
- It does this by forwarding packets to network routers, which rely on algorithms to determine the best paths for the data to travel.
- The network layer can support either connection-oriented or connectionless networks, but such a network can only be of one type and not both.

# Internet Protocol

- The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet.
- Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.
- When you send or receive data (for example, an email note or a Web page), the message gets divided into little chunks called packets.
- Each of these packets contains both the sender's Internet address and the receiver's address.
- Any packet is sent first to a gateway computer that understands a small part of the Internet.

# Internet Protocol

- The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain.
- That gateway then forwards the packet directly to the computer whose address is specified.

# IP Address

- An Internet Protocol address (IP address) is a logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network.
- The IP address is the core component on which the networking architecture is built; no network exists without it.
- An IP address is a logical address that is used to uniquely identify every node in the network.
- Because IP addresses are logical, they can change.
- They are similar to addresses in a town or city because the IP address gives the network node an address so that it can communicate with other nodes or networks.

# IP Address

- The numerals in an IP address are divided into 2 parts:
- The network part specifies which networks this address belongs to , and
- The host part further pin points the exact location.



# IPv4 addressing

- **An IP address (IPv4)** is a 32-bit sequence of ones and zeros.
- To make the IP address easier to work with, it is usually written as four decimal numbers separated by periods.
- For example, an IP address of one computer is 192.168.1.2.
- Another computer might have the address 128.10.2.1.
- This is called the dotted decimal format.
- Each part of the address is called an octet because it is made up of eight binary digits.

# IPv4 addressing

- For example, the IP address 192.168.1.8 would be 11000000.10101000.00000001.00001000 in binary notation.
- The dotted decimal notation is an easier method to understand than the binary ones and zeros method.
- This dotted decimal notation also prevents a large number of transposition errors that would result if only the binary numbers were used.
- IPv4 uses 32-bit addresses, which means that the address space is  $2^{32}$  (more than 4 billion).
- This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the internet.

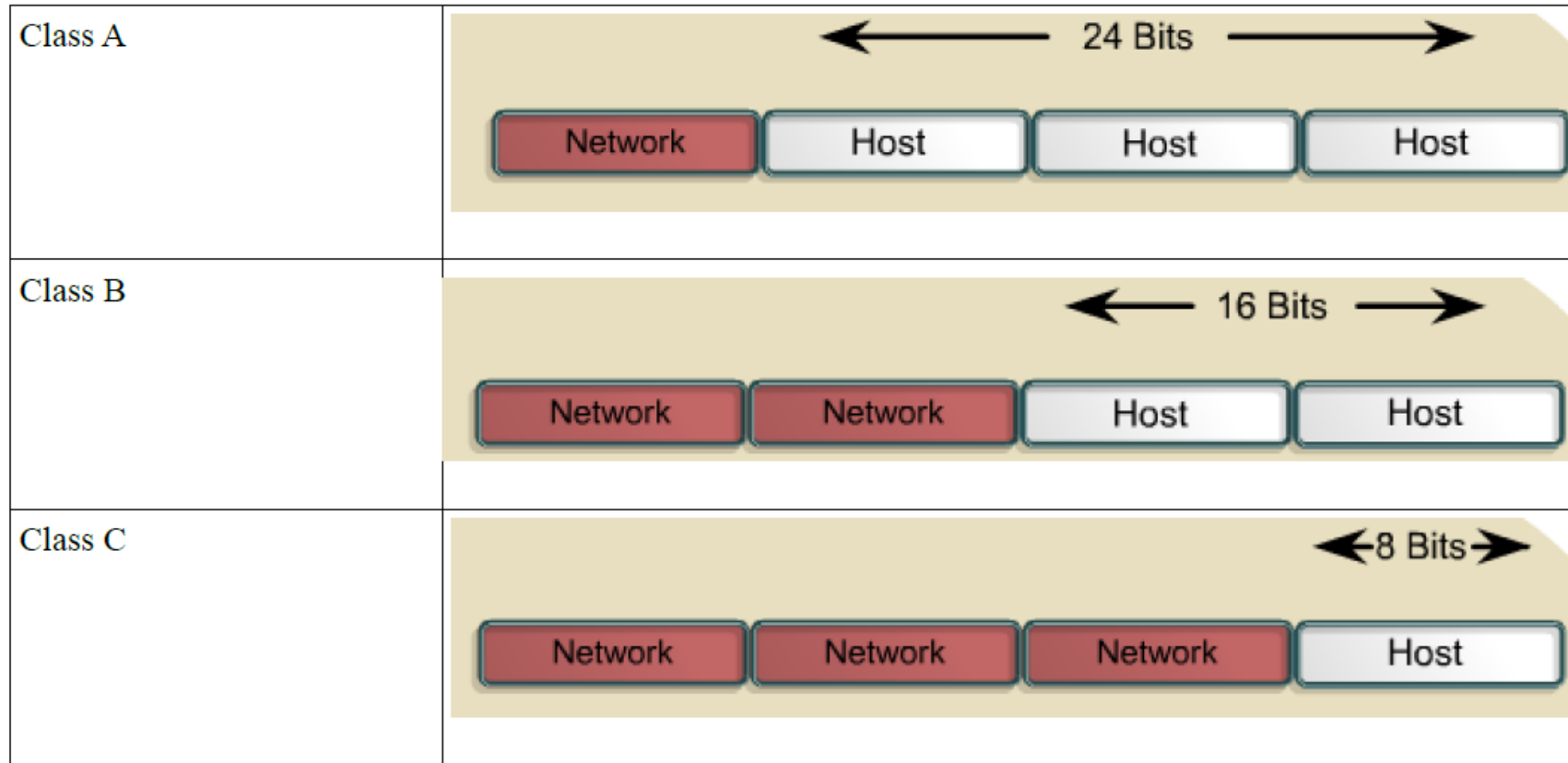
# IPv4 addressing scheme

- IP addresses falls into two types:
- Classful IP addressing is a legacy scheme which divides the whole IP address pools into 5 distinct classes—A, B, C, D and E.
- Classless IP addressing has an arbitrary length of the prefixes.

# IPv4 Classful addressing

IP Address Class	First Octet Address Range	Used for:
Class A	0-127	Unicast (Very Large Networks)
Class B	128-191	Unicast (Medium to large network)
Class C	192-223	Unicast (Small Network)
Class D	224-239	Multicast
Class E	240-255	Reserved

# IPv4 Classful addressing



- Every IP address has two parts.
- The first part identifies the network (Network ID) where the system is connected.
- Second part identifies the system (Host ID).

# Class A

- Class A address block was designed to support extremely large networks with more than 16 million host addresses.
- Class A IPv4 addresses use a fixed /8 prefix with the first octet to indicate the network address.
- The remaining three octets were used for host addresses.
- The first bit of a Class A address is always 0.
- With that first bit a 0, the lowest number that can be represented is 00000000, decimal 0.
- The highest number that can be represented is 01111111, decimal 127.
- The numbers 0 and 127 are reserved and cannot be used as network addresses.
- Any address that starts with a value between 1 and 126 in the first octet is a Class A address.

# Class A

- No of Class A Network:  $2^7=128$
- No. of Usable Host address per Network:  $2^{24}-2=16777214$ .
- 2 addresses are reserved for network and broadcast address.

# Class B

- Class B address space was designed to support the needs of moderate to large size networks with more than 65,000 hosts.
- Class B IP address uses two high-order octets to indicate the network address.
- The other two octets specifies host addresses. As with class A, address space for the remaining address classes needed to be reserved.
- The first two bits of the first octet of a Class B address are always 10.
- The remaining six bits may be populated with either 1s or 0s. Therefore, the lowest number that can be represented with a Class B address is 10000000(decimal 128).
- The highest number that can be represented is 10111111, decimal 191.



# Class B

- Any address that starts with a value in the range of 128 to 191 in the first octet is a Class B address.
- No of Class B Network:  $2^{14}=16384$
- No. of Usable Host address per Network:  $2^{16}-2=65534$ .

# Class C

- The class C address space was the most commonly available of the historic address classes.
- This address space are for small networks with a maximum of 254 hosts.
- Class C address blocks used a /24 prefix.
- Class C network uses only the last octet as host address with the three high-order octets used to indicate the network address.
- Class C address begins with binary 110. Therefore, the lowest number that can be represented is 11000000 (decimal 192).
- The highest number that can be represented is 11011111(decimal 223).

# Class C

- Address containing a number in the range of 192 to 223 in the first octet is a Class C address.
- No of Class C Network:  $2^{21}-2=2097150$ .
- No. of Usable Host address per Network:  $2^8-2=254$ .

# Class D

- The Class D address class was created to enable multicasting in an IP address.
- A multicast address is a unique network address that directs packets to predefined groups of IP addresses.
- Therefore, a single station can simultaneously transmit a single stream of data to multiple recipients.
- The Class D address space, much like the other address spaces, is mathematically constrained.
- The first four bits of a Class D address must be 1110.
- An IP address that starts with a value in the range of 224 to 239 (11100000 to 11101111) in the first octet is a Class D address.

# Class E

- Class E address is reserved for its own research by the Internet Engineering Task Force(IETF).
- Class E addresses is not been released for use in the Internet.
- The first four bits of a Class E address are always set to 1s.
- Therefore, the first octet range for Class E addresses is 11110000 to 11111111 (240 to 255).

# Classful Addressing

Class	1 <sup>st</sup> Octet Decimal Range	1 <sup>st</sup> Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 ( $2^7 - 2$ )	16,777,214 ( $2^{24} - 2$ )
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ( $2^{14} - 2$ )	65,534 ( $2^{16} - 2$ )
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ( $2^{21} - 2$ )	254 ( $2^8 - 2$ )
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	1111	Experimental; used for research			

# Classful Addressing

## Private IP Addresses

Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

# Subnet Mask

- To define the network and host portions of an address, devices use separate 32-bit pattern called a subnet mask.
- We express the subnet mask in the same dotted decimal format as the IPv4 address.
- The subnet mask is created by placing a binary 1 in each bit position representing the network portion and placing a binary 0 in each bit position represents the host portion.
- Default Subnet Mask:
  - Class A: 255.0.0.0
  - Class B: 255.255.0.0
  - Class C: 255.255.255.0



# Subnetting

## Subnetwork benefits



**Subdivide on IP network number  
is an important initial task of  
network managers**

# Subnetting

- During the era of Classful Addressing, subnetting was introduced.
- If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group and assign each group to smaller networks called subnets or in rare cases share part of the addresses with the neighbors.
- A subnetwork or subnet is a logical subdivision of an IP network.
- The practice of dividing a network into two or more networks is called subnetting.
- Subnetting increases the number of 1s in the mask.
- Subnetting is the process of borrowing host bits and increasing the number of networks.

# Subnetting

- Example:
- IP address: 192.168.1.1 is Class C address
- We need 5 networks of these IP address
- Octet format is: N.N.N.H
- N-Network bit, H-Host bit
- Default Subnet Mask: 255.255.255.0
- Subnetting is converting Host bit to required network bit.
- Means  $2^s = 5$
- Value of  $s > 2$  taking next value,  $s=3$  (where  $s$ =subnet bit)

# Subnetting

- $2^3 =$  Subnets

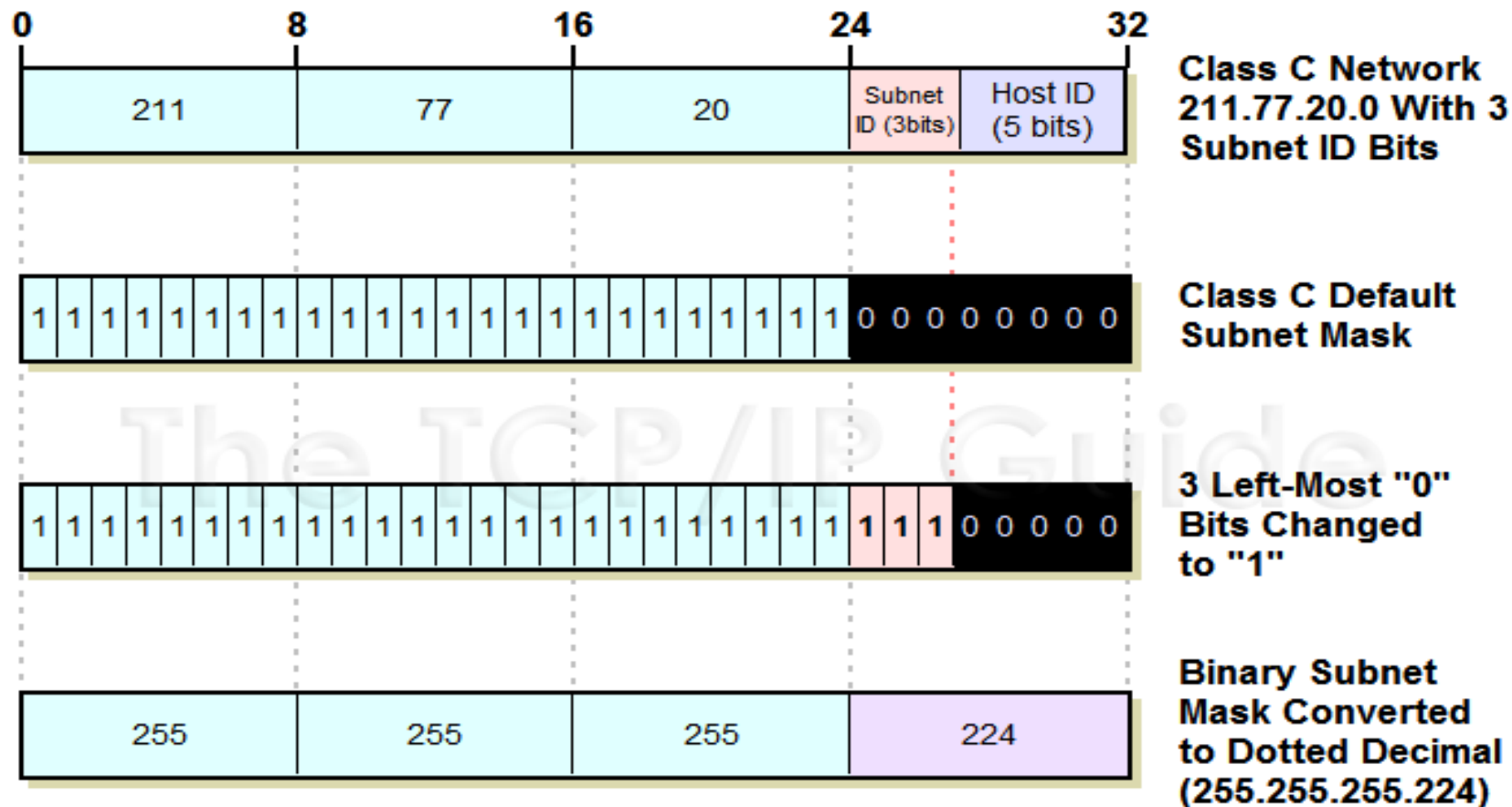
Now IP format will be as below

- IP address: 192.168.1.1
- Network address: 192.168.1.0
- 192.168.1.0
- 11000000.10101000.00000001.00000000
- nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.hhhhhhh
- After subnetting
- nnnnnnnnn.nnnnnnnnn.nnnnnnnnn.ssshhhhh

# Subnetting

- No. of host per subnet
- $= 2^h - 2$  (-2 is for network & broadcast address)
- $= 2^5 - 2 = 30$  Hosts/Subnets
- IP address range of 192.168.1.1 will be
- 1 subnet = 192.168.1.0 to 192.168.1.31
- 2 subnet = 192.168.1.32 to 192.168.1.63
- 3 subnet = 192.168.1.64 to 192.168.1.95
- 4 subnet = 192.168.1.96 to 192.168.1.127
- 5 subnet = 192.168.1.128 to 192.168.1.159
- 6 subnet = 192.168.1.160 to 192.168.1.191
- New Subnet mask will be: 255.255.255.224

# Subnetting



# Subnetting

- **Subnetting Class C Address: 192.168.10.0/26**
- We have default subnet mask :255.255.255.0
- In this example, we're going to subnet the network address 192.168.10.0 using the subnet mask 255.255.255.192.
- 192.168.10.0 = Network address
- 255.255.255.192 = Custom Subnet mask
- How many subnets?
- Since 192 is 2 bits on (11000000), the answer would be  $2^2 = 4$  subnets.
- How many hosts per subnet?
- We have 6 host bits off (11000000), so the equation would be  $2^6 - 2 = 62$  hosts.
- What are the valid subnets?  $256 - 192 = 64$ .
- Remember, we start at zero and count in our block size, so our subnets are 0, 64, 128, and 192. (Magic Number=256-Subnet Mask)

# Subnetting

- **What's the broadcast address for each subnet?**
- The number right before the value of the next subnet is all host bits turned on and equals the broadcast address.
- For the zero subnet, the next subnet is 64, so the broadcast address for the zero subnet is 63.
- **What are the valid hosts?**
- These are the numbers between the subnet and broadcast address.
- The easiest way to find the hosts is to write out the subnet address and the broadcast address.
- This way, the valid hosts are obvious.
- The following table shows the 0, 64, 128, and 192 sub-nets, the valid host ranges of each, and the broadcast address of each subnet:



# Subnetting

The subnets (do this first)	0	64	128	192
The broadcast address	63	127	191	255
Usable Host Range	1 – 62	65 – 126	129 – 190	193 - 254

# Subnetting

- **Subnetting Class B Address: 172.16.0.0/17**
- 172.16.0.0 = Network address
- 255.255.0.0 = Default Subnet mask
- 255.255.128.0 = Custom Subnet Mask
- Subnets?  $2^1 = 2$  (same as Class C).
- Hosts?  $2^{15} - 2 = 32,766$  (7 bits in the third octet, and 8 in the fourth).
- Valid subnets?  $256 - 128 = 128$ . 0, 128.
- Remember that subnetting is performed in the third octet, so the subnet numbers are really 0.0 and 128.0, as shown in the next table.
- These are the exact numbers we used with Class C; we use them in the third octet and add a 0 in the fourth octet for the network address.
- Broadcast address for each subnet? Valid hosts?

# Subnetting

- The following table shows the two subnets available, the valid host range, and the broad-cast address of each:

Subnet	172.16.0.0	172.16.128.0
Broadcast	172.16.127.255	172.16.255.255
Usable Host Range	172.16.0.1 - 172.16.127.254	172.16.128.1 - 172.16.255.254

# Subnetting

- **Subnetting Class A network: 10.0.0.0/16**
- Network Address: 10.0.0.0
- Default Subnet Mask :255.0.0.0
- Custom Subnet Mask : 255.255.0.0
- Class A addresses use a default mask of 255.0.0.0, which leaves 22 bits for subnetting since you must leave 2 bits for host addressing.
- The 255.255.0.0 mask with a Class A address is using 8 subnet bits.
- Subnets?  $2^8 = 256$ .
- Hosts?  $2^{16} - 2 = 65,534$ .

# Subnetting

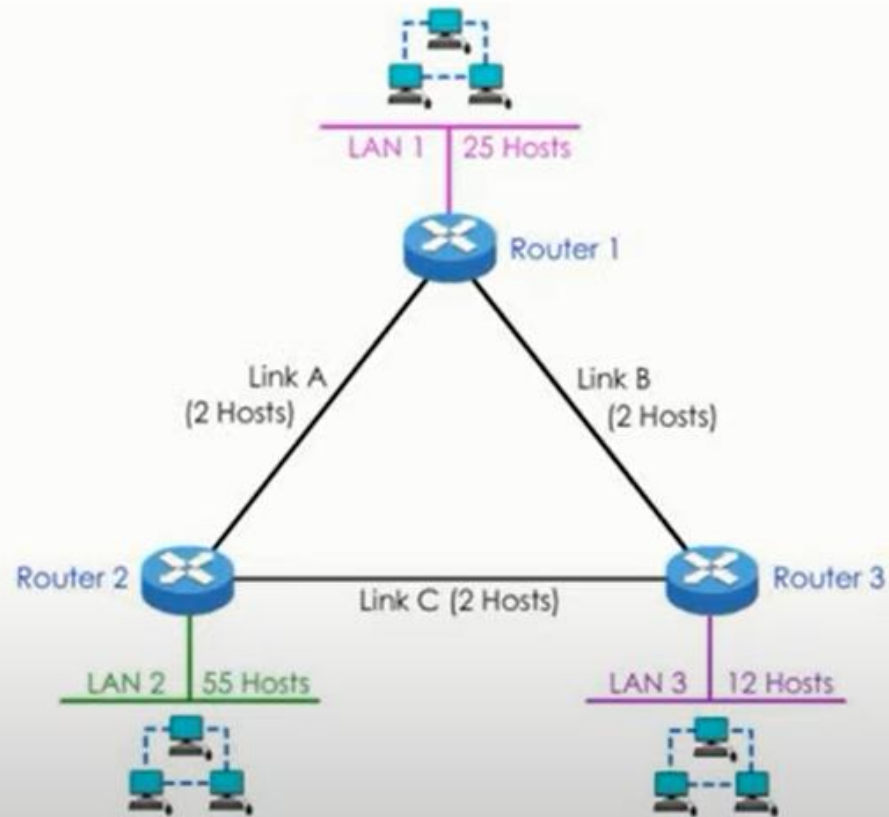
- Valid subnets? What is the interesting octet?  $256 - 255 = 1$ . 0, 1, 2, 3, etc. (all in the second octet).
- The subnets would be 10.0.0.0, 10.1.0.0, 10.2.0.0, 10.3.0.0, etc., up to 10.255.0.0.
- Broadcast address for each subnet? Valid hosts?
- The following table shows the first two and last two subnets, valid host range, and broad-cast addresses for the private Class A 10.0.0.0 network:

Subnet	10.0.0.0	10.1.0.0 ...	10.254.0.0	10.255.0.0
Broadcast	10.0.255.255	10.1.255.255 ...	10.254.255.255	10.255.255.255
First host	10.0.0.1	10.1.0.1 ...	10.254.0.1	10.255.0.1
Last host	10.0.255.254	10.1.255.254 ...	10.254.255.254	10.255.255.254

# Variable Length Subnet Masking

- Variable-Length Subnet Masking (VLSM) means "subnetting subnets," which means that VLSM allows network engineers to divide an IP address space into a hierarchy of subnets of different sizes, making it possible to create subnets with very different host counts without wasting large numbers of addresses.
- A subnet mask defines the size of the subnet (the number of host addresses in the subnet).
- Fixed-Length Subnet Masking (FLSM) creates subnets all the same size. But where some subnets will have many hosts and some have few, FLSM results in some subnets having many orphaned addresses, or some sets of hosts being too big to fit into a subnet.
- Where VLSM is enabled, a large subnet can be divided into a set of smaller sub-subnets, which can be used to handle smaller sets of hosts.

# VLSM Example



## Question

The network consists of three Local area networks: LAN 1, LAN 2, and LAN3. These three LANs are connected with three serial links: Link A, link B, and link C.

With an ID range - 192.168.4.0/24, please design an IP plan for the network using VLSM.

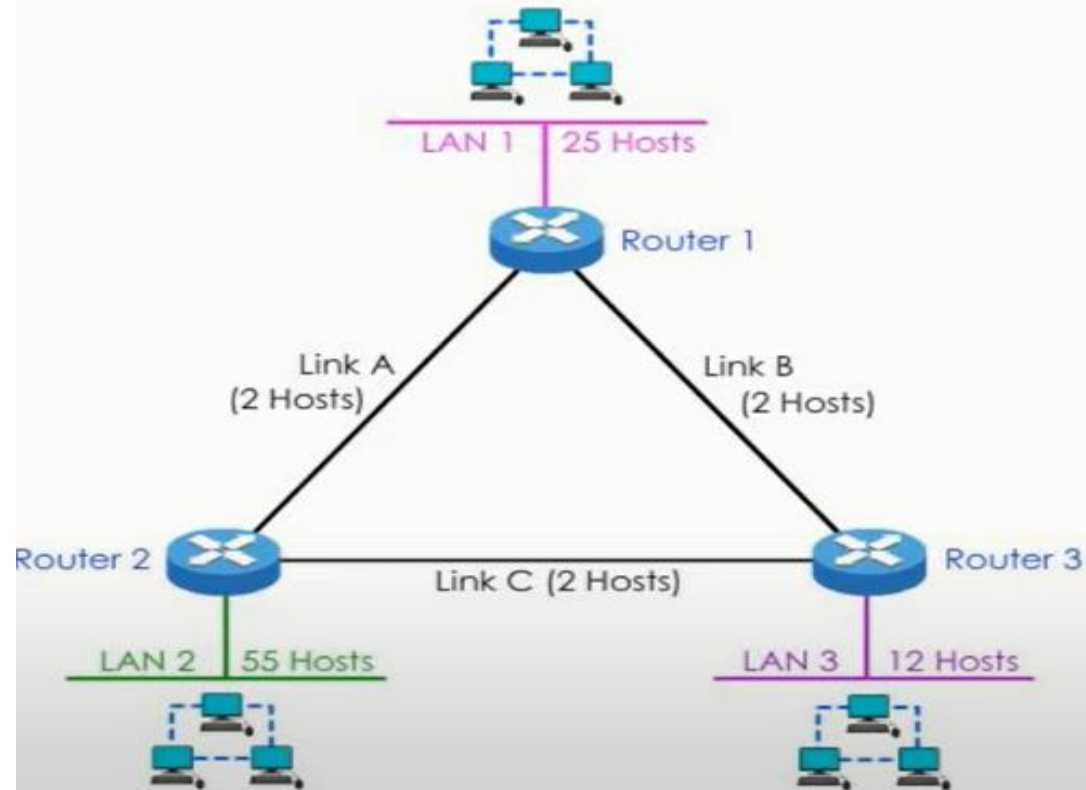
# VLSM Example

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



# VLSM Example

Step 1: Arrange the networks from the largest to the smallest



- 1 LAN 2 - 55 hosts
- 2 LAN 1 - 25 hosts
- 3 LAN 3 - 12 hosts
- 4 Link A , B, C - 2 hosts

# VLSM Example

Step 2: Pick a subnet for the largest network

**LAN 2-55 Hosts**

<b>Subnet</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>Host</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>


Given range: 192.168.4.0/24

<b>Network ID</b>	<b>Subnet Mask</b>	<b>Host</b>	<b>Network</b>
192.168.4.0	/26	64	LAN 2
192.168.4.64	/26	64	Unused
192.168.4.128	/26	64	Unused
192.168.4.192	/26	64	Unused

# VLSM Example

Step 3: Pick the next largest network

**LAN 1-25 Hosts**




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

Network ID	Subnet Mask	Host	Network
192.168.4.0	/26	64	LAN 2
192.168.4.64	/27	32	LAN 1
192.168.4.96	/27	32	Unused
192.168.4.128	/26	64	Unused
192.168.4.192	/26	64	Unused

# VLSM Example

Step 4: Pick the next largest network

**LAN 3-12 Hosts**




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

Network ID	Subnet Mask	Host	Network
192.168.4.0	/26	64	LAN 2
192.168.4.64	/27	32	LAN 1
192.168.4.96	/28	16	LAN 3
192.168.4.112	/28	16	Unused
192.168.4.128	/26	64	Unused
192.168.4.192	/26	64	Unused

# VLSM Example

Step 5: Pick the next largest network

Link A, B, C – 2 Hosts



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

Network ID	Subnet Mask	Host	Network
192.168.4.0	/26	64	LAN 2
192.168.4.64	/27	32	LAN 1
192.168.4.96	/28	16	LAN 3
192.168.4.112	/30	4	Link A
192.168.4.116	/30	4	Link B
192.168.4.120	/30	4	Link C
192.168.4.124	/30	4	Unused
192.168.4.128	/26	64	Unused
192.168.4.192	/26	64	Unused

# Supernetting

- Supernetting is the opposite of Subnetting.
- In subnetting, a single big network is divided into multiple smaller subnetworks.
- In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.
- Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks.
- This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

# Supernetting

- How to Supernet a network?
- Combining these networks into one network: (A summarized route)
  - 192.168.0.0/24
  - 192.168.1.0/24
  - 192.168.2.0/24
  - 192.168.3.0/24

Step 1: Write all the IP Addresses in binary like so:

- 192.168.0.0/24 11000000.10101000.00000000.00000000
- 192.168.1.0/24 11000000.10101000.00000001.00000000
- 192.168.2.0/24 11000000.10101000.00000010.00000000
- 192.168.3.0/24 11000000.10101000.00000011.00000000

# Supernetting

- Step 2: Find matching bits from left to right  
11000000.10101000.00000000.00000000  
11000000.10101000.00000001.00000000  
11000000.10101000.00000010.00000000  
11000000.10101000.00000011.00000000
- Step 3: Re write the matching numbers and add the remaining zeros, because you are converting network bits into host bits.
- This will be your NEW NETWORK ID, the route that you will be advertising.
- (A summarized route) 11000000.10101000.00000000.00000000 = 192.168.0.0



# Supernetting

- Step 4: Find the new subnet mask.
- Put “1s” in the matching networking part, and all zeros in the host part.  
11111111.11111111.11111100.00000000
- This your new subnet mask 255.255.252.0 •
- Your new summarized route is 192.168.0.0/22

# Classless Interdomain Routing(CIDR)

- **CIDR**
- A routing system used by routers and gateways on the backbone of the Internet for routing packets.
- CIDR replaces the old class method of allocating 8, 16, or 24 bits to the network ID, and instead allows any number of contiguous bits in the IP address to be allocated as the network ID.
- For example, if a company needs a few thousand IP addresses for its network, it can allocate 11 or 12 bits of the address for the network ID instead of 8 bits for a class C (which wouldn't work because you would need to use several class C networks) or 16 bits for class B (which is wasteful).

# Classless Interdomain Routing(CIDR)

- **How It Works**
- CIDR assigns a numerical prefix to each IP address.
- For example, a typical destination IP address using CIDR might be 177.67.5.44/13.
- The prefix 13 indicates that the first 13 bits of the IP address identify the network, while the remaining  $32 - 13 = 19$  bits identify the host.
- The prefix helps to identify the Internet destination gateway or group of gateways to which the packet will be forwarded.
- Prefixes vary in size, with longer prefixes indicating more specific destinations.
- Routers use the longest possible prefix in their routing tables when determining how to forward each packet.
- CIDR enables packets to be sent to groups of networks instead of to individual networks, which considerably simplifies the complex routing tables of the Internet's backbone routers.

# Network Address Translation (NAT)

- **Network Address Translation (NAT)**
- The number of home users and small businesses that want to use the Internet is ever increasing.
- An ISP with a block of addresses could dynamically assign an address to this user.
- Earlier, an address was given to a user when needed. But the situation is different now.
- Home users and small businesses need more than one IP addresses since they have several hosts and need an IP address for each host.
- With the shortage of addresses, this is a serious problem.
- A quick solution to this problem is called Network Address Translation.

# Network Address Translation (NAT)

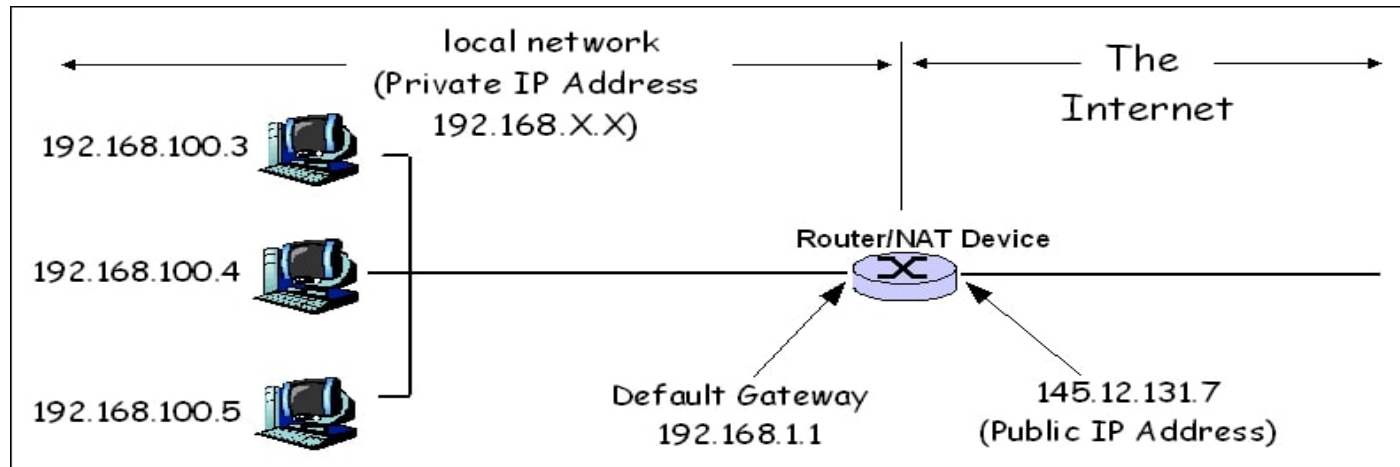
- NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally.
- The traffic inside can use the large set, the traffic outside can use the small set.
- To separate the addresses used inside the home or business and the ones used for the internet, the internet authorities have reserved three sets of addresses as private addresses.

**Table 19.3** *Addresses for private networks*

<i>Range</i>			<i>Total</i>
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	$2^{16}$

# Network Address Translation (NAT)

- Any organization can use an address out of this set without permission from the internet authorities.
- Everyone knows that these reserved addresses are for private networks.
- They are unique inside the organization, but they are not unique globally.

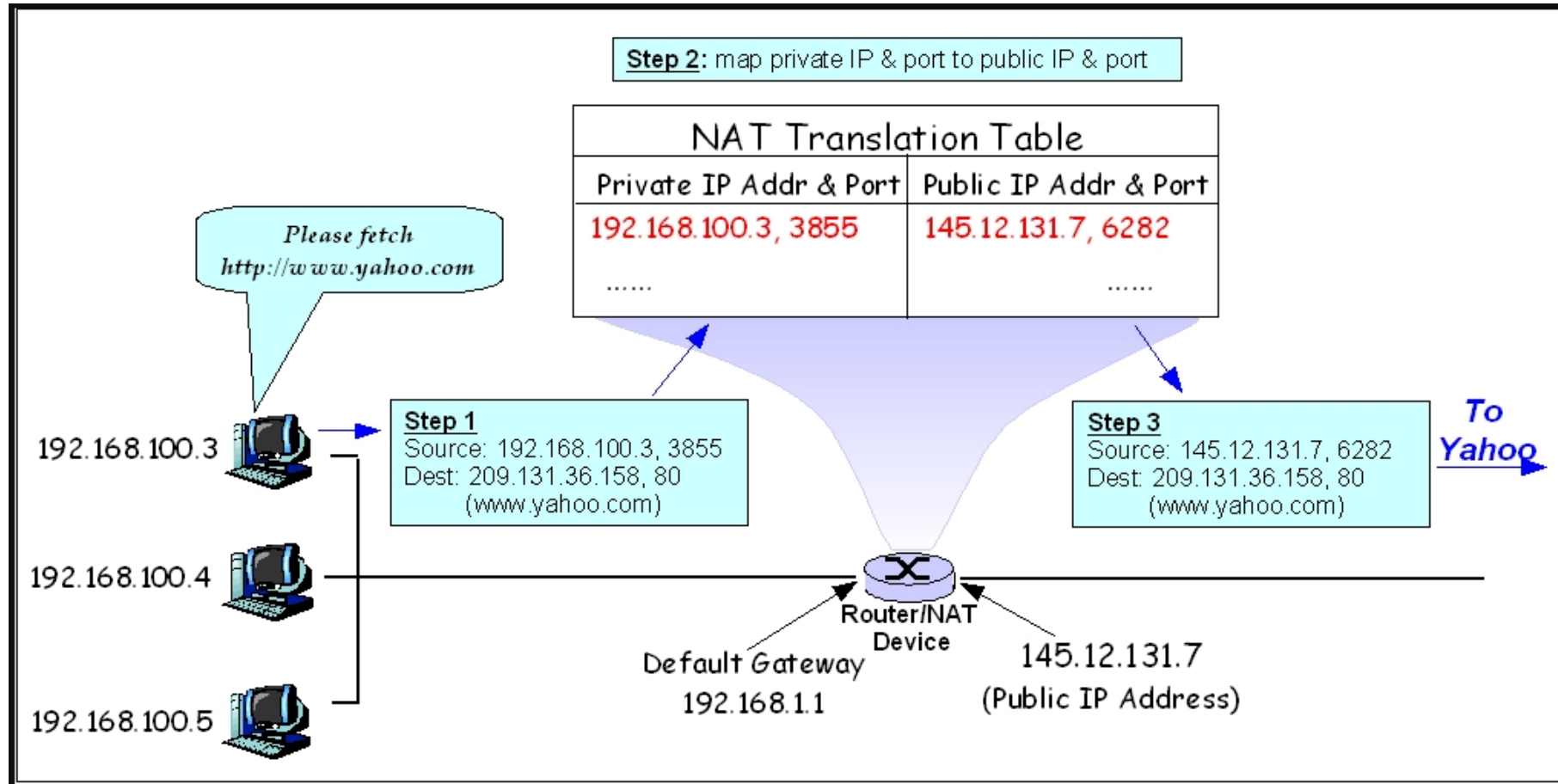


**Fig : NAT implementation**

# Network Address Translation (NAT)

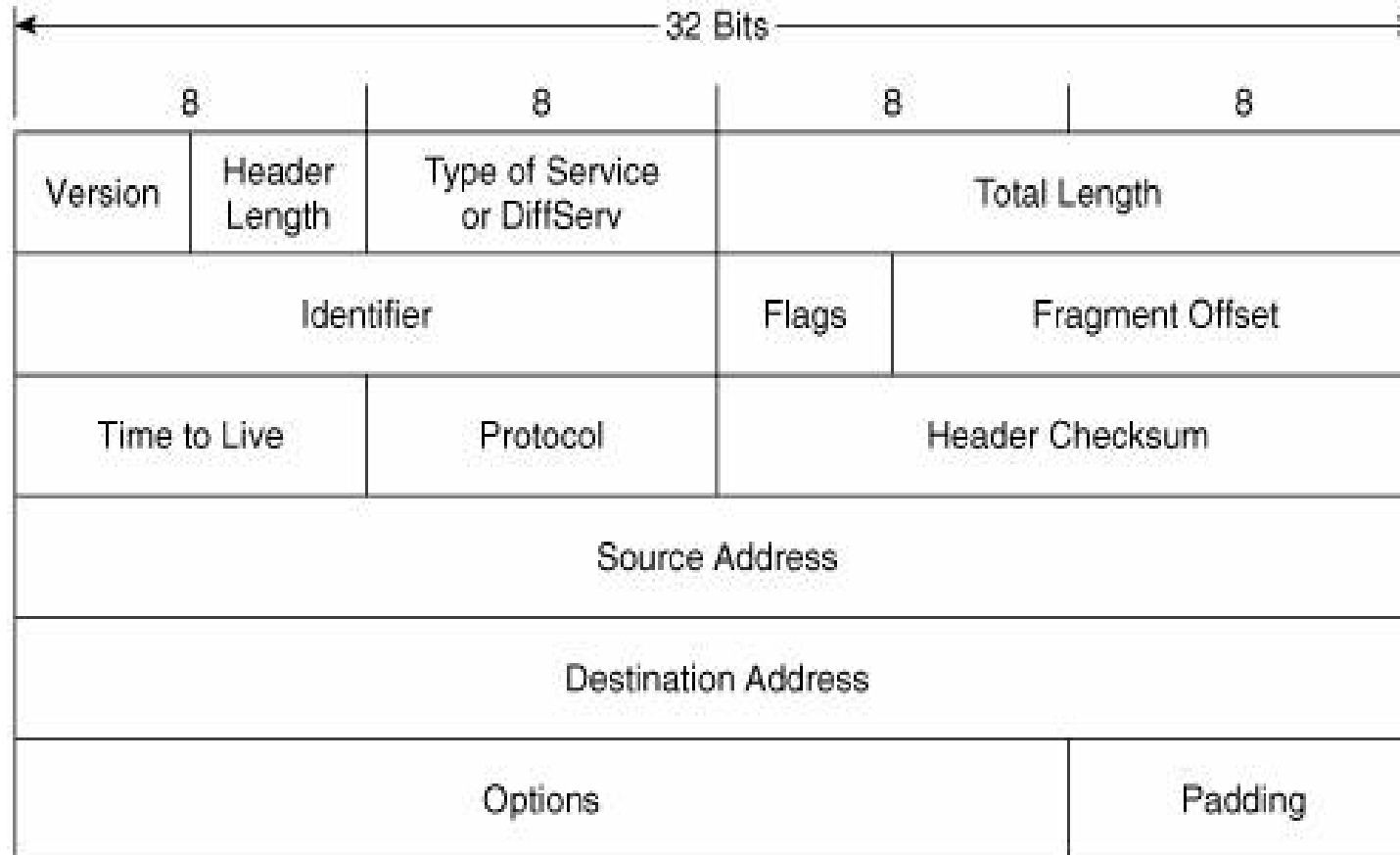
- **Address translation**
- All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address.
- All incoming packets also pass through the NAT router, which replaces the destination address in the packet(the NAT router global address) with appropriate private address.
- Figure shows an example of address translation.

# Network Address Translation (NAT)





# IPv4 Packet Structure



**Fig : IPV4 Packet**

# IPv4 Packet Structure

- Version: Version no. of Internet Protocol used (e.g. IPv4).
- IHL: Internet Header Length; Length of entire IP header.
- Type of service: This provides network service parameters.
- Total Length: Length of entire IP Packet (including IP header and IP Payload).
- Identification: If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.
- Flags: As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not.
- In this 3-bit flag, the MSB is always set to '0'.
- Fragment Offset: This offset tells the exact position of the fragment in the original IP Packet.

.

# IPv4 Packet Structure

- Time to Live: To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross.
- At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded
- Protocol: Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol.
- For example, protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- Header Checksum: This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- Source Address: 32-bit address of the Sender (or source) of the packet.
- Destination Address: 32-bit address of the Receiver (or destination) of the packet.
- Options: This is optional field, which is used if the value of IHL is greater than 5.
- These options may contain values for options such as Security, Record Route, Time Stamp, etc.

# Overview of Internet Control Protocols

- **Internet Control Message Protocol(ICMP)**
- Since IP does not have an inbuilt mechanism for sending error and control messages.
- It depends on Internet Control Message Protocol (ICMP) to provide an error control.
- It is used for reporting errors and management queries.
- It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information. e.g. the requested service is not available or that a host or router could not be reached.
- ICMP messages are divided into two broad categories: error-reporting messages and query messages.

# Overview of Internet Control Protocols

- The error reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- The query messages help a host or a network manager get specific information from a router or another host.
- For example, nodes can discover their neighbors.
- Also, hosts can discover and learn about routers on their network, and routers can help a node redirect its messages.

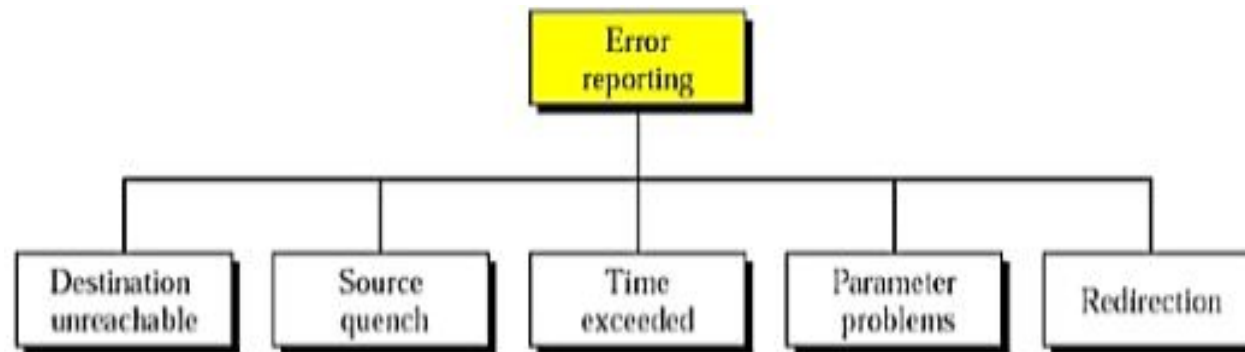


Fig1: Error-reporting messages

# Overview of Internet Control Protocols

- **Destination Unreachable**

- When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination-unreachable message back to the source host that initiated the datagram.

- **Source Quench**

- The source-quench message in ICMP was designed to add a kind of flow control to the IP.
- When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram.

- **Time Exceeded**

- When the time-to-live value reaches 0, after decrementing, the router discards the datagram.
- However, when the datagram is discarded, a time-exceeded message must be sent by the router to the original source.
- Second, a time-exceeded message is also generated when not all fragments that make up a message arrive at the destination host within a certain time limit.

# Overview of Internet Control Protocols

- **Parameter Problem**
  - Any ambiguity in the header part of a datagram can create serious problems as the datagram travels through the Internet.
  - If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source.
- **Redirection**
  - This concept of redirection is shown in Figure 2 in the next slide.
  - Host A wants to send a datagram to host B.
  - Router R2 is obviously the most efficient routing choice, but host A did not choose router R2.
  - The datagram goes to R1 instead.
  - Router R1, after consulting its table, finds that the packet should have gone to R2.
  - It sends the packet to R2 and, at the same time, sends a redirection message to host A.
  - Host A's routing table can now be updated.

# Overview of Internet Control Protocols

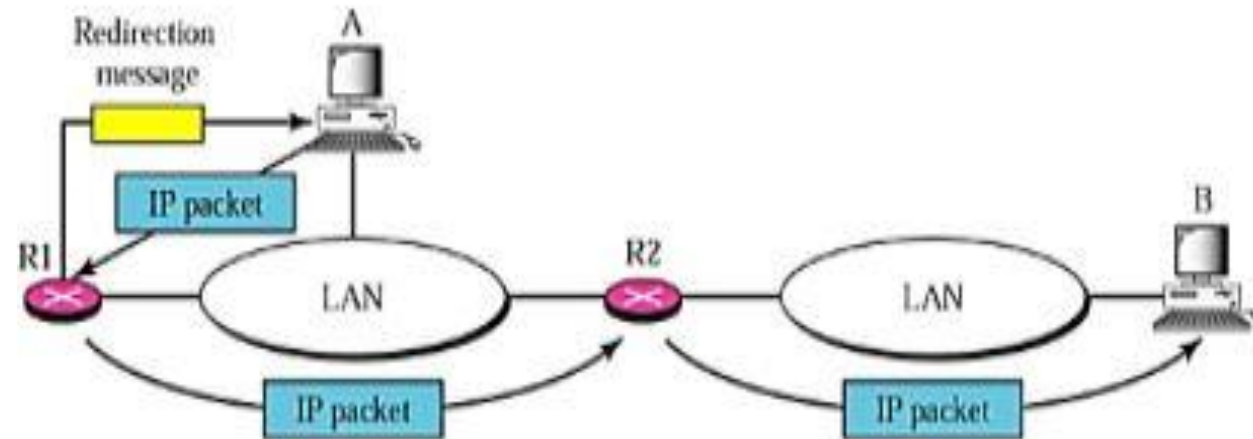


Fig2: Redirection concept



# Overview of Internet Control Protocols

- **Query**
- In addition to error reporting, ICMP can diagnose some network problems.
- This is accomplished through the query messages, a group of four different pairs of messages, as shown in Figure3

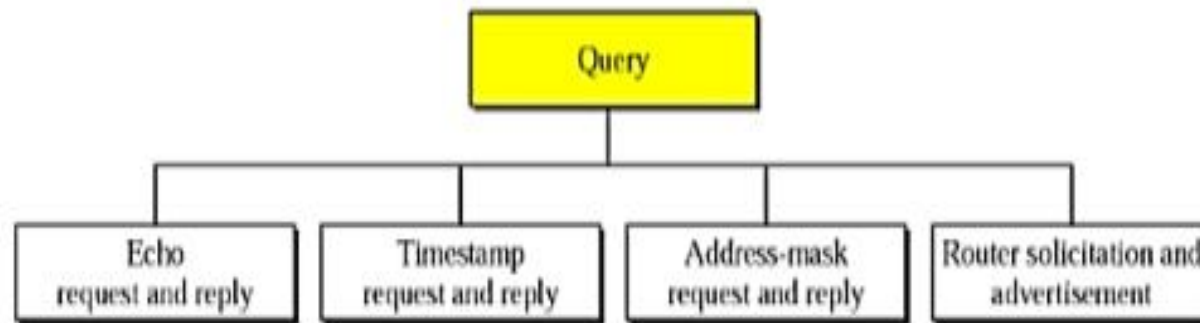


Fig3: Query messages

# Overview of Internet Control Protocols

- **Echo Request and Reply**
- The echo-request and echo-reply messages are designed for diagnostic purposes.
- Network managers and users utilize this pair of messages to identify network problems.
- **Timestamp Request and Reply**
- Two machines (hosts or routers) can use the timestamp request and timestamp reply 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.

# Overview of Internet Control Protocols

- **Address-Mask Request and Reply**
  - If the host knows the address of the router, it sends the request directly to the router.
  - If it does not know, it broadcasts the message.
  - The router receiving the address-mask-request message responds with an address-mask-reply message, providing the necessary mask for the host.
- **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.
  - The router-solicitation and router-advertisement messages can help in this situation.
- **Checksum**
  - In ICMP the checksum is calculated over the entire message (header and data).

# Overview of Internet Control Protocols

- **Internet Group Management Protocol (IGMP)**
- The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers.
- Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content.
- It is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships.
- IGMP is an integral part of IP multicast.
- IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

# Overview of Internet Control Protocols

- **Working of IGMP**
- The multicast router of the network has a list of multicast address for which the network is having any member.
- There is one multicast router for each group that distributes multicast packet to members of that group.
- It means the network will have two multicast routers, if there are two multicast groups.
- A host or a multicast router can be a member of the group.
- When a host is having membership, it means that any process running on that host is a member of the group and when a router is having membership of group, it means one of the networks connected to the router is having membership of the group.

# Overview of Internet Control Protocols

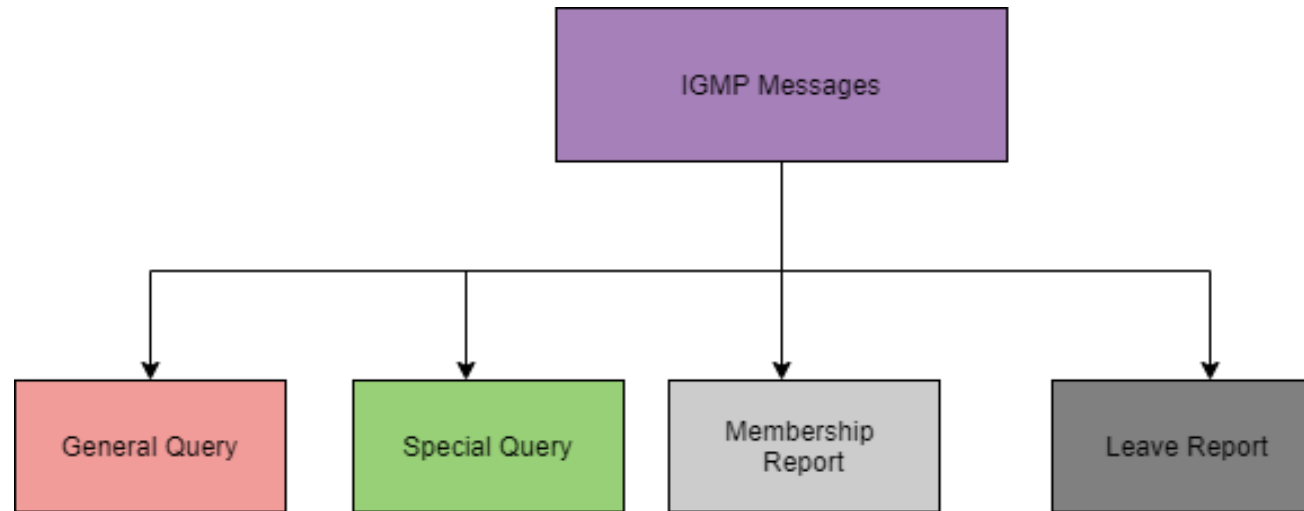
- **Joining a Group**

- Both the host and a router can join a group.
- When a process on the host wants to join a group, it sends the request to the host.
- The host adds the name of the process and group name to its list.
- If this is the first entry for that particular group, the host sends membership report message to the multicast router of the group.
- If it is not the first entry for the requested group there is no need of sending such a message.

- **Leaving a Group**

- Whenever a host sees no process interested in a group, it sends a leave report message.
- The membership is not purged by the multicast router of the group, rather it immediately transmits query packets repeatedly to see if anyone still interested.
- If the response comes in the form of membership report message, the membership of the host or network is preserved.

# Overview of Internet Control Protocols



**Fig : IGMP message types**

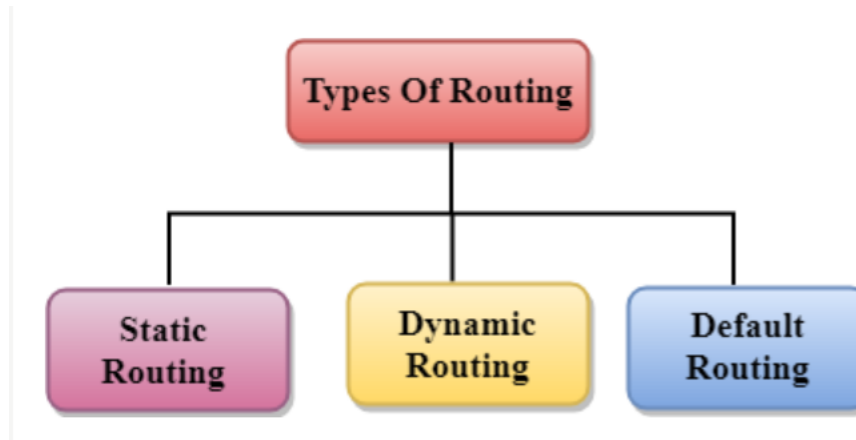
# Routing Protocols

- **Overview of OSPF (Open Path Shortest First):**
- Open Shortest Path First (OSPF) is a link state routing protocol (LSRP) that uses the Shortest Path First (SPF) network communication algorithm (Dijkstra's algorithm) to calculate the shortest connection path between known devices.
- Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information.
- OSPF sends only the part that has changed and only when a change has taken place.
- When routes change -- sometimes due to equipment failure -- the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time.



# Routing

- Routing is a process that is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.
- There are three different types of Routing. They are:



# Routing

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

# Routing

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

# Routing

- **Routing Protocol**

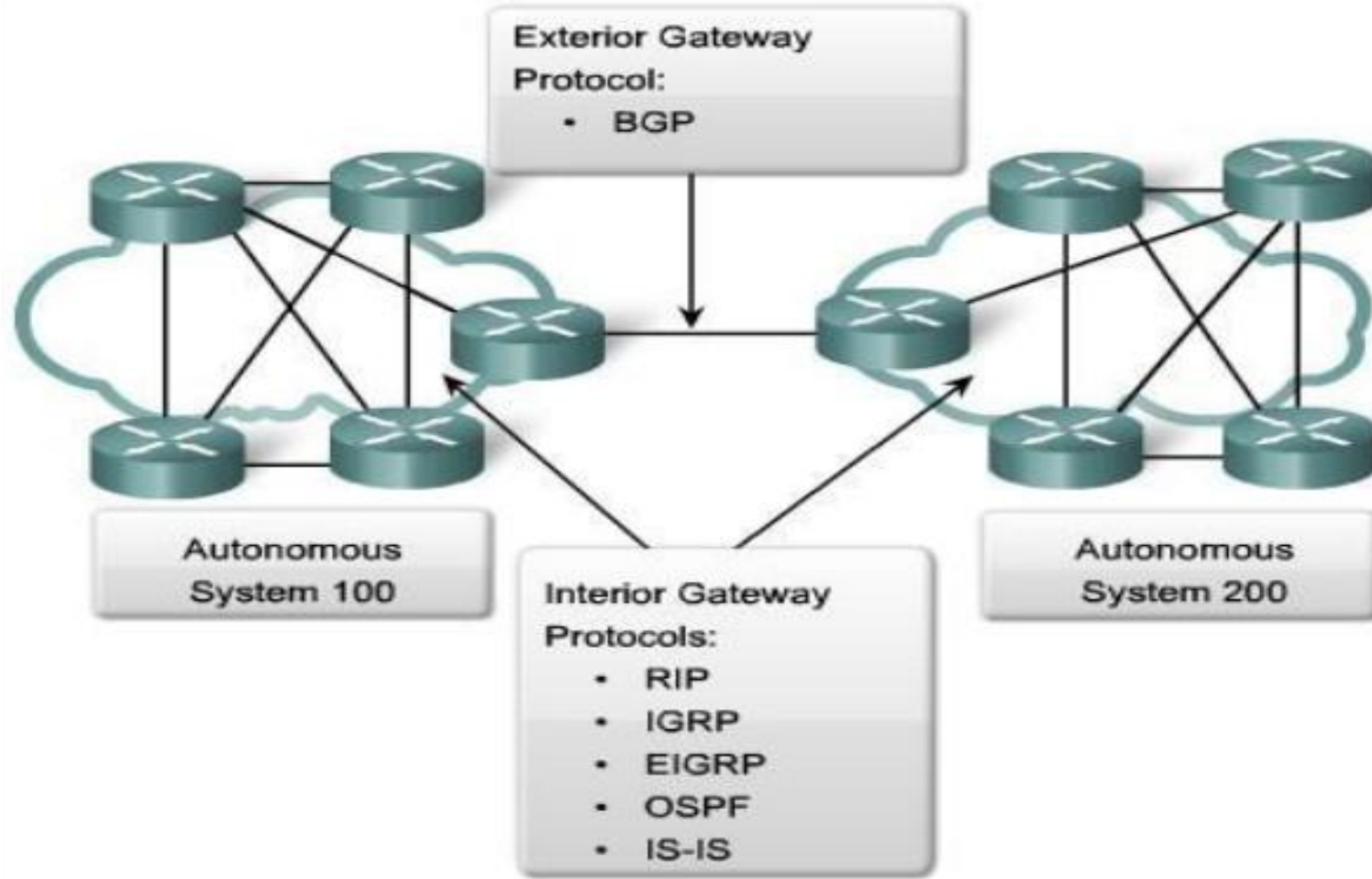
- A routing protocol is the communication used between routers.
- A routing protocol allows routers to share information about networks and their proximity to each other.
- Routers use this information to build and maintain routing tables.

- **Autonomous System**

- An AS is a collection of networks under a common administration that share a common routing strategy.
- To the outside world, an AS is viewed as a single entity.
- The AS may be run by one or more operators while it presents a consistent view of routing to the external world.
- The American Registry of Internet Numbers (ARIN), a service provider, or an administrator assigns a 16-bit identification number to each AS.



## IGP vs. EGP Routing Protocols



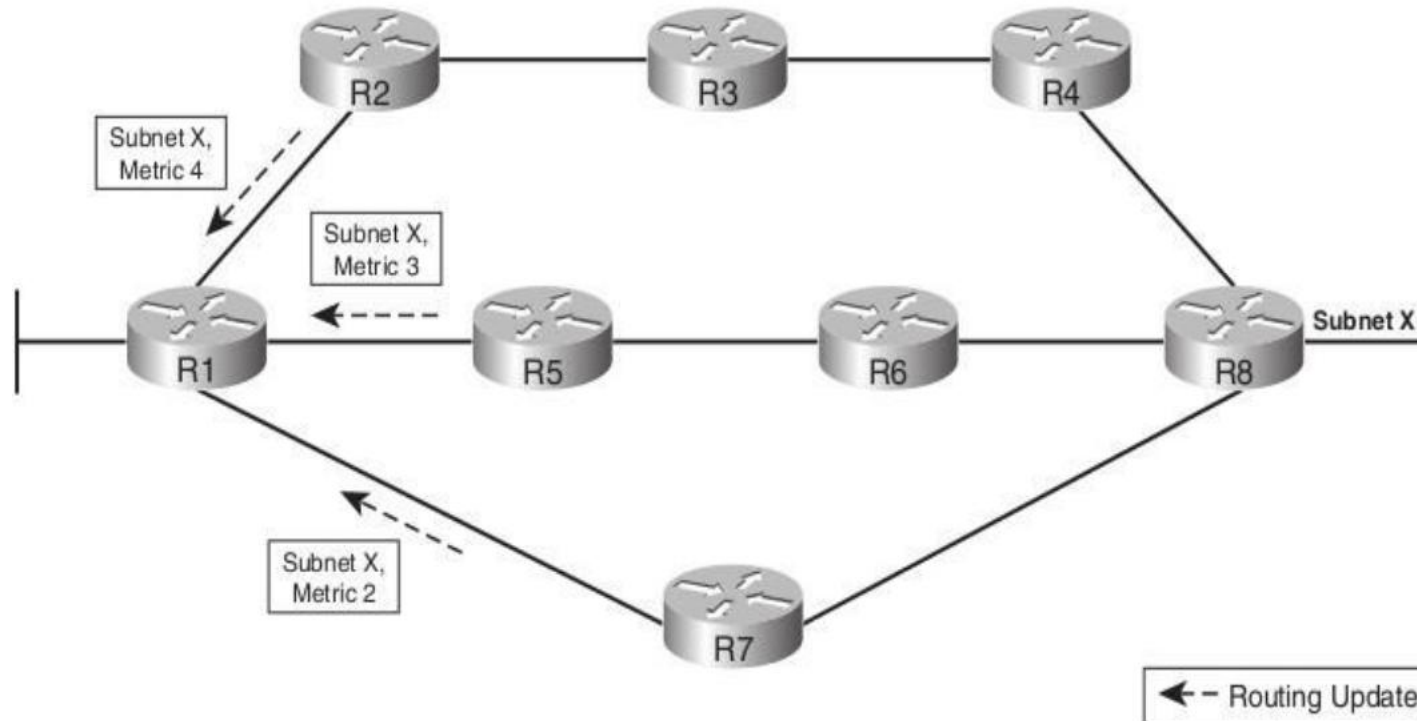
# Routing

- **Dynamic Routing Protocol:**
  - 1. Interior Gateway protocol (IGP)
    - I). Distance Vector Protocol
    - II). Link State Protocol
  - 2. Exterior Gateway Protocol (EGP)
- **Interior gateway protocol (IGP):** Within one Autonomous System.
- **Exterior Routing Protocol(EGP):** Between the Autonomous System. Example BGP (Boarder gateway protocol)

# Distance Vector Routing Algorithm

- As the name implies, distance vector means that routes are advertised as vectors of distance and direction.
- Distance is defined in terms of a metric such as hop count and direction is simply the next hop router or exit interface.
- A router using a distance vector routing protocol does not have the knowledge of the entire path to a destination network. Instead the router knows only:
- The direction or interface in which packets should be forwarded and the distance or how far it is to the destination network.

# Distance Vector Routing Algorithm





# Distance Vector Routing Algorithm

- The figure shows an internetwork in which router R1 learns about three routes to reach the subnet X:
- The four hop route through R2
- The three hop route through R3
- The two hop route through R7
- R1 learns about the subnet, and a metric associated with that subnet, and nothing more.
- R1 must then pick the best route to reach subnet X.
- In this case, it picks the two-hop route through R7, because that route has the lowest metric.

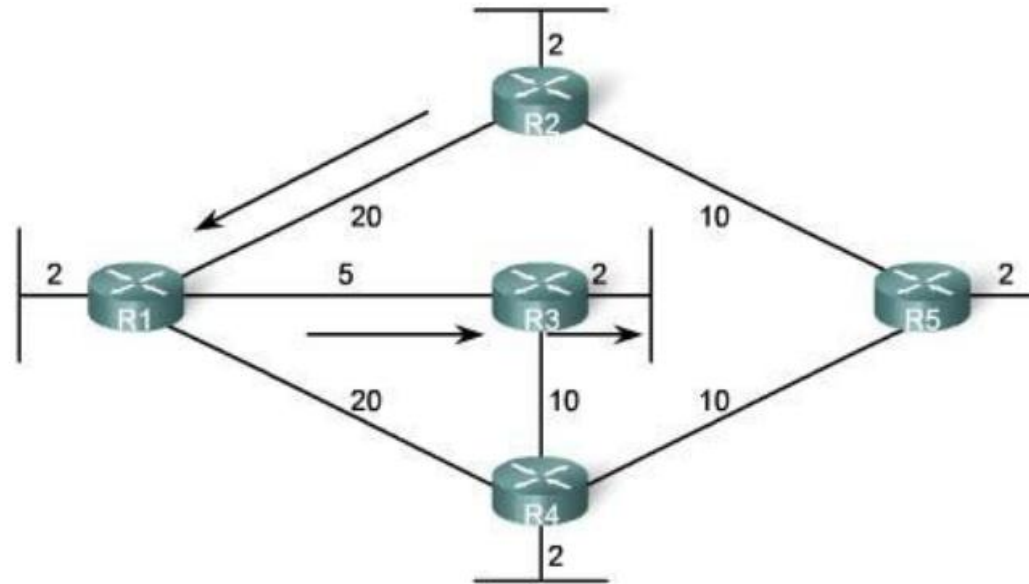
# Link State Routing Algorithm

- Also known as Shortest Path Routing Algorithm or Open Shortest Path First(OSPF)
- **Link states:**
- Information about the state of (Router interfaces) links is known as link-states. As you can see in the figure, this information includes:
- The interface's IP address and subnet mask.
- The type of network, such as Ethernet (broadcast) or Serial point-to-point link.
- The cost of that link.
- Any neighbor routers on that link.



# Routing Protocols

- OSPF bases its path choices on "link states" that take into account additional network information, including assigned cost metrics that give some paths higher assigned costs.
- For example, a person in city A wants to travel to city M and is given two options:
- Travel via cities B and C. The route would be ABCM. And the distance (or bandwidth cost in the networking case) for A-B is 10 miles, B-C is 5 miles and C-M is 10 miles.
- Travel via city F. The route would be AFM. And the distance for A-F is 20 miles and F-M is 10 miles.
- The shortest route is always the one with least amount of distance covered in total.
- Thus, the ABCM route is the better option ( $10+5+10=25$ ), even though the person has to travel to two cities as the associated total cost to travel to the destination is less than the second option with a single city ( $20+10=30$ ).
- OSPF performs a similar algorithm by first calculating the shortest path between the source and destination based on link bandwidth cost and then allows the network to send and receive IP packets via the shortest route.

# Link State Routing Algorithm



Shortest Path for host on R2 LAN to reach host on R3 LAN:  
 $R2 \text{ to } R1 (20) + R1 \text{ to } R3 (5) + R3 \text{ to LAN } (2) = 27$

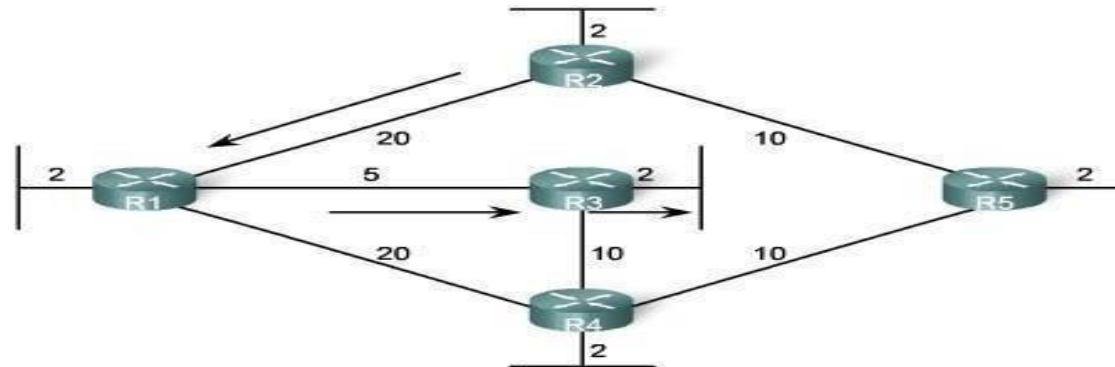
 <b>Distance Vector</b>	 <b>Link State</b>
RIP, RIPv2, IGRP, EIGRP	OSPF, ISIS
Routers communicate with <u>neighbor</u> routers advertising networks as measures of distance and vector	Routers communicate with <u>all</u> other routers exchanging link-state information to build a topology of the entire network
Distance = Metric Vector = Direction (Interface)	Link-state = interface connections or "links" to other routers and networks
Best for: <ul style="list-style-type: none"> <li>- simple, flat design, non-hierarchical networks</li> <li>- minimum administrator knowledge</li> <li>- convergence time is not an issue</li> </ul>	Best for: <ul style="list-style-type: none"> <li>- large, hierarchical networks</li> <li>- advanced administrator knowledge</li> <li>- convergence time is crucial</li> </ul>
Knowledge of the network from directly connected neighbors I	Routers have a complete view of the network, knowledge of the entire topology
Send periodic updates of entire routing table	Send triggered partial updates

# Routing Protocols

- **Border Gateway Protocol (BGP):**
- Border gateway protocol (BGP) is an interdomain routing protocol using path vector routing.
- BGP is protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers.
- BGP directs packets between autonomous systems (AS) -- networks managed by a single enterprise or service provider.
- Traffic that is routed within a single network AS is referred to as internal BGP, or iBGP.
- More often, BGP is used to connect one AS to other autonomous systems, and it is then referred to as an external BGP, or eBGP.

# Routing Protocols

- **OSPF Network Topology**
- Two routers communicating OSPF to each other exchange information about the routes they know about and the cost for them to get there.
- When many OSPF routers are part of the same network, information about all of the routes in a network are learned by all of the OSPF routers within that network technically called an area.
- Each OSPF router passes along information about the routes and costs they've heard about to all of their adjacent OSPF routers, called neighbors.



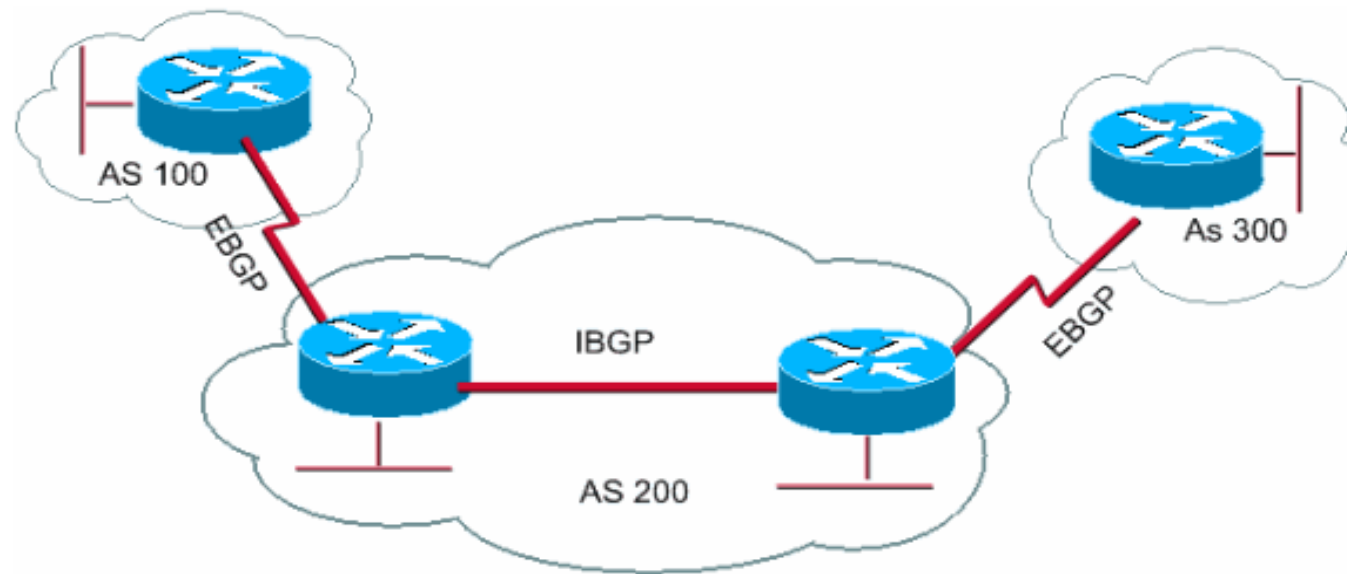
Shortest Path for host on R2 LAN to reach host on R3 LAN:  
 $R2 \text{ to } R1 (20) + R1 \text{ to } R3 (5) + R3 \text{ to LAN } (2) = 27$

# Routing Protocols

- **Border Gateway Protocol (BGP):**
- Border gateway protocol (BGP) is an interdomain routing protocol using path vector routing.
- BGP is protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers.
- BGP directs packets between autonomous systems (AS) -- networks managed by a single enterprise or service provider.
- Traffic that is routed within a single network AS is referred to as internal BGP, or iBGP.
- More often, BGP is used to connect one AS to other autonomous systems, and it is then referred to as an external BGP, or eBGP.



# Routing Protocols



**Fig :eBGP and iBGP sessions**

# Routing Protocols

- All other routing protocols are concerned solely with finding the optimal path towards all known destinations.
- BGP cannot take this simplistic approach because the peering agreements between ISPs almost always result in complex routing policies.
- To help network operators implement these policies, BGP carries a large number of attributes with each IP prefix:
- **Local Preference** – The local preference attribute is used to dictate how traffic prefers to leave a specific BGP ASN. This attribute is passed between neighbors within the same ASN.
- The highest local preference gets priority.
- **Local Routes** – Routes which have been sourced from the local router will be preferred over those sourced from other routers.

# Routing Protocols

- **Shortest AS\_PATH** – With BGP, the path is notated by the ASN of the external BGP networks that must be traversed to reach the destination network; e.g. 10 20 30 means that the traffic must pass through ASNs 10, 20, and 30 to reach the destination.
- If multiple options exist to a specific network, the one with the shortest AS path will be preferred.
- **Origin** – With origin, BGP is looking for the source of the initial network advertisement, for example if it was redistributed from an IGP, an EGP or through an unknown source.
- When analyzing this attribute, routes that have originated from an IGP are preferred to those from an EGP.
- **BGP Neighbor Type** – There are two different types of BGP neighborship: internal and external.
- A BGP neighborship that exists within the same ASN between two devices is considered internal, and a BGP neighborship that exists between devices from different ASNs is considered external. External (or eBGP) routes are preferred to Internal (iBGP) routes.
- **Lowest Router-ID** – The route with the lowest BGP router ID will be preferred
- **Lowest Neighbor Address** – The route coming through a neighbor with the lowest address will be preferred.

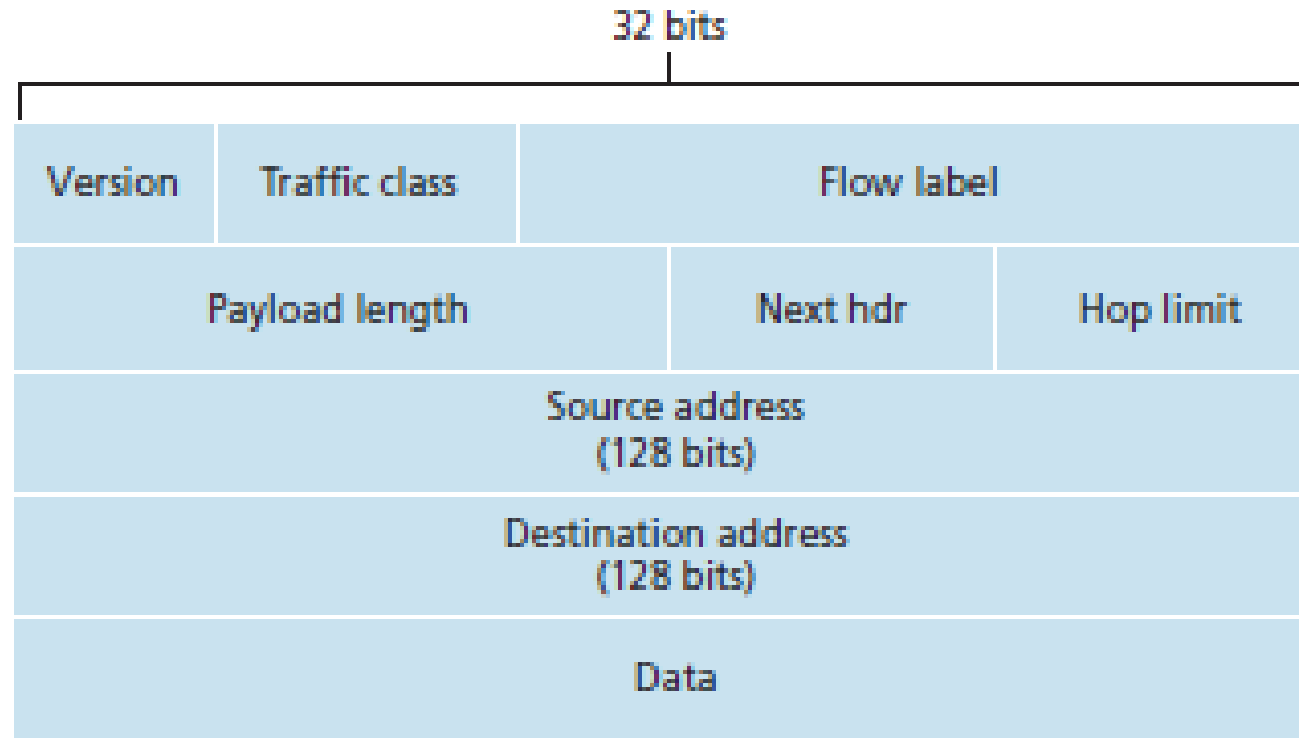
# IPv6

- **Overview of IPv6:**
- To respond to the need for a large IP address space, a new IP protocol, IPv6, was developed. Also, major issues of IPv4 are addressed in this version.
- The most important changes introduced in IPv6 are evident in the datagram format:
- **IPv6 Addresses :( IPv6 Format)**
- IPv6 address is 128 bits long and is arranged in eight groups, each of which is 16 bits
- Each group is expressed as four hexadecimal digits and the groups are separated by colons.
- An example of a full IPv6 address: FE80:CD00:0000:0CDE:1257:0000:211E:729C
- **Expanded addressing capabilities**
- IPv6 increases the size of the IP address from 32 to 128 bits.
- This ensures that the world won't run out of IP addresses.
- Now, every grain of sand on the planet can be IP-addressable.
- In addition to unicast and multicast addresses, IPv6 has introduced a new type of address, called an any-cast address, which allows a datagram to be delivered to any one of a group of hosts.

# IPv6

- **A streamlined 40-byte header**
- As discussed below, a number of IPv4 fields have been dropped or made optional.
- The resulting 40-byte fixed-length header allows for faster processing of the IP datagram.
- A new encoding of options allows for more flexible options processing.
- **Flow labeling and priority**
- IPv6 has an elusive definition of a flow.
- This allows “labeling of packets belonging to particular flows for which the sender requests special handling, such as a non-default quality of service or real-time service.”
- For example, audio and video transmission might likely be treated as a flow.

# IPV6



**Fig: IPV6 header format**

# IPV6

S.N.	Field & Description
1	Version (4-bits): It represents the version of Internet Protocol, i.e. 0110
2	Traffic Class (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router know what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	Flow Label (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information.
4	Payload Length (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data.

---

# IPv6

5	Next Header (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present, then it indicates the Upper Layer PDU.
6	Hop Limit (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0, the packet is discarded.
7	Source Address (128-bits): This field indicates the address of originator of the packet.
8	Destination Address (128-bits): This field provides the address of intended recipient of the packet.



# IPv6 vs IPv4

IPv4	IPv6
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals.
IPSec support is only optional.	Inbuilt IPSec support.
Fragmentation is done by sender and forwarding routers.	Fragmentation is done only by sender.
No packet flow identification	Packet flow identification is available within the IPv6 header using the Flow Label field.