

# Classful Addressing

---

## Overview

Classful addressing may be a concept that divides the available address space of IPv4 into five classes, namely A, B, C, D & E. Nowadays, this idea has become obsolete and has been replaced with classless addressing. IP addresses, before 1993, use the classful addressing where classes have a hard and fast number of blocks and every block features a fixed number of hosts. Each of those classes features a valid range of IP addresses. Types D and E are reserved for multicast and experimental purposes, respectively. The order of bits within the first octet determine the classes of IP address.

## The IP Address

IP (Internet Protocol) Address is an address of your network hardware. It helps in connecting your computer to other devices on your Network and everyone over the planet. An IPv4 address may be a 32-bit address. However, instead of writing out each bit value, the address is usually written in dotted-decimal notation. Consider the IP address of 10.1.2.3. This address is written in dotted-decimal notation. Notice that the IP address is split into four separate numbers, separated by periods. Each number represents one-fourth of the IP address. Specifically, each number represents an 8-bit portion of the 32 bits within the address. Because each of those four divisions of an IP address represents 8 bits, these divisions are called octets.

All devices connected to an online connection have a singular IP address, which suggests billions of IP addresses are required. An IP address has information about how to reach a selected host, especially outside the LAN. An IP address may be a 32-bit unique address having an address space of  $2^{32}$ . Generally, there are two notations during which IP address is written, dotted mathematical notation and hexadecimal notation. Addresses in IPv4 are 32-bits long. This enables for a maximum of 4,294,967,296 ( $2^{32}$ ) unique addresses. Addresses in IPv6 are 128-bits, which allows for  $3.4 \times 10^{38}$  ( $2^{128}$ ) unique addresses.

IPv4 address is split into two parts:

- **Network ID:** A network ID, within the world of Transmission Control Protocol/Internet Protocol or TCP/IP, is the portion of the TCP/IP address that identifies the Network for a given host, usually composed of three octets with dotted-decimal representation. The term "network ID" also can be applied in several ways to local network resources for user authentication. Still, the classic use of the time relates to the TCP/IP address itself, how that's wont to route information. Think of the Network ID because the suburb you reside in and therefore the Node ID your street therein suburb. You'll tell precisely where someone is that if you've got their suburb and street name. In the same way, the Network ID tells us which Network a specific computer belongs to. Therefore the Node ID identifies that computer from all the remainder that reside within the same Network.
- **Host ID:** The Host ID is the portion of an IP address that uniquely identifies a number on a given TCP/IP network. You discover the host ID by logically NANDing the binary sort of the IP address with the binary some the subnet mask for the Network. The opposite part of an IP address is the network ID, which specifies the Network to which the host belongs.

When writing a network address, or an IP address for that matter, Who must provide more detail than simply a dotted-decimal representation of an IP address's 32 bits. For instance, just being told that a tool has an IP address of 10.1.2.3 doesn't tell you the Network on which the IP address resides. To understand the network address, you would like to understand the subnet mask, which might be written in dotted-decimal notation or Lukasiewicz notation (also referred to as slash notation ). Within the Example, where we have an IP address of 10.1.2.3 and an 8-bit subnet mask, the IP address might be written as 10.1.2.3 255.0.0.0 or 10.1.2.3 /8. Similarly, the network address might be written as 10.0.0.0 255.0.0.0 or 10.0.0.0 /8.

## Classes of Addresses

Although an IP address (or a network address) needs subnet mask information to work out which bits represent the network portion of the lesson, there are default subnet masks with which you ought to be familiar. The default subnet mask for a given IP address is solely determined by the worth within the IP address's first octet.

Address Classes	Value in First Octet	Classful Mask	Slash Notation
Class A	1-126	255.0.0.0	/8
Class B	128-191	255.255.0.0	/16
Class C	192-233	255.255.255.0	/24
Class D	224-239	-	-
Class E	240-255	-	-

**Table 1: Classes in IPv4**

## Class A Addresses

Class A addresses are for networks with a sizable amount of total hosts. Class A allows for 126 networks by using the primary octet for the Network ID. the primary bit is usually set and glued to zero during this octet. And next seven bits within the octet are ready to at least one, which then complete network ID. The 24 bits within the remaining octets represent the host's ID, allowing 126 networks and approximately 17 million hosts per Network. Class A network number values begin at one and end at 127. the category A format is as follows:

### **Network.Host.Host.Host**

Class A network addresses are 1 byte long, with the primary little bit of the byte reserved and the seven remaining bits available for manipulation or address. As a result, the theoretical maximum number of sophistication A networks which will be created is 128. Why well, each of the seven-bit positions can either be a zero or one, and a couple of to the facility of seven gives you 128. The designers of the IP address scheme said that the primary little bit of the quick bite during a Class A network address should be off, or 0. this suggests Class A address must be between zero and 127 within the first byte, inclusive.

To complicate matters further, the Network of all zeros addresses is resolved by designating the default route. Additionally, the route address 127, reserved for diagnostics, cannot be used either, which suggests that you can only use the numbers 1 to 126to designate class eight network addresses. this means the particular number of usable classes in network addresses is 128 - 2 or 126.

Address	Function
Network addresses of all 0's.	They are interpreted to mean this Network or segment.
The network address of all 1's.	They are interpreted to mean all networks.
Network 127.0.0.1	Reserved for loopback test designated the localhost and allowed the host to send a test packet without generating network traffic.
Host address of all 0's.	They are interpreted to mean network addresses or any host on the precise Network.
Host address of all 1's.	Interpreted to mean all hosts on the precise Network; for instance, 126.255.255.255 means all hosts on network 126.
Entire IP address set to all 0's.	Employed by Cisco router to designate the default route could also mean any network.
entire IP address set to all 1's.	Broadcast to all or any hosts on the present Network is usually called once broadcast or limited broadcast.

**Table 2: Classes A**

Each class address has three bytes for the host address of the machine this suggests there are  $2^{24}$  unique combinations and thus precisely that a lot of potential special hosting lessons for every class within the Network. Because host addresses with two partners of all zeros and ones are reserved, the particular maximum usable number of hosts for sophistication in-network is  $2^{24} - 2$ , which equals 16,777,214.

## Class B Addresses

In a class B network addresses, the primary two bytes are assigned to the network addresses, and therefore, the remaining 2 bytes are used for host addresses. The format is as follows:

**Network.Network.Host.Host**

With a network address being two bytes, we are left with  $2^{16}$  unique combinations, but the web designers decided that each Class B network address should start with digit one, then 0. This leaves 14-bit positions available to control so. Wicked 16,384 unique class B network addresses. during a Class B network, the RFC state that the primary bit on the primary byte should be turned on, but the second bit always must be turned off if we turn the opposite six bits on all of them on we'll find the range for the category B Network:

$$10000000 = 128$$

$$10111111 = 191$$

As you'll see, a category B network is defined when the preceding byte is configured from 128 to 191.

## Class C Addresses

The first octet of sophisticated C IP addresses has its first 3 bits set to 110. Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for sophisticated C is 255.255.255.x. Class C network addresses were for little organizations and used 3bytes for the Network and 1 byte for node addresses. Class C gives 2097152 ( $2^{21}$ ) Network addresses and 254 ( $2^8-2$ ) Host addresses. Class C IP address format is:

**Network.Network.Network.Host**

In a class C network address, the primary three-bit positions are always the binary the calculation is as follows:

Three bytes, or 24 bits, minus three reserve positions, leave 21 positions. Hence, there are  $2^{21}$ , or 20,97,152 possible C Class networks. The RFC defines the primary 2 bits of the primary update as always turned on for sophisticated C networks, but the third bit will never get on. Here's the range for a category C network:

$$11000000 = 192$$

$$11011111 = 223$$

So if you see an IP address with a variety from 192 up to 223, you recognize it is a class C IP address. Each unique class C network has one byte to use for host addresses. This gets us to  $2^8$  or 256 minus the two reserved patterns for all zeros and ones for a complete of 254 available host addresses for every class C network. When deciding which network address class to use, you want to consider what percentage of local hosts there'll get on the Network and how many subnetworks will be within the organization. Therefore, if the organization is small and the Network will have fewer than 256 hosts, a category C address is perhaps sufficient. If the organization is large, then a category B or Class A address could be more appropriate.

## Class D and E Addresses

Class D addresses are used for multicasting applications. Unlike the previous classes, this is often not used for "normal" networking operations. Class D addresses have their first three bits set to "1" and their fourth bit to "0". Class D addresses are 32-bit network addresses, meaning that each one of the values within the range of 224.0.0.0 – 239.255.255.255 are wont to identify multicast groups uniquely. There are no host addresses within the category D address space since all the hosts within a gaggle share the group's IP address for receiver purposes. Example for a category D IP address: **226.22.5.172**.

Class E networks are defined by having the primary four network address bits as 1. That encompasses addresses from 240.0.0.0 to 255.255.255.255. While this class is reserved, its usage was never defined. As a result, most network implementations discard these addresses as illegal or undefined. The exception is 255.255.255.255, which is employed as a broadcast address. For example, a category E IP address is **244.124.79.31**.

Class	Higher bits	Network address bits	Host address bits	No. of networks	No. of hosts per network	Range
A	0	8	24	$2^7$	$2^{24}$	0.0.0.0 - 255.255.255
B	10	16	16	$2^{14}$	$2^{16}$	128.0.0.0 - 191.255.255
C	100	24	8	$2^{21}$	$2^8$	192.0.0.0 - 223.255.255
D	1110	Reserved	Reserved	Reserved	Reserved	224.0.0.0 - 239.255.255
E	1111	Reserved	Reserved	Reserved	Reserved	240.0.0.0 - 255.255.255

**Table 3: Classes Network Bits/ Host Bits**