7

IP Addressing and Subnetting

CERTIFICATION OBJECTIVES

7.01 IP Addressing Review

7.02 Subnetting

7.03 IP Address Planning

7.04 Determining IP Address Components

✓ Two-Minute Drill

Q&A Self Test

Probably one of the most confusing aspects of the TCP/IP protocol stack is the addressing structure used at the Internet layer, referred to as *IP addressing*. Chapter 6 briefly discussed IP addresses and their classes. This chapter focuses on IP addressing, its components, and how to plan for addressing. Note that two different versions of TCP/IP addressing are in use: IPv4 and IPv6. This chapter focuses on 32-bit IPv4 addressing; Chapter 24 focuses on 128-bit IPv6 addressing. Before beginning this chapter, you should go back to Chapter 3 and review the binary and decimal conversion process, since these concepts are used heavily in this chapter.

CERTIFICATION OBJECTIVE 7.01

IP Addressing Review

Recall from Chapter 6 that IPv4 addresses are 32 bits long, broken up into 4 bytes, and separated by decimals, commonly called the *dotted decimal format*. Two components make up the address: a *network* and *host number*. The combination of these two numbers must be unique in the entire network. You can compare an IP address to the United States postal system: The IP address works like a ZIP code. When you address a letter and put it in the mailbox, the clerk at your post office doesn't care *who* you're sending it to or their street address. He *does* pay attention to the ZIP code, however. He'll have several containers behind him and will drop the letter into the appropriately numbered one. If the ZIP starts with a *3*, for example, he'll put it in the container headed to the southeastern United States. At the regional post office, they'll drop the letter into the state container (*32* for Florida), and so on and so on, until it reaches to the post office closest to the recipient (*32765*, in Oviedo, Florida).

If IP addressing were this easy, a lot of network administrators would be unemployed. However, to complicate matters, IP addresses are broken down into address classes: A, B, C, D, and E. Each A, B, and C class address has a predefined network boundary, shown in Table 7-1. Class D addresses are used for multicasting and Class E for research purposes.

exam watch

Remember the five classes of IP addresses, and the fact that Class A addresses have, by default, 8 network bits, Class B addresses have 16 bits, and Class C addresses have 24 bits.

TABLE 7-1 Network and Host Boundaries

Address Class	Network Bytes	Host Bytes	Beginning Bit Values	Addresses (First Octet)
A	1 (8 bits)	3 (24 bits)	0	1–126; 0 and 127 are reserved
B	2 (16 bits)	2 (16 bits)	10	128–191
C	3 (24 bits)	1 (8 bits)	110	192–223
D	N/A	N/A	1110	224–239
E	N/A	N/A	11110	240–254; 255 is reserved

Distinguishing Between Classes of Addresses

Given the aforementioned class distinctions, it would seem that addressing for IP is easy. However, what distinguishes the different classes of addresses are the values to which the first to fifth bits are set, as shown in Table 7-1. When you're talking about the highest order bit or bits, this includes *all* 32 bits of the IP address. Therefore, the address's class can be determined by looking at the very first bit to the *left* of the address (the most significant bit). If the first octet contains 10000001, this represents 129 in decimal, which would be a Class B address. Given the aforementioned distinctions with the assigned high-order bit values, it is easy to tell which class of network numbers a particular address belongs to.

In Class A addresses, *0* (in the first octet) is reserved; it represents "all" IP addresses and is commonly used as a default route. The address *127* is also reserved for a loopback, which is used for local testing function. In Class E, *255* is reserved and is used as a local broadcast—all IP devices in a broadcast domain, such as a segment or virtual LAN (VLAN). Also, remember that there are three classes of private addresses: Class A, 10.0.0.0; Class B, 172.16.0.0–172.31.0.0; and Class C, 192.168.0.0–192.168.255.0. Recall from Chapter 6 that private addresses can be used internally in a network, but they must be translated to a public address space before being transmitted to a public network such as the Internet (discussed in Chapter 23).

exam watch

Remember the binary values that IP addresses begin with and be able to determine, by looking at the first binary byte, whether the address is a Class A, B, C, D, or E address.

IP Address Components

Two components make up a Class A, B, and C IP address: *network* and *host*. The host portion is actually broken into three subcomponents: the *network address*, the *host address*, and the *directed broadcast address*.

The first address in a network number is called the *network address*, or *wire number*. This address is used to uniquely identify one segment or broadcast domain/VLAN from all the other segments in the network. The last address in the network number is called the *directed broadcast address* and is used to represent all hosts on this network segment. A directed broadcast is similar to a local broadcast. The main difference is that routers will not propagate local broadcasts between segments, but they will, by default, propagate directed broadcasts. Any address between the network address and the directed broadcast address is called a *host address* for the segment. You assign these middle addresses to host devices on the segment, such as PCs, servers, routers, and switches.

exam watch

Each network has two reserved addresses: a network number (the first address) and a directed broadcast (the last address). Any addresses between these two values can be assigned to networking devices on the segment and are called host addresses.

Network and Directed Broadcast Addresses

When dealing with a network address, all the host bits in the host portion of the address are set to 0s (zeros). If all the host bits in a network number are set to 1s (ones), making it the very last address, then this is the *directed broadcast* address. Any combination of bit values between these two numbers in the *host* portion of the address is considered a *host* address.

Here's an example: 192.1.1.0 is a Class C address and is also a network number. Recall from the table that the Class C addresses range from 192 to 223 in the first octet or byte and the network number is 3 bytes long. Therefore, *192.1.1* is the network number. The last byte is the host address. This byte is 0 (all bits are zero), which is the very *first* address in the network. Therefore, the network address is *192.1.1.0*. If you would set the last 8 bits to all 1s (all the host bits), which is equivalent to 255 in decimal, this would be the directed broadcast (192.1.1.255) for the network.

Host Addresses

Any number between the network address and the directed broadcast address is a host address. In the preceding example, any number between 0 and 255 is a host address for the network 192.1.1.0: 192.1.1.1–192.1.1.254. An important item to point out about this process is that for any given network number, you *lose* two addresses. The first address in a network is reserved for the network number itself and the last address is reserved for the directed broadcast address for the network. A formula can be used to define the number of available host addresses, assuming that you know the number of bits that can be used for host numbers: $2^H - 2$. At the beginning of this formula, *2* is raised to the power of *H*, where *H* is the number of host bits.

So, for example, a Class C network has a 24-bit network number component and an 8-bit host component. Therefore, for a Class C network, the lowest address in this fourth octet is *0* and the last address in this octet is *255* (all 8 bits are set to *1*). All numbers between 1 and 254 are host addresses for the Class C network. Using the addressing formula, you can easily show that a Class C network has 254 host addresses: $2^H - 2 = 2^8 - 2 = 256 - 2 =$ *254* available host addresses. For a Class B network, the number of host addresses is 65,534: $2^H - 2 = 2^{16} - 2 = 64{,}536 - 2 =$ *65,534*. And for a Class A network, the number of host addresses is 16,777,214: $2^H - 2 = 2^{24} - 2 =$ 16,777,216 – 2 = *16,777,214*. See Chapter 3 for a review of powers of 2.

exam watch

Remember that each network loses two addresses for host assignments. Also remember the $2^H - 2$ formula, which you can use based on number of host bits (H), to determine the number of hosts a network will support.

CERTIFICATION OBJECTIVE 5.02

Subnetting

One of the problems with the original IP addressing scheme was that for Class A and B networks, address efficiency was an issue. In other words, how many hosts can you physically put on a network segment or broadcast domain? Even with the advent of VLANs, this number did not increase dramatically. With IP, you can get 200 to 500 devices in a single broadcast domain before experiencing broadcast problems. This is one to two Class C networks. If you would assign a Class B network for this broadcast domain, you'd be wasting more than 65,000 addresses.

To overcome this deficiency issue, subnetting was introduced. Subnetting allows you to take some of the *higher-order host* bits in a network number and use them to create more networks. In the process of creating more networks, each of these additional networks has a lesser number of hosts. These smaller networks are commonly called *subnets*. One disadvantage of subnetting is that you are losing more addresses, because each of these subnets has a network and directed broadcast address. However, the advantage of subnetting is that you now can more efficiently use your addresses for a class network.

Let's look at an example. A Class C network has 8 host bits, giving you a total of 256 addresses. Of these 256 addresses, you can use only 254 for host devices, such as PCs, routers, and servers. Let's assume that you use the highest order bit to create more networks, leaving 7 bits for host addresses. With this example, you are creating two subnets: $2^1 = 2$. In this formula, the *1* is the number of subnet bits. In each of these subnets you have 126 host addresses: $2^7 – 2 = 126$. Originally, you lost two addresses in a Class C network. Now that you have two subnets, you are losing a total of four addresses. However, the advantage of subnetting is that you now have two networks instead of one!

Or suppose you have two segments in your network with 100 hosts each on them. You could assign a separate Class C network to each of these segments, but this would be a very inefficient use of your addresses. By using subnetting, you can more efficiently use your addresses. In this example, one Class C network, subnetted with one subnet bit, creates two subnets with 126 host addresses each. So in this example, you are wasting a smaller number of addresses.

Subnet Masks

TCP/IP is unique among most layer 3 addressing schemes. When dealing with TCP/IP addresses, each address actually has three components: a network component, a host component, and a *subnet mask*. The function of the subnet mask is to differentiate among the network address, the host addresses, and the directed broadcast address. Subnetting was originally defined in RFC 950.

Like an IP address, a subnet mask is 32 bits long. In binary, a *1* in a bit position in the subnet mask represents a network component and a *0* in a bit position represents a host component. One restriction of subnet masks is that all the network bits (1s) must be contiguous and all the host bits (0s) are contiguous. This is true not only in a single octet, but across all the bits in all four octets. A subnet mask of 11110000.00001111.11111111.11111111 (240.31.255.255) would be invalid since all the 1s are not contiguous. A subnet mask of 11111111.11111111.11111111.11111000 (255.255.255.248), however, is valid.

You can actually use four methods to represent a subnet mask. Here is a list with a demonstration using a Class C network:

- **Dotted-decimal** 192.168.1.0 255.255.255.0
- **Number of networking bits** 192.168.1.0/24
- **Hexadecimal** 192.168.1.0 0xFFFFFF00
- **Binary** 192.168.1.0 11111111111111111111111100000000

The most common of these formats is the dotted-decimal and the number of networking bits used (the first two listed above). Hexadecimal and binary are rarely used.

exam watch

Subnet mask values, binary 1s and 0s, must be contiguous in order to be considered as a valid subnet mask. When representing subnet masks, be very familiar with both the dotted-decimal and number of networking bits nomenclature.

exam watch

Any subnet mask using a number not listed in Table 7-2 is invalid.

Subnet Mask Values

Given the fact that subnet mask values must have all 1s contiguous and all 0s contiguous, Table 7-2 shows some valid decimal numbers for subnet masks in an octet.

TABLE 7-2

Valid Subnet Mask Values in an Octet

00000000 = 0	11100000 = 224	11111100 = 252
10000000 = 128	11110000 = 240	11111110 = 254
11000000 = 192	11111000 = 248	11111111 = 255

For a Class A network, the default subnet mask is 255.0.0.0: the first octet (byte) is the network number and the last three octets are the host numbers. For a Class B network, the default subnet mask is 255.255.0.0: the first two octets are the network number and the last two octets are the host numbers. For a Class C network, the default subnet mask is 255.255.255.0: the first three octets are the network numbers and the last octet is the host number.

One important item to point out is that the subnet mask, in and of itself, means nothing without the context of the IP address associated with it. For example, most people would assume that when you see a subnet mask of 255.255.255.0, you are dealing with a Class C network. However, remember that you can perform subnetting on any class address: A, B, and C. So a subnet mask of 255.255.255.0 can also be used for Class A and B networks. Therefore, the IP address and subnet mask have a symbiotic relationship. The following sections will show you the valid subnet mask values for Class A, B, and C networks.

exam watch

When subnetting, depending on the device, the very first and last subnet in a network, referred to as *subnet 0****, might or might not be valid. For the exam, remember this, since the exam may or may not tell you one way or the other. However, when looking for an answer, you'll never see both as a valid answer; either the answer will include the first and last subnet or it won't.***

Subnet Masks for Class A Networks

Table 7-3 shows valid subnet masks for Class A networks. In this table, the number of networking bits is the total number of bits used in networking, including both the network and subnet bits. This is also true in Tables 7-4 and 7-5.

exam watch

The best subnet mask for a point-to-point link, for which you need only two host addresses, is 255.255.255.252.

TABLE 7-3 Valid Subnet Masks for Class A Networks

Subnet Mask	Networking Bits	Number of Subnets	Number of Hosts per Subnet
255.255.255.252	/30	4,194,304	2
255.255.255.248	/29	2,097,152	6
255.255.255.240	/28	1,048,576	14
255.255.255.224	/27	524,288	30
255.255.255.192	/26	262,144	62
255.255.255.128	/25	131,072	126
255.255.255.0	/24	65,536	254
255.255.254.0	/23	32,768	510
255.255.252.0	/22	16,384	1022
255.255.248.0	/21	8192	2046
255.255.240.0	/20	4096	4094
255.255.224.0	/19	2048	8190
255.255.192.0	/18	1024	16,382
255.255.128.0	/17	512	32,766
255.255.0.0	/16	256	65,534
255.254.0.0	/15	128	131,070
255.252.0.0	/14	64	262,142
255.248.0.0	/13	32	524,286
255.240.0.0	/12	16	1,048,574
255.224.0.0	/11	8	2,097,150
255.192.0.0	/10	4	4,194,302
255.128.0.0	/9	2	8,388,606
255.0.0.0	/8	1	16,777,216

exam watch

You should be very familiar with subnet masks for a given address and the number of networks that a subnet mask creates, as well as the number of host addresses for each network.

Subnet Masks for Class B Networks

Table 7-4 shows valid subnet masks for Class B networks.

Subnet Masks for Class C Networks

Table 7-5 shows valid subnet masks for Class C networks.

TABLE 7-4

Valid Subnet Masks for Class B Networks

Subnet Mask	Networking Bits	Number of Subnets	Number of Hosts per Subnet
255.255.255.252	/30	32,768	2
255.255.255.248	/29	8192	6
255.255.255.240	/28	4096	14
255.255.255.224	/27	2048	30
255.255.255.192	/26	1024	62
255.255.255.128	/25	512	126
255.255.255.0	/24	256	254
255.255.254.0	/23	128	510
255.255.252.0	/22	64	1022
255.255.248.0	/21	32	2046
255.255.240.0	/20	16	4094
255.255.224.0	/19	8	8190
255.255.192.0	/18	4	16,382
255.255.128.0	/17	2	32,764
255.255.0.0	/16	1	65,534

As you can see from Tables 7-3, 7-4, and 7-5, you can't choose just any subnet mask and apply it to any class of addresses: Some masks are valid for some classes, but not valid for others. For instance, 255.255.0.0 is a valid mask for Class A and B networks, but it is an *invalid* mask for Class C networks.

TABLE 7-5

Valid Subnet Masks for Class C Networks

Subnet Mask	Networking Bits	Number of Subnets	Number of Hosts per Subnet
255.255.255.252	/30	64	2
255.255.255.248	/29	32	6
255.255.255.240	/28	16	14
255.255.255.224	/27	8	30
255.255.255.192	/26	4	62
255.255.255.128	/25	2	126
255.255.255.0	/24	1	254

on the job

Starting in IOS 12.0, Cisco routers and switches automatically support the use of subnet 0 (the first and last subnets). Prior to this, the use of subnet 0 was, by default, disabled, but you could enable it to use on a router or switch.

CERTIFICATION OBJECTIVE 5.03

IP Address Planning

When it comes to addressing, dealing with protocols such as AppleTalk, IPX, and XNS is easy: each has a distinct network and host component. With these protocols, there is no such thing as a subnet mask that can change the boundary between network and host numbers. When I started out with TCP/IP, one of the most difficult tasks I faced in my networking career was tackling and understanding how to handle subnetting and IP addressing. To make matters worse, IP addressing has its roots in binary mathematics, since this is how computing devices deal with numbers. And considering that I have a degree in mathematics, and that I had trouble with IP addressing, imagine how strange IP addressing must be to the layperson!

Through my years of experience dealing with TCP/IP and teaching Cisco-related courses, however, I've developed a simplified six-step approach to help students plan for their IP addressing needs in their networks:

1. Determine network and host requirements.
2. Satisfy host and network requirements.
3. Determine the subnet mask.
4. Determine the network addresses.
5. Determine the directed broadcast addresses for your networks.
6. Determine the host addresses for your networks.

The following sections will cover the six steps in depth.

exam watch

Be very familiar with these six steps and how to plan out IP addressing. Many questions on the exam will have you perform this process—perhaps multiple times for a single question!

Step 1: Determine Network and Host Requirements

In this step, you need to do two things:

- Determine the number of hosts that do, or will, exist on the largest segment in your network.
- Determine the maximum number of segments that you have in your network—this will tell you how many networks, or subnets, you'll need.

If you are dealing with an existing network, you have a lot of analysis ahead of you. And, of course, if you're taking the exam, Cisco will fortunately supply this information to you. You'll need to perform the above two tasks, counting hosts on each segment and the number of segments that you have. Remember that when you are counting hosts, each device with a connection to the segment needs to be counted—this includes PCs, servers, routers, switches, printers, and other devices. Remember that a segment could be used in a logical sense, like all the ports off a switch, or a VLAN, as discussed in Chapter 13. You might even want to leave some room for growth by taking your final numbers and adding to them.

exam watch

All devices on a segment—router, switches, PCs, servers, and so on—need a host address from a network or subnet number.

To assist with the remaining five steps, I'll create an imaginary network. This network has 14 segments and the largest segment has 14 devices on it. You've been assigned a single Class C network number (192.168.1.0) to complete the task. Now you're ready to proceed to step 2.

Step 2: Satisfy Host and Network Requirements

In the second step, you'll use three formulas:

- 2^S >= number of networks you need (S represents subnet bits)
- $2^H - 2$ >= number of hosts on your largest segment (H represents host bits)
- $S + H$ <= total number of host bits you have for a class of address

In the first step, you need to figure out how many bits you need to steal from the host bits to create your subnets. In the second step, you need to figure out how many host bits you need to accommodate your host requirements. And last, you need to make sure that when you add up the bits that you stole for subnets and the bits that you need for your hosts, you don't exceed the original number of host bits that you started out with, based on the Class A, B, or C network.

As an example, if you had a Class C network and were subnetting it and needed 5 bits for subnets and 4 bits for hosts, this would total 9 bits. Unfortunately, Class C networks have only 8 host bits to begin with, so this wouldn't work. In this situation, you would need either a Class B network or two Class C networks. As another example, if you had the same Class C network and were subnetting it, and you needed 3 bits for subnets and 4 bits for host addresses, this would total 7 bits. In this situation, the Class C network has 8 bits, and you need only 7. This gives you some flexibility—you could use the extra bit either to create more subnets or have subnets with more hosts.

Let's go back to the original example of 192.168.1.0, where you need 14 subnets with a maximum of 14 hosts on each:

1. $2^S >= 14$ subnets; in this example, $S = 4$, which would result in 16 subnets.
2. $2^H - 2 >= 14$ hosts; in this example, $H = 4$, which would result in 14 hosts.
3. $S + H <= 8$ (Class C network); in this example 4 + 4 is less than or equal to 8.

Let's break this down step-by-step.

In the first step, you need to find a power of 2 that will provide a number that is either greater than or equal to the number of subnets that you need. In our example, the power of 2 needs to be 4: $2^4 >= 16$. This meets your subnet requirements, since you need only 14 subnets (there are only 14 segments). If subnet 0 were not available, then you would need 5 subnet bits instead of 4, since you would lose the first and last subnets; however, I'm assuming that subnet 0 is available in this example.

In the second step, you need to figure out your host bits by using the formula $2^H - 2 >= 14$ required hosts, where H is the necessary number of host bits. In this example, $2^4 - 2 = 14$, so you need 4 host bits to get your required 14 hosts. Remember that you need to subtract 2 since the first address in the network is the network address and the last is the directed broadcast address.

And third, since you are dealing with a Class C network, you have only 8 original host bits. You need to make sure that the total of your subnetting and host bits does not exceed this original value. In your case, 4 + 4 = 8, so you're okay. If the number of bits totaled more than 8, you would need two Class C networks or a Class B network. If the number of bits were less than 8, you could allocate the extra bit or bits to create more subnets and/or hosts. Remember that if you are ever in a situation where you have extra bits to deal with, you need to examine your network closely and figure out, based on future growth, whether you should create more subnets or allow for more hosts on a subnet.

Step 3: Determine the Subnet Mask

Now that the hardest part is over, the remaining four tasks are easy. At this point, you know the number of subnet bits you need. However, when dealing with networking and subnet masks, a subnet mask's network portion contains both network *and* subnet bits. Remember the default number of networking bits for a class address: A is 8, B is 16, and C is 24.

Given this, you can just add the class address bits to the subnet bits, and this gives you the total number of *networking* bits. In this example, 24 + 4 = 28. To make the remaining three steps easier, you can convert the number of bits of the subnet mask to a dotted-decimal mask. Tables 7-3, 7-4, and 7-5 show the lists of subnet masks if you need help. However, this process is not too difficult. First, remember that a subnet mask, just like an IP address, is represented in a dotted-decimal format, with 8 bits in each octet. That means, for a Class C mask, the first 24 bits are set to 1. In other words, the mask at least begins with 255.255.255. Your job is to figure out the mask in the last octet. Remember that the four highest bits are for subnetting, so just add up these decimal values: 128 + 64 + 32 + 16 = 240.

You can also use a shortcut (which I always use). Recall from the example that the number of host bits that are used are the four lower order bits. Add up these values: 1 + 2 + 4 + 8 = 15. The largest number represented by a byte is 255. Since you're not using these bits, just subtract this value from 255, which will give you the mask value in this byte of 255 – 15 = 240. I find it easier to add up the small values and subtract them from 255 than to add up the larger bit-decimal values. Eventually, you won't have to do this mathematical trick as you become accustomed to performing IP addressing and dealing with subnetting. Going back to our example, our subnet mask for network 192.168.1.0 is *255.255.255.240*, or 192.168.1.0/28.

exam watch

Remember how to convert a binary subnet mask value to a dotted-decimal format using the shortcut: add up the host bit values in decimal and subtract them from 255.

Step 4: Determine the Network Addresses

In step 4, you need to figure out the networks that you created with your new subnet mask. Since IP addressing is done in binary, network addresses will always increment in a multiple of something. You can use this to your advantage when figuring out what your network numbers are for your Class C network. Remember that the network number has all the host bits set to 0s.

Actually, you already know what this multiplier is: you figured this out in the second part of step 2, using the $2^H - 2 = 14$ formula. The *14* is the number of valid host values for a subnet; however, this is *not* the total number of addresses for the subnet. The subnet also has a network and broadcast address, which is the reason the formula subtracts 2 (since you can't use these addresses for host devices). Therefore, in this example, each network has a total of *16* addresses and increments by 16 from subnet-to-subnet.

You can use another method of verifying your multiplying value. In a byte, you can have numbers ranging from 0 to 255, resulting in a total of 256 numbers. For this verification, take the subnet mask decimal value in the interesting octet and subtract it from 256. The interesting octet is the octet that contains the network and host boundary. In our case, this is the fourth octet. Therefore, using this trick, 256 – 240 = 16. When you compare this number to the number in the last paragraph, you can be assured that you have done your math correctly.

Now that you have figured out the multiplier, write down the very first network, and then start adding *16* to the interesting octet. Table 7-6 lists the subnet numbers for 192.168.1.0. In this table, notice something interesting concerning the last subnet: 192.168.1.240. The network number in the last octet matches the interesting octet in your subnet mask (240). This will *always* be true when you perform subnetting.

Another important item needs to be mentioned about subnetting. In the original RFC for subnetting, you were not allowed to use the first and last subnet. For instance, in our example, you would not be able to use 192.168.1.0/28 and 192.168.1.240/28. However, today, assuming that your TCP/IP protocol stack supports subnet 0 (this refers to these two subnets—first and last), you can use 192.168.1.0/28 and 192.168.1.240/28, and this has been true since the mid-1990s. You need to make sure, though, that each device on the segment that will have one of these subnets supports this function. In today's age, this shouldn't be an issue for computers and networking devices.

exam watch

Remember that the exam might not allow you to use subnet 0. Therefore, in step 1, you might need to subtract 2 from the total valid number of networks to come up with a valid value. In this chapter, I'm assuming that subnet 0 is valid in all of the examples.

TABLE 7-6

Network Numbers for 192.168.1.0

192.168.1.0	192.168.1.64	192.168.1.128	192.168.1.192
192.168.1.16	192.168.1.80	192.168.1.144	192.168.1.208
192.168.1.32	192.168.1.96	192.168.1.160	192.168.1.224
192.168.1.48	192.168.1.112	192.168.1.176	192.168.1.240

Step 5: Determine the Directed Broadcast Addresses

After figuring out all of your subnets, you next need to determine the directed broadcast address for each subnet. This is very simple. The directed broadcast of a subnet is *one number less* than the next network number. Also, the broadcast address has all of its hosts bits (in the subnet) set to binary 1s. Table 7-7 shows our network numbers and directed broadcast addresses. For the last table entry, the directed broadcast address will be the highest possible value in a byte: 255.

exam watch

As a shortcut, remember that the directed broadcast address is one number less than the network address of the next subnet number.

TABLE 7-7 Network and Directed Broadcast Addresses for 192.168.1.0/28

Network Address	Mathematics	Directed Broadcast Address
192.168.1.0	16 – 1	192.168.1.15
192.168.1.16	32 – 1	192.168.1.31
192.168.1.32	48 – 1	192.168.1.47
192.168.1.48	64 – 1	192.168.1.63
192.168.1.64	80 – 1	192.168.1.79
192.168.1.80	96 – 1	192.168.1.95
192.168.1.96	112 – 1	192.168.1.111
192.168.1.112	128 – 1	192.168.1.127
192.168.1.128	144 – 1	192.168.1.143
192.168.1.144	160 – 1	192.168.1.159
192.168.1.160	176 – 1	192.168.1.175
192.168.1.176	192 – 1	192.168.1.191
192.168.1.192	208 – 1	192.168.1.207
192.168.1.208	224 – 1	192.168.1.223
192.168.1.224	240 – 1	192.168.1.239
192.168.1.240		192.168.1.255

Step 6: Determine the Host Addresses

Step 6 is the easiest step. Recall that any address between the network and directed broadcast address is a host address for a given network. You can then complete the rest of your addressing for 192.168.1.0, as shown in Table 7-8. If you look at the first subnet in this table, 192.168.1.0, you'll see that it has a total of 14 host addresses, which you can see using our formula $2^H - 2$: $2^4 - 2 = 14$ hosts.

on the job

For the CCNA exam, you will definitely need to understand how to figure IP addressing, and quickly. Of course, on the job, you can cheat and use an IP subnet calculator. One of my favorites is from a company called Boson Software, which offers a free download of its subnet calculator (www.boson.com). Boson's subnet calculator will even do route summarization, which is discussed in the next chapter.

TABLE 7-8

Addressing for 192.168.1.0/28

Network Number	Host Address	Directed Broadcast Address
192.168.1.0	192.168.1.1–192.168.1.14	192.168.1.15
192.168.1.16	192.168.1.17–192.168.1.30	192.168.1.31
192.168.1.32	192.168.1.33–192.168.1.46	192.168.1.47
192.168.1.48	192.168.1.49–192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65–192.168.1.78	192.168.1.79
192.168.1.80	192.168.1.81–192.168.1.94	192.168.1.95
192.168.1.96	192.168.1.97–192.168.1.110	192.168.1.111
192.168.1.112	192.168.1.113–192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129–192.168.1.142	192.168.1.143
192.168.1.144	192.168.1.145–192.168.1.158	192.168.1.159
192.168.1.160	192.168.1.161–192.168.1.174	192.168.1.175
192.168.1.176	192.168.1.177–192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193–192.168.1.206	192.168.1.207
192.168.1.208	192.168.1.209–192.168.1.222	192.168.1.123
192.168.1.224	192.168.1.225–192.168.1.238	192.168.1.239
192.168.1.240	192.168.1.241–192.168.1.254	192.168.1.255

EXERCISE 7-1

ON THE CD

Planning IP Addressing Exercise

This exercise will help reinforce the concepts you've learned in this chapter, including the six steps that you should use to come up with an appropriate subnet mask value and network, directed broadcast, and host addresses.

1. You are given a Class C network (192.168.1.0) and you have four segments in your network, where the largest segment has 50 hosts. What subnet mask should you use and what is the layout of your addresses?

   Performing the six steps, the subnet mask is 255.255.255.192 (/26), giving you four network numbers: 192.168.1.0, 192.168.1.64, 192.168.1.128, and 192.168.1.192. Each of these four networks has a total of 64 addresses, of which 62 can be used for host devices.
2. You are given a Class B network (172.16.0.0) and you have 490 segments in your network, where the largest segment needs 112 host addresses. What subnet mask should you use and what is the layout of your addresses?

   Performing the six steps, the subnet mask is 255.255.255.128 (/25), giving you 512 network numbers: 172.16.0.0, 172.16.0.128, 172.16.1.0, 172.16.1.128, 172.16.2.0, 172.16.2.128, and so on and so forth. Each of these 512 subnets has 128 addresses, of which 126 can be used to assign addressing information to host devices.
3. You are given a Class A network (10.0.0.0) and you have 9000 segments in your network, where the largest segment needs 560 host addresses. What subnet mask should you use and what is the layout of your addresses?

   Performing the six steps, the subnet mask is 255.255.252.0 (/22), giving you 16,384 network numbers: 10.0.0.0, 10.0.4.0, 10.0.8.0, 10.0.12.0, 10.0.16.0, 10.0.20.0, 10.0.24.0, and so on and so forth. Each of these 16,384 subnets has 1024 addresses, of which 1022 can be used to assign addressing information to host devices.

Now you should be more comfortable with planning IP addressing. In the next section, you will see how to determine whether an IP address is a network, directed broadcast, or host address.

exam watch

Make sure that you practice, practice, and do more practice on exercises like those presented here when preparing for your exam. This is very important. Use a subnet calculator to check your results. Many are available on the Internet for free; Boson's calculator is one example. On the exam, you might have to perform many subnet calculations to answer a single question, so time is your enemy in these situations: practice until you can perform the subnetting process quickly! Many people fail the CCNA exam because they run out of time!

CERTIFICATION OBJECTIVE 7.04

Determining IP Address Components

For purposes of the CCNA exam, you might not be given an assignment like the one described in the preceding section. However, you will have to know how to figure out how many host addresses are in a particular subnet, how many subnets you can create with a particular mask, and, given a specific IP address, whether it is a network, host, or directed broadcast address. The last section described how to plan IP addressing. This section teaches you to use a few tools to figure out these questions—more specifically, given a certain address, what type of address it is: network, host, or directed broadcast.

Recall from the last section that three types of addresses are used for each network: network, directed broadcast, and host addresses. The trick to figuring this out goes back to step 4. You need to figure out the number by which networks are incrementing. For exam purposes, you may be given an IP address and a subnet mask. Convert the decimal subnet mask to the number of bits in the mask. In the previous example, for instance, 255.255.255.240 is a 28-bit mask. Take this number and subtract it from 32. In our example, this gives you 4 bits. Since the first 28 bits are network numbers, the last 4 bits are host addresses.

Remember that every subnet has the same number of addresses. So all you need to do is raise this value to the power of 2 to figure out how many addresses are in a network, and therefore you know by how much each network number is incrementing.

In our example, 2^4 gives you a total of 16 addresses in the subnet, including the network, host, and directed broadcast addresses. Based on this information, it is easy to figure out what type of address the exam is asking about.

As you will learn, subnetting is not a difficult task, but it does take *a lot of practice*. I've developed six steps to help you out, which are covered in the following sections.

Six-Step Approach for Determining IP Address Components

When you are given a particular address and subnet mask, and asked whether the address is a network, host, or directed broadcast address, you should use the following six steps:

1. You need an IP address and a subnet mask (this is the easy part).
2. Examine the subnet mask and find the interesting octet. The interesting octet in the mask is the one in which the network and host boundary are found. This includes the following mask values in an octet: 0, 128, 192, 224, 240, 248, 252, and 254. It does *not* include 255—an octet with a mask value of 255 (all 8 bits are 1s) indicates that this octet is part of the network number. Only when an octet contains one or more binary 0s does it have a host component.
3. Subtract the interesting octet in the subnet mask from 256. This will give you the increment by which network numbers are increasing in the interesting octet.
4. On a piece of paper, start writing down the network numbers, starting with the first subnet (0), and working your way up to a network number that is higher than the address in question.
5. After you have written down the network numbers, beside each of these, write down their corresponding broadcast addresses. Remember that the broadcast address is one number less than the *next* network number. You don't have to do this with every network number—just the networks near the network number in question.
6. Between the network and broadcast addresses, write down the host addresses. Host addresses are any number between the network and directed broadcast addresses.

> **exam watch**
>
> ***Remember these six steps when trying to determine whether an IP address is a network, host, or directed broadcast number.***

Based on these six steps, you should be able to figure out whether your address is a host, network, or broadcast address. Note that these six steps are somewhat similar to the six steps used in the "IP Address Planning" section. However, the steps in this section are for CCNA test purposes and the steps in the previous section are for design purposes.

Example #1 for Determining IP Address Components

To help you out with the six steps, take a look at an example as an illustration. In step 1, you have an IP address and subnet mask. Assume that this is 192.168.1.37 255.255.255.224 (or 192.168.1.37/27). This is a Class C network. Remember this shortcut: if it's an odd address, it's either a directed broadcast or host address. Therefore, you know this address is not a network address.

> **exam watch**
>
> ***As a shortcut, remember that a network number is always an even number, a broadcast is always an odd number, and a host address can be either. With this knowledge, you can typically eliminate some answers when looking for the right one or ones.***

In step 2, you need to find the interesting octet in the subnet mask. This is the octet where the boundary exists between network and host bits. In this example, this is the fourth octet: *224*. In step 3, you need to find the increment by which network numbers are increasing. To perform this step, subtract the interesting octet from 256: 256 – 224 = 32. Therefore, there are 32 addresses in each network, and each network is incrementing by 32 in the interesting octet (fourth octet).

> **exam watch**
>
> ***Remember the shortcut of figuring out the multiples that network numbers are incrementing by in the interesting octet: 256 – subnet mask value = increment value.***

In step 4, write down the network numbers starting with the first subnet and work your way up. Here is the list of network numbers for our example: 192.168.1.*0*, 192.168.1.*32*, 192.168.1.*64*, 192.168.1.*96*, 192.168.1.*128*, 192.168.1.*160*, 192.168.1.*192*, and 192.168.1.*224*. In this example, there are eight subnets. Mathematically, this makes sense. There are 32 addresses per subnet, with a total of 256 addresses (0–255) in a Class C network. 256 ÷ 32 = 8! Remember that the interesting octet in the subnet mask will be the subnet number in the last subnet of the IP class address.

In step 5, list the directed broadcast address beside each network number. And in step 6, list the host addresses for each network. Remember that the broadcast address for a network is one number less than the next network number and that the host addresses are any IP addresses between the network and directed broadcast addresses. Table 7-9 shows the completion of steps 5 and 6.

Considering Table 7-9, the host address of 192.168.1.37 is a *host* address, since it falls in the rage of host addresses for subnet 192.168.1.32/27.

exam watch

When you are taking the CCNA exam, don't build the entire table. Instead, list the network numbers until you have a network number greater than the address in the question. Once this is done, for the last three network numbers, list the directed broadcast and host addresses, and then you'll know the answer to the exam question. In the above example, these networks would be 192.168.1.0, 192.168.32.0 and 192.168.64.0.

TABLE 7-9

Network, Broadcast, Directed, and Host Addresses of 192.168.1.0/27

Network Address	Host Address	Directed Broadcast Address
192.168.1.0	192.168.1.1–192.168.1.30	192.168.1.31
192.168.1.32	192.168.1.33–192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65–192.168.1.94	192.168.1.95
192.168.1.96	192.168.1.97–192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129–192.168.1.158	192.168.1.159
192.168.1.160	192.168.1.161–192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193–192.168.1.222	192.168.1.223
192.168.1.224	192.168.1.225–192.168.1.254	192.168.1.255

Example #2 for Determining IP Address Components

Let's look at another example to help clarify the six steps. For step 1, you are given the following address and subnet mask: 192.168.1.132 255.255.255.192 (/26), which is a Class C address. Remember the shortcut from earlier: if the last octet is even, it's either a network or host address. Therefore, you know it's not a directed broadcast address.

In the second step, you need to find the interesting octet in the subnet mask. This is the last octet. For a Class C network, this will *always* be the last octet. The value in this mask is *192*, indicating that the first two high-order bits in the octet are part of the network component and the last six low-order bits are the host component. In step 3, you need to determine by what number the network addresses are increasing. To do this step, subtract the value in the subnet mask's interesting octet from 256: 256–192 = 64. Therefore, network addresses are incrementing by 64 numbers and each network contains 64 addresses: a network address, a directed broadcast address, and 62 host addresses. Remember that since the interesting octet is in the fourth octet, the network addresses are increasing by 64 in the *interesting* (fourth) octet.

In step 4, write down the network numbers. In our example, this gives you four networks: 192.168.1.*0*, 192.168.1.*64*, 192.168.1.*128*, and 192.168.1.*192*. In the interesting octet, 2 bits are used for networking and 6 bits for host addresses. With 2 bits of networking, this gives you four networks (2^2 = 4), and with 6 bits of host addresses and 64 addresses in a network, it's 2^6 = 64.

The address in question, 192.168.1.132, is between two networks: 192.168.1.128 and 192.168.1.192. This means that you should have to perform steps 5 and 6 only on these two networks, and possibly the network before it. However, go ahead and complete steps 5 and 6 for all of the networks since this is good practice. Remember that the directed broadcast address for a network is one number less than the next network number and that the addresses between the network and directed broadcast addresses are host addresses. Table 7-10 shows the addressing for the Class C address. Our address, 192.168.1.132, is a *host* address based on this table, where its network number is 192.168.1.128 and its directed broadcast is 192.168.1.191.

TABLE 7-10

Network, Broadcast, Directed, and Host Addresses of 192.168.1.0/26

Network Address	Host Address	Directed Broadcast Address
192.168.1.0	192.168.1.1–192.168.1.62	192.168.1.63
192.168.1.64	192.168.1.65–192.168.1.126	192.168.1.127
192.168.1.128	192.168.1.129–192.168.1.190	192.168.1.191
192.168.1.192	192.168.1.193–192.168.1.253	192.168.1.254

Example #3 for Determining IP Address Components

The first two examples were fairly simple, since the addresses were from a Class C network. In this example, let's complicate matters by using a Class B network. In step 1, the address assigned is 172.16.5.0 255.255.254.0, which can also be represented as 172.16.5.0/23. This is an excellent example of an address that most test-takers would incorrectly identify on a test. Right now, try and guess what type of address this is (network, directed broadcast, or host) and then work through it step-by-step to come up with an answer. However, if you remember the shortcut from earlier, since the host portion of the address is an even number, you at least know that the address is not a directed broadcast, narrowing your choice down to two possibilities.

In step 2, you need to find the interesting octet—where the network and host boundary resides. In this case, it happens to be the *third* octet (254) of the subnet mask. It is important to point out that *all* of the *fourth* octet represents host addresses. In step 3, you need to find the increment by which network numbers are increasing: 256 – 254 = 2. *Network numbers are incrementing by 2 in the third octet*. This last sentence is very important. Remember that the entire fourth octet is the host component since the subnet mask value in this position is set to 0 (all 8 bits are 0).

In step 4, you need to write down your network numbers, starting with the first subnet, and work your way up until you go past the IP address in question: 172.16.0.0, 172.16.2.0, 172.16.4.0, 172.16.6.0, 172.16.8.0, and so on and so forth. Remember that with a Class B address, there are 16 bits in the host component. With this subnet mask, you're using 7 bits for subnets and 9 bits for hosts. Therefore, with 7 bits for subnets, you have a total of 128 subnets, where each subnet has 512 total addresses. Each network really has 510 *host* addresses, where the first and last addresses are used for the network and directed broadcast addresses, respectively. Looking at the address, 172.16.5.0, you can tell that it at least is *not* a network address.

Go ahead and do steps 5 and 6, listing the directed broadcast addresses and host addresses for these subnets, as shown in Table 7-11. Looking at this table, you can see that 172.16.5.0 is a *host* address! Even 172.16.0.255 is a host address! This example illustrates that you should *never* make assumptions about what type an address is without considering the subnet mask. Always remember that the subnet mask puts a context on the IP address and determines its type: network, directed broadcast, or host address.

For the CCNA exam, I would expect a trick question like this. In real life, I would typically not use addresses like 172.16.5.0 or 172.16.0.255 because this would *confuse* many network administrators. I've actually had to argue with people over the validity of these kinds of addresses as host addresses in network planning sessions!

TABLE 7-11 Network, Broadcast, Directed, and Host Addresses of 172.16.0.0/23

Network Address	Host Address	Directed Broadcast Address
172.16.0.0	172.16.0.1–172.16.1.254	172.16.1.255
172.16.2.0	172.16.2.1–172.16.3.254	172.16.3.255
172.16.4.0	172.16.4.1–172.16.5.254	172.16.5.255
172.16.6.0	172.16.6.1–172.16.7.254	172.16.7.255
172.16.8.0	172.16.8.1–172.16.9.254	172.16.9.255

I've learned, though, that it's pretty hard to teach an old dog new tricks, so instead of wasting my time arguing or explaining the address validity, I just don't use them. For test purposes, though, they *are* valid host addresses!

exam watch

Make sure that you practice, practice, and do more practice on exercises like these when preparing for your exam. You might see something tricky on the exam like the last example. You should be able to do these exercises fairly quickly, spending no more than one minute for each address you're given.

EXERCISE 7-2

ON THE CD

Determining Network, Directed Broadcast, and Host Components

These last few sections deal with how to determine the type of address: network, directed broadcast, or host address. The following exercises will help you practice your IP addressing skills.

1. You are given the following address: 192.168.1.63/255.255.255.248. What type of address is this—network, directed broadcast, or host?

   The interesting octet is the *fourth*: 248. Subtract this from 256: 256 – 248 = 8. Network numbers are incrementing by 8: 192.168.1.*0*, 192.168.1.*8*, 192.168.1.*16*, 192.168.1.*24*, 192.168.1.*32*, 192.168.1.*40*, 192.168.1.*48*, 192.168.1.*56*, 192.168.1.*64*, and so on and so forth. After writing down the directed broadcast addresses, you'll see that the network 192.168.1.56 has a directed broadcast address of 192.168.1.63 and host address of 57–62. Therefore, this is a broadcast address.

2. You are given the following address: 172.16.4.255/255.255.252.0. What type of address is this—network, directed broadcast, or host?

   The interesting octet is the *third*: 252. Subtract this from 256: 256 – 252 = 4. Network numbers are incrementing by 4 in the third octet: 172.16.0.0, 172.16.*4*.0, 172.16.*8*.0, 172.16.*12*.0, and so on and so forth. After writing down the directed broadcast addresses, you'll see that the network 172.16.4.0 has a directed broadcast address of 172.16.7.255 and host addresses of 172.16.4.1–172.16.7.254. Therefore, this is a host address.

INSIDE THE EXAM

IP Addressing Review

I cannot stress enough how important it is for you to know IP addressing inside and out for the CCNA exam—whether you're taking the two-exam or one-exam approach. Out of all of the topics in this book, those covered in this chapter are probably the most important. Therefore, be familiar with the classes of addresses, including the default bit lengths and beginning bit values for each address class. Also understand the three kinds of addresses in a network: network address, host addresses, and directed broadcast address. Each network loses two addresses for host purposes: the first and last.

Probably the main reason that most test takers fail any of the three CCNA exams is that they run out of time: they know the material, but when it comes to IP addressing and subnetting, they're taking too much time to answer the questions. Therefore, you need to read this chapter a few times and practice, and practice exercises like those found in the "IP Address Planning" and "Determining IP Address Components" sections until you can do these things in your sleep.

Subnetting

You need to be highly proficient in subnetting. Be able to pick out invalid masks and be able to determine the number of networks and hosts available based on a particular subnet mask value (whether it's displayed in a dotted-decimal format or by the number of networking bits). 255.255.255.252 is a good mask for point-to-point links, since it offers two hosts for the subnet. Typically, when given a subnet question, the exam will tell you whether or not subnet 0 is valid—however, in those questions where it isn't stated, you'll need to look close at the answers to determine how to answer the question, which to me is unfair.

(*continued*)

IP Address Planning

Don't be surprised to see a simulation question on the exam, for which you need to configure one or more routers as well as design an appropriate IP addressing scheme. The question will tell you how many devices need to be on each segment, and you can easily count the number of segments in the network diagram. The question will also tell you the network number—you need to come up with a subnet mask that will work for the question as well as do the subnetting, logically assign the subnets to each of the segments, and give the router interfaces a host address from each of the subnets. Therefore, make sure you practice and practice the six steps described in this section until you have subnetting down pat.

Determining IP Address Components

You might see some questions on the exam for which you have to choose the network addresses, host addresses, or directed broadcast addresses from a list of addresses. This means you'll have to figure out the address components multiple times to choose the correct answer or answers. Remember the trick to eliminate some of the answers right away: network addresses are always even numbered, directed broadcast addresses are always odd numbered, and host addresses can be either.

CERTIFICATION SUMMARY

IP addresses are 32-bits in length and are broken up into 4 bytes, with a period between the bytes. This format is referred to as dotted-decimal. There are five classes of IP addresses: A (1–126), B (128–191), C (192–223), D (224–239), and E (240–254). Class A addresses have 1 network byte and 3 host bytes. Class B addresses have 2 network and 2 host bytes. Class C addresses have 3 network bytes and 1 host byte. Private IP addresses include networks 10.0.0.0/8, 172.16.0.0/16–172.31.0.0/16, and 192.168.0.0/24–192.168.255.0/24.

IP addresses have three components: network, host, and broadcast. The first number in a network is the network or wire number. The very last address is the broadcast address of the network. Any addresses between the network and broadcast addresses are host addresses. What differentiates network, host, and broadcast addresses is the context the subnet mask places on the address. The subnet mask is used to mark the boundary between the network and host bits.

✓ TWO-MINUTE DRILL

IP Addressing Review

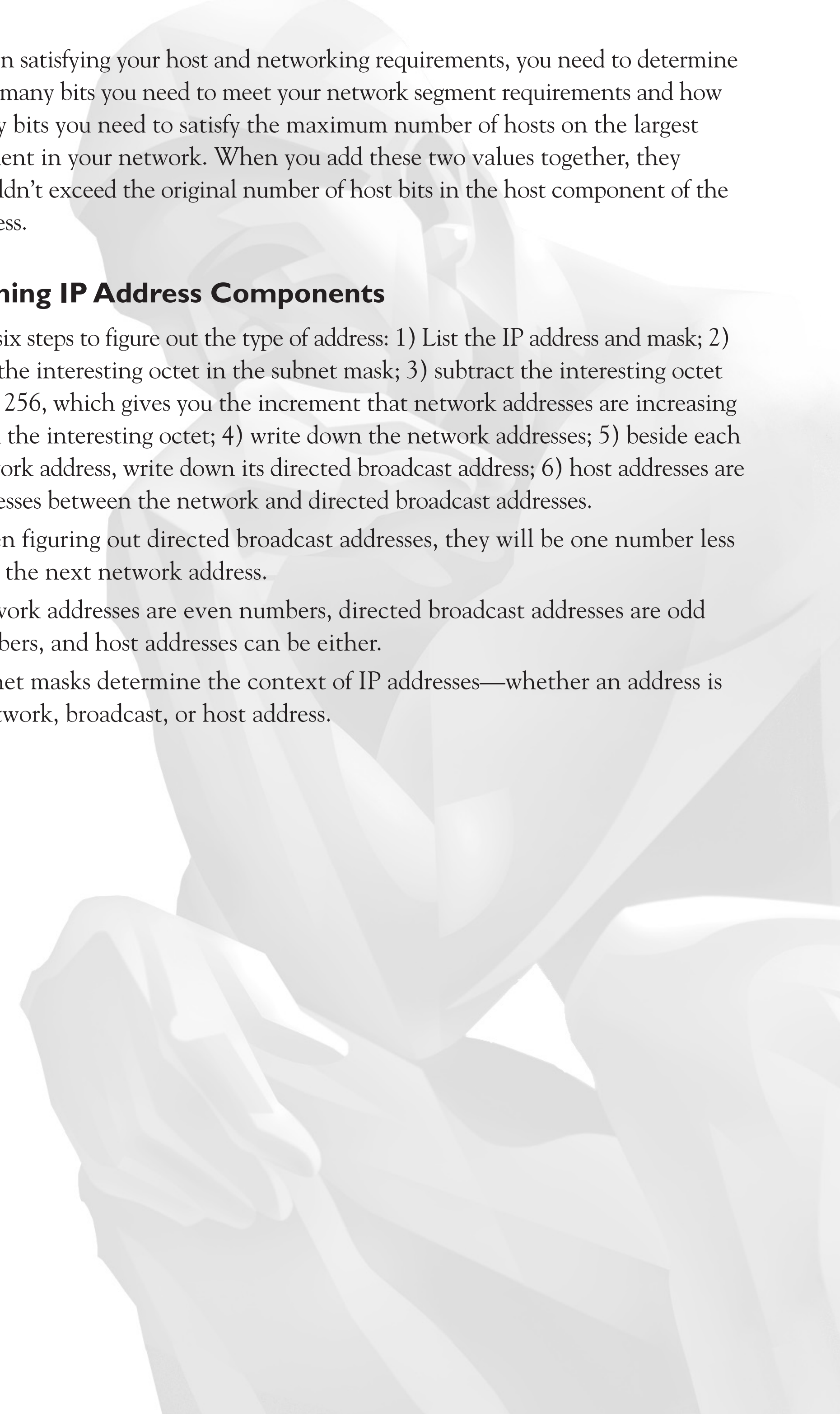
- ❑ IP addresses are 32 bits in length and are broken into 4 bytes (8 bits) with a period between the bytes. This format is called dotted-decimal.
- ❑ IP addresses are broken into five classes: A (1–126), B (128–191), C (192–223), D (224–239), and E (240–254). IP addresses are broken into two components: network and host. With Class A addresses, the first byte is a network number, Class B, the first 2 bytes, and Class C, the first 3 bytes.
- ❑ The first few bits in the first octet identity the class of address. Class A addresses begin with *0*, Class B with *10*, Class C with *110*, Class D with *1110*, and Class E with *11110*.
- ❑ Each network has three components to its address: network, directed broadcast, and host. The first number in the network is the network address, the last is the directed broadcast address, and any addresses between these two are host addresses.

Subnetting

- ❑ Subnetting allows you to break up and use an addressing space more efficiently. Basically, subnetting steals the higher-order bit or bits from the host component and uses these bits to create more subnets with a smaller number of host addresses in each of these subnets.
- ❑ Subnet masks are 32 bits long and are typically represented in dotted-decimal (such as 255.255.255.0) or the number of networking bits (such as /24). The networking bits in a mask must be contiguous and the host bits in the subnet mask must be contiguous. 255.0.255.0 is an invalid mask.

IP Address Planning

- ❑ Six steps are required for designing a network with IP addresses: 1) Figure out your network and host requirements; 2) satisfy host and network requirements; 3) figure out the subnet mask; 4) figure out the network addresses; 5) figure out the directed broadcast addresses; 6) figure out the host addresses.



- ❑ When satisfying your host and networking requirements, you need to determine how many bits you need to meet your network segment requirements and how many bits you need to satisfy the maximum number of hosts on the largest segment in your network. When you add these two values together, they shouldn't exceed the original number of host bits in the host component of the address.

Determining IP Address Components

- ❑ Use six steps to figure out the type of address: 1) List the IP address and mask; 2) find the interesting octet in the subnet mask; 3) subtract the interesting octet from 256, which gives you the increment that network addresses are increasing by in the interesting octet; 4) write down the network addresses; 5) beside each network address, write down its directed broadcast address; 6) host addresses are addresses between the network and directed broadcast addresses.
- ❑ When figuring out directed broadcast addresses, they will be one number less than the next network address.
- ❑ Network addresses are even numbers, directed broadcast addresses are odd numbers, and host addresses can be either.
- ❑ Subnet masks determine the context of IP addresses—whether an address is a network, broadcast, or host address.

SELF TEST

The following Self Test questions will help you measure your understanding of the material presented in this chapter. Read all the choices carefully, as there may be more than one correct answer. Choose all correct answers for each question.

IP Addressing Review

1. A Class B address has __________ host bits.

   A. 8

   B. 16

   C. 20

   D. 24

2. 192.168.256.135 is a Class __________ address.

   A. A

   B. B

   C. C

   D. None of the above

Subnetting

3. Which of the following is a valid subnet mask value?

   A. 255.0.255.255

   B. 0.0.0.255

   C. 255.255.254.0

   D. 255.255.255.256

4. The function of a __________ is to differentiate between the network address, the host addresses, and the directed broadcast address.

IP Address Planning

5. You are given a Class C network with 25 bits for networking. How many subnets do you have?

   A. 1

   B. 2

   C. 3

   D. 4

6. You are given a Class C network with a subnet mask of 255.255.255.248. How many host addresses are there on each subnet?

A. 4

B. 6

C. 8

D. 14

7. You are given a Class B network with a subnet mask of 255.255.255.192. How many host addresses are there on each subnet?

A. 30

B. 62

C. 126

D. 254

Determining IP Address Components

8. You are given the following addressing information: 192.168.37.192/25. What type of address is this?

A. Network

B. Directed broadcast

C. Host

9. You are given the following addressing information: 172.17.16.255/23. What type of address is this?

A. Network

B. Directed broadcast

C. Host

10. You are given the following addressing information: 10.0.8.0/22. What type of address is this?

A. Network

B. Directed broadcast

C. Host

SELF TEST ANSWERS

IP Addressing Review

1. ☑ **B.** Class B addresses have 16 host bits and 16 networking bits.
☒ **A** is true for Class C networks. **C** is true only for subnetted Class A and B networks. **D** is for Class C networks and subnetted Class A and B networks.

2. ☑ **D.** It's impossible to represent 256 in a byte (see the third octet)—the values range from 0 to 255.
☒ **A**, **B**, and **C** are incorrect.

Subnetting

3. ☑ **C.** 255.255.254.0 is a valid subnet mask—the 1s and 0s must be contiguous.
☒ **A** has noncontiguous 1s. **B** is an inverted mask, with the network and host bits reversed. **D** has an invalid mask value in the fourth octet: 256.

4. ☑ The function of a *subnet mask* is to differentiate between the network address, the host addresses, and the directed broadcast address.

IP Address Planning

5. ☑ **B.** Class C networks have 24 bits—this example steals 1 bit. 2 raised to the power of 1 equals 2 subnets.
☒ **A**, **C**, and **D** are incorrect.

6. ☑ **B.** There are 3 host bits, with 2 raised to the power of 3 resulting in 8 addresses in a network, but you lose 2 for the network and directed broadcast address, resulting in 6 host addresses. You could also subtract 248 from 256, resulting in a total of 8 addresses per network, of which the first and last are reserved.
☒ **A**, **C**, and **D** are incorrect.

7. ☑ **B.** There are 6 host bits, with 2 raised to the power of 6, resulting in 64 addresses in a network, but you lose 2 for the network and directed broadcast address, resulting in 62 host addresses. You could also subtract 192 from 256, resulting in a total of 64 addresses in a network—but you can't use the first and the last, so the answer is 62.
☒ **A**, **C**, and **D** are incorrect.

Determining IP Address Components

8. ☑ **C.** There is 1 subnet bit for this Class C network, resulting in two networks—192.168.37.0 and 192.168.37.128—making 192.168.37.192 a host address. Host addresses for this subnet range from 192.168.37.129 to 192.168.37.254.
   ☒ **A** is true for 192.168.37.0 and 192.168.37.128. **B** is true for 192.168.37.127 and 192.168.37.255.

9. ☑ **C.** Network addresses are incrementing by 2 in the *third* octet. 172.17.16.255 is a host address. Host addresses range from 172.17.16.1 to 172.17.17.254.
   ☒ **A** is true for 172.17.16.0. **B** is true for 172.17.17.255.

10. ☑ **A.** Network addresses are incrementing by 4 in the third octet. 10.0.8.0 is a network address. Other network addresses include 10.0.0.0, 10.0.4.0, 10.0.8.0, 10.0.12.0, and so on and so forth.
    ☒ **B** is true for 10.0.3.255, 10.0.7.255, 10.0.11.255, 10.0.15.255, and so on and so forth. **C** is true for 10.0.8.1 to 10.0.11.255, as well as other host addresses in other subnets.