**UNIT -04**

**IP Addressing**

4.1 Internet Protocol and IPv4 Packet format,

4.2 Addressing, Physical Addresses, Logical

Addresses

Port Addresses, Specific Addresses

4.3 IP Address- Network Part and Host Part

4.4 Network Masks, Network Addresses and,

Broadcast

Addresses, Loop Back Address

4.5 Address Classes

4.6 TCP and UDP Connections

4.7 TCP Performance in wireless network

4.8 Overview of IPv6

4.9 IP Routing - Types of routing protocol, Border

Gateway Protocol (BGP), Routing Information

Protocol (RIP), Open Shortest Path First (OSPF),

Routing Table concept

**4.1 Internet Protocol and IPv4 Packet format,**

The network layer is the third layer (from bottom) in the OSI Model. The network layer is concerned with the delivery of a packet across multiple networks.

Network layer protocols exist in every host or router. The router examines the header fields of all the IP packets that pass through it.

IPv4:

IPv4 is a connectionless protocol used for packet-switched networks. It operates on a best effort delivery model, in which neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured. Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet.

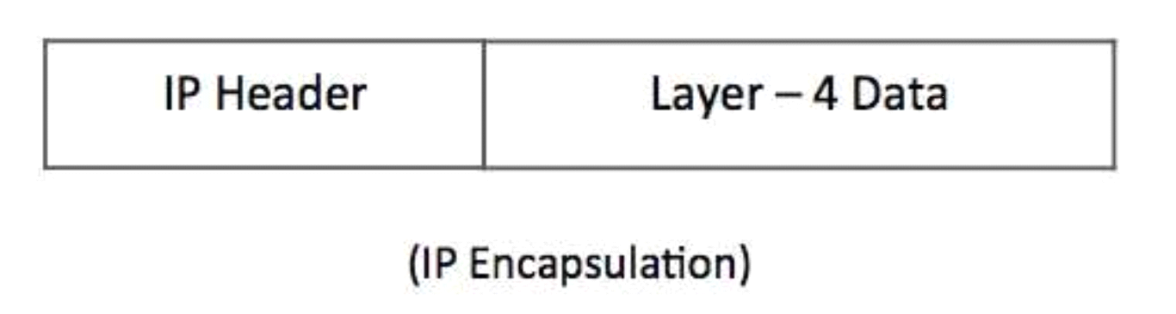
IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for military purposes, while class E addresses are reserved for future use.

IPv4 uses 32-bit (4 byte) addressing, which gives 232 addresses. IPv4 addresses are written in the dot-decimal notation, which comprises of four octets of the address expressed individually in decimal and separated by periods, for instance, 192.168.1.5.

IPv4 Datagram Header

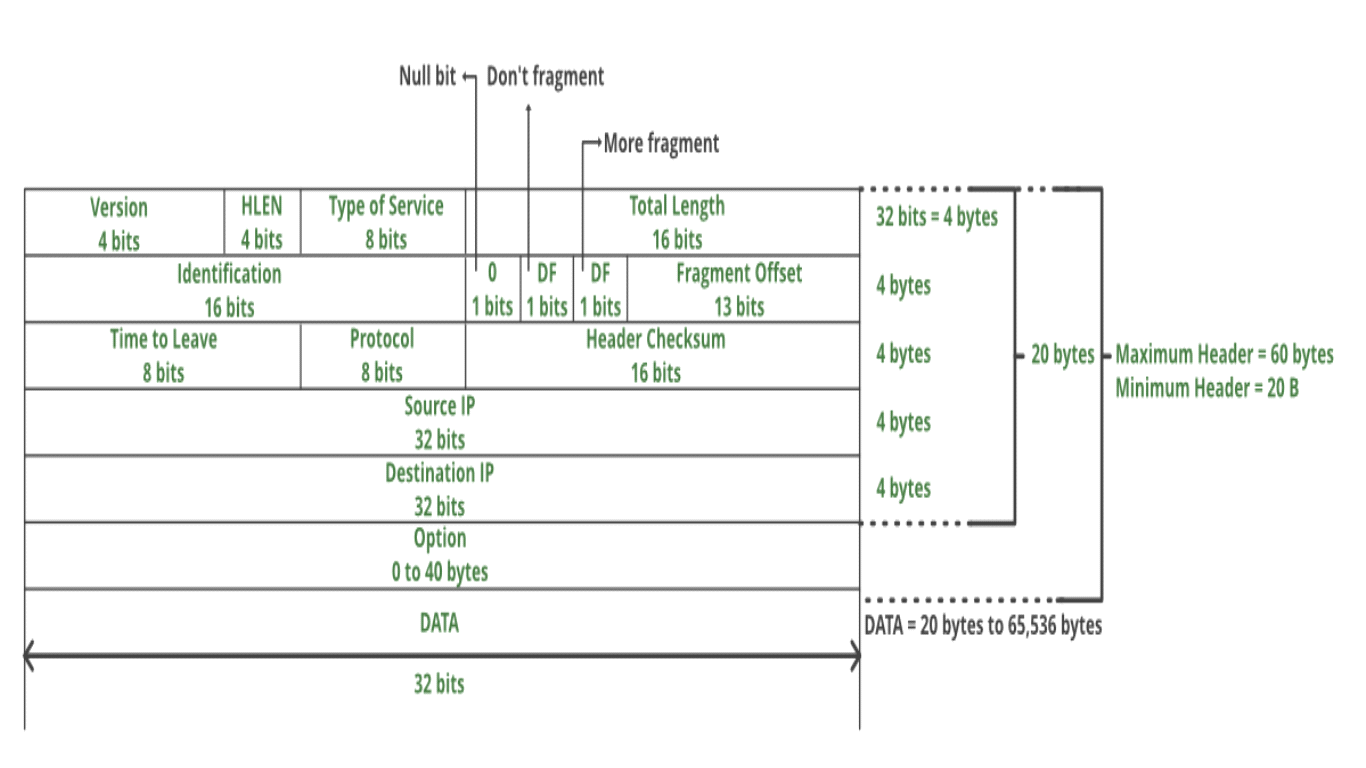
Size of the header is 20 to 60 bytes.

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.



**IP Encapsulation**

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



Following are various components/fields of IP packet header

* Version: The first IP header field is a 4-bit version indicator. In IPv4, the value of its four bits is set to 0100, which indicates 4 in binary. However, if the router does not support the specified version, this packet will be dropped.
* IHL − Internet Header Length; Length of entire IP header.
* Type of Service: Type of Service is also called Differentiated Services Code Point or DSCP. This field is provided features related to the quality of service for data streaming or VoIP calls. The first 3 bits are the priority bits. It is also used for specifying how you can handle Datagram. (8 Bits)
* Total Length − Length of entire IP Packet (including IP header and IP Payload).The minimum size of an IP datagram is 20 bytes and the maximum, it can be 65535 bytes . HELEN and Total length can be used to calculate the dimension of the payload. All hosts are required to be able to read 576-byte datagrams. However, if a datagram is too large for the hosts in the network, the fragmentation method is widely used.
* Identification − If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
* IP Flags: Flag is a three-bit field that helps you to control and identify fragments. The following can be their possible configuration:

Bit 0: is reserved and has to be set to zero

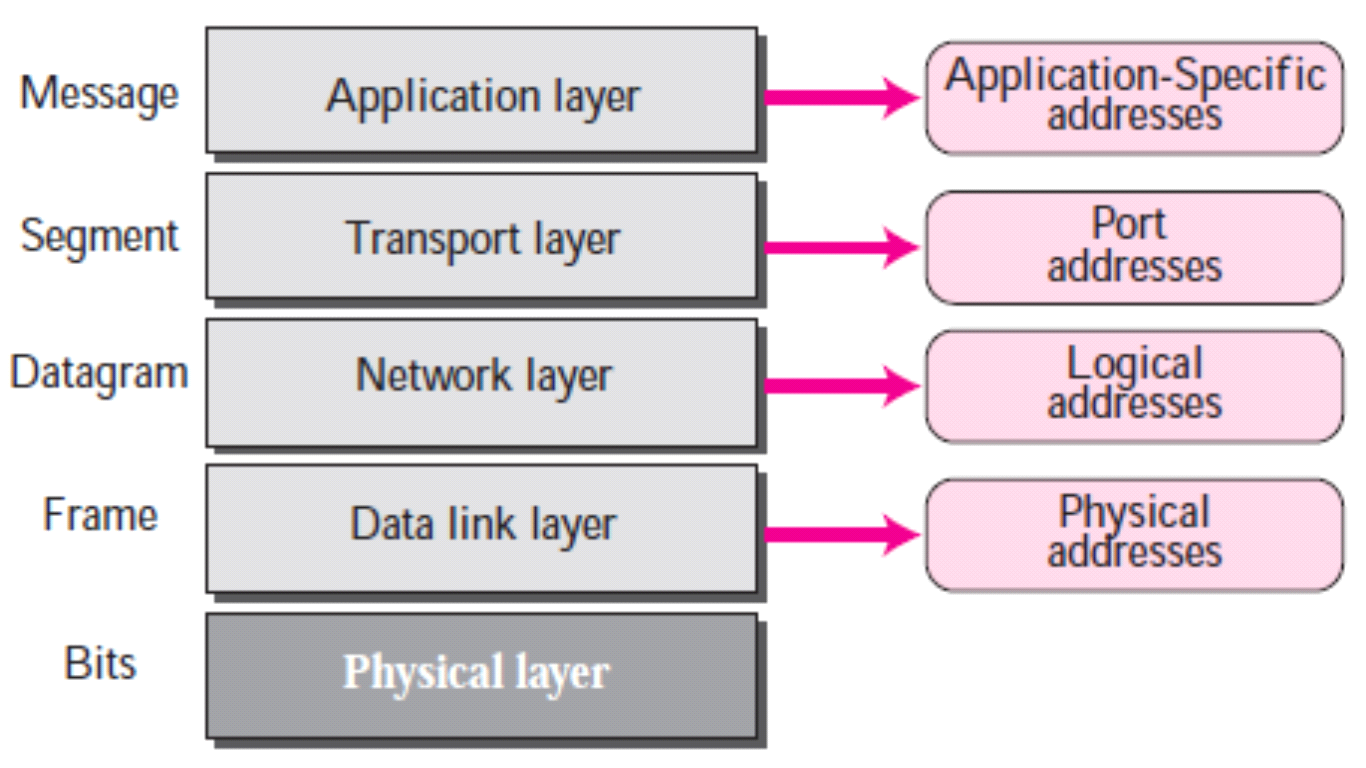
Bit 1: means do not fragment

Bit 2: means more fragments.

* Fragment Offset − This offset tells the exact position of the fragment in the original IP Packet
* Time to Live − Datagram’s lifetime (8 bits).To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
* Protocol − Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
* Header Checksum − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.The IP header is compared to the value of its checksum. When the header checksum is not matching, then the packet will be discarded.
* Source IP address: 32 bits IP address of the sender
* Destination IP address: 32 bits IP address of the receiver
* Option: Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.
* Data: This field stores the data from the protocol layer, which has handed over the data to the IP layer.

**4.2 Addressing, Physical Addresses, Logical Addresses**

Four levels of addresses are used in the TCP/IP protocol: physical address, logical address, port address, and application-specific address as shown in Figure.



**Physical Addresses**

The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.

The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address.

**Logical Addresses**

Logical addresses are used by networking software to allow packets to be independent of the physical connection of the network, that is, to work with different network topologies and types of media.

A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. An internet address in IPv4 in decimal numbers 132.24.75.9. It is unique address.

**The physical addresses will change from hop to hop, but the logical addresses remain the same.**

**Port Addresses**

There are many application running on the computer. Each application run with a port no.(logically) on the computer.**a port address is a 16-bit address**

A port number is part of the addressing information used to identify the senders and receivers of messages.

Port numbers are most commonly used with TCP/IP connections.

These port numbers allow different applications on the same computer to share network resources simultaneously.

**The physical addresses change from hop to hop, but the logical and port addresses usually remain the same.**

**Application-Specific Addresses**

Some applications have user-friendly addresses that are designed for that specific application.

Examples include the e-mail address (for example, forouzan@fhda.edu) and the Universal Resource Locator (URL) (for example, [www.mhhe.com](http://www.mhhe.com/)). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.

**4.3 IP Address- Network Part and Host Part**

**192.8.16.0**

## **How does IP address work?**

IP address works in an IP network like a postal address. For example, a postal address combines two addresses, address, or your area your house address.

The address or your area is a group address of all houses that belong to a specific area. The house address is the unique address of your homes in that area. Here, your area is represented by a PIN code number.

In this example, the network address comprises all hosts which belong to a specific network. The host address is the unique address of a particular host in that network.

## **What is Classful Addressing?**

Classful addressing is a network addressing the Internet's architecture from 1981 till Classless Inter-Domain Routing was introduced in 1993.

This addressing method divides the IP address into five separate classes based on four address bits.

Here, classes A, B, C offers addresses for networks of three distinct network sizes. Class D is only used for multicast, and class E reserved exclusively for experimental purposes.

Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

IP address classes

**Classful Addressing**  
The 32 bit IP address is divided into five sub-classes. These are:

* Class A
* Class B
* Class C
* Class D
* Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.  
IPv4 address is divided into two parts:

* Network ID
* Host ID

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.

IP Address are Represented in two forms

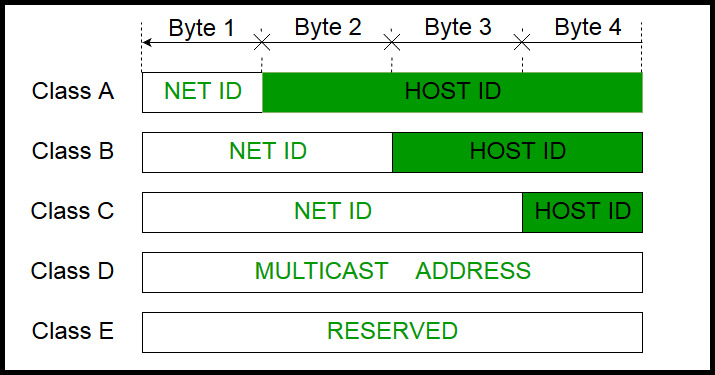
**Decimal Representation Binary Representation**  
0 to 127  **0**1101111.0000101.00000000.00000000

128-191 **10**111111.11111111.00000000.00000000

192-223 **110**10111.11011110.11111111.00000000

224 to 255 **1110**1010.10101010.11001010.10101010

|  |  |  |
| --- | --- | --- |
| **Class** | **Leading bits** | **Start address** |
| Class A | 0 | 0.0.0.0 |
| **Class B** | 10 | 128.0.0.0 |
| **Class C** | 110 | 192.0.0.0 |
| **Class D** (multicast) | 1110 | 224.0.0.0 |
| **Class E(Reserve)** |  |  |

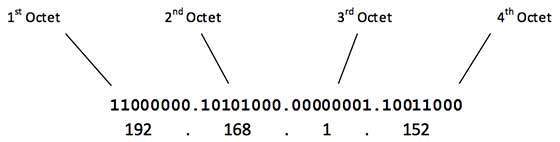
Class A = 255.0.0.0 11111111.0000000.00000000.00000000

Class B = 255.255.0.0 11111111.11111111.00000000.00000000

Class C = 255.255.255.0 11111111.11111111.11111111.00000000

Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address −

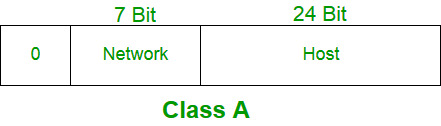


**Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.**

The number of networks and the number of hosts per class can be derived by this formula −



CLASS -A

[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_4.jpg)

IP address belonging to class A are assigned to the networks that contain a large number of hosts.

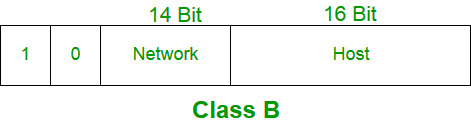
* The network ID is 8 bits long.
* The host ID is 24 bits long.

The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

* 2^7-2= 126 network ID(Here 2 address is subracted because 0.0.0.0 and 127.x.y.z are special address. )
* 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x

Class B:

[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_5.jpg)

IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

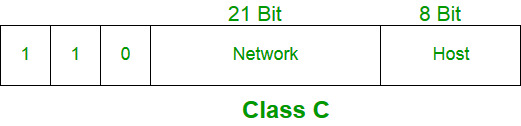
* The network ID is 16 bits long.
* The host ID is 16 bits long.

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

* 2^14 = 16384 network address
* 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.

Class C:

[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_6.jpg)

IP address belonging to class C are assigned to small-sized networks.

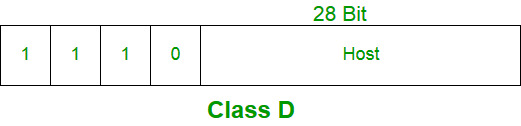
* + - The network ID is 24 bits long.
    - The host ID is 8 bits long.

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

* + - 2^21 = 2097152 network address
    - 2^8 – 2 = 254 host address

IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.

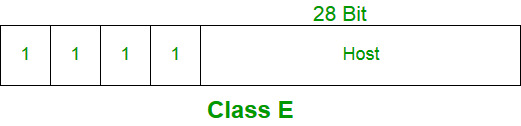
Class D:

[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_7.jpg)

IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.

Class E:

[](https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_8.jpg)

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn’t have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.

Range of special IP addresses:

169.254.0.0 – 169.254.0.16 : Link local addresses  
127.0.0.0 – 127.0.0.8 : Loop-back addresses  
0.0.0.0 – 0.0.0.8 : used to communicate within the current network.

## Limitations of classful IP addressing

Here are the drawbacks/ cons of the classful IP addressing method:

* Risk of running out of address space soon
* Class boundaries did not encourage efficient allocation of address space

**Subnetting**

is the practice of dividing a network into two or smaller networks. It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain.

IP Subnetting designates high-order bits from the host as part of the network prefix. This method divides a network into smaller subnets.

It also helps you to reduce the size of the routing tables, which is stored in routers. This method also helps you to extend the existing IP address base & restructures the IP address.

When a bigger network is divided into smaller networks, in order to maintain security, then that is known as Subnetting. so, maintenance is easier for smaller networks.

| lass | Default subnet mask | No. of networks | No. of host per network |
| --- | --- | --- | --- |
| A | 255.0.0.0 | 256 | 16,777,214 |
| B | 255.255.0.0 | 65,536 | 65,534 |
| C | 255.255.255.0 | 16,77,216 | 126 |

q.1 Subnet the Class C IP Address 205.11.2.0 so that you have 30 subnets.

What is the subnet mask for the maximum number of hosts?

How many hosts can each subnet have?

What is the IP address of host 3 on subnet 2 ?

ANS:

Current mask= 255.255.255.0

Bits needs for 30 subnets =5 =25 =32 possible subnets

Bits left for hosts = 3 = 23  = 8-2=6 possible hosts.

So our mask in binary =**11111000**= **248** decimal

Final Mask =**255.255.255.248**

Address of host 3 on subnet 2 is

subnet 2 =00010000 host 3 =000000011

Add the two together =00010011=19

therefore IP address of host 3 on subnet  2 =205.11.2.19

**Transmission Control Protocol**

## What is TCP?

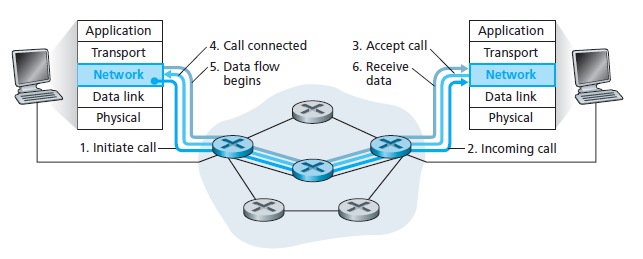
TCP/IP helps you to determine how a specific computer should be connected to the internet and how you can transmit data between them. It helps you to create a virtual network when multiple computer networks are connected.

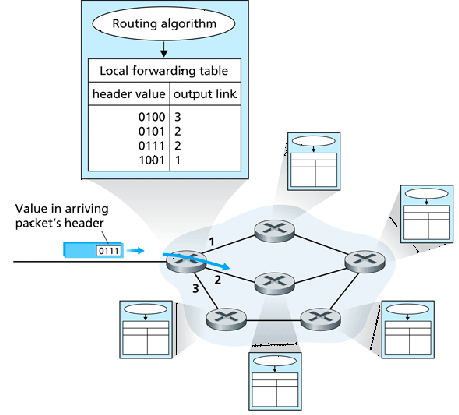
TCP/IP stands for Transmission Control Protocol/ Internet Protocol. It is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.

1 connctiopn establishment

2. data transfer

3. realease connection





## What is UDP?

UDP is a Datagram oriented protocol. It is used for broadcast and multicast type of network transmission. The full form of UDP is User Datagram Protocol (A datagram is a transfer unit associated with a packet-switched network.) The UDP protocol works almost similar to TCP, but it throws all the error-checking stuff out, all the back-and-forth communication and deliverability.

## KEY DIFFERENCES:

* TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol.
* The speed for TCP is slower while the speed of UDP is faster
* TCP uses handshake protocol like SYN, SYN-ACK, ACK while UDP uses no handshake protocols
* TCP does error checking and also makes error recovery, on the other hand, UDP performs error checking, but it discards erroneous packets.
* TCP has acknowledgment segments, but UDP does not have any acknowledgment segment.
* TCP is heavy-weight, and UDP is lightweight.

## How TCP work?

A TCP connection is established with the help of three-way handshake. It is a process of initiating and acknowledging a connection. Once the connection is established, data transfer begins, and when the transmission process is finished, the connection is terminated by the closing of an established virtual circuit.

## How UDP work?

UDP uses a simple transmission method without implied hand-shaking dialogues for ordering, reliability, or data integrity. UDP also assumes that error checking and correction is not important or performed in the application, to avoid the overhead of such processing at the network interface level. It is also compatible with packet broadcasts and multicasting.

## Features of TCP

Here, are some important features of TCP

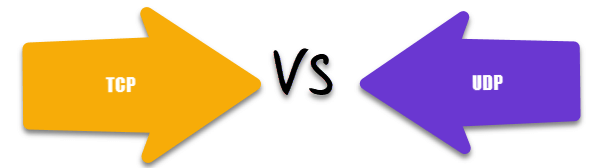
* Delivery Acknowledgements
* Re transmission
* Delays transmission when the network is congested
* Easy Error detection

Here, are some important feature of UDP:

* Supports bandwidth-intensive applications that tolerate packet loss
* Less delay
* It sends the bulk quantity of packets.
* Possibility of the Data loss
* Allows small transaction ( DNS lookup)

## Difference between TCP and UDP

Here, are the differences between TCP and UDP

[](https://www.guru99.com/images/1/011720_0714_TCPvsUDPWha1.png)

|  |  |
| --- | --- |
| **TCP** | **UDP** |
| It is a connection-oriented protocol. | It is a connectionless protocol. |
| TCP reads data as streams of bytes, and the message is transmitted to segment boundaries. | UDP messages contain packets that were sent one by one. It also checks for integrity at the arrival time. |
| TCP messages make their way across the internet from one computer to another. | It is not connection-based, so one program can send lots of packets to another. |
| TCP rearranges data packets in the specific order. | UDP protocol has no fixed order because all packets are independent of each other. |
| The speed for TCP is slower. | UDP is faster as error recovery is not attempted. |
| Header size is 20 bytes | Header size is 8 bytes. |
| TCP is heavy-weight. TCP needs three packets to set up a socket connection before any user data can be sent. | UDP is lightweight. There are no tracking connections, ordering of messages, etc. |
| TCP does error checking and also makes error recovery. | UDP performs error checking, but it discards erroneous packets. |
| Acknowledgment segments | No Acknowledgment segments |
| Using handshake protocol like SYN, SYN-ACK, ACK | No handshake (so connectionless protocol) |
| TCP is reliable as it guarantees delivery of data to the destination router. | The delivery of data to the destination can't be guaranteed in UDP. |
| TCP offers extensive error checking mechanisms because it provides flow control and acknowledgment of data. | UDP has just a single error checking mechanism which is used for checksums. |

## Application of TCP

Here, are pros/benefits of using the TCP/IP model:

* It helps you to establish/set up a connection between different types of computers.
* Operates independently of the operating system
* Supports many routing-protocols.
* It enables the internetworking between the organizations.
* It can be operated independently.
* Supports several routing protocols.
* TCP can be used to establish a connection between two computers.

## Application of UDP

* UDP method is largely used by time-sensitive applications as well as by servers that answer small queries from a larger client base.
* UDP is compatible with packet broadcasts for sending all over the network and for multicasting sending.
* It is also used in Domain Name System, Voice over IP, and online games.

## Advantage of TCP

Here, are pros/benefits of TCP:

* It helps you to establish/set up a connection between different types of computers.
* It operates independently of the operating system.
* It supports many routing-protocols.
* It enables the internetworking between the organizations.
* TCP/IP model has a highly scalable client-server architecture.
* It can be operated independently.
* Supports several routing protocols.
* It can be used to establish a connection between two computers.

## Advantage of UDP

Here are the pros/benefits of UDP:

* It never restricts you to a connection-based communication model; that's why startup latency in distributed applications is low.
* The recipient of UDP packets gets them unmanaged, which also includes block boundaries.
* Broadcast and multicast transmission are also available with UDP
* Data loss can be made
* Small transaction ( DNS lookup)
* Bandwidth intensive app which endures packet loss

## Disadvantages of TCP

Here, are disadvantage of using TCP:

* TCP never conclude a transmission without all data in motion being explicitly asked.
* You can't use for broadcast or multicast transmission.
* TCP has no block boundaries, so you need to create your own.
* TCP offers many features that you don't want. It may waste bandwidth, time, or effort.
* In this, model the transport layer does not guarantee delivery of packets.
* Replacing protocol in TCP/IP is not easy.
* It doesn't offer clear separation from its services, interfaces, and protocols.

## Disadvantages of UDP

Here, are important cons/drawback of UDP:

* In UDP protocol, a packet may not be delivered or delivered twice. It may be delivered out of order, so you get no indication.
* Routers are quite careless with UDP, so they never retransmit it if it collides.
* UDP has no Congestion Control, and flow control, so implementation is the job of a user application.
* UDP mostly like to suffer from worse packet loss

## When to use UDP and TCP?

* TCP is an ideal choice, and even it has associated overhead, Therefore, when most of the overhead is in the connection, your application stays connected for any length of time.
* UDP is ideal to use with multimedia like VoIP.
* Use TCP sockets when both client and server independently send packets at that time; an occasional delay is acceptable. (e.g., Online Poker).
* You should use user UDP if both client and server may separately send packets, and occasional delay is also not acceptable. (e.g., Multiplayer games).

**IPV6**

Internet Protocol version 6 is a new addressing protocol designed to incorporate all the possible requirements of future Internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on the Network Layer (Layer-3). Along with its offering of an enormous amount of logical address space, this protocol has ample features to which address the shortcoming of IPv4.

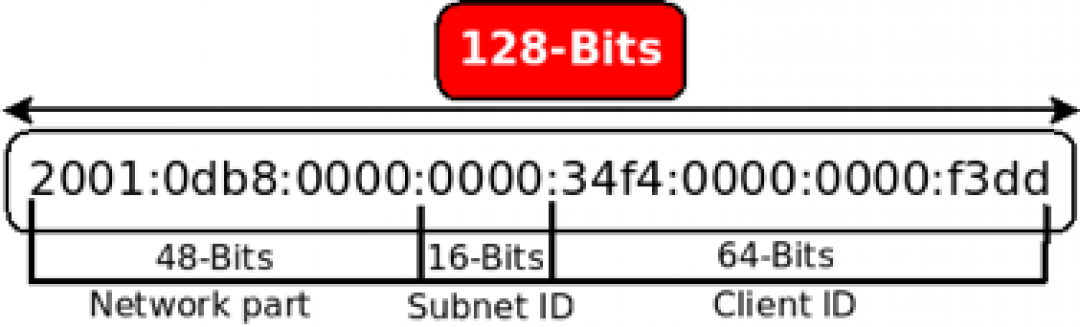
## Why New IP Version?

At the time of its birth, Internet was limited only to a few universities for their research and to the Department of Defense. IPv4 is 32 bits long and offers around **4,294,967,296** **(232) addresses**. This address space was considered more than enough that time. Given below are the major points that played a key role in the birth of IPv6:

* Internet has grown exponentially and the address space allowed by IPv4 is saturating. There is a requirement to have a protocol that can satisfy the needs of future Internet addresses that is expected to grow in an unexpected manner.
* IPv4 on its own does not provide any security feature. Data has to be encrypted with some other security application before being sent on the Internet.
* Data prioritization in IPv4 is not up to date. Though IPv4 has a few bits reserved for Type of Service or Quality of Service, but they do not provide much functionality.
* IPv4 enabled clients can be configured manually or they need some address configuration mechanism. It does not have a mechanism to configure a device to have globally unique IP address.

IPv6 uses 128-bit (2128) addresses, allowing 3.4 x 1038 unique IP addresses. This is equal to 340 trillion trillion trillion IP addresses. IPv6 is written in hexadecimal notation, separated into 8 groups of 16 bits by the colons, thus (8 x 16 = 128) bits in total.

The successor of IPv4 is not designed to be backward compatible. Trying to keep the basic functionalities of IP addressing, IPv6 is redesigned entirely. It offers the following features:



* **Larger Address Space**

In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×1038 different combinations of addresses. This address can accumulate the aggressive requirement of address allotment for almost everything in this world. According to an estimate, 1564 addresses can be allocated to every square meter of this earth.

* **Simplified Header**

IPv6’s header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 provided the fact that IPv6 address is four times longer.

* **End-to-end Connectivity**

Every system now has unique IP address and can traverse through the Internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.

* **Auto-configuration**

IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way, absence of a DHCP server does not put a halt on inter segment communication.

* **Faster Forwarding/Routing**

Simplified header puts all unnecessary information at the end of the header. The information contained in the first part of the header is adequate for a Router to take routing decisions, thus making routing decision as quickly as looking at the mandatory header.

* **IPSec**

Initially it was decided that IPv6 must have IPSec security, making it more secure than IPv4. This feature has now been made optional.

* **No Broadcast**

Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any broadcast support any more. It uses multicast to communicate with multiple hosts.

* **Anycast Support**

This is another characteristic of IPv6. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, send the packet to the nearest destination.

* **Mobility**

IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.

* **Enhanced Priority Support**

IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide Quality of Service but it could only be used if the end-to-end devices support it, that is, the source and destination device and underlying network must support it.

In IPv6, Traffic class and Flow label are used to tell the underlying routers how to efficiently process the packet and route it.

* **Smooth Transition**

Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This mechanism saves IP addresses and NAT is not required. So devices can send/receive data among each other, for example, VoIP and/or any streaming media can be used much efficiently.

Other fact is, the header is less loaded, so routers can take forwarding decisions and forward them as quickly as they arrive.

* **Extensibility**

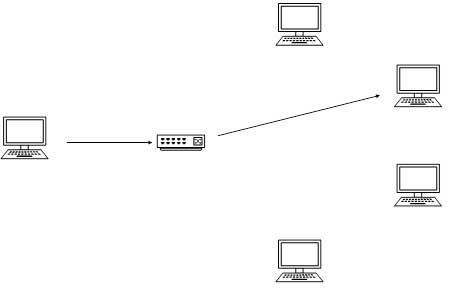
One of the major advantages of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options, whereas options in IPv6 can be as much as the size of IPv6 packet itself.

# **IPv6 - Addressing Modes**

In computer networking, addressing mode refers to the mechanism of hosting an address on the network. IPv6 offers several types of modes by which a single host can be addressed. More than one host can be addressed at once or the host at the closest distance can be addressed.

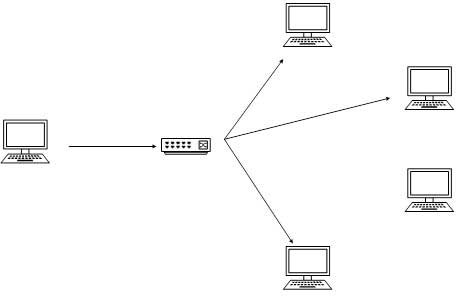
## Unicast

In unicast mode of addressing, an IPv6 interface (host) is uniquely identified in a network segment. The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment.When a network switch or a router receives a unicast IP packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host.



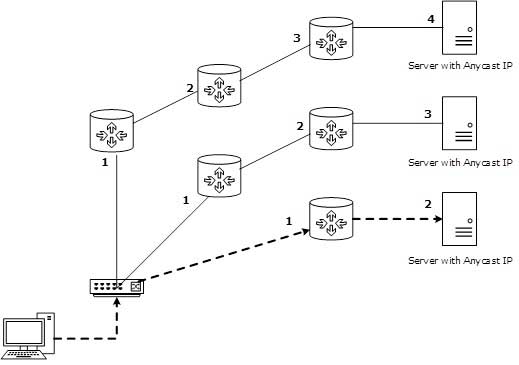
## Multicast

The IPv6 multicast mode is same as that of IPv4. The packet destined to multiple hosts is sent on a special multicast address. All the hosts interested in that multicast information, need to join that multicast group first. All the interfaces that joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.



## Anycast

IPv6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message. With the help of complex routing mechanism, that Unicast message is delivered to the host closest to the Sender in terms of Routing cost.

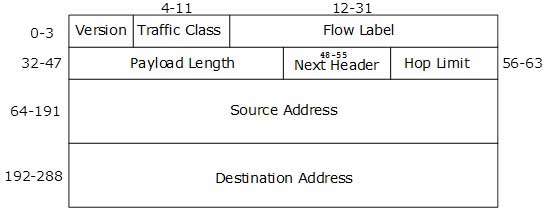


Let’s take an example of TutorialPoints.com Web Servers, located in all continents. Assume that all the Web Servers are assigned a single IPv6 Anycast IP Address. Now when a user from Europe wants to reach TutorialsPoint.com the DNS points to the server that is physically located in Europe itself. If a user from India tries to reach Tutorialspoint.com, the DNS will then point to the Web Server physically located in Asia. Nearest or Closest terms are used in terms of Routing Cost.

In the above picture, when a client computer tries to reach a server, the request is forwarded to the server with the lowest Routing Cost.

The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

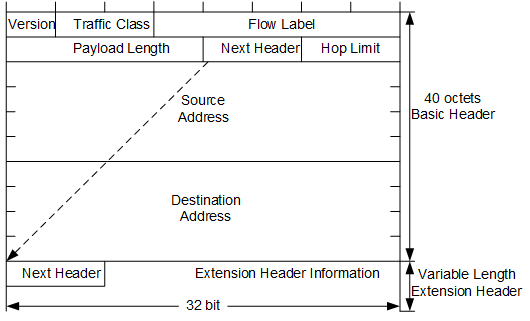
## Fixed Header

[*Image: IPv6 Fixed Header*]

IPv6 fixed header is 40 bytes long and contains the following information.

|  |  |
| --- | --- |
| S.N. | Field & Description |
| 1 | **Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110. |
| 2 | **Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN). |
| 3 | **Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media. |
| 4 | **Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0. |
| 5 | **Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4’s. |
| 6 | **Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded. |
| 7 | **Source Address** (128-bits): This field indicates the address of originator of the packet. |
| 8 | **Destination Address** (128-bits): This field provides the address of intended recipient of the packet. |

## Extension Headers

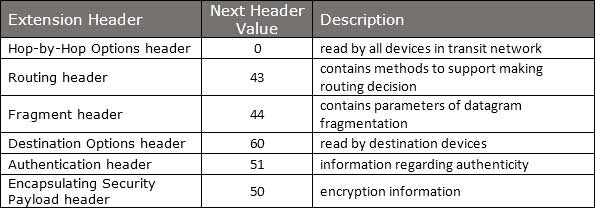


In IPv6, the Fixed Header contains only that much information which is necessary, avoiding those information which is either not required or is rarely used. All such information is put between the Fixed Header and the Upper layer header in the form of Extension Headers. Each Extension Header is identified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

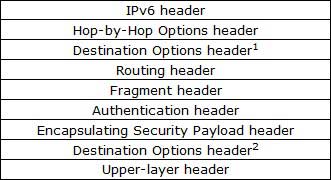
When Extension Headers are used, IPv6 Fixed Header’s Next Header field points to the first Extension Header. If there is one more Extension Header, then the first Extension Header’s ‘Next-Header’ field points to the second one, and so on. The last Extension Header’s ‘Next-Header’ field points to the Upper Layer Header. Thus, all the headers points to the next one in a linked list manner.

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

The following Extension Headers must be supported as per RFC 2460:



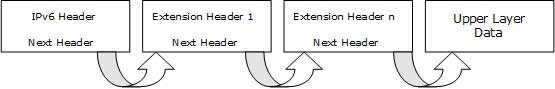
The sequence of Extension Headers should be:



These headers:

* 1. should be processed by First and subsequent destinations.
* 2. should be processed by Final Destination.

Extension Headers are arranged one after another in a linked list manner, as depicted in the following diagram:

[*Image: Extension Headers Connected Format*]

## **What is IP routing?**

**IP Routing** is a process that sends packets from a host on one network to another host on a different remote network. It helps you examine the destination IP address of a packet, determine the next-hop address, and forward it. IP routers use routing tables to determine the next-hop address to which the packet should be delivered.

In CISCO IP routing, data is routed from its source to its destination through routers and across multiple networks. The IP Routing protocols allow routers to build up a forwarding table that correlates final destinations with next-hop addresses.

## **Routing Metrics**

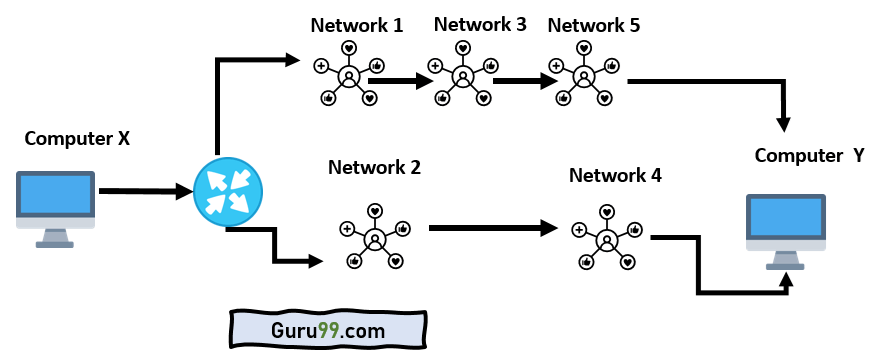
Routing metric are the value that allows the routers to decide the best route for the data packet

Different routing metrics are:

* Hops
* Bandwidth
* Load
* Cost
* Reliability

## Why Routing Protocols?

Consider the below given image-

[](https://www.guru99.com/images/2/110620_0425_IPRoutingWh1.png)How routing protocol works?

* Should data pass through networks 1, 3, and 5 or networks 2 and 4?.
* At first glance, data should take the shorter path through networks 2 and 4.
* But networks 1, 3, and 5 might be faster at forwarding packets than 2 and 4.
* These are the kinds of choices network routers constantly make.

## What is the Default gateway?

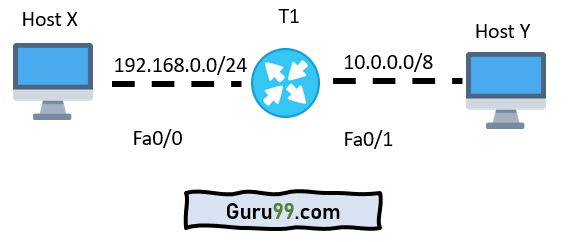
PROTOCOL CONVERTER

A default gateway is a router that hosts use to communicate with other hosts on remote networks. A default gateway is used when a host does not have a route entry for the particular remote network and does not know how to reach that network.

Hosts should be configured to send all packets destined to the default gateway's remote networks, which has a route to reach that specific network.

## How does IP routing work?

The following example explains the concept of a default gateway more thoroughly.

[](https://www.guru99.com/images/2/110620_0425_IPRoutingWh2.png)Default gateway

* Host X has an IP address of the router T1 configured as the default gateway address.
* Here, host X is trying to communicate with host Y, which is a host on another remote network.
* This host looks up in its routing table to check if there is an entry for the destination network address.
* If the entry is found, the host will send all data to the router T1.
* Router T1 then receives the packets and forwards them to host Y.

## Routing Table

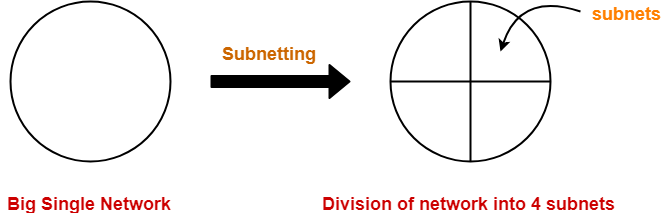
Every router maintains a routing table which is stored in its RAM. A routing table is widely used by routers to decide the path to the destination network. There are mainly three different methods for populating a routing table:

* Directly connected subnets
* Using static routing
* Using dynamic routing

Before you go through this article, make sure that you have gone through the previous article on [Subnetting](https://www.gatevidyalay.com/subnetting-ip-subnetting-examples/).

We have discussed-

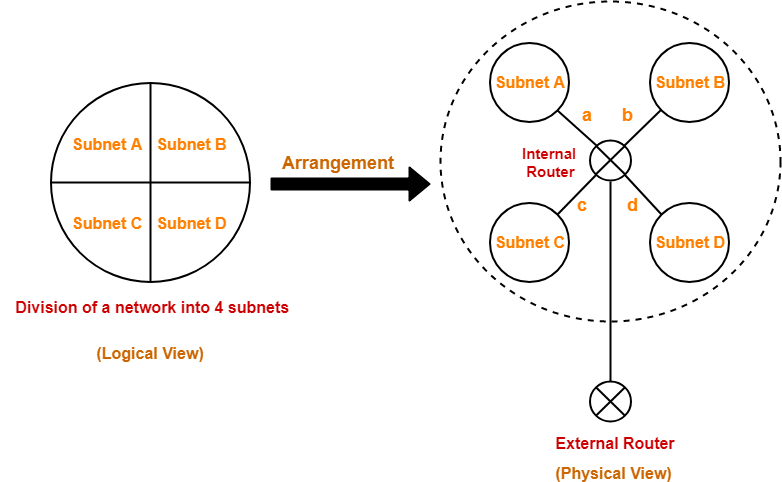
* Subnetting is a process of dividing a single network into multiple smaller networks.
* The number of sub networks created depends upon the requirement.



## Arrangement Of Subnets-

* All the subnets are connected to an internal router.
* Internal router is connected to an external router.
* The link connecting the internal router with a subnet is called as an interface.

## Example-



## Working-

When a data packet arrives,

* External router forwards the data packet to the internal router.
* Internal router identifies the interface on which it should forward the incoming data packet.
* Internal router forwards the data packet on that interface.

## Routing Table-

* A table is maintained by the internal router called as Routing table.
* It helps the internal router to decide on which interface the data packet should be forwarded.

 Routing table consists of the following three fields-

1. IP Address of the destination subnet
2. Subnet mask of the subnet
3. Interface

## Example-

Consider a network is subnetted into 4 subnets as shown in the above picture.

The IP Address of the 4 subnets are-

1. 200.1.2.0 (Subnet A)
2. 200.1.2.64 (Subnet B)
3. 200.1.2.128 (Subnet C)
4. 200.1.2.192 (Subnet D)

Then, Routing table maintained by the internal router looks like-

|  |  |  |
| --- | --- | --- |
| Destination | Subnet Mask | Interface |
| 200.1.2.0 | 255.255.255.192 | a |
| 200.1.2.64 | 255.255.255.192 | b |
| 200.1.2.128 | 255.255.255.192 | c |
| 200.1.2.192 | 255.255.255.192 | d |
| Default | 0.0.0.0 | e |

Routing Table Example

When a data packet arrives to the internal router, it follows the following steps-

## Step-01:

Router performs the bitwise ANDing of-

* Destination IP Address mentioned on the data packet
* And all the subnet masks one by one.

## Step-02:

Router compares each result with their corresponding IP Address of the destination subnet in the routing table.

Then, following three cases may occur-

### Case-01:

If there occurs only one match,

* Router forwards the data packet on the corresponding interface.

### Case-02:

If there occurs more than one match,

* Router forwards the data packet on the interface corresponding to the longest subnet mask.

### Case-03:

If there occurs no match,

* Router forwards the data packet on the interface corresponding to the default entry.

PRACTICE PROBLEMS BASED ON ROUTING TABLE-

## Problem-01:

A router uses the following routing table-

|  |  |  |
| --- | --- | --- |
| Destination | Mask | Interface |
| 144.16.0.0 | 255.255.0.0 | eth0 |
| 144.16.64.0 | 255.255.224.0 | eth1 |
| 144.16.68.0 | 255.255.255.0 | eth2 |
| 144.16.68.64 | 255.255.255.224 | eth3 |

A packet bearing a destination address 144.16.68.117 arrives at the router. On which interface will it be forwarded?

1. eth0
2. eth1
3. eth2
4. eth3

## Solution-

Router performs the bitwise ANDing of-

* Destination address mentioned on the data packet
* And each subnet mask one by one.

### 1st Row-

144.16.68.117 AND 255.255.0.0

= 144.16.0.0

Since result is same as the given destination address, so a match occurs.

1111111.11111111.00000000.00000000

1010101.00110011.10101111.11100011

### 2nd Row-

144.16.68.117 AND 255.255.224.0

= 144.16.64.0

Since result is same as the given destination address, so a match occurs.

### 3rd Row-

144.16.68.117 AND 255.255.255.0

= 144.16.68.0

Since result is same as the given destination address, so a match occurs.

### 4th Row-

144.16.68.117 AND 255.255.255.224

= 144.16.68.96

Since result is not same as the given destination address, so a match does not occur.

Now,

* Clearly, there occurs more than one match.
* So, router forwards the packet on the interface corresponding to the longest subnet mask.
* Out of all, 255.255.255.0 is the longest subnet mask since it has maximum number of 1s.

So,

* Router forwards the packet on the interface corresponding to the subnet mask 255.255.255.0.
* The corresponding interface is eth2.

Thus, Option (C) is correct.

[Routing Table in Networking | Examples | Gate Vidyalay](https://www.gatevidyalay.com/subnetting-in-networking-routing-table/)

**Types of Routing**

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

**There are 3 types of routing:  
1. Static routing**   
Static routing is a process in which we have to manually add routes in routing table.  
**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.

**2. 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.

and [**OSPF**](https://www.geeksforgeeks.org/computer-network-open-shortest-path-first-ospf-protocol-fundamentals/)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:

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

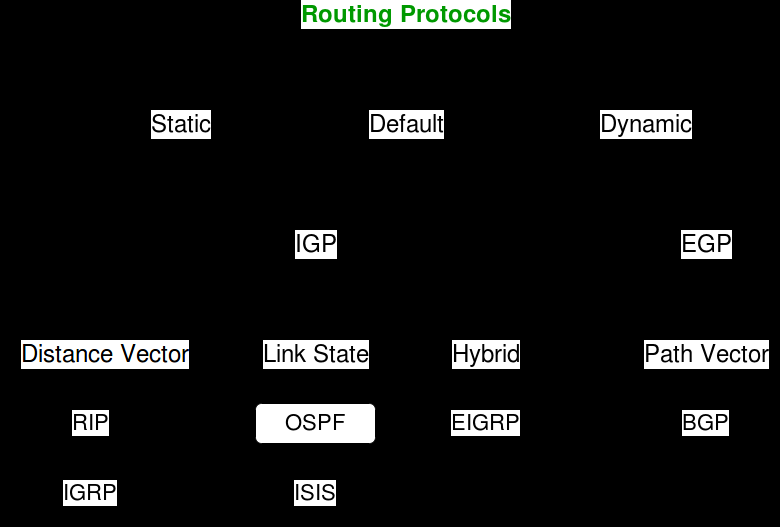
Advantages –

* 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.

## Types of Routing Protocols



The following protocols help data packets find their way across the Internet:

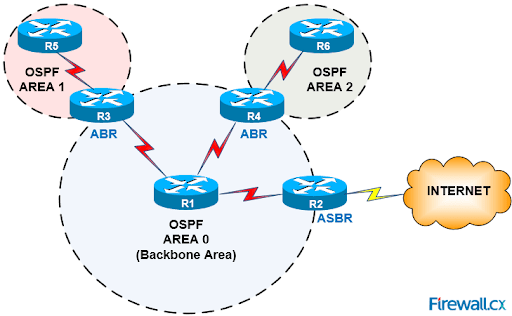
### IP:

The Internet Protocol (IP) specifies the origin and destination for each data packet. Routers inspect each packet's IP header to identify where to send them.

### **OSPF:**

In Area, the special router also exists. The special routers are those that are present at the border of an area, and these special routers are known as Area Border Routers. This router summarizes the information about an area and shares the information with other areas.

All the areas inside an autonomous system are connected to the backbone routers, and these backbone routers are part of a primary area. The role of a primary area is to provide communication between different areas.



### How does OSPF work?

There are three steps that can explain the working of OSPF:

Step 1: The first step is to become OSPF neighbors. The two connecting routers running OSPF on the same link creates a neighbor relationship.

Step 2: The second step is to exchange database information. After becoming the neighbors, the two routers exchange the LSDB information with each other.

Step 3: The third step is to choose the best route. Once the LSDB information has been exchanged with each other, the router chooses the best route to be added to a routing table based on the calculation of SPF.

Open Shortest Path First (OSPF) protocol is **a link-state** IGP tailor-made for IP networks using the Shortest Path First (SPF) method.

The OSPF (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.

There are four types of links in OSPF:

1. Point-to-point link: The point-to-point link directly connects the two routers without any host or router in between.
2. Transient link: When several routers are attached in a network, they are known as a transient link.  
   The transient link has two different implementations:  
   Unrealistic topology: When all the routers are connected to each other, it is known as an unrealistic topology.  
   Realistic topology: When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.
3. Stub link: It is a network that is connected to the single router. Data enters to the network through the single router and leaves the network through the same router.
4. Virtual link: If the link between the two routers is broken, the administration creates the virtual path between the routers, and that path could be a long one also.

There are five different types of packets in OSPF:

* **Hello**

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

* **Database Description**
* After establishing a connection, if the neighbor router is communicating with the system first time, it sends the database information about the network topology to the system so that the system can update or modify accordingly.
* **Link state request**
* The link-state request is sent by the router to obtain the information of a specified route. Suppose there are two routers, i.e., router 1 and router 2, and router 1 wants to know the information about the router 2, so router 1 sends the link state request to the router 2. When router 2 receives the link state request, then it sends the link-state information to router 1.
* **Link state update**
* The link-state update is used by the router to advertise the state of its links. If any router wants to broadcast the state of its links, it uses the link-state update.
* **Link state Acknowledgment**
* The link-state acknowledgment makes the routing more reliable by forcing each router to send the acknowledgment on each link state update. For example, router A sends the link state update to the router B and router C, then in return, the router B and C sends the link- state acknowledgment to the router A, so that the router A gets to know that both the routers have received the link-state update.

E T U

A F H G D

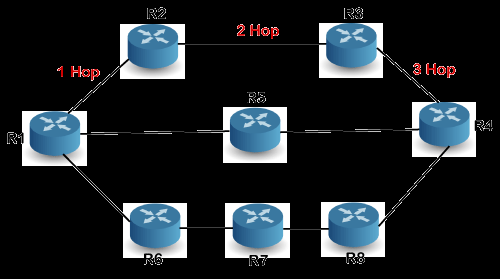
B K L

### RIP:

RIP is used in both LAN and WAN Networks**.** It also runs on the application layer of the OSI model. The full form of RIP is the Routing Information Protocol. Two versions of RIP are

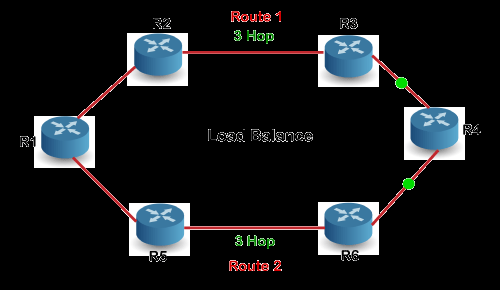
1. RIPv1
2. RIPv2

### How does the RIP work?



If there are 8 routers in a network where Router 1 wants to send the data to Router 3. If the network is configured with RIP, it will choose the route which has the least number of hops. There are three routes in the above network, i.e., Route 1, Route 2, and Route 3. The Route 2 contains the least number of hops, i.e., 2 where Route 1 contains 3 hops, and Route 3 contains 4 hops, so RIP will choose Route 2.

### Let's look at another example.

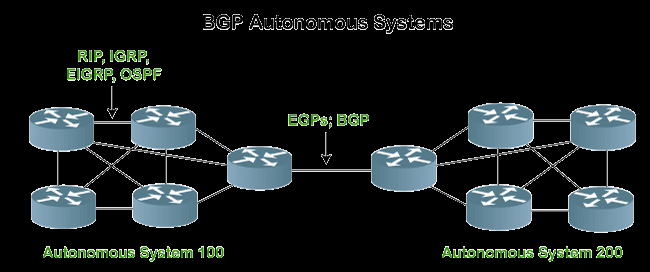


Suppose R1 wants to send the data to R4. There are two possible routes to send data from r1 to r2. As both the routes contain the same number of hops, i.e., 3, so RIP will send the data to both the routes simultaneously. This way, it manages the load balancing, and data reach the destination a bit faster.

### BGP:

BGP is a routing protocol of the Internet, which is classified as a DPVP (distance path vector protocol). The full form of BGP is the Border Gateway Protocol.

It is an interdomain routing protocol, and it uses the path-vector routing. It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet.

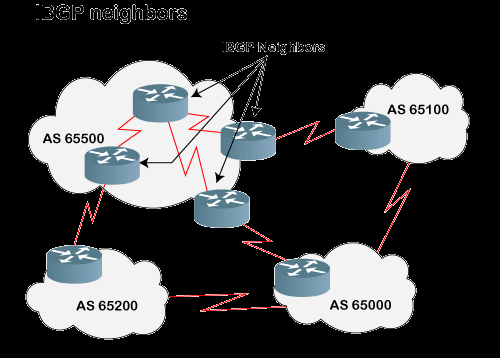


### BGP Neighbors

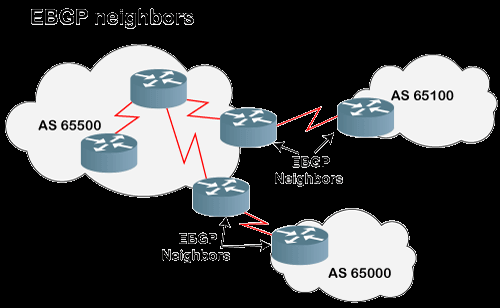
BGP neighborship is similar to the OSPF neighborship, but there are few differences. BGP forms the neighboring relationship with the help of the [TCP](https://www.javatpoint.com/tcp) connection on port number 179 and then exchanges the BGP updates. They exchange the updates after forming the neighbor relationship. In BGP, the neighbor relationship is configured manually. BGP neighbors are also known as BGP peers or BGP speakers.

There are two types of neighbor relationship:

* IBGP (Internal BGP): If all the routers are neighbors of each other and belong to the same autonomous number system, the routers are referred to as an IBGP.



EBGP (External BGP): If all the routers are neighbors of each other and they belong to the different autonomous number systems, then the routers are referred to as an EBGP.



### Types of packets

There are four different types of packets exist in BGP:

* **Open**: When the router wants to create a neighborhood relation with another router, it sends the Open packet.
* Update: The update packet can be used in either of the two cases:

1. It can be used to withdraw the destination, which has been advertised previously.
2. It can also be used to announce the route to the new destination.

* **Keep Alive**: The keep alive packet is exchanged regularly to tell other routers whether they are alive or not. For example, there are two routers, i.e., R1 and R2. The R1 sends the keep alive packet to R2 while R2 sends the keep alive packet to R1 so that R1 can get to know that R2 is alive, and R2 can get to know that R1 is alive.
* Notification: The notification packet is sent when the router detects the error condition or close the connection.