

<https://www.ciscopress.com/articles/article.asp?p=330807&seqnum=2>

IPv4 Addressing

This section covers some of the basic concepts of IPv4 addressing, such as how the Internet's address architecture uses the binary and dotted-decimal versions of IPv4 addressing. This section also reviews the structure of IPv4 addresses, such as the various classes of IPv4 addresses. Finally, this section reviews how IPv4 addresses use subnet masks to help divide and manage the size and growth of the Internet and computer networks.

Address Architecture of the Internet

When TCP/IP was introduced in the 1980s, it relied on a two-level addressing scheme. At the time, this scheme offered adequate scalability. The 32-bit-long IPv4 address identifies a network number and a host number, as shown in Figure 2-1.

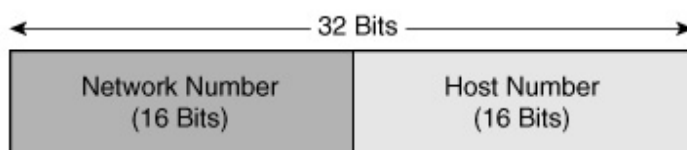


Figure 2-1 IP Address Structure

Together, the network number and the host number uniquely identify all hosts connected by way of the Internet. It is possible that the needs of a small networked community, such as a LAN, could be satisfied with just host addresses. However, network addresses are necessary for end systems on different networks to communicate with each other. Routers use the network portion of the address to make routing decisions and to facilitate communication between hosts that belong to different networks.

Unlike routers, humans find working with strings of 32 1s and 0s tedious and clumsy. Therefore, 32-bit IP addresses are written using dotted-decimal notation. Each 32-bit address is divided into four groups of eight, called octets. Each octet is converted to decimal and then separated by decimal points, or dots. This is illustrated as follows:

- A 32-bit IP address is a binary number:

10101100000111101000000000010001

- This binary number can be divided into four octets:

10101100 00011110 10000000 00010001

- Each octet (or byte) can be converted to decimal:

172 30 128 17

- Finally, the address can be written in dotted-decimal notation:

172.30.128.17

In the dotted-decimal address 172.30.128.17, which of these four numbers represents the network portion of the address? Which numbers are the host numbers? Finding the answers to these questions is complicated by the fact that IP addresses are not really four numbers. They actually consist of 32 different numbers, or 32 bits.

In the early days of TCP/IP, a class system was used to define the network and host portions of the address. IPv4 addresses were grouped into five distinct classes. This was done according to the value of the first few bits in the first octet of the address. Although the class system can still be applied to IP addresses, networks today often ignore the rules of class in favor of a classless IP scheme.

The next few sections cover all of the following topics related to IP addressing:

- The limitations of the IP address classes
- The subsequent addition of the subnet mask
- The addressing crisis that led to the adoption of a classless system

Class A and B IP Addresses

In a class system, IP addresses can be grouped into one of five different classes:

- A
- B
- C
- D
- E

Each of the four octets of an IP address represents either the network portion or the host portion of the address, depending on the address class. The network and host portions of the respective Class A, B, C, and D addresses are shown in Figure 2-2.

Class A	Network		Host	
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Figure 2-2 Address Structure

Only the first three classes—A, B, and C—are used to address actual hosts on IP networks. Class D addresses are used for multicasting. Class E addresses are reserved for experimentation and are not shown in Figure 2-2. The following sections explore each of the five classes of addresses.

Class A Addresses

If the first bit of the first octet of an IP address is a binary 0, the address is a Class A address. With that first bit being a 0, the lowest number that can be represented is 00000000, decimal 0. The highest number that can be represented is 01111111, decimal 127. Any address that starts with a value between 0 and 127 in the first octet is a Class A address. These two numbers, 0 and 127, are reserved and cannot be used as a network address.

Class A addresses were intended to accommodate very large networks, so only the first octet is used to represent the network number. This leaves three octets, or 24 bits, to represent the host portion of the address. With 24 bits total, 2^{24} combinations are possible, yielding 16,777,216 possible addresses. Two of those possibilities, the lowest and highest values, are reserved for special purposes. The low value is 24 0s, and the high value is 24 1s. Therefore, each Class A address can support up to 16,777,214 unique host addresses.

Why are two host addresses reserved for special purposes? Every network requires a network number. A network number is an ID number that is used to refer to the entire range of hosts when building routing tables. The address that contains all 0s in the host portion is used as the network number and cannot be used to address an individual node. 46.0.0.0 is a Class A network number. Similarly, every network requires a broadcast address that can be used to address a message to every host on a network. It is created when the host portion of the address has all 1s. For example, a broadcast address for network 46.0.0.0 would be 46.255.255.255.

With almost 17 million host addresses available, a Class A network actually provides too many possibilities for one company or campus. Although it is easy to imagine an enormous global network with that many nodes, the hosts in such a network could not function as members of the same logical group. Administrators require much smaller logical groupings to control broadcasts, apply policies, and troubleshoot problems. Fortunately, the subnet mask allows subnetting, which breaks a large block of addresses into smaller groups called subnetworks. All Class A networks are subnetted. If they were not, Class A networks would represent huge waste and inefficiency.

How many Class A addresses are there? Because only the first octet is used as a network number, and it contains a value between 0 and 126, 126 Class A networks exist. Each of the 126 Class A addresses has almost 17 million possible host addresses that make up about half of the entire IPv4 address space. Recall that the network address 127.0.0.1 is reserved for the local loopback address, which is why Class A addresses stop at 126.0.0.0 and Class B addresses start at 128.0.0.0. Under this system, a mere handful of organizations control half of the available Internet addresses.

Class B Addresses

Class B addresses start with a binary 10 in the first 2 bits of the first octet. Therefore, the lowest number that can be represented with a Class B address is 10000000, decimal 128. The highest number that can be represented is 10111111, decimal 191. Any address that starts with a value in the range of 128 to 191 in the first octet is a Class B address.

Class B addresses were intended to accommodate medium-size networks. Therefore, the first two octets are used to represent the network number, which leaves two octets or 16 bits to represent the host portion of the address. With 16 bits total, 2^{16} combinations are possible, yielding 65,536 Class B addresses. Recall that two of those numbers, the lowest and highest values, are reserved for special purposes. Therefore, each Class B address can support up to 65,534 hosts. Although it is significantly smaller than the networks created by Class A addresses, a logical group of more than 65,000 hosts is still unmanageable and impractical. Therefore, like Class A networks, Class B addresses are subnetted to improve efficiency.

Because the first 2 bits of a Class B address are always 10, 14 bits are left in the network portion of the address, resulting in 2^{14} or 16,384 Class B networks. The first octet of a Class B address offers 64 possibilities, 128 to 191. The second octet has 256 possibilities, 0 to 255. That yields 16,384 addresses, or 25 percent of the total IP space. Nevertheless, given the popularity and importance of the Internet, these addresses have run out quickly. This essentially leaves only Class C addresses available for new growth.

Classes of IP Addresses: C, D, and E

This section covers Class C, D, and E IP addresses.

Class C Addresses

A Class C address begins with binary 110. Therefore, the lowest number that can be represented is 11000000, decimal 192. The highest number that can be represented is 11011111, decimal 223. If an IPv4 address contains a number in the range of 192 to 223 in the first octet, it is a Class C address.

Class C addresses were originally intended to support small networks. The first three octets of a Class C address represent the network number. The last octet may be used for hosts. One host octet yields 256 (2^8) possibilities. After the all-0s network number and the all-1s broadcast address are subtracted, only 254 hosts may be addressed on a Class C network. Whereas Class A and Class B networks prove impossibly large without subnetting, Class C networks can impose an overly restrictive limit on hosts.

Because the first 3 bits of a Class C address are always 110, 21 bits are left in the network portion of the address, resulting in 2^{21} or 2,097,152 Class C networks. With 2,097,152 total network addresses containing a mere 254 hosts each, Class C addresses account for 12.5 percent of the Internet address space. Because Class A and B addresses are nearly exhausted, the remaining Class C addresses are all that is left to be assigned to new organizations that need IP networks. Table 2-1 summarizes the ranges and availability of the three address classes used to address Internet hosts.

Table 2-1 IP Addresses Available to Internet Hosts

Address Class	First Octet Range	Number of Possible Networks	Number of Hosts Per Network
Class A	0 to 126	127 (2 are reserved)	16,777,214
Class B	128 to 191	16,384	65,534
Class C	192 to 223	2,097,152	254

Class D Addresses

A Class D address begins with binary 1110 in the first octet. Therefore, the first octet range for a Class D address is 11100000 to 11101111, or 224 to 239. Class D addresses are not used to address individual hosts. Instead, each Class D address can be used to represent a group of hosts called a host group, or multicast group.

For example, a router configured to run Enhanced Interior Gateway Routing Protocol (EIGRP) joins a group that includes other nodes that are also running EIGRP. Members of this group still have unique IP addresses from the Class A, B, or C range, but they also listen for messages addressed to 224.0.0.10. The 224 octet designates the address as a Class D address. Therefore, a single routing update message can be sent to 224.0.0.10, and all EIGRP routers will receive it. A

single message sent to several select recipients is called a multicast. Class D addresses are also called multicast addresses.

A multicast is different from a broadcast. Every device on a logical network must process a broadcast, whereas only devices configured to listen for a Class D address receive a multicast.

Class E Addresses

If the first octet of an IP address begins with 1111, the address is a Class E address. Therefore, the first octet range for Class E addresses is 11110000 to 11111111, or 240 to 255. Class E addresses are reserved for experimental purposes and should not be used to address hosts or multicast groups.

Subnet Masking

Subnet masking, or subnetting, is used to break one large group into several smaller subnetworks, as shown in Figure 2-3. These subnets can then be distributed throughout an enterprise. This results in less IP address waste and better logical organization. Formalized with RFC 950 in 1985, subnetting introduced a third level of hierarchy to the IPv4 addressing structure. The number of bits available to the network, subnet, and host portions of a given address varies depending on the size of the subnet mask.

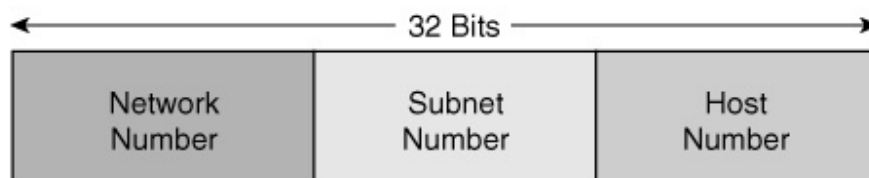


Figure 2-3 IP Address Structure After Subnetting

A subnet mask is a 32-bit number that acts as a counterpart to the IP address. Each bit in the mask corresponds to its counterpart bit in the IP address. Logical ANDing is applied to the address and mask. If a bit in the IP address corresponds to a 1 bit in the subnet mask, the IP address bit represents a network number. If a bit in the IP address corresponds to a 0 bit in the subnet mask, the IP address bit represents a host number.

When the subnet mask is known, it overrides the address class to determine whether a bit is either a network or a host. This allows routers to recognize addresses differently than the format dictated by class. The mask can be used to tell hosts that although their addresses are Class B, the first three octets, instead of the first two, are the network number. In this case, the additional octet acts like part of the network number, but only inside the organization where the mask is configured.

The subnet mask applied to an address ultimately determines the network and host portions of an IP address. The network and host portions change when the subnet mask changes. If a 16-bit mask, 255.255.0.0, is applied to an IP address, only the first 16 bits, or two octets, of the IP address 172.24.100.45 represent the network number. Therefore, the network number for this host address is 172.24.0.0. The colored portion of the address shown in Figure 2-4 indicates the network number.

IP Address 172.24.100.45

Dotted Decimal	172	24	100	45
Binary	10101100	00011000	01100100	00101101

Subnet Mask 255.255.0.0

Binary	11111111	11111111	00000000	00000000
Dotted Decimal	255	255	0	0

Figure 2-4 Class B Address Without Subnetting

Because the rules of class dictate that the first two octets of a Class B address are the network number, this 16-bit mask does not create subnets within the 172.24.0.0 network.

To create subnets with this Class B address, a mask must be used that identifies bits in the third or fourth octet as part of the network number.

If a 24-bit mask such as 255.255.255.0 is applied, the first 24 bits of the IP address are specified as the network number. The network number for the host in this example is 172.24.100.0. The gray portion of the address shown in Figure 2-5 indicates this.

Routers and hosts configured with this mask see all 8 bits in the third octet as part of the network number. These 8 bits are considered to be the subnet field because they represent network bits beyond the two octets prescribed by classful addressing.

Inside this network, devices configured with a 24-bit mask use the 8 bits of the third octet to determine to what subnet a host belongs. Because 8 bits remain in the host field, 254 hosts may populate each network. Just as hosts must have identical network addresses, they also must match subnet fields to communicate with each other directly. Otherwise, the services of a router must be used so that a host on one network or subnet can talk to a host on another.

IP Address 172.24.100.45			Subnet Field	
Dotted Decimal	172	24	100	45
Binary	10101100	00011000	01100100	00101101

Subnet Mask 255.255.255.0			Subnet Field	
Binary	11111111	11111111	11111111	00000000
Dotted Decimal	255	255	255	0

Figure 2-5 Class B Address with Subnetting

A Class B network with an 8-bit subnet field creates 2^8 , or 256, potential subnets, each one equivalent to one Class C network. Because 8 bits remain in the host field, 254 hosts may populate each network. Two host addresses are reserved as the network number and broadcast address, respectively. By dividing a Class B network into smaller logical groups, the internetwork can be made more manageable, more efficient, and more scalable.

Notice that subnet masks are not sent as part of an IP packet header. This means that routers outside this network will not know what subnet mask is configured inside the network. An outside router, therefore, treats 172.24.100.45 as just one of 65,000 hosts that belong to the 172.24.0.0 network. In effect, subnetting classful IP addresses provides a logical structure that is hidden from the outside world.

Interactive Media Activity Fill in the Blank: Subnet Tool

After completing this activity, you will have a better understanding of the concept of subnetting.