2 Understanding TCP/IP

Exam Objectives in this Chapter:

- Troubleshoot TCP/IP addressing.
- Diagnose and resolve issues related to incorrect configuration.

Why This Chapter Matters

As a network administrator, you will be working with Transmission Control Protocol/Internet Protocol (TCP/IP) every day. Among your responsibilities will be, no doubt, assigning configurations to TCP/IP hosts on the one hand and then troubleshooting configuration errors on the other. To even begin to fulfill this duty, you will need a thorough understanding of the concepts behind IP addressing. This chapter will explain these concepts and enable you to diagnose problems related to the incorrect configuration of IP subnets, default gateways, subnet masks, or addresses. It will also enable you to verify an address space configuration by teaching you how to determine the number of bits to reserve for a subnet ID and host ID.

Lessons in this Chapter:

Before You Begin

To complete this chapter, you must have

- A basic understanding of computer networks, including terms such as *broadcast*, *router*, *switch*, and *hub*

Lesson 1: Understanding TCP/IP

TCP/IP is a suite of protocols that provides the foundation for Windows networks and the Internet. The TCP/IP protocol stack is based on a four-layer reference model, including the network interface, internet, transport, and application layers.

The core of TCP/IP services exists at the internet and transport layers. In particular, Address Resolution Protocol (ARP), IP, TCP, User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) are used in all TCP/IP installations.


After this lesson, you will be able to

- Describe the four layers of the TCP/IP model
- Give examples of the protocols that exist at each layer of the TCP/IP protocol stack
- Describe the basic functions of ARP, IP, ICMP, TCP, and UDP

Estimated lesson time: 10 minutes

Exploring the Layers of the TCP/IP Model

End-to-end communication through TCP/ IP is based on four conceptual steps, or layers. Figure 2-1 shows these four layers of the TCP/IP model.
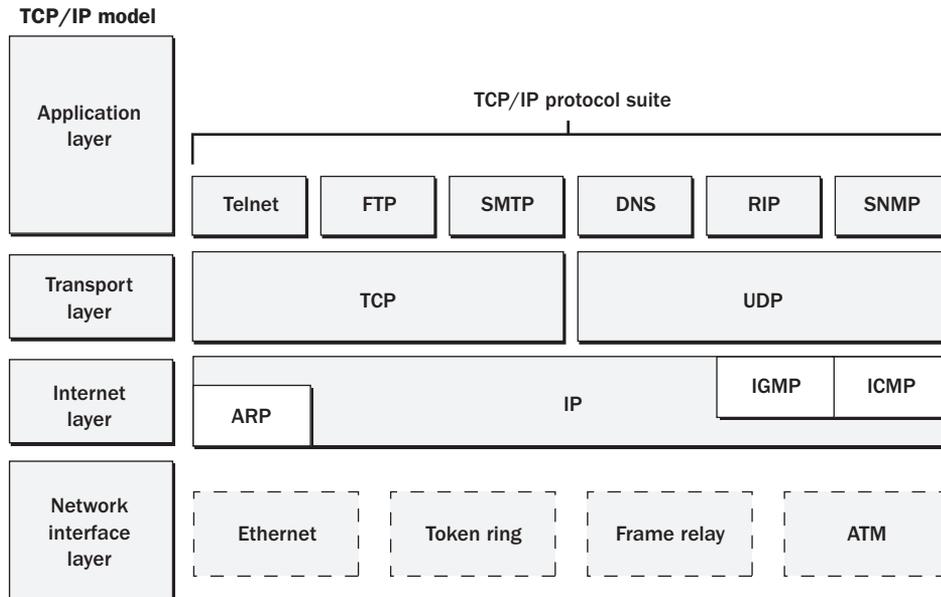
Figure 2-1   Four-layer TCP/IP model and protocol stack

Network Interface Layer

The *network interface layer* is the step in the communication process that describes standards for physical media and electrical signaling. Examples of standards defined at the network interface layer include Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), X.25, Frame Relay, RS-232, and V.35.

Internet Layer

The *internet layer* of the TCP/IP model is the step in the communication process during which information is packaged, addressed, and routed to network destinations. ARP, IP, and ICMP are examples of internet-layer protocols within the TCP/IP suite.

■ **ARP**   Whereas IP routes packets to logical addresses that might be dozens of network segments away, ARP finds the physical computers for which IP packets are destined within each network segment. After using ARP to look up hardware addresses, TCP/IP hosts store known IP-to-MAC address mappings in a local ARP cache. You can view this cache with the ARP –a command or clear it with the ARP –d command.

> **Off the Record**   In the MCSE exam world, the ARP –d command supposedly saves your day whenever you cannot connect to a computer, located in broadcast range, whose network card has just been changed. Here's what you're supposed to see: The new adapter has furnished the seemingly stranded computer with a fresh hardware address, thus rendering obsolete your currently stored IP-to-MAC address mapping for that remote host. Until you clear your local ARP cache, your computer will keep trying to reach the remote one by calling out a defunct hardware address. So goes the theory.
>
> In reality, virtually all ARP entries are dynamic, which means they are automatically added and aged out of the cache as needed. Dynamic ARP entries have a life span of only two minutes if they are not renewed. So, if your computer happens to cache the IP-to-MAC address mapping of another host, immediately after which someone shuts down that remote box, opens it up, replaces its network card, and miraculously gets it back online before all of 120 seconds have elapsed, and if, despite this feat, you are still too impatient to wait out the intervening moments before you can ping same address, then the ARP –d command really might save your day. Otherwise, you needn't worry about it.

■ **IP**   IP is primarily responsible for addressing and routing packets between hosts. An IP packet can be lost, delivered out of sequence, duplicated, or delayed, as can information in any other protocol. However, IP itself does not attempt to recover from these types of errors. The acknowledgment of packets delivered, the sequencing of packets, and the recovery of lost packets are the responsibility of a higher-layer protocol, such as TCP.

■ **ICMP**   With ICMP, hosts and routers that use IP can report errors and exchange limited control and status information. You can use the Ping command to send ICMP echo request messages and record the receipt of ICMP echo reply messages. With these messages, you can detect communication failures and troubleshoot common TCP/IP connectivity problems.

> **Real World   ICMP and Firewalls**
>
> As a network administrator, you typically need to concern yourself with ICMP message types when you are configuring firewalls that face the public Internet. Most firewalls allow you to specify the ICMP message requests to which the firewall responds. For example, if you want to be able to ping the firewall, you need to configure the firewall to respond to incoming echo requests.

Transport Layer

The *transport layer* of the TCP/IP model is the step in the communication process during which the standards of data transport are determined. TCP and UDP are examples of transport-layer protocols within the TCP/IP suite.

■ **TCP**   TCP receives data from the application layer and processes the data as a stream of bytes. These bytes are grouped into segments that TCP then numbers and sequences for delivery to a network host. When TCP receives a stream of data from a network host, it sends the data to the intended application.

TCP ports enable different applications and programs to use TCP services on a single host, as shown in Figure 2-2. Each program that uses TCP ports listens for messages arriving on its associated port number. Data sent to a specific TCP port is thus received by the application listening at that port.
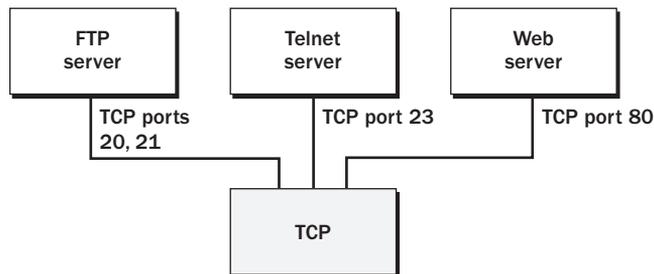
Figure 2-2   TCP ports

Exam Tip   By using packet filtering at a router, you can block or allow TCP or UDP traffic based on port number. Some exam questions require you to know which ports you must leave open to allow the following protocols to pass through to your network: File Transfer Protocol (FTP; TCP ports 20 and 21), Hypertext Transfer Protocol (HTTP; TCP port 80), Hypertext Transfer Protocol Secure/Secure Sockets Layer (HTTPS/SSL; TCP port 443), Domain Name System (DNS; UDP port 53), SMTP (Simple Mail Transfer Protocol; TCP Port 25), Point-to-Point Tunneling Protocol (PPTP; TCP port 1723), and L2TP/IPSec (UDP ports 500, 1701, and 4500). Be sure to memorize these port numbers before taking the exam!

- **UDP**   Many network services (such as DNS) rely on UDP instead of TCP as a transport protocol. UDP enables fast transport of datagrams by eliminating the reliability features of TCP such as delivery guarantees and sequence verification. Unlike TCP, UDP is a *connectionless* service that provides only best-effort datagram delivery to network hosts. A source host that needs reliable communication must use either TCP or a program that provides its own sequencing and acknowledgment services.

Exam Tip   For the exam, you need to know that connectionless services in TCP/IP networks rely on UDP as a transport.

Application Layer

The *application layer* of the TCP/IP model is the step in the communication process during which end-user data is manipulated, packaged, and sent to and from transport-layer ports. Application-layer protocols often describe a user-friendly method of presenting, naming, sending, or receiving data over TCP/IP. Common examples of application-layer protocols native to the TCP/IP suite include HTTP, Telnet, FTP, Trivial File Transfer Protocol (TFTP), Simple Network Management Protocol (SNMP), DNS, Post Office Protocol 3 (POP3), SMTP, and Network News Transfer Protocol (NNTP).

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the "Questions and Answers" section at the end of this chapter.

1. Which is the only layer of the TCP/IP reference model that does not contain any TCP/IP protocols?

   a. The network interface layer

   b. The internet layer

   c. The transport layer

   d. The application layer

2. Which of the following TCP/IP protocols does not function at the internet layer?

   a. IP

   b. ARP

   c. TCP

   d. ICMP

3. Which of the following is a transport-layer protocol?

   a. IGMP

   b. UDP

   c. DNS

   d. Ethernet

4. Which of the following services connect to UDP ports? (Choose all that apply.)

   a. NetBIOS

   b. DNS

   c. Ethernet

   d. Telnet

Lesson Summary

■ The TCP/IP protocol stack is based on a four-layer reference model, including the network interface, internet, transport, and application layers.

■ Whereas IP routes packets to logical addresses that might be dozens of network segments away, ARP finds the physical computers for which IP packets are destined within each network segment.

■ TCP is a required TCP/IP standard that provides reliable, connection-oriented packet delivery service. UDP provides a connectionless datagram service that, unlike TCP, does not guarantee delivery or verify sequencing for any datagrams. Both TCP and UDP provide ports at which applications can connect to transport-layer services.

Lesson 2: Working with IP Address Blocks

On the 70-291 exam, you are likely to encounter questions related to IP addressing that require you to be comfortable working with IP addresses, IP address blocks, and subnet masks. This lesson is designed specifically to help you answer questions related to addressing features of single-subnet networks.

After this lesson, you will be able to

- Describe the component parts of an IP address
- Explain the function of a subnet mask
- Describe the relationship between address blocks, subnets, default gateways, and broadcast domains
- Describe the difference between public addresses and private addresses
- Convert a subnet mask between slash notation and dotted-decimal notation
- Determine the host capacity of an address block configured as a single subnet, given the block's subnet mask expressed in slash notation or dotted-decimal notation
- Determine an appropriately sized address block, given a requirement for a number of hosts

Estimated lesson time: 120 minutes

The Structure of IP Addresses

IP addresses are 32 bits in length and are composed of 4 *octets* of 8 bits apiece. The usual representation of an IP address is in *dotted-decimal* notation, with each of the four numbers—for example, 192.168.23.245—representing an octet separated from each other by a period (dot). This common dotted-decimal notation, however, is only ever displayed for human benefit. Computers actually read IP addresses in their native 32-bit binary notation such as

11000000 10101000 00010111 11110101

This point becomes important if you want to understand how IP works.

IP is an addressing system—a system to help *find* devices—and not merely an identification system. Every IP address on a network must be unique, but an address cannot be assigned randomly to a networked device because that would provide no way of finding the device. The way that IP achieves both uniqueness and findability is by dividing addresses into two parts: the *network ID* and the *host ID*.

Network ID and Host ID

The first part of an IP address is the *network ID*. The job of the network ID is to identify a particular network within a larger IP internetwork (such as the Internet). The last part of an IP address is the *host ID*. The host ID identifies an IP host (a computer, router, or other IP device) within the network defined by the network ID.

> **Tip**   If n = the number of bits in the network ID and h = the number of bits in the host ID, n + h is equal to 32.

Figure 2-3 shows a sample view of an IP address (131.107.16.200) as it is divided into network ID and host ID sections. The letters w, x, y, and z are often used to designate the four octets within an IP address. In this example, the network ID portion (131.107) is indicated by octets w and x. The host ID portion (16.200) is indicated by octets y and z.
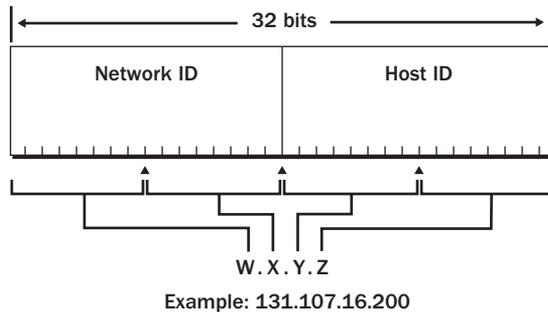
Figure 2-3   Network and host IDs

IP Addresses and ZIP+4 Compared   This system of dividing the IP address into a network ID and a host ID is reminiscent of the "ZIP+4" system used by most post offices in the United States Postal System. This system is used to route and deliver mail to individual post office boxes across the country.

> **Note**   For the purposes of our analogy, we will assume that the +4 digits only ever represent individual post office boxes.

Taken together, the 5-digit zip code (also known as a postal code) and the 4-digit box number represent a unique 9-digit ZIP+4 address similar in structure and function to the 32-bit IP address. The first part of the ZIP+4 address—the five-digit zip code—represents a findable area, not a unique address. The second part represents a specific 4-digit mailbox within the 5-digit zip code area, a mailbox to which the post office represented by the zip code has the responsibility to deliver mail.

However, ZIP+4 addresses are much simpler than IP addresses in one respect. When you look at a ZIP+4 address, you know for certain which part of the address represents the post office (the zip code) and which part represents the individual mailbox (the +4). The dividing line between them never changes. The first five digits and the last four digits always have the same function.

The tricky thing about IP addresses is that the size of the network ID and the size of the host ID vary. Just by looking at an IP address such as 192.168.23.245, you cannot determine which of the 32 bits are used for the network ID and which are used for the host ID. To do this, you need an additional piece of information. That piece of information is the subnet mask.

Subnet Masks

The subnet mask is used to determine which part of a 32-bit IP address should be considered its network ID. For example, when we write 192.168.23.245 /24, the /24 represents the subnet mask and indicates that the first 24 of the 32 bits in that IP address should be considered its network ID. For the IP address 131.107.16.200 shown in Figure 2-3 above, the first 16 bits according to the picture are used for the network ID. Therefore, the appropriate subnet mask to be used by a host assigned that address is /16.

The two subnet masks we have just mentioned—/16 and /24—are relatively easy to interpret. Because their values are divisible by 8, these subnet masks indicate that the network ID is composed of, respectively, the the first two complete octets and the first three complete octets of an IP address. In other words, the network ID of a host assigned the address 131.107.16.200 /16 is 131.107, and the host's network address is therefore 131.107.0.0. The network ID of a host assigned the address 192.168.23.245 /24 is 192.168.23, and host's network address is therefore192.168.23.0. However, subnet masks are not always divisible by 8 and are not always so easy to interpret, as we shall see below.

Subnet Mask Notations   We have been discussing subnet masks in *slash notation*— also known as Classless Inter Domain Routing (CIDR) notation or network prefix notation. Slash notation is a common way of referring to subnet masks both on the 70-291 exam and in the real world. However, subnet masks are represented just as commonly in 32-bit dotted-decimal notation.

In dotted-decimal notation, the subnet mask takes the form of a 32-bit IP address. For example, the subnet mask /16 is represented in dotted-decimal notation as 255.255.0.0, and the subnet mask /24 is represented in dotted-decimal notation as 255.255.255.0.

To translate a subnet mask between slash notation and its dotted-decimal equivalent, you first have to translate the slash notation to binary notation. To begin, take the value

after the slash in slash notation—for example, the 16 in /16—and represent it as an equivalent number of ones in binary notation, with a space after each 8 bits or octet.

11111111 11111111

Then, to complete the 32-bit subnet mask in binary notation, add a string of 0s until the values of all 32 bits are represented (again with a space after each 8 bits):

11111111 11111111 00000000 00000000

Finally, translate this binary notation into dotted-decimal notation. Because 11111111 is the binary equivalent of the decimal 255 and 00000000 is the binary equivalent of the decimal 0, you can represent each octet as either 255 or 0. For this reason, /16 is equivalent to 255.255.0.0.

> **Important**   You might see in other sources that a /8 address is called *Class A*, a /16 address is called *Class B*, and a /24 address is called *Class C*. This refers to an older system of routing rarely used today (even though its vocabulary survives). Because the 70-291 exam does not use these terms, they have been avoided in this chapter.

Subnet Mask Mid-Range Values   The subnet masks we have been looking at in dotted-decimal notation have octets whose values are represented as either 255 or 0. This limits our discussion to only three possible subnet masks: /8 (255.0.0.0), /16 (255.255.0.0), and /24 (255.255.255.0). In fact, these are the most common subnet masks used for addresses on the Internet (especially /24 or 255.255.255.0).

However, both on the 70-291 exam and in the real world, you will also encounter subnet masks such as /25 or /22 which, when expressed in dotted-decimal notation, include a mid-range value octet such as 128 or 252. This situation arises whenever the length of a network ID (expressed in bits) is not divisible by 8.

Table 2-1 below compares the slash, binary, and dotted-decimal notations for all subnet masks from /8 to /30. These are the only subnet masks you are ever likely to see. However, the subnet masks you will encounter most frequently (both on the 70-291 exam and in the real world) are in the /16 – /28 range.

> **Important**   Definitely spend some time browsing this table until you are comfortable with subnet mask values and how the three notations relate to each other.

Table 2-1   Subnet Mask Notations Compared

Slash Notation (/n)	Binary Notation	Dotted-Decimal Notation
/8	11111111 00000000 00000000 00000000	255.0.0.0
/9	11111111 10000000 00000000 00000000	255.128.0.0
/10	11111111 11000000 00000000 00000000	255.192.0.0
/11	11111111 11100000 00000000 00000000	255.224.0.0
/12	11111111 11110000 00000000 00000000	255.240.0.0
/13	11111111 11111000 00000000 00000000	255.248.0.0
/14	11111111 11111100 00000000 00000000	255.252.0.0
/15	11111111 11111110 00000000 00000000	255.254.0.0
/16	11111111 11111111 00000000 00000000	255.255.0.0
/17	11111111 11111111 10000000 00000000	255.255.128.0
/18	11111111 11111111 11000000 00000000	255.255.192.0
/19	11111111 11111111 11100000 00000000	255.255.224.0
/20	11111111 11111111 11110000 00000000	255.255.240.0
/21	11111111 11111111 11111000 00000000	255.255.248.0
/22	11111111 11111111 11111100 00000000	255.255.252.0
/23	11111111 11111111 11111110 00000000	255.255.254.0
/24	11111111 11111111 11111111 00000000	255.255.255.0
/25	11111111 11111111 11111111 10000000	255.255.255.128
/26	11111111 11111111 11111111 11000000	255.255.255.192
/27	11111111 11111111 11111111 11100000	255.255.255.224
/28	11111111 11111111 11111111 11110000	255.255.255.240
/29	11111111 11111111 11111111 11111000	255.255.255.248
/30	11111111 11111111 11111111 11111100	255.255.255.252

Note   The Slash Notation column in Table 2-1 has also been labeled "/n" to provide consistency with references to that value that appear elsewhere in this chapter. The variable *n* represents the number of bits in the network ID.

Important   All of the exercises included at the end of this lesson are designed to be completed as you progress through the lesson. To reinforce the concepts introduced above, proceed immediately to Exercise 1, "Choosing an Appropriate Subnet Mask," in the Practice section at the end of this lesson. Then continue to "Using Public IP Addresses," the next section in this lesson.

Using Public IP Addresses

Every IP address on the public Internet is unique. To allow networks to obtain unique addresses for the Internet, the Internet Assigned Numbers Authority (IANA) divides up the nonreserved portion of the IP address space and delegates responsibility for address allocation to a number of regional registries throughout the world. These registries include Asia-Pacific Network Information Center (APNIC), American Registry for Internet Numbers (ARIN), and Réseaux IP Européens Network Coordination Centre (RIPE NCC). The regional registries then allocate *blocks* of addresses to a small number of large Internet service providers (ISPs) that then assign smaller blocks to customers and smaller ISPs.

Using Private IP Addresses

The IANA has also reserved a certain number of IP addresses that are never used on the global Internet. These private IP addresses are used for hosts that require IP connectivity but that do not need to be seen on the public network. For example, a user connecting computers in a home TCP/IP network does not need to assign a public IP address to each host. The user can instead take advantage of the address ranges shown in Table 2-2 to provide addresses for hosts on the network.

Table 2-2   Private Address Ranges

Starting Address	Ending Address
10.0.0.0	10.255.255.254
172.16.0.0	172.31.255.254
192.168.0.0	192.168.255.254

Hosts addressed with a private IP address can connect to the Internet through the use of a Network Address Translation (NAT) server. The NAT server can be a Windows Server 2003 computer or a dedicated routing device. Windows Server 2003 and Windows XP Professional also include the Internet Connection Sharing (ICS) feature, which provides simplified NAT services to clients in a private network.

Address Blocks, Networks, and Subnets

Most organizations use a combination of public and private addresses. Often, public addresses are assigned to publicly available servers and private addresses are assigned to client computers, but there are many exceptions. What is certain is that every organization that wants to communicate on the Internet must have at least one public address. This public address can then be leveraged by many clients through NAT and private address ranges.

Typically, your ISP assigns you one public IP address for each computer directly connected to that ISP. Although small organizations might be able to get by with only a single public IP address, many organizations need far more than that. Organizations needing more than one public address purchase those addresses from their ISP as a block.

An *address block* is the complete group of individual IP addresses that shares any single network ID. For example, an organization may purchase from an ISP a /24 address block with network ID 206.73.118. The range of addresses associated with this address block would thus be 206.73.118.0 – 206.73.118.255.

> **Note**   The range of addresses associated with a given address block is also known as the block's *address space*.

It is essential to understand that the addresses within an address block comprise a single network, and unless the network is subnetted—a possibility we will consider next lesson—that address block will serve a *single broadcast domain* with a single router or way out of the network. The *default gateway* is the address within the same broadcast domain and assigned to that router.

Stated another way, an address block by default is designed to serve a single *subnet*. A subnet is a group of hosts within a single broadcast domain that share the same network ID and the same default gateway address.

> **Exam Tip**   There are a few things you need to know about default gateways for the 70-291 exam. First—as you should know already—a default gateway must share the same network ID and be located within the same broadcast domain as the hosts it is serving. Second—as you also probably know already—if a host has no default gateway setting configured, that host will be unable to connect to the Internet or to any computers beyond broadcast range (such as, beyond the local router). For example, a private internal server that occasionally needs to download content off the Internet needs to have a default gateway configured. Third—and this you might not realize—leaving the default gateway setting unconfigured on a host prevents access *to* that host from all points beyond the local subnet. In certain situations, therefore, you might in fact want to leave the default gateway setting unconfigured for security reasons.

Figure 2-4 displays a network served by the address block 206.73.118.0/24.
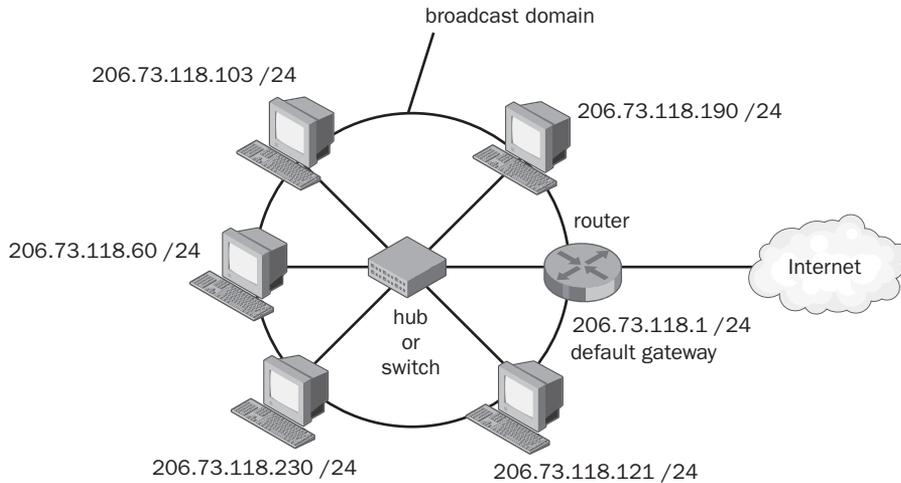
Figure 2-4 A single-subnet network

Memorizing Powers of 2

Throughout the rest of this lesson, we are going to be discussing how to answer certain types of IP addressing questions that appear on the 70-291 exam. To handle many of these questions efficiently, you need to memorize the values of the powers of 2 from 2^1 through 2^{12}.

Use Table 2-3 below to help you memorize these values. Begin by using your hand to cover the right column of the table. (The values in this column have been labeled *p values* to provide consistency with references to these values found elsewhere in the chapter.) When you can recite without hesitation the p value associated with any Power of 2 value chosen at random from the left column, proceed to cover up the left column with your hand. (The exponent in this column has been assigned the variable *h* to correspond to references found elsewhere in the chapter.) Proceed further with the lesson only after you can recite without hesitation the exponential value of 2 (h value) associated with any p value chosen at random from the right column.

Table 2-3   The Powers of 2

Power of 2 (2^h)	Equivalent Value (p value)
2^1	2
2^2	4
2^3	8
2^4	16
2^5	32

Table 2-3   The Powers of 2

Power of 2 (2^h)	Equivalent Value (p value)
2^6	64
2^7	128
2^8	256
2^9	512
2^{10}	1024
2^{11}	2048
212	4096

Powers of 2 Beyond 2^{12}

It is unlikely that you will need to calculate on the 70-291 exam any power of 2 beyond 2^{12}. However, if this need arises, use the memorized value of 2^{12} (4096) to help you. For each power of 2 beyond 2^{12}, simply multiply 4096 by a factor of 2. For example, if you need to calculate 2^{14}, multiply 4096 by (2×2) or 4096 ×4. To calculate 2^{15}, multiply 4096 by ($2 \times 2 \times 2$) or 4096 × 8.

Important   Before continuing to the next section in this lesson, proceed to Exercise 2, "Mastering the Powers of 2," in the Practice section at the end of this lesson.

Memorizing Subnet Mask Octet Values

To handle IP addressing questions on the 70-291 exam, you will also need to memorize the nine possible values that might appear in a subnet mask octet.

Use Table 2-4 below to help you memorize these values. (The values in the top and middle rows have been labeled *d values* and *r values* respectively to provide consistency with references to these values that appear elsewhere in the chapter.)

Begin by covering the top row of the table. Once you can recite without hesitation the d value associated with any particular r value or binary value chosen at random from the bottom two rows, proceed to cover up the bottom two rows. Once you can recite without hesitation the r value associated with any d value chosen at random from the top row, proceed to memorize the *sequence* of d values from left to right and right to left.

Table 2-4   Subnet Mask Octet Values

Decimal (d) value	0	128	192	224	240	248	252	254	255
Number of 1-bits (r value)	0	1	2	3	4	5	6	7	8
Binary value	00000000	100000000	11000000	11100000	11110000	11111000	11111100	1111110	11111111

You need to know these sequences forward and backward so well that you can look at a number such as 192 and know that when moving from left to right, this value is the second after 0 and is therefore *2 bits removed* from the 0 octet value. In the same way, you need to be able to look at 248 and know that when moving from right to left, it is the third after 255 and therefore *three bits removed from 255.*

When you have thoroughly memorized these d values and their associated r values, proceed to Exercise 3 in the Practice section at the end of this lesson.

> **Important**   Before continuing to the next section in this lesson, proceed to Exercise 3, "Mastering Subnet Mask Octet Values," in the Practice section at the end of this lesson.

Analyzing Dotted-Decimal and Slash Equivalents

Although memorizing the equivalent dotted-decimal and slash notations for subnet mask values is not strictly speaking *necessary*, it is nonetheless *highly recommended* that you learn the most common of these associated pairs. Memorizing the most commonly seen subnet mask values (those shown in Table 2-5) in both notations will help you see the pattern in the notation conversion process, reduce the intimidation factor on the 70-291 exam, and save you time.

To use the chart below as a tool for memorization or analysis, begin with the middle entry: the /24 address block consisting of 256 addresses. As you should know by this point, a /24 subnet mask is equivalent to 255.255.255.0. Each of the first three octets expressed in binary would thus be represented 11111111. If we move up one row in the table to the /23 address block, we can see that the equivalent dotted-decimal notation (255.255.254.0) has a mid-range value in the third (y) octet. This mid-range value, 254, corresponds to a binary notation 11111110 (*r* value = 7), a correspondence you have memorized in the previous exercise.

More interesting, perhaps, is that the size of the address block doubles to 512 when we shorten by one the string of 1-bits in the subnet mask (for example, from /24 to /23). If we proceed up one more row to the /22 address block, we can see that the

mid-range value octet has now changed to 252, which, as you have memorized, corresponds to 11111100 in binary (r value = 6). Once again, this process doubles the size of the block to 1,024 addresses.

> **Exam Tip**   Incrementing downward by one the slash value in a subnet mask always doubles the size of the associated address block. Incrementing upward by one always halves it.

Table 2-5   Memorizing Common Subnet Masks

Slash Notation (/n)	Dotted-Decimal Notation	Addresses per Block (p value)
/22	255.255.252.0	1024
/23	255.255.254.0	512
/24	**255.255.255.0**	**256**
/25	255.255.255.128	128
/26	255.255.255.192	64

We can then move back to our starting point of the /24 network and proceed in the other direction. When we move from /24 to /25, the dotted-decimal notation of the subnet mask changes from 255.255.255.0 to 255.255.255.128. Notice that the mid-range value is now located in the fourth (z) octet. This mid-range value, 128, corresponds to the binary value 10000000 (r value = 1) that you have memorized in the previous exercise. Notice also that the size of the address block is halved from 256 to 128.

When we then move from /25 to /26, the value of the fourth (z) octet assumes the value 192, which as you have memorized, is equivalent to the binary 11000000 (r value = 2). And once again, the size of the block is halved to 64 addresses.

Converting Subnet Mask Notations

On the 70-291 exam, you will occasionally need to convert subnet masks from slash notation to dotted-decimal notation, or vice-versa. Most often the conversion is not sufficient by itself to answer a question correctly but is nonetheless a necessary step toward determining the correct response.

If you need to perform a subnet mask notation conversion that you have not memorized, use the following methods.

Converting from Slash to Dotted-Decimal Notation

To convert the subnet mask of a network from /*n* notation to *w.x.y.z* notation, perform the following steps. Ideally, you should perform this entire calculation in your head, but use a scratch pad if you need to.

1. Visualize four spaces separated by three dots, corresponding to the *w.x.y.z* format of a subnet mask in dotted-decimal notation.

2. Look at the subnet mask in slash notation. Taking the /n value, divide 8 into n. For as many times as 8 goes into this n value, add a 255 into the visualized octet spaces from left to right.

   For example, for a /20 network, 8 goes into 20 two times. Therefore, picture 255.255 in the w and x spaces for the first two octets.

3. Take the remainder of the last calculation. This remainder corresponds to the r value in Table 2-4, or the number of 1-bits in a string at the beginning of a binary octet. Use your memorizations of subnet mask octet values to visualize in the next available space the decimal value (d value) associated with this r value.

   For example, the remainder when 20 is divided by 8 is 4. This remainder or r value corresponds to 11110000 in binary, which, as you have memorized, corresponds to 240 in decimal notation. Therefore, you should add a 240 into the next space to yield 255.255.240.

4. If there are any remaining octets, fill them in with a 0.

   In our example, there is one remaining octet, so we complete the conversion by adding a 0 into the last space. This yields the subnet mask 255.255.240.0.

Off the Record   If you have not memorized the subnet mask octet (d) values associated with the possible remainders (r values), you can just use this simple formula:

d = [(2r-1)/2r] × 256

You can do that in your head, right?

But seriously, the best alternative to memorization would be to use the remainder (r value) to write out the octet in binary notation and then perform binary-to-decimal conversion (a process that isn't discussed in this book).

Although the subject of binary math is quite interesting—especially if you're the type to spend your Friday nights playing with calculators—you actually only need to know 8 binary values for the 70-291 exam. You are much better off simply memorizing these values than learning how to translate any number between binary and decimal. The bottom line is that you can't afford to be wasting time on the 70-291 exam performing binary-to-decimal conversions. If you have to do that, you just haven't prepared for the exam enough.

Important   Before continuing to the next section in this lesson, proceed to Exercise 4, "Converting Subnet Masks to Dotted-Decimal Notation," in the Practice section at the end of this lesson.

Converting from Dotted-Decimal to Slash Notation

To convert the subnet mask of a network from *w.x.y.z* notation to */n* notation, perform the following steps. Ideally, you should perform this entire calculation in your head, but use a scratch pad if you have difficulty.

1. Take the subnet mask in w.x.y.z (dotted-decimal) format. For every octet in the subnet mask whose value is 255, add 8.

   For example, if the subnet mask is 255.255.255.224, add 8 + 8 + 8 to obtain 24.

2. If you have a mid-range value octet (value between 0 and 255), add the r value associated with this mid-range octet value. You should have this value memorized.

   In our example we have a mid-range value octet of 224. Since we know from our memorizations that the r value corresponding to this decimal (d) octet value is 3, we need to add 3 to our subtotal (24) from the last step to obtain a total of 27.

3. Put a slash before the resulting value, and you're done.

   In our example, the final result is /27.

Off the Record   If you are frustrated with having to rely on memorizations to determine the r value associated with a given d value, simply use the following formula:

r = 8 − [log(256-d) / log(2)]

It's much easier to calculate that than to recall a few memorized values, right? Okay, seriously: the best alternative to memorization in this case is to write out the mid-range value octet and then perform a decimal-to-binary conversion (a process not described in this book). But again I insist—you simply don't have time to be wasting on decimal-to-binary conversions on the 70-291 exam.

Important   Before continuing to the next section in this lesson, proceed to Exercise 5, "Converting Subnet Masks to Slash Notation," in the Practice section at the end of this lesson.

Determining the Host Capacity of a Network

The host capacity of a network is the number of computers that can be accommodated by the address block assigned to that network. On the 70-291 exam, you will probably encounter questions in which you need to determine a network's host capacity. Often this information is not sufficient by itself to answer a question correctly but is nonetheless an important component of the correct response.

Within the range of any address block assigned to a subnet, the lowest address (the host ID consisting of all zeroes) and the highest address (the host ID consisting of all ones) cannot be assigned to network devices such as computers. This is because the all-zeroes host ID is always reserved for the subnet's network address, and the all-ones host ID is always reserved for the subnet's broadcast address. For this reason, *the host capacity of a subnet is always two fewer than the number of addresses in the subnet's address range.*

Important   Because the lowest and highest addresses in a subnet's address range cannot be assigned to computers, the host capacity of a subnet's address range is always two fewer than the actual number of addresses in that range.

Determining the Host Capacity of a /n Network

To determine the host capacity of a network whose subnet mask is expressed in slash notation as /n, use the following formula: $c = 2^{(32-n)} - 2$, where c represents the number of computers that can be accommodated by a given network, and n represents the number of bits in the network ID of that network.

For example, in a /20 network, n = 20. Therefore $c = 2^{(32-20)} - 2$, or $2^{12} - 2$, or 4096 – 2, or 4094. So, a /20 network can accommodate 4094 computers.

Here is another example: In a /28 network, n = 28. Therefore, $c = 2^{(32-28)} - 2$, or $2^4 - 2$, or 16 – 2, or 14. So, a /28 network can accommodate 14 computers.

This formula might look somewhat complicated, but if you have memorized your powers of 2, you should actually be able to perform the calculation in your head.

If you are not able to perform this calculation in your head, the problem might be that you are averse to mathematical formulas. In this case, use the following step-by-step instructions:

1. Take the value after the slash (n) and subtract it from 32. (This determines the value *h* or number of bits in the host ID. For example, in a /21 network, subtract 21 from 32 to obtain an h value of 11.)

2. Raise 2 to this power (h). (This yields a value p. You should have this value memorized. Following our example, you would raise 2 to the 11th power to obtain the value 2048.)

3. Subtract 2 (from p). (In our example, you would subtract 2 from 2048 to get 2046.)

   That's it! In our example, we have determined that a /21 network can accommodate 2046 hosts.

> **Tip**   Because you know that a /24 network contains 256 addresses, you can easily deter-
> mine in your head the host capacity for networks whose size is close to /24. The key to this
> method is the fact that every increment downwards of 1 in the slash notation doubles the
> size of a network, and every increment upwards halves it. For example, to determine the num-
> ber of addresses in a /23 network, simply double the size of a /24 network (256) to obtain
> 512. To determine the number of addresses in a /22 network, double again to obtain 1024.
> To work the other way, a /25 network must have one-half of the 256 addresses in a /24 net-
> work (128), and a /26 network must have half of that (64). Don't forget that this doubling and
> halving only yields the number of addresses in a network. To then determine the *host capacity*
> of a given network, you must subtract 2.

Host Capacity for Networks with *w.x.y.z* Subnet Masks

When the subnet mask of a network is expressed in dotted-decimal notation, determin-
ing the network's host capacity is very easy when that subnet mask is between
255.255.255.0 and 255.255.255.255. When this is the case, simply *subtract the value of
the last octet from 256 to determine the address block size, and then subtract 2.* This
process can be expressed as the following formula: $c = 256 - z - 2$, where c represents
the number of computers that can be accommodated by a given network, and z repre-
sents the value of the last octet in the subnet mask. You want to subtract 2 as a separate
and final step in this calculation because 256-z will yield one of the d values you have
memorized from Table 2-4. Knowing this will help you perform the subtraction oper-
ation in your head.

For example, for a network with a subnet mask of 255.255.255.224, c = 256 – 224 – 2,
or 32 – 2, or 30. So, a network with a subnet mask of 255.255.255.224 can accommo-
date 30 computers.

Another example: For a network with a subnet mask of 255.255.255.192, c=256 – 192
– 2, or 64 – 2, or 62. So, a network with a subnet mask of 255.255.255.192 can accom-
modate 30 computers.

When the subnet mask of a network is *not* between 255.255.255.0 and 255.255.255.255,
you should first try to determine the network's host capacity by using the "doubling
from 256" shortcut described in the tip above. For example, if you recognize that
255.255.252.0 is two bits removed from 255.255.255.0, you can double 256 twice to get
1024, and then subtract 2 to get a host capacity of 1022 for the 255.255.252.0 network.

If you are not able to use this doubling method, convert the dotted-decimal subnet
mask to slash notation. Then, simply perform the calculation described in the section
above, entitled "Determining the Host Capacity of a /n Network."

> **Important** Before continuing to the next section in this lesson, proceed to Exercise 6, "Determining the Host Capacity of Networks," in the Practice section at the end of this lesson.

Determining Block Size Requirements

So far, we have learned how to calculate the host capacity of a given address block. On the 70-291 exam, you might also need to determine the block size required for a single subnet network needing c computers.

Determining Block Size Requirements in /n Terms

To determine in /n terms the block size of a network required to accommodate c computers, use the following step-by-step procedure:

1. Add 2 to c. This yields a new value q, the number of addresses required in your address block.

   For example, if you want to determine the block size requirement for a network with 128 computers, q= 128 + 2 = 130. Your address block must thus include at least 130 addresses.

2. Determine the lowest exponential value (h value) that, when applied to 2, yields a value that is equal to or greater than q.

   For example, 2^7 = 128 and 2^8 = 256. Therefore, the lowest power of 2 (h value) equal to or greater than 130 is 8. The variable h stands for the number of bits in the required network's *host* ID. Our next step is to determine the number of bits in the address block's *network* ID.

3. Subtract 32- h. This yields our desired value, n.

   In our example, 32-8 = 24. Therefore, n = 24.

4. Add a slash before n, and you are done.

   In our example, we have determined that a /24 network is needed to accommodate 128 computers.

> **Important** Before continuing to the next section in this lesson, proceed to Exercise 7, "Determining Network Size Requirements in Slash Notation Terms," in the Practice at the end of this lesson.

Determining Block Size Needs in Terms of a *w.x.y.z* Subnet Mask

To determine in terms of a dotted-decimal subnet mask the block size requirements of a network needing to accommodate c computers, use the following step-by-step procedure:

1. Add 2 to c. This yields a new value q, the number of addresses required in your address block.

2. If q is less than or equal to 256, move on to the next step. Otherwise, skip to step 5.

3. Determine the lowest value that is a power of 2 (p value) and that is equal to or greater than q. For example, if your c value is 25 and your q value is 27, your p value is 32.

4. Calculate 256 – p. This calculation results in a d value that is placed in the fourth (z) octet of your subnet mask; the value 255 is placed in the three preceding octets (w, x, and y). In our example, the 256 – 32 = 224. Therefore, the network block size we would need to accommodate 25 computers can be defined by the subnet mask 255.255.255.224.

5. (From step 2). If possible, use the "double from 256" shortcut method and memorized subnet mask octet values (d values) to determine the appropriate subnet mask. For example, if you need to accommodate 900 computers, you need 902 addresses in your address block. Since a subnet mask 255.255.255.0 provides 256 addresses, you should be able to determine in your head that a subnet mask of 255.255.254.0 would provide 512 addresses, and a subnet mask of 255.255.252.0 would provide 1024 addresses. To accommodate 902 addresses, then, you would need a subnet mask of 255.255.252.0.

6. If you are unable to use the shortcut described in the previous step, use instead the instructions in the previously described procedure to determine the required size of the network in /n terms. Then, simply convert the subnet mask from slash notation to dotted-decimal notation.

> **Important**   Before continuing to the next section in this lesson, proceed to Exercise 8,"Determining Network Size Requirements in Terms of a Dotted-Decimal Subnet Mask," in the Practice at the end of this lesson.

Practice: Learning to Work with Address Blocks

In this practice, you perform exercises that help solidify your understanding of address blocks, subnet masks, and host capacity.

Exercise 1: Choosing an Appropriate Subnet Mask

You are adding a new server to each of the following subnets. Given the addresses of the existing computers on that subnet, determine which subnet mask you should assign to the new server.

Exam Tip   It is likely that you will have to perform a similar task on the exam. Most likely, this task will not be sufficient by itself to answer a question correctly, but it will be, nonetheless, a necessary step on the way to determining the right answer.

1. Which subnet mask would you assign to the new server?

   Subnet 1: Existing computers

   10.2.12.1
   10.2.41.23
   10.2.41.100
   10.2.41.101

   a. 255.0.0.0 (/8)

   b. 255.255.0.0 (/16)

   c. 255.255.255.0 (/24)

2. Which subnet mask would you assign to the new server?

   Subnet 2: Existing computers

   192.168.34.1
   192.168.34.55
   192.168.34.223
   192.168.34.5

   a. 255.0.0.0 (/8)

   b. 255.255.0.0 (/16)

   c. 255.255.255.0 (/24)

Exercise 2: Mastering the Powers of 2

Complete the table below by providing the lowest value that is a power of 2 (p value) and that is *equal to or greater than* each of the values in the left column. Then, provide the exponential value of 2 (h value) associated with the each p value. If you have memorized the powers of 2 sufficiently, you should be able to complete this exercise in less than 2 minutes.

The first row is provided as an example.

Value	p value	h value (exponent of 2)
200	256	8
40		
312		
1544		
20		
96		
1		
12		
600		
150		
3		
2500		
6		
64		
10		
1775		
103		
17		
255		
3242		

Exercise 3: Mastering Subnet Mask Octet Values

Complete the table below by providing the correct binary notation, r value, and d value as shown in the example provided in the first line. If you have memorized the subnet mask octet values sufficiently, you should be able to complete this exercise in less than 2 minutes.

Binary Value	Number of 1-bits (r value)	Decimal value (d value)
11110000	4	240
	6	
11000000		
	5	
		254
11100000		
	8	
		240
00000000		
	1	
		224
	2	
11111000		
	7	
		128
11111100		
	4	
		255
11111110		
	3	
10000000		
11110000		
		192
		248
		252

Exercise 4: Converting Subnet Masks to Dotted-Decimal Notation

Convert the following subnet masks in slash notation to dotted-decimal in your head by using memorizations from Table 2-5 and the steps described in the earlier section, "Converting Subnet Mask Notations." Write only the final answer in each space provided.

Slash Notation	Dotted-Decimal Notation
/18	
/28	

Slash Notation	Dotted-Decimal Notation
/21	
/30	
/19	
/26	
/22	
/27	
/17	
/20	
/29	
/23	
/25	

Exercise 5: Converting Subnet Masks to Slash Notation

Use the steps described above to convert the subnet masks in dotted-decimal notation to slash notation in your head. Write only the final answer in each space provided.

Dotted-Decimal Notation	Slash Notation
255.255.240.0	
255.255.255.248	
255.255.192.0	
255.255.255.128	
255.255.248.0	
255.255.255.224	
255.255.252.0	
255.255.128.0	
255.255.255.252	
255.255.224.0	
255.255.254.0	
255.255.255.192	
255.255.255.240	

Exercise 6: Determining the Host Capacity of Networks

For each of the given address blocks below, determine in your head the number of hosts that can be supported. Write down only the final answer in the space provided in the right column.

Address Block	Number of Supported Hosts (c value)
131.107.16.0 /20	
10.10.128.0 Subnet mask: 255.255.254.0	
206.73.118.0 /26	
192.168.23.64 Subnet mask: 255.255.255.224	
131.107.0.0 Subnet mask: 255.255.255.0	
206.73.118.24 /29	
10.4.32.0 /21	
172.16.12.0 /22	
192.168.1.32 Subnet mask: 255.255.255.128	
131.107.100.48 /28	
206.73.118.12 Subnet mask: 255.255.255.252	
10.12.200.128 /25	
192.168.0.0 Subnet mask: 255.255.248.0	
172.20.43.0 /24	
131.107.32.0 Subnet mask 255.255.255.240	
10.200.48.0 Subnet mask: 255.255.240.0	
192.168.244.0 /23	
10.0.0.0 /30	
172.31.3.24 Subnet mask: 255.255.255.248	
206.73.118.32 /27	
131.107.8.0 Subnet mask: 255.255.252.0	
192.168.0.64 Subnet mask: 255.255.255.192	

Exercise 7: Determining Network Size Requirements in Slash Notation Terms

Each of the values in the left column of the table below refers to a number of computers that a given network must support. In the corresponding space in the right column,

specify with a subnet mask in slash notation the smallest network size that will accommodate those computers. You should attempt to perform these calculations in your head. Use a scratch pad only if necessary.

The first row is provided as an example.

Number of Network Hosts	Subnet Mask (/n)
18	/27
125	
400	
127	
650	
7	
2000	
4	
3500	
20	
32	

Exercise 8: Determining Network Size Requirements in Terms of a Dotted-Decimal Subnet Mask

Each of the values in the leftmost column of the table below refers to a number of computers that a given network must support. In the corresponding space in the rightmost column, specify with a subnet mask in dotted-decimal notation the smallest network size that will accommodate those computers. You should attempt to perform these calculations in your head. Use a scratch pad only if necessary.

The first row is provided as an example.

Number of Network Hosts	Subnet Mask (w.x.y.z)
100	255.255.255.128
63	
1022	
6	
1100	
12	
150	
2500	

Number of Network Hosts	Subnet Mask (w.x.y.z)
20	
300	
35	

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the "Questions and Answers" section at the end of this chapter.

1. Which of the following is true of an address block?

    a. An address block does not necessarily consist of contiguous address space.

    b. By default, an address block serves a single subnet.

    c. Every address in an address block can be assigned to computers.

2. Which of the following is not a private address?

    a. 198.162.0.0 /24

    b. 172.31.0.0 /16

    c. 10.255.255.254 /24

3. Your network address is 131.107.0.0 /28. How many computers can this network accommodate?

    a. 254

    b. 256

    c. 16

    d. 14

4. Your organization purchased the 208.147.66.128 /25 block from an ISP two years ago. Currently, the network has 100 computers. Within the next year, you plan to purchase another 100. You intend to ask the ISP to change your subnet mask so that it will accommodate your network needs over the next year. Which subnet mask should you request?

    a. 255.255.255.192

    b. 255.255.254.0

    c. 255.255.252.0

    d. 255.255.255.0

5. From memory, write out from left to right in the space below the sequence of nine possible values for a subnet mask octet in ascending order.

Lesson Summary

■ A portion of an IP address represents a network ID, and a portion represents its host ID.

■ A subnet mask is used to determine which part of an IP address should be considered its network ID. A subnet mask can be represented in slash notation or dotted-decimal notation. To handle questions involving subnet masks on the 70-291 exam, you should be able to convert between these two notations.

■ Public IP addresses are the globally unique addresses that are connected to the Internet. Private IP addresses are confined to specific ranges and can be used by any private network.

■ Organizations that need more than one public address typically purchase those addresses from their ISP as an address block. An address block is a complete group of addresses that share a network ID.

■ To handle questions about IP address blocks on the 70-291 exam, you should memorize the powers of 2 from 2^1 through 2^{12} and all of the possible values in a subnet mask.

■ The host capacity of a single-subnet network is always two fewer than the number of addresses in the network's address range.

Lesson 3: Subnetting IP Networks

By default, an address block such as 131.107.0.0/16 is designed to serve a single subnet or broadcast domain. You can, however, customize an address block by configuring hosts internal to your organization with a subnet mask that lengthens the network ID. This process generates multiple network IDs within your address space and is known as *subnetting*. Through subnetting, you can subdivide networks into distinct and separate groups.

After this lesson, you will be able to

- Manipulate subnet masks to configure subnets for a variety of network restrictions and needs
- Given any network address and subnet mask, determine the number of subnets and hosts available
- Determine an appropriate subnet mask given a requirement for a number of subnets or a number of subnets and hosts
- Determine whether two addresses are on the same subnet
- Describe the features and benefits of using variable-length subnet masks

Estimated lesson time: 90 minutes

What Is Subnetting?

Subnetting refers to the practice of logically subdividing a network address space by extending the string of 1-bits used in the subnet mask of a network. This extension enables you to create multiple subnets or broadcast domains within the original network address space.

For example, let's assume that from your ISP you have purchased the address block 131.107.0.0 /16 for use within your organization. Externally, the ISP then uses the /16 (255.255.0.0) subnet mask on its routers to forward to your organization IP packets (or *datagrams*) that have been addressed to *131.107.y.z*.

Let us then assume in a first scenario that within your organization you configure the subnet mask at its original 255.255.0.0 value on all internal hosts. In this case, all IP addresses within the address space, such as 131.107.1.11 and 131.107.2.11, for example, are logically seen by hosts to share the same network ID (131.107) and to belong to the same subnet. All hosts within this address space therefore attempt to communicate with one another by means of a broadcast. This configuration requires that internal to the network, only devices such as hubs, switches, and wireless bridges that do not block broadcasts can be used.

However, if in another scenario you decide to alter the subnet mask used within your organization to /24 or 255.255.255.0, internal hosts will read the addresses 131.107.1.11 and 131.107.2.11 as having different network IDs (131.107.1 vs. 131.107.2) and consider these addresses as belonging to different subnets. Whenever a host then attempts to send an IP datagram to a host on another subnet, it sends the datagram to its default gateway, at which address a router is responsible for forwarding the packet toward its destination.

For example, to communicate with each other, the hosts assigned the addresses 131.107.1.11/24 and 131.107.2.11/24 send IP packets to their respective default gateways, an address which must lie within broadcast range. The router owning the default gateway address is then responsible for routing the datagram toward the destination subnet. Hosts external to the organization continue to use the /16 subnet mask to communicate with hosts within the network.

Figure 2-5 and Figure 2-6 illustrate these two possible versions of the network.
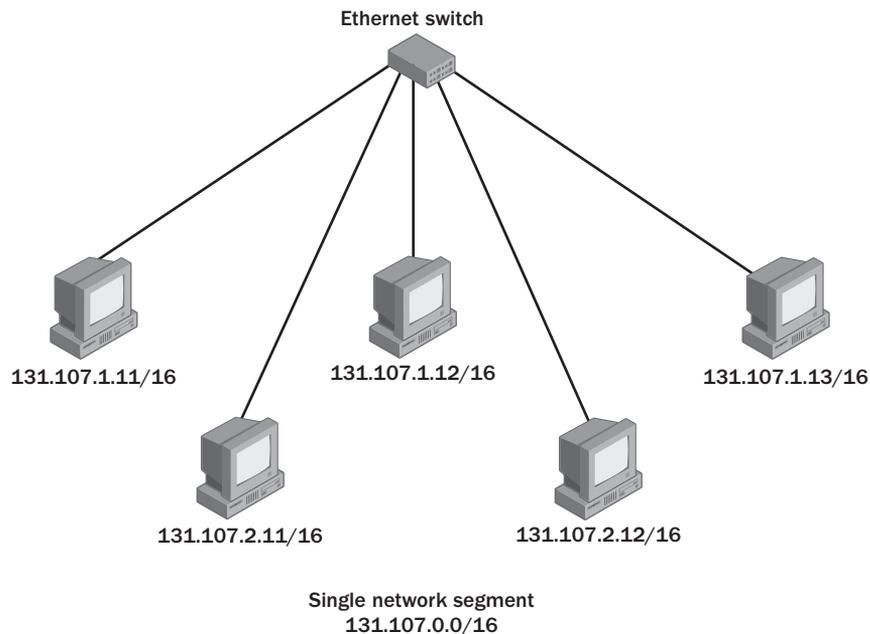
Figure 2-5   A /16 address space not subnetted
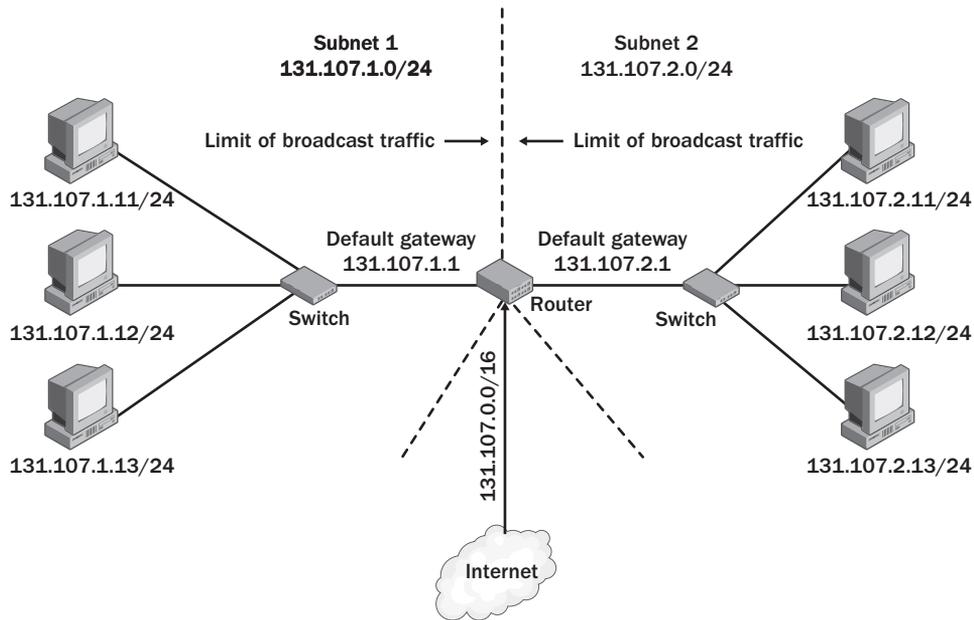
Figure 2-6   Subnetted /16 address space

Whereas the original /16 network address space in Figure 2-5 consisted of a single subnet including up to 65,534 (216 – 2) hosts, the new subnet mask configured in Figure 2-6 allows you to subdivide this original space into 256 (28) subnets with as many as 254 (28 – 2) hosts each.

Advantages of Subnetting

Subnetting is often used to accommodate a divided physical topology or to restrict broadcast traffic on a network. Other advantages of subnetting include improved security (by restricting unauthorized traffic behind routers) and simplified administration (by delegating control of subnets to other departments or administrators).

Accommodating Physical Topology

Suppose you are designing a campus network with 200 hosts spread over four buildings—Voter Hall, Twilight Hall, Monroe Hall, and Sunderland Hall. You want each of these four buildings to include 50 hosts. If your ISP has allocated to you the /24 network 208.147.66.0, you can use the addresses 208.147.66.1– 208.147.66.254 for your 200 hosts. However, if these hosts are distributed among four physically separate locations, the distances among them might be too great to allow the hosts to communicate with one another by means of a local network broadcast. By extending the subnet mask to /26 and borrowing 2 bits from the host ID portion of your address space, you can divide the network into four logical subnets. You can then use a router in a central location to connect the four physical networks. Figure 2-9 illustrates this scenario.

208.147.66.0/26
Subnet ID (in binary):00

Voter Hall

208.147.66.64/26   Router   208.147.66.128/26
Subnet ID (in binary):01   Subnet ID (in binary):10

Twilight Hall   Monroe Hall

Sunderland Hall

208.147.66.192/26
Subnet ID (in binary):11
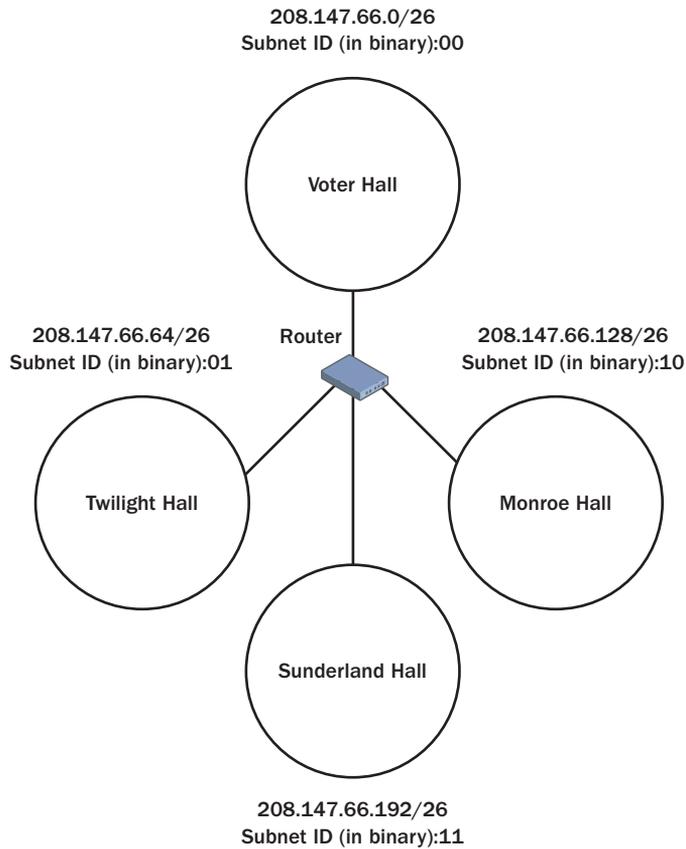
Figure 2-7   Subnetting in a divided physical topology

Restricting Broadcast Traffic

A *broadcast* is a network message sent from a single computer and propagated to all other devices on the same physical network segment. Broadcasts are resource-intensive because they use up network bandwidth and request the attention of every network adapter and processor on the LAN.

Routers block broadcasts and protect networks from becoming overburdened with unnecessary traffic. Because routers also define the logical limits of subnets, subnetting a network allows you to limit the propagation of broadcast traffic within that network.

Note   As a means to restrict broadcast traffic in large networks, virtual local area network (VLAN) switches are becoming an increasingly popular alternative to subnetting. Through VLAN software that integrates all the VLAN switches on the network, you can design broadcast domains in any manner, independently of the network's physical topology.

The Subnet ID

Every 32-bit IP address consists of a host ID and a network ID. When you obtain an address block from your ISP (or from your central network administrator in a multi-branch network), that address block contains a single network ID that cannot be changed. In other words, if you are given a /16 network, for example, the values of the first 16 bits of your address block are not configurable. It is only the remaining portion—the portion reserved for the host ID—that represents your configurable address space.

When you decide to subnet your network, you are essentially taking some of your configurable address space from the host ID and moving it to the network ID, as shown in Figure 2-8. This string of bits you use to extend your network ID internally within your organization (relative to the original address block) is known as the subnet ID.

External View

Network ID
(16 bits)   **Host ID**
                     (16 bits)

`1 0 1 0 1 1 0 0 0 0 0 0 1 0 0 0 0`

   172   16   0–255   0–255

Internal View

Network ID
(24 bits)   **Host ID**
                       (8 bits)

`1 0 1 0 1 1 0 0 0 0 0 0 1 0 0 0 0`

   172   16   0–255   0–255
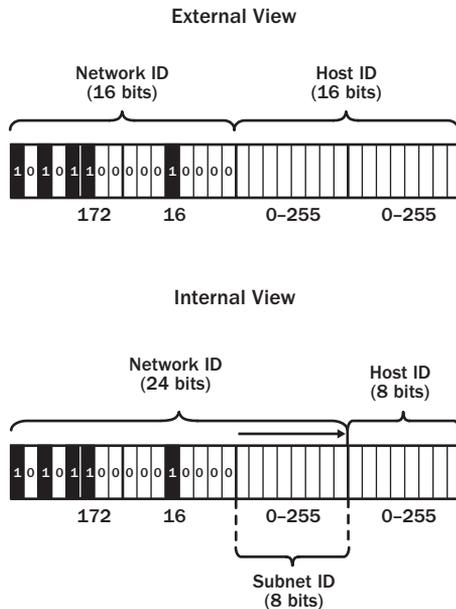
Subnet ID
(8 bits)

Figure 2-8 The subnet ID is taken from the host ID

The example provided in Figure 2-8 is easy to visualize and understand because both the original and modified subnet masks (/16 and /24) are divisible by 8. However, this is not always the case. For example, you might be granted a /23 address block whose address space you decide to subnet with a /26 subnet mask.

Determining the Number of Subnets

On the 70-291 exam, it is sometimes necessary to determine how many logical subnets have been created by a given subnet mask. Most often, this information is not sufficient by itself to answer a question correctly but is, nonetheless, an important component of the correct response.

To determine the number of subnets in a given network, use the formula:

$$s = 2^b$$

where s = the number of subnets and b = the number of bits in the subnet ID. To calculate the number of bits of the subnet ID, use the following formula:

$$b = n_{int} - n_{ext}$$

where n_{int} is the length (in bits) of the network ID used internally within the organization, and n_{ext} is the length of the original network ID assigned externally to the entire address block.

Here is an example. If you work in a large organization, a central network administrator at the office headquarters might grant you the 10.10.100.0/24 address block for use within your branch office. In this scenario, then, your n_{ext} = 24. If you decide to modify the subnet mask internally to /27, your n_{int} = 27. Therefore, b = 27 − 24 = 3, and s = 2^3 = 8. Therefore, by changing the subnet mask internally from /24 to /27 (255.255.255.224), you generate 8 subnets.

As we have just seen, calculating the number of subnets available is easy if we have been given the external and internal subnet mask values in slash notation. If you are given the subnet mask values in dotted-decimal notation, your best bet is to first translate those subnet masks to slash notation.

For example, if you have purchased a 255.255.252.0 address block from your ISP, you might decide to subnet the address space by using a subnet mask of 255.255.255.0 internally. Because 255.255.252.0 = /22 and 255.255.255.0 = /24, b = 24 − 22 = 2, and s = 2^2 = 4. Therefore, by changing the subnet mask internally from 255.255.252.0 to 255.255.255.0, you generate 4 subnets.

Tip   You might also be able to calculate the number of bits in the subnet ID simply through visualization. For example, you might see that 255.255.255.0 is 2 bits removed from 255.255.252.0. In this case, you know that b = 2, and you can simply move on to the formula s = 2^b.

Determining Hosts per Subnet

Determining the number of hosts per subnet is no different from determining the number of hosts per network, as covered in Lesson 2 of this chapter. Simply use the formula $c = 2^{(32-n)} - 2$, where c = number of computers or hosts that can be supported by the address range and n = the number of bits in the new, modified network ID.

It is important to remember that when you have subnetted your network, you should use the number of bits that you have allocated to the network ID *internally*. For example, if you have been granted a /24 address block for which you are using a subnet mask of /28 internally, then n = 28. Each subnet will therefore be able to accommodate $2^{32-28} - 2 = 2^4 - 2 = 16 - 2 = 14$ hosts.

Also remember that if you are dealing with an internal subnet mask in dotted-decimal notation whose value is between 255.255.255.0 and 255.255.255.255, you do not need to calculate the number of bits in the network ID to determine the number of hosts per subnet. Simply subtract the value of the last octet from 256, and then subtract 2. For example, if your internal subnet mask is 255.255.255.192, the number of hosts per subnet = 256 – 192 – 2, or 64 – 2, or 62.

Determining the Subnet Mask for a Required Number of Subnets

On the 70-291 exam, you will likely encounter a question in which you need to determine an appropriate subnet mask to be used within your organization when you are given a requirement for a specific number of subnets. With such questions, you are always given the original (external) subnet mask that belongs to the address block.

Exam Tip   If your only stated requirement were to determine a subnet mask that would generate enough subnets to suit your network needs (say 16), there would be nothing to stop you from choosing a subnet mask that would create 32, 64, 128 subnets or more. To avoid ambiguity, the exam usually states an additional requirement to "conserve network address space." This should be interpreted as a signal to choose a subnet mask that generates no more subnets than necessary.

To answer such questions, use the following step-by-step procedure:

1. Determine the number of bits (*b*) required in the subnet ID. To do so, assign the number of required subnets to the variable *t* and then determine the *lowest value of b* where the following is true:

   $2^b \geq t$

In other words, you need to find the lowest exponential value that, when applied to 2, yields a value that is greater than or equal to the number of subnets you need.

For example, let us suppose that you need to accommodate 15 subnets in your network. In this case, t = 15. Since 2^3 = 8 and 2^4 = 16, the lowest exponential value of b that yields a value equal to or greater than 15 is 4. Our b value, therefore, = 4.

The variable b stands for the number of bits in the *subnet* ID in the internal network. Our next step is to determine the number of bits to be used in the internal *network* ID.

2. If your original subnet mask has been provided in slash notation, proceed to the next step. Otherwise, skip to step 6.

3. Calculate n_{int} where n_{int} = n_{ext} + b

   In this equation, n_{int} stands for the number of bits used in the network ID internally, and n_{ext} stands for the number of bits assigned externally to the address block.

   For example, if your address block has an original subnet mask of a /24, your n_{ext} = 24. If you have determined that you need to allocate 4 bits to the subnet ID, then your b = 4. In this case, n_{int} = 24 + 4, or 28.

4. Put a slash before the n_{int}, and if slash notation suffices for your final answer, you're done. If slash notation is not sufficient, convert your subnet mask from slash notation to dotted-decimal notation. (You should be able to perform this conversion in your head fairly easily. If you are unable to do so, review Lesson 2 in this chapter.)

5. (From Step 2). If your original subnet mask has been provided in dotted-decimal notation, use your knowledge of the sequence of possible subnet mask values (corresponding to an ascending order from /8 to /30) to determine the subnet mask value that is *b* bits removed from and after the original. For example, if your original subnet mask is 255.255.255.0 and b = 3, your subnet mask is 255.255.255.224 because in the ascending order of subnet mask values, that is the subnet mask that is 3 bits removed from and after 255.255.255.0. (For a visual representation of this sequence, see Table 2-1, "Subnet Mask Notations Compared.")

   If you are unable to perform this calculation easily in your head, simply convert the subnet mask to slash notation, and go back to Step 3.

6. If dotted-decimal notation is sufficient for your final answer, you're done. If dotted-decimal notation is not sufficient, convert your subnet mask from dotted-decimal notation to slash notation. (You should be able to perform this conversion in your head fairly easily. If you are unable to do so, review Lesson 2 in this chapter.)

Determining the Subnet Mask for a Required Number of Subnets and Computers

For some exam questions, you might be asked to determine an internal subnet mask when you are given the external subnet mask of the address block, the required number of subnets, and an additional piece of information—the maximum number of computers per subnet. If this is the case, simply use the additional information (the maximum number of computers per subnet) as a way to double-check your answer.

If, for example, you are asked to calculate a new subnet mask for a /22 address block that will allow 20 subnets and 25 computers per subnet, first calculate the subnet mask needed for 20 subnets. (To accommodate 20 subnets, you will need 5 bits in the subnet ID; therefore, your new subnet mask should be /22+5, or /27.)

After you obtain this information, determine the number of hosts per subnet given the new subnet mask. In this case, $c = 2^{(32-27)} - 2 = 2^5 - 2 = 32 - 2 = 30$. Since this value is sufficient to meet the required number of hosts per subnet, the calculation of your new subnet mask is correct.

Determining Address Block Size

You might also be asked to determine the address block size you will need to satisfy requirements for a certain number of subnets and computers. In this case, use procedures described elsewhere in this chapter to determine b, the number of bits in the subnet ID, and h, the number of bits in the host ID. With these values, determine the length in bits of the external network ID (n_{ext}) by using the following equation.

$n_{ext} = 32 - (b + h)$

Put a slash before your value of n_{ext}, and you're done. (Convert the subnet mask to dotted-decimal if you need to.)

For example, if you need to support 60 subnets of 120 hosts apiece, $b = 6$ and $h = 7$. By using the equation, we can determine that $n_{ext} = 32 - (6 + 7) = 32 - 13 = 19$. Therefore, we will need a /19 address block to accommodate 60 subnets of 120 hosts apiece. (If you then need to convert the subnet mask to dotted-decimal notation, do so.)

> **Exam Tip**   On the exam, the correct subnet mask never provides more subnets or hosts than necessary.

Estimating Subnet Address Ranges

When you look at the subnet mask used internally within a subnetted network, it is important that you be able to estimate the address ranges of the various subnets in

your head whenever possible. The key to performing this estimate is to convert the subnet mask to dotted-decimal notation.

Estimating Subnet Ranges—Basic Level

If both the subnet mask assigned externally to the entire address block and the subnet mask used internally consist only of octets whose value is either 255 or 0, there should be no confusion about the subnet address ranges. In this case, one full octet will be dedicated to the subnet ID. The value of this octet/subnet ID will increment by 1 as the rightmost octet(s) range from 0-255, as shown in Table 2-6 below:

Table 2-6   Subnet Address Ranges for Basic Subnetting Scenarios

Original Subnet Mask (assigned to entire address block)	Internal Subnet Mask (used for creating subnets)	Subnet Address Ranges (example)
255.0.0.0	255.255.0.0	10.0.0.0 – 10.0.255.255, 10.1.0.0 – 10.1.255.255, 10.2.0.0 – 10.2.255.255, etc.
255.255.0.0	255.255.255.0	172.16.0.0 – 172.16.0.255, 172.16.1.0 – 172.16.1.255, 172.16.2.0 -172.16.2.255, and so on

Estimating Subnet Ranges—Intermediate Level

In many scenarios on the exam and in the real world, the original subnet mask will be 255.255.0.0 or 255.255.255.0, and the internal subnet mask will include a mid-range value octet. For example, you might work with a /24 (255.255.255.0) address block that you have subnetted as /26 (255.255.255.192), or you might be given a /16 (255.255.0.0) network that you have subnetted as /20 (255.255.240.0).

In such cases, the key to estimating the subnet address ranges is to use the value of the internal subnet mask's mid-range value octet. Specifically, subtract the value of the mid-range value octet from 256 to obtain the grouping value for the subnets. For example, if you have subnetted a /24 (255.255.255.0) network as /26 (255.255.255.192), your grouping value is 256-192 = 64. If you have subnetted a /16 (255.255.0.0) network as /20 (255.255.240.0), your grouping value is 256-240=16.

This grouping value determines the starting point of each subnet address block. For example, if you have subnetted your 192.168.100.0/24 address as 192.168.100.0 /26 and your grouping (g) value is 64, each subnet address range will thus begin with a multiple of 64, *including 0*. The subnet address ranges will then naturally be formed in *groups of 64 addresses*, as shown below:

192.168.100.**0** – 192.168.100.63,

192.168.100.**64** – 192.168.100.127,

192.168.100.**128** – 192.168.100.191,

192.168.100.**192** – 192.168.100.255,

If you have subnetted a 10.100.0.0/16 network as /20 and your grouping (g) value is 16, the multiples of *g* (including 0) again define the starting point of each address range. And again, these multiples appear in the octet whose position corresponds to the mid-range value octet in the subnet mask, which, in this case is the third octet. The value of the rightmost octet then ranges from 0 – 255, as shown below:

10.100.**0**.0 – 10.100.15.255,

10.100.**16**.0 – 10.100.31.255,

10.100.**32**.0 – 10.100.47.255,

10.100.**48**.0 – 10.100.63.255,

and so on.

> **Off the Record**   Although you need to know how to perform these calculations for the exam, most sysadmins avoid doing so on the job. Administrators who need to determine subnet-related information typically use what is called a *subnet calculator* or *network calculator*. You can download many of these utilities for free, and some even operate directly from Web pages. Typically, subnet calculators allow you to enter some addressing requirements, such as a network address and number of hosts per subnet, and then automatically calculate the rest of the addressing information for you. This information can include the appropriate subnet mask, the number of subnets, the subnet address ranges, and the subnet broadcast addresses.

Estimating Subnet Ranges—Advanced Level

It is unlikely—though possible—that on the 70-291 exam you will need to determine the address ranges for a network whose original address block size is between /17 and /23 and that you have subnetted as /24. For example, you might encounter a question in which you are given a 172.16.128.0 /21 (255.255.248.0) address block that you have subnetted as 172.16.128.0 /24 (255.255.255.0).

The difference in this method is that the *g* value actually represents the number of subnets. In this case, g = 256-248=8, so the complete range of addresses will include 8 subnets. To determine the address ranges in those subnets, begin with the original value

of the third octet in the network address and then *increment that value by one* in each of the remaining subsequent ranges, as shown below:

172.16.**128**.0 – 172.16.128.255,

172.16.**129**.0 – 172.16.129.255,

172.16.**130**.0 – 172.16.130.255,

and so on.

For subnetting scenarios of this type, remember that the highest value of the third octet value will be the original value plus (g-1). In our scenario, the highest value of the third octet will thus be 128 + (8-1) = 128 + 7 = 135.

Estimating Subnet Ranges—Expert Level

It is very unlikely that you will need to determine address ranges for a network in which both the original address block and the subnetted version of the network contain subnet masks with a mid-range value octet.

For example, you will probably not ever need to estimate the subnet address ranges for a 172.16.100.128 /26 (255.255.255.192) network that you have subnetted with a /29 (255.255.255.248) subnet mask. In the real world, you will most likely use a subnet calculator such a problem, and on the 70-291 exam you will not likely see a question in which such a calculation is necessary.

If you do need to make such a calculation, however, use the following procedure:

First, in the network address of the entire address block, use the value of the octet whose position corresponds to the mid-range value octet in the subnet mask *to determine the starting point of the subnet ranges*. In our example, the value 128 in the address 172.16.100.128 corresponds to the position of the mid-range value octet in our external subnet mask 255.255.255.192.

Then, determine the grouping value by using the internal subnet mask as you would if you were subnetting from /16 or /24. In our example, the subnet mask of the subnetted network is 255.255.255.248, so our grouping value is 256-248 = 8. This grouping value will act as our increment in each successive subnet range after the first, as in the following pattern:

172.16.100.**128** – 172.16.100.135

172.16.100.**136** – 172.16.100.143

172.16.100.**144** – 172.16.100.151

172.16.100.**152** – 172.16.100.159

Remember not to exceed 2^b subnets, where b = the number of bits in the subnet ID. Since in our current example we are subnetting from /26 to /29, there are 3 bits in the subnet ID, and there will be a total of 2^3 or 8 subnets.

Subnetting Through Octets

The most difficult subnet address range calculation to make—and the one you are least likely to need to make on the 70-291 exam—is for a scenario in which the subnet masks of the original and subnetted networks have a mid-range value octet in third and fourth octet positions, respectively. For example, you will almost certainly not need to determine the address ranges of a 192.168.64.0 /23 (255.255.254.0) address block that you have subnetted as 192.168.64.0 /25 (255.255.255.128). However, this information is provided here for completeness.

To solve this type of problem, use three steps. First, use the procedure described in the "Advanced Level" section to determine the first three octets of your address ranges as if you were subnetting *from* your original (for example, /23) network *to* an internal subnet mask of /24 (255.255.255.0).

Subnetting from /23 to /24:

192.168.64.0 – 192.168.64.255,

192.168.65.0 – 192.168.65.255

Then use the procedure described in the "Intermediate Level" section to determine the last octet of your subnet address ranges as if you were subnetting *from* /24 (255.255.255.0) *to* your eventual target (for example, /26 or 255.255.255.128).

Subnetting from /24 to /25:

192.168.64.0 – 192.168.64.127,

192.168.64.128 – 192.168.64.255

Finally, for each three-octet block in the first group, add all the ranges for the last octet value in the second group, as shown in the following example:

Subnetting from /23 to /25:

192.168.64.0 – 192.168.64.127,

192.168.64.128 – 192.168.64.255,

192.168.65.0 – 192.168.65.127,

192.168.65.128 – 192.168.65.255

Remember not to exceed 2^b subnets, where b = the number of bits in the subnet ID. Since, in our current example, we are subnetting from /23 to /25, there are 2 bits in the subnet ID, there will be a total of 2^2 or 4 subnets. In other words, in this case we have written out the complete list of subnet address ranges.

Determining Whether Two Addresses Are on the Same Subnet

When the subnet mask used by a network is /8, /16, or /24, you can determine whether any two addresses are on the same subnet simply by comparing the values of the first 1, 2, or 3 octets, respectively.

However, when your subnet mask has a mid-range value octet such as 192 or 248, determining whether two addresses are on the same subnet requires a brief calculation, as described in the following procedure:

1. Convert the subnet mask to dotted-decimal notation (if necessary).

2. Where *d* = the value of the mid-range value octet in the subnet mask and *k1* and *k2* = the respective values of the octets in each IP address whose position corresponds to *d,* calculate the value of *f1* and *f2* according to the following formulas:

   $f_1 = [k_1 \div (256\text{-}d)]$ – any remainder

   $f_2 = [k_2 \div (256\text{-}d)]$ – any remainder

> **Tip**   Notice how the term 256-d used in these formulas corresponds to the grouping value (g) used in the previous section, "Estimating Subnet Address Ranges."

For example, if our subnet mask is 255.255.252.0 and the two IP addresses we are comparing are 192.168.100.200 and 192.168.103.203, d = 252, k_1 = 100, and k_2 = 103. According to the first formula, f_1 = 100 ÷ (256-252) = 100 ÷ 4 = 25. According to the second formula, f_2 = 103 ÷ (256-252) = 103 ÷ 4 = 25 (without the remainder).

3. If f1 = f2, the two addresses are found on the same subnet. If f1 does not equal f2, the two addresses are found on different subnets.

   In our example, both f_1 and f_2 = 25. Therefore, the addresses 192.168.100.200 and 192.168.103.203 are found on the same subnet when they use the subnet mask 255.255.252.0.

> **Exam Tip**   It is likely that you will need to use this procedure on the exam. Don't hesitate to use the exam's built-in calculator to help you perform the arithmetical operation.

Using Variable-Length Subnet Masks

Throughout this lesson, we have been exploring scenarios in which one subnet mask is used externally for an address block and another subnet mask is used internally within the actual network. However, a more complicated scenario is also possible in which one subnet mask is used externally and *multiple subnet masks* are used internally. This practice can allow you to use your network address space more efficiently.

Exam Tip   It is highly unlikely that you will need to *calculate* variable-length subnet masks on the 70-291 exam. However, you should not be surprised to notice subnet masks of various lengths used in question scenarios. It is for this reason alone that this topic is covered here.

For example, if your /24 address block needs one subnet to accommodate 100 computers, a second subnet to accommodate 50 computers, and a third subnet to accommodate 20 computers, this arrangement cannot be designed with traditional subnet mask options. As Table 2-7 shows, any single default mask fails to accommodate either enough subnets or enough hosts per subnet to meet all your network needs.

Table 2-7   Traditional Options for Subnetting a /24 Address Block

Network Address	Subnets	Hosts per Subnet
Internal subnet mask: 255.255.255.0	1	254
Internal subnet mask: 255.255.255.128	2	126
Internal subnet mask: 255.255.255.192	4	62
Internal subnet mask: 255.255.255.224	8	30

In situations such as these, you can assign different subnet masks to different subnets. This will allow you to accommodate your specific network needs without having to acquire new address space from your ISP.

Figure 2-9 illustrates how you can use subnet masks of various lengths to accommodate three subnets of 100, 50, and 20 hosts, respectively. This particular network configuration will allow for up to four more subnets to be added later.
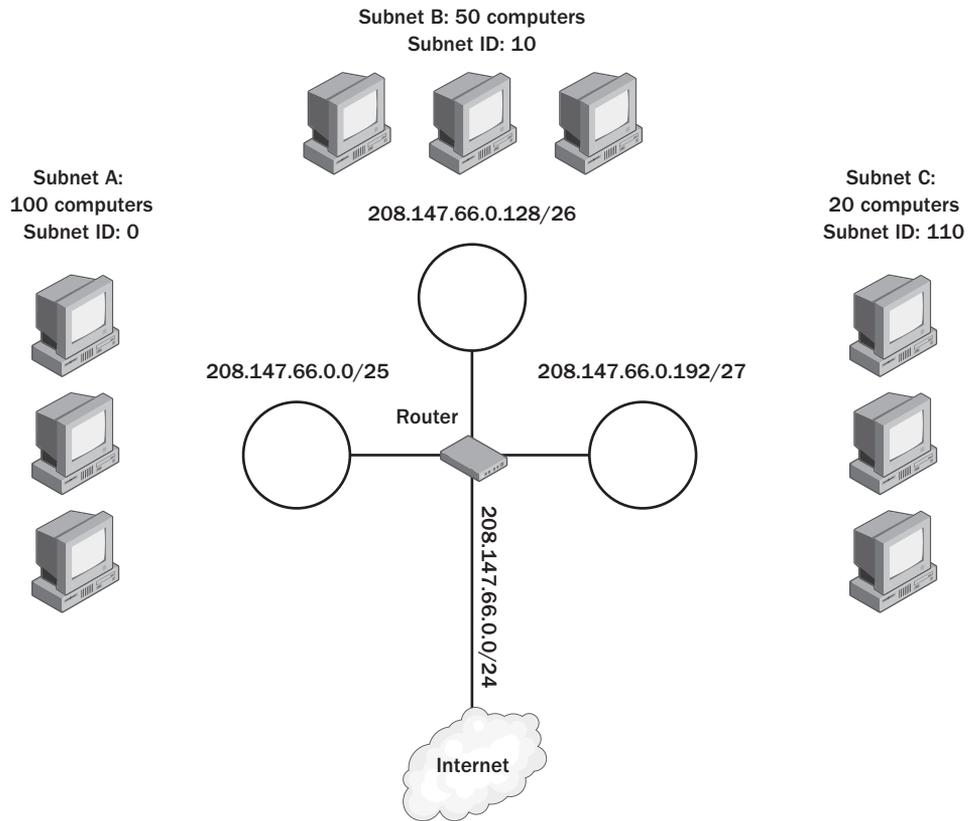
Figure 2-9   Using variable-length subnet masks for flexible subnetting

When using variable-length subnet masks to divide your network into subnets of vary-ing sizes, a *specific pattern* of subnet IDs with trailing 0s must be used, up to a maxi-mum of seven subnets for a /24 address block. These trailing 0s prevent the subnet address spaces from overlapping with each other. When the subnet IDs with variable-length subnet masks are fixed in the specific pattern shown in Table 2-8, subnets do not overlap, and addresses are interpreted unambiguously.

Table 2-8   Variable-length Subnet IDs

Subnet Number	Subnet ID (Binary)	Subnet Mask	Hosts per Subnet	Example Subnet Address
1	0	255.255.255.128	126	208.147.66.0.0/25
2	10	255.255.255.192	62	208.147.66.0.128/26
3	110	255.255.255.224	30	208.147.66.0.192/27
4	1110	255.255.255.240	14	208.147.66.0.224/28
5	11110	255.255.255.248	6	208.147.66.0.240/29
6	111110	255.255.255.252	2	208.147.66.0.248/30
7	111111	255.255.255.252	2	208.147.66.0.252/30

Maximizing Available Address Space

In Table 2-8, notice that the seventh and final subnet listed is the same size as the sixth and is distinguished by an all-1s subnet ID instead of by the trailing 0s used with the other subnet IDs. As an alternative to using the maximum 7 subnets presented, you could define the all-1s subnet ID at any level in the table to replace all the subnets listed below that subnet.

For example, you could define a subnet ID of 11 to replace subnets 3 through 7 listed in the table. Doing so would give you an additional subnet of 62 hosts, instead of 5 other subnets accommodating a total of 54 hosts. This technique thus allows you to maximize the number of hosts your 3-subnet network can accommodate.

This three-subnet scenario is presented in Figure 2-10.
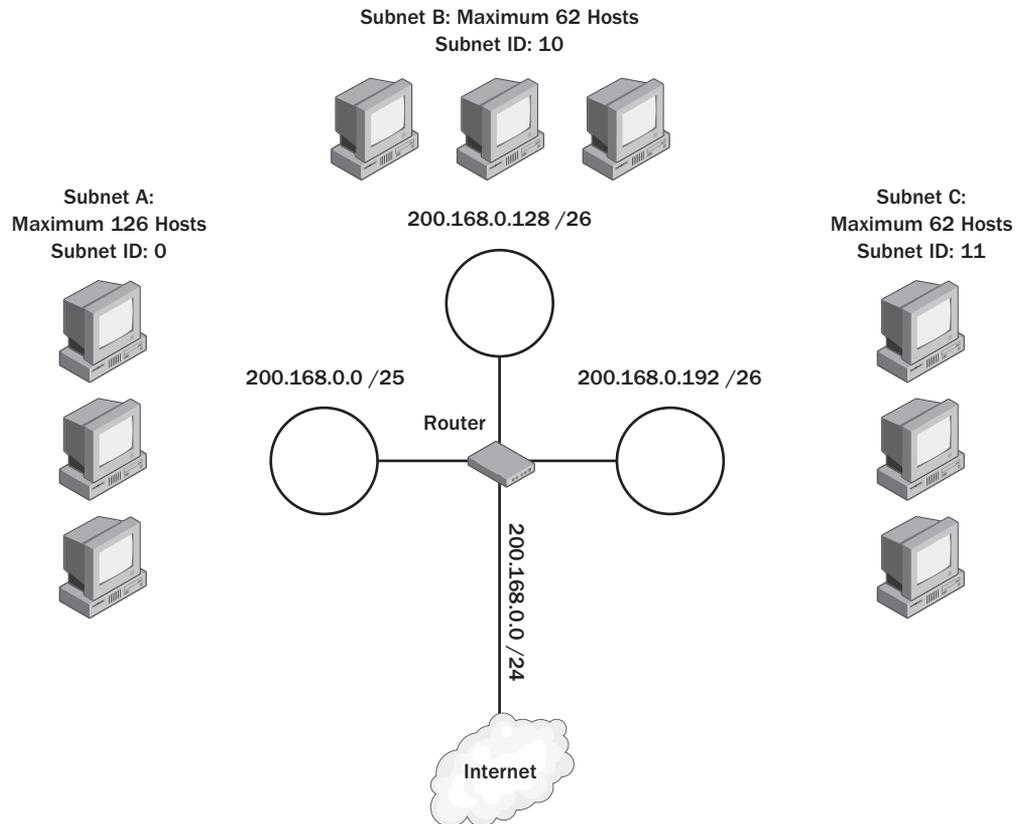
Figure 2-10   Maximizing address space in a 3-subnet network

Practice: Working with Subnet Masks and Subnets

In this practice, use the methods described above to determine the missing subnet information.

Exercise 1: Calculate Subnet Masks

Assume that your ISP has allocated you the network address 206.73.118.0/24. Using the requirement shown at the top of the table, complete the table by determining the number of bits required for the subnet ID or host ID, the number of bits left for the host ID or subnet ID, the slash notation version of the subnet mask, and then the dotted-decimal version of the subnet mask.

Example: Requirement = 6 subnets

Number of bits required for subnet ID	3
Number of bits left for host ID	5
Slash notation version of subnet mask	/27
Dotted-decimal version of subnet mask	255.255.255.224

Requirement = 9 subnets

Number of bits required for subnet ID	
Number of bits left for host ID	
Slash notation version of subnet mask	
Dotted-decimal version of subnet mask	

Requirement = 3 subnets

Number of bits required for subnet ID	
Number of bits left for host ID	
Slash notation version of subnet mask	
Dotted-decimal version of subnet mask	

Requirement = 20 hosts per subnet

Number of bits required for host ID	
Number of bits left for subnet ID	
Slash notation version of subnet mask	
Dotted-decimal version of subnet mask	

Exercise 2: Calculate Various Subnet Information

For each address block and internally configured subnet mask, determine the number of available subnets and hosts per subnet. (Hint: First convert the internally configured subnet mask to slash notation.)

Original Address Block	Internally Configured Subnet Mask	Number of Available Subnets	Number of Available Hosts per Subnet
207.209.68.0 /27	255.255.255.240		
131.107.0.0 /20	255.255.255.0		
10.0.0.0 /13	255.255.240.0		
208.147.66.0 /25	255.255.255.248		

Exercise 3: Estimate Subnet Address Ranges

In this exercise, you estimate subnet address ranges by determining the ranges of the first three subnets within a subnetted network. For each address block given in column A, subtract from 256 the value of the mid-range value octet given in the subnet mask in column B. List this value as the grouping value in column C. Then, beginning with 0, list the first four multiples of this same value in column D. Use these values to complete columns E and F, as shown in the example given.

(A) Original Address Block	(B) Internally Configured Subnet Mask	(C) Grouping Value	(D) First Four Multiples of C (Including 0)	(E) Beginning Address of First Three Subnet Ranges	(F) Ending Address of First Three Subnet Ranges
10.0.0.0 /8	255.240.0.0	256 – 240 = 16	0, 16, 32, 48	10.0.0.0, 10.16.0.0, 10.32.0.0	10.15.255.255, 10.31.255.255, 10.47.255.255
172.16.0.0 /16	255.255.224.0				
172.18.0.0 /16	255.255.248.0				
192.168.1.0 /24	255.255.255.192				

Exercise 4: Determine Whether Two Addresses Are on the Same Subnet

Using the method in this lesson above, complete the following table. Feel free to use a calculator. The first row is provided as an example.

Subnet Mask	Address #1	Result Of Division Operation	Address #2	Result of Division Operation	Same Subnet?
255.255.255.192	192.168.1.116	116 / (256- 192) = 116 / 64 = 1	192.168.1.124	124 / 64 = 1	YES
255.255.255.224	192.168.0.180		192.168.0.192		
255.255.252.0	172.16.100.234		172.16.98.234		
255.255.240.0	172.16.64.10		172.16.72.200		
255.255.255.192	10.10.10.32		10.10.10.63		
255.255.255.240	192.168.10.18		192.168.10.15		
/27	192.168.10.31		192.168.10.32		
/25	10.1.1.250		10.1.1.128		
/29	172.16.100.248		172.16.100.252		
/23	10.0.0.1		10.0.1.1		
/21	10.10.8.100		10.10.7.100		

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the "Questions and Answers" section at the end of this chapter.

1. You are a new network administrator for Contoso, Inc. Contoso headquarters are located in Albany, but your branch office is located in Binghamton. The central administrator at headquarters has provided the Binghamton branch with the 192.168.10.0/24 address block, and you have noticed that hosts at the local branch are all configured with a subnet mask of 255.255.255.192. How many subnets are enabled by the locally configured subnet mask?

    a. 4

    b. 8

    c. 16

    d. 32

2. How many hosts are available per subnet in the Binghamton branch network described in the previous question?

    a. 6

    b. 14

    c. 30

    d. 62

3. You are the network administrator for the Albany branch office of Contoso, Inc. A year ago, from the central IT department at the New York headquarters, you obtained for use in the Albany office an address block that you have currently divided into 5 subnets, with a maximum of 20 computers per subnet. In the next year, you plan to add 3 more subnets to the branch office. You want to allow enough address space for any subnet to support up to 50 hosts, and you also want to have the flexibility of using a single address block for the entire Albany office network. You need to approach the central IT department about obtaining enough address space for your network. What size address block should you ask for?

    a. /20

    b. /21

    c. /22

    d. /23

4. You have obtained the 192.168.0.0/20 address block from a central network administrator. Within your network, you want the addresses 192.168.3.1 and 192.168.4.1 to belong to the same subnet, but you also want to maximize the number of subnets available. Which subnet mask should you configure within your organization?

    a. /20

    b. /21

    c. /22

    d. /23

5. When is it desirable to use subnet masks of various lengths within your organization?

Lesson Summary

■ Subnetting refers to the practice of logically subdividing a network address space by extending the string of 1-bits used in the subnet mask of a network. This extension enables you to create multiple subnets or broadcast domains within the original network address space.

■ Subnetting can be used to accommodate a divided physical topology, to restrict broadcast traffic on a network, to improve security, and to simplify network administration.

■ This string of bits you use to extend your network ID internally within your organization (relative to the original address block) is known as the subnet ID.

- To determine the number of subnets in a given network, use the formula $s = 2b$, where s = the number of subnets and b = the number of bits in the subnet ID.

- To determine the number of hosts per subnet, use the formula $c = 2^{(32-n)} - 2$, where c = the number of computers that a subnet can accommodate and n = the number of bits used in the network ID *internally* within the network.

Case Scenario Exercise

You work as a network consultant, and you have been hired by three companies to solve problems related to network connectivity. While visiting each company, you draw sections of the relevant portions of the network. Use the following drawings to determine the IP configuration error that has led to a disruption of network connectivity at each company.

1. What is the configuration error?

2. What is the configuration error?

Client A
IP address: 192.168.2.178/27
Default gateway: 192.168.2.177

Hub

Client B
IP address: 192.168.2.180/27
Default gateway: 192.168.2.177

192.168.2.177/27   207.209.68.1/24

Hub

Internet

Client C
IP address: 192.168.2.164/27
Default gateway: 192.168.2.161

Router/Firewall

192.168.2.161/27

Client D
IP address: 192.168.2.165/27
Default gateway: 192.168.2.161

3. What is the configuration error?

Client A
IP address: 131.107.63.1/21
Default gateway: 131.107.56.1

Client B
IP address: 131.107.62.1/21
Default gateway: 131.107.56.1

Hub

131.107.56.1/21   131.107.8.1/24

Hub

Internet

Router/Firewall

Client C
IP address: 131.107.127.1/21
Default gateway: 131.107.120.1

131.107.120.1/21

Client D
IP address: 131.107.128.1/21
Default gateway: 131.107.120.1
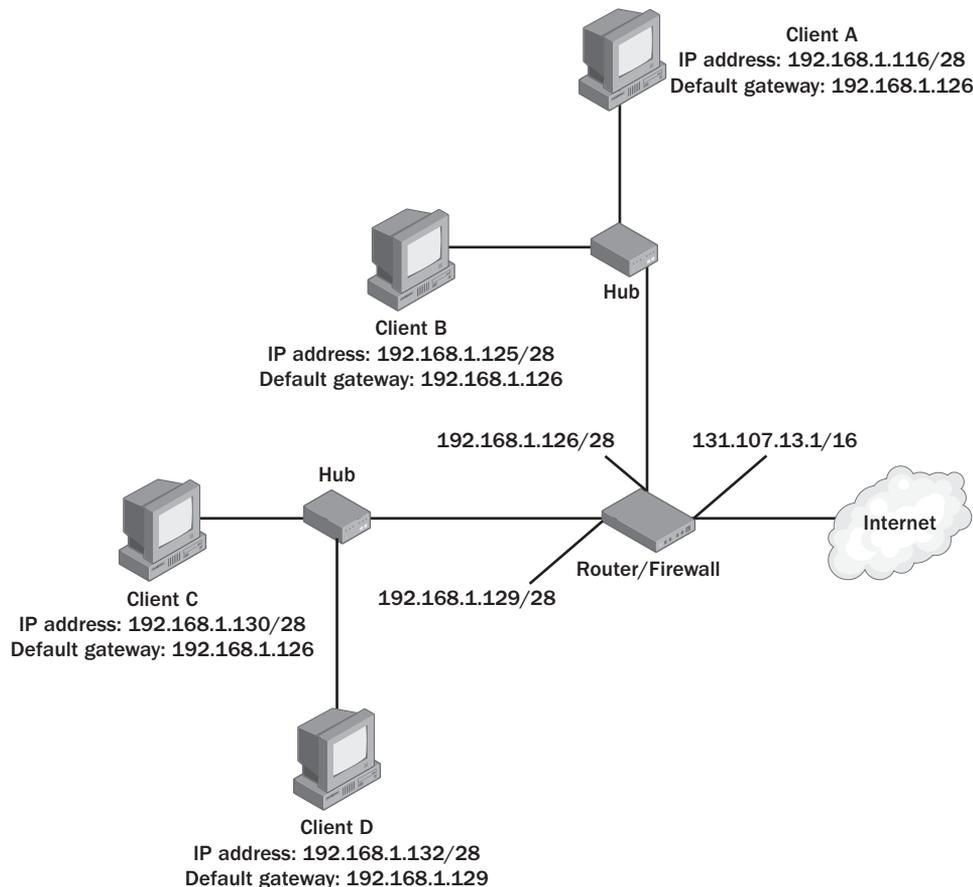
Chapter Summary

- TCP/IP provides the networking foundation for Windows networks and for the Internet. TCP includes the internet-layer protocols ARP, IP, and ICMP and the transport-layer protocols TCP and UDP.

- Host IP addresses need to be unique on every IP network.

- The first part of an IP address is always used as a network address or network ID, and the last part is used as a host address or host ID.

- The subnet mask is used to determine which part of an address should be considered the network ID and which part should be considered the host ID.

- To determine the number of hosts that can be accommodated by a given network, calculate $2^h - 2$, where h = the number of bits in the host ID.

- Multiple logical subnets of a network can be created when the network ID assigned externally to an address block is extended for use internally within an organization.

Exam Highlights

Before taking the exam, review the key points and terms that are presented below to help you identify topics you need to review. Return to the lessons for additional practice, and review the "Further Reading" sections in Part 2 for pointers to more information about topics covering the exam objectives.

Key Points

- Know the function of the Arp command.

- Know the ports associated with the following protocols: FTP, HTTP, DNS, SSL, PPTP, and IPSec

- Memorize the values of 2^1 to 2^{12}, along with all the possible values of a subnet mask octet (in sequence), before you take the exam.

- Be comfortable performing the following tasks in your head:

  ❏ Converting between the slash notation and dotted-decimal notation of a subnet mask

  ❏ Determining the host capacity of a network

  ❏ Determining the number of subnets per network

  ❏ Determining the appropriate subnet mask for an address block given a required number of hosts, subnets, or both

- Be able to estimate the subnet address ranges of a network by looking at the dotted-decimal form of its subnet mask.

- Be able to determine whether two addresses are found on the same subnet.

- Be able to spot configuration errors such as an incorrect default gateway or an incompatible IP address.

Key Terms

Address Resolution Protocol (ARP)   In TCP/IP, a protocol that uses broadcast traffic on the local network to resolve a logically assigned IP address to its physical hardware or MAC layer address.

Internet Control Message Protocol (ICMP)   A required maintenance protocol in the TCP/IP suite that reports errors and allows simple connectivity; the Ping utility uses ICMP to perform TCP/IP troubleshooting.

Host ID   The portion of the IP address that identifies a particular host within a newtork.

Network ID   The portion of the IP address that identifies a particular network.

broadcast domain   A physical portion of a network in which all network devices receive messages sent to the broadcast address of 255.255.255.255.

Questions and Answers

Lesson 1 Review

1. Which is the only layer of the TCP/IP reference model that does not contain any TCP/IP protocols?

    a. The network interface layer

    b. The internet layer

    c. The transport layer

    d. The application layer

    a

2. Which of the following TCP/IP protocols does not function at the internet layer?

    a. IP

    b. ARP

    c. TCP

    d. ICMP

    c

3. Which of the following is a transport-layer protocol?

    a. IGMP

    b. UDP

    c. DNS

    d. Ethernet

    b

4. Which of the following services connect to UDP ports? (Choose all that apply.)

    a. NetBIOS

    b. DNS

    c. Ethernet

    d. Telnet

    a, b

Lesson 2, Practice, Exercise 1

1. Which subnet mask would you assign to the new server?

Subnet 1:Existing computers

10.2.12.1

10.2.41.23

10.2.41.100

10.2.41.101

---

   a. 255.0.0.0 (/8)

   b. 255.255.0.0 (/16)

   c. 255.255.255.0 (/24)

b

2. Which subnet mask would you assign to the new server?

Subnet 2: Existing computers

192.168.34.1

192.168.34.55

192.168.34.223

192.168.34.5

---

   a. 255.0.0.0 (/8)

   b. 255.255.0.0 (/16)

   c. 255.255.255.0 (/24)

c

Lesson 2, Practice, Exercise 2

Complete the table below by providing the lowest value that is a power of 2 (p value) and that is *equal to or greater than* each of the values in the left column. Then, provide the exponential value of 2 (h value) associated with the each p value.

Value	p value	h value (exponent of 2)
40	64	6
312	512	9
1544	2048	11

Value	p value	h value (exponent of 2)
20	32	5
96	128	7
1	2	1
12	16	4
600	1024	10
150	256	8
3	4	2
2500	4096	12
6	8	3
64	64	6
10	16	4
1775	2048	11
103	128	7
17	32	5
255	256	8
3242	4096	12

Lesson 2, Practice, Exercise 3

Complete the table below by providing the correct binary notation, r value, and d value as shown in the example provided in the first line.

Binary Value	Number of 1-bits (r value)	Decimal value (d value)
11111100	6	252
11000000	2	192
11111000	5	248
11111110	7	254
11100000	3	224
11111111	8	255
11110000	4	240
00000000	0	0
10000000	1	128
11100000	3	224
11000000	2	192
11111000	5	248
11111110	7	254
10000000	1	128
11111100	6	252

Binary Value	Number of 1-bits (r value)	Decimal value (d value)
11110000	4	240
11111111	8	255
11111110	7	254
11100000	3	224
10000000	1	128
11110000	4	240
11000000	2	192
11111000	5	248
11111100	6	252

Lesson 2, Practice, Exercise 4

Convert the following subnet masks in slash notation to dotted-decimal in your head by using memorizations from Table 2-5 and the steps described in the earlier section, "Converting Subnet Mask Notations."

Slash Notation	Dotted-Decimal Notation
/18	255.255.192.0
/28	255.255.255.240
/21	255.255.248.0
/30	255.255.255.252
/19	255.255.224.0
/26	255.255.255.192
/22	255.255.252.0
/27	255.255.255.224
/17	255.255.128.0
/20	255.255.240.0
/29	255.255.255.248
/23	255.255.254.0
/25	255.255.255.128

Lesson 2, Practice, Exercise 5

Use the steps described above to convert the subnet masks in dotted-decimal notation to slash notation in your head.

Dotted-Decimal Notation	Slash Notation
255.255.240.0	/20
255.255.255.248	/29
255.255.192.0	/18
255.255.255.128	/25
255.255.248.0	/21
255.255.255.224	/27
255.255.252.0	/22
255.255.128.0	/17
255.255.255.252	/30
255.255.224.0	/19
255.255.254.0	/23
255.255.255.192	/26
255.255.255.240	/28

Page
2-27

Lesson 2, Practice, Exercise 6

For each of the given address blocks below, determine in your head the number of hosts that can be supported.

Address Block	Number of Supported Hosts (c value)
131.107.16.0 /20	4,094
10.10.128.0 Subnet mask: 255.255.254.0	510
206.73.118.0 /26	62
192.168.23.64 Subnet mask: 255.255.255.224	30
131.107.0.0 Subnet mask: 255.255.255.0	254
206.73.118.24 /29	6
10.4.32.0 /21	2046
172.16.12.0 /22	1022
192.168.1.32 Subnet mask: 255.255.255.128	126
131.107.100.48 /28	14
206.73.118.12 Subnet mask: 255.255.255.252	2

Address Block	Number of Supported Hosts (c value)
10.12.200.128 /25	126
192.168.0.0 Subnet mask: 255.255.248.0	2046
172.20.43.0 /24	254
131.107.32.0 Subnet mask 255.255.255.240	14
10.200.48.0 Subnet mask: 255.255.240.0	4094
192.168.244.0 /23	510
10.0.0.0 /30	2
172.31.3.24 Subnet mask: 255.255.255.248	6
206.73.118.32 /27	30
131.107.8.0 Subnet mask: 255.255.252.0	1022
192.168.0.64 Subnet mask: 255.255.255.192	62

Lesson 2, Practice, Exercise 7

Each of the values in the left column of the table below refers to a number of computers that a given network must support. In the corresponding space in the right column, specify with a subnet mask in slash notation the smallest network size that will accommodate those computers.

Number of Network Hosts	Subnet Mask (/n)
125	/25
400	/23
127	/24
650	/22
7	/28
2000	/21
4	/29
3500	/20
20	/27
32	/26

Lesson 2, Practice, Exercise 8

Each of the values in the leftmost column of the table below refers to a number of computers that a given network must support. In the corresponding space in the rightmost column, specify with a subnet mask in dotted-decimal notation the smallest network size that will accommodate those computers.

Number of Network Hosts	Subnet Mask (w.x.y.z)
63	255.255.255.128
1022	255.255.252.0
6	255.255.255.248
1100	255.255.248.0
12	255.255.255.240
150	255.255.255.0
2500	255.255.240.0
20	255.255.255.224
300	255.255.254.0
35	255.255.255.192

Lesson 2 Review

1. Which of the following is true of an address block?

    a. An address block does not necessarily consist of contiguous address space.

    b. By default, an address block serves a single subnet.

    c. Every address in an address block can be assigned to computers.

    b

2. Which of the following is not a private address?

    a. 198.162.0.0 /24

    b. 172.31.0.0 /16

    c. 10.255.255.254 /24

    a

3. Your network address is 131.107.0.0 /28. How many computers can this network accommodate?

    a. 254

    b. 256

    c. 16

    d. 14

  d

4. Your organization purchased the 208.147.66.128 /25 block from an ISP two years ago. Currently, the network has 100 computers. Within the next year, you plan to purchase another 100. You intend to ask the ISP to change your subnet mask so that it will accommodate your network needs over the next year. Which subnet mask should you request?

    a. 255.255.255.192

    b. 255.255.254.0

    c. 255.255.252.0

    d. 255.255.255.0

  d

5. From memory, write out from left to right in the space below the sequence of nine possible values for a subnet mask octet in ascending order.

  0, 128, 192, 224, 240, 248, 252, 254, 255

Lesson 3, Practice, Exercise 1

Assume that your ISP has allocated you the network address 206.73.118.0/24. Using the requirement shown at the top of the table, complete the table by determining the number of bits required for the subnet ID or host ID, the number of bits left for the host ID or subnet ID, the slash notation version of the subnet mask, and then the dotted-decimal version of the subnet mask.

Requirement = 9 subnets

Number of bits required for subnet ID	4
Number of bits left for host ID	4
Slash notation version of subnet mask	/28
Dotted-decimal version of subnet mask	255.255.255.240

Requirement = 3 subnets

Number of bits required for subnet ID	2
Number of bits left for host ID	6
Slash notation version of subnet mask	/26
Dotted-decimal version of subnet mask	255.255.255.192

Requirement = 20 hosts per subnet

Number of bits required for host ID	5
Number of bits left for subnet ID	3
Slash notation version of subnet mask	/27
Dotted-decimal version of subnet mask	255.255.255.224

Page
2-50

Lesson 3, Practice, Exercise 2

For each address block and internally configured subnet mask, determine the number of available subnets and hosts per subnet. (Hint: First convert the internally configured subnet mask to slash notation.)

Original Address Block	Internally Configured Subnet Mask	Number of Available Subnets	Number of Available Hosts per Subnet
207.209.68.0 / 27	255.255.255.240	2	14
131.107.0.0 /20	255.255.255.0	16	254
10.0.0.0 /13	255.255.240.0	128	4,094
208.147.66.0/ 25	255.255.255.248	8	6

Page
2-50

Lesson 3, Practice, Exercise 3

In this exercise, you estimate subnet address ranges by determining the ranges of the first three subnets within a subnetted network. For each address block given in column A, subtract from 256 the value of the mid-range value octet given in the subnet mask in column B. List this value as the grouping value in column C. Then, beginning with 0, list the first four multiples of this same value in column D. Use these values to complete columns E and F, as shown in the example given.

(A) Original Address Block	(B) Internally Configured Subnet Mask	(C) Grouping Value	(D) First Four Multiples of B (Including 0)	(E) Beginning Address of First Three Subnet Ranges	(F) Ending Address of First Three Subnet Ranges
172.16.0.0 /16	255.255.224.0	256 − 224 = 32	0, 32, 64, 96	172.16.0.0, 172.16.32.0, 172.16.64.0	172.16.31.255, 172.16.63.255, 172.16.95.255
172.18.0.0 /16	255.255.248.0	256 − 248 = 8	0, 8, 16, 24	172.18.0.0, 172.18.8.0, 172.18.16.0	172.18.7.255, 172.18.15.255, 172.18.23.255
192.168.1.0 /24	255.255.255.192	256 − 192 = 64	0, 64, 128, 192	192.168.1.0, 192.168.1.64, 192.168.1.128	192.168.1.63, 192.168.1.127, 192.168.1.191

Page
2-50

Lesson 3, Practice, Exercise 4

Using the method in this lesson above, complete the following table. Feel free to use a calculator. The first row is provided as an example.

Subnet Mask	Address #1	Result of division operation (f_1)	Address #2	Result of division operation (f_2)	Same Subnet?
255.255.255.192	192.168.1.116	116 / (256- 192) = 116 / 64 = 1	192.168.1.124	124 / 64 = 1	YES
255.255.255.224	192.168.0.180	180 / (256-224) = 180 / 32 = 5	192.168.0.192	192 / 32 = 6	NO
255.255.252.0	172.16.100.234	100 / (256 − 252) = 100 / 4 = 25	172.16.98.234	98 / 4 = 24	NO
255.255.240.0	172.16.64.10	64 / (256 − 240) = 64 / 16 = 4	172.16.72.200	72 / 16 = 4	YES
255.255.255.192	10.10.10.32	32 / (256-192) = 32 / 64 = 0	10.10.10.63	63 / 64 = 0	YES
255.255.255.240	192.168.10.18	18 / (256-240) = 18 / 16 = 1	192.168.10.15	15 / 18 = 0	NO
/27	192.168.10.31	31 / (256-224) = 31 / 32 = 0	192.168.10.32	32 / 32 = 1	NO
/25	10.1.1.250	250 / (256 − 128) = 250 / 128 = 1	10.1.1.128	128 / 128 = 1	YES

Subnet Mask	Address #1	Result of division operation (f_1)	Address #2	Result of division operation (f_2)	Same Subnet?
/29	172.16.100.248	248 / (256 − 248) = 248 / 8 = 32	172.16.100.252	252 / 8 = 32	YES
/23	10.0.0.1	0 / (256 − 254) = 0 / 2 = 0	10.0.1.1	1 / 2 = 0	YES
/21	10.10.8.100	8 / (256 − 248) = 8 / 8 = 1	10.10.7.100	7 / 8 = 0	NO

Lesson 3 Review

1. You are a new network administrator for Contoso, Inc. Contoso headquarters are located in Albany, but your branch office is located in Binghamton. The central administrator at headquarters has provided the Binghamton branch with the 192.168.10.0/24 address block, and you have noticed that hosts at the local branch are all configured with a subnet mask of 255.255.255.192. How many subnets are enabled by the locally configured subnet mask?

   a. 4

   b. 8

   c. 16

   d. 32

   a

2. How many hosts are available per subnet in the Binghamton branch network described in the previous question?

   a. 6

   b. 14

   c. 30

   d. 62

   d

3. You are the network administrator for the Albany branch office of Contoso, Inc. A year ago, from the central IT department at the New York headquarters, you obtained for use in the Albany office an address block that you have currently divided into 5 subnets, with a maximum of 20 computers per subnet. In the next year, you plan to add 3 more subnets to the branch office. You want to allow enough address space for any subnet to support up to 50 hosts, and you also want

to have the flexibility of using a single address block for the entire Albany office network. You need to approach the central IT department about obtaining enough address space for your network. What size address block should you ask for?

   a. /20

   b. /21

   c. /22

   d. /23

d

4. You have obtained the 192.168.0.0/20 address block from a central network administrator. Within your network, you want the addresses 192.168.3.1 and 192.168.4.1 to belong to the same subnet, but you also want to maximize the number of subnets available. Which subnet mask should you configure within your organization?

   a. /20

   b. /21

   c. /22

   d. /23

b

5. When is it desirable to use subnet masks of various lengths within your organization?

When you want to accommodate subnets of various sizes

Page
2-53

Case Scenario Exercise

You work as a network consultant, and you have been hired by three companies to solve problems related to network connectivity. While visiting each company, you draw sections of the relevant portions of the network. Use the following drawings to determine the IP configuration error that has led to a disruption of network connectivity at each company.

1. What is the configuration error?

Client C has an incorrectly configured default gateway. The default gateway should be set to 192.168.1.129.

Client A
IP address: 192.168.1.116/28
Default gateway: 192.168.1.126

Hub

Client B
IP address: 192.168.1.125/28
Default gateway: 192.168.1.126

192.168.1.126/28   131.107.13.1/16

Hub

Internet

Client C
IP address: 192.168.1.130/28
Default gateway: 192.168.1.126

192.168.1.129/28   Router/Firewall

Client D
IP address: 192.168.1.132/28
Default gateway: 192.168.1.129
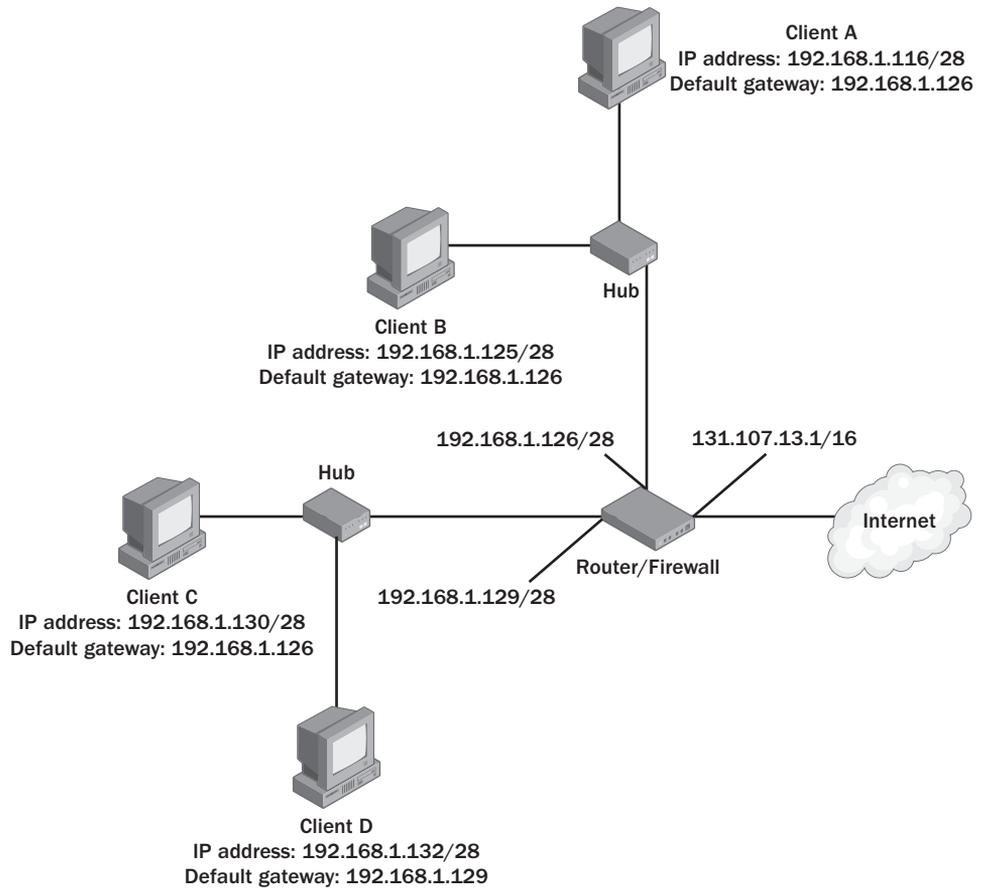
2. What is the configuration error?

The subnet mask is improperly connected for the network. It should be set to 255.255.255.240 or /28.

Client A
IP address: 192.168.2.178/27
Default gateway: 192.168.2.177

Hub

Client B
IP address: 192.168.2.180/27
Default gateway: 192.168.2.177

192.168.2.177/27   207.209.68.1/24

Hub

Internet

Router/Firewall

Client C
IP address: 192.168.2.164/27
Default gateway: 192.168.2.161

192.168.2.161/27

Client D
IP address: 192.168.2.165/27
Default gateway: 192.168.2.161
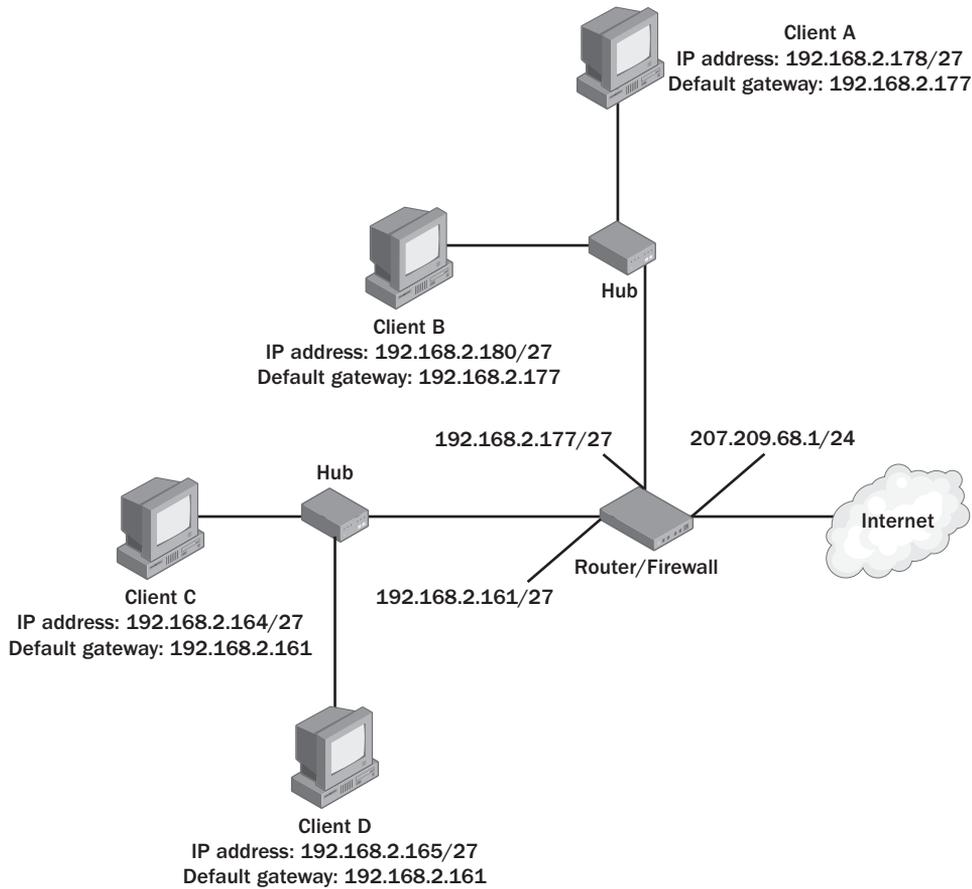
3. What is the configuration error?

Client D's IP address is configured in the wrong logical subnet. The third octet must be in the range from 120 through 127.

Client A
IP address: 131.107.63.1/21
Default gateway: 131.107.56.1

Hub

Client B
IP address: 131.107.62.1/21
Default gateway: 131.107.56.1

131.107.56.1/21   131.107.8.1/24

Hub

Internet

Client C
IP address: 131.107.127.1/21
Default gateway: 131.107.120.1

131.107.120.1/21   Router/Firewall

Client D
IP address: 131.107.128.1/21
Default gateway: 131.107.120.1