# UNIT 2

# Network Layer Services: Packetizing, Routing and Forwarding, Other Services

**Network layer** is the third layer in the OSI model of computer networks. It's main function is to transfer network packets from the source to the destination. It is involved both at the source host and the destination host. At the source, it accepts a packet from the transport layer, encapsulates it in a datagram and then deliver the packet to the data link layer so that it can further be sent to the receiver. At the destination, the datagram is decapsulated, the packet is extracted and delivered to the corresponding transport layer.

## Features :

1. Main responsibility of Network layer is to carry the data packets from the source to the destination without changing or using it.
2. If the packets are too large for delivery, they are fragmented i.e., broken down into smaller packets.
3. It decides the route to be taken by the packets to travel from the source to the destination among the multiple routes available in a network (also called as routing).
4. The source and destination addresses are added to the data packets inside the network layer.

The **services** which are offered by the network layer protocol are as follows:

### 1. Packetizing –

The process of encapsulating the data received from upper layers of the network(also called as payload) in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination is known as packetizing.
The source host adds a header that contains the source and destination address and some other relevant information required by the network layer protocol to the payload received from the upper layer protocol, and delivers the packet to the data link layer.

The destination host receives the network layer packet from its data link layer, decapsulates the packet, and delivers the payload to the corresponding upper layer protocol. The routers in the path are not allowed to change either the source or the destination address. The routers in the path are not allowed to decapsulate

the packets they receive unless they need to be fragmented.

2. **Routing and Forwarding –**

   These are two other services offered by the network layer. In a network, there are a number of routes available from the source to the destination. The network layer specifies has some strategies which find out the best possible route. This process is referred to as routing. There are a number of routing protocols which are used in this process and they should be run to help the routers coordinate with each other and help in establishing communication throughout the network.
   Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces. When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network (unicast routing) or to some attached networks(in case of multicast routing).

Some of the other **services which are expected** from the network layer are:

1. **Error Control –**
   Although it can be implemented in the network layer, but it is usually not preferred because the data packet in a network layer maybe fragmented at each router, which makes error checking inefficient in the network layer.

2. **Flow Control –**
   It regulates the amount of data a source can send without overloading the receiver. If the source produces a data at a very faster rate than the receiver can consume it, the receiver will be overloaded with data. To control the flow of data, the receiver should send a feedback to the sender to inform the latter that it is overloaded with data.
   There is a lack of flow control in the design of the network layer. It does not directly provide any flow control. The datagrams are sent by the sender when they are ready, without any attention to the readiness of the receiver.

3. **Congestion Control –**
   Congestion occurs when the number of datagrams sent by source is beyond the capacity of network or routers. This is another issue in the network layer protocol. If congestion continues, sometimes a situation may arrive where the system collapses and no datagrams are delivered. Although congestion control is indirectly implemented in network layer, but still there is a lack of congestion control in the network layer.

## PACKET SWITCHING:

The packets received at the router will get switched to the other router, and the 'packets are switched' in two different ways.

1. Datagram switching [Connectionless Service]
2. Virtual-Circuit OR Circuit Switching [Connection Oriented Service]

# SWITCHING

The passage of a message from a source to a destination **involves many decisions.** When a message reaches a connecting device, a decision needs to be made to select one of the output ports through which the packet needs to be send out.

## Packet Switching

- The network layer is responsible for **host-to-host delivery** and for **routing the packets** through the routers.
- A connecting device such as a router acts as a switch. When a packet arrives from one of its ports (interface), the packet is forwarded through another port tothe next switch (or final destination).
- A process called switching occurs at the connecting device.

# Circuit Switching

- A physical circuit (or channel) is established between the source and destination of the message before the delivery of the message. After the circuit is established, the entire message, is transformed from the source to the destination.
- The circuit switching was never implemented at the network layer; it is mostly used at the physical layer.
- In circuit switching, the whole message is sent from the source to the destination without being divided into packets.

# Packet Switching

- The network layer in the Internet today is a packet-switched network.
- In packet switching, the message is first divided into manageable packets at the source (normally called **Datagrams** in the network layer) before being transmitted. The packets are assembled at the destination.
- The connecting devices in a packet-switching network still need to decide how to route the packets to the final destination.
- Today, a packet-switched network can use two different approaches to route the packets: the datagram approach and the virtual circuit approach.

# Packet Switching at Network Layer

- The network layer is designed as a packet-switched network.
- The packet-switched network layer of the Internet was originally designed as a ***Connectionless service,*** but recently there is a tendency to change this *to a* ***Connectionoriented service.*** We first discuss the dominant trend and thenbriefly discuss the new one.

# Datagram Approach: Connectionless Service

- When the Internet started, the network layer was designed to provide a connectionless service.
- The network layer protocol **treats each packet independently**.
- The packets in a message **may or may not travel the same path to their destination.**
- The switches in this type of network are called **routers**.
- Each packet is routed based on the information contained in its header.
- In a connectionless packet-switched network, the forwarding decision is based on the **destination address of the packet**.

**Figure 18.3** *A connectionless packet-switched network*

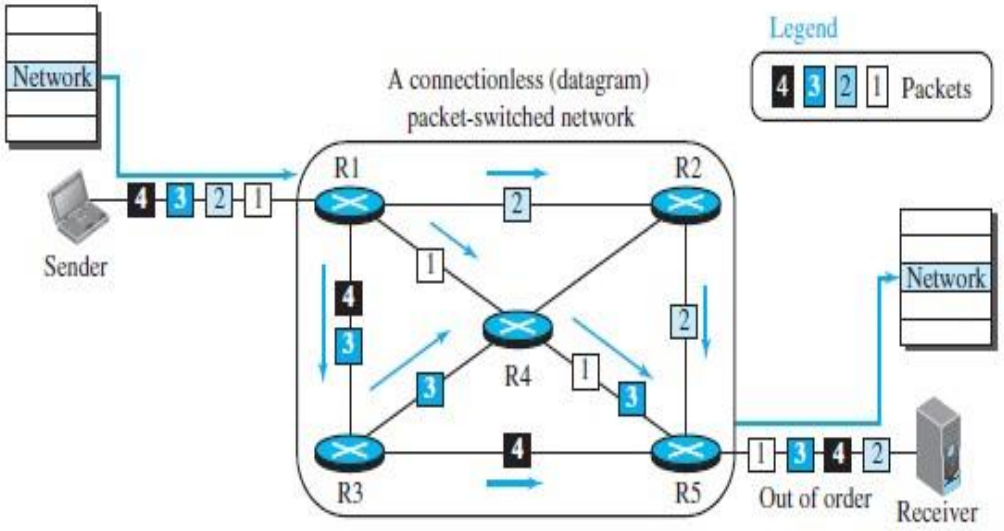
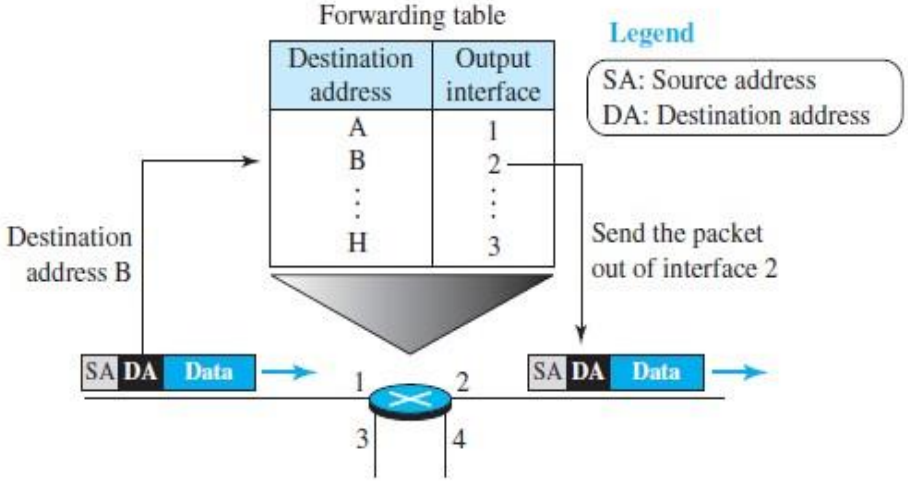



**Figure 18.4** *Forwarding process in a router when used in a connectionless network*




**In the datagram approach, the forwarding decision is based on the destination address of the packet.**

# Virtual-Circuit Approach: Connection-Oriented Service

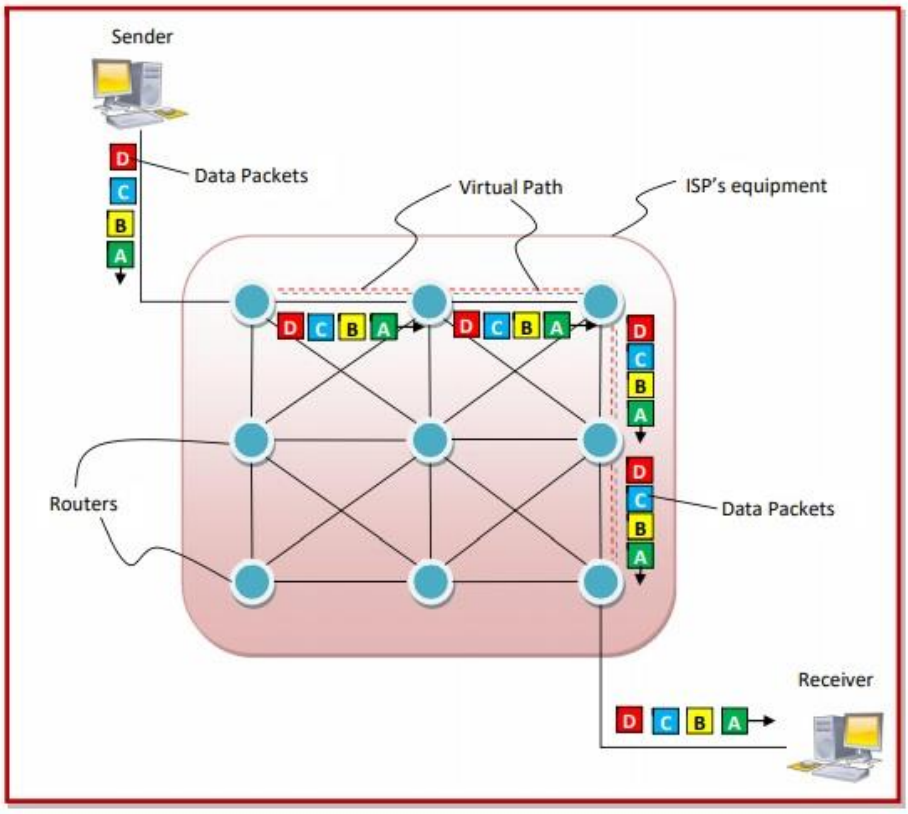
- In a connection-oriented service, there is a relation between all packetsbelonging to a message.
- Before all datagrams in a message can be sent, **a virtual connection should beset up to define the path for the datagrams.**
- After connection setup, the datagrams can follow the same path.
- In this type of service, not only must the packet contain the source and destination addresses, it must also contain **a *flow label,* a *virtual circuitidentifier*** that defines the virtual path the packet should follow.
- In a connection-oriented packet switched network, **the forwarding decision** isbased on the ***label*** of the packet.

## Phases of Virtual - Circuit Transmission

There are three phases of transmission by virtual circuits, set up, data transfer and teardown.

- **Set up Phase** − In this phase, a virtual circuit or a route is established from the source to the destination through number of switches. The source and destination use global addresses using which the switches make routing table entries.
- **Data Transfer** − Once the virtual circuit is set up, all packets follow the route established during the set up phase adhering to the routing tables.
- **Teardown Phase** − When data transfer is complete, the source sends a teardown request. The destination responds using a teardown confirmation. The switches flush their routing table entries, thus relinquishing the circuit.

In the following diagram, we can that a virtual circuit is created, as denoted by the dotted lines, and all the packets from the sender to the receiver are being routed along this virtual circuit.




## NETWORK-LAYER PERFORMANCE: Delay, Throughput, Packet Loss

# How do you measure Network Performance?

The examination and review of collective network information to describe the quality of services delivered by the underlying computer network is known as "network performance".

It is a qualitative and quantitative procedure that assesses and defines a network's performance level. Thus, it assists a network administrator in reviewing, evaluating, and improving network services.

## Parameters Used to Measure Network Performance

The following parameters are used to measure Network Performance −

- Bandwidth
- Throughput
- Latency

- Packet Loss
- Jitter

Let us discuss each of these parameters in detail.

## Bandwidth

The quantity of bandwidth allocated to the network is one of the most important conditions of a website's performance. The web server's bandwidth controls how quickly it can transfer the requested data. While there are many elements to consider regarding a site's speed, bandwidth is frequently the limiting issue.

The amount of data or information that can be transmitted in a given amount of time is referred to as bandwidth. The phrase can be applied in two ways, each having its own set of estimating values. The bandwidth of digital devices is measured in bits per second (bps) or bytes per second (bps). The bandwidth of analog devices is measured in cycles per second, or Hertz (Hz).

## Throughput

The number of messages successfully delivered per unit time is referred to as throughput. Throughput is influenced by the available bandwidth, as well as the available signal-to-noise ratio and device limitations.

To separate the concepts of throughput and latency, throughput will be calculated from the arrival of the first bit of data reaching the receiver for this article. The terms 'throughput' and 'bandwidth' are frequently interchanged in discussions of this nature.

The Time Window refers to the time frame in which the throughput is calculated. The selection of a suitable time window will frequently determine whether or not latency affects throughput. Likewise, whether or not latency is taken into account will determine whether or not latency impacts throughput.

## Latency

Latency is simply the time it takes for data to travel from one designated location to another regarding network performance evaluation. The term "delay" is sometimes used to describe this attribute. The latency of a network should be as low as possible.

Speed of light is the fundamental factor for latency, but packet queuing and refractive index of fiber optic cable are also two factors that can be used to reduce latency.

## Packet Loss

Packet loss refers to the number of packets that fail to transfer from one destination to another regarding network performance measurement. This statistic can be measured by recording traffic data on both ends and then identifying lost packets and packet retransmission.

Network congestion, router performance, and software difficulties, among other things, can cause packet loss.

## Jitter

The variance in time delay for data packets carried over a network is known as jitter. This variable denotes an interruption in data packet sequencing that has been identified. Jitter and latency are linked because jitter generates increased or uneven latency between data packets, which can damage network performance and cause packet loss and congestion.

While some jitter is to be expected and can typically be tolerated, quantifying network jitter is an integral part of measuring overall network performance.

# Congestion Control

The reduction in the quality of service that occurs when a network node or a link carries more data than it can handle is called "Network Congestion". The congestion in the network can lead to effects like packet loss or even blocking of new connections.

Therefore, congestion in networks can be defined as, "A state that occurs in network layers because of the heavy message traffic that results in slowing down the network response time is called congestion".

## Effects of Congestion

Following are the effects of Congestion −

- Because of the increase in the response time, the overall performance is reduced.
- Also, in worst situations, because of the delay that takes place, re-transmission can also occur which worsens the scenario.

## Congestion Control techniques

To control the congestion in networks, the control techniques are broadly classified under two categories, which are as follows −

- **The Open loop** refers to the protocols that should be used in order to prevent congestion. That is, the congestion should not occur in the first place. This is based on the technique of having a good design implementation in order to prevent the congestion from taking place.

- **The Close loop** allows the system to enter in the congestion state if it occurs, detects it and then proceeds to remove the congestion. This is based on the feedback mechanism that is received. With the help of the feedback, one can detect and remove the congestion from the network.

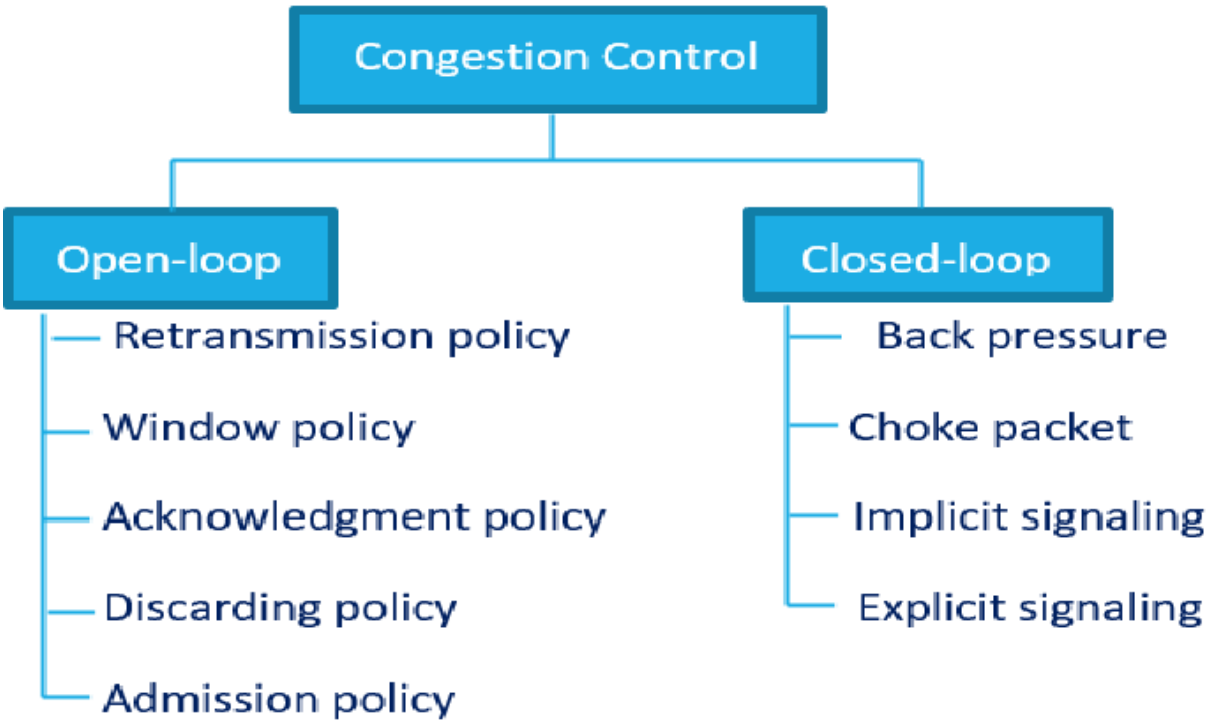



Fig. 2 Classification of congestion control techniques

Now let us discuss about open loop congestion control in detail −

## Open Loop Congestion Control

In this control policies are applied to prevent congestion before it happens. It is handled either by the source or the destination.

- **Retransmission Policy** − This type of policy is sometimes unavoidable. If the sender feels that a packet is lost or corrupted, then it thinks to retransmit. So, a retransmission policy can prevent congestion.

- **Window Policy** − In this type of window the sender may also affect congestion. The selective repeat window is better than the Go-Back-N window for congestion control. In the Go-Back-N window, when the timer for a packet times out, a number of packets may be resent, although some may have arrived safe and sound at the receiver.

- **Acknowledgement Policy** − This policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires. A receiver may decide to acknowledge only N packets at a time.

- **Discarding Policy** − A discarding policy by the routers prevents congestion and at the same time may not harm the integrity of the transmission.
- **Admission Policy** − An admission policy is a quality-of-service mechanism, which prevents congestion in virtual circuit networks.

# Closed Loop Congestion Control

The basic mechanisms of closed loop congestion control are as follows −

## Backpressure

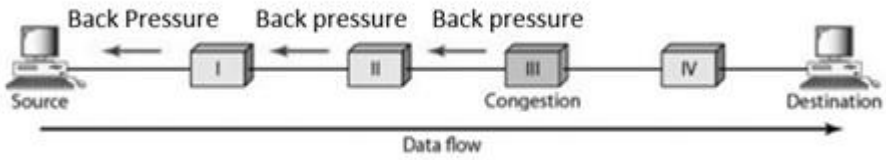
When a router is congested, it informs the previous upstream router to reduce the rate of outgoing packets.

If a node becomes congested it can slow down or halt flow of packets from other nodes and halt flow of packets from other nodes.

It means that other nodes have to apply control on incoming packet rates control on incoming packet rates.

Propagates back to source and it is not used in ATM or frame relay.

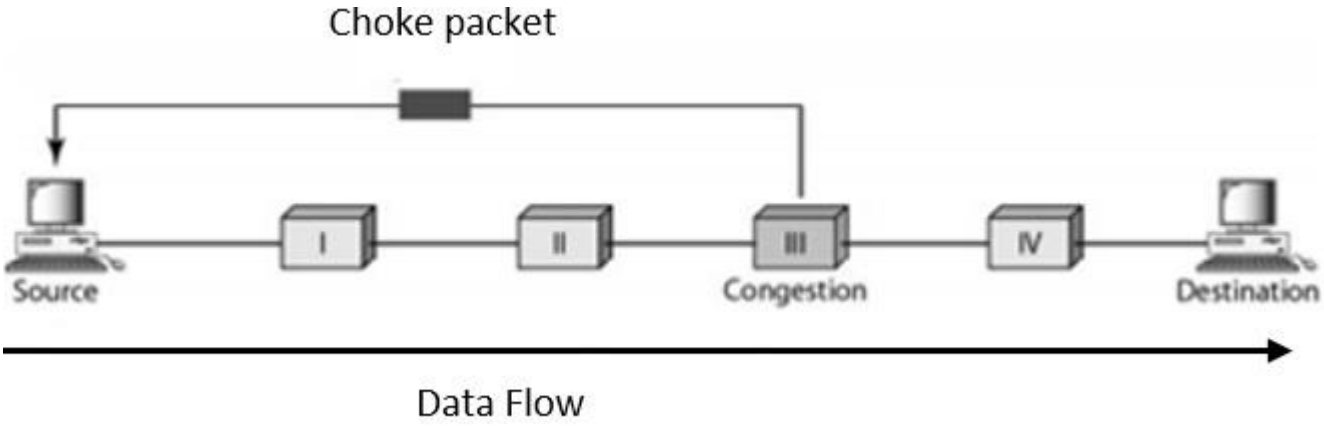
It is diagrammatically represented as follows −




# Choke packet of choke point

It is sent by router to source, similar to ICMP's source quench packet.

It is diagrammatically represented as follows −




# Implicit signaling

It looks for delay in some other action.

Transmission delay may increase with Transmission delay may increase with congestion.

Packets may be discarded and the source can detect these as implicit indications of congestion.

Useful on connectionless (datagram) networks and it is used in frame relay LAPF.

## Explicit signaling

The router sends an explicit signal. The network alerts end systems of increasing congestion and is used on connection-oriented networks. The end systems take steps to reduce offered load.

Backwards − Congestion avoidance info sent in opposite direction of packet travel.

Forwards − Congestion avoidance info sent in the same direction as packet travel.

# IPV4 ADDRESSES: Classful Addressing, Classless Addressing

## 1) Classful Addressing

IPv4 addressing used the concept of classes. This architecture is known as **classful addressing**.

In the classful addressing, there are 5 classes in which the address space is divided: **A, B, C, D, and E**.

Each class occupies some fraction of the address space.

We can find the class of an address when given the address in binary notation or dotted-decimal notation by checking the first few bits or first byte.

## Classes and Blocks

There is a problem with the classful addressing that is "each class is divided into a fixed number of blocks with each block having a fixed size".

| Class name | Number of blocks | Block size | Application |
|---|---|---|---|
| A | 128 | 16,777,216 | Unicast |
| B | 16,384 | 65,536 | Unicast |

| | | | |
|---|---|---|---|
| C | 2,097,152 | 256 | Unicast |
| D | 1 | 268,435,456 | Multicast |
| E | 1 | 268,435.456 | Multicast |

The **"class A addresses"** are designed for large organizations to manage a large number of attached hosts or routers.

The **"class B addresses"** are designed for midsize organizations to manage tens of thousands of attached hosts or routers.

The **"class C addresses"** are designed for small organizations to manage a small number of attached hosts or routers.

## 2) Classless Addressing

**Classful addressing** leads to address depletion. That's the big issue for this schema and that's why it's not used nowadays.

To overcome the problem of address depletion and to give more organizations access to the Internet, the classless addressing was designed and implemented. In this scheme of classless addressing, there are no classes, but the addresses are still granted in blocks.

## Address Blocks

In classless addressing, when an entity(organization or a single household (small organization) or whatever which uses the internet) needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature, size, and need of the entity.

For example, a household (small organization) may be given only two addresses; a large organization may be given thousands of addresses. On the other hand. An ISP, as the Internet service provider, may be given hundreds of thousands based on the number of customers it may serve.

Three restrictions on classless address blocks:

1. The addresses in a block must be contiguous that means one after another.
2. The number of classless addresses in a block must be a power of 2.
3. The first address must be evenly divisible by the number of addresses.

# Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. In DHCP, port number 67 is used for the server and 68 is used for the client.

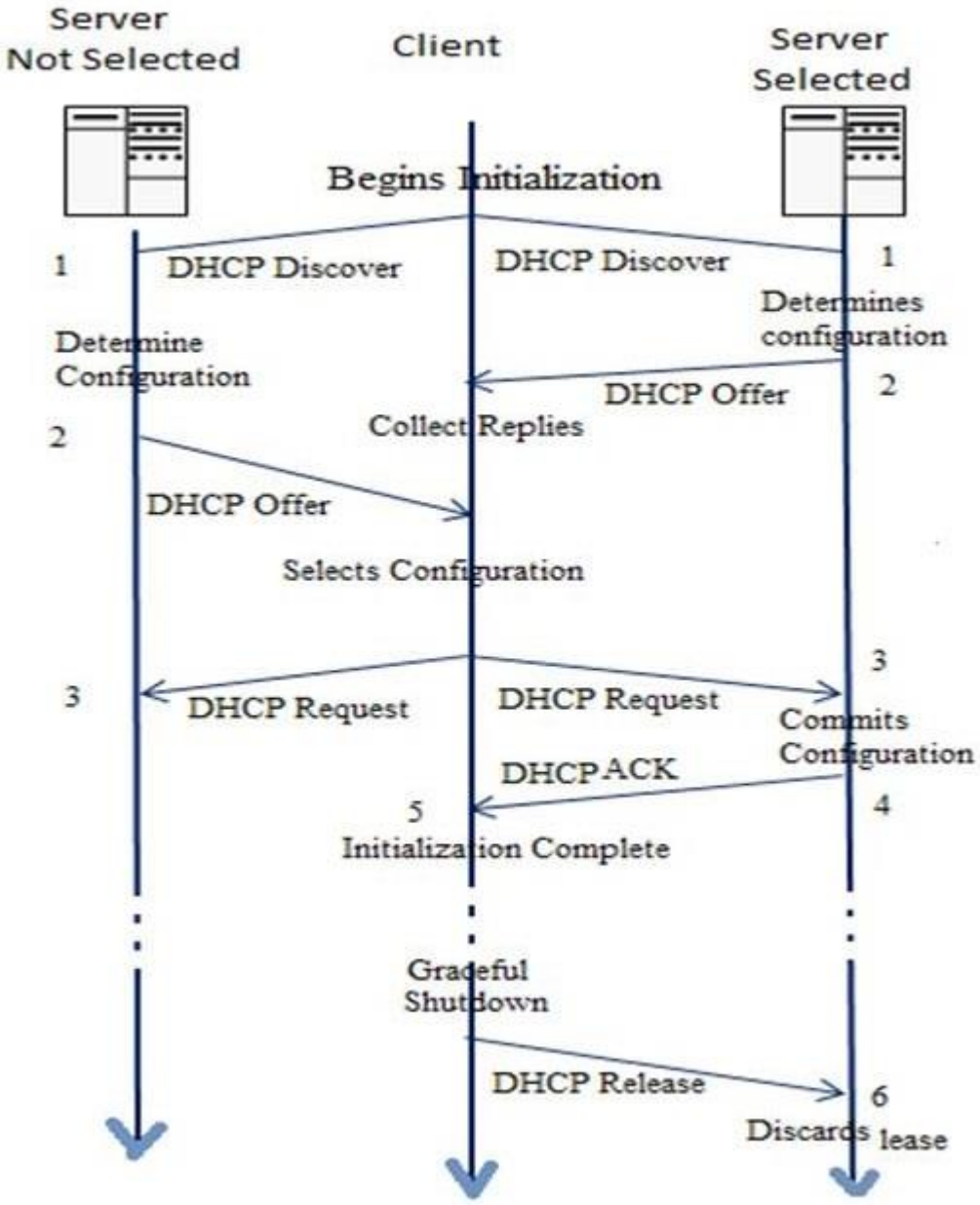
DHCP allows a network administrator to supervise and distribute IP addresses from a central point and automatically sends a new Internet Protocol (IP) address when a computer is plugged into a different place in the network.

DHCP is an application layer protocol that provides −

- Subnet Mask
- Router Address
- IP Address

## DHCP Client-Server Communication Diagram

In DHCP, the client and the server exchange DHCP messages to establish a connection.




## DHCP Discover Message − Client Requests DHCP Information

- It is the first message produced by a client in the communication process between the client and server with the target address 255.255.255.255 and the source address 0.0.0.0.
- This message is produced by the client host to discover if there are any DHCP servers present in a network or not.

- The message might contain other requests like subnet mask, domain name server, and domain name, etc.
- The message is broadcast to all the devices in a network to find the DHCP server.

## DHCP Offer Message − DHCP Server Offers Information to Client

- The DHCP server will reply/respond to the host in this message, specifying the unleashed IP address and other TCP configuration information.
- This message is broadcasted by the server.
- If there are more than one DHCP servers present in the network, then the client host accepts the first DHCP OFFER message it receives.
- Also, a server ID is specified in the packet to identify the server.

## DHCP Request Message − Client Accepts DHCP Server Offer

- The Client receives the DHCP offer message from the DHCP server that replied/responded to the DHCP discover message.
- After receiving the offer message, the client will compare the offer that is requested, and then select the server it wants to use.
- The client sends the DHCP Request message to accept the offer, showing which server is selected.
- Then this message is broadcast to the entire network to let all the DHCP servers know which server was selected.

## DHCP Acknowledgment Message − DHCP server acknowledges the client and leases the IP address.

- If a server receives a DHCP Request message, the server marks the address as leased.
- Servers that are not selected will return the offered addresses to their available pool.
- Now, the selected server sends the client an acknowledgment (DHCP ASK), which contains additional configuration information.

- The client may use the IP address and configuration parameters. It will use these settings till its lease expires or till the client sends a DHCP Release message to the server to end the lease.

## DHCP Request, DHCP ACK Message − Client attempts to renew the lease

- The client starts to renew a lease when half of the lease time has passed.
- The client requests the renewal by sending a DHCP Request message to the server.
- If the server accepts the request, it will send a DHC ACK message back to the client.
- If the server does not respond to the request, the client might continue to use the IP address and configuration information until the lease expires.
- As long as the lease is still active, the client and server do not need to go through the DHCP Discover and DHCP Request process.
- When the lease has expired, the client must start over with the DHCP Discover process.

## The client ends the lease − DHCPRELEASE

- The client ends the lease by sending a DHCP Release message to the DHCP server.
- The server will then return the client's IP address to the available address pool and cancel any remaining lease time.

# What is NAT in computer networks?

NAT stands for network address translation. It's a way to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.

## Key Points

We generally have two types of IP address, which are as follows −

- Private IP address
- Public IP address

Private IP address normally used in the LAN (Local area network) side of the Network.

Public IP address provided by the ISP is configured in the WAN side of the network.

Public IP addresses are always paid, while the private IP address is free.

Private IP addresses range as follows −

- 192.168.0.0 - 192.168.255.255 (65,536 IP addresses)
- 172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses)
- 10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses)

Now let us try to understand what Network Address Translation (NAT) is.

**Step 1** − Consider you have internet provided by Internet Service Provider ABC.

**Step 2** − So, they will give you connection to your Modem. That connection we used to call WAN.

**Step 3** − This connection is always configured with a Public IP address.

**Step 4** − Then, your LAN side of the MODEM is configured with a Private IP address.

**Step 5** − That means your computer or laptop connected to the network receives a Private IP address.

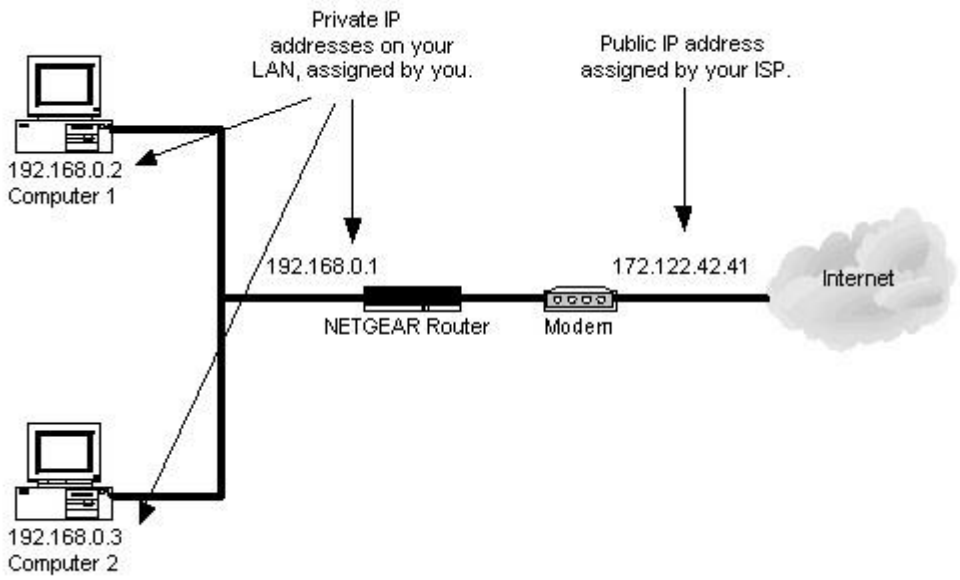
**Step 6** − As per the standard Private IP will not communicate with Public IP address at any Point of time.

**Step 7** − To achieve this, Private IP addresses need to be translated to Public IP addresses with help of NAT.

**Step 8** − In simple words, Network Address translation is used to translate Private IP address to Public IP address to communicate LAN side of the Device

to Global Network. Network address translation can be processed in Router or Firewall.

Given below is the diagram of the NAT −




## Working of NAT

Usually we used gateway router / Border devices used for NAT configuration. One of the interfaces for that device is connected to the local Area network (INSIDE) and one of the interfaces for this device connected to the outside network (OUTSIDE).

When we have received a request from our local machine it will hit the configuration pool then that Private IP will convert it into Public IP address and vice versa.

**Inside worldwide location** − IP address that speaks to at least one inside nearby IP delivers to the rest of the world. This is within have as observed from the external organization.

**Outside residential area** − This is the genuine IP address of the objective host in the nearby organization after interpretation.

**Outside worldwide location** − This is the external host as observed to structure the external organization. It is the IP address of the external objective host before interpretation.

## Examples of NAT

Given below are some of the examples of NAT −

- Usage included with Windows work area working frameworks.

- Local bundle channel.
- Linux filter.
- Window third party implementation.

# IPV6

## What is an IPv6 Address?

**IPv6 Address** is the new generation **IP address** that is mainly developed to overcome **IPv4** exhaust and its limitations. As you know, **IPv4 Addresses** were limited and exhaused shortly. For the new technologies, more IP addresess needed and for this need a new IP version has developed. This new Internet Protocol version is **IPv6 (Internet Protocol version 6)**. We can say that, IPv6 is the new Internet Protocol version that we will use alone or beside IPv4 on our network devices anymore.

**IPv4** is widespread implementation of IP protocol. It has **32 bit** adress space, so it allow to use almost $\mathbf{2^{32}=4,294,967,296}$ addresses in internet. Because of the fact that these addresses has run out, a new version of IP has revealed. With this new IP version, more addresses are available. The number of these new version of ip addresses are especially mentioned as almost unlimited.

Before **IPv4** addresses run out, some techniques like **CIDR, NAT, Priviate Addresses** are used to alleviate this shortage. But with the development of information technology, more devices has joined to the internet and they are still joining.

The new and the next generation version of IP, IPv6 has **128 bit** address space. So, almost $\mathbf{2^{128}}$ available addresses can be created with this new IP version. This is almost **340 undecilion** available addresses, **nearly unlimited!**

With the development of this new internet protocol, some new features has also created. These are the new features that **IPv6 Brings**. These new benefits that comes with IPv6 are given below:

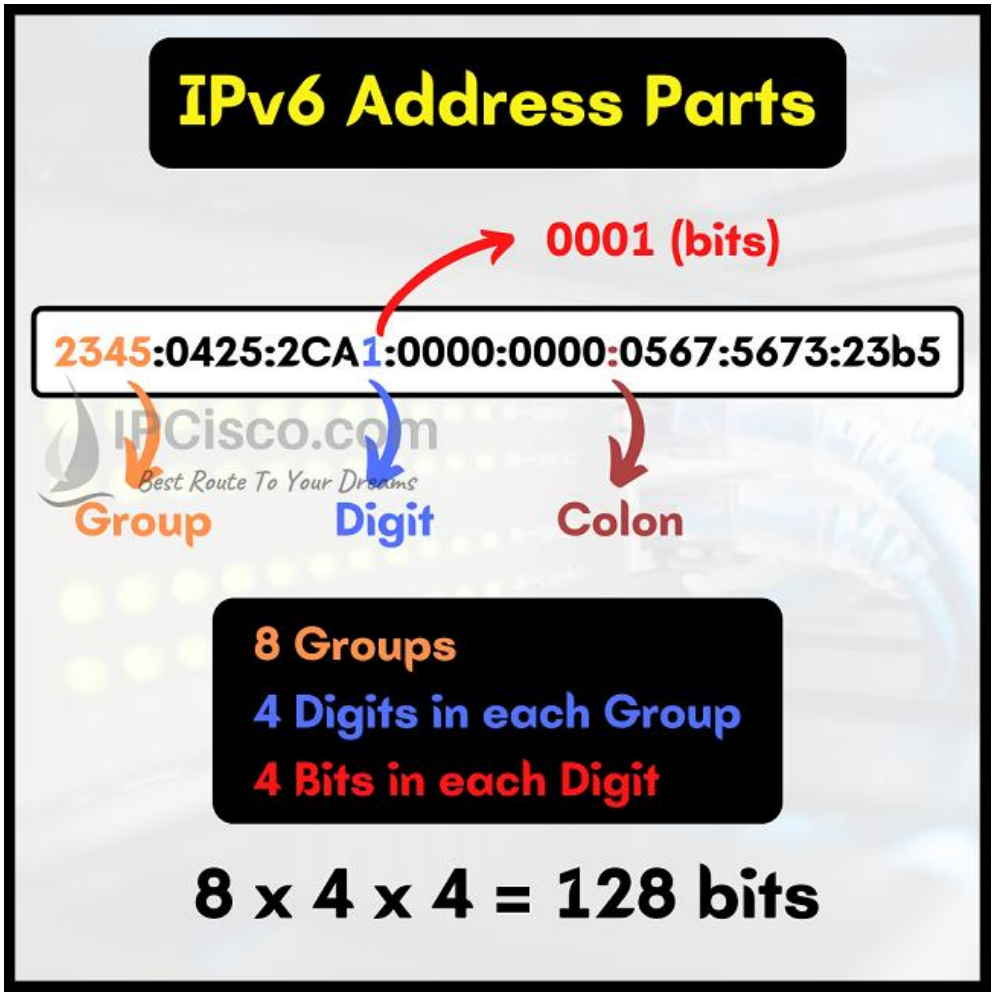
- **Increased address space**

- **Simplified configuration (with auto configuration)**
- **Integrated security (IPSec)**
- **Backward compatibility with IPv4**

# IPv6 Address Example

As you remember, IPv4 addresses are written with **Decimal** numbers. Different than IPv4, **IPv6 addresses** are written with **hexadecimal** digits. There are 10 numbers is the decimal numbering system. Beside, in Hexadecimal numbering system, there are **10 numbers** and **6 letters (A, B, C, D, E, F)**. We can use both numbers and these letters (A, B, C, D, E, F) to create an IPv6 address.

IPv6 address consists of **8 groups** (separated with colons) and in each colons, there are **4 digits**. Each digit can be creatd with **4 bits**. So, with these numbers, the address become **8 x 4 x 4 bit = 128 bits**.



To understand the structure of an IPv6 address, let's give an example:

**2345:0425:2CA1:0000:0000:0567:5673:23b5**

As you can see above, our IPv6 address has **8 groups** and each group is seperated by colons. In each group, there are **4 digits**. Each of these digits can be created with **4 bits.** Total there are **128 bits** address.

IPv6 addresses are very logn addresses, so sometimes we need to shorten these addresses. To do this we use specific abbreviatioins in IPv6 World. In other words, there are some **abbreviations** that are used with IPv6 address. These abbreviations are mentioned below with related IPv6 examples

# Leading Zeros Can Be Dropped

During IPv6 address creation, there can be leading zeros at each groups.  There is no need to write the leaing zeros in an address. Leading zeros can be dropped to shorten the address. In the below examole, we drop the leading zeros. Here,the importan point is this: Only the leading zeros an be droped. we can not drop any zero at the middle or at the end of a group.

2345:0425:2CA1:0000:0000:0567:5673:23b5 ==>
2345:**425**:2CA1:0000:0000:**567**:5673:23b5

As you can see above, instead of writing 0425, we wrote 425. Again, instead of writing 0567, we wrote 567. The zeros at the beginning of each group has dropped.

# Using Zero for Entire Zero Group

In an IPv6, a group can consist of all zeros. In such a case, we do not need to write, all the zeros in the address. Instead of it, we can write one zero that means four zeros in the group.

Below, you can find an example of this IPv6 usage.

2345:0425:2CA1:0000:0000:0567:5673:23b5 ==>
2345:0425:2CA1:**0:0**:0567:5673:23b5

In this address, we have used **0:0**, instead of using **0000:0000**.

# Double Colon For Continuous Zeros

There can be many zeros in many groups of an IPv6 address. To write all these zeros are very difficult for an IP address consist of 128 bits. To overcome this, IPv6 has a "**double colon**" shorten mechanims. We can use double colon **to shorten continuous zeros** in an address. In other words, if we have an entire field of zeros in ana address, we can use only one 0 for each colon. Here, the important point is this: We can use double colon **only once** in an ipv6 address.

2345:0425:2CA1:0000:0000:0567:5673:23b5 ==>
2345:0425:2CA1**::**0567:5673:23b5

Here, instead of writing **0000:00000**, we wrOte **::**

# IPv6 Address Parts

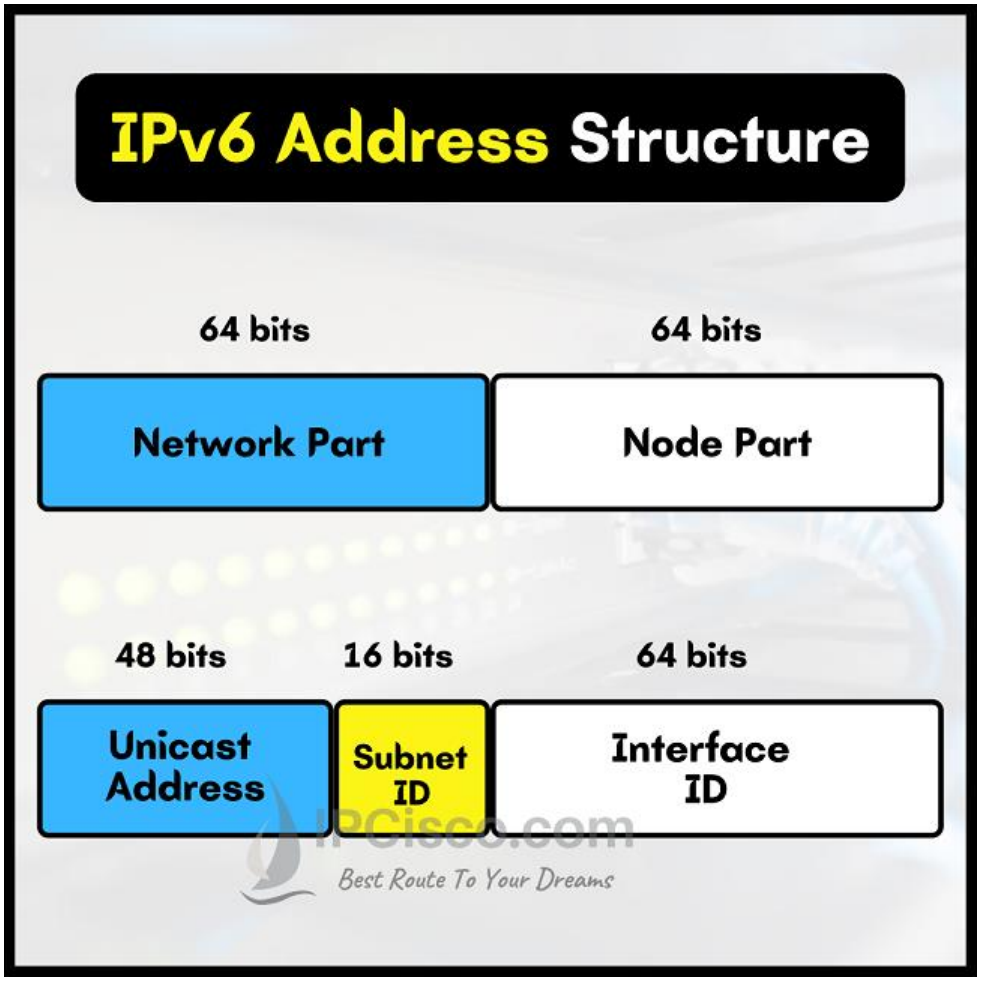
IPv6 addresses are consist of **two** different parts. These parts are given below:

- **Network Part**
- **Node Part**

Network Part is used to identify the network and used for routing. Node part is used to identify the node itself.

Beside this, we also divide network part into **two**. These parts are Unicast Address and Subnet ID. So, we can say that, ipv6 address consist of mainly in **three parts:**

- **Unicast Address**
- **Subnet ID**
- **Interface ID**

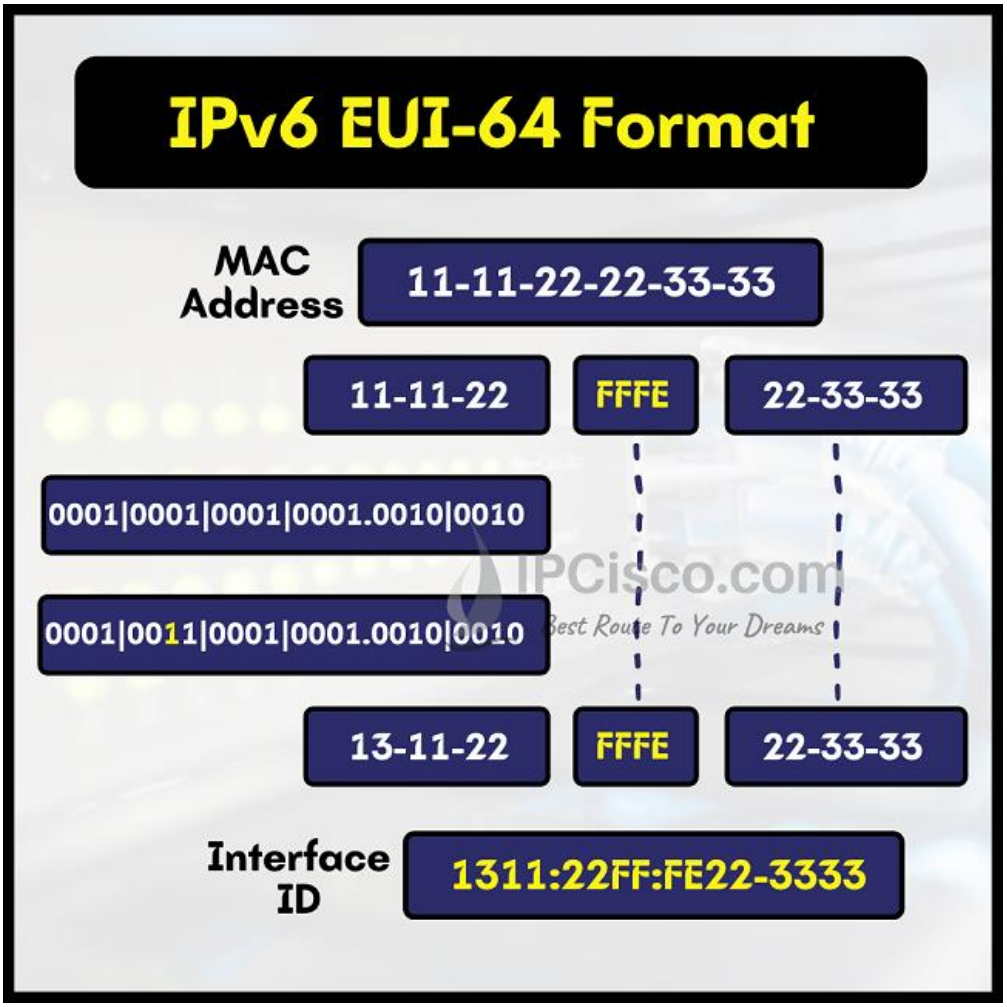



---

## DIFFERENCE BETWEEN IPV4 and IPV6

| Ipv4 | Ipv6 | |
|---|---|---|
| **Address length** | IPv4 is a 32-bit address. | IPv6 is a 128-bit address. |
| **Fields** | IPv4 is a numeric address that consists of 4 fields which are separated by dot (.). | IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon. |
| **Classes** | IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E. | IPv6 does not contain classes of IP addresses. |
| **Number of IP address** | IPv4 has a limited number of IP addresses. | IPv6 has a large number of IP addresses. |
| **VLSM** | It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes. | It does not support VLSM. |
| **Address configuration** | It supports manual and DHCP configuration. | It supports manual, DHCP, auto-configuration, and renumbering. |
| **Address space** | It generates 4 billion unique addresses | It generates 340 undecillion unique addresses. |
| **End-to-end connection integrity** | In IPv4, end-to-end connection integrity is unachievable. | In the case of IPv6, end-to-end connection integrity is achievable. |

| | | |
|---|---|---|
| **Security features** | In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind. | In IPv6, IPSEC is developed for security purposes. |
| **Address representation** | In IPv4, the IP address is represented in decimal. | In IPv6, the representation of the IP address in hexadecimal. |
| **Fragmentation** | Fragmentation is done by the senders and the forwarding routers. | Fragmentation is done by the senders only. |
| **Packet flow identification** | It does not provide any mechanism for packet flow identification. | It uses flow label field in the header for the packet flow identification. |
| **Checksum field** | The checksum field is available in IPv4. | The checksum field is not available in IPv6. |
| **Transmission scheme** | IPv4 is broadcasting. | On the other hand, IPv6 is multicasting, which provides efficient network operations. |
| **Encryption and Authentication** | It does not provide encryption and authentication. | It provides encryption and authentication. |
| **Number of octets** | It consists of 4 octets. | It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16. |


IPv6 EUI-64 Format
MAC Address
11-11-22-22-33-33
11-11-22
FFFE
22-33-33
0001|0001|0001|0001.0010|0010
0001|0011|0001|0001.0010|0010
IPCisco.com
Best Route To Your Dreams
13-11-22
FFFE
22-33-33
Interface ID
1311:22FF:FE22-3333