MODULE 4

Module - 4 (Network Layer in the Internet) IP protocol, IP addresses, Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Bootstrap Protocol (BOOTP), Dynamic Host Configuration Protocol (DHCP). Open Shortest Path First (OSPF) Protocol, Border Gateway Protocol (BGP), Internet multicasting, IPv6, ICMPv6.

NETWORK LAYER

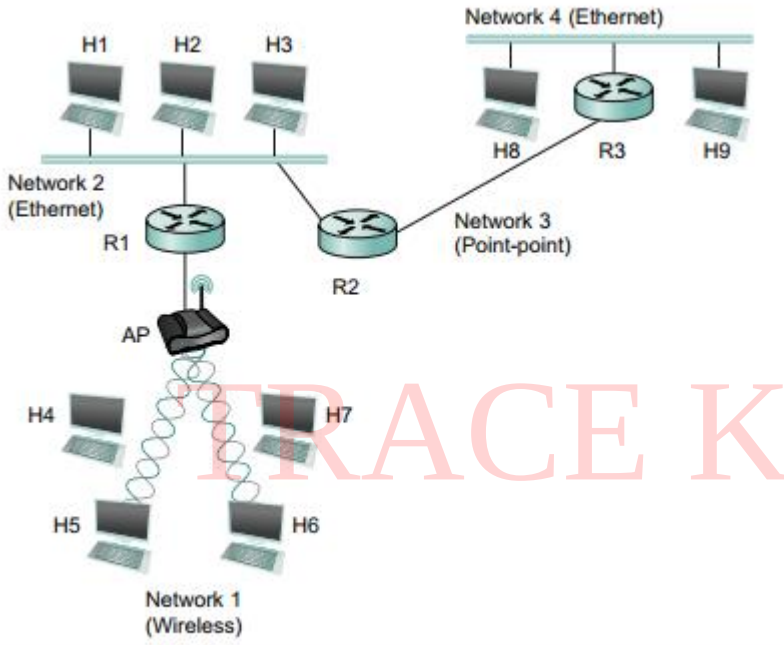
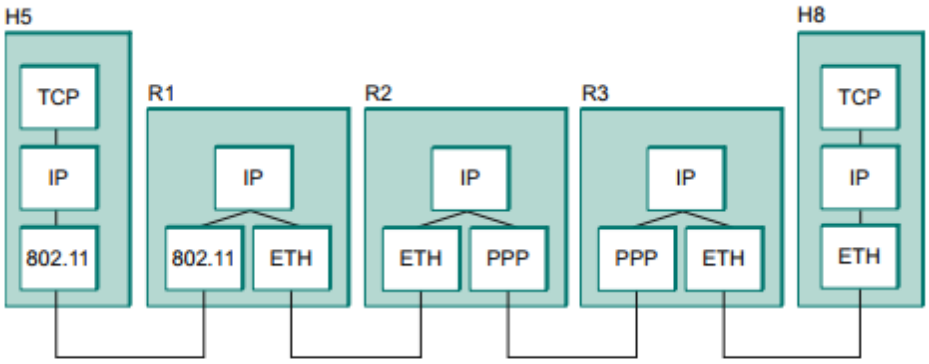


FIGURE 3.14 A simple internetwork. H*n* = host; R*n* = router.

- An internetwork is often referred to as a "network of networks" because it is made up of lots of smaller networks. In this figure, we see Ethernets, a wireless network, and a point-to-point link.
- Each of these is a single-technology network. The nodes that interconnect the networks are called routers. They are also sometimes called gateways, but since this term has several other connotations, we restrict our usage to router.
- The Internet Protocol is the key tool used today to build scalable, heterogeneous internetworks.
- IP is that it runs on all the nodes (both hosts and routers) in a collection of networks and defines the infrastructure that allows these nodes and networks to function as a single

logical internetwork.



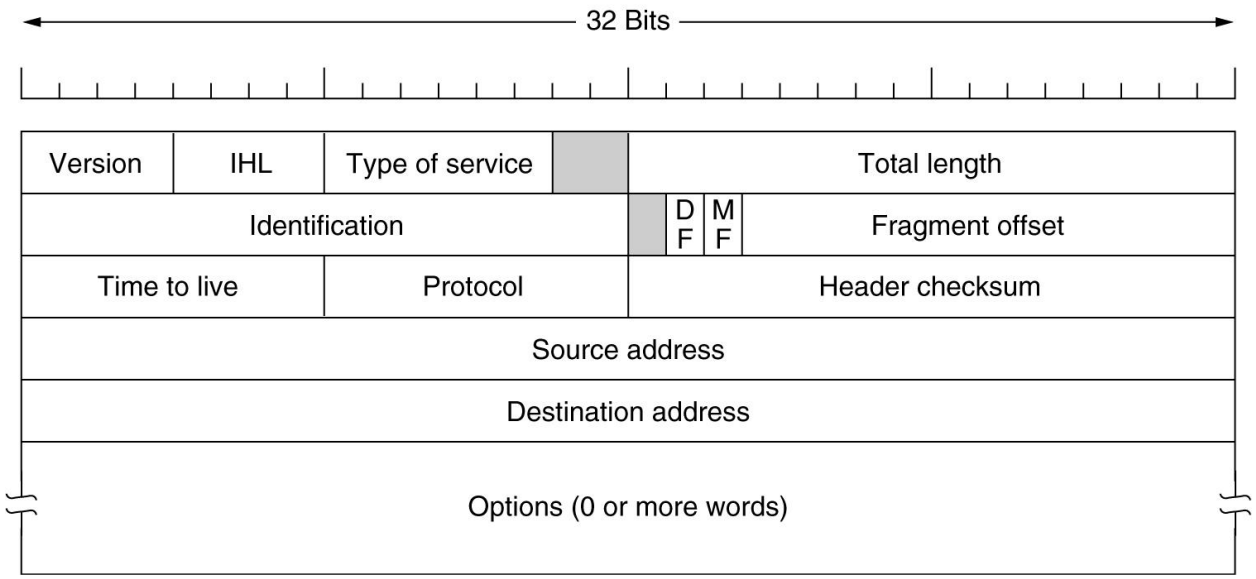
■ FIGURE 3.15 A simple internetwork, showing the protocol layers used to connect H5 to H8 in Figure 3.14. ETH is the protocol that runs over the Ethernet.

- At the network layer, the Internet can be viewed as a collection of **sub networks** or **Autonomous Systems** (ASes) that are interconnected.
- There is no real structure, but several major **backbones** exist.
- These are **constructed** from high-bandwidth lines and fast routers.
- Attached to the **backbones** are regional (midlevel) networks
- The glue that holds **the whole Internet** together is the network layer protocol, **IP (Internet Protocol).**
- The **job** of the network layer is to provide a best-efforts way to transport datagram from source to destination
- The Internet is an interconnected collection of many networks

The IP Protocol

- **Unreliable and connection less protocol**
- **IP transmit the data in form of datagrams**

Ipv4 header format



The IPv4 (Internet Protocol) header

IP datagram consists of a header part and a payload part
- header has a 20-byte fixed part and a variable length optional part
- It is transmitted in big-endian order: from left to right, with the high-order bit of the Version field going first.
- The SPARC is big endian; the Pentium is little-endian.
- On little endian machines, software conversion is required on both transmission and reception

Version field
- keeps track of which version of the protocol the datagram belongs to.
- Currently a transition between IPv4 and IPv6 is going on,IPv5 was an experimental real-time stream protocol that was never widely used.

IHL field(IP header length)
- Since the header length is not constant, IHL is provided to tell how long the header is, in 32-bit words.
- The minimum value is 5, which applies when no options are present.
- The maximum value of this 4-bit field is 15, which limits the header to 60 bytes, and thus the Options field to 40 bytes.

Type of service field.
- to distinguish between different classes of service
- Various combinations of reliability and speed are possible.

- For digitized voice, fast delivery beats accurate delivery.
- For file transfer, error-free transmission is more important than fast transmission.
- 6-bit field contained a three-bit Precedence field and three flags, D, T, and R.
- The Precedence field was a priority from 0 (normal) to 7(network control packet)
- The three flag bits allowed the host to specify from the set{Delay, Throughput, Reliability}
- Current routers often ignore the Type of service field

Total length field

- Includes everything in the datagram—both header and data.
- The maximum length is 65,535 bytes.

Identification field

- needed to allow the destination host to determine which datagram a newly arrived fragment belongs to.
- All the fragments of a datagram contain the same Identification value.

two 1-bit fields: DF & MF

- DF stands for Don't Fragment.
- It is an order to the routers not to fragment the datagram because the destination is incapable of putting the pieces back together again.
- the datagram must avoid a small-packet network on the best path and take a suboptimal route.
- MF stands for More Fragments.
- All fragments except the last one have this bit set.

It is needed to know when all fragments of a datagram have arrived

Fragment offset field:

- tells where in the current datagram this fragment belongs.
- All fragments except the last one in a datagram must be a multiple of 8 bytes, the elementary fragment unit.
- Since 13 bits are provided, there is a maximum of 8192 fragments per datagram

Time to live field

- counter used to limit packet lifetimes.
- It is supposed to count time in seconds, allowing a maximum lifetime of 255 sec.
- It must be decremented on each hop
- It is supposed to be decremented multiple times when queued for a long time in a router.

▪In practice, it just counts hops.When it hits zero, the packet is discarded and a warning packet is sent back to the source host.
▪ This feature prevents datagrams from wandering around forever

Protocol field
▪ tells it which transport process to give it to.
▪ Possibilities are TCP, UDP and some others.
▪ The numbering of protocols is global across the entire Internet.

Header checksum field
▪ verifies the header only.
▪ Such a checksum is useful for detecting errors generated by bad memory words inside a router.
▪ The algorithm is to add up all the 16-bit half words as they arrive,using one's complement arithmetic and then take the one's complement of the result. This algorithm is more robust than using a normal add.
▪ Note that the Header checksum must be recomputed at each hop because at least one field (the Time to live field) always changes

Source address and Destination address
▪ indicate the network number and host number.
▪ Discussed in detail in IP addressing

Options field
▪ was designed to provide an escape to allow subsequent versions of the protocol
▪ to include information not present in the original design,
▪ to permit experimenters to try out new ideas, and
▪ to avoid allocating header bits to information that is rarely needed.
▪ The options are variable length.Each begins with a 1-byte code identifying the option.
▪ Some options are followed by a 1-byte option length field,and then one or more data bytes.
▪ The Options field is padded out to a multiple of four bytes.
▪ Originally, five options were defined

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Fig: Some of the IP options

Security option tells how secret the information is.In theory, a military router might use this field to specify not to route through certain countries the military considers to be "bad guys."In practice, all routers ignore it

Strict source routing option

- gives the complete path from source to destination as a sequence of IP addresses.
- The datagram is required to follow that exact route.
- It is most useful for system managers to send emergency packets when the routing tables are corrupted, or for making timing measurements.

Loose source routing option

- requires the packet to traverse the list of routers specified, and in the order specified,but it is allowed to pass through other routers on the way.
- Normally, this option would only provide a few routers, to force a particular path.
- For example, to force a packet to go west instead of east.This option is most useful when political or economic considerations dictate passing through or avoiding certain countries.

IP Addresses

- There are two types of address:

1. **Physical Address** (MAC address): The length is 48bits
2. **Logical address** (IP address): IPV4 (32bits), IPV6(128bits)

- An IP address is a unique global address for a network interface
- An IP address:
  - is a **32 bit long** identifier
  - encodes a network number (**network prefix**) and **host number**

- Every host and router on the Internet has an IP address,which encodes its network number and host number.

- The combination is unique: no two machines on the Internet have the same IP address.
- All IP addresses are 32 bits long & are used in the Source address and Destination address fields of IP packets.
- It is important to note that an IP address does not actually refer to a host.
- It really refers to a network interface, so if a host is on two networks, it must have two IP addresses.
- However, in practice, most hosts are on one network and thus have one IP address.

For several decades, IP addresses were divided into the five categories. This allocation was called **classful addressing.**

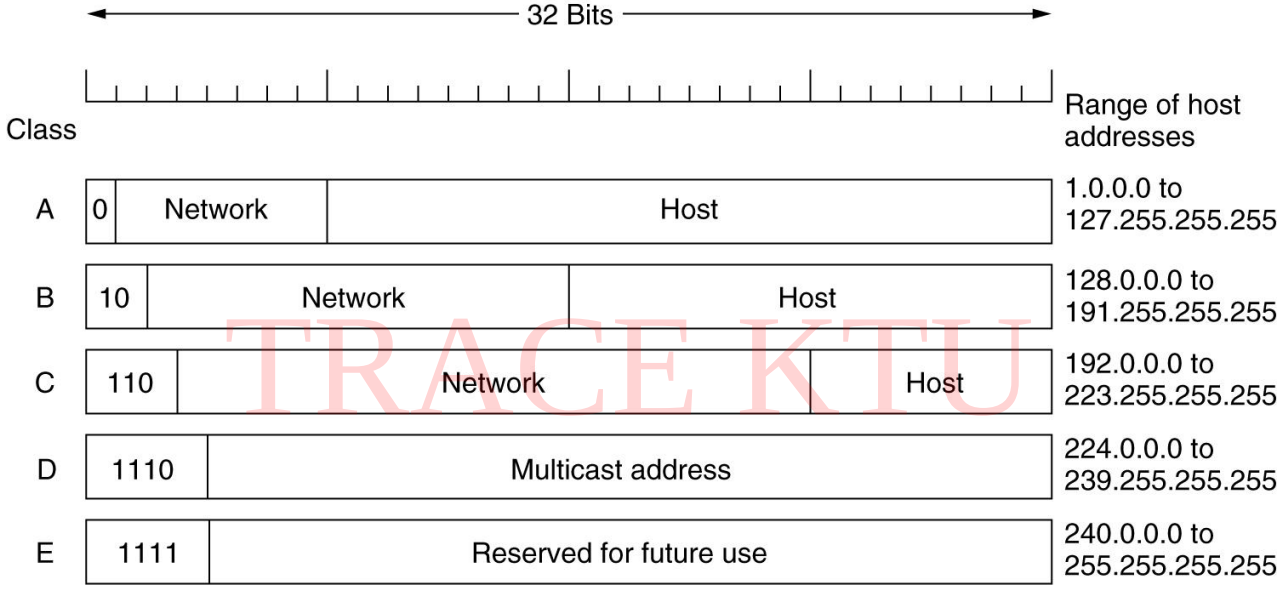
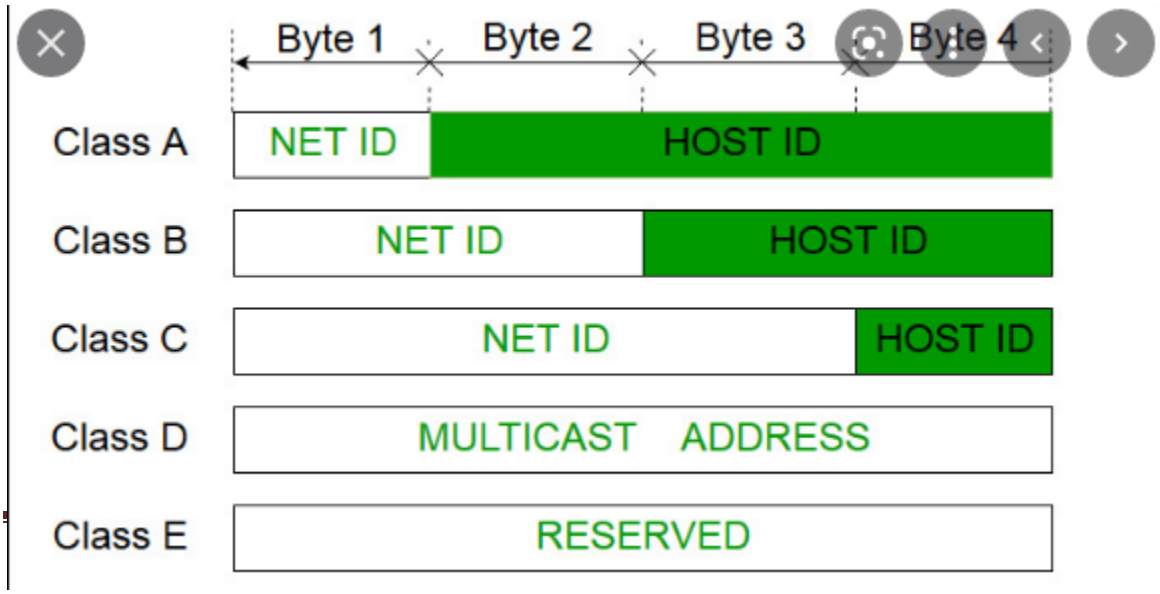


Fig:IP address formats



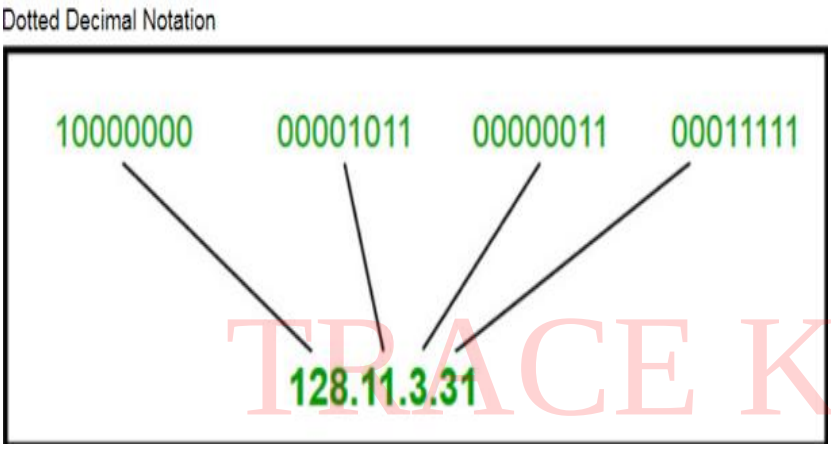
Network numbers are managed by a nonprofit corporation called **ICANN (Internet Corporation for Assigned Names and Numbers)** to avoid conflicts

- Network addresses, which are 32-bit numbers, are usually written in **dotted decimal notation.**
- In this format, each of the 4 bytes is written in decimal, from 0 to 255.

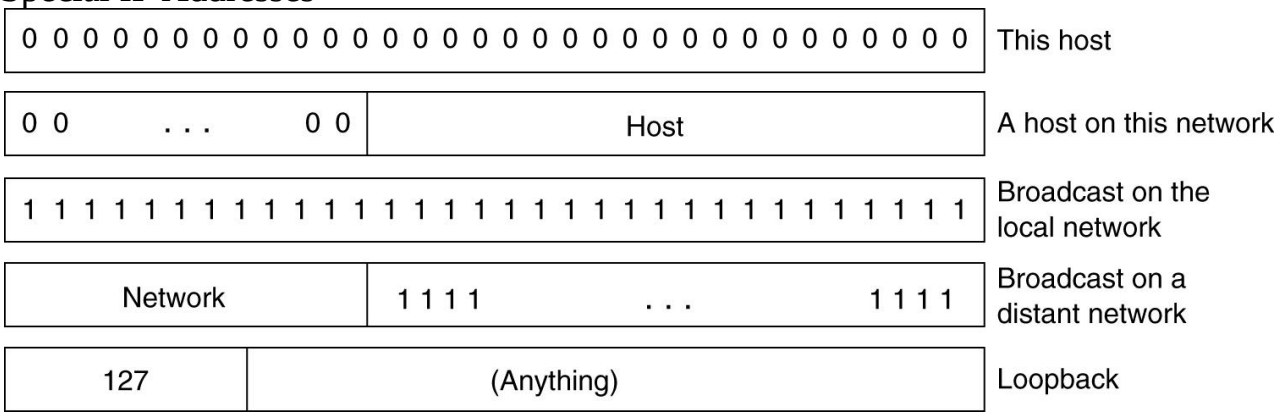
The lowest IP address is 0.0.0.0 and the highest is 255.255.255.255.

- The values 0 and -1 (all 1s) have special meanings
- value 0 means this network or this host.
- value of -1 is used as a broadcast address to mean all

hosts on the indicated network



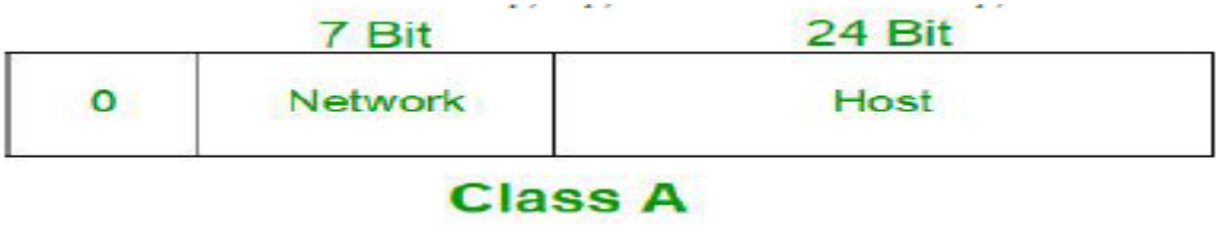
Special IP Addresses



- The IP address 0.0.0.0 is used by hosts when they are being booted.
- IP addresses with 0 as network number refer to the current network.

- The address consisting of all 1s allows broadcasting on the local network, typically a LAN.
- The addresses with a proper network number and all 1s in the host field allow machines to send broadcast packets to distant LANs anywhere in the Internet
- All addresses of the form 127.*xx.yy.zz* are reserved for loopback testing. Packets sent to that address are not put out onto the wire.They are processed locally and treated as incoming packets**.**

Class A

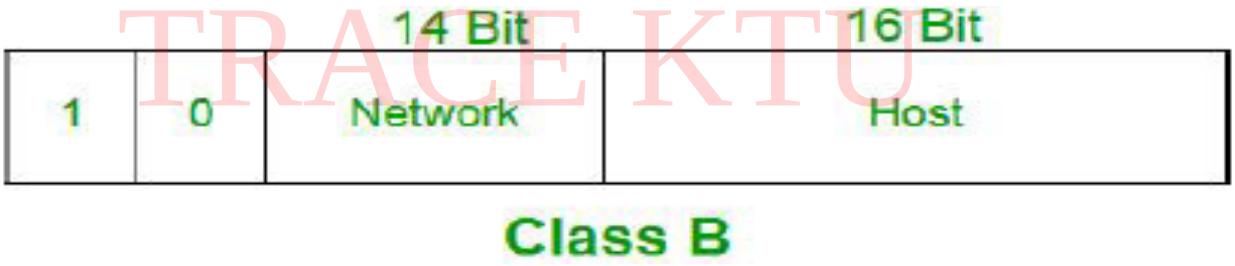


- The first bit of the first octet is always set to 0 (zero).
- Thus the first octet ranges from 1 – 127, i.e.00000001 – 01111111
- Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only.
- The IP range 127.x.x.x is reserved for loopback.
- Class A IP address format is thus: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH
- IP address belonging to class A are assigned to the networks that contain a large number of hosts.
- The network ID is 8 bits long. The host ID is 24 bits long.
- The **higher order bits** of the first octet in class A is always set to 0.
- The **remaining 7 bits** in first octet are used to determine network ID.
- The **24 bits of host ID** are used to determine the host in any network.
- The default sub-net mask for class A is 255.x.x.x.

- Start adress:0.0.0.0
- End address:127.255.255.255

Class B

- An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.
- Thus the first octet ranges from **128 – 191** ie.,10000000 - 10111111
- Class B IP Addresses range from 128.0.x.x to 191.255.x.x.
- The default subnet mask for Class B is 255.255.x.x.
- Class B IP address format is **10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH**
- IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.



- The **network ID** is 16 bits long.
- The **host ID** is 16 bits long.
- The higher order bits of the first octet of IP addresses of class B are always set to **10**.
- The remaining 14 bits are used to determine **network ID**.
- The 16 bits of **host ID** is used to determine the host in any network.
- The default sub-net mask for class B is 255.255.x.x.
- Class B has a total of:

- 2^14 = 16384 network address
- 2^16 = 65536 host address
- Ranges from 128.0.0.0 to 191.255.0.0 as class B

Class C

Class C

- The first octet of Class C IP address has its first 3 bits set to 110, that is:
- The first octet ranges from 192-223 ie.,11000000-11011111
- Class C IP addresses range from 192.0.0.x to 223.255.255.x.
- The default subnet mask for Class C is 255.255.255.x.
- Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH**
- IP address belonging to class C are assigned to small-sized networks.
- The network ID is 24 bits long. The host ID is 8 bits long.
- The higher order bits of the first octet of IP addresses of class C are always set to 110.
- The remaining 21 bits are used to determine network ID.
- The 8 bits of host ID is used to determine the host in any network.
- The default sub-net mask for class C is 255.255.255.x.
- Class C has a total of

- 2^21 = 2097152 network address
- 2^8 = 256 host address

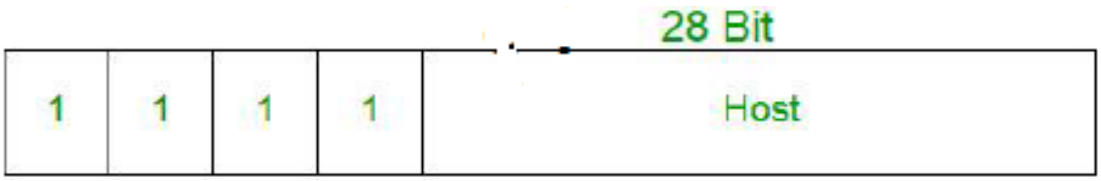
- IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.
- Example :192.168.178.1

Class D

Class D

- The first octet ranges from 224-239 ie., 11100000-11101111
- Class D has IP address rage from 224.0.0.0 to 239.255.255.255.
- Class D is reserved for **Multicasting**.
- In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.
- The **higher order bits** of the first octet of IP addresses belonging to class D are always set to 1110.
- The remaining bits are for the address that interested hosts recognize.
- Class D does not posses any sub-net mask.
- IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.

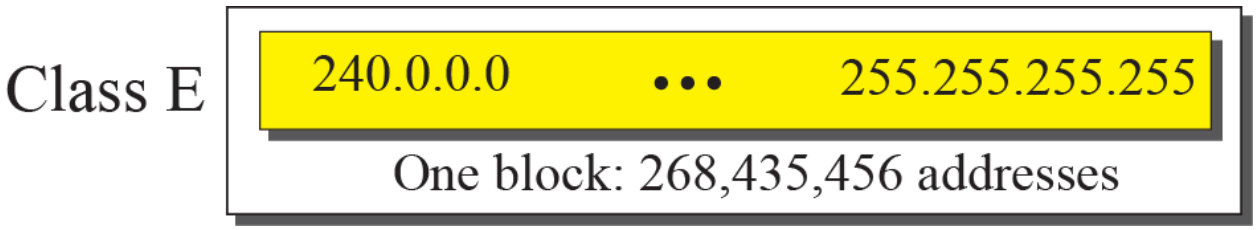
Class E



Class E

- IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254.
- Like Class D, this class too is not equipped with any subnet mask.

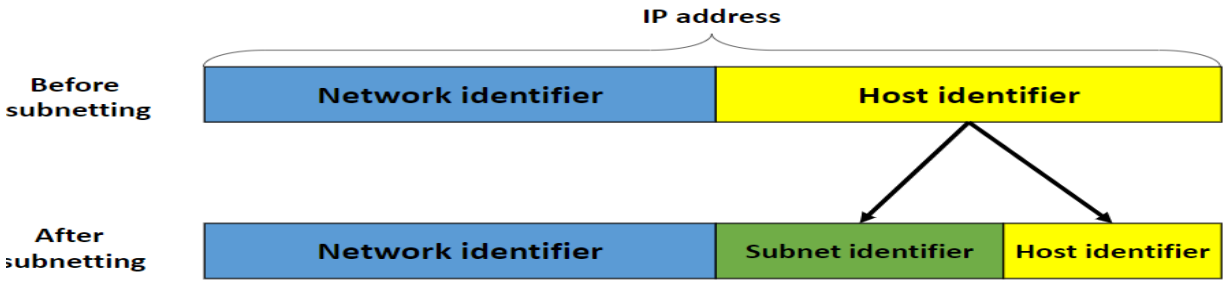
- IP addresses belonging to class E are reserved for experimental and research purposes.
- IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254.
- This class doesn't have any sub-net mask.
- The higher order bits of first octet of class E are always set to1111.



Range of special IP addresses:

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Subnets



- all the hosts in a network must have the same network number.
- This property of IP addressing can cause problems as networks grow
- The problem is the rule that a single class A, B, or C address refers to one network, not to a collection of LANs.As more and more organizations ran into this situation, a small change was made to the addressing system to deal with it.
- The solution is to allow a network to be split into several parts for internal use but still act like a single network to the outside world.

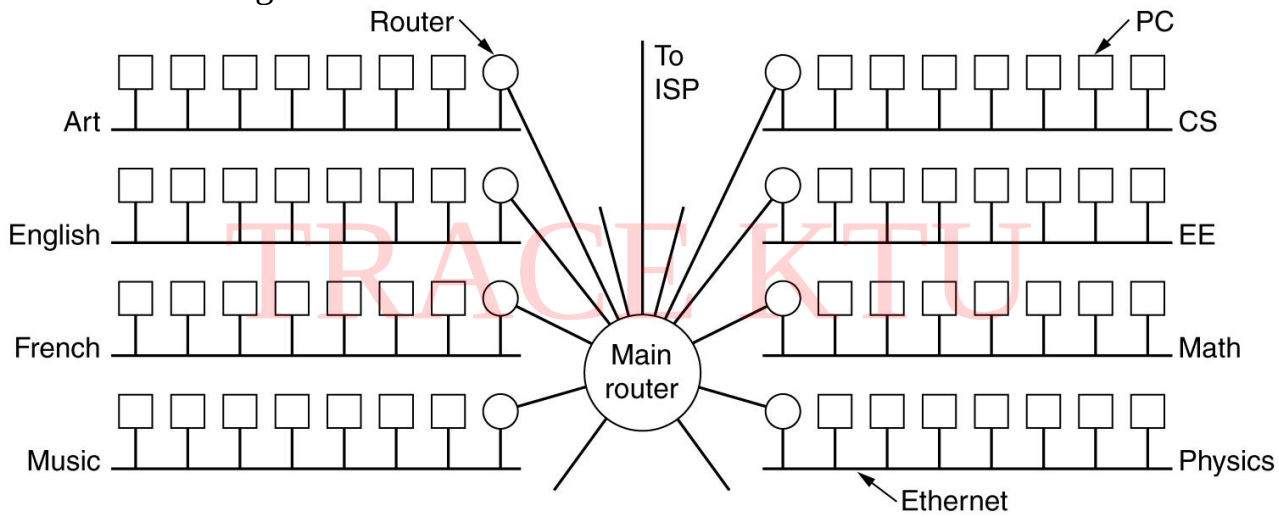
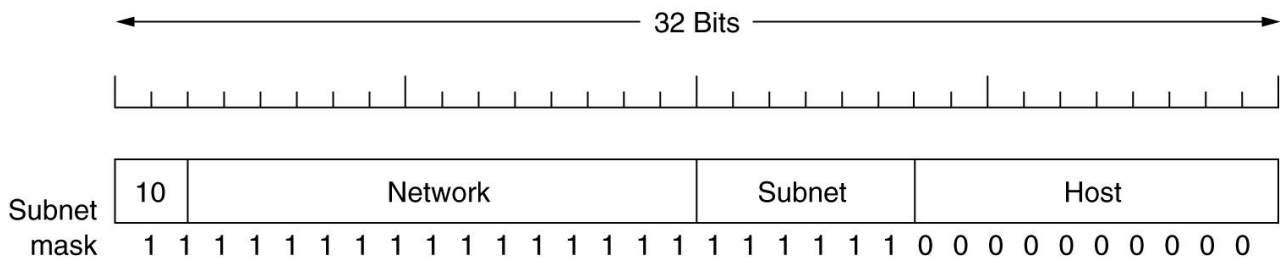


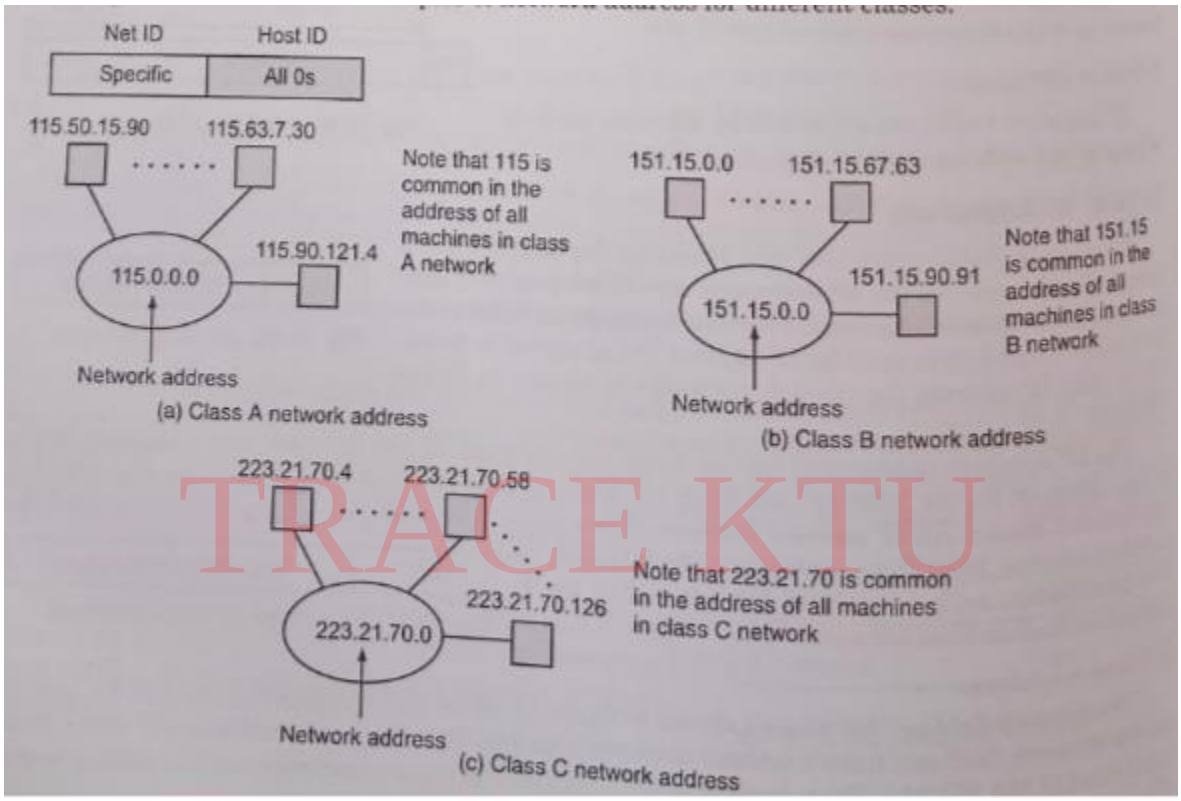
Fig:A campus network consisting of LANs for various departments.

Parts of the network (in this case, Ethernets) are called **subnets.**When a packet comes into the main router, how does it know which subnet (Ethernet) to give it to? One way would be to have a table with 65,536 entries in the main router telling which router to use for each host on campus.This idea would work, but it would require a very large table in the main router and a lot of manual maintenance as hosts were added, moved, or taken out of service.Instead, a different scheme was invented.

To implement subnetting, the main router needs a **subnet mask** that indicates the split between network + subnet number and host, as shown in Fig



Network Address and Mask



- **Network address** – It identifies a **network** on internet.

  Using this,

  - we can find range of addresses in the network
  - and total possible number of hosts in the network.

- **Mask** (subnetting)

  - It is a 32-bit binary number that **masks** an **IP address**, and divides the **IP address** into network address and host address.

- Network mask is obtained by putting All bits of netid as 1's and host id as 0's
- It gives the network address in the **address block**
- ✓ when **AND operation** is bitwise applied on the mask and any IP address of the block.

- The default mask in different classes are :

Class A – 255.0.0.0

Class B – 255.255.0.0

Class C – 255.255.255.0

- **Example** : Given IP address 132.6.17.85 and default class B mask, find the beginning address (network address).
- **Solution** : The default mask is 255.255.0.0, which means that the only the first 2 bytes are preserved(existing state) and the other 2 bytes are set to 0. Therefore, the network address is 132.6.0.0.

Mask: 11111111 11111111 00000000 00000000

IP Address: 10000100 00000110 00010001 01010101

Then do an **AND operation**, it will produce

10000100 00000110 00000000 00000000

➔ which is equivalent to **132.6.0.0**

Class	*Mask in binary*	*Mask in dotted-decimal*
A	**11111111** 00000000 00000000 00000000	**255**.0.0.0
B	**11111111 11111111** 00000000 00000000	**255.255**.0.0
C	**11111111 111111111 11111111** 00000000	**255.255.255**.0

When a packet comes into the main router, how does the router know which subnet to give it to?

- When a packet arrives, the router looks at the destination address of the packet and checks which subnet it belongs to.

➢ The router can do this by ANDing the destination address with the mask for each subnet and

➢ checking to see if the result is the corresponding prefix(a network corresponds to a contiguous block of IP address space).

- Outside the network, the subnetting is not visible, so allocating a new subnet does not require contacting ICANN or changing any external databases.

Classless Addressing

- Classless addressing system is also known as **CIDR(Classless Inter-Domain Routing** or **super netting).**
- It is a way to allocate and specify the **Internet addresses** used in inter-domain routing.
- What happened in **classfull addressing** is that

➢ if any **company needs more than 254 host machines** but far fewer than the 65,533 host addresses,

➢ then the only option for the company is to take the class B address.

- Now suppose **company needs only 1000 IP addresses** for its host computers

➢ then in this (65533-1000=64533) IP addresses get wasted.

CIDR Notation

- CIDR IP addresses can be described as consisting of two groups of bits.

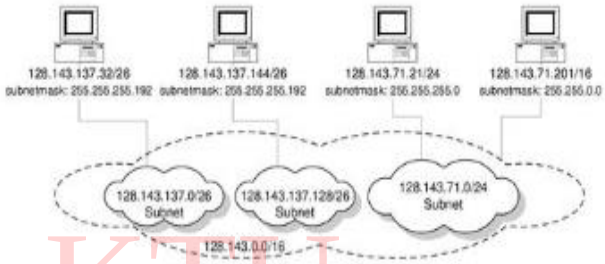
➢ The **most significant group** of bits denotes the **prefix** i.e., a network address that is used for the identification of a network or sub-network.

➢ The **least significant group** of bits is known as host identifier that determines the total number of bits in the address.

- ✓ It is used to signify the device on the work that will receive incoming information packets.
- A CIDR network address looks like this : **192.30.250.0/15**
- ➢ The **"192.30.250.0"** is the network address itself
- ➢ **"15"** says that the first **15 bits** are the network part of the address, leaving the last **17 bits** for specific host addresses.
- One **advantage** of classless addressing is that it sends subnet information.

Subnetting and Supernetting

- **Subnetting**:
  - Subnets are created by extending the network prefix



- **Supernetting**:
  - Multiple prefixes can be summarized with a single prefix, by reducing the network prefix:

    128.143.0.0/16
    128.142.0.0/16 ⟹ 128.142.0.0/15

  - If neighboring networks have similar address blocks, supernetting reduces the size of routing tables
  - Route Aggregation: Routing table entries can be reduced, when prefixes can be collapsed and networks have the same outgoing interface

Sub netting	Super netting
A process of dividing a network into the sub networks.	A process of combining small networks into a larger network.
The number of bits of network addresses is increased.	The number of bits of host addresses is increased.
Mask bits are moved towards right of the default mask.	Mask bits are moves towards left of the default mask.
Sub netting is implemented using VLSM (variable length subnet mask)	Super netting is implemented using CIDR classless inter domain routing.
The objective is to reduce the address depletion.	The objective is to simplify and fasten the routing process.

Problems on subnetting

Fixed Length Subnetting-

Fixed length subnetting also called as **classful subnetting** divides the network into subnets where-

- All the subnets are of same size.
- All the subnets have equal number of hosts.
- All the subnets have same subnet mask**.**

$2 = 2^{1}$ $8 = 2$

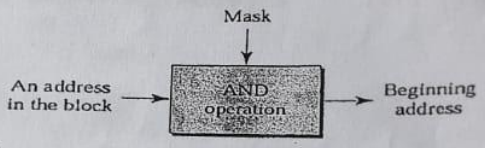
$4 = 2^{2}$

Example: 1 How many subnets can be created from a given IP address and subnet mask ?

To calculate the number of subnets from given subnet mask we use 2^N where N = number of bits borrowed from host bits to create subnets. For example given an IP address 192.168.1.0 and subnet mask 255.255.255.224. The default mask of class C is 255.255.255.0 . The number of bits borrowed from host part is 3. Thus N is 3 and number of subnets created is 8.

- ✓ Given an IP address 200.1.2.35 and subnet mask 255.255.255.192. Find the number of subnets. and no: of hosts in each subnet

Example: 2 How to calculate the Network Id of a subnet, if an IP address and its subnet mask is given?



- ✓ Given an IP address 200.1.2.35 and subnet mask 255.255.255.192. Find the Network Id to which the IP address belongs to.

↗ power of 2 (2, 4, 8, 16, 32 ...)

Example: 3 What is block size for subnet mask?

Block size is used to calculate the valid subnets. To figure out the block size, use the formula block size = 256 - Subnet mask. For example block size for subnet mask 255.255.255.240 is 256 - 240 = 16.

Example: 4 What are the total hosts in a subnet?

Total hosts are the hosts available per subnet. To calculate total hosts use formula 2^H where H is number host bits.

Example: 5 How many valid hosts are available per subnet?

Valid hosts are the number of hosts those can be assigned to devices. We need to reduce two address per subnet, one for network ID and another for broadcast ID. So to calculate valid hosts the formula is Valid hosts =Total hosts – 2.

Example: 6 How to find subnet mask from block size ?

Subnet Mask = 256 - block size

(2, 4, 8, 16, 32 etc)

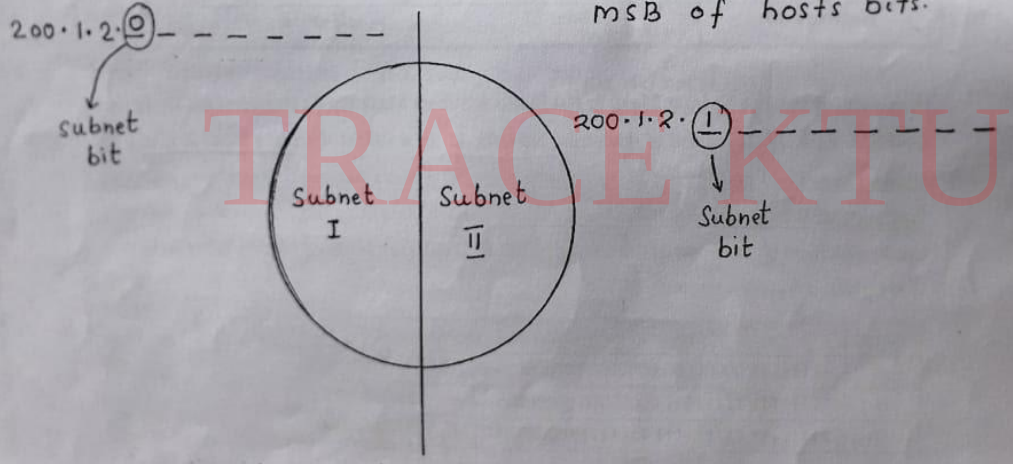
SUBNETTING- An Example for classical subnetting (dividing network into power of 2)

Consider an IP address 200.1.2.0 which belongs to class C network. In class C network, total number of IP address available for host are 256. (recall classful addressing). Divide this network into 2 subnets. Also find subnet mask.

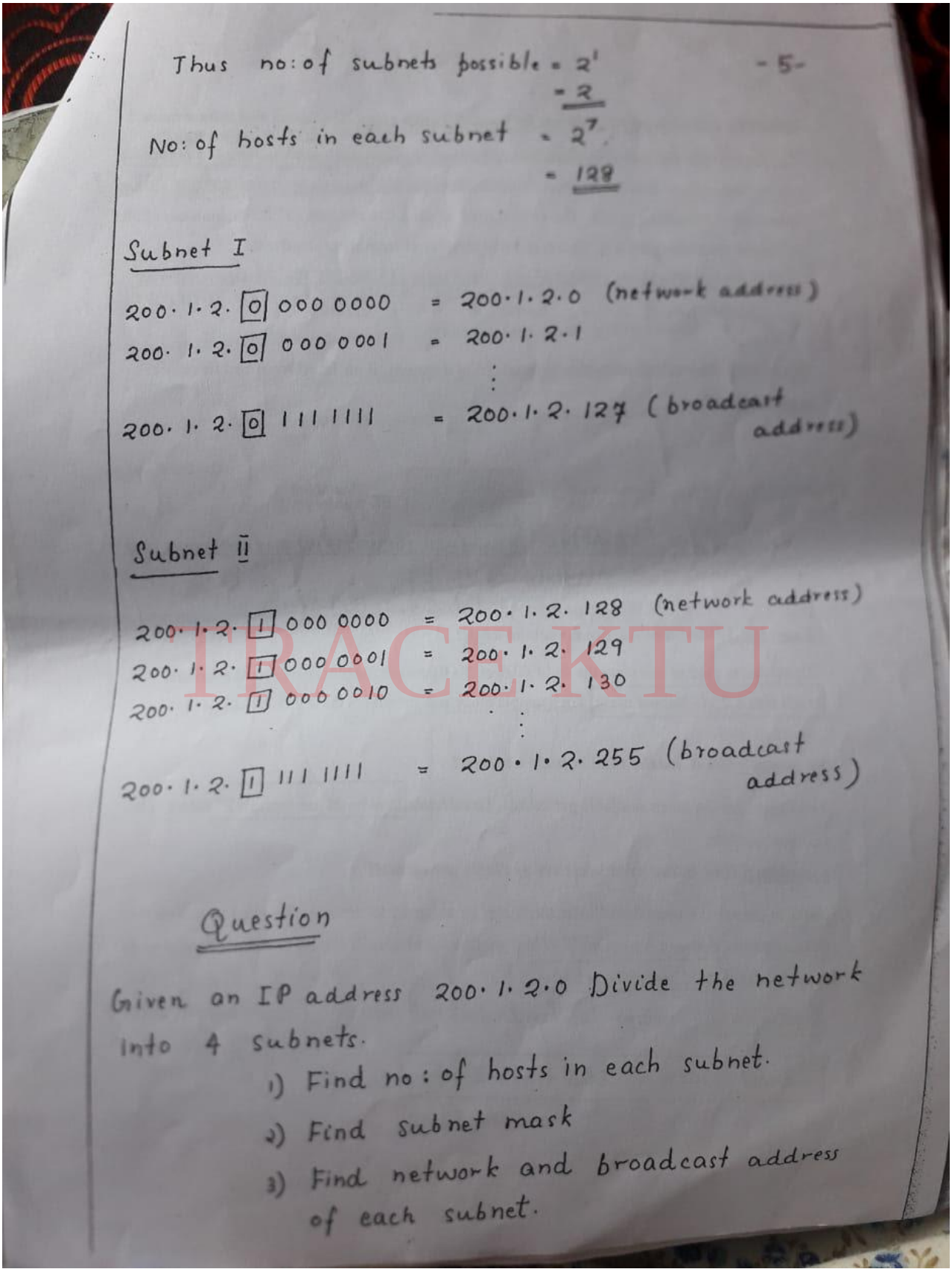
Solution

Default subnet mask of class C = 255.255.255.0

To create two subnets, number of bits required for subnet id = one i.e one bit is choosed from the MSB of hosts bits.



∴ No: of network bits = 24 bits
No: of subnet bits = 01 bits
No: of hosts bits = 07 bits
Thus Subnet Mask : 255.255.255.1 000 0000
- 255.255.255.128



Thus no: of subnets possible = 2^1 -5-
= 2

No: of hosts in each subnet = 2^7
= 128

Subnet I

200.1.2.[0]000 0000 = 200.1.2.0 (network address)
200.1.2.[0]000 0001 = 200.1.2.1
⋮
200.1.2.[0]111 1111 = 200.1.2.127 (broadcast address)

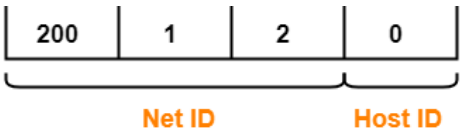
Subnet II

200.1.2.[1]000 0000 = 200.1.2.128 (network address)
200.1.2.[1]000 0001 = 200.1.2.129
200.1.2.[1]000 0010 = 200.1.2.130
⋮
200.1.2.[1]111 1111 = 200.1.2.255 (broadcast address)

Question

Given an IP address 200.1.2.0 Divide the network into 4 subnets.

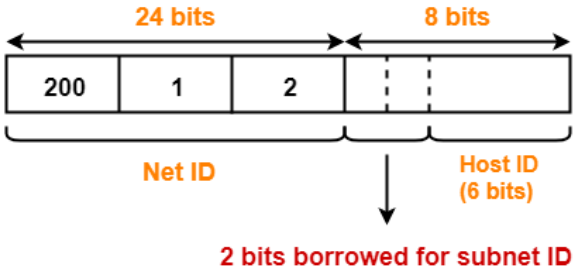
1) Find no: of hosts in each subnet.
2) Find subnet mask
3) Find network and broadcast address of each subnet.



For creating four subnets and to represent their subnet IDs, we require 2 bits.

So,

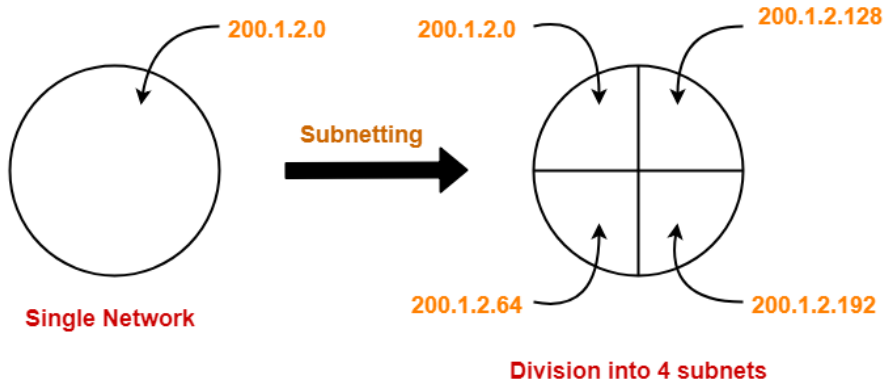
- We borrow two bits from the Host ID part.
- After borrowing two bits, Host ID part remains with only 6 bits.



- If borrowed bits = 00, then it represents the 1st subnet.
- If borrowed bits = 01, then it represents the 2nd subnet.
- If borrowed bits = 10, then it represents the 3rd subnet.
- If borrowed bits = 11, then it represents the 4th subnet.

IP Address of the four subnets are-

- 200.1.2.**00**000000 = 200.1.2.0
- 200.1.2.**01**000000 = 200.1.2.64
- 200.1.2.**10**000000 = 200.1.2.128
- 200.1.2.**11**000000 = 200.1.2.192



For 1st Subnet-

- IP Address of the subnet = 200.1.2.0
- Total number of IP Addresses = 2^6 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.**00**000000, 200.1.2.**00**111111] = [200.1.2.0, 200.1.2.63]
- Direct Broadcast Address = 200.1.2.**00**111111 = 200.1.2.63
- Limited Broadcast Address = 255.255.255.255

For 2nd Subnet-

- IP Address of the subnet = 200.1.2.64
- Total number of IP Addresses = 2^6 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.**01**000000, 200.1.2.**01**111111] = [200.1.2.64, 200.1.2.127]
- Direct Broadcast Address = 200.1.2.**01**111111 = 200.1.2.127
- Limited Broadcast Address = 255.255.255.255

For 3rd Subnet-

- IP Address of the subnet = 200.1.2.128
- Total number of IP Addresses = 2^6 = 64
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.**10**000000, 200.1.2.**10**111111] = [200.1.2.128, 200.1.2.191]
- Direct Broadcast Address = 200.1.2.**10**111111 = 200.1.2.191
- Limited Broadcast Address = 255.255.255.255

For 4th Subnet-

- IP Address of the subnet = 200.1.2.192
- Total number of IP Addresses = 2^6 = 64

- Total number of hosts that can be configured = 64 – 2 = 62
- Range of IP Addresses = [200.1.2.**11**000000, 200.1.2.**11**111111] = [200.1.2.192, 200.1.2.255]
- Direct Broadcast Address = 200.1.2.**11**111111 = 200.1.2.255
- Limited Broadcast Address = 255.255.255.255

Problem3

suppose a network with IP Address 192.16.0.0. is divided into 2 subnets, find number of hosts per subnet.

Also for the first subnet, find-

1. Subnet Address
2. First Host ID
3. Last Host ID
4. Broadcast Address

Solution-

- Given IP Address belongs to class C.
- So, 24 bits are reserved for the Net ID.
- The given network is divided into 2 subnets.
- So, 1 bit is borrowed from the host ID part for the subnet IDs.
- Then, Number of bits remaining for the Host ID = 7.
- Thus, Number of hosts per subnet = 2^7 = 128.

For 1st Subnet-

- Subnet Address = First IP Address = 192.16.0.**0**0000000 = 192.16.0.0
- First Host ID = 192.16.0.**0**0000001 = 192.16.0.1
- Last Host ID = 192.16.0.**0**1111110 = 192.16.0.126
- Broadcast Address = Last IP Address = 192.16.0.**0**1111111 = 192.16.0.127

For 2ND Subnet-

- Subnet Address = First IP Address = 192.16.0.**0**0000000 = 192.16.0.128
- First Host ID = 192.16.0.**0**0000001 = 192.16.0.129
- Last Host ID = 192.16.0.**0**1111110 = 192.16.0.254
- Broadcast Address = Last IP Address = 192.16.0.**1**1111111 = 192.16.0.255

Calculating the maximum possible number of hosts in a subnet:

To find the maximum number of hosts, look at the number of binary bits in the host number above. The easiest way to do this is to subtract the netmask length from 32 (number of bits in an IPv4 address). This gives you the number of host bits in the address.

***Maximum Number of hosts* = 2^(32 - netmask_length) - 2**

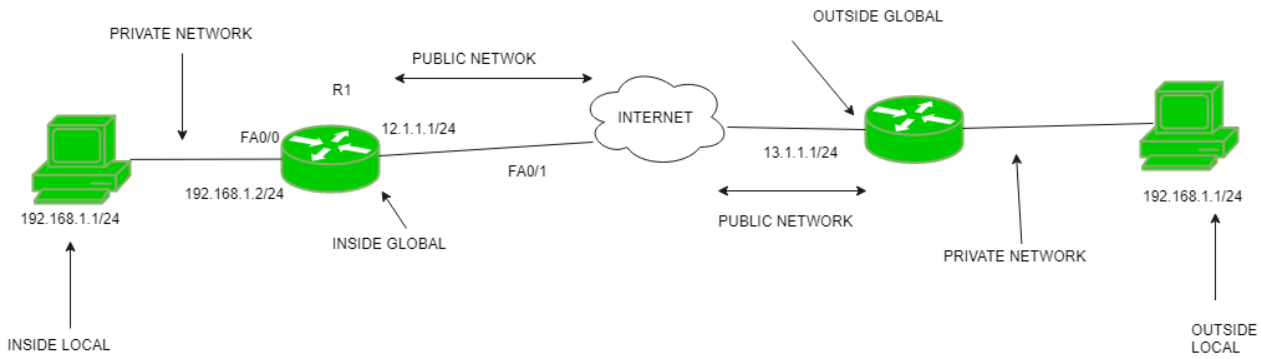
The reason we subtract 2 above is because the all-ones and all-zeros host numbers are reserved. The all-zeros host number is the network number; the all-ones host number is the broadcast address.

Using the example subnet of 128.42.0.0/21 above, the number of hosts is...

Maximum Number of hosts = 2**(32 - 21) - 2 = 2048 - 2 = 2046

Network Address Translation (NAT)

- The idea of NAT is to allow multiple devices to access the Internet through a single public address.
- To achieve this, the translation of a private IP address to a public IP address is required.
- **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.
- NAT generally operates on a router or firewall.



Network Address Translation (NAT) working –

- Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network.
- When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address.
- When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

Advantages

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.

Internet Control Protocols

In addition to IP, which is used for data transfer, the Internet has several control protocols used in the network layer, including ICMP, ARP, RARP, BOOTP, and DHCP

ICMP - Internet Control Message Protocol:

- 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 is used by networks devices like routers for sending error messages and operations information.

▪ The operation of the Internet is monitored closely by the routers.
▪ When something unexpected occurs, the event is reported by the ICMP
▪ ICMP is also used to test the Internet.
▪ About a dozen types of ICMP messages are defined. The most important ones are listed in Fig.
▪ Each ICMP message type is encapsulated in an IP packet.

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

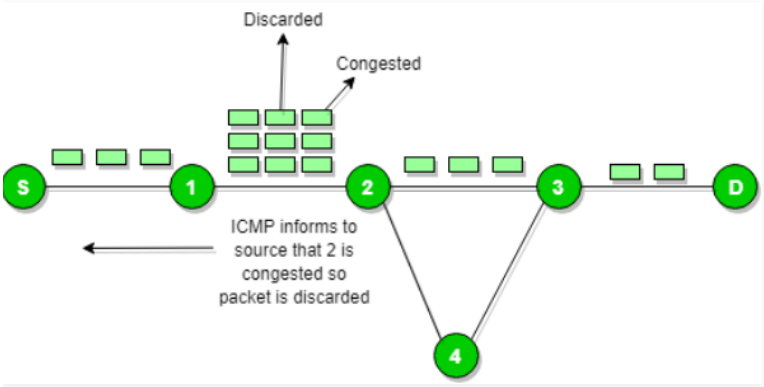
DESTINATION UNREACHABLE message

▪ used when the subnet or a router cannot locate the destination or when a packet with the *DF bit cannot be delivered because a "small-packet" network stands in the way*

TIME EXCEEDED message
▪ sent when a packet is dropped because its counter has reached zero.

PARAMETER PROBLEM message
▪ indicates that an illegal value has been detected in a header field.
▪ This problem indicates a bug in the sending host's IP software or possibly in the software of a router transited.

SOURCE QUENCH message



- used to block hosts that were sending too many packets.
- When a host received this message, it was expected to slow down.
- It is rarely used any more because when congestion occurs, these packets tend to add more fuel to the fire.
- Congestion control in the Internet is now done largely in the transport layer

REDIRECT message
- used when a router notices that a packet seems to be routed wrong.
- It is used by the router to tell the sending host about the probable error.

ECHO and ECHO REPLY messages
- used to see if a given destination is reachable and alive.
- Upon receiving the ECHO message, the destination is expected to send an ECHO REPLY message back.

TIMESTAMP REQUEST and TIMESTAMP REPLY messages
- similar, except that the arrival time of the message and the departure time of the reply are recorded in the reply.
- This facility is used to measure network performance

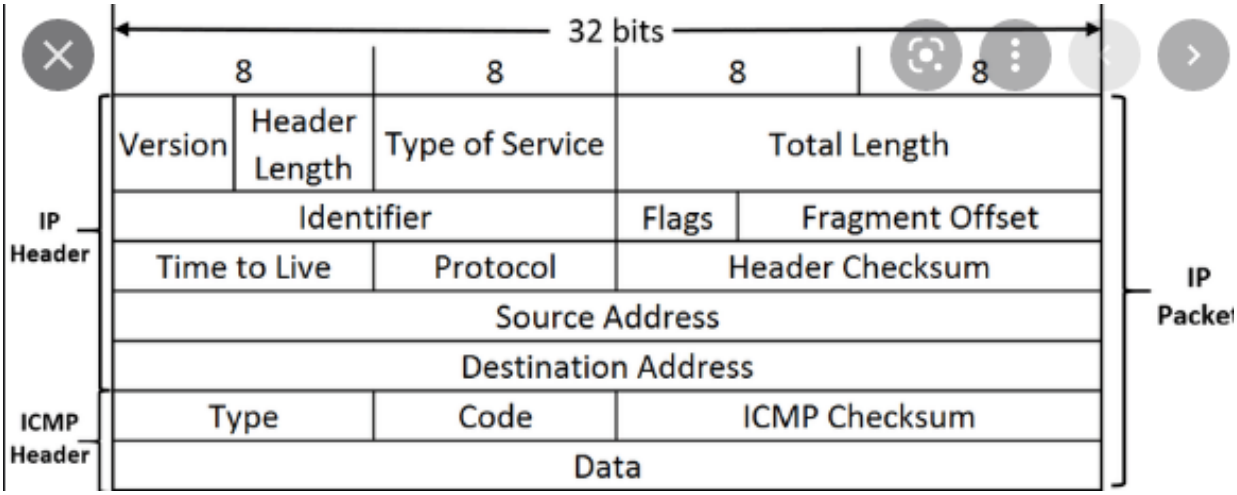
Address-Mask Request and Reply

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. 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 thenecessary mask for the host.

4.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. 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. A router can also periodically send router-advertisement messages even if no host has solicited.Note that when a router sends out an advertisement, it announces not only its ownpresence but also the presence of all routers on the network of which it is aware.

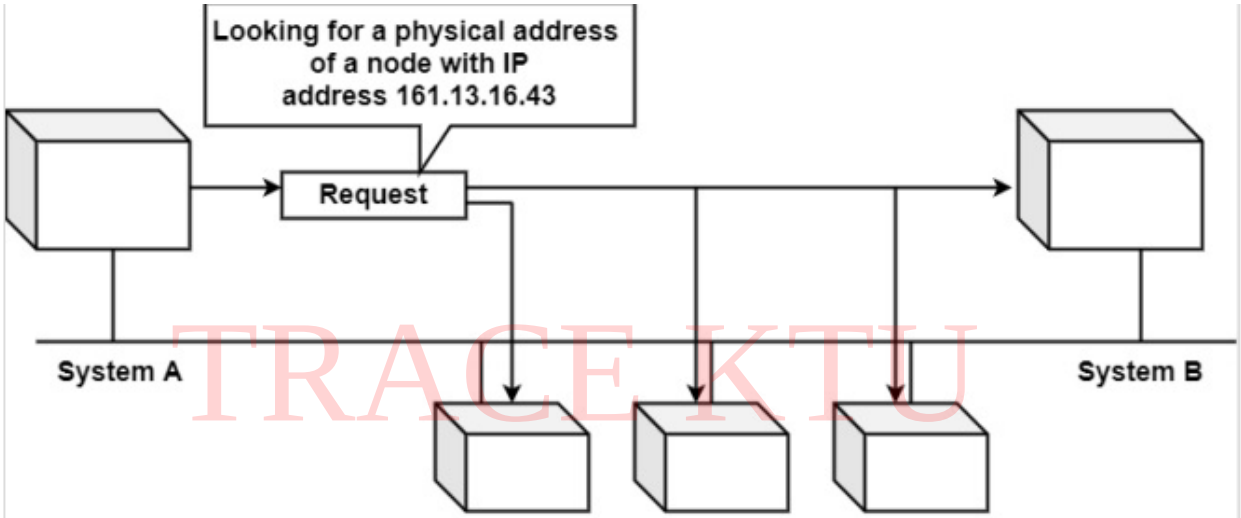


ARP - The Address Resolution Protocol

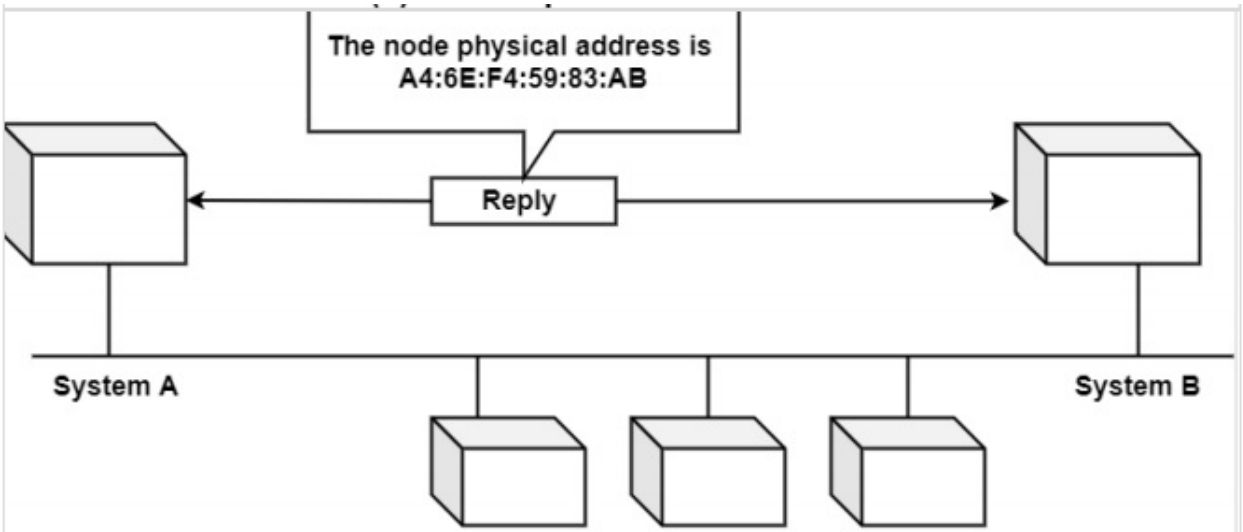
- **ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.**

IP addresses cannot actually be used for sending packets because the data link layer hardware does not understand Internet addresses.

- most hosts at companies and universities are attached to a LAN by an interface board that only understands LAN addresses.
- For example, every Ethernet board comes equipped with a 48-bit Ethernet address.
- Manufacturers of Ethernet boards request a block of addresses from a central authority to ensure that no two boards have the same address
- The boards send and receive frames based on 48-bit Ethernet addresses.
- They know nothing at all about 32-bit IP addresses.



(a) ARP request is broadcast



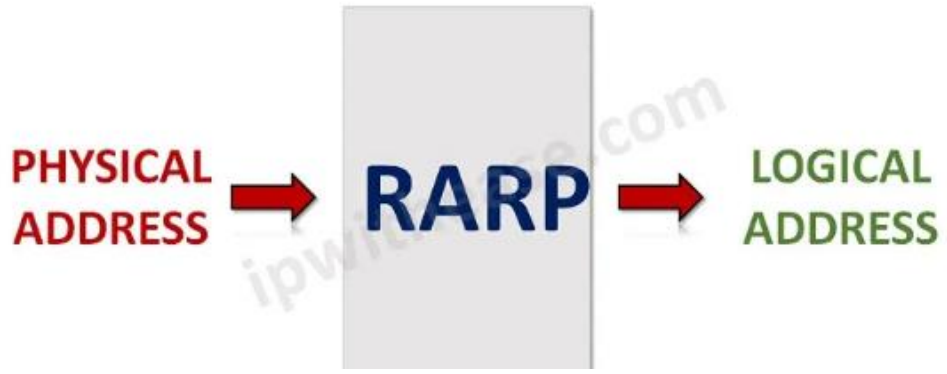
(b) ARP reply is unicast

- The goal of ARP is to enable each host on a network to build up a table of mappings between IP addresses and link-level addresses.
- Since these mappings may change over time because an Ethernet card in a host breaks and is replaced by a new one with a new address, the entries are timed out periodically and removed. This happens on the order of every 15 minutes. **The set of mappings currently stored in a host is known as the ARP cache or ARP table.**

Steps

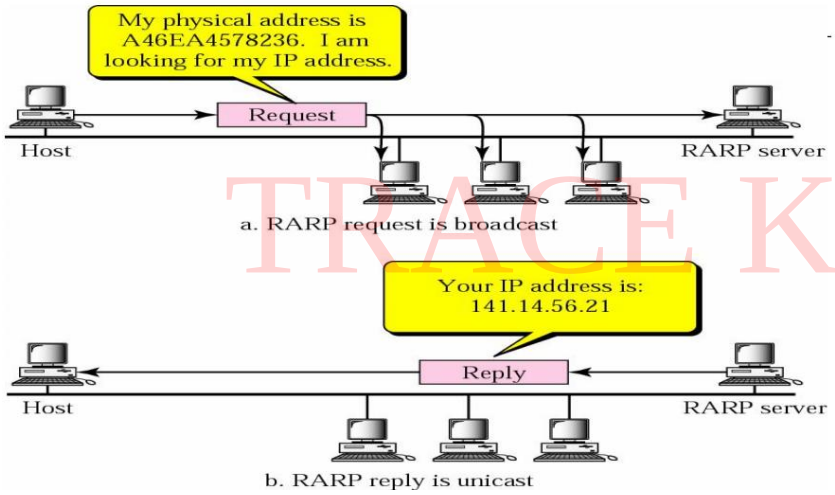
- When a host tries to interact with another host, an ARP request is initiated. If the IP address is for the local network, the source host checks its ARP cache to find out the hardware address of the destination computer.
- If the correspondence hardware address is not found, ARP broadcasts the request to all the local hosts.
- All hosts receive the broadcast and check their own IP address. If no match is discovered, the request is ignored.
- The destination host that finds the matching IP address sends an ARP reply to the source host along with its hardware address, thus establishing the communication. The ARP cache is then updated with the hardware address of the destination host.

REVERSE ADDRESS RESOLUTION PROTOCOL



- The **Reverse Address Resolution Protocol** (**RARP**) is an obsolete computer networking protocol used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address.
- The client broadcasts the request and does not need prior knowledge of the network topology or the identities of servers capable of fulfilling its request.
- RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses.
- Media Access Control (MAC) addresses need to be individually configured on the servers by an administrator.
- RARP is limited to serving only IP addresses.

RARP Operation



Disadvantage of RARP

- uses a destination address of all 1s (limited broadcasting) to reach the RARP server. Such broadcasts are not forwarded by routers. So, a RARP server is needed on each network.
- To overcome this problem, **BOOTP** was invented

BOOTP

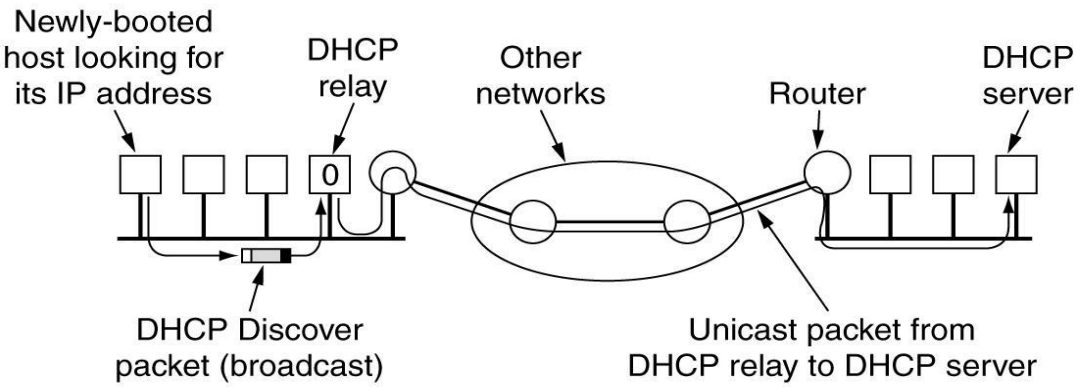
- Bootstrap Protocol (BOOTP) is a networking protocol which is used by networking administration to give IP addresses to each member of that network for participating with other networking devices by the main server**.**
- BOOTP uses UDP messages, which are forwarded over routers.
- It also provides a diskless workstation with additional information, including IP address of the file server holding the memory image, IP address of the default router, and subnet mask to use.
- Problem with BOOTP requires manual configuration of tables mapping IP address to Ethernet address.
- When a new host is added to a LAN, it cannot use BOOTP until an administrator has assigned it an IP address and entered its (Ethernet address, IP address) into the BOOTP configuration tables by hand.
- To eliminate this error-prone step, BOOTP was extended and given a new name: **DHCP (Dynamic Host Configuration Protocol)**

DHCP (Dynamic Host Configuration Protocol)

- DHCP allows both manual IP address assignment and automatic assignment. In most systems, it has largely replaced RARP and BOOTP.
- Like RARP and BOOTP, DHCP is based on the idea of a special server that assigns IP addresses to hosts asking for one.
- This server need not be on the same LAN as the requesting host.
- Since the DHCP server may not be reachable by broadcasting, a **DHCP relay agent** is needed on each LAN

DHCP Working

- To find its IP address, a newly booted machine broadcasts a DHCP DISCOVER packet.
- The DHCP relay agent on its LAN captures all DHCP broadcasts.
- When it finds a DHCP DISCOVER packet, it sends the packet as a unicast packet to the DHCP server, possibly on a distant network.
- The only piece of information the relay agent needs is the IP address of the DHCP server.



Issue that arises with automatic assignment of IP addresses from a pool

▪ how long an IP address should be allocated.

▪ If a host leaves the network and does not return its IP address to the DHCP server, that address will be permanently lost.

▪ After a period of time, many addresses may be lost.

▪ To prevent that from happening, IP address assignment may be for a fixed period of time, a technique called **leasing.**

▪ Just before the lease expires, the host must ask the DHCP for a renewal.

▪ If it fails to make a request or the request is denied, the host may no longer use the IP address it was given earlier.

The Dynamic Host Configuration Protocol (DHCP) has been devised to provide

static and dynamic address allocation that can be manual or automatic.

Static Address Allocation In this case DHCP acts as BOOTP does. It is backward compatiblewith BOOTP, which means a host running the BOOTP client can request astatic address from a DHCP server. A DHCP server has a database that statically bindsphysical addresses to IP addresses.

Dynamic Address Allocation DHCP has a second database with a pool of availableIP addresses. This second database makes DHCP dynamic. When a DHCP

client requestsa temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time

Internet Multicasting

- Ability to send to a large number of receivers simultaneously

Eg:

- updating replicated, distributed databases, transmitting stock quotes to multiple brokers and handling digital conference telephone calls
- IP supports multicasting using class D addresses
- Each class D address identifies a group of hosts
- 28 bits are available for identifying groups, so over 250 million groups can exist at the same time.
- When a process sends a packet to a class D address, a best-efforts attempt is made to deliver it to all the members of the group addressed, but no guarantees are given some members may not get the packet.

Two kinds of group addresses are supported:

- permanent addresses
- temporary addresses .

- permanent group is always there and does not have to be set up.
  - Each permanent group has a permanent group address
  - Some examples of permanent group addresses are:
  - 224.0.0.1 All systems on a LAN
  - 224.0.0.2 All routers on a LAN
  - 224.0.0.5 All OSPF routers on a LAN
  - 224.0.0.6 All designated OSPF routers on a LAN

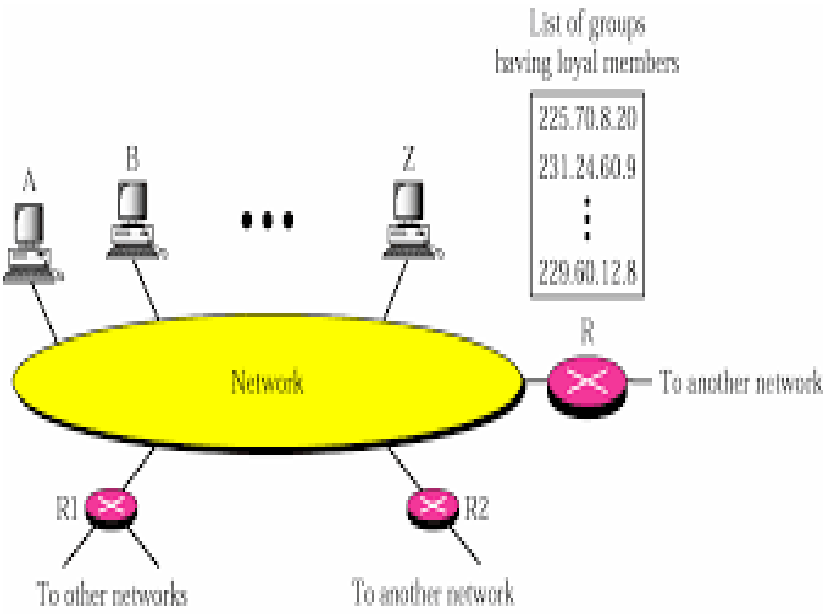
Temporary groups must be created before they can be used.

- A process can ask its host to join a specific group.
- It can also ask its host to leave the group.
- When the last process on a host leaves a group, that group is no longer present on the host.
- Each host keeps track of which groups its processes currently belong to.

- Multicasting is implemented by special multicast routers
- About once a minute, each multicast router sends a hardware (i.e., data link layer) multicast to the hosts on its LAN(address 224.0.0.1) asking them to report back on the groups their processes currently belong to.
- Each host sends back responses for all the class D addresses it is interested in.
  - These query and response packets use a protocol called **IGMP (Internet Group Management Protocol)**

IGMP

- The **Internet Group Management Protocol** (**IGMP**) 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.
- it is a protocol that manages group membership status of hosts connected to Internet to multicast routers.
- If the multicast router doesn't know membership status, it must broadcast packets which creates a lot of traffic. Thus IGMP keeps a list of groups in the network and update this list.(**Group Management**)
- **Joining a group**
    - A host or router can join a group by sending membership report. A membership report is sent twice, one after the other. If the first one is lost or damaged, the second one replaces it.
- **Leaving a group**
    - A host or router can leave a group by sending leave report. However, when a multicast router receives a leave report, it cannot immediately remove that group from its list. Because the report comes from just one host, there may be other hosts that are still interested in that group.
    - Thus multicast router sends a special query message containing group ID and waits for some time. If no membership report is received, remove the group from the list.
- **Monitoring Membership**
    - Consider the situation in which only one host is interested in a group, but host is shut down. To handle such situation, multicast router periodically sends (every 125 sec) a general query message which contains the address 0.0.0.0. The multicast router is expecting an answer from each group in its list.
    - when hosts receive general query message, it responds with membership report , if it is interested in a group.



IPv6

Drawbacks of IPv4

1. Address depletion
2. No Encryption and Authentication

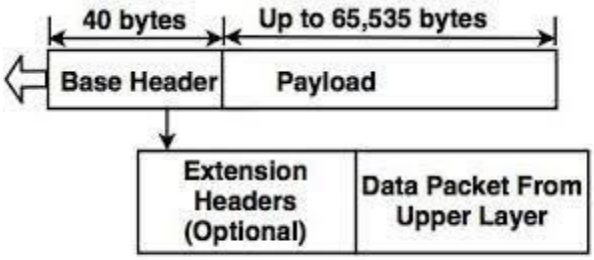
IPV6 was developed to accommodate the growth of Internet. The related protocol ICMP is also modified to as ICMPv6. Other network layer protocols like ARP, RARP and IGMP were either deleted or included in ICMPv6.

Advantages of IPv6

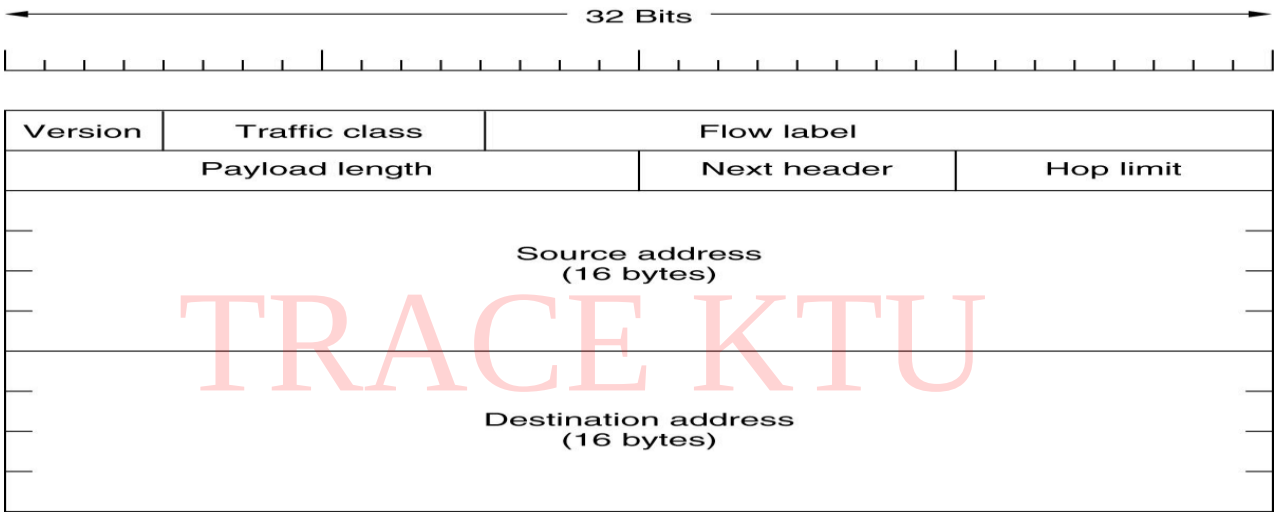
1. Address Space : IPv6 has a 128 bit long address, which is larger than IPv4.
2. Header format : IPv6 has a new header format, in which options are separated from the base header and inserted between the base header and the upper layer data.
3. Extension : IPv6 is designed to allow the extension of the protocol, if required for new applications.
4. Security : Encryption and authentication mechanism provides confidentiality and integrity to the packets in IPv6.IPv6 Packet Format

Packet Format of IPv6
The IPv6 packet is shown in the diagram. Each packet is composed of base header and the payload. The payload consists of two fields, optional extension headers and

the data from upper layer. The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain upto 65,535 bytes of information.



IPv6 Datagram Header and Payload



Version field is always 6 for IPv6 (4 for IPv4)

Traffic class field

- used to distinguish between packets with different real-time delivery requirements.
- A field designed for this purpose has been in IP since the beginning, but it has been only periodically implemented by routers.
- These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).

Flow label field (20 bit)

- 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. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.

Payload length field

- tells how many bytes follow the 40-byte main header
- The name was changed from the IPv4 Total length field because the meaning was changed slightly:
- (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. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.

Next header field (8 bit)

- there can be additional (optional) extension headers.
- This field tells which of the (currently) six extension headers follow this one.
- If this header is the last IP header, the Next header field tells which transport protocol handler (e.g., TCP, UDP) to pass the packet to.

Hop limit field

- used to keep packets from living forever.
- same as the Time to live field in IPv4, namely, a field that is decremented on each hop.
- In theory, in IPv4 it was a time in seconds, but no router used it that way
- so the name was changed to reflect the way it is actually used

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.

Source address and Destination address fields

- 16-byte addresses
- They are written as eight groups of four hexadecimal digits with colons between the groups 8000:0000:0000:0000:0123:4567:89AB:CDEF.Since many addresses will have many zeros inside them, three optimizations have been authorized.

1. leading zeros within a group can be omitted, so 0123 can be written as 123.
2. one or more groups of zero bits can be replaced by a pair of colons

The above address now becomes 8000::123:4567:89AB:CDEF

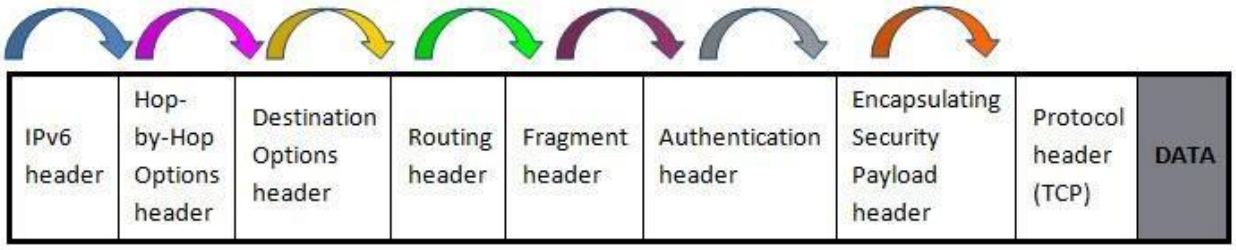
- Checksum field is gone because calculating it greatly reduces performance (data link layer and transport layers normally have their own checksums)

Extension Headers

In IPv6, the Fixed Header contains only that much information which is necessary, avoiding those information which is either not required or is rarely used. All such information is put between the Fixed Header and the Upper layer header in the form of Extension Headers. Each Extension Header is identified by a distinct value.

When Extension Headers are used, IPv6 Fixed Header's Next Header field points to the first Extension Header. If there is one more Extension Header, then the first Extension Header's 'Next-Header' field points to the second one, and so on.

If the Next Header field contains the value 59, it indicates that there are no headers after this header, not even Upper Layer Header.



It can be extended upto six extension headers.

1. Hop by hop option : It is used when the source needs to pass the information to all routers visited by the datagram.
2. Source routing : It combines the concepts of the strict source route and the loose source route options of IPv4.(A *source route* is a list of IP addresses specified by the sender of the IP datagram. If the source route is *strict*, then the datagram must pass through each listed node and only the listed nodes. That is, all the nodes listed in the source route must be neighbors. But if the source route is *loose*, the datagram must pass through each listed node, but can also pass through other nodes that do not appear in the source route.)
3. Fragmentation : The data travels through the different networks, each router first decapsulates the IPv6 datagram from the received frame, then processes it and again encapsulates in another frame.
4. Authentication : Authentication validates the message sender and ensures the integrity of the data.
5. Encrypted Security Payload (ESP) : It is an extension that provides confidentiality and protects against eavesdropping .
6. Destination option : It is used when the source needs to forward information to the destination only and not to intermediate routers.

Transition from IPv4 to IPv6

Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly. It takes a considerable amount of time before every system in the Internet can move from IPv4 to IPv6. The transition must be smooth to

prevent any problems between IPv4 and IPv6 systems. Some transition strategies are tunneling and header translation.

Tunneling:

Tunneling strategy is used when two computers using IPv6 wants to communicate with each other and the packet must go through a region that uses only IPv4. The sending host send its IPv6 packet to the router that connects the IPv6 network to the IPv4 Internet. The router then encapsulates the packet within an IPv4 packet and address it to the other side router that connects to the IPv6 network. When this wrapped packet arrives, the router removes the original IPv6 packet and sends it onward to the destination host.

IPv4 and IPv6

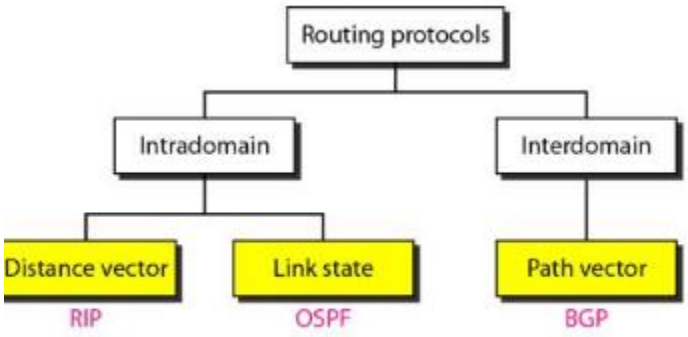
Compare the IPv4 header with the IPv6 header

- IHL field is gone because the IPv6 header has a fixed length.
- Protocol field was taken out because the Next header field tells what follows the last IP header (e.g., a UDP or TCP segment).
- All the fields relating to fragmentation were removed because IPv6 takes a different approach to fragmentation
- hosts are expected to dynamically determine the datagram size to use.
- router that is unable to forward it sends back an error message
- This message tells the host to break up all future packets to that destination

	Ipv4	Ipv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C,	IPv6 does not contain classes of IP

	Class D, and Class E.	addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.

Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.



- An AUTONOMOUS SYSTEM/domain is a set of networks and routers under the control of a single administrative _authority.
- Routing within an autonomous system is intra domain routing/interior routing.

- Routing between autonomous systems is inter domain_routing/exterior routing

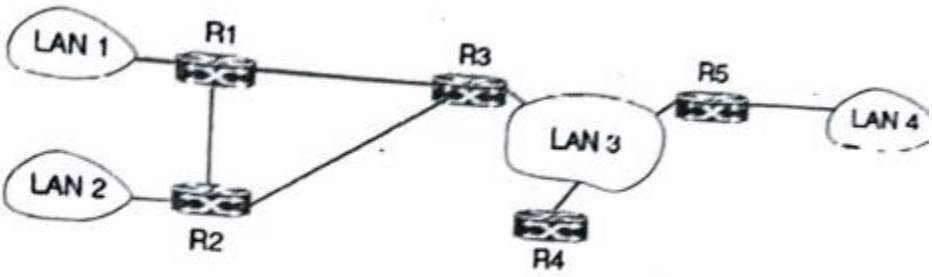
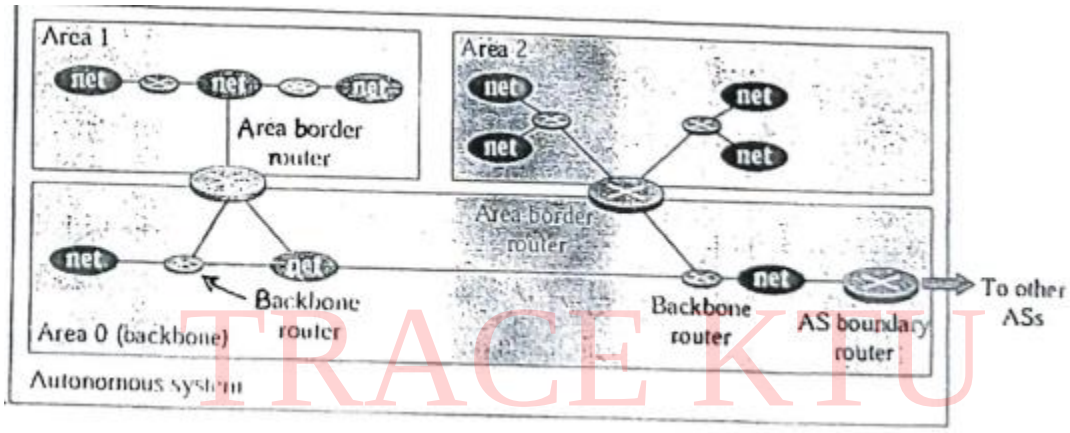
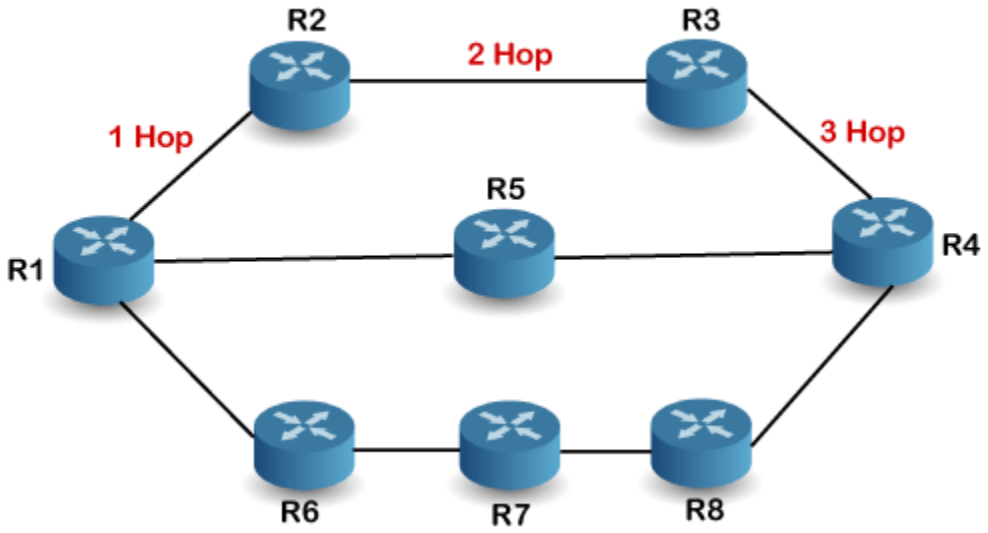


Fig:- Autonomous System (AS)



RIP (Routing Information Protocol)

- RIP stands for Routing Information Protocol. RIP is an intra-domain routing protocol used within an autonomous system
- It uses hop count as a routing metric to find the best path between the source and the destination network.
- It is a distance-vector routing protocol that works on the Network layer of the OSI model.
- RIP uses port number 520.
- Hop Count

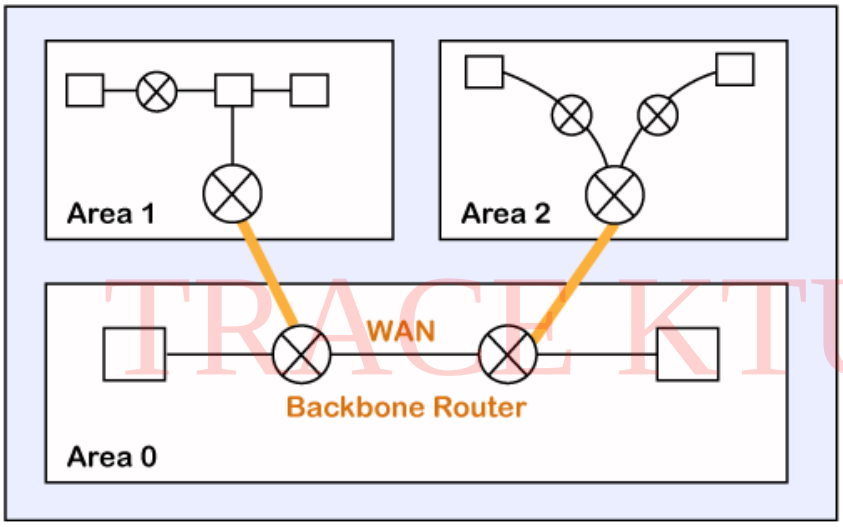


- Hop count is the number of networks occurring in between the source and destination network.
- The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table.
- RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

- Features of RIP
  - Updates of the network are exchanged periodically.
  - Updates (routing information) are always broadcast.
  - Full routing tables are sent in updates.
  - Routers always trust routing information received from neighbor routers.

The Open Shortest Path First Protocol (OSPF)

- Open shortest path first (OSPF) is a **link-state routing protocol** that is used to find the best path between the source and the destination router using its own shortest path first (SPF) algorithm.
- A link-state routing protocol is a protocol that uses the concept of triggered updates, i.e., if there is a change observed in the learned routing table then the updates are triggered only

- OSPF is an Intradomain routing protocol based on link state routing. OSPF divides an Autonomous System (AS) into areas. An area is a collection of networks, hosts and routers all contained within an autonomous system. All networks within an area must be connected. Routers inside an area flood the routing information. At the border of an area, special routers called area **border routers** summarize the information about an area and send it to another area. All areas inside an AS must be connected to a backbone. The routers inside the backbone are called **backbone routers**. Each area has an identification number. The identification number of backbone is zero. The metric (cost) is based on delay, throughput etc and is assigned by network admin
- 

- The OSPF achieves by learning about every router and subnet within the entire network. Every router contains the same information about the network.
- The way the router learns this information by sending LSA (Link State Advertisements).
- These LSAs contain information about every router, subnet, and other networking information. Once the LSAs have been flooded, the OSPF stores the information in a link-state database known as LSDB.
- The main goal is to have the same information about every router in an LSDBs.

OSPF messages –
OSPF uses certain messages for the communication between the routers operating OSPF.

1 Hello packet

The Hello packet is used to create a neighborhood relationship and check the neighbor's reachability. Therefore, the Hello packet is used when the connection between the routers need to be established.

2. Database Description

After establishing a connection, if the neighbor router is communicating with the system first time, it sends the database information about the network topology to the system so that the system can update or modify accordingly.

3. Link state request

The link-state request is sent by the router to obtain the information of a specified route. Suppose there are two routers, i.e., router 1 and router 2, and router 1 wants to know the information about the router 2, so router 1 sends the link state request to the router 2. When router 2 receives the link state request, then it sends the link-state information to router 1.

4. Link state update

The link-state update is used by the router to advertise the state of its links. If any router wants to broadcast the state of its links, it uses the link-state update.

5. Link state acknowledgment

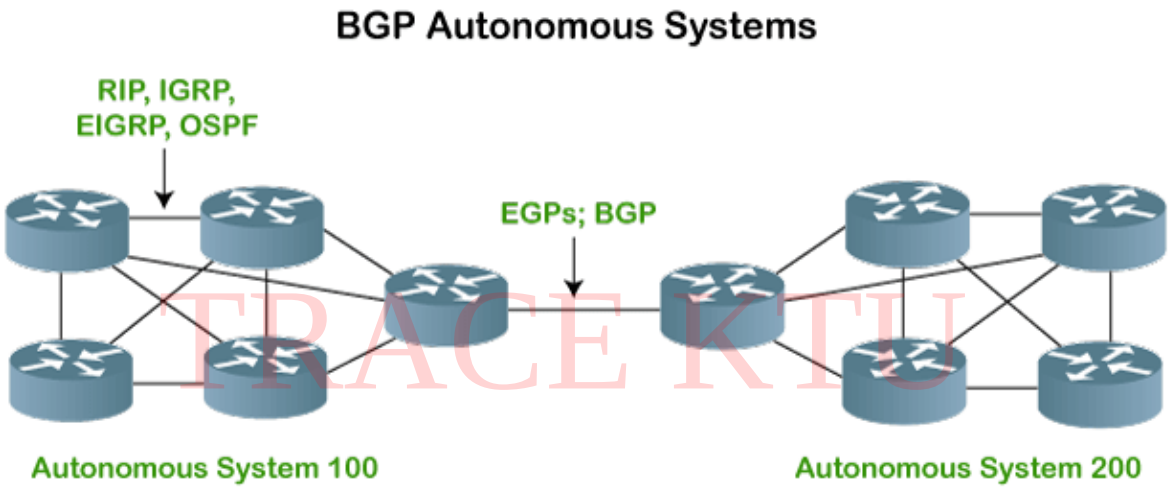
The link-state acknowledgment makes the routing more reliable by forcing each router to send the acknowledgment on each link state update. For example, router A sends the link state update to the router B and router C, then in return, the router B and C sends the link- state acknowledgment to the router A, so that the router A gets to know that both the routers have received the link-state update.

Working of OSPF

- Routers inside an area FLOOD the routing information. This information allows each router to construct the graph tor its area(s) and compute the shortest paths
- The backbone area docs this work, too. In addition, the backbone routers accept information from the area border routers and compute the best route from each backbone router to every other router.

- This information is propagated back to the area border routers, which advertise it within their areas.
- Using this information, internal routers can select the best route to a destination outside their area.

BGP(Border Gateway Protocol)

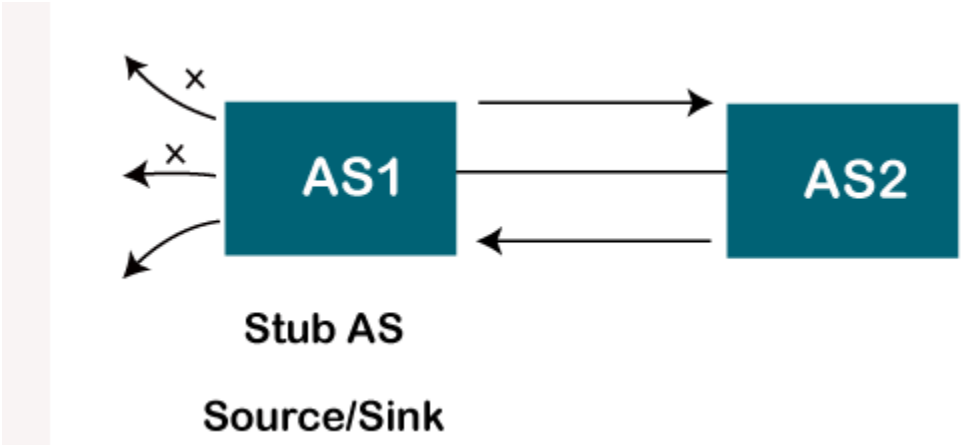


- Between AS, a different protocol, called BGP (Border Gateway Protocol), is used for exchanging information.
- BGP uses the services of TCP via port 179.
- Features
  - **Open standard:**It is a standard protocol which can run on any window device.
  - **Exterior Gateway Protocol**
  - **Supports internet:**It is the only protocol that operates on the internet backbone.
  - **Classless**

Types of Autonomous systems

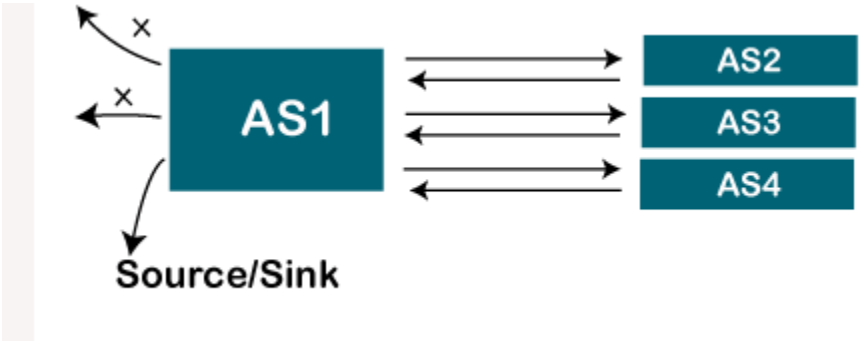
- In BGP, autonomous systems are divided into 3 categories:
- Stub AS. Multi-homed AS and Transit AS.

- **Stub autonomous system**



- A stub AS has only one connection to another AS.
- The data traffic cannot be passed through the stub autonomous system. The Stub AS can be either a source or a sink. If we have one autonomous system, i.e., AS1, then it will have a single connection to another autonomous system, AS2. The AS1 can act either as a source or a sink. If it acts as a source, then the data moves from AS1 to AS2. If AS1 acts as a sink, means that the data gets consumed in AS1 which is coming from AS2, but the data will not move forward from AS1.

- **Multihomed autonomous system**



- A muiti-homed AS has more than one connection to other ASs. It does not allow data coming from one AS and going to another AS to pass through.(i.e no transit traffic).

- **Transient Autonomous System**

- Transit AS is a multi homed AS that allows transit traffic.
- BGP is a form of distance vector protocol, but it is quite unlike distance vector protocols such as RIP.
- Instead of maintaining just the cost of the rOute to catch destination, each BGP router keeps track of the path used. **This approach is called a path vector protocol.**
- The path consists of the next hop router and the sequence of ASes. Finally, pairs of BGP routers communicate with each other by establishing TCP connections.

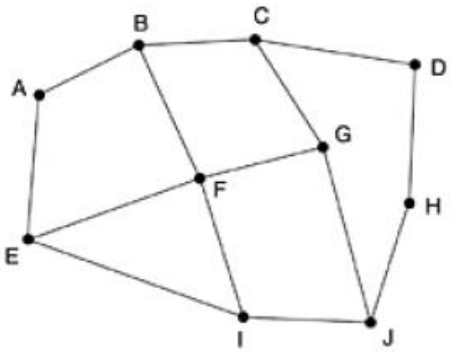
Working of BGP

Consider the routers shown in the following figure (a). In particular, consider the routing table of router F. Router F wants to send a packet to router D. The neighbors of F gives their routing information, which includes their complete path and cost to reach D

- After all the paths come in from the neighbors, *F* examines them to see which is the best. It quickly discards the paths from *I* and *E*, since these paths pass through *F* itself. The choice is then between using *B* and *G*.

- Every BGP router contains a module that examines routes to a given destination and scores them, returning a number for the "distance" to that destination for each route.
- Any route violating a policy constraint automatically gets a score of infinity.
- The router then adopts the route with the shortest distance. The scoring function is not part of the BGP protocol and can be any function the system managers want.
- The router adapts the route with shorter distance, Let it be GCD(shorter than BCD

Figure 5-67. (a) A set of BGP routers. (b) Information sent to F.



(a)

Information F receives from its neighbors about D

From B: "I use BCD"
From G: "I use GCD"
From I: "I use IFGCD"
From E: "I use EFGCD"

(b)

BGP can easily solve count to infinity problem as the complete path to destination is shared. Suppose the link FG goes down. This cause F → D = infinity. Now receives routes from its three remaining neighbors. These routes are BCD, IFGCD & EFGCD. Router F can immediately see that the latter two routes are pointless, as they passes through F itself. Hence F choose FBCD as its new route to destination D.

Types of messages in BGP:

OPEN

KEEPALIVE

UPDATE

NOTIFICATION

BGP peers form a TCP connection, use the OPEN message to establish BGP connection. Connections are kept open by KEEPALIVE messages. Initially routing table is exchanged. Modifications (Route additions and withdrawals) are made by UPDATE messages. Errors are reported by NOTIFICATION messages.

ICMPv6

On IPv6 networks, ICMP for IPv6 (ICMPv6) fulfills the same functions as ICMPv4 on IPv4 networks-namely, to provide a mechanism for exchanging error messages and informational messages.

- The ARP AND IGMP protocol in version 4 are combined in ICMPv6.
- The RARP protocol is dropped from the suite because it was rarely used and BOOTP has the same functionality.
- ICMP messages divided into two categories
  1.error reporting
  2.query

ERROR REPORTING:

- One of the main responsibilities of ICMP is error reporting.
- five types of error are handled
  1.destination unreachable
  2.packet too big
  3.time exceeded
  4.paramter problems
  5.redirection

ICMPv6 forms an error packet which is encapsulated in an IP datagram. This is delivered to the original source of the failed datagram.

Type of message	Version 4	Version 6
Destination unreachable	yes	yes
Source quench	yes	no
Packet too big	no	yes
Time exceeds	yes	yes
Parameter problem	yes	yes
redirection	yes	yes

Packet too big:

This is a new type of message added to version 6. if a router receives a datagram that is larger than the maximum transmission unit(MTU) size of the network through which the datagram should pass, two things happen.

1.the router discard the datagram

2.then an ICMP error packet – a packet too big message-is sent to the source.

Query

In addition to error reporting, ICMP can diagnose some network problems through the query message. Different groups of query messages

1.echo request and reply

2.solicitation and advertisement

3.neighbour solicitation and advertisement

4.group membership

Type of message	Version 4	Version 6
Echo request and reply	yes	yes
Timestamp request and reply	yes	no
Address –mask request and reply	yes	No
Router solicitation and advertisement	yes	yes

Neighbour solicitation and advertisement	ARP	yes
Group membership	IGMP	yes

Neighbour solicitation and advertisement

The network layer in version 4 contains an independent protocol called address resolution protocol(ARP). In version 6, the protocol is eliminated and its duties are included in ICMPv6. The idea is same as ARP but the frame format is changed in icmpv6.

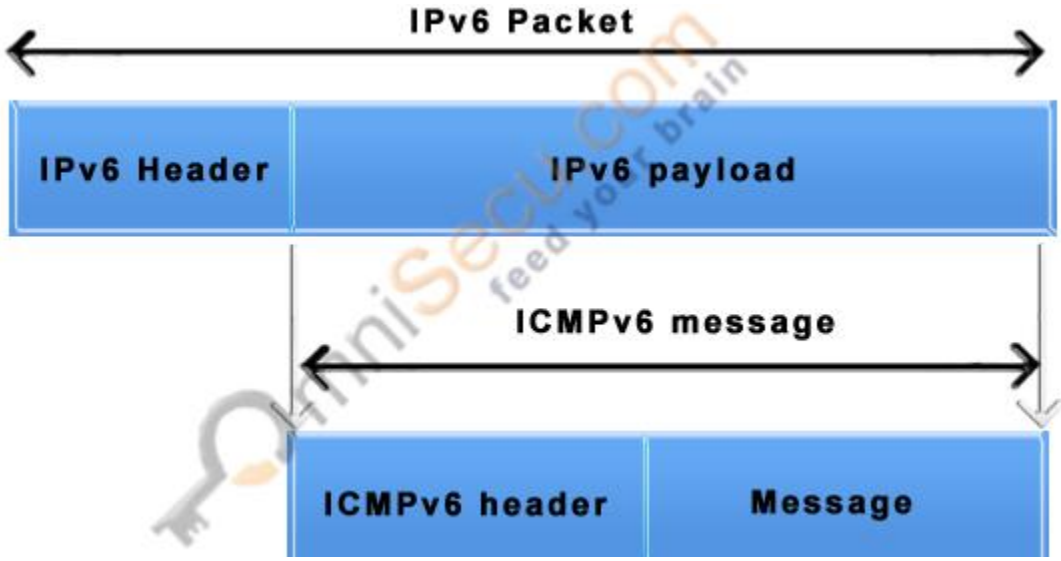
Group Membership:

The network layer in version4 contains an independent protocol called IGMP. In version 6 this protocol is eliminated and its duties are included in ICMPv6. In ICMPv6 the purpose is exactly same.

Echo request and Reply and router solicitation and advertisement

Both use the same idea and format as in version 4.

Packet format



Type Field in ICMPv6 Message	Code Field in ICMPv6 Message	Description
Destination Unreachable (Value 1)	0	No Route to destination network
	1	Administratively prohibited
	2	Beyond scope of source address
	3	IPv6 address unreachable
	4	Port unreachable
	5	Source address failed
	6	Reject route to destination
	7	Error in Source Routing Header
Packet Too Big (Value 2)	0	Packet too big for next hop link
	0	Hop Limit exceeded
Time Exceeded (Value 3)	0	Hop Limit exceeded
	1	Fragment reassembly time exceeded
Parameter Problem (Value 4)	0	Header field error
	1	Unrecognized Next Header type
	2	Unrecognized IPv6 option