Sophia

Internet Protocol Version 4 (IPv4)

by Sophia

WHAT'S COVERED

In this lesson, you will learn IP terminology and the IPv4 addressing scheme.

Specifically, this lesson will cover the following:

1. The Hierarchical IP Addressing Scheme

An IP Version 4 (IPv4) address consists of 32 bits of information. These bits are divided into four sections referred to as octets or bytes, and four octets sum up to 32 bits (8 × 4 = 32).

KEY CONCEPT

You can depict an IP address using one of three methods:

- Dotted decimal, as in 172.16.30.56
- Binary, as in 10101100.00010000.00011110.00111000
- Hexadecimal, as in AC.10.1E.38

Each of these examples validly represents the same IP address. Hexadecimal is used with IP Version 6 (IPv6), and IPv4 addressing uses dotted decimal or binary, but you might still find an IPv4 address stored in hexadecimal in some programs.

The 32-bit IP address is known as a structured, or hierarchical, address, as opposed to a flat, or nonhierarchical, address. The creators of IP addressing chose **hierarchical addressing** for a very important reason. It can handle a large number of addresses, namely, 4.3 billion (a 32-bit address space with two possible values for each position—either 0 or 1—gives you 2^{32}, or 4,294,967,296). The disadvantage of the flat-addressing scheme, and the reason it is not used for IP addressing, relates to routing. If every address were unique, all routers on the internet would need to store the address of each and every machine on the internet. This would make efficient routing impossible, even if only a fraction of all possible addresses were used.

The solution to this problem is to use a two- or three-level hierarchical addressing scheme that is structured by the network and the host or by the network, the subnet, and the host.

This two- or three-level scheme is comparable to a telephone number. The first section, the area code, designates a very large area. The second section, the prefix, narrows the scope to a local calling area. The final segment, the customer number, zooms in on the specific connection. IP addresses use the same type of layered structure. Rather than all 32 bits being treated as a unique identifier, as in flat addressing, a part of the address is designated as the network address and the other part is designated as either the subnet and the host or just the host address.

Next, we will cover IP network addressing and the different classes of addresses used for our networks.

TERM TO KNOW

Hierarchical Addressing
An addressing scheme made up of several levels.

---

2. Network Addressing

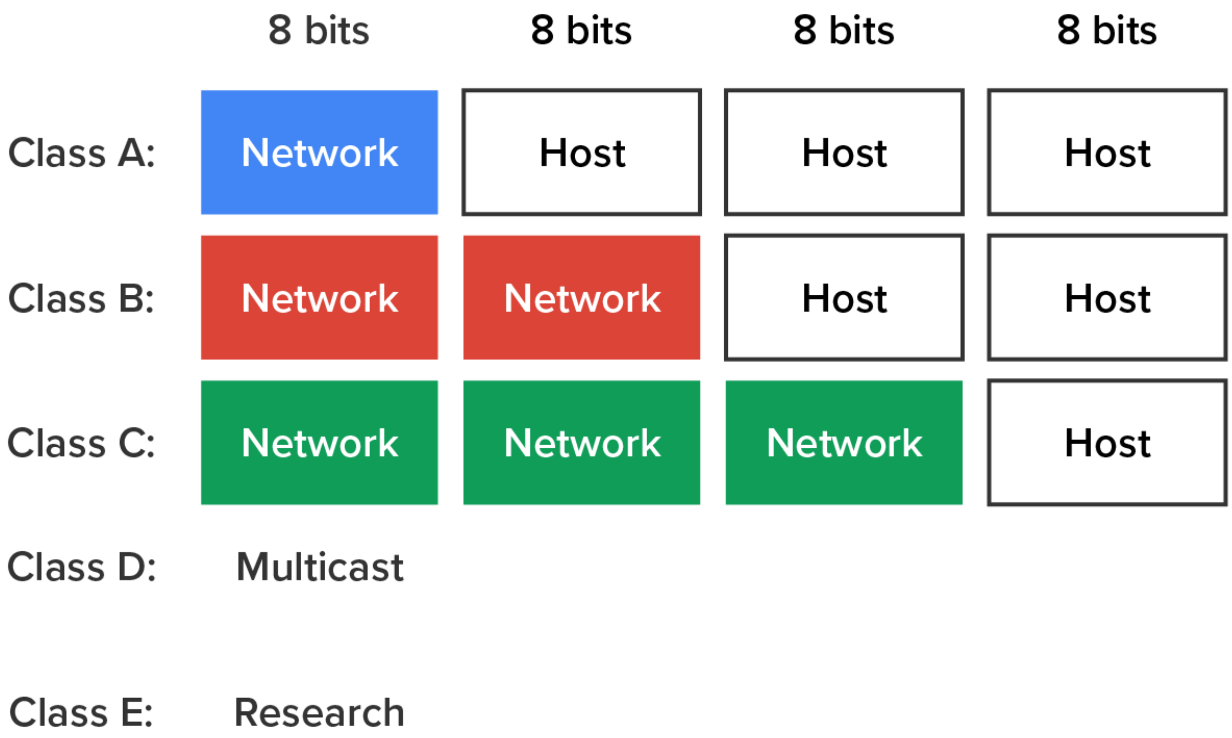
The **network address** uniquely identifies each network. Every machine on the same network shares that network address as part of its IP address. For example, in the IP address 172.16.30.56, 172.16 is the network address.

The **host address** is assigned to, and uniquely identifies, each machine on a network. This part of the address must be unique because it identifies a particular machine—an individual—as opposed to a network, which is a group. So, in the sample IP address 172.16.30.56, the 30.56 is the host address.

KEY CONCEPT

The designers of the internet decided to create classes of networks based on network size. For the small number of networks possessing a very large number of hosts, they created the rank *Class A network*. At the other extreme is the *Class C network*, which is reserved for the numerous networks with a small number of hosts. The class distinction for medium-sized networks is predictably the *Class B network*.

EXAMPLE Subdividing an IP address into a network and host address is determined by the class designation of your network. The diagram below summarizes the IPv4 classes of networks.



TERMS TO KNOW

Network Address
The portion of an IP address that uniquely identifies a network.

Host Address
The portion of an IP address that uniquely identifies a host on a network.

2a. Class A Addresses

In a Class A network address, the first byte is assigned to the network address, and the three remaining bytes are used for the host addresses. The Class A format is as follows: *network.host.host.host*

EXAMPLE In the IP address 49.22.102.70, 49 is the network address, and 22.102.70 is the host address. Every machine on this particular network would begin with the distinctive network address of 49.

Class A network addresses are 1-byte long, with the first bit of that byte reserved and the 7 remaining bits available for manipulation, or addressing. As a result, the theoretical maximum number of Class A networks that can be created is 128. Why? Well, each of the 7 bit positions can be either a 0 or a 1 and 2^7 gives you 128.

The designers of the IP address scheme said that the first bit of the first byte in a Class A network address must always be off, or 0. This means a Class A address must be between 0 and 127 in the first byte, inclusive.

Consider the following network address:
0*xxxxxxx*

If we turn all the other 7 bits off and then turn them all on, we'll find the Class A range of network addresses:
00000000 = 0
01111111 = 127

So, a Class A network is defined in the first octet between 0 and 127, and it cannot be less or more.

To complicate matters further, the network address of all 0s (0000 0000) is reserved to designate the default route (see the table below). Additionally, the address 127, which is reserved for **loopback** diagnostics, cannot be used either, which means that you can really only use the numbers 1 to 126 to designate Class A network addresses. This means the actual number of usable Class A network addresses is 128 minus 2, or 126.

TCP	UDP
Network address of all 0's	Interpreted to mean "this network or segment."
Network address of all 1's	Interpreted to mean "all networks."
Network 127.0.0.1	Reserved for loopback tests. Designates the local host and allows that host to send a test packet to itself without generating network traffic.
Host address of all 0s	Interpreted to mean "network address" or any host on a specified network.
Host address of all 1s	Interpreted to mean "All hosts" on the specified network; for example, 126.255.255.255 means "all hosts on network 126 (Class A address).
Entire IP address set to all 0s	Used by Cisco routers to designate the default route. Could also mean "any network"
Entire IP address set to all 1s (same as 255.255.255.255)	Broadcast to all hosts on the current network; sometimes called an "all 1s broadcast" or limited broadcast.

Each Class A address has 3 bytes (24 bit positions) for the host address of a machine. This means there are 2^{24}—or 16,777,216—unique combinations and, therefore, precisely that many potential unique host addresses for each Class A network.

EXAMPLE Here is a method to figure out the valid host IDs in a Class A network address:

- All host bits off is the network address 10.0.0.0.
- All host bits on is the broadcast address 10.255.255.255.

The valid hosts are the numbers in between the network address and the broadcast address: 10.0.0.1 through 10.255.255.254. Notice that 0s and 255s can be valid host IDs. All you need to remember when trying to find valid host addresses is that the host bits cannot ever be all unset (turned off) or all set (turned on) at the same time.

TERM TO KNOW

Loopback
The routing of a signal from its origin back to the origin, primarily as a means of testing the network connectivity.

2b. Class B Addresses

In a Class B network address, the first 2 bytes are assigned to the network address and the remaining 2 bytes are used for host addresses.

The format is as follows:
network.network.host.host

EXAMPLE In the IP address 172.16.30.56, the network address is 172.16 and the host address is 30.56.

With a network address being 2 bytes (8 bits each), we are left with 2^{16} unique combinations. But the internet designers decided that all Class B network addresses should start with the binary digit 1, then 0. This leaves 14 bit positions available to manipulate, so in reality, we get 16,384 (that is, 2^{14}) unique Class B network addresses.

EXAMPLE In a Class B network, the RFCs state that the first bit of the first byte must always be turned on, but the second bit must always be turned off. If we turn the other 6 bits all off and then all on, we will find the range for a Class B network:

$10000000 = 128$
$10111111 = 191$

As you can see, a Class B network is defined when the first byte is configured from 128 to 191.
A Class B address uses 2 bytes for host addresses. This is 2^{16} minus the two reserved patterns (all 0s and all 1s), for a total of 65,534 possible host addresses for each Class B network. Here is an example of how to find the valid hosts in a Class B network:

- All host bits turned off is the network address: 172.16.0.0.
- All host bits turned on is the broadcast address: 172.16.255.255.

The valid hosts would be the numbers in between the network address and the broadcast address: 172.16.0.1 through 172.16.255.254.

2c. Class C Addresses

The first 3 bytes of a Class C network address are dedicated to the network portion of the address with only 1 measly byte remaining for the host address. Here is the format: *network.network.network.host*

Using the example IP address 192.168.100.102, the network address is 192.168.100 and the host address is 102.

In a Class C network address, the first 3 bit positions are always the binary 110. The calculation is as follows: 3 bytes, or 24 bits, minus 3 reserved positions leaves 21 positions. Hence, there are 2^{21}, or 2,097,152, possible Class C networks.

For Class C networks, the RFCs define the first 2 bits of the first octet as always turned on, but the third bit can never be on. Following the same process as the previous classes, convert from binary to decimal to find the range. Here is the range for a Class C network:
11000000 = 192
11011111 = 223

So, if you see an IP address with a range from 192 up to 223, you will know it's a Class C IP address.

Each unique Class C network has 1 byte to use for host addresses. This gets us to 2^{8}, or 256, minus the two reserved patterns of all 0s and all 1s for a total of 254 available host addresses for each Class C network.

EXAMPLE Here is method to find a valid host ID in a Class C network:

- All host bits turned off is the network ID: 192.168.100.0.
- All host bits turned on is the broadcast address: 192.168.100.255.

The valid hosts would be the numbers in between the network address and the broadcast address: 192.168.100.1 through 192.168.100.254.

2d. Class D and E Addresses

Addresses with the first octet of 224 to 255 are reserved for Class D and E networks. Class D (224–239) is used for multicast addresses and Class E (240–255) for scientific purposes. But they are really beyond the scope of this course, so we are not going to go into detail about them here. But you do need to know that the multicast range is from 224.0.0.0 through 239.255.255.255.

Address Class	Reserved Address Space
Class D	Multicast 224-239
Class E	Scientific 24-255

2e. Private IP Addresses (RFC 1918)

The people who created the IP addressing scheme also created what we call **private IP addresses**. These addresses can be used on a private network, but they are not routable through the internet. This is designed for the purpose of creating a measure of much-needed security, but it also conveniently saves valuable IP address space.

If every host on every network had to have routable IP addresses, we would have run out of available IP addresses to hand out years ago. But by using private IP addresses, ISPs, corporations, and home users need only a relatively tiny group of bona fide IP addresses to connect their networks to the internet. This is economical because they can use private IP addresses on their inside networks and get along just fine.

To accomplish this task, the ISP and the corporation—the end users, no matter who they are—need to use something called **Network Address Translation (NAT)**, which basically takes a private IP address and converts it for use on the internet. NAT provides security in that these IP addresses cannot be seen by external users. External users will only be able to see the **public IP address** to which the private IP address has been mapped. Moreover, multiple devices in the same private network can use the same public IP address to transmit out onto the internet.

The table below lists the reserved private addresses.

Address class	Reserved address space
Class A	10.0.0.0 through 10.255.255.255
Class B	172.16.0.0 through 172.31.255.255
Class C	192.168.0.0 through 192.168.255.255

TERMS TO KNOW

Private IP Address
An IP address that is not routable on the public internet.

Network Address Translation (NAT)
A process of translating a private IP address to a public IP address and vice versa.

Public IP Address
An IP address that is routable on the public internet.

SUMMARY

In this lesson, you learned about IPv4's **hierarchical addressing scheme**. You also learned about private **IP network addressing** (RFC 1918) including Class A, Class B, Class C, and Classes D and E.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source [Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)]

TERMS TO KNOW

Hierarchical Addressing
An addressing scheme made up of several levels.

Host Address
The portion of an IP address that uniquely identifies a host on a network.

Loopback
The routing of a signal from its origin back to the origin, primarily as a means of testing the network connectivity.

Network Address
The portion of an IP address that uniquely identifies a network.

Network Address Translation (NAT)
A process of translating a private IP address to a public IP address and vice versa.

Private IP Address
An IP address that is not routable on the public internet.

Public IP Address
An IP address that is routable on the public internet.