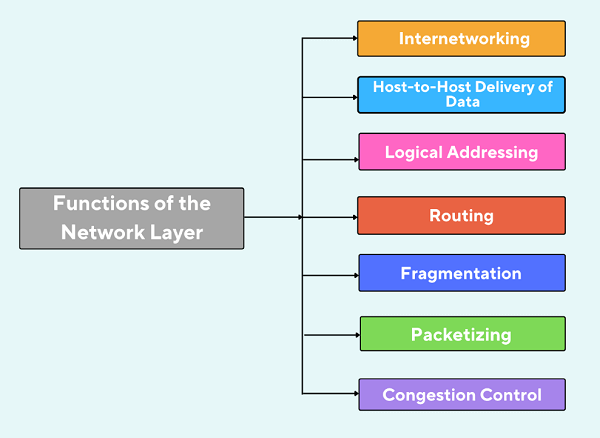
**NETWORK LAYER**

## **Functions(SERVICES) of Network Layer in the OSI Model:**



* **Internetworking:** It is the process of connecting different networks by using intermediate devices such as switches, routers, gateways, and more to forward the data packets.
* **Host-to-Host delivery of data:** It is also known as source-to-destination data delivery or machine-to-machine data delivery. The network layer has the responsibility of transmitting packets of data from one host to another. It makes sure that the data packets reach the correct destination system.
* **Logical Addressing:** The data packets sent by the sender contain both source and destination IP addresses in the header so that the data packets can reach their desired destination without any problem. An IP address is utilized to recognize the device in the network. An IP address is a mixture of two things: Host ID and Network ID. There are many networks, hosts, machines, or servers, so adding an IP address to the header identifies the correct host the data packet should reach.
* **Routing:** It is the process of choosing the best path for securely transmitting data packets from the source host to the destination host. There are many routers between the sender and receiver, and routing is done with the help of these routers. Packets of data are routed from one router to another router and then to another router based on the information available in the header and forwarding table; thus, the data packets reach the destination device. There are various routing algorithms which are protocols that are followed to transmit data packets using the routing process.
* **Fragmentation:** Each node has a size capacity to receive data. The maximum capacity that a node can achieve is called the Maximum Transmission Unit (MTU). Different nodes may have different capacities. If the data size exceeds the Maximum Transmission Unit (MTU), then the data packet is broken into fragments, and the process is called fragmentation. After that, all the fragments are sent to the destination host. Fragmentation is done in the network layer by routers.
* **Packetizing:** It handles the data received from the upper layer and converts it into packets to reach the destination. If the packet is segmented at the source, then the network layer must ensure that each fragment reaches the destination properly and correctly.
* **Congestion Control:** If the load on the network exceeds the capacity of the network leads to congestion which can also be handled in the network layer

**IP Addressing And Its Classification In Computer Networks**

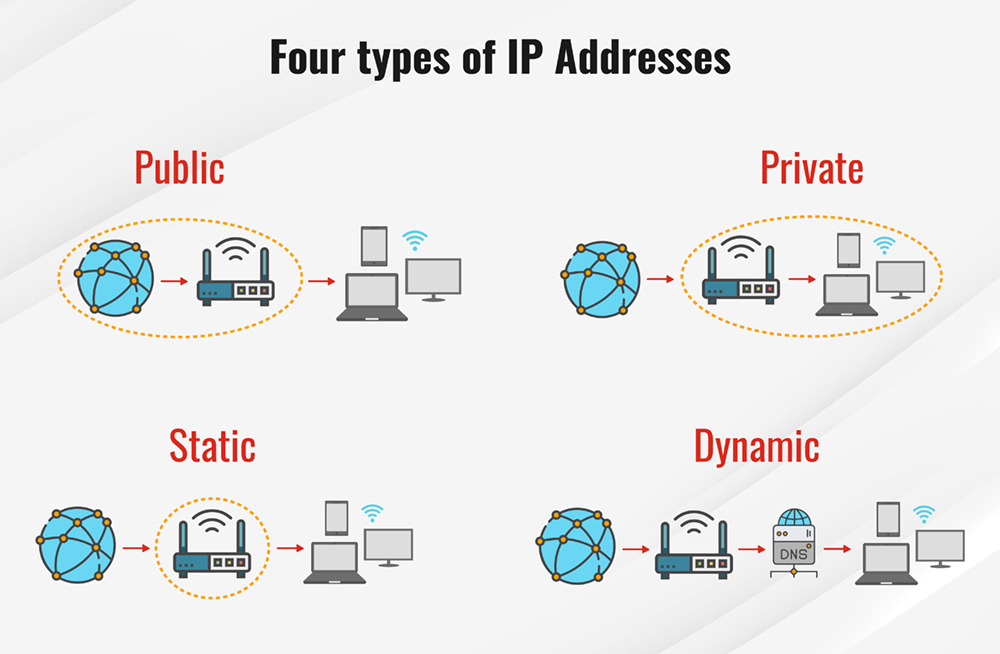
# IP ADDRESS DEFINITION:

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for “Internet Protocol,” which is the set of rules governing the format of data sent via the internet or local network.

IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication.

The internet needs a way to differentiate between different computers, routers, and websites.

IP addresses provide a way of doing so and form an essential part of how the internet works.



### Public IP address

A public IP address, or external-facing IP address, applies to the main device people use to connect their business or home internet network to their internet service provider (ISP). In most cases, this will be the router. All devices that connect to a router communicate with other IP addresses using the router’s IP address.

Knowing an external-facing IP address is crucial for people to open ports used for online gaming, email and web servers, media streaming, and creating remote connections.

### Private IP address

A private IP address, or internal-facing IP address, is assigned by an office or home intranet (or local area network) to devices, or by the internet service provider (ISP). The home/office router manages the private IP addresses to the devices that connect to it from within that local network. Network devices are thus mapped from their private IP addresses to public IP addresses by the router.

Private IP addresses are reused across multiple networks, thus preserving valuable IPv4 address space and extending addressability beyond the simple limit of IPv4 addressing (4,294,967,296 or 2^32).

In the IPv6 addressing scheme, every possible device has its own unique identifier assigned by the ISP or primary network organization, which has a unique prefix. Private addressing is possible in IPv6, and when it's used it's called Unique Local Addressing (ULA).

### Static IP address

All public and private addresses are defined as static or dynamic.

An IP address that a person manually configures and fixes to their device’s network is referred to as a static IP address.

A static IP address cannot be changed automatically.

An internet service provider may assign a static IP address to a user account. The same IP address will be assigned to that user for every session.

### Dynamic IP address

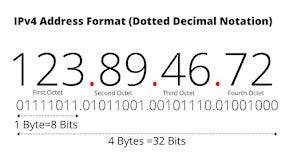
A dynamic IP address is automatically assigned to a network when a router is set up. The [**Dynamic Host Configuration Protocol (DHCP)**](https://www.fortinet.com/resources/cyberglossary/dynamic-host-configuration-protocol-dhcp) assigns the distribution of this dynamic set of IP addresses. The DHCP can be the router that provides IP addresses to networks across a home or an organization.

Each time a user logs into the network, a fresh IP address is assigned from the pool of available (currently unassigned) IP addresses. A user may randomly cycle through several IP addresses across multiple sessions.

# What is an IP Address?

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

IP addresses are not random. They are mathematically produced and allocated by the **Internet Assigned Numbers Authority (IANA),** a division of the Internet Corporation for Assigned Names and Numbers (ICANN). Each time anyone registers a domain on the internet, they go through a domain name registrar, who pays a small fee to ICANN to register the domain



# How do IP addresses work:

If you want to understand why a particular device is not connecting in the way you would expect or you want to troubleshoot why your network may not be working.

Internet Protocol works the same way as any other language, by communicating using set guidelines to pass information. All devices find, send, and exchange information with other connected devices using this protocol. By speaking the same language, any computer in any location can talk to one another.

The use of IP addresses typically happens behind the scenes. The process works like this:

1. 1)Your device indirectly connects to the internet by connecting at first to a network connected to the internet, which then grants your device access to the internet.
2. Your IP address is assigned to your device by your ISP.
3. Your internet activity goes through the ISP, and they route it back to you, using your IP address. Since they are giving you access to the internet, it is their role to assign an IP address to your device.
4. Now take a example: traveling — and you take your device with you, your home IP address does not come with you. This is because you will be using another network (Wi-Fi at a hotel, airport, or coffee shop, etc.) to access the internet and will be using a different (and temporary) IP address, assigned to you by the ISP of the hotel, airport or coffee shop.

* Two types of IP address are:

1)**IPv4:**

1. **IP** stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.  
   IP version four addresses are 32-bit integers which will be expressed in decimal notation.  
   Example- 192.0.2.126 could be an IPv4 address.

* Parts of IPv4

**Network part:**  
The network part indicates the distinctive variety that’s appointed to the network. The network part conjointly identifies the category of the network that’s assigned.

**Host Part:**  
The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.  
For each host on the network, the network part is the same, however, the host half must vary.

**Subnet number:**  
This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

2) **IPv6:**

IP 6 or internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. IPv6 was designed by Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding the IPv4 due to the global exponentially growing internet users.

1. Example- 25.59.209.224 could be an IPv6 address.

* parts of IPv6 Address

1. Now that we know about what is IPv6 address let’s take a look at its different types.

* **Unicast addresses** It identifies a unique node on a network and usually refers to a single sender or a single receiver.
* **Multicast addresses** It represents a group of IP devices and can only be used as the destination of a datagram.
* **Anycast addresses** It is assigned to a set of interfaces that typically belong to different nodes.

**Two types of classification are:**

1) CLASSFUL ADDRESS

2) CLASSLESS ADDRESS

# Classful Address:

The first addressing system to be implemented as part of the Internet Protocol was Classful Addressing. In the year 1981, the Classful addressing network architecture was first used on the Internet. The Classful addressing system was superseded by a Classless addressing scheme with the introduction of Classless Inter-Domain Routing (CIDR) in 1993.

* The IP address comprises up of 32 bits and is split into four sections separated by dots: **part 1, part 2, part 3, and part 4**.
* The IP address is made up of four parts, each of which is eight bits long (1 byte).
* Further, the 4 parts of the IP address is divided into parts: a **network ID** and a **Host ID**.
* Types of classful address:

**Class A, Class B, Class C, Class D, and Class E** are the five varieties of Classful addresses. In IPv4, this classification is known as Classful addressing or IP address classes.

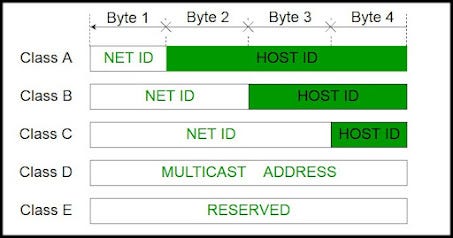
The 32 bit IP address is divided into five sub-classes. These are:

* 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



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

## **class A:**

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:

2⁷-2= 126 network ID(Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address. )

2²⁴ — 2 = 16,777,214 host ID.

## **Class B:**

* 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:
* 2¹⁴ = 16384 network address
* 2¹⁶ — 2 = 65534 host address

## **Class C:**

* 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:
* 2²¹ = 2097152 network address
* 2⁸ — 2 = 254 host address
* IP addresses belonging to class C ranges from 192.0.0.x — 223.255.255.x.

## **Class D & Class E:**

* 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.
* 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.

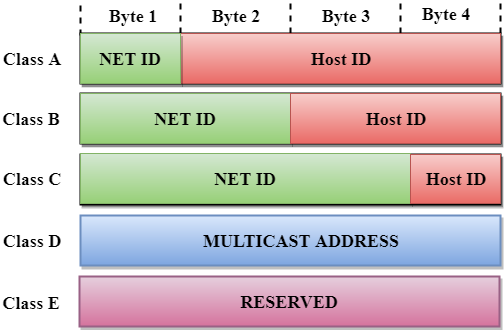
## **Classful Addressing**

An IP address is 32-bit long. An IP address is divided into sub-classes:

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

**An ip address is divided into two parts:**

* **Network ID:** It represents the number of networks.
* **Host ID:** It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

## **Class A**

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

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

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 27 = 128 network address

The total number of hosts in Class A = 224 - 2 = 16,777,214 host address



## **Class B**

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

* The Network ID is 16 bits long.
* The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 214 = 16384 network address

The total number of hosts in Class B = 216 - 2 = 65534 host address



## **Class C**

In Class C, an IP address is assigned to only small-sized networks.

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

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = 221 = 2097152 network address

The total number of hosts = 28 - 2 = 254 host address



## **Class D**

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



## **Class E**

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.

# Network Addressing

## **Rules for assigning Host ID:**

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

* The Host ID must be unique within any network.
* The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.
* The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

## **Rules for assigning Network ID:**

If the hosts are located within the same local network, then they are assigned with the same network ID.

The following are the rules for assigning Network ID:

* The network ID cannot start with 127 as 127 is used by Class A.
* The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.
* The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

## **Problems with Classful Addressing:**

The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993. We will be discussing Classless addressing in next post.

# Classless Addressing:

Classless Inter-Domain Routing (CIDR) is another name for classless addressing. This addressing type aids in the more efficient allocation of IP addresses. This technique assigns a block of IP addresses based on specified conditions when the user demands a specific amount of IP addresses. This block is known as a “CIDR block”, and it contains the necessary number of IP addresses.

When allocating a block, classless addressing is concerned with the following three rules.

**Rule 1** − The CIDR block’s IP addresses must all be contiguous.

**Rule 2** − The block size must be a power of two to be attractive. Furthermore, the block’s size is equal to the number of IP addresses in the block.

**Rule 3** − The block’s first IP address must be divisible by the block size.

**For example,** assume the classless address is 192.168.1.35/27.

* The network component has a bit count of 27, whereas the host portion has a bit count of 5. (32–27)
* The binary representation of the address is: (00100011 . 11000000 . 10101000 . 00000001).
* (11000000.10101000.00000001.00100000) is the first IP address (assigns 0 to all host bits), that is, 192.168.1.32
* (11000000.10101000.00000001.00111111) is the most recent IP address (assigns 1 to all host bits), that is, 192.168.1.63
* The IP address range is 192.168.1.32 to 192.168.1.63.

# Difference Between Classful and Classless Addressing:

1. Classful addressing is a technique of allocating IP addresses that divides them into five categories. Classless addressing is a technique of allocating IP addresses that is intended to replace classful addressing in order to reduce IP address depletion.
2. The utility of classful and classless addressing is another distinction. Addressing without a class is more practical and helpful than addressing with a class.
3. The network ID and host ID change based on the classes in classful addressing. In classless addressing, however, there is no distinction between network ID and host ID. As a result, another distinction between classful and classless addressing may be made.