# Network Layer

Compiled By:

Hiranya Prasad Bastakoti

# Contents

- Introduction and Functions
- IPv4 Addressing
- Class-full and Classless Addressing
- IPv4 Sub-netting/ Super-netting
- IPv6 Addressing and its Features
- IPv4 and IPv6 Datagram Formats
- Comparison of IPv4 and IPv6 Addressing
- NATing
- Example Addresses Unicast, Multicast and Broadcast

# Contents

- Routing  Introduction and Definition
- Types of Routing  Static vs Dynamic, Unicast vs Multicast, Link State vs Distance Vector, Interior vs Exterior
- Path Computation Algorithms  Bellman Ford, Dijkstra's
- Routing Protocols :  RIP, OSPF & BGP
- Overview of IPv4 to IPv6 Transition Mechanisms
- Overview of ICMP/ICMPv6
- Overview of Network Traffic Analysis
- Security Concepts :  Firewall & Router Access Control

# Introduction to Network Layer

- The network layer is the third layer of the Open Systems Interconnection Model (OSI Model) and the layer that provides data routing paths for network communication.
- Data is transferred in the form of packets via logical network paths in an ordered format controlled by the network layer.
- Logical connection setup, data forwarding, routing and delivery error reporting are the network layer's primary responsibilities.
- The network layer involves each and every host and router in the network. The role of the network layer in a sending host is to begin the packet on its journey to the receiving host.
- Three important network-layer functions are:

- Path determination.:
- The network layer must determine the route or path taken by packets as they flow from a sender to a receiver. The algorithms that calculate these paths are referred to as routing algorithms.
- Switching:

When a packet arrives at the input to a router, the router must move it to the appropriate output link.

- Call setup:
- With TCP, a three-way handshake is required before data actually flow from sender to receiver. This allowed the sender and receiver to set up the needed state information (for example, sequence number and initial flow control window size).
- some network architectures require router call setup along path before data flows

# What is IP

- **IP** (Internet Protocol) is the primary network protocol used on the Internet, developed in the 1970s.
- An IP address is a unique global address for a network interface
- An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.
- An IP address serves two principal functions: host or network interface identification and location addressing
- On the Internet and many other networks, IP is often used together with the Transport Control Protocol (TCP) and referred to interchangeably as TCP/IP
- IP supports unique addressing for computers on a network. Most networks use the Internet Protocol version 4 (*IPv4*) standard that features IP addresses four bytes (32 bits) in length.
- The newer Internet Protocol version 6 (IPv6) standard features addresses 16 bytes (128 bits) in length.

# IPv4 addressing

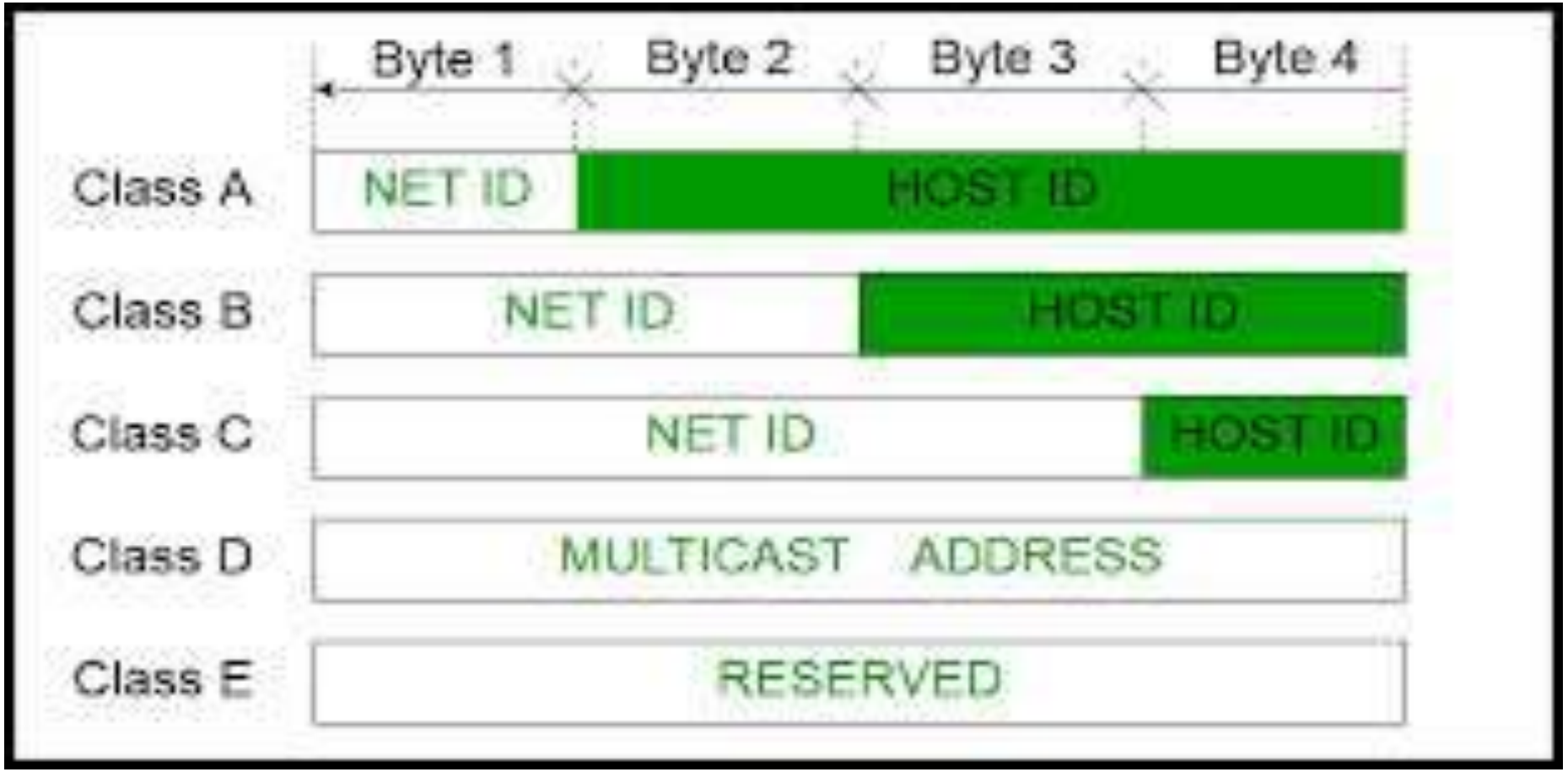
- *An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet*
- The IPv4 addresses are unique and universal.
- The address space of IPv4 is $2^{32}$ or 4,294,967,296
- IP address: 32-bit identifier for host, router *interface*
- *interface:* connection between host, router and physical link
  - router's typically have multiple interfaces
  - host may have multiple interfaces
  - IP addresses associated with interface, not host, or router.
- The **IP address** space is managed globally by the Internet **Assigned** Numbers Authority (IANA), and by five regional Internet registries (RIRs) responsible in their designated territories for **assignment** to end users and local Internet registries, such as Internet service providers

- IP address has two parts:
- The network prefix identifies a network and the host number identifies a specific host (actually, interface on the network)
  - network part :high order bits
  - host part :low order bits

Within the IPv4 address range , there are three types of addresses:

- **Network Address** - The address by which we refer to the network.
- **Broadcast Address** - A special address used to send data to all hosts in the network.
- **Host Address** - The addresses assigned to the end devices in the network.

# IPv4 Classful addresses



| Address Class | Bit Pattern of First Byte | First Byte Decimal Range | Host Assignment Range in Dotted Decimal |
|---|---|---|---|
| A | 0xxxxxxx | 1 to 127 | 1.0.0.1 to 126.255.255.254 |
| B | 10xxxxxx | 128 to 191 | 128.0.0.1 to 191.255.255.254 |
| C | 110xxxxx | 192 to 223 | 192.0.0.1 to 223.255.255.254 |
| D | 1110xxxx | 224 to 239 | 224.0.0.1 to 239.255.255.254 |
| E | 11110xxx | 240 to 255 | 240.0.0.1 to 255.255.255.255 |

| Class | IP Address Range (Theoretical) | Start-Bits | Application / Used for |
|---|---|---|---|
| A | 0.0.0.0 to 127.255.255.255 | 0 | Very large networks |
| B | 128.0.0.0 to 191.255.255.255 | 10 | Medium networks |
| C | 192.0.0.0 to 223.255.255.255 | 110 | Small networks |
| D | 224.0.0.0 to 239.255.255.255 | 1110 | Multicast |
| E | 240.0.0.0 to 247.255.255.255 | 1111 | Experimental |

**Class A Address**

- The first bit of the first octet is always set to zero. So that the first octet ranges from 1 – 127.
- The class A address only include IP starting from 1.x.x.x to 126.x.x.x. The IP range 127.x.x.x is reserved for loop back IP addresses.
- The default subnet mask for class A IP address is 255.0.0.0. This means it can have 126 networks ($2^7$-2) and 16777214 hosts ($2^{24}$-2).
- Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH.

**Class B Address**

- Here the first two bits in the first two bits is set to zero.
- 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 has 16384 ($2^{14}$) Network addresses and 65534 ($2^{16}$-2)
- Host addresses. Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

**Class C Address**

- The first octet of this class has its first 3 bits set to 110. 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 gives 2097152 ($2^{21}$) Network addresses and 254 ($2^{8}$-2)
- Host addresses. Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

**Class D Address**

- The first four bits of the first octet in class D IP address are set to 1110.
- 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 intended for a particular host, but multiple ones. That is why there is no need to extract host address from the class D IP addresses.
- The Class D does not have any subnet mask.

**Class E Address**

- The class E IP addresses are reserved for experimental purpose only for R&D or study.
- IP addresses in the class E ranges from 240.0.0.0 to 255.255.255.254.
- This class too is not equipped with any subnet mask.

# Summary

| Class | Leading bits | Size of *network number* bit field | Size of *rest* bit field | Number of networks | Addresses per network | Start address | End address |
|---|---|---|---|---|---|---|---|
| Class A very large network | 0 | 8 | 24 | 128 ($2^7$) | 16,777,216 ($2^{24}$) | 0.0.0.0 | 127.255.255.255 |
| Class B medium network | 10 | 16 | 16 | 16,384 ($2^{14}$) | 65,536 ($2^{16}$) | 128.0.0.0 | 191.255.255.255 |
| Class C small network | 110 | 24 | 8 | 2,097,152 ($2^{21}$) | 256 ($2^8$) | 192.0.0.0 | 223.255.255.255 |
| Class D (multicast) | 1110 | not defined | not defined | not defined | not defined | 224.0.0.0 | 239.255.255.255 |
| Class E (reserved) | 1111 | not defined | not defined | not defined | not defined | 240.0.0.0 | 255.255.255.255 |

# Classless Addressing

- **To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address.**
- **We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28.**
- **Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.**

# Classless Inter Domain Routing(CIDR)

- **CIDR is a new addressing scheme for the Internet which allows for more efficient allocation of IP addresses than the old Class A, B, and C address scheme.**
- **CIDR allowed for more efficient use of IPv4 address space and prefix aggregation, known as route summarization or supernetting.**

**CIDR introduction allowed for:**

- **More efficient use of IPv4 address space**
- **Prefix aggregation, which reduced the size of routing tables**

**CIDR allows routers to group routes together to reduce the bulk of routing information carried by the core routers. With CIDR, several IP networks appear to networks outside the group as** a single, larger entity.

- **CIDR is based on variable-length subnet masking (VLSM). This allows it to define prefixes of arbitrary lengths making it much more efficient than the old system. CIDR IP addresses are composed of two sets of numbers.**
- **With CIDR, IP addresses and their subnet masks are written as four octets, separated by periods, followed by a forward slash and a two-digit number that represents the subnet mask e.g.**
- **10.1.1.0/30**
- **172.16.1.16/28**
- **192.168.1.32/27 etc**
- **IP 10.0.0.0/24 equivalent to**

  **10.0.0.0-10.0.0.255(11111111.11111111.11111111.00000000)**

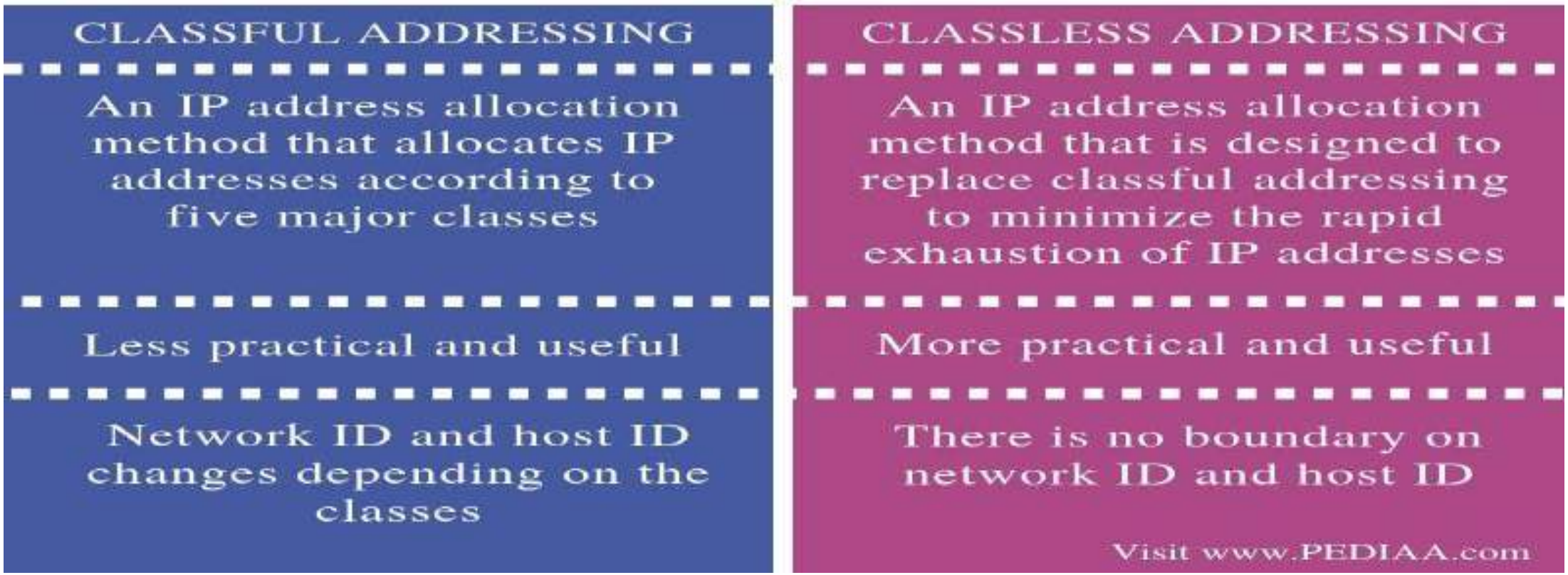
**Network mask equivalent to 255.255.255.0**

**The advantages of CIDR over the classful IP addressing are:**

**1. CIDR can be used to effectively manage the available IP address space.**

**2. CIDR can reduce the number of routing table entries**

# CLASSFUL ADDRESSING VERSUS CLASSLESS ADDRESSING



# Subnetting

- **IP Subnetting is a process of dividing a large IP network in smaller IP networks.**
- **In Subnetting we create multiple small manageable networks from a single large IP network.**
- **Subnetting is the process of breaking down an IP network into smaller sub-networks called “subnets.” Each subnet is a non-physical description (or ID) for a physical sub-network .**
- **Subnetting is a process of segmentation of a network id into multiple broadcast domains.**
- **Subnetting originally referred to the subdivision of a class-based network into many subnetworks, but now it generally refers to the subdivision of a CIDR block in to smaller CIDR blocks.**
- **Subnetting allows single routing entries to refer either to the larger block or to its individual constituents.**

# Advantages of Subnetting

- **Through subnetting, we can reduce network traffic and thereby improve network performance. we only allow traffic that should move to another network (subnet) to pass through the router and to the other subnet.**
- **Subnettiing can be used to restrict broadcast traffic on the network.**
- **Subnetting facilitates simplified management. we can delegate control of subnets to other administrators.**
- **Troubleshooting network issues is also simpler when dealing with subnets than it is in one large network**.

# Subnet Mask

- **An IP address has two components, the network address and the host address. A subnet mask separates the IP address into the network and host addresses.**
- **A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s.**

**Class A**
Subnet Mask

| Netwok | Host | Host | Host |
|---|---|---|---|
| 255 | 0 | 0 | 0 |

**Class B**
Subnet Mask

| Netwok | Network | Host | Host |
|---|---|---|---|
| 255 | 255 | 0 | 0 |

**Class C**
Subnet Mask

| Netwok | Network | Network | Host |
|---|---|---|---|
| 255 | 255 | 255 | 0 |

www.smartPCtricks.com

# CIDR and Subnet Mask

| CIDR | Subnet Mask | CIDR | Subnet Mask |
|---|---|---|---|
| /8 | 255.0.0.0 | /21 | 255.255.248.0 |
| /9 | 255.128.0.0 | /22 | 255.255.252.0 |
| /10 | 255.192.0.0 | /23 | 255.255.254.0 |
| /11 | 255.224.0.0 | /24 | 255.255.255.0 |
| /12 | 255.240.0.0 | /25 | 255.255.255.128 |
| /13 | 255.248.0.0 | /26 | 255.255.255.192 |
| /14 | 255.252.0.0 | /27 | 255.255.255.224 |
| /15 | 255.254.0.0 | /28 | 255.255.255.240 |
| /16 | 255.255.0.0 | /29 | 255.255.255.248 |
| /17 | 255.255.128.0 | /30 | 255.255.255.252 |
| /18 | 255.255.192.0 | /31 | 255.255.255.254 |
| /19 | 255.255.224.0 | /32 | 255.255.255.255 |
| /20 | 255.255.240.0 | | |

# Class C Subnetting

| # of Subnets | # of Hosts/Subnet | NetMask | 4th Octet | CIDR Notation |
|---|---|---|---|---|
| 2 | 126 | 255.255.255.128 | 10000000 | /25 |
| 4 | 62 | 255.255.255.192 | 11000000 | /26 |
| 8 | 30 | 255.255.255.224 | 11100000 | /27 |
| 16 | 14 | 255.255.255.240 | 11110000 | /28 |
| 32 | 6 | 255.255.255.248 | 11111000 | /29 |
| 64 | 2 | 255.255.255.252 | 11111100 | /30 |

# Subnetting Steps

- Let's  use the IP address **192.168.10.44** with subnet mask **255.255.255.248 (/29).**

**1.Total number of subnets:** Using the subnet mask 255.255.255.248, number value 248 (11111000) indicates that 5 bits are used to identify the subnet. To find the total number of subnets available simply raise **2 to the power of 5 (2^5)** and you will find that the result is **32 subnets**.

**2.Hosts per subnet:** 3 bits are left to identify the host therefore the total number of hosts per subnet is **2 to the power of 3 minus 2** (1 address for subnet address and another one for the broadcast address)**(2^3-2)** which equals to **6** hosts per subnet.

**3. Subnets, hosts and broadcast addresses per subnet:** To find the valid subnets for this specific subnet mask you have to **subtract 248 from the value 256 (256-248=8)** which is the first available subnet address.

Next subnet address is 8+8=**16**, next one is 16+8=**24** and this goes on until we reach value 248. The following table provides all the calculated information.

- Example:255.255.255.224/27
- Network address=192.168.10.0
- Subnet Mask=255.255.255.224
- Subnet ?224 binary=11100000,2^3=8
- Host?2^5-2=30
- Valid subnet ?256-224=32.32,64,96……224
- Subnet: 32 64 96 128 160 192
- First Host: 33 65 97 129 161 193
- Last Host: 62 94 126 258 190 222
- Broadcast: 63 95 127 259 191 223

our IP address (192.168.10.44) lies in subnet 192.168.10.40.

| Subnet | 0 | 8 | 16 | ... | 40 | ... | 248 |
|---|---|---|---|---|---|---|---|
| First Host | 1 | 9 | 17 | ... | 41 | ... | 249 |
| Last Host | 6 | 14 | 22 | ... | 46 | ... | 254 |
| Broadcast | 7 | 15 | 23 | ... | 47 | ... | 255 |

- Example:255.255.255.248/29
- Network address=192.168.10.0
- Subnet Mask=255.255.255.248
- Subnet ?248 binary=11111000,2^5=32
- Host?2^3-2=6
- Valid subnet ?256-248=8,16,24……240
- Subnet: 8 16 24 ……224 232 240..248
- First Host: 9 17 25……225 233 241
- Last Host: 14 22 30……230 238 246
- Broadcast: 15 23 31……231 239 247

- Example:255.255.192.0/18
- Network address=172.16.10.0
- Subnet Mask=255.255.192.0
- Subnet ?192 binary=11000000,2^2-2=2
- Host?2^14-2=16,382
- Valid subnet ?256-192=64,64 ,64+64=128
- Subnet: 64 128
- First Host: 64.1 128.1
- Last Host: 127.254 191.254
- Broadcast: 127.255 191.255

- Example:255.255.240.0/20
- Network address=172.16.0.0
- Subnet Mask=255.255.240.0
- Subnet ?240 binary=11110000,2^4=16
- Host?2^12-2=4094
- Valid subnet ?256-240=16.16,32 ,48….224
- Subnet: 16 32 48… 224
- First Host: 16.1 32.1 48.1
- Last Host: 31.254 47.254 63.254
- Broadcast: 31.255 47.255 63.255

Example using the Class C mask of 255.255.255.240. Here are the answers:

- How many subnet bits are used in this mask?

Answer: 4 bits or 2^4-2=14 subnets

- How many host bits are available per subnet?

Answer: 4 bits or 2^4-2=14 hosts per subnet

- What are the subnet addresses?

Answer: 256-240 =16, 32, 48, 64, 80, 96, 112, 128, 144. 160, 176, 192, 208 and 224 (14 subnets found by continuing to add 16 to itself.)

- What is the broadcast address of each subnet?

Answer: Here are some examples of the broadcast address: The broadcast address for the 16 subnet is 31. The broadcast address for the 32 subnet is 47. The broadcast address for the 64 subnet is 79. The broadcast address for the 96 subnet is 111. The broadcast address for the 160 subnet is 175. The broadcast address for the 192 subnet is 207.

- What is the valid host range of each subnet?

Answer: The valid hosts are the numbers in between the subnet and broadcast addresses. The 32 subnet valid hosts are 33-46.

Example: 255.255.255.192:

- How many subnet bits are used in this mask?

Answer: 2 2^2-2=2 subnets

- How many host bits are available per subnet?

Answer: 6 2^6-2=62 hosts per subnet

- What are the subnet addresses?

Answer: 256-192=64 (the first subnet)64+64=128 (the second subnet)64+128=192. However, although 192 is the subnet mask value, it's not a valid subnet. The valid subnets are 64 and 128.

- What is the broadcast address of each subnet?

Answer: 64 is the first subnet and 128 is the second subnet. The broadcast address is always the number before the next subnet. The broadcast address of the 64 subnet is 127. The broadcast address of the 128 subnet is 191.

- What is the valid host range of each subnet?

Answer: The valid hosts are the numbers between the subnet number and the mask. For the 64 subnet, the valid host range is 64-126. For the 128 subnet, the valid host range is 129-190.

# IPv6 Address

- IPv6 is short for "Internet Protocol Version 6". IPv6 is the Internet's next-generation protocol, designed to replace the current Internet Protocol, IP Version 4.
- Internet Protocol Version 6 (IPv6) is a network layer protocol that enables data communications over a packet switched network. Packet switching involves the sending and receiving of data in packets between two nodes in a network.
- The most important feature of IPv6 is a much larger address space than in IPv4. IPv6 addresses are 128 bits long, compared to only 32 bits previously.
- While the IPv4 address space contains only about 4.3 billion addresses, IPv6 supports approximately 340 undecillion (3.4×10^38) unique addresses, deemed enough for the foreseeable future.

# IPv6 Address:Categories

1.Unicast addresses :used for one-to-one communication. A unicast address identifies a single network interface. The protocol delivers packets sent to a unicast address to that specific interface.

There are 3 types of unicast addresses namely global, unique-local and link-local

2.Multicast addresses :used for one-to-many communication. Multicast address is also assigned to a set of interfaces that typically belong to different nodes. A packet that is sent to a multicast address is delivered to all interfaces identified by that address. Multicast addresses are easily identifiable because the value of a IPv6 multicast address begins with "FF

3.Anycast addresses :used for one-to-one-of-many communication An anycast address is assigned to a group of interfaces, usually belonging to different nodes. A packet sent to an anycast address is delivered to just one of the member interfaces, typically the “nearest” according to the routing protocol’s choice of distance.

# IPv6 Address Notation

- IPv6 addresses are denoted by eight groups of hexadecimal quartets separated by colons in between them.

  Following is an example of a valid IPv6 address:
  2001:cdba:0000:0000:0000:0000:3257:9652

  Any four-digit group of zeroes within an IPv6 address may be reduced to a single zero or altogether omitted. Therefore, the following IPv6 addresses are similar and equally valid:

  2001:cdba:0000:0000:0000:0000:3257:9652
  2001:cdba:0:0:0:0:3257:9652
  2001:cdba::3257:9652

# Features of IPv6

1 IPv6 provides better end-to-end connectivity than IPv4.

2) Comparatively faster routing.

3) IPv6 offers ease of administration than IPv4.

4) More security for applications and networks.

5) It provides better Multicast and Anycast abilities.

6) Better mobility features than IPv4.

7) IPv6 follows the key design principles of IPv4 and so that the transition from IPv4 to IPv6 is smoother.

# Features of IPV6

**New Header Format**

- The IPv6 header has a new format designed to minimize header overhead and this optimization is achieved by moving both non-essential fields and optional fields to extension headers that appear after the IPv6 header.
- IPv4 headers and IPv6 headers do not interoperate. IPv6 is not a superset of functionality that is backward compatible with IPv4. A host or router must use an implementation of both IPv4 and IPv6 to recognize and process both header formats. The IPv6 header is only twice as large as the IPv4 header, even though IPv6 addresses are four times as large as IPv4 addresses.

**Larger Address Space**

- IPv6 has 128-bit (16-byte) source and destination IP addresses. Although 128 bits can express over 3.4×1038 possible combinations, the large address space of IPv6 has been designed for multiple levels of subnetting and address allocation from the Internet backbone to the individual subnets within an organization.
- With a much larger number of available addresses, address-conservation techniques, such as the deployment of NATs, are no longer necessary.

**Efficient and Hierarchical Addressing and Routing Infrastructure**

- IPv6 global addresses that are used on the IPv6 portion of the Internet are designed to create an efficient, hierarchical, and summarizable routing infrastructure that is based on the common occurrence of multiple levels of Internet service providers.

### Stateless and Stateful Address Configuration

- To simplify host configuration, IPv6 supports both stateful address configuration (as in the presence of a DHCP server) and stateless address configuration (as in the absence of a DHCP server).
- With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link (called link-local addresses) and with addresses that they derive from prefixes that local routers advertise. Even in the absence of a router, hosts on the same link can configure themselves with link-local addresses and communicate without manual configuration.

### Built-in Security

- The IPv6 protocol suite requires support for IPSec. This requirement provides a standards-based solution for network security needs and promotes interoperability between different IPv6 implementations.

### Better Support for QoS

- New fields in the IPv6 header define how traffic is handled and identified. Traffic identification (using a Flow Label field in the IPv6 header) allows routers to identify and provide special handling for packets belonging to a flow, which is a series of packets between a source and a destination. Because the IPv6 header identifies the traffic, QoS can be supported even when the packet payload is encrypted through IPSec.

## New Protocol for Neighboring Node Interaction

- The Neighbor Discovery protocol for IPv6 is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manage the interaction of nodes on the same link (known as neighboring nodes). Neighbor Discovery replaces the broadcast-based Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast Neighbor Discovery messages.

## Extensibility

- IPv6 can easily be extended by adding extension headers after the IPv6 header. Unlike options in the IPv4 header, which can support only 40 bytes of options, the size of IPv6 extension headers is constrained only by the size of the IPv6 packet.

# Comparision Between IPv4 and IPv6

| | |
|---|---|
| IPv4 has 32-bit address length | IPv6 has 128-bit address length |
| It Supports Manual and DHCP address configuration | It supports Auto and renumbering address configuration |
| In IPv4 end to end connection integrity is Unachievable | In IPv6 end to end connection integrity is Achievable |
| It can generate $4.29\times10^{9}$ address space | Address space of IPv6 is quite large it can produce $3.4\times10^{38}$ address space |
| Security feature is dependent on application | IPSEC is inbuilt security feature in the IPv6 protocol |
| Address representation of IPv4 in decimal | Address Representation of IPv6 is in hexadecimal |
| Fragmentation performed by Sender and forwarding routers | In IPv6 fragmentation performed only by sender |

| | |
|---|---|
| In IPv4 Packet flow identification is not available | In IPv6 packet flow identification are Available and uses flow label field in the header |
| In IPv4 checksum field is available | In IPv6 checksum field is not available |
| It has broadcast Message Transmission Scheme | In IPv6 multicast and any cast message transmission scheme is available |
| In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication are provided |

# Key Differences between IPv4 and IPv6

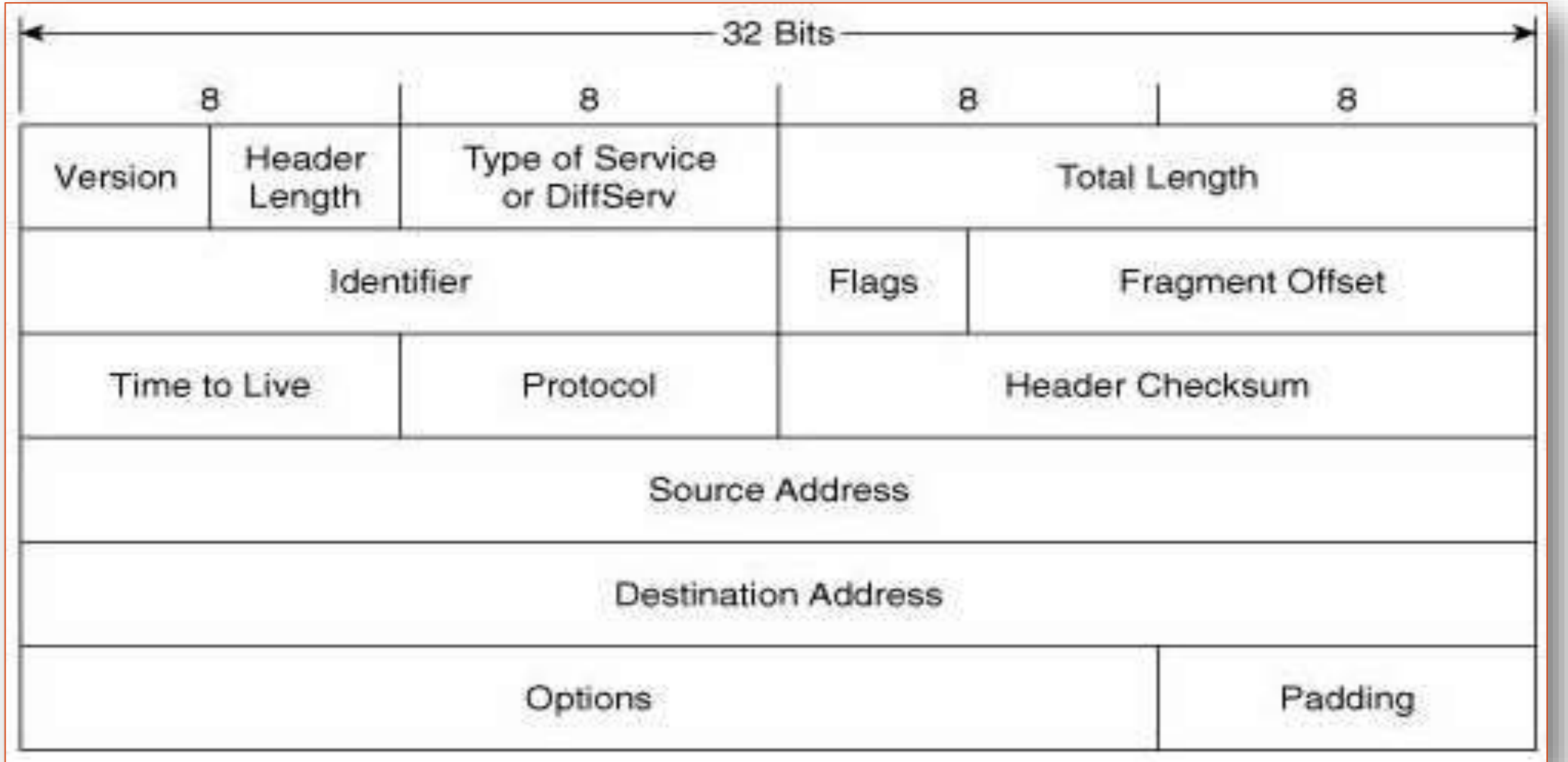
- IPv4 has 32-bit address length whereas IPv6 has 128-bit address length.
- IPv4 addresses represent the binary numbers in decimals. On the other hand, IPv6 addresses express binary numbers in hexadecimal.
- IPv6 uses end-to-end fragmentation while IPv4 requires an intermediate router to fragment any datagram that is too large.
- Header length of IPv4 is 20 bytes. In contrast, header length of IPv6 is 40 bytes.
- IPv4 uses checksum field in the header format for handling error checking. On the contrary, IPv6 removes the header checksum field.
- In IPv4, the base header does not contain a field for header length, and 16-bit payload length field replaces it in the IPv6 header.
- The option fields in IPv4 are employed as extension headers in IPv6.
- The Time to live field in IPv4 refers to as Hop limit in IPv6.
- The header length field which is present in IPv4 is eliminated in IPv6 because the length of the header is fixed in this version.
- IPv4 uses broadcasting to transmit the packets to the destination computers while IPv6 uses multicasting and anycasting.
- IPv6 provides authentication and encryption, but IPv4 doesn’t provide it.

# IPv4 Datagram Formats

An IPv4 datagram is a variable-length packet comprised of a header (20 bytes) and data (up to 65,536 along with header). The header contains information essential to routing and delivery.

**Version:** It defines the version number of IP, i.e., in this case, it is 4 with a binary value of 0100.
**Header length (HLEN):** It represents the length of the header in multiple of four bytes.
**Service type:** It determines how datagram should be handled and includes individual bits such as level of throughput, reliability, and delay.
**Total length:** It signifies the entire length of the IP datagram.
**Identification:** This field is used in fragmentation. A datagram is divided when it passes through different networks to match the network frame size. At that time each fragment is determined with a sequence number in this field.
**Flags:** The bits in the flags field handles fragmentation and identifies the first, middle or last fragment, etc.

# IPv4 Datagram Formats



**Fragmentation offset:** It's a pointer that represents the offset of the data in the original datagram.
**Time to live:** It defines the number of hops a datagram can travel before it is rejected. In simple words, it specifies the duration for which a datagram remains on the internet.
**Protocol:** The protocol field specifies which upper layer protocol data are encapsulated in the datagram (TCP, UDP, ICMP, etc.).
**Header checksum:** This is a 16-bit field confirm the integrity of the header values, not the rest of the packet.
**Source address:** It's a four-byte internet address which identifies the source of the datagram.
**Destination address:** This is a 4-byte field which identifies the final destination.
**Options:** This provides more functionality to the IP datagram. Furthermore can carry fields like control routing, timing, management, and alignment.
IPv4 is a two-level address structure (net id and host id) classified into five categories (A, B, C, D, and E).

# IPv6 Datagram Format

- IPv6 has a much simpler packet header compared with IPv4, by including only the information needed for forwarding the IP datagram.
- IPv4 has a fixed length header of size 40 bytes. Fixed length IPv6 header allows the routers to process the IPv6 datagram packets more efficiently.

- **Version:** The size of the Version field is 4 bits. The Version field shows the version of IP and is set to 6.
- **Traffic Class:** The size of Traffic Class field is 8 bits. Traffic Class field is similar to the IPv4 Type of Service (ToS) field. TheTraffic Class field indicates the IPv6 packet's class or priority.
- **Flow Label:** The size of Flow Label field is 20 bits. The Flow Label field provide additional support for real-time datagram delivery and quality of service features. The purpose of Flow Label field is to indicate that this packet belongs to a specific sequence of packets between a source and destination and can be used to prioritized delivery of packets for services like voice.
- **Payload Length:** The size of the Payload Length field is 16 bits. The Payload Length field shows the length of the IPv6 payload, including the extension headers and the upper layer protocol data

- **Next Header**: The size of the Next Header field is 8 bits. The Next Header field shows either the type of the first extension (if any extension header is available) or the protocol in the upper layer such as TCP, UDP, or ICMPv6.
- **Hop Limit**: The size of the Hop Limit field is 8 bits The Hop Limit field shows the maximum number of routers the IPv6 packet can travel. This Hop Limit field is similar to **IPv4 Time to Live (TTL) field**.
- **Source Address**: The size of the Source Address field is 128 bits. The Source Address field shows the **IPv6 address** of the source of the packet.
- **Destination Address**: The size of the Destination Address field is 128 bits. The Destination Address field shows the **IPv6 address** of the destination of the packet.

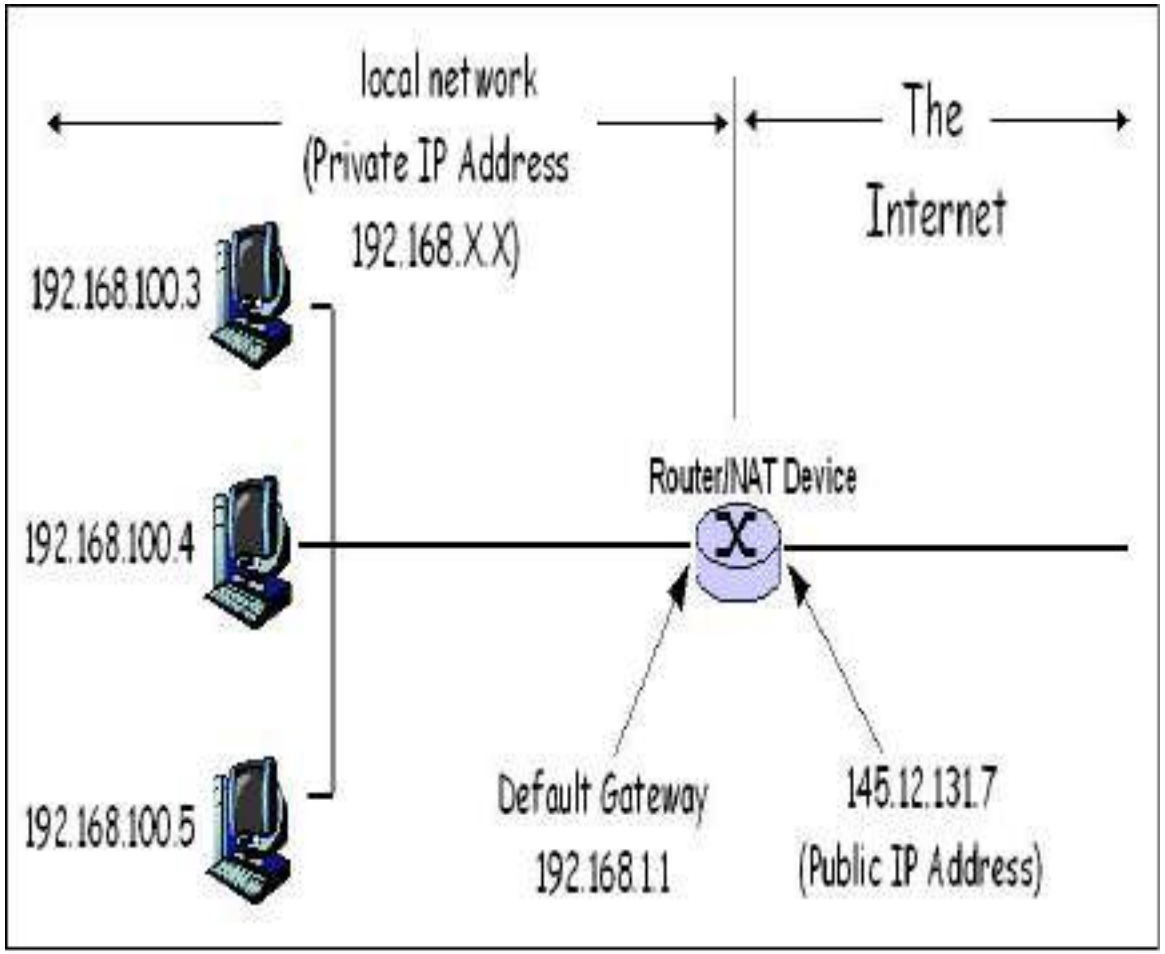
# Comparsion between IPv4 and IPv6 Header Format

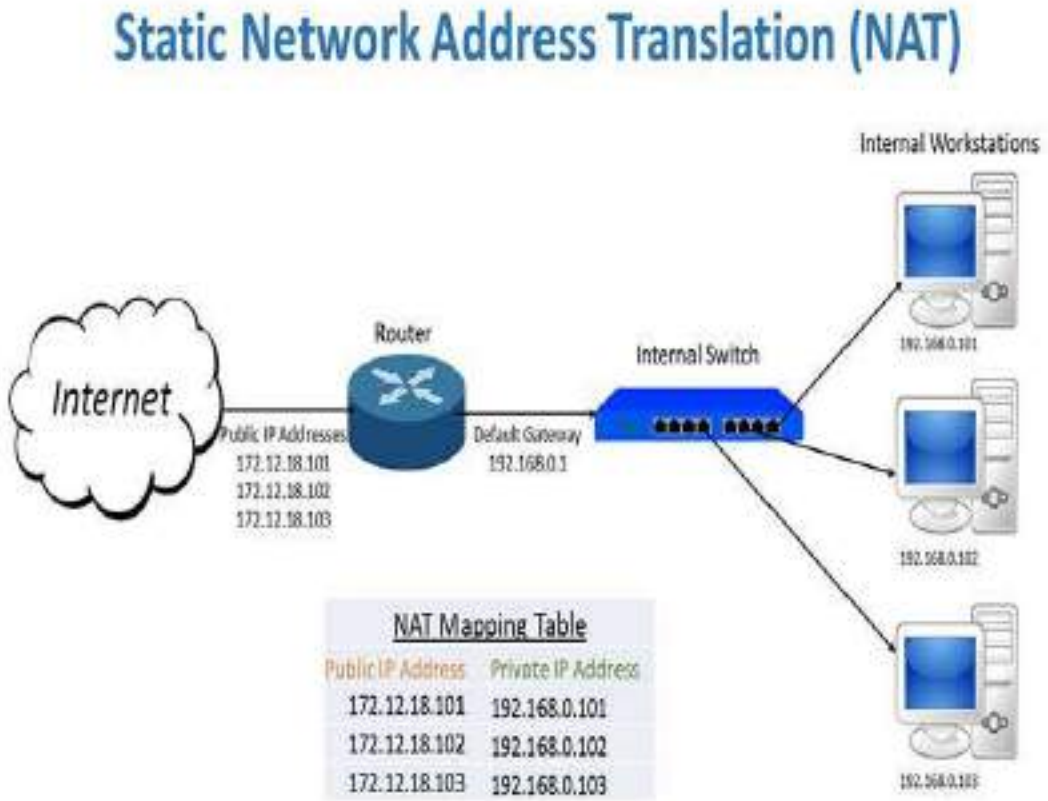
- IPv6 header is much simpler than IPv4 header.
- The size of IPv6 header is much bigger than that of IPv4 header, because of IPv6 address size. IPv4 addresses are 32bit binary numbers and IPv6 addresses are 128 bit binary numbers.
- In IPv4 header, the source and destination IPv4 addresses are 32 bit binary numbers. In IPv6 header, source and destination IPv6 addresses are 128 bit binary numbers.
- IPv4 header includes space for IPv4 options. In IPv6 header, we have a similar feature known as extension header. IPv4 datagram headers are normally 20-byte in length. But we can include IPv4 option values also along with an IPv4 header. In IPv6 header we do not have options, but have extension headers.
- The fields in the IPv4 header such as IHL (Internet Header Length), identification, flags are not present in IPv6 header.
- • Time-to-Live (TTL), a field in IPv4 headers typically used for preventing routing loops, is renamed to it's exact meaning, "Hop Limit”.

# NAT(Network Address Translator)

- **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.
- Network Address Translation (NAT) is a way to map an entire network (or networks) to a single IP address
- Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to destination. It then makes the corresponding entries of ip address and port number in the NAT table. NAT generally operates on router or firewall.
- Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.
- Basically, NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.

# NAT(Network Address Translator)



# Advantages

- NAT saves public IP addresses
- NAT hides the internal network's IP addresses.
- It simplifies routing.
- NAT is transparent to the client and, therefore, allows you to support a wider range of clients.
- NAT supports a wide range of services with a few exceptions. Any application that carries and uses the IP address inside the application does not work through NAT.
- NAT consumes fewer computer resources and is more efficient than using application proxy servers.
- The Universal Connection can flow through NAT

# Disadvantages

- NAT (Network Address Translation) is a processor and memory resource consuming technology, since NAT (Network Address Translation) need to translate IPv4 addresses for all incoming and outgoing IPv4 datagrams and to keep the translation details in memory.
- NAT (Network Address Translation) may cause delay in IPv4 communication.
- •NAT (Network Address Translation) cause loss of end-device to end-device IP traceability
- Some technologies and network applications will not function as expected in a NAT (Network Address Translation) configured network.

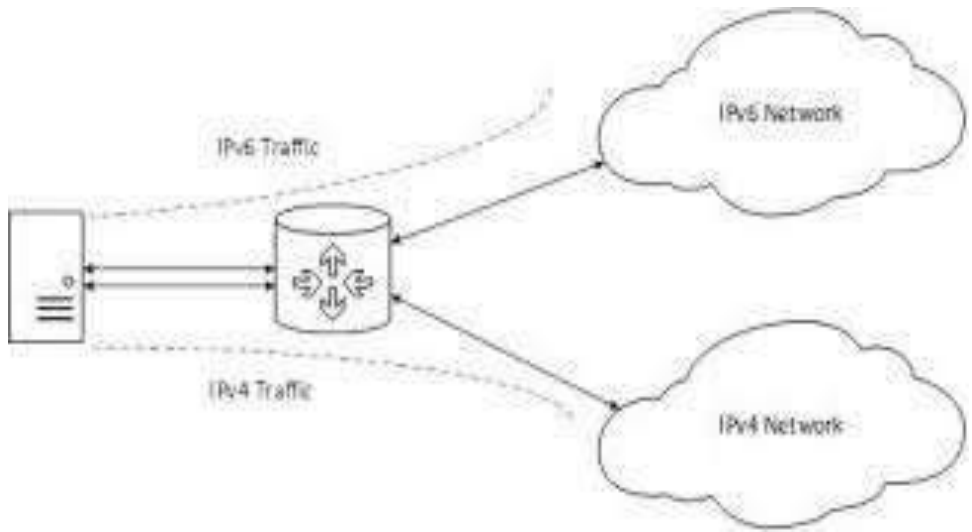
# IPv4 to IPv6 Transition Mechanisms

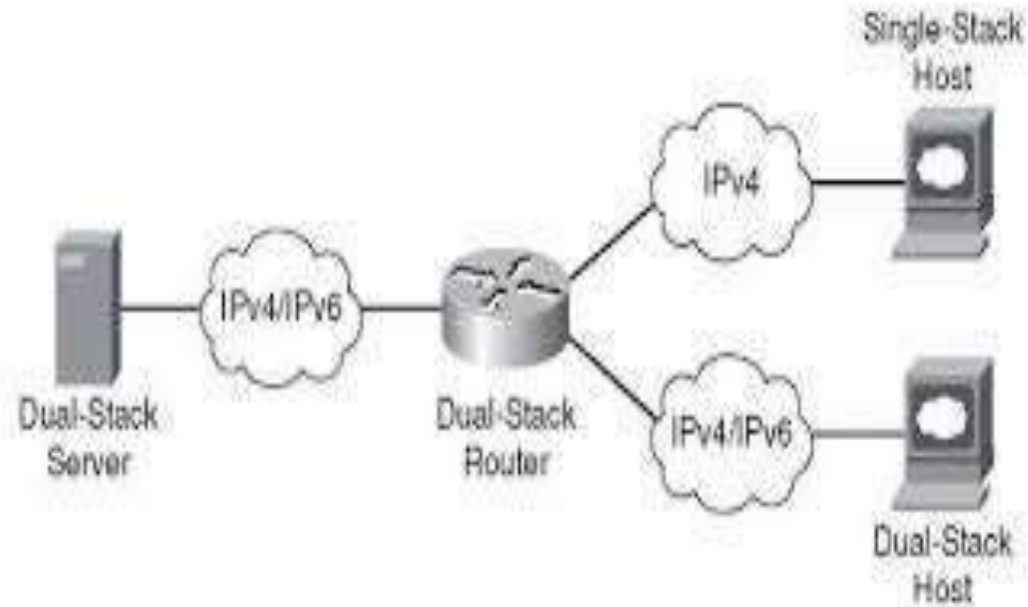
- **IPv6 transition mechanisms** are technologies that facilitate the transitioning of the Internet from its initial (and current) IPv4 infrastructure to the successor addressing and routing system of Internet Protocol Version 6 (IPv6).
- There are a couple of main methods that can be used when transitioning a network from IPv4 to IPv6; these include:
- **Dual Stack** – Running both IPv4 and IPv6 on the same devices
- **Tunneling** – Transporting IPv6 traffic through an IPv4 network transparently
- **Translation** – Converting IPv6traffic to IPv4 traffic for transport and vice versa.

# Dual Stack

- The term “dual-stack” refers to TCP/IP capable devices providing support for both IPv4 and IPv6.
- It is important to understand that having a device being able to communicate over both IPv4 or IPv6 does not necessarily means that all applications operating within this device are capable of utilizing both IPv4 and IPv6.
- The term “Dual-stack routing” refers to a network that is dual IP, that is to say all routers must be able to route both IPv4 and IPv6.
- Dual-stacked hosts running on a dual-stack network allow applications to migrate one at a time from IPv4 transport to IPv6 transport

# Dual Stack


IPv6 Traffic
IPv6 Network
IPv4 Traffic
IPv4 Network


Single-Stack Host
IPv4
IPv4/IPv6
Dual-Stack Server
Dual-Stack Router
IPv4/IPv6
Dual-Stack Host

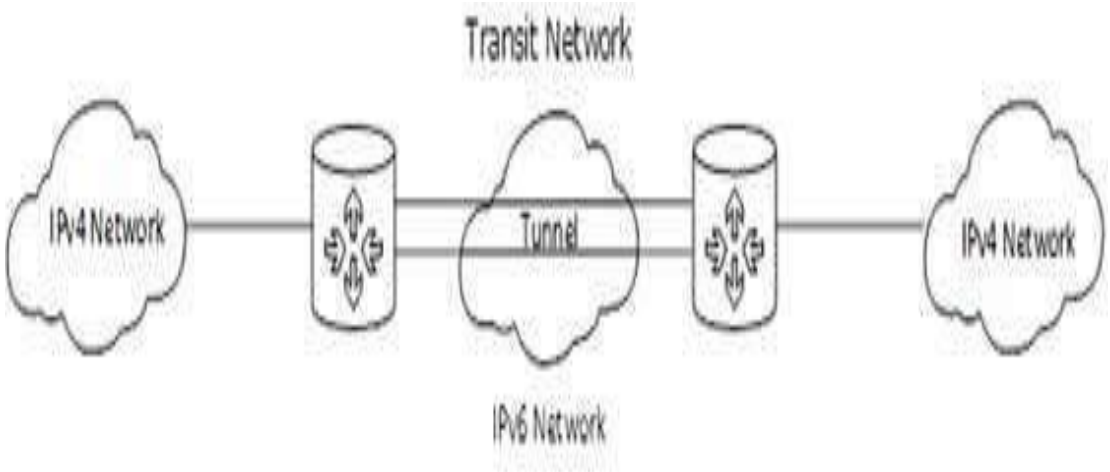
# Tunneling

- The term “tunneling” refers to a means to encapsulate one version of IP in another so the packets can be sent over a backbone that does not support the encapsulated IP version.
- For example, when two isolated IPv6 networks need to communicate over an IPv4 network, dual stack routers at the network edges can be used to set up a tunnel which encapsulates the IPv6 packets within IPv4, allowing the IPv6 systems to communicate without having to upgrade the IPv4 network infrastructure that exists between the networks

These are the five methods of tunneling IPv6 traffic:

- Manual IPv6 tunnels
- Automatic IPv4-Compatible tunnels
- GRE(Generic Routing Encapsulation )
- Automatic 6to4 tunnels
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Tunnels

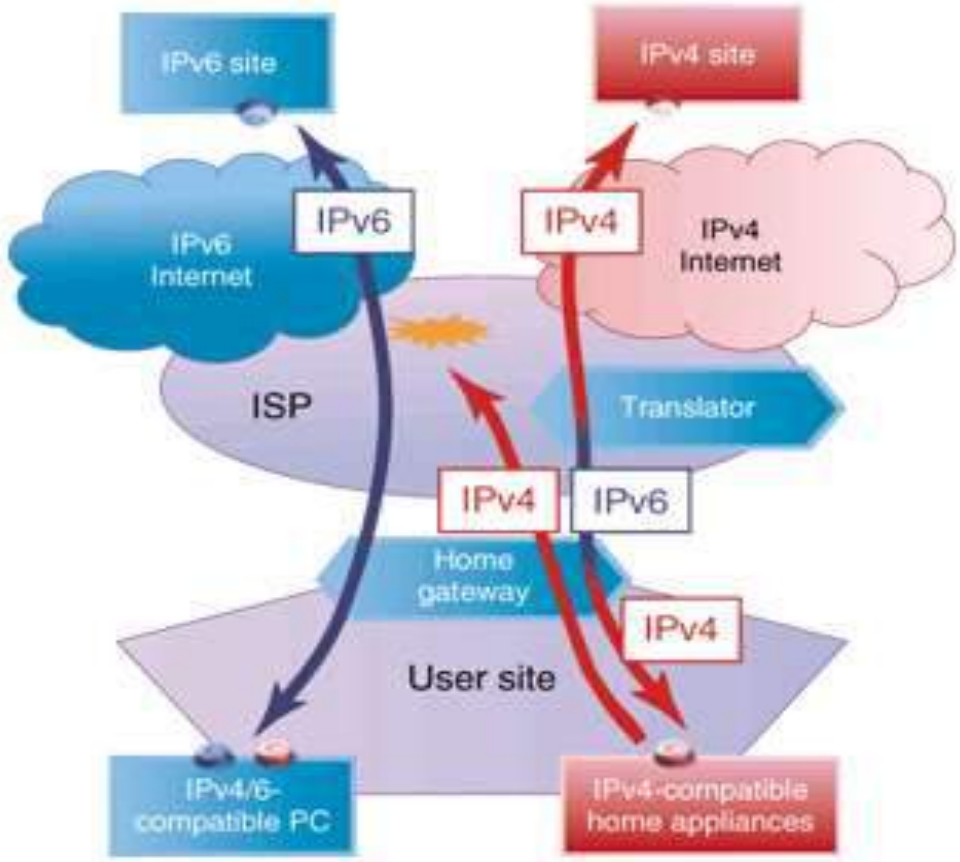
# Tunneling

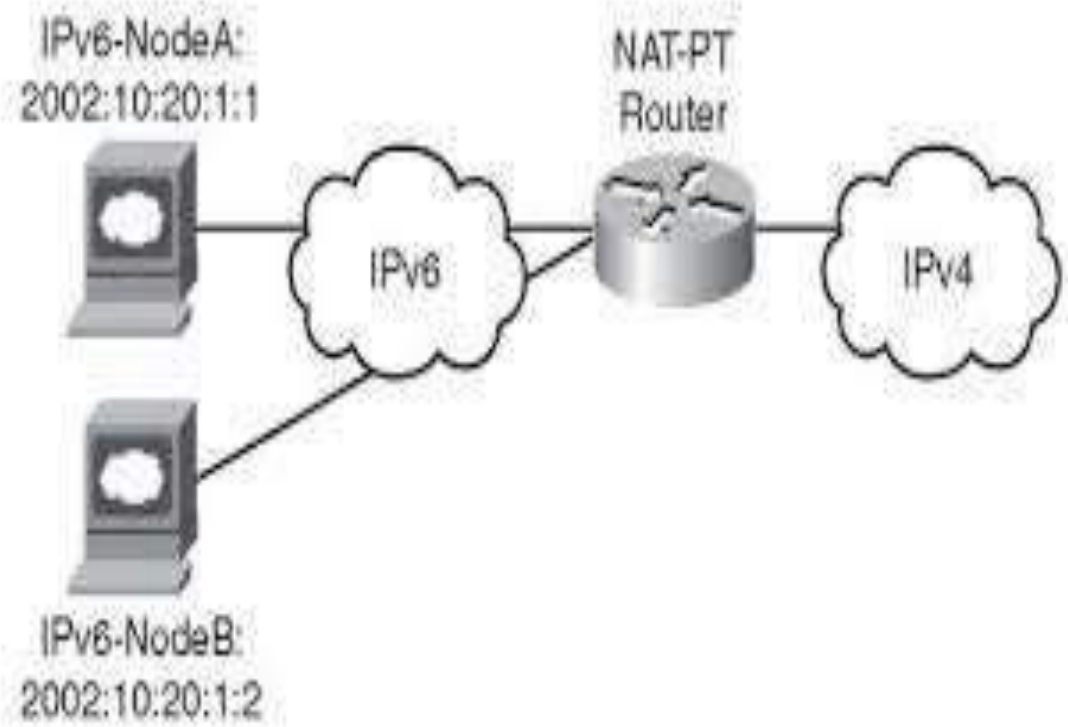

Transit Network
IPv4 Network
Tunnel
IPv4 Network
IPv6 Network

# Translation

- The term “translators” refers to devices capable of translating traffic from IPv4 to IPv6 or vice  versa.
- This mechanism is intended to eliminate the need for dual-stack network operation by translating traffic from IPv4-only devices to operate within an IPv6 infrastructure.
- This option is recommended only as a last option because translation interferes with objective of end-to-end transparency in network communications.
- Use of protocol translators cause problems with NAT and highly constrain the use of IP-addressing

# Translation



# Translation

- There are two methods that are typically used with translated IPv6 networks; these include:
- **Network Address Translation**—Protocol Translation (NAT-PT) – The NAT-PT method enables the ability to either statically or dynamically configure a translation of a IPv4 network address into an IPv6 network address and vice versa. For those familiar with more typically NAT implementations, the operation is very similar but includes a protocol translation function. NAT-PT also ties in an Application Layer Gateway (ALG) functionality that converts Domain Name System (DNS) mappings between protocols.
- **NAT64** – One of the main limitations to NAT-PT was that it tied in ALG functionality; this was considered a hindrance to deployment. With NAT64 also came DNS64, both of which are configured and implemented separately; when these were defined and accepted the use of NAT-PT was depreciated. NAT64 offers both a stateless and stateful option when deploying, the later that keeps track of bindings and enables 1-to-N functionality.

# ICMP/ICMPv6

- ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet
- **ICMP** is a network protocol useful in Internet Protocol (IP) network management and administration.
- ICMP is a complementary protocol to IP (Internet Protocol). Like IP, ICMP resides on the Network Layer of the OSI Model.
- ICMP is designed for sending control and test messages across IP networks.
- ICMP is a control protocol, meaning that it does not carry application data, but rather information about the status of the network itself.

**Features:**

ICMP: Used by IP to send error and control messages

ICMP uses IP to send its messages (Not UDP)

ICMP does not report errors on ICMP messages.

ICMP message are not required on datagram checksum errors. (Some implementations still do)

ICMP reports error only on the first fragment

**ICMP can be used to report:**

- errors in the underlying communications of network applications
- availability of remote hosts
- network congestion

The best known example of ICMP in practice is the :

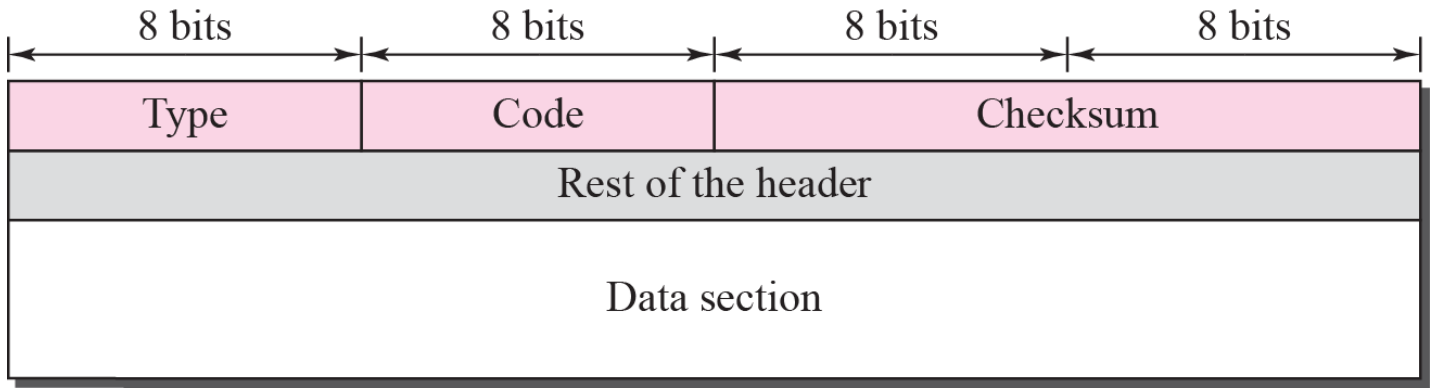
- Ping utility, that uses ICMP to probe remote hosts for responsiveness and overall round-trip time of the probe messages.
- Traceroute that can identify intermediate "hops" between a given source and destination.

# ICMP Packet Format

**Table 9.1** *ICMP messages*

| *Category* | *Type* | *Message* |
|---|---|---|
| Error-reporting messages | 3 | Destination unreachable |
| | 4 | Source quench |
| | 11 | Time exceeded |
| | 12 | Parameter problem |
| | 5 | Redirection |
| Query messages | 8 or 0 | Echo request or reply |
| | 13 or 14 | Timestamp request or reply |

ICMP Packet Format



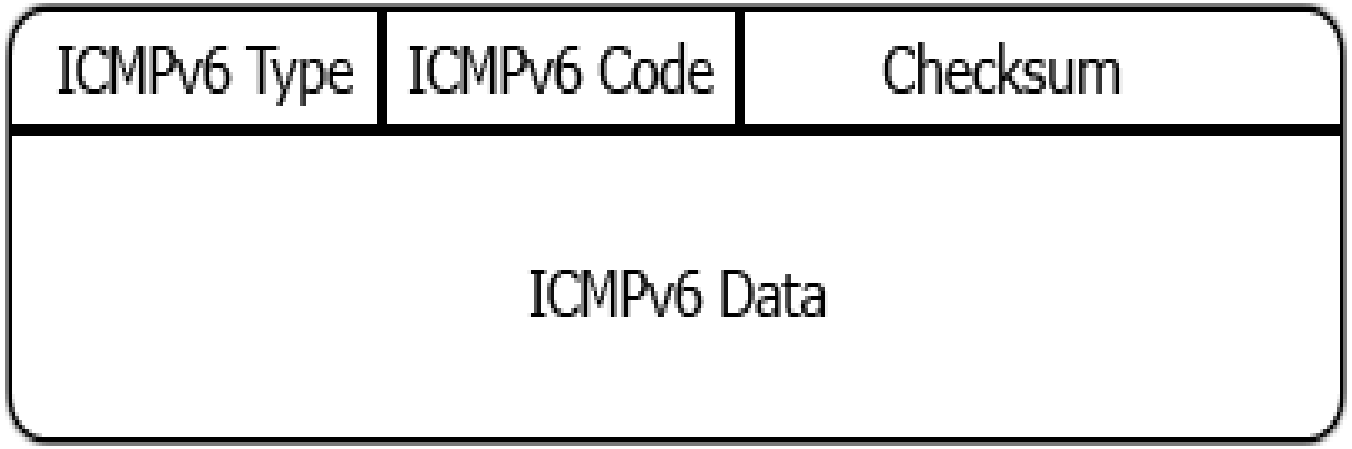
- Headers are 32 bits in length; all contain same three fields
  - type - 8 bit message type code
    - thirteen message type are defined
  - code - 8 bit; indicating why message is being sent
  - checksum - standard internet checksum
    - 16 bit 1's complement sum of the payload and header
      - for purpose of calculation the checksum field is set to zero
- Data section in
  - **Error Messages** carries information to find the original packet that had the error
    - Rest of Header unused (all 0s), except for **Redirection message format**
  - **Query Messages** carries extra information based on type of the query.
    - Rest of Header = Identifier (8 bits) + Sequence Number (8 bits)

# ICMPv6

- The Internet Control Message Protocol Version 6 (ICMPv6) is a new version of the ICM protocol.
- ICMPv6 messages are transported within an IPv6 packet that may include IPv6 extension headers.
- ICMPv6 is a multipurpose protocol and is used for a variety of activities including error reporting in packet processing, diagnostic activities, Neighbor Discovery process and IPv6 multicast membership reporting.
- To perform these activities, ICMPv6 messages are subdivided into two classes: error messages and information messages.
- **Error Messages** – The Internet Control Message Protocol Version 6 (ICMPv6) error messages belong to four different categories: Destination Unreachable, Time Exceeded, Packet Too Big, and Parameter Problems.
- **Information Messages** – The Internet Control Message Protocol Version 6 (ICMPv6) information messages are subdivided into three groups: diagnostic messages,Neighbor Discovery messages, and messages for the management of multicast groups

# ICMPv6

- ICMPv6 packets have the format shown in the figure.
- The 8-bit Type field indicates the type of the message. If the high-order bit has value zero (values in the range from 0 to 127), it indicates an error message; if the high-order bit has value 1 (values in the range from 128 to 255), it indicates an information message.
- The 8-bitCodefield content depends on the message type.
- The Checksum field helps in the detection of errors in the ICMP message and in part of the IPv6 message.



# ICMPv6 Message

| Type | Meaning |
|---|---|
| **ICMPv6 error messages** | |
| 1 | Destination unreachable |
| 2 | Packet too big |
| 3 | Time exceeded |
| 4 | Parameter problem |
| 100 | Private experimentation |
| 101 | Private experimentation |
| 127 | Reserved for expansion of ICMPv6 error messages |
| **ICMPv6 informational messages** | |
| 128 | Echo request |
| 129 | Echo reply |
| 133 | Router solicitation |
| 134 | Router advertisement |
| 135 | Neighbor solicitation |
| 136 | Neighbor advertisement |
| 200 | Private experimentation |
| 201 | Private experimentation |
| 255 | Reserved for expansion of ICMPv6 informational messages |

# Routing

- Routing is the process of forwarding packets from one network to the destination address in another network.
- **Routing** is the process of selecting a path for traffic in a network or between or across multiple networks
- Router, a packet forwarding device between two networks, is designed to transmit packets based on the various routes stored in routing tables. Each route is known as a routing entry.
- The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations.

# Routing Protocols

- A **routing protocol** specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network.

Every network routing protocol performs three basic functions:

- *discovery* – identify other routers on the network
- *route management* – keep track of all the possible destinations (for network messages) along with some data describing the pathway of each
- *path determination* – make dynamic decisions for where to send each network message

# Routing Algorithm

- **Routing** is process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table table is created which contains information regarding routes which data packets follow.
- Routing is the process of transferring the packets from one network to another network and delivering the packets to the hosts.
- Various routing algorithm are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach destination efficiently.

The traffic is routed to all the networks in the internetwork by the routers. In the routing process a router must know following things:

- Destination device address.
- Neighbor routers for learning about remote networks.
- Possible routes to all remote networks.
- The best route with the shortest path to each remote network.
- How the routing information can be verified and maintained

# Types of Routing:Static and Dynamic

- Static routing is a process in which we have to manually add routes in routing table.
- **Static routing** does not involve any change in routing table unless the network administrator changes or modify them manually.
- Static routing algorithms function well where the network traffic is predictable.
- This is simple to design and easy to implement. There is no requirement of complex routing protocols.
  **Advantages –**
- 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 particular networks only.
- No bandwidth usage between routers.

**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 has to manually add each route so he should have very good knowledge of the routes of the topology

# Dynamic Routing

- Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table.
- Dynamic routing uses protocols to discover network destinations and the routes to reach it.
- RIP and OSPF are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.

A dynamic protocol have following features:

- The routers should have the same dynamic protocol running in order to exchange routes.
- When a router finds a change in the topology then router advertises it to all other routers.

**Advantages –**

- Easy to configure.
- More effective at selecting the best route to a destination remote network and also for discovering remote network.

**Disadvantage –**

- Consumes more bandwidth for communicating with other neighbors.
- Less secure than static routing.

| BASIS FOR COMPARISON | STATIC ROUTING | DYNAMIC ROUTING |
| --- | --- | --- |
| Configuration | Manual | Automatic |
| Routing table building | Routing locations are hand-typed | Locations are dynamically filled in the table. |
| Routes | User defined | Routes are updated according to change in topology. |
| Routing algorithms | Doesn't employ complex routing algorithms. | Uses complex routing algorithms to perform routing operations. |
| Implemented in | Small networks | Large networks |
| Link failure | Link failure obstructs the rerouting. | Link failure doesn't affect the rerouting |

| | | |
|---|---|---|
| Security | Provides high security. | Less secure due to sending broadcasts and multicasts. |
| Routing protocols | No routing protocols are indulged in the process. | Routing protocols such as RIP, EIGRP, etc are involved in the routing process. |
| Additional resources | Not required | Needs additional resources to store the information. |

# Distance Vector Routing

- It is a dynamic routing algorithm in which each router computes distance between itself and each possible destination i.e. its immediate neighbors.
- The router share its knowledge about the whole network to its neighbors and accordingly updates table based on its neighbors.
- The sharing of information with the neighbors takes place at regular intervals.
- It makes use of **Bellman Ford Algorithm** for making routing tables.
- RIP and IGRP is a commonly used distance vector protocol that uses hop counts or its routing metrics.
- **Problems –** Count to infinity problem which can be solved by splitting horizon.
  – Persistent looping problem i.e. loop will be there forever

# Link State Routing

- It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network.
- A router sends its information about its neighbours only to all the routers through flooding.
- Information sharing takes place only whenever there is a change.
- It makes use of **Dijkastra's Algorithm** for making routing tables.
- **Problems –** Heavy traffic due to flooding of packets.
  **–** Flooding can result in infinite looping which can be solved by using **Time to leave (TTL)** field.

| BASIS FOR COMPARISON | DISTANCE VECTOR ROUTING | LINK STATE ROUTING |
|---|---|---|
| Algorithm | Bellman ford | Dijsktra |
| Network view | Topology information from the neighbour point of view | Complete information on the network topology |
| Best path calculation | Based on the least number of hops | Based on the cost |
| Updates | Full routing table | Link state updates |
| Updates frequency | Periodic updates | Triggered updates |
| CPU and memory | Low utilisation | Intensive |
| | | |

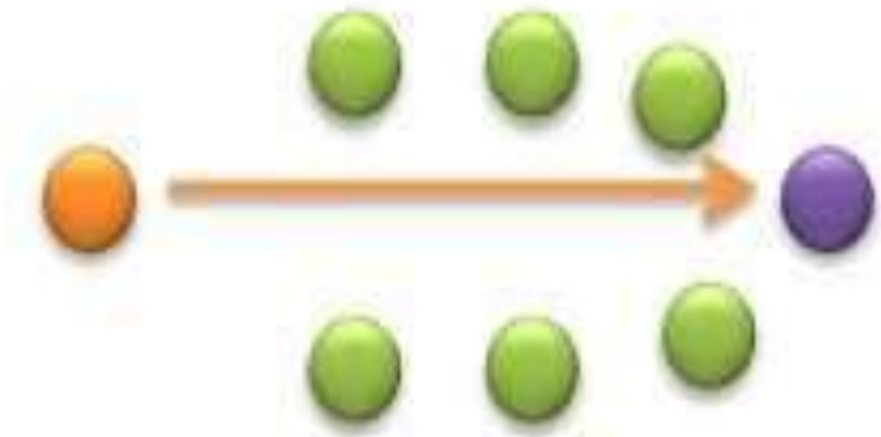
| | | |
|---|---|---|
| Simplicity | High simplicity | Requires a trained network administrator |
| Convergence time | Moderate | Fast |
| Updates | On broadcast | On multicast |
| Hierarchical structure | No | Yes |
| Intermediate Nodes | No | Yes |

# Unicast and Multicast

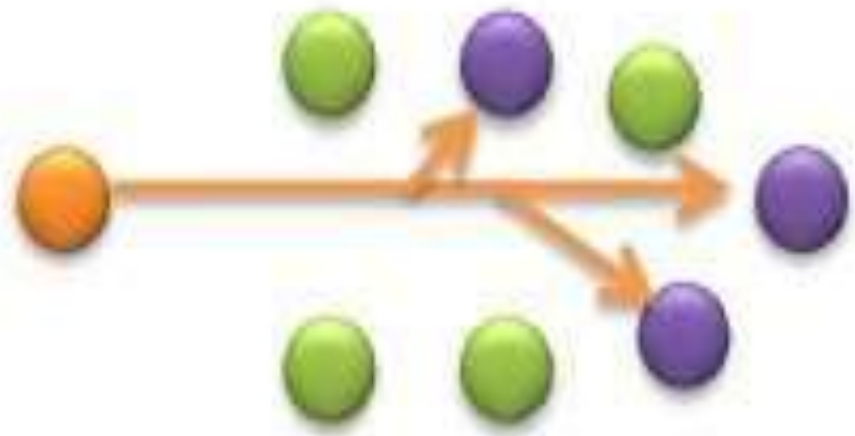
- The term **unicast** is a transmission method where one station sends information to another station.
- It is a one-to-one communication. Unicast transmission is used, where one station transmits some private or unique information to another station.
- Examples of the unicast transmission are web surfing, file transfer as here the there is a single service requestor and a single service provider.
- If one station needs to send packets to multiple stations, it has to send multiple unicast packets, each packet containing the address of the specific station and it is called "**multiple unicasting**".
- Multiple unicasting utilizes the maximum bandwidth of the network. TCP protocol supports unicasting.

# Multicast

- **Multicast,** is an information transmission method where one station transmits the information packet to the interested stations only. It is a one-to-many communication method.
- It is a mixture between unicast and broadcast, where unicasting sends the packet to only one station, and broadcasting sends the packet to all the stations, their multicasting sends the packet to only some selected stations in the network. Examples of multicasting are forwarding emails, multimedia delivery, etc



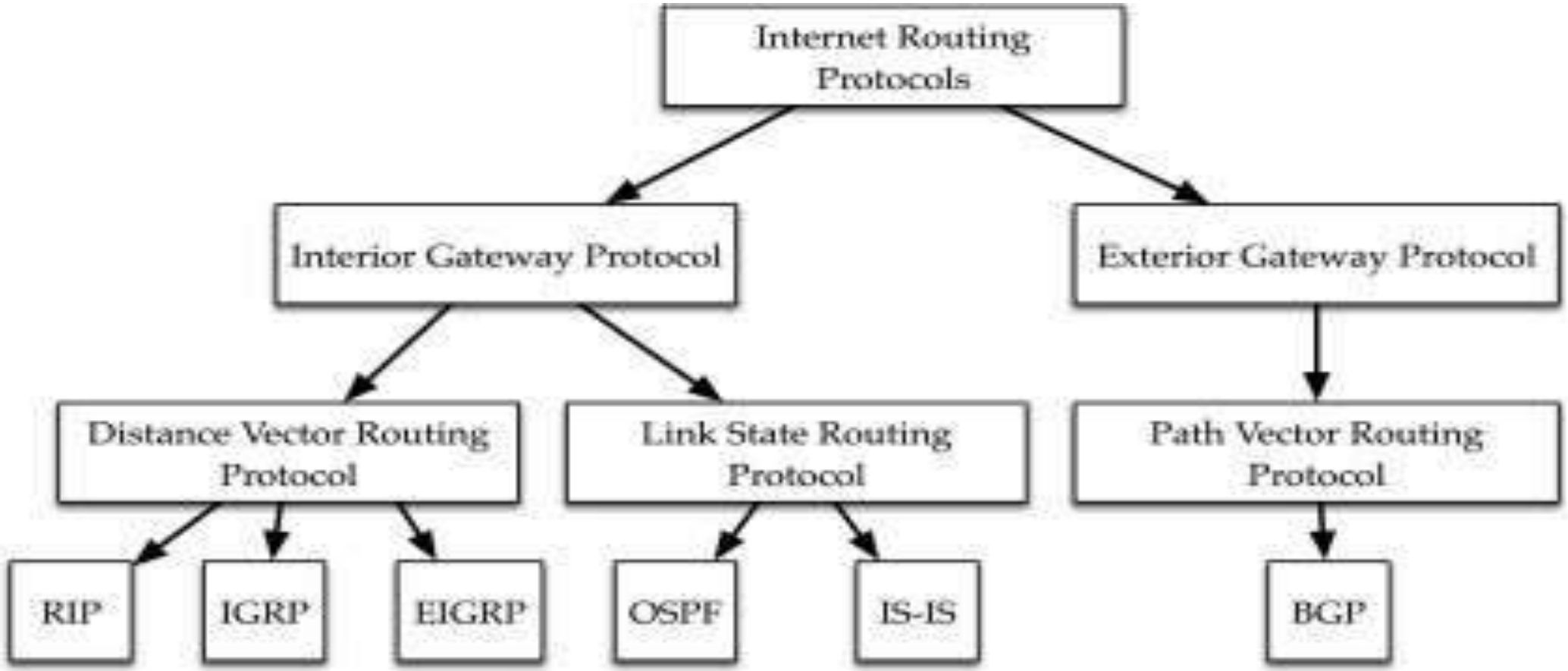
Unicast



Multicast

| BASIS FOR COMPARISON | UNICAST | MULTICAST |
| --- | --- | --- |
| Basic | One sender and one receiver. | One sender and multiple receivers. |
| Bandwidth | Multiple unicasting utilizes more bandwidth as compared to multicast. | Multicasting utilizes bandwidth efficiently. |
| Scale | It does not scale well for streaming media. | It does not scale well across large networks. |
| Mapping | One-to-one. | One-to-many. |
| Examples | Web surfing, file transfer | Multimedia delivery, stock exchange |

# Different types of routing Protocols



- Interior gateway protocols: as the Internet community calls them, are typically used in small, cooperative set of networks such as might be found on a university campus.
- One of the oldest interior protocols is Routing Information Protocol, or RIP.
- Newer interior protocols include Interior Gateway Routing Protocol, or IGRP, and Open Shortest Path First, or OSPF.
- Cisco network devices can also use Cisco's proprietary Enhanced Interior Gateway Routing Protocol, or EIGRP.
- Interior protocols are fairly easy to set up, but do not scale well to large networks.
- Exterior Gateway Protocol (EGP): is a protocol or exchanging routing information between two neighbor gateway hosts (each with its own router) in a network of autonomous systems.
- EGP is commonly used between hosts on the Internet to exchange routing table information.
- The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen.

# Open Shortest Path First(OSPF)

- **Open Shortest Path First** is a link state and hierarchical IGP routing algorithm.
- It is an enhanced version of RIP, which comprises features like multipath routing, least cost routing, and load balancing. Its major metric is the cost to determine the best path.
- OSPF involves the **type of service** routing which means multiple routes can be installed according to the priority or type of service.
- OSPF offers **load balancing** in which it distributes overall traffic routes equally. It also allows networks and routers partitioned into subsets and areas which enhance the growth and ease of management.

| BASIS FOR COMPARISON | RIP | OSPF |
|---|---|---|
| **Stands for** | Routing Information Protocol. | Open Shortest Path First |
| **Class** | Distance vector routing protocol | Link State Routing Protocol |
| **Default metric** | Hop count | Bandwidth (cost) |
| **Administrative distance** | 120 | 110 |
| **Convergence** | Slow | Fast |
| **Summarization** | Auto | Manual |
| **Update timer** | 30 seconds | Only when changes occur |
| **Hop count limit** | 15 | None |
| **Multicast address used** | 224.0.0.9 | 224.0.0.5 and 224.0.0.6 |
| **Protocol and port used** | UDP and port 20 | IP and port 89 |

# BGP (Border Gateway Protocol)

- Border Gateway Protocol (BGP) is an Internet Engineering Task Force (IETF) standard, and the most scalable of all routing protocols.
- BGP (Border Gateway Protocol) is protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers.
- BGP directs packets between autonomous systems (AS) -- networks managed by a single enterprise or service provider.

- BGP is the routing protocol of the global Internet, as well as for Service Provider private networks. BGP has expanded upon its original purpose of carrying Internet reachability information, and can now carry routes for Multicast, IPv6, VPNs, and a variety of other data.
- Traffic that is routed within a single network AS is referred to as internal BGP, or iBGP. More often, BGP is used to connect one AS to other autonomous systems, and it is then referred to as an external BGP, or eBGP.

# Network Traffic Analysis

- Network traffic analysis is the process of recording, reviewing and analyzing network traffic for the purpose of performance, security and/or general network operations and management.
- It is the process of using manual and automated techniques to review granular-level detail and statistics within network traffic.
- Network traffic analysis is primarily done to get in-depth insight into what type of traffic/network packets or data is flowing through a network. Typically, network traffic analysis is done through a network monitoring or network bandwidth monitoring software/application.

The traffic statistics from network traffic analysis helps in:

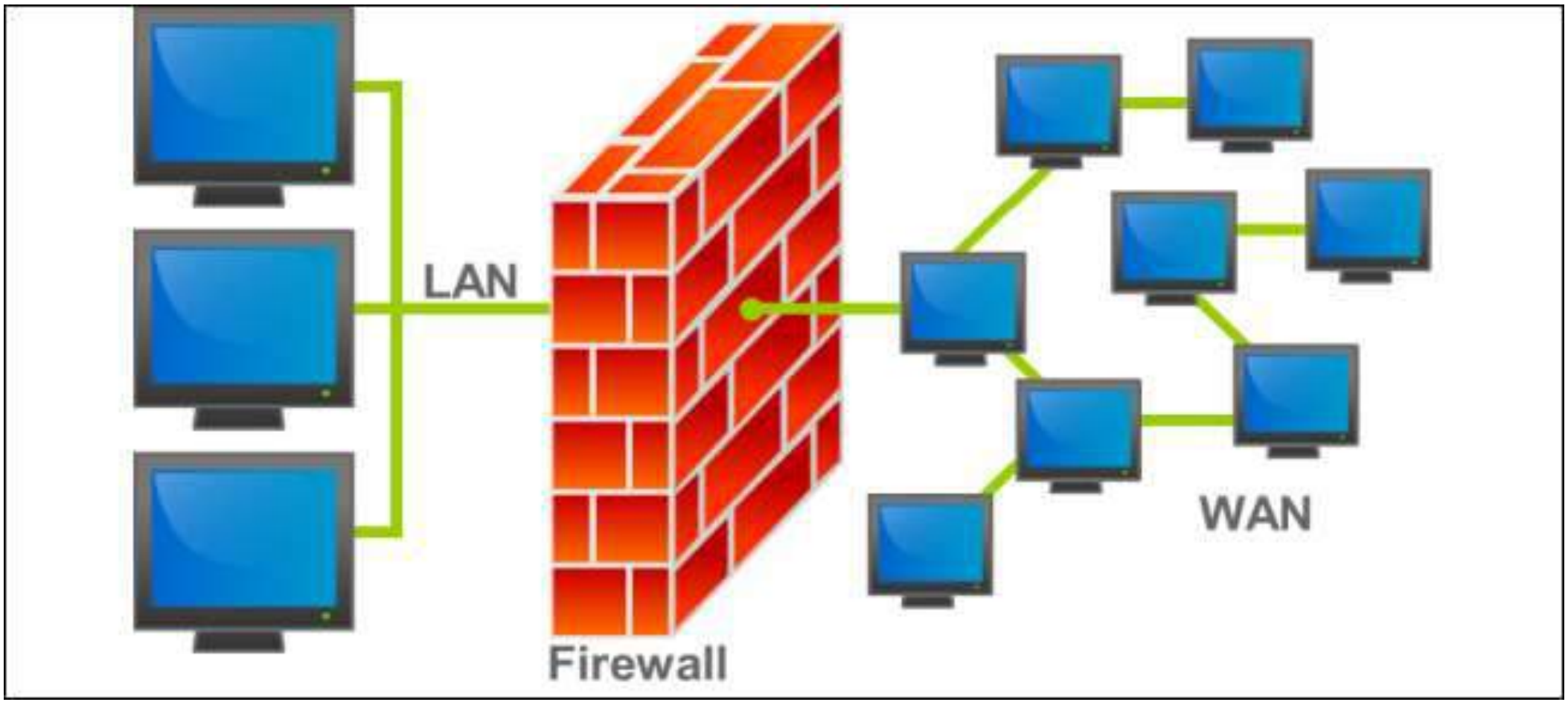
- Understanding and evaluating the network utilization
- Download/upload speeds
- Type, size, origin and destination and content/data of packets
- Network security staff uses network traffic analysis to identify any malicious or suspicious packets within the traffic. Similarly, network administrations seek to monitor download/upload speeds, throughput, content, etc. to understand network operations.
- Network traffic analysis is also used by attackers/intruders to analyze network traffic patterns and identify any vulnerabilities or means to break in or retrieve sensitive data.

# Tools

- Wireshark: kicks off our list being a network protocol analyser and capture utility, captured data can easily be sent to another application for analysis or filtered within WireShark itself.
- Angry IP:  scanner scans IP addresses and ports finding live hosts and providing you with information about them.
- Fiddler captures HTTP between computers and the Internet to help with debugging, you see incoming and outgoing data including encrypted HTTPS traffic, allowing you to test your website performance or the security of your web applications.
- NetworkMiner:  is classed as a network forensics analysis tool and is used to capture packets it then extract files and images from that data allowing you to reconstructed his actions.
- xirrus wifi inspector which manages connections locate devices detect rogue access point and has connection speed quality tests.
- zenoss core keeps an eye on your application's servers, storage, networking and virtualization giving you performance and availability stats.

# Security Concepts:Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- A firewall is a network security system that monitors and controls over all incoming and outgoing network traffic based on advanced and a defined set of security rules.
- Firewalls is a first line of defense in network security
- They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
- A firewall can be hardware, software, or both.


LAN
Firewall
WAN

# How does Firewall Work

- Firewall examine all the data packets passing through them to see if they meet the rules defined by the ACL (Access Control List) made by the administrator of the network. Only, If the Data Packets are allowed as per ACL, they will be Transmitted over the Connection.
- Firewalls generally also maintain a log of Important Activities in Inside the Network. A Network Administrator can define what is important for him and configure the Firewall to make the Logs accordingly.
- Firewall can filter contents on the basis of Address, Protocols, Packet attributes and State.
- Firewalls generally only Screen the Packet Headers

# Types of Firewall

- Packet Filtering Firewalls
- Circuit Level Gateway Firewalls
- Application level Gateway Firewalls
- Stateful Multilayer Inspection Firewalls

# Packet Filtering Firewall

- Packet Filtering Firewalls are normally Deployed on the Routers which connect the Internal Network to Internet. Packet Filtering Firewalls can only be Implemented on the Network Layer of OSI Model.
- Packet Filtering Firewalls work on the Basis of Rules defines by Access Control Lists. They check all the Packets and screen them against the rules defined by the Network Administrator as per the ACLs. If in case, any packet does not meet the criteria then that packet is dropped and Logs are updated about this information.
- Administrators can create their ACLs on the basis Address, Protocols and Packet attributes.

**Advantage:**

- The Biggest Advantage of Packet Filtering Firewalls is Cost and Lower Resource Usage. Best Suited for Smaller Networks.

**Disadvantage:**

- Packet Filtering Firewalls can work only on the Network Layer and these Firewalls do not support Complex rule based models. Also Vulnerable to Spoofing in some Cases.

# Circuit Level Gateway Firewalls

- Circuit level gateways are deployed at the Session layer of the OSI model and they monitor sessions like TCP three way handshake to see whether a requested connection is legitimate or not.
- Major Screening happens before the Connection is Established.
- Information sent to a Computer outside the network through a circuit level gateway appears to have originated from the Gateway. This helps in creating a stealth cover for the private network from outsiders.
- **Advantage:**
- Circuit level gateways are comparatively inexpensive and provide Anonymity to the private network.
- **Disadvantage:**
- Circuit level Gateways do not filter Individual Packets. After Establishing a Connection, an Attacker may take advantage of this.

# Application level Gateway Firewalls

- Application level gateways work on the Application layer of the OSI model and provide protection for a specific Application Layer Procotol. Proxy server is the best example of Application Level Gateways Firewalls.
- Application level gateway would work only for the protocols which is configured. For example, if we install a web proxy based Firewall than it will only allow HTTP Protocol Data. They are supposed to understand application specific commands such as HTTP:GET and HTTP:POST as they are deployed on the Application Layer, for a Specific Protocol.
- Application level firewalls can also be configured as Caching Servers which in turn increase the network performance and makes it easier to log traffic.

# Stateful Multilayer Inspection Firewall

- Stateful multilayer Inspection Firewall is a combination of all the firewalls that we have studied till now.
- They can Filter packets at Network layer using ACLs, check for legitimate sessions on the Session Layers and they also evaluate packets on the Application layer (ALG).
- Stateful Multilayer Inspection Firewall can work on a Transparent mode allowing direct connections between the client and the server which was earlier not possible.
- Stateful Multilayer Inspection firewall can also implement algorithms and complex security models which are protocol specific, making the connections and data transfer more secure.

# Access Control Lists

- Access Control Lists “ACLs” are network traffic filters that can control incoming or outgoing traffic.
- ACLs **work on a set of rules that define how to forward or block a packet at the router’s interface.** An ACL is the same as a Stateless Firewall, which only restricts, blocks, or allows the packets that are flowing from source to destination.
- When you define an ACL on a routing device for a specific interface, all the traffic flowing through will be compared with the ACL statement which will either block it or allow it.
- The criteria for defining the ACL rules could be the source, the destination, a specific protocol, or more information.
- ACLs are common in routers or firewalls, but they can also configure them in any device that runs in the network, from hosts, network devices, servers, etc.