

Chapter 4

Network Layer



Network Layer

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

The main functions performed by the network layer are:

- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- **Fragmentation and Reassembly:** It splits large packets into smaller fragments for transmission and reassembles them at the destination.
- **Packetizing:** It encapsulates data into packets for efficient transmission.
- **Network Address Translation (NAT):** Maps private IP addresses to a public IP for internet access, conserving IPs and adding security.

IP Addressing

An **IP (Internet Protocol) address** is a numerical label assigned to each device connected to a computer network that uses the IP for communication. It serves two main functions:

- **Identification** – Identifies the device on the network.
- **Location Addressing** – Specifies where the device is located.

IP Addressing

There are **two versions** of IP addresses:

1. IPv4 (Internet Protocol version 4)

- Format:** 32-bit address, written in decimal as four numbers separated by dots (e.g., 192.168.1.1). Thus, a total of 2^{32} (4,294,967,296 i.e. nearly 4 billion) IP address is possible in IPv4. IPV4 Supported Address Types – Unicast, multicast and broadcast.

- Range:** 0.0.0.0 to 255.255.255.255

- Example:** 172.16.254.1

2. IPv6 (Internet Protocol version 6)

- Format:** 128-bit address, written in hexadecimal and separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Thus, a total of 2^{128} IP address is possible in IPv6. IPV6 Supported Address Types – Unicast, multicast and anycast.

- More space:** Can support vastly more devices than IPv4

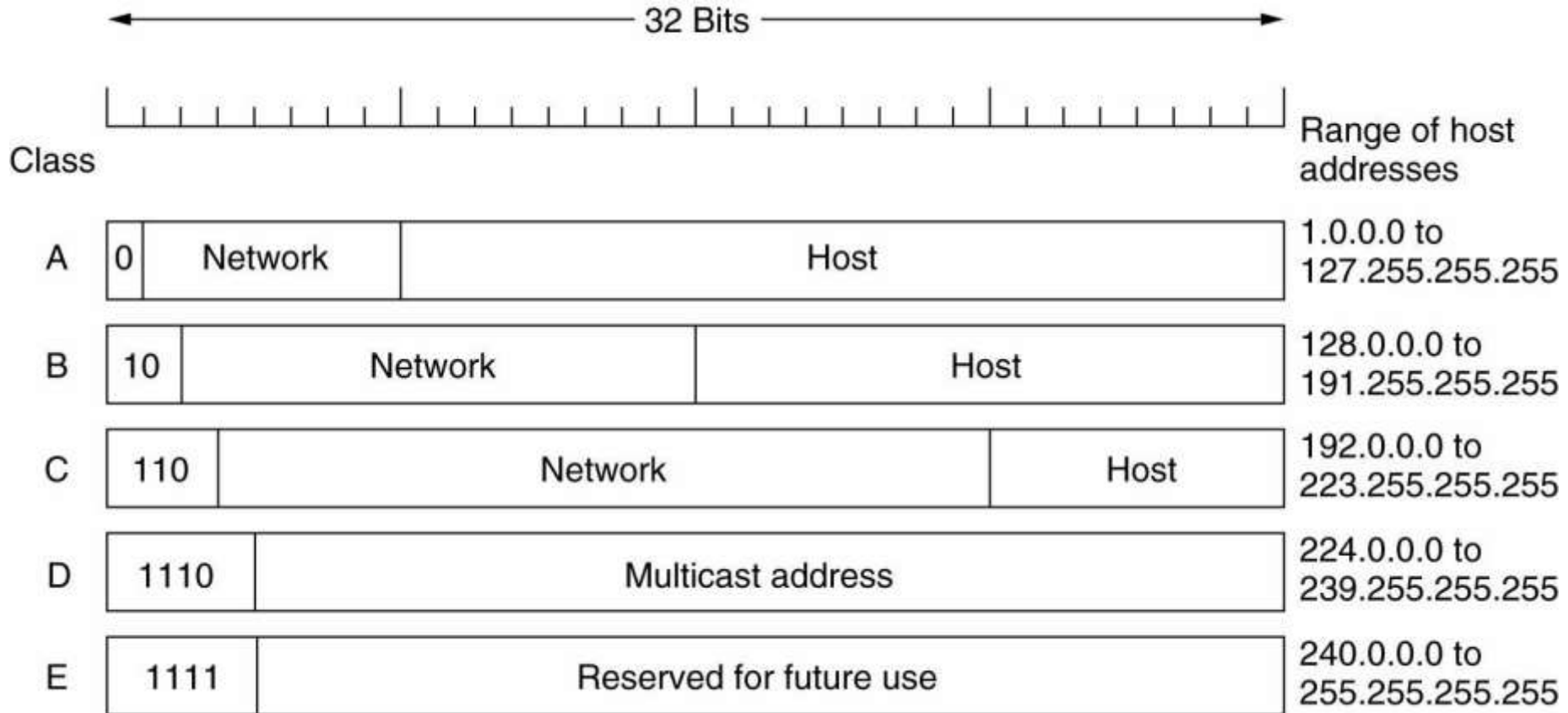
IPv4 Addressing

- 32 bits of IP address is divided into network and host portion.



- Classes
 - A (8 bits is used for networks and rest 24 bits for host)
 - B (16 bits is used for networks and rest 16 bits for host)
 - C (24 bits is used for networks and rest 8 bits for host)
 - D (Used for Multicasting)
 - E (For Future Use)

Class-full IPv4 Address



IPv4 Address Class

Class A

- Range : 0 – 127
- So total of 126 (2^7) Networks are possible and total host = 2^{24} in each Network.
- Default subnet mask is 255.0.0.0

Class B

- Range : 128 – 191
- So total of 2^{14} Networks are possible and total host = 2^{16} in each Network.
- Default subnet mask is 255.255.0.0

IPv4 Address Class

Class C

- Range : 192 – 223
- So total of 2^{21} Networks are possible and total host = 2^8 in each Network.
- Default subnet mask is 255.255.255.0

Class D

- Range : 224 – 239
- Used for Multicasting
- E.g. 224.0.0.1 (group)

Class E

- Range 240-255
- Not used (for future use)

Public and Private IP Address

- Public IP globally Unique
 - e.g. 202.70.91.7
- Visible to public, people can access your device.
- Private IP significant in Local Sites only.
- Private IP are commonly used when the public IP couldn't be obtained for all devices.
- Private IP address Range

IP Classes	Private IP Address Range
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255

Network Addresses



Download

- The **network portion** of the address, is used to represent the entire network
 - It represents a group of IP addresses that can be used on that network
- The **network address** consists of the network field plus **all 0's** in the host portion of the address
 - 192.168.18.00000000
 - 192.168.18.0
- The Network address is **not a usable host IP address**
- Network addresses are **only used by routers** to decide how to get packets to their destination

Broadcast Address

Dov

- A Broadcast Address is the address used to send messages to every host on the same network
- A Broadcast Address consists of the Network address, plus all 1's in the host field
- The Broadcast address is NOT a USABLE host address and can not be assigned to a host

Usable Host Addresses

Down

- As we just saw, the Network address and the Broadcast address are NOT usable host addresses
- A **usable host IP address** is an IP address that:
 - Is not a Network Address (all 0's in host field)
 - Is not a Broadcast Address (all 1's in host field)
 - Is not a reserved Address (127 addresses)
 - Is a Class A, B or C address
- Only a usable host IP address can be assigned to a host device

Determining Usable Host Addresses



Download

Network	Usable Hosts	Broadcast
10.0.0.0	10.0.0.1 – 10.255.255.254	10.255.255.255
172.16.0.0	172.16.0.1-172.16.255.254	172.16.255.255
192.168.1.0	192.168.1.1-192.168.1.254	192.168.1.255

The Loopback Address



- There are also private addresses that can be used for the diagnostic testing of devices.
- This type of private address is known as a loopback address.
- The class A, 127.0.0.0 network address, is reserved for loopback testing.
- The **loopback IP address**, **127.0.0.1** is used to test a NIC card to verify that it is sending and receiving signals.

Subnet Masks

Down

- A **subnet mask** is a 32 bit address which tells devices which part of the IP address is network and which part is host
 - Let routers & hosts figure out which network or subnet an IP address belongs to
- Subnet Masks contain:
 - all **1's** in the **network field**
 - all **0's** in the **host field**
- Example Subnet Masks:
 - 255.255.255.0
 - 255.255.0.0
 - 255.255.255.128
 - 255.254.0.0

Default Subnet Masks

- A default Subnet Mask is used when a network has NOT been subnetted
- Default Subnet Masks
 - **Class A: 255.0.0.0 OR /8**
 - 11111111.00000000.00000000.00000000
 - 8 bits for network, 24 bits for host
 - **Class B: 255.255.0.0 OR /16**
 - 11111111.11111111.00000000.00000000
 - 16 bits for network, 16 bits for host
 - **Class C: 255.255.255.0 OR /24**
 - 11111111.11111111.11111111.00000000
 - 24 bits for network, 8 bits for host

Subnetting

- Subnetting is the process of dividing a large network into smaller, manageable sub-networks (subnets).
- It allow you to divide a class A,B,C network address into smaller subnetworks, with their own network addresses.
- Each subnet acts like its own LAN and it is connected to its own router interface.
- Purpose:
 - - Efficient IP address utilization
 - - Improved security and performance
 - - Reducing broadcast traffic

Subnetting

- **IP Address:** A 32-bit number (IPv4) uniquely identifying a host.
- **Subnet Mask:** Separates the network portion from the host portion.
- **Network Address:** The first address in a subnet; identifies the subnet.
- **Broadcast Address:** The last address in a subnet; used to reach all hosts.

Fixed Length Subnet Masking (FLSM)

- All subnets have the same number of hosts.
- Example:
 - - IP: 192.168.1.0/24
 - - Divide into 4 subnets → 192.168.1.0/26
 - Subnets:
 - - 192.168.1.0 – 192.168.1.63
 - - 192.168.1.64 – 192.168.1.127
 - - 192.168.1.128 – 192.168.1.191
 - - 192.168.1.192 – 192.168.1.255

Variable Length Subnet Masking (VLSM)

- Subnets have different sizes based on need.
- Allows efficient IP usage.
- Example:
 - One department needs 60 hosts → /26
 - Another needs 30 → /27
 - Another needs 14 → /28

Subnetting Formulae

- **Number of Subnets:** 2^n (where n is number of borrowed bits)
- **Number of Hosts per Subnet:** $2^h - 2$ (where h is number of host bits)
- **Valid Host Range:** Between Network and Broadcast addresses

Subnetting Step-by-Step

- 1. Identify Class (A, B, C)
- 2. Convert subnet mask to binary
- 3. Calculate total subnets and hosts
- 4. List subnets (Network, Broadcast, Range)

Subnetting

Example:

- Given: 192.168.10.0/24 - Required: 4 Subnets
- Borrow 2 bits → New mask: /26

Subnet 1:

- Network: 192.168.10.0
- Broadcast: 192.168.10.63
- Hosts: 192.168.10.1 – 192.168.10.62
- Repeat for others.

Calculating Network & Broadcast Address

- Use subnet block size: $\text{Block Size} = 2^h$
- Next network address = Current network + block size
- Broadcast = Next Network – 1

□ Network Address

Calculating Network & Broadcast Address

- Calculating Network Address from given IP.
 1. Convert IP Address to Binary
 2. Convert Subnet Mask to Binary
 3. Perform Bitwise AND Operation
 4. Convert Result Back to Decimal

Calculating Network & Broadcast Address

- Calculating Broadcast address from given IP.
 1. Get the Network Address
 2. Invert Subnet Mask to Binary (Change all **1s** in the subnet mask to **0s**, and all **0s** to **1s**.)
 3. Perform Bitwise OR Operation
 4. Convert Result Back to Decimal

Calculating Network & Broadcast Address

Given: 192.168.1.10/24

Find

- **Subnet Mask ?**
- **Network Address ?**
- **Broadcast Address ?**
- **1st Usable Host ?**
- **4th Usable Host ?**
- **Last Usable Host ?**

Calculating Network & Broadcast Address

Given: 192.168.1.10/24

Solution:

- **Subnet Mask:** 255.255.255.0 → Block size = 256
- **Network Address:** 192.168.1.0
- **Broadcast Address:** 192.168.1.255
- **1st Usable Host:** 192.168.1.1
- **4th Usable Host:** 192.168.1.4
- **Last Usable Host :** 192.168.1.254

Calculating Network & Broadcast Address

Question 2

Given: 10.0.0.50/26

Find

- **Subnet Mask ?**
- **Network Address ?**
- **Broadcast Address ?**
- **1st Usable Host ?**
- **4th Usable Host ?**

Calculating Network & Broadcast Address

Question 2

Given: 10.0.0.50/26

Solution:

- **Subnet Mask:** 255.255.255.192 → Block size = 64
- **Network Address:** 10.0.0.0
- **Broadcast Address:** 10.0.0.63
- **1st Usable Host:** 10.0.0.1
- **4th Usable Host:** 10.0.0.4

Calculating Network & Broadcast Address

Question 3

Given: 10.10.10.33/30

Solution:

- **Subnet Mask ?**
- **Network Address ?**
- **Broadcast Address ?**
- **1st Usable Host ?**
- **4th Usable Host ?**

Calculating Network & Broadcast Address

Question 3

Given: 10.10.10.33/30

Solution:

- **Subnet Mask:** 255.255.255.252 → Block size = 4
- **Network Address:** 10.10.10.32
- **Broadcast Address:** 10.10.10.35
- **1st Usable Host:** 10.10.10.33
- **4th Usable Host:** ✗ Only 2 hosts in /30 → Not available

Number of Hosts & Networks

- For Class C (example):
 - Default: /24 → 256 addresses
 - Submitted: /26 → 4 subnets (64 addresses each)
 - Hosts/Subnet = $64 - 2 = 62$
- Why subtract 2?
 - 1 for Network Address
 - 1 for Broadcast Address

Summary Table

• CIDR	Subnet Mask	Subnets	Hosts/Subnet
• /24	255.255.255.0	1	254
• /25	255.255.255.128	2	126
• /26	255.255.255.192	4	62
• /27	255.255.255.224	8	30
• /28	255.255.255.240	16	14
• /29	255.255.255.248	32	6

• **CIDR (/n)**: Short for *Classless Inter-Domain Routing*, this tells how many bits are used for the **network portion** of the IP address.

• **Subnet Mask**: Shows the same thing as CIDR but in dotted decimal format (e.g., /25 = 255.255.255.128).

• **Subnets**: Number of subnets created if you're subnetting a /24 network.

• **Hosts/Subnet**: Number of usable host IP addresses in each subnet (excluding network and broadcast addresses).

Conclusion

- Subnetting is essential for organizing and managing IP networks.
- FLSM: Equal-size subnets
- VLSM: Custom-size subnets for better efficiency
- Use formulas and binary calculations for precise planning

Class C Network: 192.168.1.0



- **Addresses Available:**

- 192.168.1.0 - 192.168.1.255 (256 total)
- 192.168.1.1 - 192.168.1.254 are usable (254 usable)

- **Goal:**

- Need 4 separate network addresses for 4 company LANs

- **Solution:**

- Subnet the Network Address

- **How?**

- 256 Addresses to work with
- $256 / 4$ Subnets needed = 64 Addresses per Subnet

Subnet 1

0 to 63

Subnet 2

64 to 127

Subnet 3

129 to 191

Subnet 4

192 to 255

IP Sub-netting

Suppose there are 4 Departments A(23 Hosts), B(16), C(28), D(13). Given a network 202.70.64.0/24, perform sub-netting in such way that IP wastage in each sub-network is minimum. Find Subnet mask, N/W ID, Broadcast ID and usable host range for each network.

- Available Network is 202.70.64.0/24
- i.e. Total range of available IP addresses :
 - 202.70.64.0 – 202.70.64.255
- We proceed sub-netting with the department with highest no. of host i.e. C and then A, B and D respectively.

IP Sub-netting

For Dept. C (Start with network with maxm hosts)

- No. of hosts = 28
- For No. of bits required for host(Suffix) part (H),
 - $2^H - 2 \geq 28 \Rightarrow H = 5$ (Select minimum value of H)
 - ie. Total no. of IP addresses this n/w can provide = $2^5 = 32$
- No. of bits for Network(Prefix) part = $32 - 5 = 27$
- No. of Subnets that can be created = $2^{27-24} = 8$, which are given below:
- Available Subnets: 202.70.64.0/27 , 202.70.64.32/27, 202.70.64.64/27,
202.70.64.96/27 , 202.70.64.128/27, 202.70.64.160/27,
202.70.64.192/27 , 202.70.64.224/27
- Let us Select Subnet for C as 202.70.64.0/27, then,
- Subnet Mask = $255.255.255.[11100000] = 255.255.255.224$
- Network ID = 202.70.64.0 (The first ip address of network)
- Broadcast ID = 202.70.64.31 (The last ip address of network)
- Usable Host IP range = 202.70.64.1/27 – 202.70.64.30/27

IP Sub-netting

For Dept. A

- No. of hosts = 23
- For No. of bits required for host(Suffix) part (H),
 - $2^H - 2 \geq 23 \Rightarrow H = 5$ (Select minimum value of H)
 - ie. Total no. of IP addresses this n/w can provide = $2^5 = 32$
- No. of bits for Network(Prefix) part = $32 - 5 = 27$
- No. of Subnets that can be created = $2^{27-24} = 8$, which are given below: 202.70.64.0 / 27 is already used for Department C so cannot be used.
- Available Subnets: 202.70.64.32/27, 202.70.64.64/27, 202.70.64.96/27, 202.70.64.128/27, 202.70.64.160/27, 202.70.64.192/27, 202.70.64.224/27
- Let us Select Subnet for A as 202.70.64.32/27, then,
- Subnet Mask = $255.255.255.[11100000] = 255.255.255.224$
-
- Usable Host IP range = 202.70.64.33/27 – 202.70.64.62/27
- - Network ID = 202.70.64.32 (The first ip address of network)
 - Broadcast ID = 202.70.64.63 (The last ip address of network)

IP Sub-netting

- For Dept. B

- No. of hosts = 16
- For No. of bits required for host(Suffix) part (H),
 - $2^H - 2 \geq 16 \Rightarrow H = 5$ (Select minimum value of H)
 - ie. Total no. of IP addresses this n/w can provide = $2^5 = 32$
- No. of bits for Network(Prefix) part = $32 - 5 = 27$
- No. of Subnets that can be created = $2^{27-24} = 8$, which are given below:
202.70.64.0 / 27 and 202.70.64.32/27 are already used for Departments C and A, so cannot be used.
- Available Subnets: 202.70.64.64 / 27, 202.70.64.96/27, 202.70.64.128/27, 202.70.64.160 / 27, 202.70.64.192/27 , 202.70.64.224/27
- Let us Select Subnet for B as 202.70.64.64 / 27, then,
- Subnet Mask = 255.255.255.[11100000] = 255.255.255.224
- Network ID = 202.70.64.64 (The first ip address of network)
- Broadcast ID = 202.70.64.95 (The last ip address of network)
- Usable Host IP range = 202.70.64.65/27 – 202.70.64.94/27

IP Sub-netting

- For Dept. D

- No. of hosts = 13
- For No. of bits required for host(Suffix) part (H),
 - $2^H - 2 \geq 13 \Rightarrow H = 4$ (Select minimum value of H)
 - ie. Total no. of IP addresses this n/w can provide = $2^4 = 16$
- No. of bits for Network(Prefix) part = $32 - 4 = 28$
- No. of Subnets that can be created = $2^{28-24} = 16$
- (IP addresses upto 202.70.64.95 are already occupied)
- Let us Select Subnet for D as 202.70.64.96 / 28, then,
- Subnet Mask = 255.255.255.[11110000] = 255.255.255.240
- Network ID = 202.70.64.96 (The first ip address of network)
- Broadcast ID = 202.70.64.111 (The last ip address of network)
- Usable Host IP range = 202.70.64.97/28 – 202.70.64.110/28

#Assignment

1) A large number of consecutive IP addresses are available at 202.70.64.0/19. Suppose that four organization A, B, C, D request 100, 500, 800 and 400 addresses respectively. How the subnetting can be performed so that address wastage will be minimum ?

2) Baniya Bank need to allocate 15 IPs in HR department, 30 in finance Department, 24 in customer care unit and 25 in ATM machines. If you have one network of class C range public IP address. Describe how you will manage it ?

Classful Addressing

Classful addressing divides the IP address space into **fixed-size classes**. Each class has a default **subnet mask** and **range**.

Class	Starting Bits	Range (Decimal)	Default Subnet Mask	Hosts per Network
A	0xxxxxxx	1.0.0.0 – 126.255.255.255	255.0.0.0 (/8)	~16 million
B	10xxxxxx	128.0.0.0 – 191.255.255.255	255.255.0.0 (/16)	~65,000
C	110xxxxx	192.0.0.0 – 223.255.255.255	255.255.255.0 (/24)	254
D	1110xxxx	224.0.0.0 – 239.255.255.255	(Multicast)	-
E	1111xxxx	240.0.0.0 – 255.255.255.255	(Experimental)	-

Classless Addressing (CIDR – Classless Inter-Domain Routing)

Classless addressing does not use fixed classes. Instead, it uses a prefix length (e.g., /24, /16) to define the network and host portions.

CIDR Notation:

- Written as: IP address/prefix
- Example: 192.168.1.0/24
→ 24 bits for network, 8 bits for host.

Features:

- Efficient IP usage (no wastage).
- Flexible: You can divide and assign blocks as per need.
- Used for subnetting and supernetting.

Example:

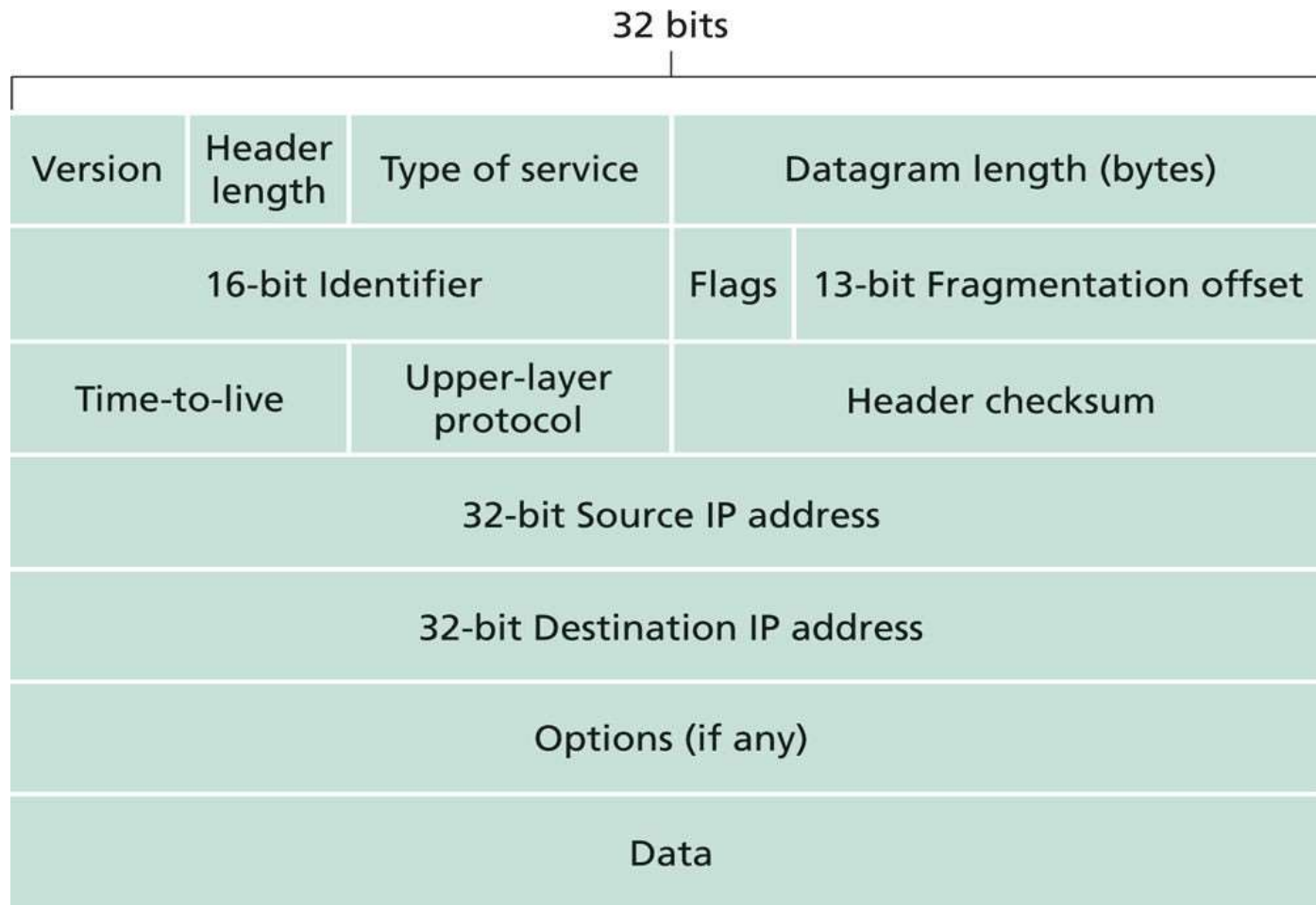
CIDR Notation	Subnet Mask	Hosts Available
/30	255.255.255.252	2 hosts
/24	255.255.255.0	254 hosts
/16	255.255.0.0	65,534 hosts

Classful Addressing Vs Classless Addressing

Feature	Classful Addressing	Classless Addressing
Based on Classes	Yes (A, B, C)	No
Subnet Mask	Fixed	Variable (customizable)
Flexibility	Low	High
IP Utilization	Inefficient (wasteful)	Efficient
Used in modern internet?	No (mostly outdated)	Yes (widely used today)

IPv4 Datagram Format

An **IPv4 datagram** is a packet of data that is transmitted over an **IPv4 (Internet Protocol version 4)** network.



IPV4 Datagram Format

- ***Version (4 bits):*** IP version (always 4 for IPv4)
- ***Header Length (4 bits):*** Because an IPV4 datagram can contain a variable number of options these four bits are needed to determine where in the IP datagram the data actually begins(minimum HLEN = 20 bytes).
- ***Type of Service (8 bits):*** TOS is included in the IPV4 header to allow different types of IP datagram(e.g. datagram particularly requiring low delay, high throughput, or reliability) to be distinguished from other. Eg. Realtime data requires fast delivery, file transfer requires reliability.
- ***Datagram Length(16 bits):*** contains the total length of datagram (Header+ Datagram)

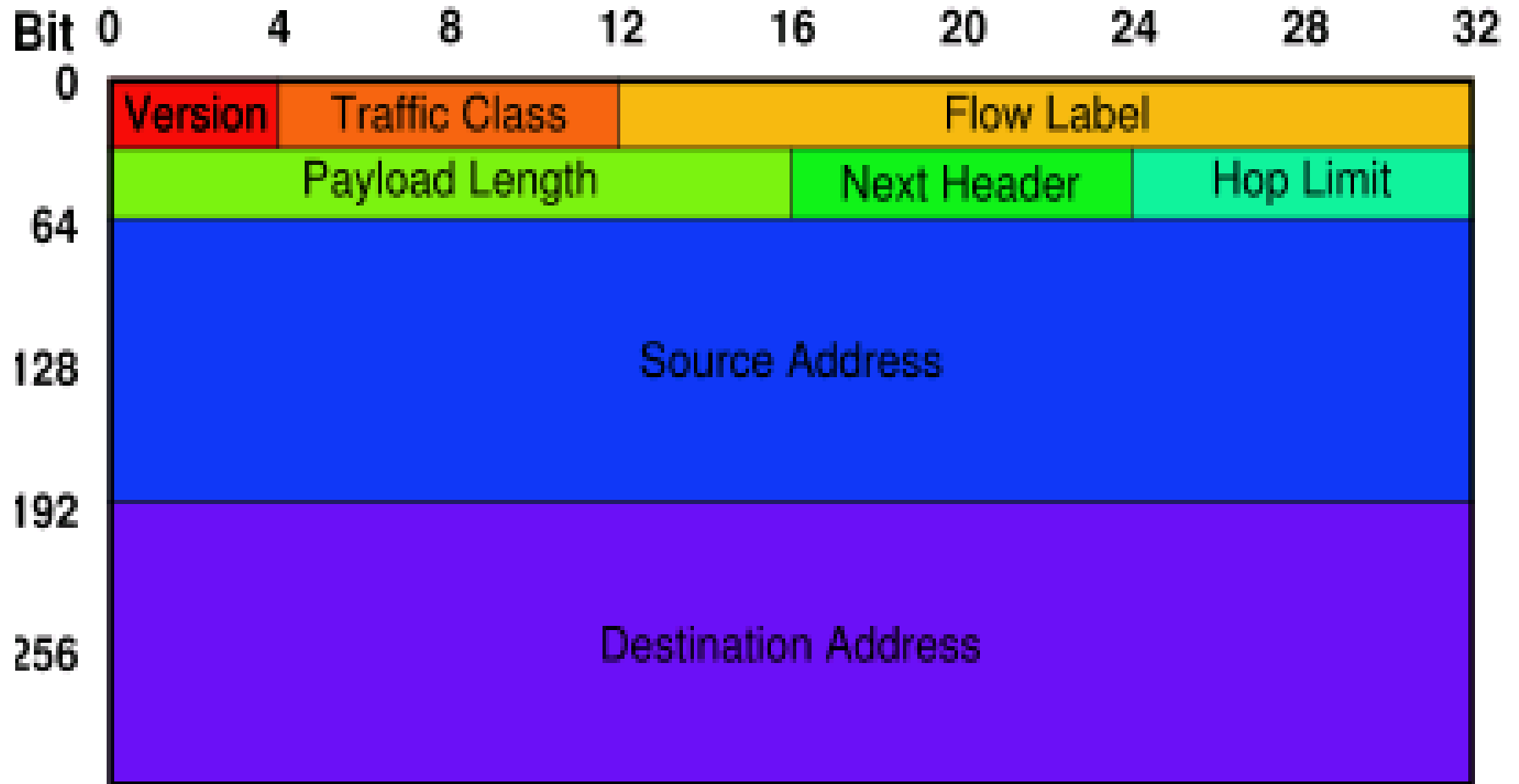
IPv4 Datagram Format

- ***Identifier, flag and Fragmentation offset*** : Used for identifying fragments of the same datagram.
- ***Time to Live (8 bits)*** : to ensure that the datagram don't circulate forever in the network. Limits Packet Life. In practice, just counts hops. Each router decrements the TTL and upon hitting 0, packet is discarded.
- ***Upper layer Protocol(8bits)***: The Protocol field in the IPv4 header is an 8-bit field that tells what kind of data (which protocol) is inside the datagram. In other words. It tells the IP layer which upper-layer protocol (like TCP, UDP, ICMP, etc.) should handle the payload.

IPV4 Datagram Format

- ***Header Check sum (16 bits)***: used to detect an error that may occur in the header.
- ***Source and Destination address***: Carries 32-bits source and destination address.
- ***Options***: used to identify several additional services, not used in every datagram.
- ***Data***: contains the user data.

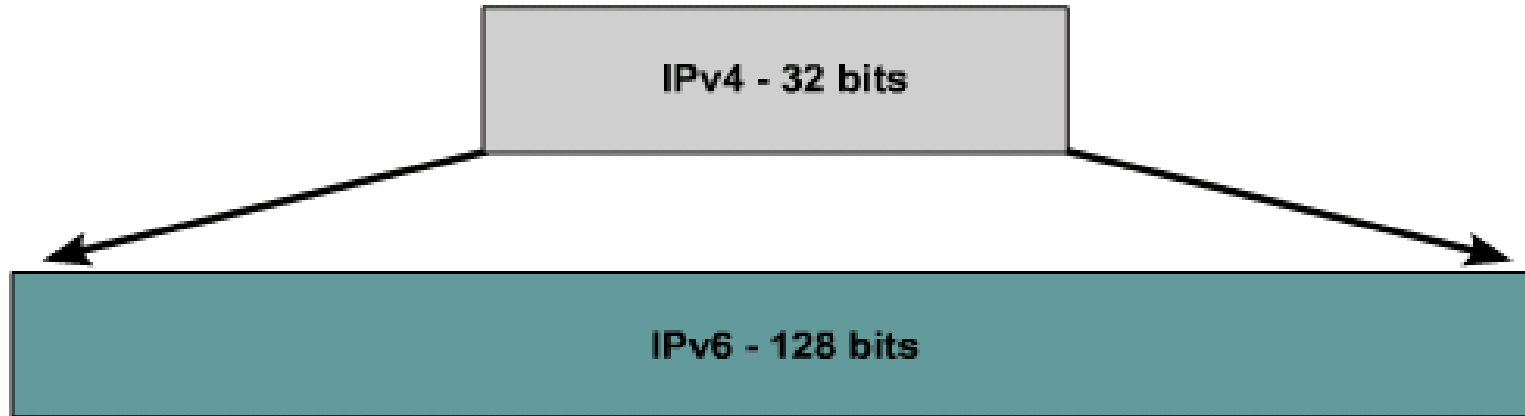
IPv6 Packet Format



IPv6 Packet Format

- **Version** – Always 6 for IPV6.
- **Traffic Class** - Similar to IPv4's Type of Service (used for priority and QoS)
- **Flow label** - Used to label packets in the same "flow" (for QoS)
- **Payload Length** - Length of the payload (excluding header)
- **Next Header** - Identifies the next header .
- **Hop Limit** - Same as TTL in IPv4; decrements at each router
- **Source Address** - IPv6 address of the sender.
- **Destination Address** - IPv6 address of the receiver.

IPv6: Large Address Space



IPv4

- 32 bits or 4 bytes long
 - $\approx 4,200,000,000$ possible addressable nodes

IPv6

- 128 bits or 16 bytes: four times the bits of IPv4
 - $\approx 3.4 \times 10^{38}$ possible addressable nodes
 - $\approx 340,282,366,920,938,463,374,607,432,768,211,456$
 - $\approx 5 \times 10^{28}$ addresses per person

IP Packet

An IP packet has two fundamental components:

- 1. IP header**

- contains many fields that are used by routers to forward the packet from network to network to a final destination.
- identify the sender, receiver, and transport protocol and define many other Parameters.





- 2. Payload**

- Represents the information (data) to be delivered to the receiver by the sender.
- Contains data & upper-layer information.

IPv4 vs IPv6 Header

IPv4 Header

Version	IHL	Type of Service	Total Length	
Indentification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options			Padding	

Legend		- Field names kept from IPv4 to IPv6
		- Fields not kept in IPv6
		- Name & position changed in IPv6
		- New field in IPv6

IPv6 Header

Version	Traffic Class	Flow Label		
Payload Length			Next Header	Hop Limit
Source Address				
Destination Address				

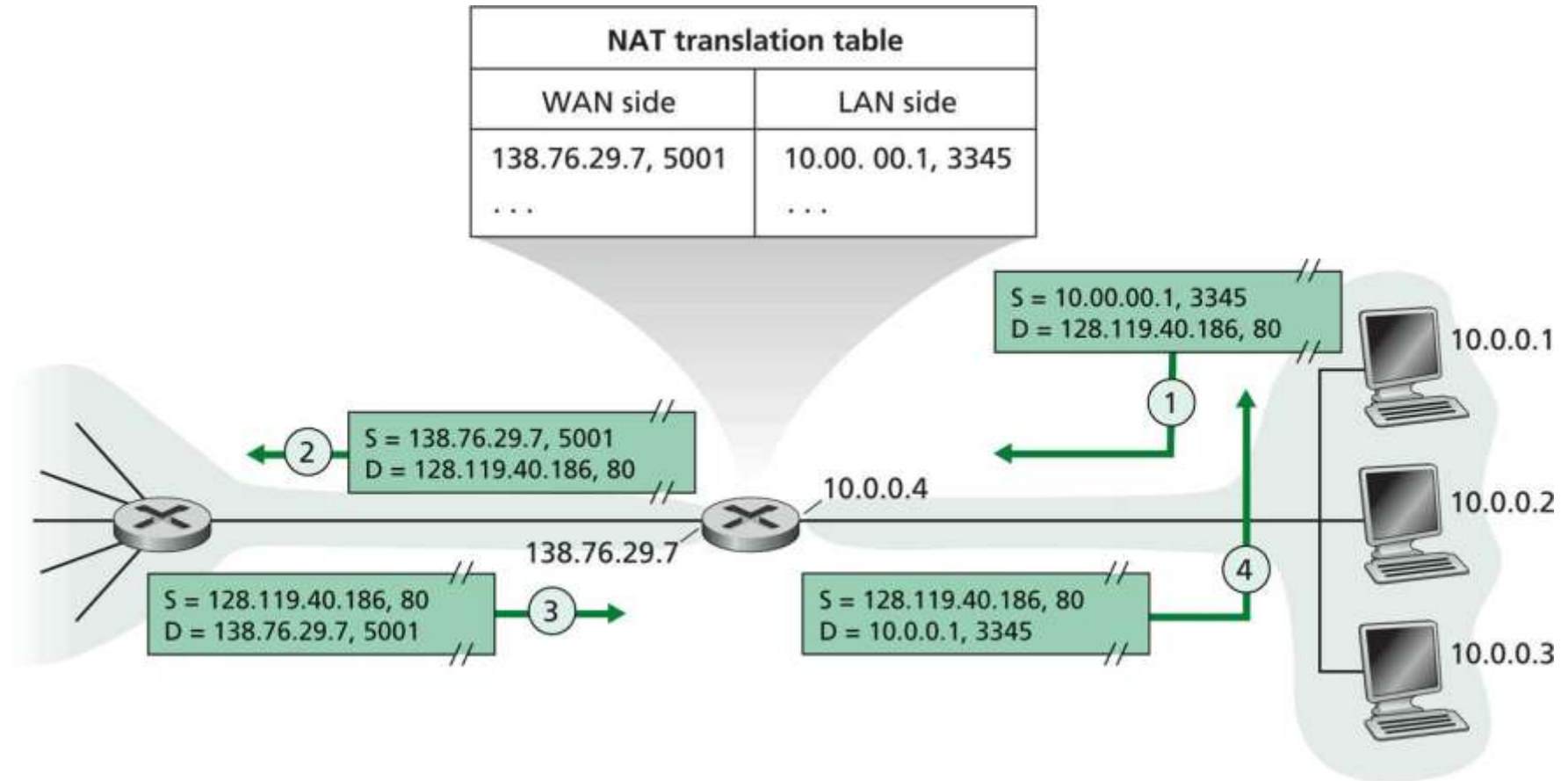
- **Limitations of IPv4**

- ☐ Address Space
- ☐ Various unnecessary and Variable header fields
- ☐ Fragmentation in Router
- ☐ Addressing Model
- ☐ NAT
- ☐ Broadcast Versus Multicast
- ☐ Quality of Service

- **Most important changes introduced in IPv6**

- ☐ Expanded addressing capabilities
- ☐ Size increases from 32 bits to 128 bits. This ensures that the IP address wouldn't run out of IP addresses.
- ☐ In addition to unicast and multicast addresses, it introduced anycast address, which allows a datagram to be delivered to any one of a group of hosts.
- ☐ A streamlined 40 bytes header
- ☐ Allows for faster processing of the IP datagram
- ☐ Flow labelling and priority
- ☐ Has an elusive definition of flow.(according to quality of service or real time service e.g. audio and video transfer).

Network Address Translation (NAT)



Network Address Translation (NAT)

Network Address Translation (NAT) is a process used in computer networks to modify the IP address information in IP packet headers while they are in transit across a router or firewall. NAT allows multiple devices on a private network to share a single public IP address when accessing the internet.

Why is NAT needed?

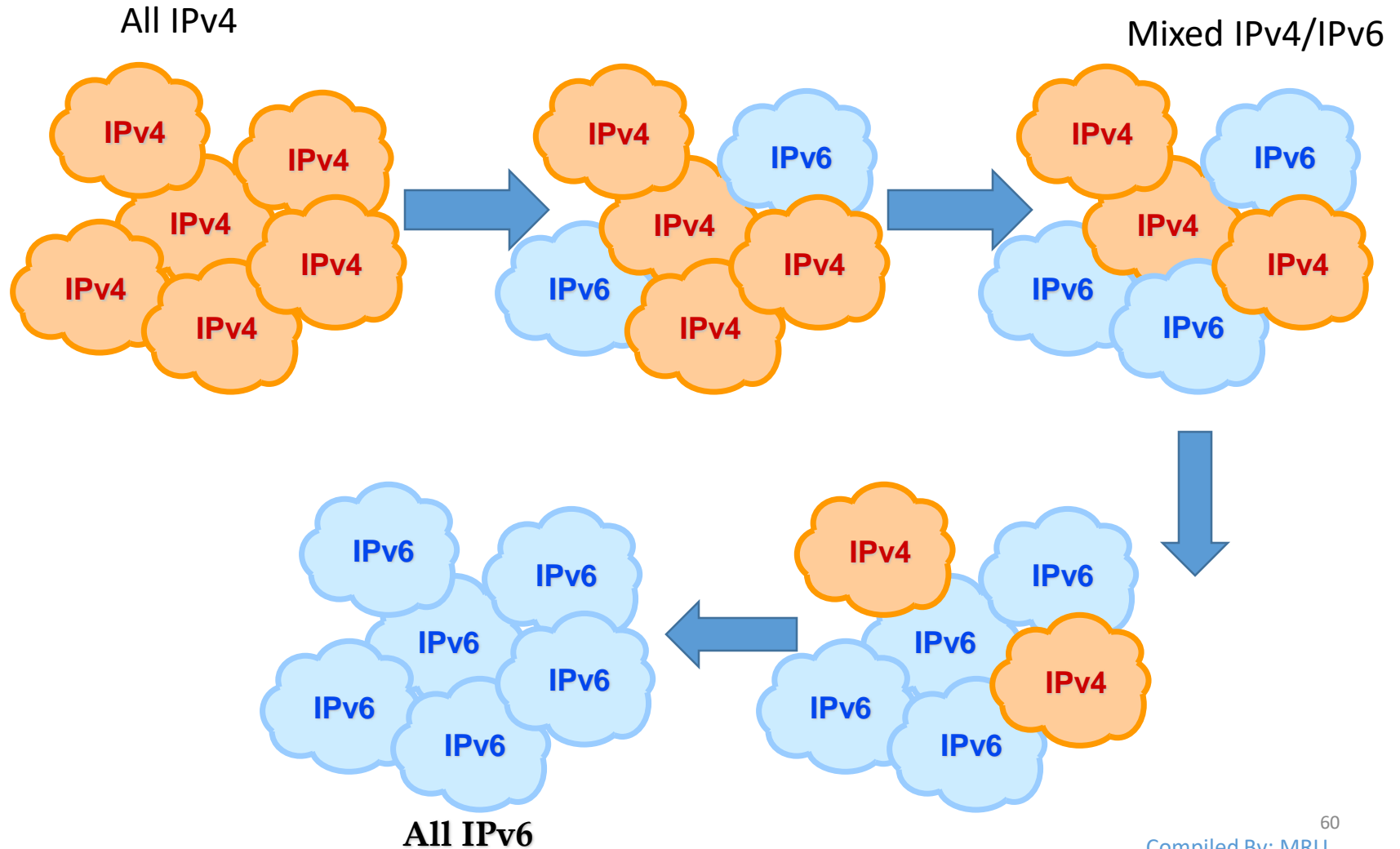
- **IPv4 address shortage:** There are limited IPv4 addresses, and NAT helps conserve them by allowing many devices to share one public IP.
- **Security:** NAT hides internal private IP addresses from the external network, providing a layer of security.
- **Simplifies IP management:** Private IPs can be reused inside different networks without conflict.

Network Address Translation (NAT)

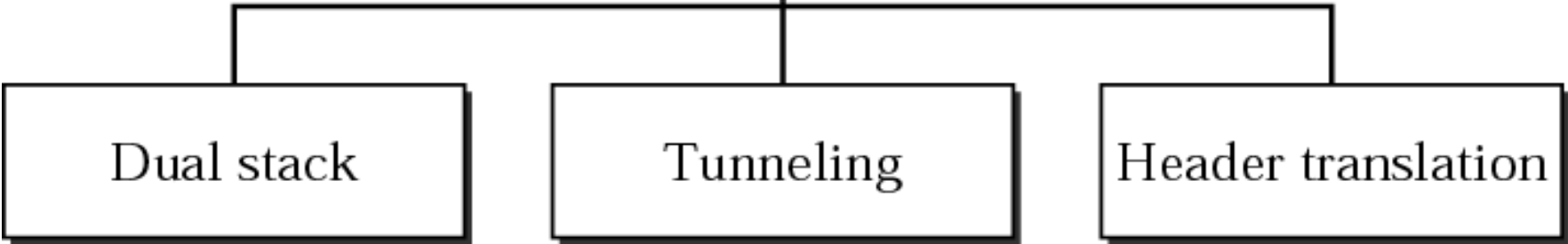
How NAT works:

- Devices inside a private network have private IP addresses (e.g., 192.168.x.x, 10.x.x.x).
- When a device wants to communicate with the internet, the NAT-enabled router translates the private IP to the router's public IP.
- The router keeps track of outgoing connections using **port numbers** so that responses can be routed back to the correct internal device.
- When the response arrives, the NAT device translates the public IP back to the private IP and forwards the packet inside.

Transition scenarios from IPv4 to IPv6



Transition
strategies



How Transition Happens From IPv4 to IPv6?

Various organizations are currently working with IPv4 technology and in a very short time, we can not switch directly from IPv4 to IPv6. Instead of only using IPv6, we use a combination of both and transition means not replacing IPv4 but co-existing of both.

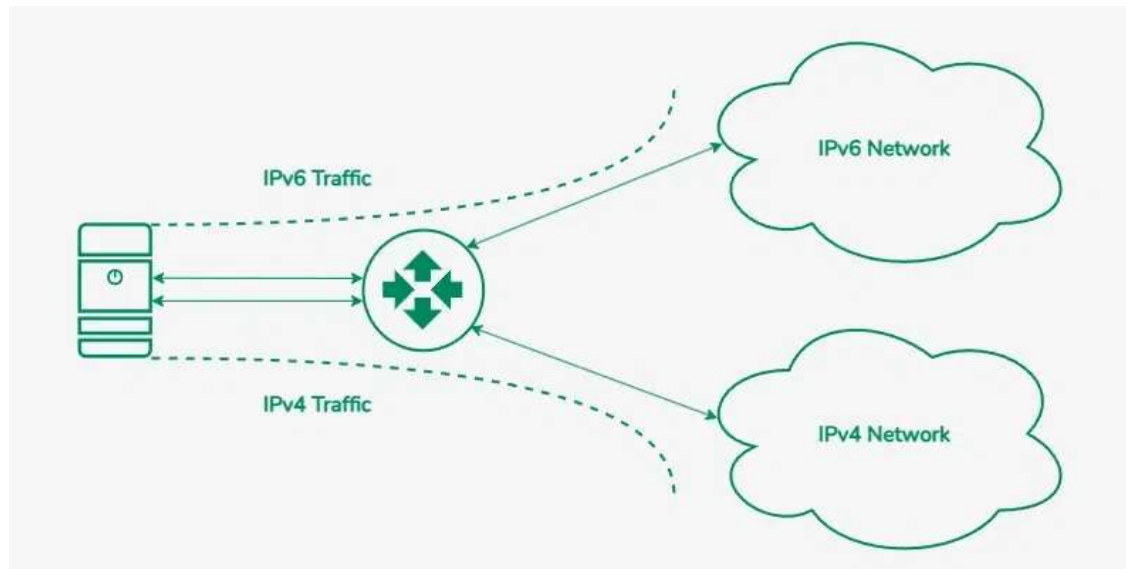
When we want to send a request from an IPv4 address to an IPv6 address, it is not possible because IPv4 and IPv6 transition is not compatible. For a solution to this problem, we use some technologies that help in an easy transition from IPv4 to IPv6. These technologies are mentioned below:

1. Dual Stack Routers
2. Tunneling
3. Header Translation

Dual stack

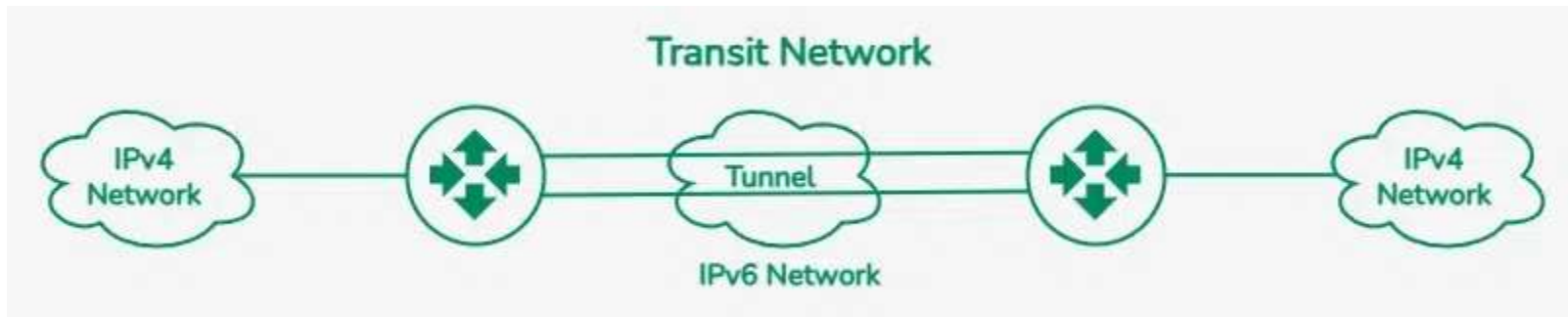
Dual-Stack Routers

A **dual-stack router** is a network device that can support both IPv4 and IPv6 protocols simultaneously. It allows communication between devices using any of the protocol, making it a key component during the transition from IPv4 to IPv6. In dual-stack router, A router's interface is attached with IPv4 and IPv6 addresses configured are used in order to transition from IPv4 to IPv6.



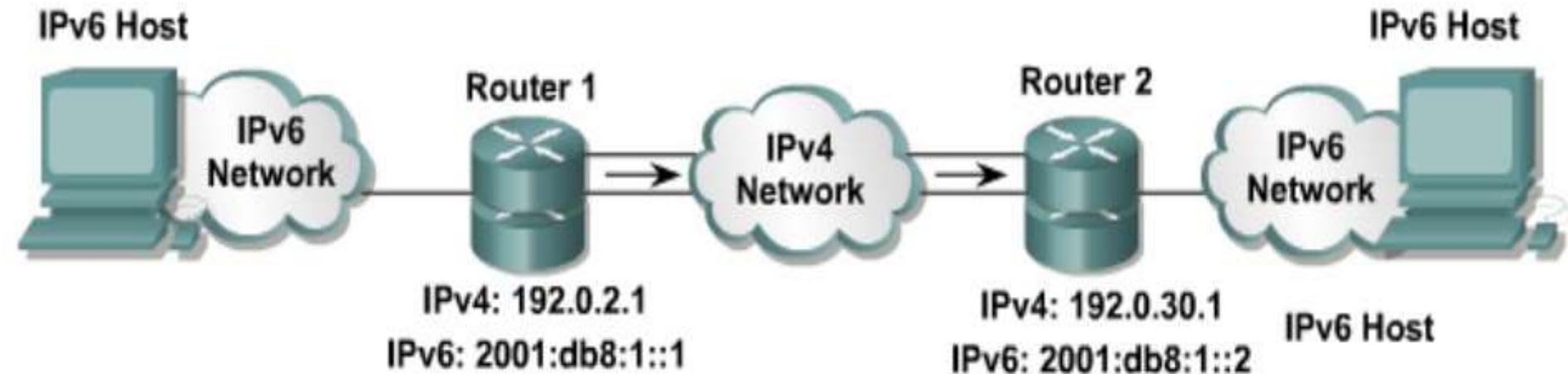
Tunneling

Tunneling is a technique used to enable communication between IPv4 and IPv6 networks during the transition from IPv4 to IPv6. **Tunneling** encapsulates IPv6 packets within IPv4 packets (or vice versa). Tunneling is used as a medium to communicate the transit network with the different IP versions.



Tunneling technique

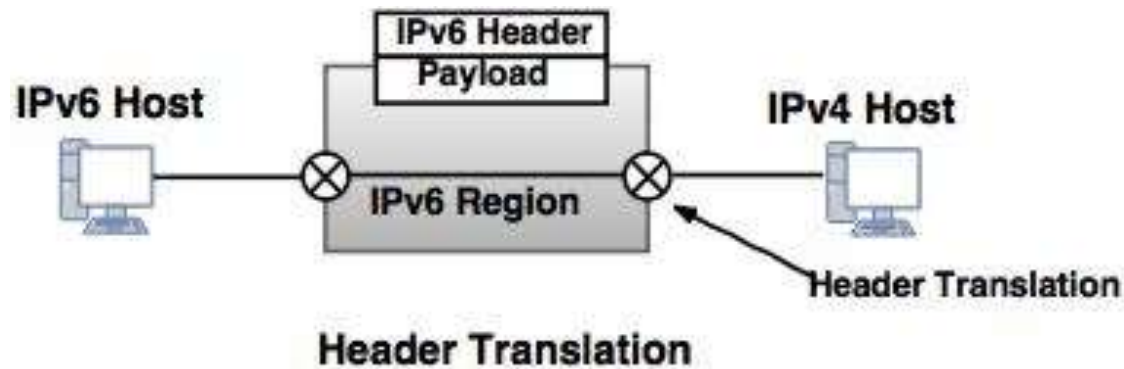
- With manually configured IPv6 tunnels, an IPv6 address is configured on a tunnel interface, and manually configured IPv4 addresses are assigned to the tunnel source and the tunnel destination. The host or router at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks.



Header translation

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

Header Translation changes the **packet header** from IPv6 to IPv4 or vice versa, allowing **direct communication between IPv4 and IPv6** devices. This is done using **protocol translation** techniques like **NAT64** and **DNS64**.



Header translation protocol

<i>Header Translation Procedure</i>	
1.	The IPv6 mapped address is changed to an IPv4 address by extracting the rightmost 32 bits.
2.	The value of the IPv6 priority field is discarded.
3.	Set the type of service field in IPv4 to zero.
4.	The checksum for IPv4 is calculated and inserted in the corresponding field.
5.	The IPv6 flow label is ignored.
6.	Compatible extension headers are converted to options and inserted in the IPv4 header.
7.	The length of IPv4 header is calculated and inserted into the corresponding field.
8.	The total length of the IPv4 packet is calculated and inserted in the corresponding field.

Datagram Fragmentation and Re-assembly

- MTU(Maximum Transfer Unit) is defined for a network link. Eg. MTU for Ethernet packet is usually 1500 bytes
- So, if data size is greater than MTU, it must be fragmented into smaller packet before transmitting to the link and
- re-assembled at receiver side to get original packet.
- In case of IPv4, Fragmentation is done at router just before the link with smaller MTU (where as, in case of IPv6, it must be done by the sender)
- For each Fragment, Header must be attached with Datagram ID, offset and Flag.

Datagram Fragmentation and Re-assembly

Datagram Size = 4000

Actual data size = 4000-20
= 3980 bytes

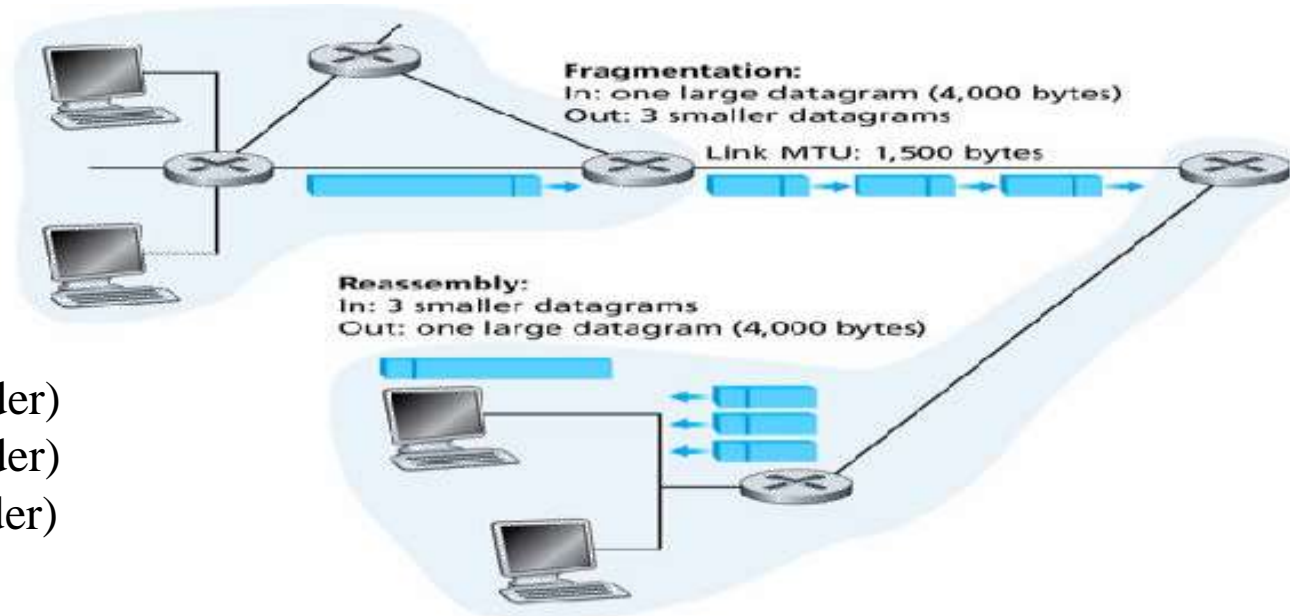
MTU = 1500 including 20
byte header

So fragmented packet size:

1st frag. : 1480 + 20 (Header)

2nd frag. : 1480 + 20 (Header)

3rd frag. : 1020 + 20 (Header)



Fragment	Bytes	ID	Offset	Flag (MF)
1st Fragment	1480 bytes in data field of IP Datagram	777 (eg.)	Offset = 0 (Beginning part)	MF = 1 (more fragments)
2st Fragment	1480 bytes in data field of IP Datagram	777	Offset = 1480 (beginning at byte 1480)	MF = 1 (more fragments)
3st Fragment	1020 bytes in data field of IP Datagram	777	Offset = 2960 (beginning at byte 2960)	MF = 0 (no more fragments)

ICMP (Internet Control Message Protocol)

- **ICMP** stands for **Internet Control Message Protocol**.
- It is an integral part of the **IP protocol suite** (used with **IPv4** and **IPv6**).
- ICMP is primarily used for **error reporting** and **diagnostic functions** in an IP network.
- It is **not used for sending data between systems**, but for sending **control messages** related to network operations

ICMP (Internet Control Message Protocol)

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

Note: Source Quench- It is used to tell a sender to slow down the rate of packet transmission.

ICMP Packet Format

Type(8 bit)	Code(8 bit)	Checksum(16 bit)
Extended Header(32 bit)		
Data/Payload(Variable Length)		

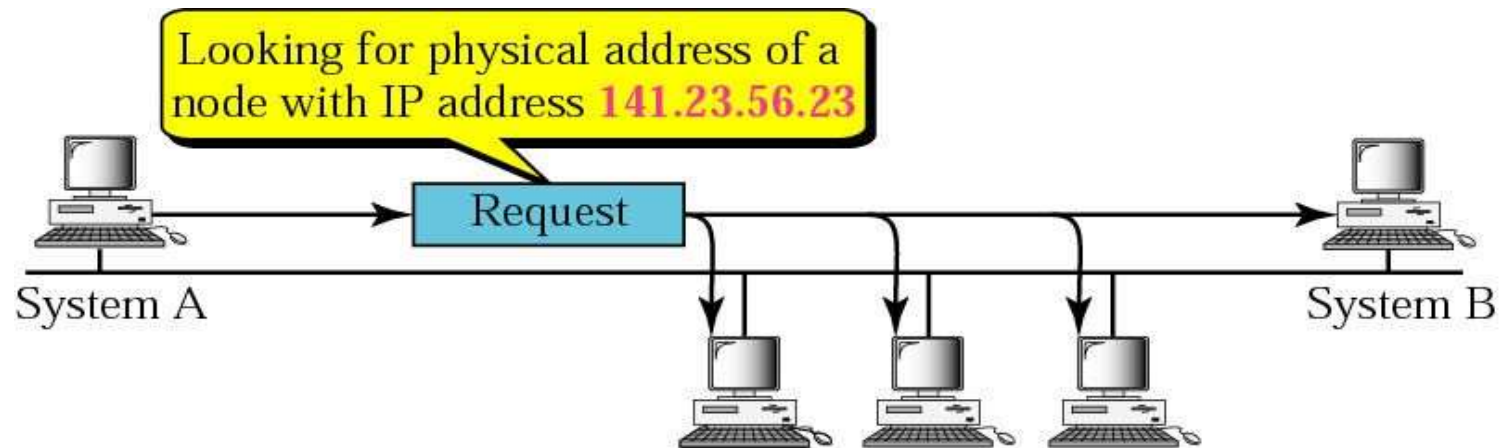
ICMP Packet Format

Field Name	Size (bits)	Description
Type	8 bits	Specifies the type of ICMP message (e.g., Echo Request = 8, Echo Reply = 0)
Code	8 bits	Provides further information about the Type (e.g., 0 = network unreachable, 1 = host unreachable)
Checksum	16 bits	Used for error-checking the ICMP message (like parity for errors)
Extended Header	32 bits	Varies depending on the Type and Code. For example: • Echo messages include an Identifier and Sequence Number • Error messages contain the IP header and first 8 bytes of the original packet

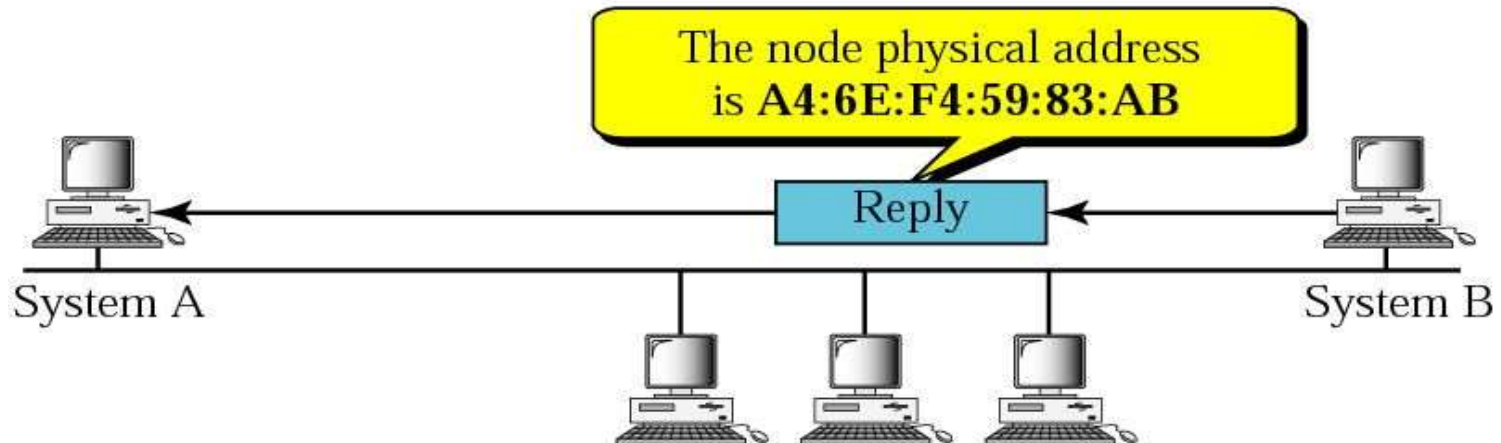
ARP (Address Resolution Protocol)

- In a local LAN, Computers communicates using MAC address.
- Sometimes it may so happen that Source knows IP address of destination, but not Physical address.
- In such Case, the source broadcasts an ARP packet asking for MAC address of computer with given IP.
- Obviously, IP will match with at most one host in network that will reply back with it's MAC address.
- ARP associates an IP address with its physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address that is usually imprinted on the NIC.

ARP (Address Resolution Protocol)



a. ARP request is broadcast

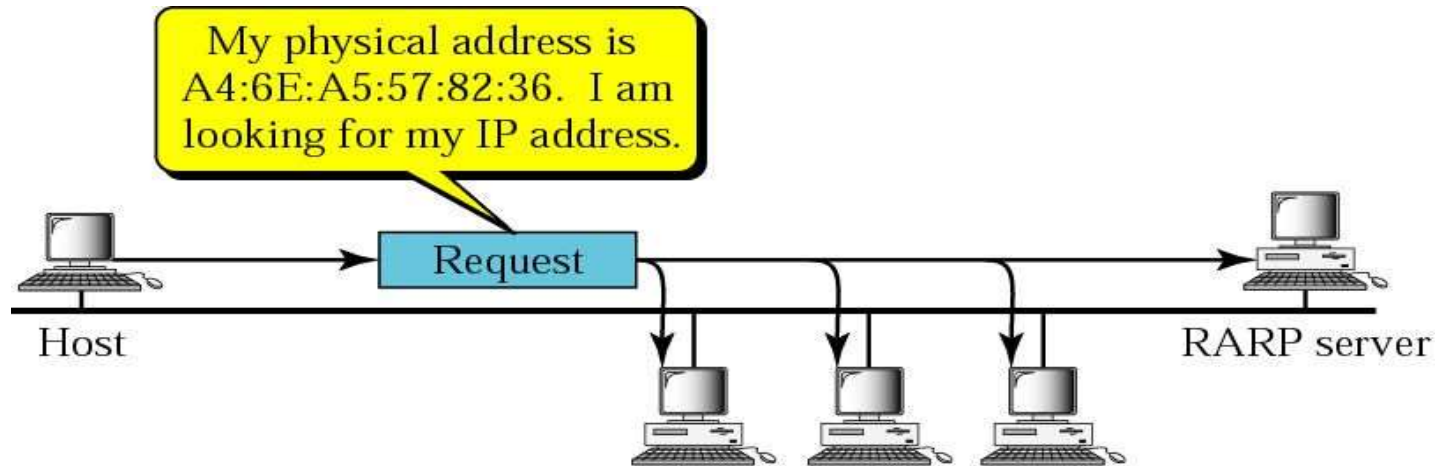


b. ARP reply is unicast

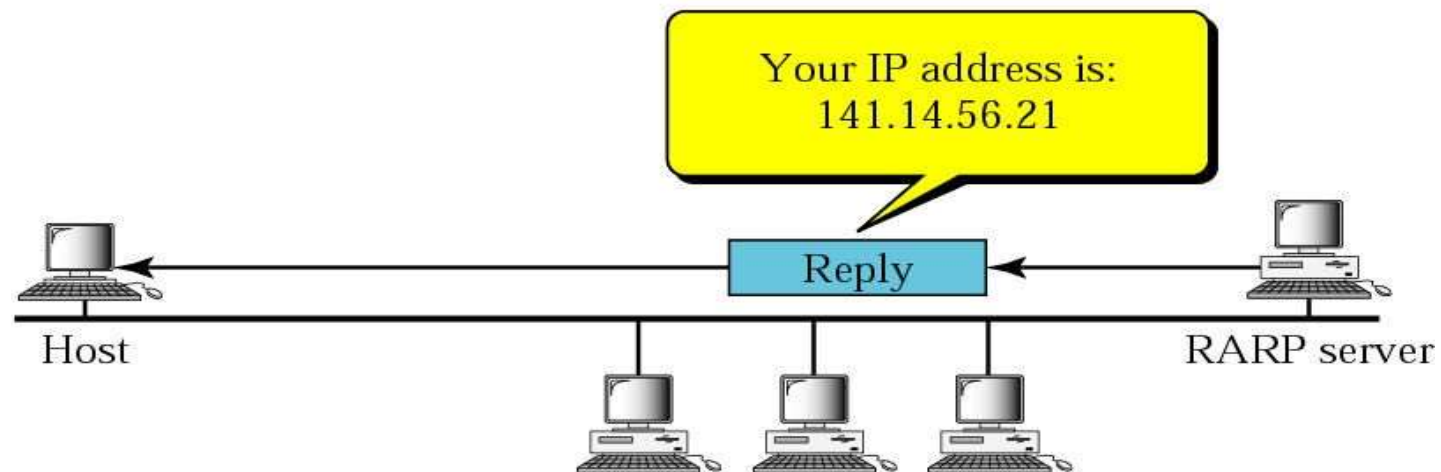
RARP (Reverse Address Resolution Protocol)

- Just a reverse of ARP
- RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache.
- A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses.
- When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.
- RARP requests are broadcast, RARP replies are unicast.
- DHCP have replaced RARP. RARP is now obsolete.

RARP (Reverse Address Resolution Protocol)



a. RARP request is broadcast



b. RARP reply is unicast

Routing

- **Routing** is the process of selecting paths in a network along which to send network traffic. It occurs at the **Network Layer (Layer 3)** of the OSI model and involves moving packets from source to destination across multiple networks.
- **Key Terms:**
 - Router:** A device that forwards packets between networks.
 - Routing Table:** A data table stored in a router that lists the routes to particular network destinations.
 - Hop:** A step from one router to the next in a path.

Routing Techniques

- **Routing Types**
 - Static Routing (Non-adaptive) Algorithm
 - Dynamic Routing (Adaptive) Algorithm
- **Routing Algorithms**
 - Shortest Path Algorithm
 - Flooding
 - Optimality Principle (Bellman's Principle)
 - Distance Vector Routing Algorithm
 - Link State Routing Algorithm
- **Routing Protocols**
 - RIP(Routing Information Protocol)
 - OSPF(Open Shortest Path First)
 - BGP(Border Gateway Protocol)

Autonomous System

- An Autonomous System (AS) is a group of network devices, such as routers, that are under a single administrative control and have a common routing policy.
- An Autonomous System (AS) is a collection of IP networks and routers under the control of a single organization, which follows a single, consistent routing policy.
- Each AS is assigned a unique Autonomous System Number (ASN) by a central authority (e.g., IANA or regional Internet registries like APNIC, ARIN, etc.).
- ASes are a fundamental building block of the internet's routing infrastructure, and they play a critical role in determining the paths that data takes as it travels across the internet. Within an AS, routing decisions are made based on the policies of the network administrator.

Routing

- Routing is the process of determining the best path for data to travel between two or more networked devices. When data is transmitted over a network, it is broken up into packets, each of which contains a destination address. The routing process determines the path that each packet should take to reach its destination.
- Different algorithms and protocols can be used to figure out how to best route data packets, and which nodes should be used.

- **Key Terms:**

Router: A device that forwards packets between networks.

Routing Table: A data table stored in a router that lists the routes to particular network destinations.

Hop: A step from one router to the next in a path.

- The following are the different types of routing:
 - Static Vs Dynamic Routing
 - Unicast Vs Multicast Routing
 - Interior Vs Exterior Routing
 - Link State Vs Distance Vector Routing

Static Vs Dynamic Routing

- Static routing is a method of configuring the network routing manually by the network administrator. In this method, the network administrator configures the routing table on each network device with static routes, which specify the next hop for data packets to travel to reach their destination.
- **Advantages –**
 - simple and efficient for small networks with a fixed topology that do not change frequently.
 - No routing overhead for router CPU which means a cheaper router can be used to do routing.
 - It adds security because only administrator can allow routing to networks only.
- **Disadvantage –**
 - For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
 - The administrator should have good knowledge of the topology. If a new administrator comes, then he must manually add each route so he should have very good knowledge of the routes of the topology.
 - Static routing does not adapt to changes in the network topology and requires manual intervention to update the routing table if changes occur, which can be time-consuming and error-prone.

Static Vs Dynamic Routing

- **Dynamic routing**, on the other hand, is a method of exchanging routing information automatically between network devices using routing protocols.
- In this method, the network devices exchange information about the network topology and use algorithms to calculate the best path for data packets to travel to their destination.
- Dynamic routing is more flexible than static routing and can adapt to changes in the network topology, such as the addition or removal of network devices or links, without requiring manual intervention.
- Examples of dynamic routing protocols include OSPF (Open Shortest Path First), BGP (Border Gateway Protocol), and RIP (Routing Information Protocol).

Static Vs Dynamic Routing

Feature	Static Routing	Dynamic Routing
Definition	Routes are manually configured by a network admin.	Routes are learned and updated automatically using routing protocols.
Configuration	Manual	Automatic via routing protocols (e.g., RIP, OSPF)
Routing Table Update	Only changes if the admin updates it	Updates dynamically based on network conditions
Protocols Used	No protocol needed	Uses RIP, OSPF, EIGRP, BGP, etc.
Scalability	Poor — hard to manage large networks	Good — suitable for large, complex networks
Security	More secure — no external updates	Less secure — vulnerable to route poisoning, spoofing
Maintenance	High — must update routes manually	Low — routes updated automatically

Unicast Vs Multicast Routing

- Unicast routing is a method of transmitting data packets from a single sender to a single receiver. In this method, the data packet is sent to a specific IP address, and the network devices along the way use routing protocols to forward the packet to its destination. This method is commonly used for communication between two devices, such as a web browser requesting a web page from a server.
- Multicast routing, on the other hand, is a method of transmitting data packets from a single sender to multiple receivers. In this method, the data packet is sent to a group of IP addresses, and the network devices along the way use multicast routing protocols to replicate and forward the packet to all the devices in the group. This method is commonly used for streaming media, such as video or audio, to multiple devices at the same time.

Unicast Vs Multicast Routing

Feature	Unicast Routing	Multicast Routing
Definition	Sends packets from one sender to one specific receiver (one-to-one).	Sends packets from one sender to multiple selected receivers (one-to-many).
Communication Type	One-to-one	One-to-many
Packet Delivery	One packet per destination	One packet sent once, duplicated by routers only when needed
Addressing	Uses unicast IP addresses (e.g., 192.168.1.1)	Uses multicast IP addresses (224.0.0.0 to 239.255.255.255)
Routing Table	Contains entries for each destination	Maintains multicast group membership info
Delivery Model	Direct packet delivery to a single IP	Packet replication happens at routers to reach group members

Interior Vs Exterior Routing

- **Interior routing** is a Routing mechanism which is used to find network path information within an Autonomous System. Known Interior Routing Protocols are Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), etc.
- **Exterior routing** is a Routing mechanism which is used to find network path information between different Autonomous Systems. Exterior Routing Protocols are commonly used on the Internet to exchange routing table information. There is only one Exterior routing protocol exists now and it is Border Gateway Protocol (BGP).

Interior Vs Exterior Routing

Feature	Interior Routing (IGP)	Exterior Routing (EGP)
Scope	Operates within a single Autonomous System (AS)	Operates between different Autonomous Systems (ASes)
Used By	Enterprises, ISPs (internally)	ISPs, large-scale Internet backbone providers
Routing Focus	Optimizes routing inside a network	Manages routing between networks on the Internet
Common Protocols	RIP, OSPF, EIGRP, IS-IS	BGP (Border Gateway Protocol)
Routing Control	Fully controlled by a single organization	Policy-based, partial control across different networks
Complexity	Simpler to manage	More complex, requires agreement between ASes

Popular Routing Algorithms

- A routing algorithm is a set of step-by-step operations used to direct Internet traffic efficiently.
- When a packet of data leaves its source, there are many different paths it can take to its destination.
- The routing algorithm is used to determine mathematically the best path to take.
- Dynamic routing algorithms are basically categorized as follows:
 - Shortest Path Algorithm: Bellman-Ford's algorithm and Dijkstra's Algorithm
 - Distance Vector Algorithm: Routing Information Protocol (RIP)
 - Link State Algorithm: Open Shortest Path First (OSPF)
 - Path Vector Algorithm: Border Gateway Protocol (BGP).

Thank You !