

IP Address

An IP (Internet Protocol) address is a unique address that different computers on a computer network use to identify and communicate with one another. An IP address is used as an identifier to find electronic devices connected to one another on a network. Therefore, each device in the network must have its own unique address. An IP address is like a mailing address that is used to deliver data (files) to a computer.

Some IP addresses are meant to be unique within the scope of the Internet, whereas others are meant to be unique within the scope of a specific network. The Internet Assigned Numbers Authority (IANA) creates and manages IP addresses for the public Internet. IANA allocates the superblocks of addresses to Regional Internet Registries, which in turn allocate smaller blocks of addresses to Internet service providers.

An IP address is 32 (thirty two) bits long, which can be divided into a network portion and a host portion with the help of a subnet mask. It is represented in the form of four octets, where 1 octet = 8 bits. Each octet is converted to a decimal format and is separated by a dot (.). For this reason, an IP address is said to be expressed in a 'dotted decimal format.'

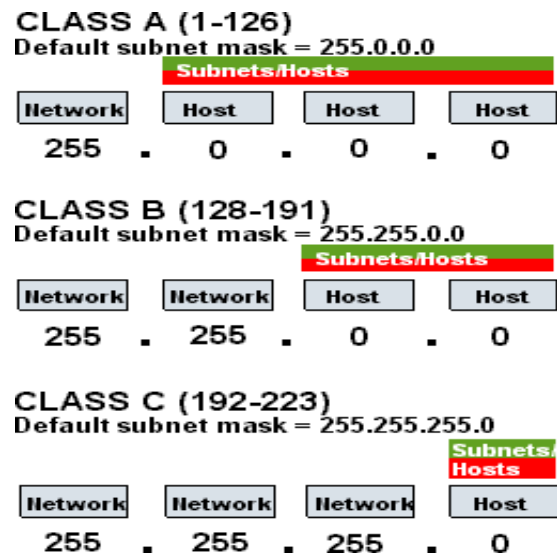
Examples of IP addresses in decimal format: 10.1.1.1, 255.255.255.255, 220.3.1.5

The value in each octet ranges from 0 to 255 in decimal format. The 'dotted decimal format' makes it easier for humans to read and remember the numbers, but computers use IP addresses in a binary format only.

Example of an IP address in binary format: 10011101.11100010.10101110.11101000

Binary Octet to Decimal Format Conversion

There exists a well defined method for converting binary IP addresses into its equivalent decimal format and vice versa. Humans prefer to operate on the dotted



decimal format, whereas behind the curtain, computers deal with IP addresses in the binary form.

The right most bit or the least significant bit of an octet holds a value of 1. The bit just to the left of it has a value of 2. This series continues until the left most 8th bit gets a value of 128. Hence, if all the binary bits of an octet are 1, then the decimal equivalent would be 255.

1	1	1	1	1	1	1	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

11111111 (binary octet) = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 128 = 255 (decimal format)

Below is an example where all octet bits are not 1.

0	1	0	0	0	0	0	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

01000001 (binary octet) = 1+0+0+0+0+0+64+0 = 65 (decimal format)

Types of IP Addresses

- **Unicast IP Address** : It is used to transmit information to a specific network device on the network.
- **Broadcast IP Address** : It allows information to be sent to all the computers on a given subnet rather than a particular machine. The exact notation can differ by the operating system, but the standard is laid out in RFC 919. Each and every machine on the subnet receives the [IP packets](#) directed to the broadcast address. It is generally used for mass communication such as a radio transmission to multiple listeners.

The broadcast address is calculated by taking the bit complement of the subnet mask and then applying OR operating bitwise with the IP address. Example: To broadcast a packet to an entire class B subnet with a [private IP](#) address space, the broadcast address would be 172.16.255.255. This can be done with the help of the subnet mask; 255.255.0.0, and the IP address; for e.g. 172.16.48.196. The complement of the subnet mask is 0.0.255.255 and 172.16.48.196 ||

0.0.255.255 = 172.16.255.255.255.255.255.255 is a limited broadcast IP address, which does not reach every node on the Internet only nodes on LAN.

- **Multicast IP Address** : Multi-cast IP addresses are reserved and used only for specific groups of machines residing in a large domain. For example, an IP packet destined for a multi-cast address will be sent only to machines that are part of that Multi-cast Group. The address range of class D IP addresses from 224.0.0.0 to 239.255.255.255, or equivalent 224.0.0.0/4, is particularly reserved for Multicasting.

Examples are RIP, which uses 224.0.0.9 and OSPF, which uses 224.0.0.5 address.

- **Private IP Address** : These are local addresses that cannot be routed over the Internet. Two organizations can use the same private IP address. These addresses are free for everyone.
- **Public IP Address** : It is a unique IP address that IANA (Internet Assigned Network Authority) assigns. Duplication of the public IP addresses is impossible. Hence, these addresses need to be bought.

Understanding Private IP Addresses and Public IP Addresses

Public IP addresses are IP addresses that are connected to the public Internet. To ensure that these IP addresses are unique, the Internet Assigned Numbers Authority (IANA) divides up the non-reserved portion of the IP address space. It then delegates responsibility for public IP address allocation to registries such as the American Registry for Internet Numbers (ARIN) and Asia-Pacific Network Information Center (APNIC). The registries are responsible for allocating blocks of addresses to large Internet Providers (ISPs). ISPs allocate smaller blocks of addresses to small Internet Service Providers (ISPs) and customers. What normally occurs is that the ISP allocates one public IP address to each computer which is connected to the particular ISP. The particular public IP addresses can be assigned dynamically to each computer when it connects to the ISP, or the IP address can be reserved statically for a dedicated line or a particular dial-up account.

Only those addresses that the IANA has registered are visible on the Internet. IANA functions as the registrar of public IP addresses in order to prevent the duplication of

these addresses. The addresses obtained from IANA are simply network identifiers. Administrators then have to assign unique host identifiers (IDs) to each computer and network device. To calculate the IP addresses for computers, you have to combine the network ID assigned by IANA with a unique host ID.

While you can assign public IP addresses to each network device, you should consider the following disadvantages of implementing this strategy:

- You would deplete the pool of available IP addresses if you assign public IP address to each of your network devices.
- The private network is vulnerable when public IP addresses are used on the [private network](#). Systems that have a public IP address on the Internet would be able to access your [private network](#). Your devices would also be able to access systems on the Internet.

Private IP addresses are IP addresses that are used on the private network. These addresses are not visible on the public Internet. Private addresses are typically used on [TCP/IP](#) networks for servers and workstations accessed by your internal network users. The Internet Assigned Numbers Authority (IANA) has specifically reserved IP addresses which are used for computers on the private network that need to access the Internet. A number of methods can be used to assign private addresses to computers so that they can access the Internet, but are not visible on the Internet.

In RFC 1918 / Address Allocation for Private Internets; IANA has reserved the following three private IP address ranges for private network utilization.

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- [192.168.0.0](#) to [192.168.255.255](#)

Hosts that have a private IP address can use one of the following methods to access the Internet:

- Set up a [Network Address Translation](#) (NAT) server.
- A proxy server

IP Address Assignment Methods

An IP address can be static or dynamic. If the computer uses the same IP address whenever it connects to the network, it is said to have a static IP address. If the IP address changes frequently whenever the computer connects to the network, it is said to have a dynamic IP address. The network administrator manually assigns static IP addresses, whereas the Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses. An operating system can also assign itself a dynamic address when a DHCP server and the network administrator are unavailable. The operating system uses Zero-conf for this purpose. Dynamic addresses are usually used for LANs and broadband networks, whereas static addresses locate servers within an enterprise.

At present, two versions of Internet Protocol are in use: IPv4 and IPv6. IPv4 uses 32-bit addresses, so its address space is limited to 4,294,967,296 unique addresses, with a large part reserved for special purposes. So, fewer addresses are available for the public Internet. IPv6 was designed as a replacement for IPv4, as the addresses are 128 bits wide. Therefore, IPv6 offers a large address space.

Dynamic IP Address Assignment

You can configure a computer as a DHCP server so that the DHCP server can automatically assign IP addresses to DHCP clients. IP addresses that are assigned via a DHCP server are regarded as dynamically assigned IP addresses. The DHCP server assigns IP addresses from a predetermined IP address range(s). You can set up the DHCP server to assign clients automatically with a number of options, such as:

- Addresses of [DNS](#) servers and WINS servers
- Gateway addresses
- TCP/IP configuration parameters.

Static IP Address Assignment

Manually assigning IP addresses occurs under the following conditions:

- When there are no configured DHCP servers on the network and the network has multiple network segments.

- When you are configuring a computer as a DHCP server, you assign that computer a static IP addresses.
- When you configure computers as important network servers such as domain controllers, or DNS servers; you manually assign the IP address to these computers.

Manually assigning IP addresses can be time consuming, and can lead to duplicated IP address assignments. You should only choose to utilize the manual [IP addressing](#) method when you cannot use DHCP to automatically assign IP addresses.

Automatic Private [IP Addressing](#) (APIPA)

[APIPA](#) can be used as an alternative when no DHCP server exists to dynamically assign IP address. APIPA works well in smaller networks, when a computer is used on more than one network.

Understanding the Hierarchical IP Addressing Structure

As mentioned earlier, IP addresses are 32-bit unique identifiers. The bits of an IP address are divided into octets. The notations used to indicate IP addresses are:

- Dotted-decimal notation
- [Binary](#) notation
- Hexadecimal notation

The 32-bit IP address is a hierarchical structured address. IP addresses are not flat addresses. IP addresses are considered hierarchical addresses because the address space is divided into ordered chunks. The 32 bits are not in its entirety a unique identifier. A segment of the IP address is the network address, and another segment is the host (node) address. This segregation is what makes IP addresses hierarchical structured addresses.

- The network address or network ID uniquely identifies a network. All computers and all other devices on the same network, have the identical network address as a segment of their IP address. When using network addresses or IDs, remember the following important rules:

- Because 127 is reserved for loopback addresses, a network address cannot have 127 as the first octet.
- All bits of the network ID cannot be set to ones (1s). This is used for broadcast addresses.
- All bits of the network ID cannot be set to zeroes (0s). This is used to designate the local host.
- If you have different network segments, each network address has to be unique to the IP address.
- Each TCP/IP host on the network, such as a server, router or workstation has a uniquely assigned host address (Host ID), or node address. The host address has to be unique so that each machine on the network can be uniquely identified. When using host addresses or host IDs, remember the following important rules:
 - You cannot set all the bits in the host address to all 1s, or to all 0s.
 - A host ID has to be unique in the network that it belongs to.

When the Internet was designed, it was decided to create classes of networks. These classes of networks are based on the size of the network.

- *Class A network*: The Class A network was designed for a very small number of networks which have a large number of nodes or hosts.
- *Class B network*: The Class B network was designed for networks between very small and very large.
- *Class C network*: The Class C network was designed for a very large number of networks that have a small number of nodes or hosts.

The characteristics of the network address classes are listed below:

- Class A network:
 - Leading bit pattern: 0
 - Decimal Range of first byte of the network address: 1 – 126
 - Maximum number of networks: 126
 - Maximum nodes per network: 16,777,214
- Class B network:
 - Leading bit pattern: 10
 - Decimal Range of first byte of the network address: 128 -191
 - Maximum number of networks: 16,384
 - Maximum nodes per network: 65,534
- Class C network:

- Leading bit pattern: 110
- Decimal Range of first byte of the network address: 192 -223
- Maximum number of networks: 2,097,152
- Maximum nodes per network: 254

Understanding Reserved IP addresses

A few IP addresses are reserved for specific special purposes. The reserved IP addresses are:

- Network segment of the address specified to zeros/0s: Indicates this network or subnet (local network).
- Network segment of the address specified to ones/1s: Indicates this network and all associated subnets.
- Network address 127: The address is reserved for loopback testing.
- Host address of all zeros/0s: The address is typically used in routing tables, and when referencing a network, but not particular hosts on the network.
- Host address of all ones/1s: This is used as a broadcast address for all the nodes on a particular network.
- Full IP address specified as specified as zeros/0s: The address is used by the RIP protocol to specify the default route.
- Full IP address specified as specified as ones/1s: The address is use to broadcast to all nodes on the current network.

Converting Between the Binary Notation and Decimal Notation

In the dotted-decimal notation, the digits 0 to 9 are used. With the 32-bit IP addresses, the octets and bit places are numbered from the left to the right. Each number in the decimal system can be represented in the binary format. The binary system uses only two digits, which are 0 and 1. A binary digit is called a bit. With IP addressing, an octet is formed by 8 bits. An IP address consists of 32 bits, or four octets.

The initial octet refers to the leftmost octet. The bit places 1 to 8 signify the eight leftmost bit places. The second octet signifies the following eight bits, which is bit places 9 to 16. The third octet signifies the following eight bits, which is bit places 17 to 24. The fourth octet signifies the following eight bits, which is bit places 25 to 32.

- In the dotted-decimal notation, periods are used to divide the four octets.
- In the binary notation, spaces are used to separate the four octets.

If you want to convert a binary number to a decimal number, add the value of each bit position set to 1. If you want to convert a decimal number to a binary number, determine the largest binary bit represented.

Understanding the Different IP Address Classes

The different [IP Address](#) classes are:

- Class A addresses were created for tremendously large networks with many hosts. With Class A addresses, the first high-order bit is zero. The Class A address format is defined below:
 - Network.Node.Node.Node.The Class A addresses has the following characteristics:
 - The first 8 bits or octet is the network address.
 - The second octet, third octet and fourth octet defines the host address or ID.
 - The maximum number of Class A networks that can be created is 128, of which only 126 is considered possible usable network addresses. This is due to 127 being defined for loopback testing. In addition to this, all bits of the network ID cannot be set to ones (1s) nor can all bits of the network ID be set to zeroes (0s).
 - There is also a multitude of usable unique host addresses for a Class A network. The precise figure of possible host addresses is 16,777,216. Of this figure, two addresses are considered reserved IP addresses.
- Class B addresses were created for networks that are medium of size and which have an average number of hosts. With a Class B address, the initial two high-order bits are set to 10. The Class B address format is defined below:
 - Network.Network.Node.Node.The Class B addresses have the following characteristics:
 - The first 2 octets define the network address

- A Class B network has more network IDs than a Class A network
- A Class B network has fewer host IDs than a Class A network
- The third octet and fourth octet defines the host address or ID.
- The maximum number of Class B networks that can be created is 16,384.
- Each Class B network can have 65,534 possible host addresses or IDs
- Class C addresses were created for networks that are small and that have few hosts. With a Class C address, the initial three high-order bits are set to 110. The Class C address format is defined below:
 - Network.Network.Network.Node.The Class C addresses have the following characteristics:
 - The first 3 octets define the network address.
 - The fourth octet defines the host address or ID.
 - The maximum number of Class C networks that can be created is 2,097,152.
 - Each Class C network can have 254 possible host addresses or IDs
- Class D addresses are reserved for multicasting only. The initial four high-order bits are set to 1110, and the last 28 bits are used for multicast addresses. Multicast Backbone on the Internet (MBONE) uses Class D addresses. MBONE is an extension to the Internet that enables a packet to have more than one destination. The Class D addresses utilize the address range 224.0.0.0 through to 239.255.255.255.
- Class E addresses are reserved for future use. The initial five high-order bits are set to 11110. The Class E addresses use the address range 240.0.0.0 to 255.255.255.255.

Source: <http://www.tech-faq.com/ip-address.html>