

# IP Addresses: Intro to IPv4

Reading

15 - 30 minutes

✓ Status Incomplete

## Introduction

**IPv4** is a connectionless protocol for switched networks. It operates on a best-effort delivery model, in which no delivery is guaranteed, nor is proper sequencing or prevention of duplicate delivery assured. IPv4 is the fourth revision of the IP, and it's a protocol widely used in data communication over networks such as **Ethernet**, providing identification for each device.

## Reading

### *What is an IP Address and how is it structured?*

From Internet routers to complex computer networks and wireless home networks to phones and mobile devices — these are just some of the many devices that require an IP address to connect. Depending on the network type and usability, there are many ways to configure IPv4 with all devices, including manual and automatic configurations.

IPv4 addresses are written in **dot-decimal notation**, with **four octets** of the address expressed individually in decimal and separated by dots. For example, **192.168.0.1**.

Have you ever used or seen the address **192.168.0.1**?

This sequence of numbers represents a type of IPv4 addressing (decimal) used in **local networks**.

Decimal = 192.168.0.1

- Octet 1 - 192
- Octet 2 - 168
- Octet 3 - 0
- Octet 4 - 1

IPv4 addressing is divided into two parts of Network and Host. This division is given by the netmask used together with the address.

Following the example:

IP = 192.168.0.1

Netmask = 255.255.255.0

The sequence of numbers 255.255.255.0 represents the netmask. A netmask shows which part of an IP Address refer to the network and which part identifies the individual hosts. Any octet position with a 255 is part of the network address and octets in the zero position represent the host address. In this case the network is all numbers up to the third octet and the fourth octet will identify any given host.

So in our example, every host on the network would begin with 192.168.0 because they belong to the same network. The fourth octet would be used to identify individual hosts within that network. 192.168.0.1, 192.168.0.2 and so on.

The **netmask** follows the exact representation as the IP address, using decimal and binary notation.

Decimal = 255.255.255.0

? For the IP address 142.88.9.12 and a netmask of 255.255.0.0, which part identifies the network and which part identifies the host?

*Toggle the answer below to see the response.*

Network Address: 142.88

Host Address: 9.12

Toggle Answer

## Communication Classes

At the beginning of IPv4 addressing, separations were made for using these numbers based on a system of classes.

Each class had its mask, number of networks, and hosts.

The classes are separated into A, B, C, D, and E. Classes A, B, and C have different bit lengths for addressing the network host. Class D addresses are reserved for military purposes, while Class E addresses are reserved for future use.

Class	Start IP Range	End IP Range	Subnet Mask
A	0.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	undefined

The IPv4 specifications for addressing make it possible to generate more than four billion different addresses. Class D and E addresses are not so common, so for this course you will focus only on classes A, B, and C.

**Class A:** Use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.54.36.12 would be a class A address.

**Class B:** Use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.18.51.64 is a class B address.

**Class C:** Use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.99.143.182 is a class C address.

Below is a table providing typical subnets for IPv4.

Network Mask	Usable Hosts per Subnet
128.0.0.0	2,147,483,646
192.0.0.0	1,073,741,822
224.0.0.0	536,870,910
240.0.0.0	268,435,454
248.0.0.0	134,217,726
252.0.0.0	67,108,862
254.0.0.0	33,554,430
Class A	
255.0.0.0	16,777,214
255.128.0.0	8,388,606
255.192.0.0	4,194,302
255.224.0.0	2,097,150
255.240.0.0	1,048,574
255.248.0.0	524,286
255.252.0.0	262,142
255.254.0.0	131,070
Class B	

255.255.0.0	65,534
255.255.128.0	32,766
255.255.192.0	16,382
255.255.224.0	8,190
255.255.240.0	4,094
255.255.248.0	2,046
255.255.252.0	1,022
255.255.254.0	510
Class C	
255.255.255.0	254
255.255.255.128	126
255.255.255.192	62
255.255.255.224	30
255.255.255.240	14
255.255.255.248	6
255.255.255.252	2
255.255.255.254	0
255.255.255.255	0

### ***An alternative method for viewing a IP subnet***

CIDR stands for Classless Inter-Domain Routing (CIDR) and it is an allocation method for IPV4 addresses. It also provides an alternative way for stating an IP Address subnet mask.

Let's look at the following example: IP = 192.168.0.1

Lets say it has a subnet mask of 255.255.255.0, so the first three octets (192.168.0) identifies the network and only the 1 represents the host.

Another way to write this is 192.168.0.0/24. This may seem confusing but let's break it down: Each octet = 8 bits

So if a network uses the first three octets for the network that equals 24 bits. So when you see something saying 192.168.0.0/24 this simply means "The first 24 bits (three octets) represent the network". If it read 192.168.0.0/16, this means that the first 16 bits (two octets) represent the network.



For the IP Address 143.18.4.16 with a subnet mask of 143.0.0.0/8, what part of the IP Address is reserved for the network?

*Toggle the answer below to see the response.*

Network Address: 143

Host Address: 18.4.16

Toggle Answer

## How Subnet Masks Work

Subnet masks serve as a sort of filter for an IP address. With a subnet mask, devices can look at an IP address and determine which parts are the network and host bits. If you've looked through the network settings on your router or computer, you've probably seen this number: 255.255.255.0. If you've already done this, you've seen a standard subnet mask for simple home networks.

Another way of expressing this is with a network ID, which is just the network portion of the IP address. So, the network ID of address 192.168.0.1 with a subnet mask of 255.255.255.0 is the network 192.168.0.0/24. It doesn't matter which way you write it, but most agree that /24 is much easier to write than 255.255.255.0.

The main problem with classed IP addresses is that they are inefficient and can lead to many wasted IP addresses.

For example, imagine being part of a large organization. Your company has 1,000 employees, thus belonging to Class B, and if you reference the table above, you will see that a Class B network can support 65,534 usable addresses. That's far more than your organization would likely need, even if each employee had multiple devices, each with a unique address.

There would also be no way for your organization to be part of Class C. In that case, there would not be enough IP addresses for it. So while classed IP addresses were in use when IPv4 addresses were widespread, it quickly became apparent that a better system was needed to ensure that all of the approximately 4.2 billion usable addresses were not consumed.

## The Default Gateway and Broadcast

Suppose we have two devices in different subnets (the third octet for each is different, for example, of a /24 network). The default gateway is the destination of all traffic not on the same subnet. The gateway is a layer 3 device, such as a router or multilayer switch, used to route traffic hop-by-hop and permanently resides in the same subnet as the end device IP.

The gateway can be any address within the subnet itself. For sorting and good documentation, the network admins prefer to use the first IP number of the subnet as the gateway since the last is the broadcast IP.

Therefore, 192.168.0.1 would be the default gateway, and 192.168.0.255 would be the broadcast, given that we have a 192.168.0.0/255.255.255.0 subnet.

In computer networks, a broadcast address is a logical IP address in which all devices connected can receive datagrams, and all hosts connected to the network can obtain a message sent to a broadcast address. In this case, there is only one sender, but the information is sent to all connected receivers. Broadcast transmission is essential when sending the same message to all devices on the local network.

In conclusion, our initial IP example should demonstrate our initial subnetwork with the following information:

```
Network: 192.168.0.0
Gateway: 192.168.0.1
Broadcast: 192.168.0.255
Network mask: 255.255.255.0
CIDR notation: /24
IP class: C
Total number of hosts: 256
Number of usable IP addresses: 254
Usable IP range: 192.168.0.1 – 192.168.0.254
IP type: private
```

To calculate the **CIDR**, the network number and hosts, you can use many online tools found on these websites:

Online Calculator Resources:

[IP Subnet Calculator](#)

[Free Subnet Calculator](#)

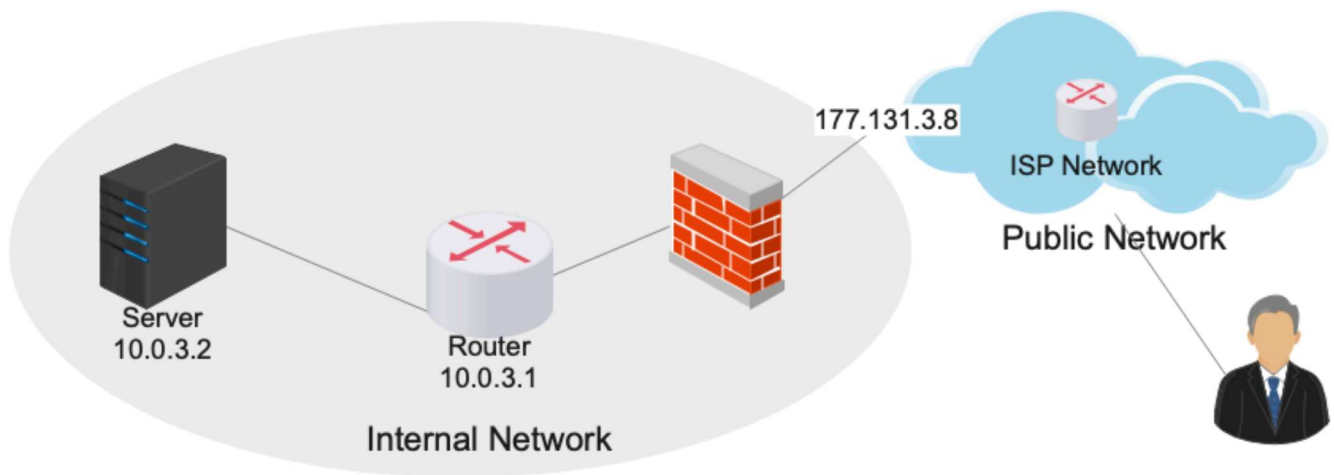
## Other Solutions

Another solution created to organize and avoid the end of IPv4 and conflicts between addresses was the **Dynamic Host Configuration Protocol (DHCP)**. Through DHCP, a host can obtain an IP address automatically and acquire additional information such as a subnet mask, default router address, and local DNS server address.

DHCP allows you to assign temporary IP addresses to your connected clients. With this method, obtaining an address for each client becomes unnecessary, only giving addresses dynamically through its DHCP server. This server will have a list of available IP addresses. Every time a new client connects to the network, it will be arbitrarily assigned one of these addresses, and the moment the client disconnects, the address is returned.

**Network address translation (NAT)** was another way to solve the problem of IPv4 address exhaustion. Its basic idea is to allow that, with a single IP address or a small number of them, several hosts can travel on the Internet. Each computer is assigned a unique private IP address within a network, which is used for routing internal traffic. However, when a packet needs to be routed out of the network, an address translation is performed, converting private IP addresses into globally unique public IP addresses.

## NAT - Network Address Translator



Three ranges of private IP addresses are chosen to be used, and the only rule of use is that no packet containing these addresses can travel on the public Internet.

The three reserved tracks are:

10.0.0.0 to 10.255.255.255 /8 (16,777,216 hosts)

172.16.0.0 to 172.31.255.255 /12 (1,048,576 hosts)

192.168.0.0 to 192.168.255.255 /16 (65,536 hosts)

The use of **NAT** has been proven efficient in terms of saving IP addresses, in addition to presenting some other positive aspects, such as facilitating the internal numbering of networks, hiding the network topology, and only allowing the entry of packets generated in response to a network request. However, using NAT has drawbacks that do not outweigh the advantages offered.


NAT breaks the end-to-end model of the Internet, and does not allow direct connections between two hosts, which makes it difficult for many applications such as **P2P, VoIP and VPNs** to work. Other problems are the low scalability, as the number of simultaneous connections is limited, and it demands a great deal of processing power from the translator device.

The use of NAT also makes it impossible to trace the path of the packet, through tools such as **TRACEROUTE**, for example, and makes it challenging to use some security techniques such as **IPSec**. In addition, its use gives a false sense of security because, despite not allowing the entry of unauthorized packets, NAT does not perform any filtering or verification on the packages that pass through it.

But even with all the solutions created, the IPv4 addressing is running out. To solve this problem, a new type of addressing was designed and is already being used to replace IPv4, called the **IPv6**. IPv6 has a larger address space, allowing for more devices to be connected to the Internet, and also includes new features such as improved security and autoconfiguration. It is backward-compatible with IPv4, which means that IPv6 devices can communicate with IPv4 devices, and IPv6 networks can be connected to IPv4 networks.

If you'd like a quick recap, check out this external video:

✓ Mark Completed



Previous  
Packets on the Network

Next  
IP Addresses: Intro to IPv6



How well did this activity help you to understand the content?  
Let us know how we're doing
















# W01D2

Tue Jun 25

> Lectures (1)

✓ Work (15)

8 hrs + 1 hr stretch 

	<u>Managing Linux Processes</u>	✓
	<u>Fork vs Exec</u>	
	<u>Adjusting Process Priority</u>	
	<u>Managing Linux Software</u>	✓
	<u>Linux Processes and Software</u>	✓
	<u>OSI layer models</u>	✓
	<u>The Encapsulation Process</u>	✓
	<u>Encapsulation Process Demonstration</u>	✓
	<u>Packets on the Network</u>	
	<u>IP Addresses: Intro to IPv4</u>	
	<u>IP Addresses: Intro to IPv6</u>	
	<u>The Value of Group Work!</u>	✓
	<u>Addressing Scheme</u>	✓



 AI Literacy Pre-Assessment



 Introduction to AI



[W01D2 Schedule »](#)

Powered by Lighthouse Labs.