2 Planning a TCP/IP Network Infrastructure

Exam Objectives in this Chapter:

- Plan a TCP/IP network infrastructure strategy.
  - Analyze IP addressing requirements.
  - Plan an IP routing solution.
  - Create an IP subnet scheme.
- Troubleshoot TCP/IP addressing.
  - Diagnose and resolve issues related to client computer configuration.
  - Diagnose and resolve issues related to DHCP server address assignment.

Why This Chapter Matters

Assigning appropriate IP addresses to individual computers is an essential part of the network design process. Using unregistered IP addresses is the most effective means of preventing unauthorized access to your network from the Internet, but you must also understand when using registered IP addresses is required. Learning how to subnet a network address and calculate IP addresses and subnet masks not only prepares you to design a network, it also helps you troubleshoot problems related to IP addressing and TCP/IP configuration.

Routing is another TCP/IP function that is essential to network design. Understanding the functions of routers and switches helps you choose the correct components for a network, learn how the Internet functions, and deal with problems involving internetwork communications.

Lessons in this Chapter:

- Lesson 1: Determining IP Addressing Requirements ........................................... 2-3
- Lesson 2: Planning an IP Routing Solution ......................................................... 2-14
- Lesson 3: Planning an IP Addressing and Subnetting Strategy ............................. 2-25
- Lesson 4: Assigning IP Addresses ...................................................................... 2-35
- Lesson 5: Troubleshooting TCP/IP Addressing .................................................. 2-42
Before You Begin

This chapter includes basic information on IP addressing, routing, and subnetting, but also assumes a working knowledge of TCP/IP protocols, the structure of an IP address, and how routers connect networks and forward IP traffic to its destination. You should also read and complete the case scenario in Chapter 1, “Planning a Network Topology,” before proceeding with this chapter.
Lesson 1: Determining IP Addressing Requirements

TCP/IP is the most popular protocol suite for data network installations, but not because it is the easiest to set up. When, during network infrastructure planning, you decide to use TCP/IP, you must be aware of the additional effort this decision implies. Network administrators must configure every TCP/IP computer with a unique IP address, as well as with other configuration parameters. Before administrators can do this, however, they must determine what types of IP addresses to use, based on the communication requirements of the network.

After this lesson, you will be able to

- Understand the difference between public and private IP addresses
- List the IP address ranges designated by the Internet Assigned Numbers Authority (IANA) for private use
- Describe how computers with private IP addresses are able to access the Internet
- Understand the differences between a network address translation (NAT) router and a proxy server
- Specify which computers on a network should use public addresses and which should use private addresses

Estimated lesson time: 20 minutes

Using Public and Private Addresses

The TCP/IP protocols use IP addresses to identify the computers on a network. Every packet that a TCP/IP computer transmits contains the IP address of the computer that is the packet’s intended recipient, and routers use that address to forward the packet to the appropriate destination. For this system to function properly, every computer must have a unique IP address. If duplicate addresses were to exist on the network, routers would contain incorrect information and packets would end up in the wrong place.

On a private network, network administrators are responsible for ensuring that the address assigned to every computer is unique. As long as the address assigned to each computer is different, it doesn’t matter what addresses the administrators use, as long as they subnet them properly. On a public network such as the Internet, however, IP address assignments are more complicated because the Internet consists of thousands of connected networks, each with its own administrators. If the administrators of each network were to select their own IP addresses at random, duplication and chaos would result.
IP Addresses and Subnet Masks

IP addresses are typically expressed using *dotted decimal notation*, in which an address consists of four integers—often called *quads*, *octets*, or *bytes*—between 0 and 255, separated by periods. Like an IP address, a subnet mask consists of 32 bits. In decimal form, the subnet mask appears much like an IP address. In binary form, each of the 32 bits has a value of 0 or 1. When you compare a subnet mask with an IP address, the address bits that correspond to the 1 bits in the mask are the network identifier bits. The address bits that correspond with the 0 bits in the mask are the host identifier bits. For example, a typical IP address and subnet mask, expressed in the decimal notation used when configuring a TCP/IP computer, appears as follows:

**IP address:** 192.168.32.114  
**Subnet mask:** 255.255.255.0

When you convert the address and mask into binary notation, they appear as follows:

**IP address:** 11000000 10 101000 00100000 01110010  
**Subnet mask:** 11111111 11111111 11111111 00000000

Because the first 24 bits in the subnet mask have the value 1, this indicates that the first 24 bits in the IP address make up the network identifier. The final eight bits in the mask have the value 0, which means that the final eight bits in the address are the host identifier. If the subnet mask value were 255.255.0.0 instead, this would indicate that the network identifier and host identifier each consists of 16 bits. The division between the 1 and 0 bits can occur almost anywhere in the subnet mask, as long as both the network and host identifiers are each at least two bits long.

Using Registered Addresses

To prevent IP address duplication on the Internet, an administrative body called the IANA functions as the official IP address registrar. To connect computers directly to the Internet, you must obtain a network address from the IANA. A network address is just a network identifier. The administrators of the network using that identifier are responsible for assigning unique host identifiers to the individual computers and other devices on the network. By combining the network identifier assigned by the IANA with a unique host identifier, the administrators are able to calculate the IP addresses for the computers on that network.

**Off the Record** Although the IANA ultimately assigns all Internet network addresses, network administrators today do not deal with the address registrar directly. Instead, they obtain a network address from an Internet service provider (ISP). The ISP might have obtained the network address from a local (LIR), national (NIR), or regional Internet registry (RIR) (which is assigned pools of addresses by the IANA directly), but it is also likely that the ISP obtained the address from its own service provider. Internet addresses often pass through several layers of service providers in this way before they get to the organization that actually uses them.
Lesson 1  Determining IP Addressing Requirements  2-5

Why Use Registered Addresses?  If you have computers on your network that you want to be accessible from the Internet (such as Web servers), you must configure them with IP addresses that the IANA has registered. This is because only registered addresses are visible from the Internet. For a user on the Internet to access your company Web server, a client application, such as a Web browser, must initiate communication by sending a request to the server. The browser can’t do that if it doesn’t have the server’s address. (Users on your network who want to access Internet services do not require registered addresses; this matter is covered later in this lesson.)

Why Not Use Registered Addresses?  Theoretically, you can use registered IP addresses for all the computers on your network, but this practice has two serious drawbacks:

■ It depletes the IP address space. If every device with an IP address today (which includes a great many mobile telephones, automobiles, and other devices, in addition to computers) had a registered IP address, the pool of available addresses would be well on its way to depletion. Even now, a program to expand the IP address space from 32 (called Internet Protocol Version 4 or IPv4) to 128 bits, called IPv6, is currently under way to prevent the possibility of depleting the entire IP address space in the future.

See Also  For more information about IPv6, see Understanding IPv6 (Microsoft Press, 2003). Additionally, the Internet Engineering Task Force (IETF) has published a number of proposed Requests for Comments (RFC) standards that you can consult, such as RFC 2464, “Transmission of IPv6 Packets over Ethernet Networks.”

■ Using registered IP addresses on a private network presents a serious security hazard. Not only can a computer with a registered IP address access systems on the Internet, the systems on the Internet can also access the computer.

Security Alert  You must set up some sort of firewall to protect Web servers and other computers that must have registered addresses. For example, you can use packet filtering to permit only Hypertext Transfer Protocol (HTTP) traffic using port 80 to reach your Web server from the Internet. This means that Internet users can access the Web server using only standard browser requests. Other types of traffic—such as those used by Internet predators to plant viruses, steal data, and cause mayhem—are blocked. Without some protection, an intruder will eventually target a registered system, and the results can range from irritating to catastrophic.

Protecting computers with registered addresses is a complex process that requires constant vigilance from the network’s administrators. If you configure all your computers with registered addresses, you compound this protection process unnecessarily. You can use several methods to assign unregistered IP addresses to your network’s computers while still enabling them to access the Internet.
Chapter 2 Planning a TCP/IP Network Infrastructure

General practice in network design calls for using registered IP addresses only on computers that must be accessible from the Internet, such as Web and mail servers. You can obtain the addresses you need from your ISP. In most cases, designers place these computers on a *perimeter network* that is separate from the servers and workstations needed by the organization’s internal users, as shown in Figure 2-1. This perimeter network is sometimes referred to colloquially as a demilitarized zone (DMZ) because these registered computers are not as fully protected as the internal systems. Although the registered computers are still behind a firewall, they are able to receive more traffic from the Internet than the internal computers can.

![Diagram of a network infrastructure](image_url)

*Figure 2-1  Computers with registered IP addresses located in a perimeter network*
Lesson 1  Determining IP Addressing Requirements  2-7

Using Unregistered Addresses

Most TCP/IP networks use unregistered IP addresses (also called private network addresses) for the servers and workstations that only internal users need to access. These are addresses that are not registered with the IANA, and as a result, they are invisible to the Internet. Because they are invisible, Internet criminals cannot specifically target them for virus distribution or other types of compromise (although they are still vulnerable in other ways). As described in RFC 1918, “Address Allocation for Private Internets,” the IANA has set aside three IP address ranges for use by private networks. These addresses are not registered to any single network, so anyone can use them for computers and other devices on a private network.

The private IP address ranges designated by the IANA are as follows:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

Tip  On a private network that is not connected to the Internet in any way, you can use any IP addresses you want to, registered or not, because there is no way for them to conflict with the registered users of those addresses on the Internet. However, if your network users access the Internet in any way, you should always use the designated private address ranges to prevent conflicts with Internet computers.

Accessing the Internet from a Private Network

The logical question that remains, however, when you elect to use unregistered IP addresses on your network, is how your users can access the Internet. If unregistered addresses are invisible to the Internet, how is an Internet Web server supposed to respond to a request from a browser on an unregistered network? The answer is that the network designer incorporates a mechanism into the network infrastructure that enables unregistered clients to access Internet services. The two most common mechanisms of this type are NAT and proxy servers.

Using Network Address Translation

*Network address translation* is an application built into a router that functions as an intermediary between unregistered clients on a private network and registered Internet servers. Client computers can use NAT to send requests to Internet servers and receive replies, despite the fact that the clients have unregistered network addresses. This provides the unregistered computers with Internet access, without compromising their protection from Internet intrusion.
Chapter 2 Planning a TCP/IP Network Infrastructure

Connecting to the Internet with Routers

A router is a network layer device that connects two networks and permits traffic to pass between them. Routers therefore have two network interfaces and two IP addresses, one for each network. If you want to give your network users access to the Internet, you must have a router connecting your network with that of an ISP. A router can be a software application running on a normal computer, or it can be a dedicated hardware device costing anywhere from under one hundred to many thousands of dollars. For more information on routers and TCP/IP routing, see Lesson 3 of this chapter.

Understanding Routing

To get the request to the destination server, the client computer sends it to a nearby router, which receives the datagram, evaluates the destination address, and forwards the packet to the appropriate location, either the specified server or another router. The datagram might pass through a dozen or more routers on its journey. Eventually, the destination server receives the datagram, processes the request contained inside, and generates a reply using the sender’s address from the original datagram as the destination. The routing process then occurs in reverse, with the reply datagram eventually finding its way back to the client computer.

If the sender’s IP address in the request datagram is unregistered, however, the reply can never make it back to the client computer because routers cannot process unregistered addresses properly. When you use NAT, the first router that receives the request datagram from the client makes some slight modifications to it. A NAT router connects both to a private network, using unregistered addresses, and to an ISP’s registered network. This means that the NAT router has one unregistered address and one registered address.

Understanding NAT Routing

Under normal conditions, routers do not modify datagrams any more than the postal service modifies envelopes. A NAT router, however, modifies each datagram it receives from an unregistered client computer by changing the sender’s IP address. When a client sends a request message in a datagram to a NAT router, NAT substitutes its own registered IP address for the client computer’s unregistered address in the datagram and then forwards it to the destination in the normal manner. The NAT router also maintains a table of unregistered addresses on the private network so that it can keep track of the datagrams it has processed.
When the destination server receives the request, it processes it in the normal manner and generates its reply datagram. However, because the sender's address in the request datagram contained the NAT router's registered address, the destination server addresses the reply datagram to the NAT router, and routers can forward it in the normal manner. When the NAT router receives the reply from the server, it modifies the datagram again, substituting the client's unregistered address for the destination address in the datagram, and forwards the packet to the client on the private network.

The NAT router's processes are invisible to the client and the server. The client has generated a request and sent it to a server, and it eventually receives a reply from that server. The server receives a request from the NAT router and transmits its reply to the same router. Both the client and the server have functioned normally, unaware of the NAT router's intervention. More importantly, the client computer remains invisible to the Internet and is protected from most types of unauthorized access.

Microsoft Windows Server 2003 can function as a router, and it contains a NAT implementation as part of the Routing and Remote Access service (RRAS). Because the NAT router functions are invisible to the unregistered computer, users can access the Internet with any client application. The one thing you can't do with a standard NAT implementation is run an Internet server. This is because the client must initiate the client/server transaction, and a client computer on the Internet has no way of contacting the server running on an unregistered computer first.

Tip

Some NAT implementations enable you to assign registered IP addresses to specific unregistered computers on the private network. This ability allows you to use an unregistered computer to establish a presence on the Internet without compromising the security of the unregistered computer. All the incoming client traffic is actually going to the NAT router, which relays it to the server on the unregistered network.

Using Proxy Servers

A proxy server is similar to a NAT router in that it functions as an intermediary between client computers on a private network and servers on the Internet. Unlike NAT, however, a proxy server is an independent software product that runs at the application layer and is not incorporated into a router. When an unregistered client wants to send a request to an Internet server, the computer forwards the request datagram to a proxy server instead. The proxy server sends an identical request to the destination server, receives a reply, and relays the results back to the client. For the proxy server to communicate with Internet servers, it must have a registered IP address.

Unlike NAT routers, proxy servers do not process all TCP/IP traffic. Proxy servers only work with specific client applications, and you must configure the clients themselves to send their messages to the proxy server instead of to the actual destination, using an
interface like the one shown in Figure 2-2. At one time, the need to configure individual clients was the primary drawback of proxy servers, but some client applications can now detect the presence of a proxy server on the network and configure themselves to use the server automatically.

Proxy servers also differ from NAT routers in that they enable the network administrator to exercise more control over users' access to the Internet. For example, administrators running a proxy server that gives clients access to Internet Web servers can, in most cases, create a list of specific Web sites that users are not permitted to access, as well as restrict times that users are permitted to access the Web. Proxy servers can also log users' activity, enabling administrators to examine users' access patterns and maintain a record of specific Internet activities. In addition, proxy servers are usually able to cache information from frequently visited sites. When a user requests a Web page that the proxy server has recently downloaded for another user, the server can send a reply to the client immediately using cached information. This speeds up the user's response time and reduces traffic on the network's Internet connection.

Proxy servers provide client computers with the same degree of security as NAT routers. Because only the proxy server communicates directly with the Internet, the actual clients on the unregistered network remain invisible to potential intruders. However, despite the protection that both NAT and proxy servers provide for unregistered computers on a private network, they cannot always overcome the shortsightedness of the network's users. As mentioned earlier, there is no way for an Internet predator to access a computer on an unregistered network directly, because with NAT and proxy servers, the client must initiate communications. However, if the client computer does initiate communications with the wrong computers on the Internet (whether intentionally or not), it is vulnerable to all kinds of attacks.
Security Alert  One of the most common ploys used by Internet criminals today is to dupe an unsuspecting user into downloading and running a program that is essentially a special-purpose server application. The intruders may camouflage these programs, called Trojan horses or just Trojans, as image files or other innocent applications, which are typically delivered through e-mail or downloaded from a Web site. When the user runs the program, it broadcasts the computer’s availability to the Internet, enabling unauthorized users to take control of it at will. Private addressing therefore provides a distinct advantage over using public addresses, but it is not a panacea.

Planning IP Addresses

A first step in creating an IP addressing plan for your network is determining what types of Internet access each computer requires, if any. Most organizations today give their network computers some access to the Internet, and in these cases, you should know the circumstances in which you must use registered IP addresses. For computers that are strictly Internet clients, that is, for users who need access to the Web and similar services, unregistered IP addresses are the best solution, along with either a NAT router or a proxy server. Whether you use NAT or a proxy server depends on how much Internet freedom you want to grant your users and what types of client applications they will use.

For computers that must function as Internet servers, registered IP addresses are required. Most networks need only a few registered IP addresses, and they lease them from their ISP for a nominal fee. For organizations with a large Internet presence requiring many addresses, you might have to acquire a network address of your own and assign host addresses as needed.

Using registered IP addresses affects the network infrastructure design in other ways as well. As mentioned earlier, most organizations put Web servers and other registered computers on a network of their own. This also means that you should not use these same computers to run important internal services. For example, you should not use the same computer to host your Web server and your company’s private customer database. A registered computer is inevitably more vulnerable to attack than an unregistered one, and it should contain only the information needed to perform its primary function.
Practice: Using Registered and Unregistered IP Addresses

For each of the following types of computers, specify whether it should have a registered or an unregistered IP address, or both, and why. You can find answers to the questions in the “Questions and Answers” section at the end of this chapter.

1. A corporate Web server providing product information to Internet clients around the world

2. A NAT router enabling clients on a private network to access Internet servers

3. An intranet Web server on a private network used to provide human resources information to employees

4. A client computer that accesses Web servers on the Internet using a NAT router

5. A proxy server providing Internet Web access to clients on a private network

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.
Lesson 1  Determining IP Addressing Requirements

1. Which of the following statements about NAT routers and proxy servers are true? Choose all answers that are correct.
   a. NAT routers and proxy servers must have two IP addresses.
   b. A NAT router can provide Internet access to any client application on the private network.
   c. Proxy servers can cache information they receive from Internet servers.
   d. The Windows Server 2003 operating system includes a proxy server.

2. What are the two primary reasons why you should use unregistered IP addresses for Internet client computers?

3. Which of the following best describes the function of a subnet mask?
   a. A subnet mask indicates whether an IP address is registered or unregistered.
   b. A subnet mask specifies the sizes of the network and host identifiers in an IP address.
   c. A subnet mask is a value assigned by the IANA to uniquely identify a specific network on the Internet.
   d. A subnet mask enables an IP address to be visible from the Internet.

Lesson Summary

- Every computer on a TCP/IP network must have a unique IP address.
- Computers that are visible from the Internet must have IP addresses that are registered with the IANA.
- For security, a network designer often places computers with registered IP addresses on a separate network.
- Computers on private networks typically use unregistered IP addresses to protect them from unauthorized access and to conserve the IP address space.
- Computers with unregistered IP addresses can access the Internet as clients using a NAT router or a proxy server.
Lesson 2: Planning an IP Routing Solution

An IP router is a hardware or software device that connects two local area networks (LANs), relaying traffic between them as needed. Part of designing a network infrastructure is determining how many LANs you will create and how you will connect them. When you are designing a small network, routing is not a major consideration because you can put all your computers on a single LAN. For medium-to-large networks, this is not a practical solution. You have to create several LANs and then connect them so that any computer on the network can communicate with any other computer.

Your IP routing plan can be simple or complex, depending on the size of the network installation, the number of LANs you decide to create, and how you choose to connect the LANs. A small network might have a single router connecting the LAN to an ISP to provide network users with Internet access. A large network installation might consist of many different LANs, all connected with routers. The ultimate IP routing scenario is the Internet itself, which is composed of thousands of networks connected by thousands of routers.

Typically, an IP routing plan specifies how many LANs there will be in your network installation and how you will connect the LANs. The plan should also specify the types of routers the network will use, and how the routers will get the information they need to forward packets to their destinations.

After this lesson, you will be able to
- Understand router functions
- Use routers to connect LANs and wide area networks (WANs)
- Understand the difference between routing and switching

Estimated lesson time: 20 minutes

Understanding IP Routing

When a computer on a TCP/IP network transmits a packet, the datagram in the packet contains the IP address of the destination computer, as well as the address of the sender. If the destination address is on the same LAN as the sender, the packet travels directly to that destination. If the destination is on a different network, the sender transmits a packet to a router instead. This router is known as the computer’s default gateway. (In TCP/IP parlance, the term gateway is synonymous with router.) You specify the default gateway address for your computers along with their IP addresses and subnet mask during the TCP/IP configuration process.

The default gateway is the interface between the sender’s own network and all the other connected networks. When the router receives a packet, it reads the destination address and compares the address to the entries in its routing table. A routing table is
a list of destination addresses, with the information needed to forward traffic to those destinations. Using the information in its routing table, the router determines where to send the packet next. The router might be able to transmit the packet directly to its destination (if the router has an interface on the destination network), or it might send the packet to another router, where the entire process begins again. On a private network, packets might travel through several routers on the way to a given destination. On the Internet, packets commonly pass through a dozen routers or more.

Tip To see a list of the routers between your computer and a specific destination address, you can use the traceroute utility that is provided with most TCP/IP implementations. On computers running the Microsoft Windows operating systems, the traceroute utility is called Tracert.exe. To use it, display a Command Prompt window and type `tracert address`, where `address` is the IP address of a destination computer.

Routers obtain the information in their routing tables in one of two ways. Either an administrator manually enters the information, which is called static routing, or the router receives the information automatically from another router using a specialized routing protocol. This is called dynamic routing. On Internet routers, the routing tables can be long and complex, but the tables on private network routers are simple.

**Creating LANs**

Ethernet LANs are typically defined in terms of broadcast domains and collision domains.

- A **broadcast domain** is a group of computers, all of which receive broadcasts transmitted by any one of the computers in a group. For example, when you connect 100 computers using only Ethernet hubs, any one of those computers can generate a broadcast and all the other computers will receive it.

- A **collision domain** is a group of computers that are connected in such a way that when any two computers transmit packets at exactly the same time a collision occurs. The collision destroys both packets and forces the computers to retransmit them.

When you create two LANs and join them using a router, you are creating two separate broadcast domains, because routers do not forward broadcast transmissions from one network to another, and two separate collision domains, because packets transmitted on the same network may collide, but packets on different networks do not.

**Planning** The reason to split a private network into multiple LANs is to create different broadcast domains and collision domains.
If you were to have thousands of computers all connected to the same LAN, each computer would have to devote an inordinate amount of time to processing broadcast messages. In addition, there would be a high collision rate because so many computers would be contending for the network medium at the same time. More collisions mean more packet retransmissions. The result would be a slow, inefficient network. By splitting that network into multiple LANs, you create individual broadcast and collision domains, reducing the number of broadcasts each system has to process and the number of collisions that occur.

Routing and Network Topology Design

In Lesson 3 of Chapter 1, “Planning a Network Topology,” you learned that network designers often split the network into a series of horizontal networks, each of which is connected to a backbone network using a router. This design provides an efficient routing solution. No matter how many horizontal networks you have in your installation, a transmitted packet never has to travel through more than two routers to get to any destination on the network (as shown in Figure 1-7). Each packet passes through one router to get from its origin network to the backbone and through a second router to get from the backbone to the destination network. Connecting the horizontal networks in series would require packets to pass through a separate router for each network they traverse.

The number of LANs you create and the number of computers in each LAN depend on the data-link layer protocol you select for your network. Some protocols have specific limitations on the number of computers they support on a single LAN while others have implied limits based on other factors, such as the maximum number of hubs you can use. In many cases, however, a network’s LAN configuration is based on geographical or political factors. For example, if you are designing a network for a multi-story office building, creating a separate LAN for each floor might be the most convenient solution. In other cases, designers create a separate LAN for each department or division in the organization.

Another advantage of routers is that they can connect networks running completely different protocols at the data-link layer. Whenever a packet arrives at a router, it travels up through the protocol stack only as high as the network layer (see Figure 2-3). The router strips off the data-link layer frame from the packet and processes the IP datagram contained inside. When the router has determined how to forward the datagram to its next destination, it repackages the datagram in a new data-link layer frame prior to transmission. This new frame can be the same as, or different from, the original frame on the packet when it arrived on the router. So if your network infrastructure
design calls for different data-link layer protocols or different network media to satisfy the requirements of different users, you can connect those different networks using routers. You can connect two different types of Ethernet, such as connecting a 100Base-TX Fast Ethernet horizontal LAN (using Category 5 unshielded twisted pair cable) to a 1000Base-SX Gigabit Ethernet backbone (using fiber-optic cable), or even connecting an Ethernet LAN to a Token Ring LAN.

Creating WANs

In addition to connecting LANs, routers can also connect a LAN to a WAN connection, enabling you to join networks at different locations. This is the most common application for routers today. Every network connected to the Internet uses a router to connect the private network to an ISP's network. The ISP in turn has its own routers that provide the connection to the Internet. Even a simple Windows computer using the Internet Connection Sharing (ICS) feature is functioning as a router.

Some network installations also use routers and WAN connections to join distant offices. For example, a branch office might be connected to corporate headquarters using a T-1 line, which is a permanent, digital telephone connection between the two sites. To connect the networks at those sites, each one has a router connecting it to one end of the T-1, as shown in Figure 2-4. The T-1 itself then becomes a two-node network, connecting the two remote LANs. A computer at one site that has to send traffic to a computer at the other site sends its packets to the router on the local network. The router then forwards the packets over the T-1 to the router at the other site. The second router then forwards the packets to the LAN in the other office.
You will learn later in this chapter that there are alternatives to routers for connecting LANs at the same site. However, routers are essential for connecting networks using a WAN. This is because WANs use different data-link layer protocols than LANs. A typical WAN connection uses a TCP/IP protocol called the Point-to-Point Protocol (PPP) at the data-link layer. PPP is designed solely for connections between two nodes. With PPP, unlike Ethernet, there is no contention for the network medium and no need for packet addressing. The control overhead of the PPP is therefore much lower than that of Ethernet or Token Ring. The routers not only provide the interface to the WAN, they also repackage the datagrams for transmission over a different type of network.

Using Routers

The routers you use to connect your LANs can take many different forms. Some routers are software products. A Windows Server 2003 computer is capable of functioning as a router, providing you install two network interface adapters in the computer and configure RRAS to function as a LAN router. Windows Server 2003 can also function as a router connecting a LAN to the Internet. The only differences between the two router functions are the RRAS configuration and the fact that one of the network interfaces is a modem or other device providing a WAN connection to an ISP.

On most networks, routers are more likely to be separate hardware devices than standard computers. Stand-alone routers are available in many sizes and price ranges. The smallest and most inexpensive routers are devices the size of an external modem that are designed to connect a home or small business LAN to the Internet. More elaborate Internet access routers are designed to support larger networks. Most of these routers can use NAT so that the clients on the private network can use unregistered IP addresses.

Planning

Routers for connecting LANs tend to be high-end devices and are frequently modular. This type of device consists of a router frame, which you typically install in a data center and populate with modules that provide interfaces to your various networks. The advantage of this design is that you can connect LANs (or WANs) of any type by purchasing the appropriate modules and inserting them into the frame.
Using Switches

While routers are necessary for connecting distant networks with WANs, today's networks do not use them for connecting LANs together as often as they used to. Switches have largely replaced routers on internal networks. A switch is a network connection device similar in appearance to a hub but with different internal functions.

A typical Ethernet hub is strictly a physical layer device. Electrical (or fiber-optic) signals generated by devices on the network enter the hub through one of its ports. The hub then amplifies the signals and transmits them through all the other ports simultaneously. The hub does not read the contents of the data packets it forwards or even recognize that they are data packets. The hub's function is strictly electrical (or photonic). It has no intelligence.

Switches receive signals from network devices in the same way as a hub, but the switch is intelligent and can read the contents of the data packets it receives. The switch reads the destination address in each incoming packet, amplifies the signals like a hub, and then forwards the packet, but only through the port providing the connection to the packet's destination.

When you connect a group of computers to a hub, every packet transmitted by every computer is forwarded to every other computer. This means that the network interfaces in the computers spend a significant amount of time reading the addresses of incoming packets and discarding them because they are intended for another destination. Connect the same group of computers to a switch, and the amount of traffic on the network is reduced substantially because packets travel directly from the source only to their destinations and nowhere else. Each pair of computers on the network has, in effect, a dedicated connection between them, using the full bandwidth of the network medium. There is less contention for the network medium, and therefore there are fewer collisions.

You can use switches in place of hubs on your individual horizontal networks. These are called workgroup switches or switching hubs. As a replacement for routers, however, you can also use a single high-performance switch in place of a backbone network. By using switching hubs on your horizontal networks and connecting them to a single backbone switch, you create a network infrastructure in which every computer can open a dedicated connection to any other computer. For larger networks, you can add a third level of switches, connecting your workgroup switches to a departmental switch and your departmental switches to a backbone switch.
Off the Record  You can connect standard hubs to departmental or backbone switches, providing each horizontal network with a dedicated connection to every other horizontal network. This is not as efficient as a fully switched network, but it provides a performance improvement over routers and a backbone that all computers in the enterprise share.

Real World  Switches, Routers, and Performance

Because they are more intelligent, switches are more expensive than standard Ethernet hubs, but they are less expensive than comparable routers. Routing is a more complicated task than switching because a router has to strip off each packet’s data-link layer frame, process the information in the IP datagram, and then package the datagram in a new frame before transmitting it. A basic switch, in contrast, only has to read the data-link layer address in each packet and forward it to the appropriate port. For this reason, switching is also far faster than routing.

Replacing the routers on an existing network with switches usually results in an increase in performance. Designing a network from the outset to use switches enables you to achieve peak performance from the network equipment you select. Even a standard 10-megabit-per-second (Mbps) Ethernet network can yield exceptional performance when each workstation has a dedicated, full-bandwidth connection to every other workstation.

Combining Routing and Switching

Unlike routers, which operate at the network layer, switches are data-link layer devices, and this presents a new problem. By connecting LANs with switches, you are essentially creating one huge LAN. Although switching eliminates the problem of having one huge collision domain, all computers on the network are still in the same broadcast domain. When a computer on the network transmits a broadcast message, every computer on the entire network receives it. This type of setup can consume large amounts of bandwidth unnecessarily.

The solution to this problem lies in a switch’s ability to create virtual LANs, or VLANs. A virtual LAN is a group of computers on a switched network that functions as a subnet. When one computer in a VLAN generates a broadcast transmission, only the other computers in the same VLAN receive it. Network administrators create VLANs in the switch by specifying the addresses of the computers in each subnet.
Planning One big advantage to creating subnets with VLANs is that the computers in a subnet can have physical locations anywhere in the enterprise. With VLANs, you can create subnets based on criteria other than physical proximity, such as membership in a workgroup or department.

VLANs are logical constructions that form an overlay to the switched network. The computers are still switched, but the VLANs enable them to behave as though they are routed. Further difficulty arises, however, when computers on different VLANs have to communicate with each other. In this case, some element of actual routing is necessary, and various types of switches treat this requirement in different ways. Switches that are strictly layer 2 (that is, data-link layer) devices sometimes have a port for a connection to a router. This type of device operates under a “switch where you can, route where you must” philosophy. The device switches all traffic between computers on the same VLAN, but it sends all traffic between computers on different VLANs to the router for processing.

Another solution to this problem is most commonly called layer 3 switching, although specific switching hardware manufacturers have other names for the technique, including multilayer routing and cut-through routing. A layer 3 switch has the capabilities of a switch and a router built into a single device. Rather than examine the datagram information for every packet, a layer 3 switch examines the first packet in each series to determine its final destination, and then uses standard layer 2 switching for the subsequent packets sent to the same destination. The philosophy for this type of device is “route once, and switch afterwards.”

Workgroup and departmental switches are relatively simple devices. Some manufacturers have lines of hubs and switches that are outwardly identical, differing only in their internal construction. Layer 3 switches are much more complex, typically taking modular form, like high-end routers. Installing this type of switch enables you to connect different types of horizontal networks, providing essentially the same functions as a router, but with greater speed and efficiency.
Practice: Designing an Internetwork

In the following exercises, the diagrams represent a network installation that consists of four independent LANs. Working directly on the diagrams, add the components necessary to fulfill the requirements given in each exercise. Be sure to add all the necessary cables, hubs, routers, or switches, and label them accordingly. Don't forget to label the device connecting the computers in each LAN as well. You can find answers to the exercises in the “Questions and Answers” section at the end of this chapter.

**Exercise 1: Internetwork Design with a Single Broadcast Domain and Multiple Collision Domains**

In the following diagram, add the components needed to connect the LANs to an internetwork that consists of a single broadcast domain and several collision domains.
Exercise 2: Internetwork Design with Multiple Broadcast and Collision Domains

In the following diagram, add the components needed to connect the LANs in an internetwork that consists of five broadcast domains and five collision domains.

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. Replacing the hubs and routers on an internetwork with switches creates a network that has which of the following?

   a. One broadcast domain and one collision domain
   b. One broadcast domain and multiple collision domains
   c. One collision domain and multiple broadcast domains
   d. Several collision domains and several broadcast domains
2. Specify the OSI reference model layer at which each of the following devices operates.
   a. A switch
   b. A router
   c. A hub

3. Which of the following Windows Server 2003 TCP/IP configuration parameters specifies the address of a router?
   a. Preferred DNS server
   b. Subnet mask
   c. Default gateway
   d. IP address

4. When you replace the routers on an internetwork with switches that include no VLAN or layer 3 capabilities, which of the following is a possible reason for poor network performance?
   a. Excessive collisions
   b. Excessive broadcast traffic
   c. Excessive number of workstations on the LAN
   d. Excessive number of collision domains

Lesson Summary

- Large networks typically consist of multiple LANs connected by routers. Routers are network layer devices that enable communication between the networks while maintaining separate broadcast and collision domains.

- Routers can take the form of software or hardware, and range from Routing and Remote Access in Windows Server 2003 to inexpensive Internet access devices to expensive modular installations that support large networks.

- A typical network design consists of several horizontal networks, all connected to a single backbone network.

- A switch is a data-link layer device that intelligently forwards traffic to specified destinations. Switches can replace many routers in your network infrastructure design, creating a network that is more efficient and economical.

- Replacing routers with switches creates a network with a single broadcast domain. Virtual LANs are logical subnets that exist inside switches, enabling you to limit the propagation of broadcasts throughout the network.
Lesson 3: Planning an IP Addressing and Subnetting Strategy

Once you have determined what types of IP addresses your network will use and have decided how many LANs you are going to create and how you’re going to connect them, you can begin the process of calculating the network’s IP addresses, subnet masks, and default gateway addresses. You can also plan how the network administrators are actually going to perform the TCP/IP configuration tasks.

After this lesson, you will be able to
■ Understand how to subnet a network
■ Calculate a subnet mask
■ Calculate IP addresses on subnets

Estimated lesson time: 30 minutes

Obtaining Network Addresses

In Lesson 1 of this chapter, you learned about the circumstances under which to use registered and unregistered IP addresses, and you have presumably used this information to design a network infrastructure in which the computers use the appropriate address types. If some or all of your computers require registered IP addresses, you can obtain them in one of two forms, depending on how many addresses you need.

Planning  If you need only a few registered addresses, you can obtain them singly from your ISP along with an appropriate subnet mask, although you will almost certainly have to pay an extra monthly fee for them. If the computers requiring the registered address are all on the same LAN and must communicate with each other, be sure that you obtain addresses in the same subnet. If you need a large number of registered IP addresses, you can obtain a network address from the ISP and use it to create as many host addresses as you need.

A network address is the network identifier portion of an IP address plus a subnet mask. For example, if your ISP were to assign you the network address 192.168.65.0, with a subnet mask of 255.255.255.0, you can assign IP addresses ranging from 192.168.65.1 to 192.168.65.254 to your computers. The network address you receive from the ISP depends on the class of the address and on the number of computers you have requiring registered addresses.

Off the Record  In practice, the network address your ISP assigns you will not be part of the private address range used in this example. Also, it will probably be more complex than the address shown here, because the ISP will be assigning you only a small portion of the addresses assigned to them.
Understanding IP Address Classes

The IANA divides the IP address space into three basic classes. Each class provides a different number of possible network and host identifiers, and therefore, each is suitable for installations of a specific size. The three classes, and the relative sizes of the network and host identifiers, are shown in Figure 2-5.

![Figure 2-5 IP address classes](image.png)

Table 2-1 provides additional information about each of the address classes, including the value of the first binary bits and the first decimal byte in each class. The value of the first bits and first byte are what you use to determine the class of a particular network address. The table also specifies the number of bits in the network and host identifiers for each class, as well as the number of possible addresses you can create with each identifier.

<table>
<thead>
<tr>
<th>IP Address Class</th>
<th>Class A</th>
<th>Class B</th>
<th>Class C</th>
</tr>
</thead>
<tbody>
<tr>
<td>First bit values (binary)</td>
<td>0</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>First byte value (decimal)</td>
<td>1–127</td>
<td>128–191</td>
<td>192–223</td>
</tr>
<tr>
<td>Number of network identifier bits</td>
<td>8</td>
<td>16</td>
<td>24</td>
</tr>
<tr>
<td>Number of host identifier bits</td>
<td>24</td>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>Number of possible networks</td>
<td>126</td>
<td>16,384</td>
<td>2,097,152</td>
</tr>
<tr>
<td>Number of possible hosts</td>
<td>16,777,214</td>
<td>65,534</td>
<td>254</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.0.0.0</td>
<td>255.255.0.0</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
Lesson 3  Planning an IP Addressing and Subnetting Strategy

To compute the number of possible addresses you can create with a given number of bits, you use the formula $2^x - 2$, where $x$ is the number of bits. You subtract two because the original IP addressing standard states that you cannot use the values consisting of all zeros and all ones for network or host addresses. Most routers and operating systems, including Windows Server 2003, now enable you to use all zeros for a network or subnet identifier, but you must be sure that all your equipment supports these values before you decide to use them.

**Exam Tip**  Be sure to familiarize yourself with the information in Table 2-1, especially the number of possible networks and hosts available for the three IP address classes, and with the formula for computing the number of possible addresses. It is common for the exam to contain questions requiring you to know how many network or host identifier bits are required for a given installation.

In Lesson 1, you learned about the IP address ranges designated by the IANA for use by private networks. Each of the three ranges corresponds to one of the IP address classes, as follows:

- **Class A**: 10.0.0.0 through 10.255.255.255
- **Class B**: 172.16.0.0 through 172.31.255.255
- **Class C**: 192.168.0.0 through 192.168.255.255

**Off the Record**  In addition to Classes A through C, there are two additional address classes, Class D and Class E. The IANA has allocated Class D addresses for use as multicast identifiers. A multicast address identifies a group of computers on a network, all of which possess a similar trait. Multicast addresses enable TCP/IP applications to send traffic to computers that perform specific functions (such as all the routers on the network), even if they are located on different subnets. Class E addresses are defined as experimental and are as yet unused.

**Understanding Subnetting**

Whether you obtain a registered network address from your ISP or you use one of the private IP address ranges designated by the IANA, you are free to subnet that address as needed. Subnetting is the process of creating individual network addresses out of a larger network address. To create a subnet, you borrow some host identifier bits from a network address and use them to create a subnet identifier. You can then increment the value of the subnet identifier to create multiple subnets, and increment what’s left of the host identifier to create individual hosts on each subnet.

Subnetting is an essential part of the IP addressing process, as you can probably tell when you study the table of IP address classes shown earlier in this lesson. There are
only 126 Class A network addresses available in the entire IP address space, for example, and each one of those addresses supports more than 16 million hosts. There are some very large network installations in this world, but none of them have as many as 16 million computers. Assigning an entire Class A network address to a particular organization for its exclusive use would therefore be extremely wasteful if subnetting was not involved.

In a standard Class A address, the network address is the first 8 bits, which in decimal form translates to the first quad in the address. For example, 10.0.0.0 is an example of a Class A address, and it would use a subnet mask value of 255.0.0.0. Because a Class A address has 24 host identifier bits, far more than are needed for any single network, it is no problem to borrow some of those bits to create a subnet identifier. If you decide to borrow 8 bits for the subnet identifier, the breakdown of the address changes as shown in Figure 2-6. You also change the subnet mask of the address to 255.255.0.0 because the primary function of the mask is to specify where in the IP address the host identifier begins.

To use the subnetted Class A address, you increment the subnet identifier and the host identifier separately. For example, to create your first subnet, you give the subnet identifier a value of one. This means that the network address for this subnet is 10.1.0.0. You now have 16 bits left for the host identifier, which means you can create up to 65,534 host addresses in that one subnet \((2^{16} - 2 = 65,534)\). The first host address in this subnet is therefore 10.1.0.1. This is the IP address value you use to configure the first computer in the subnet, along with the subnet mask value of 255.255.0.0. The second address in the subnet is 10.1.0.2, and the next addresses can proceed from 10.1.0.3 all the way to 10.1.255.254, utilizing all 16 bits of the host identifier.

To create the second subnet, you simply increment the subnet identifier value again, giving you a network address of 10.2.0.0 and IP addresses ranging from 10.2.0.1 to 10.2.255.254. Because you have allocated 8 bits to the subnet identifier, you can create up to 254 subnets on this network \((2^8 - 2 = 254)\). The network address for the last subnet would be 10.254.0.0, with the IP addresses in that subnet ranging from 10.254.0.1 to 10.254.255.254.
Subnetting Between Bytes

When the boundaries between your network, subnet, and host identifiers fall between the bytes of your IP address, subnetting is quite easy. However, you can use any number of bytes for a subnet identifier, and sometimes you are forced to create subnets that don’t work out so evenly. For example, if you have a Class C network address you want to subnet, you obviously can’t create an 8-bit subnet identifier because there would be no bits left for the host identifier. Therefore, you have to use fewer than 8 bits, which means your subnet identifier and host identifier values must be combined in the IP address into a single decimal number.

Tip  A number of software tools are available that can simplify the process of calculating IP addresses and subnet masks for complex subnetted networks. One of these, available as freeware, is Wild Packets’ IP Subnet Calculator, available for download at http://www.wildpackets.com/products/free_utilities/ipsubnetcalc/overview. However, you should be aware that tools like these are not permitted when taking Microsoft Certified Professional (MCP) exams, so you must be capable of performing the calculations manually.

For example, we can assume you have access to the entire 192.168.42.0 Class C network address, and you have to create five subnets containing 25 computers each. Because this is a Class C address, you have 8 bits for the host identifier, some of which you must borrow for the subnet identifier. Using the $2^x - 2$ formula, you determine that a 3-bit subnet identifier enables you to create up to six subnets ($2^3 - 2 = 6$), leaving you a 5-bit host identifier, with which you can create up to 30 hosts ($2^5 - 2 = 30$) on each subnet. At this point, the subnetting process becomes more difficult. You still have to increment the subnet and host identifiers separately, as you did earlier with the Class A address, but you also must combine the subnet and host identifier values into a single decimal number that forms the fourth quad of the IP address.

Calculating IP Addresses Using the Binary Method

To understand the problem more clearly, it helps to view the IP address in binary form, as follows:

192 168 42 0
11000000 10101000 00101010 00000000

The first three quads of the IP address (192.168.42) are the network identifier, and these remain the same for all IP addresses on the network; only the fourth and final quad will change. To create your first subnet, you assign the subnet identifier a value of 1, which appears as follows in binary form:

001 00000
Chapter 2  Planning a TCP/IP Network Infrastructure

You then increment the host identifier, using a value of 1 for the first IP address in the first subnet, resulting in the following binary value:

001 00001

To express these binary subnet and host identifier values as a single 8-bit decimal number, you combine them before converting them, as follows:

000100001=33

The IP address of the first computer on the first subnet is therefore 192.168.42.33. To compute the address of the second computer on the same network, you increment the host identifier only and convert the result to a decimal. A 5-bit host identifier value of 2, in binary form, is 00010, which results in the following conversion:

00100010=34

The IP address of the second computer on the first subnet is therefore 192.168.42.34. You can then continue to increment the host identifier until you reach the maximum value for a 5-bit identifier, as follows:

00111110=62

The IP address of the last computer on the first subnet is therefore 192.168.42.62.

To create the second subnet, you increment the 3-bit subnet identifier from 001 to 010, and then you increment the host identifier in the same way as before. The first and last addresses on the second subnet are as follows:

01000001=65
01011110=94

The result is that the IP addresses for the second subnet range from 192.168.42.65 to 192.168.42.94. You can then continue incrementing the subnet identifier until you reach the sixth and last subnet, which provides the following first and last host values:

11000001=193
11011110=222

The range of addresses for the final subnet is therefore 192.168.42.193 to 192.168.42.222.

Calculating a Subnet Mask

In addition to calculating the IP addresses, you also have to calculate the subnet mask value for your subnetted network. Once again, this task is easier to understand if you express the values in binary form. The combined network and subnet identifiers for the Class C network in this example total 27 bits, as follows:

11111111 11111111 11111111 11000000
Lesson 3 Planning an IP Addressing and Subnetting Strategy

Because the first three quads are all ones, they all have the value 255, as in any Class C network. The binary value of the fourth quad (11100000), when converted to decimal form, is 224. The resulting subnet mask for all the computers on this Class C network is therefore 255.255.255.224.

Exam Tip In some publications, and particularly in the MCP exams, you are likely to see IP address assignments notated in the form of a network address, followed by a slash and the number of 1-bits in the subnet mask. For example, the address 192.168.42.32/27 refers to a network address of 192.168.42.32 with a subnet mask of 255.255.255.224.

Converting Binaries to Decimals
The easiest way to convert binary values to decimals is, of course, to use a calculator. The Windows Calculator in Scientific mode does this easily. However, when taking the MCSE exam, the version of Windows Calculator that you are permitted to use has standard mode only, which cannot perform binary-to-decimal conversions (or exponent calculations). Therefore, you should know how to do these calculations by hand. To convert a binary number to a decimal, you assign a numerical value to each bit, starting from the right with 1 and proceeding to the left, doubling the value each time. The values for an 8-bit number are therefore as follows:

\begin{align*}
1 & 2 & 8 & 6 & 4 & 3 & 2 & 1 \\
128 & 64 & 32 & 16 & 8 & 4 & 2 & 1
\end{align*}

You then line up the values of your 8-bit binary number with the eight conversion values, as follows:

\begin{align*}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
128 & 64 & 32 & 16 & 8 & 4 & 2 & 1
\end{align*}

Finally, you add together the conversion values for the 1-bits only:

\begin{align*}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
128 & +64 & +32 & +0 & +0 & +0 & +0 & +0 = 224
\end{align*}

Therefore, the decimal equivalent to the binary value 11100000 is 224.

Calculating IP Addresses Using the Subtraction Method
Manually calculating IP addresses using binary values can be a slow and tedious task, especially if you are going to have hundreds or thousands of computers on your network. However, when you have the subnet mask for the network and you understand the relationship between subnet and host identifier values, you can calculate IP addresses without having to convert them from binary to decimal values.
Chapter 2   Planning a TCP/IP Network Infrastructure

To calculate the network address of the first subnet, begin by taking the decimal value of the quad in the subnet mask that contains both subnet and host identifier bits and subtracting it from 256. Using the previous example of the Class C network with the subnet mask of 255.255.255.224, the result of 256 minus 224 is 32. The network address of the first subnet is therefore 192.168.42.32. To calculate the network addresses of the other subnets, you repeatedly increment the result of your previous subtraction by itself. For example, if the network address of the first subnet is 192.168.42.32, the addresses of the remaining five subnets are as follows:

192.168.42.64  
192.168.42.96  
192.168.42.128  
192.168.42.160  
192.168.42.192

To calculate the IP addresses in each subnet, you repeatedly increment the host identifier by one. The IP addresses in the first subnet are therefore 192.168.42.33 to 192.168.42.62. The 192.168.42.63 address is omitted because this address would have a binary host identifier value of 11111, which is a broadcast address. The IP address ranges for the subsequent subnets are as follows:

192.168.42.65 to 192.168.42.94  
192.168.42.97 to 192.168.42.126  
192.168.42.129 to 192.168.42.158  
192.168.42.161 to 192.168.42.190  
192.168.42.193 to 192.168.42.222

Practice: Subnetting IP Addresses

For each of the following IP address assignments, specify the number of bits in the subnet identifier, the number of possible IP addresses in each subnet, the subnet mask for the IP addresses, and the IP address ranges for the first and last subnet.

10.0.0.0/19

1. Number of bits in subnet identifier: ____________  
2. Number of possible IP addresses in each subnet: ____________  
3. Subnet mask: ____________  
4. First subnet: ____________  
5. Last subnet: ____________
Lesson 3 Planning an IP Addressing and Subnetting Strategy

192.168.214.0/29

1. Number of bits in subnet identifier: __________
2. Number of possible IP addresses in each subnet: __________
3. Subnet mask: __________
4. First subnet: __________
5. Last subnet: __________

172.28.0.0/20

1. Number of bits in subnet identifier: __________
2. Number of possible IP addresses in each subnet: __________
3. Subnet mask: __________
4. First subnet: __________
5. Last subnet: __________

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 the correct formula for calculating the number of subnets or hosts you can create with a given number of bits represented by $x$?
   a. $x^2 + 2$
   b. $2^x + 2$
   c. $2^x - 2$
   d. $x^2 - 2$

2. What is the correct subnet mask to use on a Class B network with a 10-bit subnet identifier?
   a. 255.192.255.255
   b. 255.255.255.192
   c. 255.255.192.0
   d. 255.192.0.0
3. How many hosts can you create on a subnet with 9 bits available for the host identifier?

4. In the IP address assignment 10.54.113.0/24, what does the number 24 represent?
   a. The number of bits in the subnet identifier
   b. The number of bits in the host identifier
   c. The number of bits in the combined subnet and host identifiers
   d. The number of bits in the combined network and subnet identifiers

5. Which IP address class provides the largest number of hosts per subnet?

Lesson Summary

- If you require registered IP addresses for your network, you must obtain them from your ISP. For an unregistered network, you can use any of the addresses in the private address ranges designated by the IANA.
- You can create subnets using any network address by using some of the host identifier bits to create a subnet identifier.
- You use the formula $2^x - 2$ to calculate how many hosts or subnets you can create using a given number of bits.
- You can calculate subnet masks and IP addresses by using the binary values of the numbers, incrementing them as needed, and then converting the results back into decimals.
Lesson 4: Assigning IP Addresses

Once you have calculated the IP addresses and subnet mask for the computers on your network, you should include in your plan just how the actual TCP/IP configuration process for each of the computers is going to proceed. There are two basic alternatives from which to choose. You can manually configure each computer, or you can use DHCP, an automated TCP/IP configuration service included with Windows Server 2003 and many other operating systems.

After this lesson, you will be able to

- List the drawbacks of manual TCP/IP client configuration
- Understand how DHCP automatically configures TCP/IP clients

Estimated lesson time: 15 minutes

Manually Configuring TCP/IP Clients

Configuring the TCP/IP client on a Windows computer by hand is a relatively simple task, but when compounded by hundreds or thousands of computers, it can become an administrative nightmare. Not only does an administrator have to travel to each computer to configure its settings, but the administrator must also take steps to ensure that each computer is assigned an IP address that is appropriate for the subnet on which the computer is located and that does not duplicate the IP address of any other computer in the enterprise. For a large network installation in which time is at a premium, you might have to bring in temporary personnel to help with the TCP/IP configuration chores.

Planning  Keep in mind that in addition to the time and staff needed to perform the initial TCP/IP configurations, you will also need to spend time to manually reconfigure a computer if you later decide to move it to a different subnet.

Off the Record  For a large network installation, manually configuring TCP/IP clients is time-consuming, inefficient, and prone to errors. DHCP enables you to automatically configure your computers and reconfigure them each time they start up. If you decide to move a computer to a different subnet, DHCP assigns it a new address and reclaims the old one for assignment to another computer.
Installing a DHCP Server

DHCP consists of an application layer protocol and a service running on one or more of your network servers. Windows Server 2003 includes a DHCP implementation, as do most other network server operating systems. All current Windows operating systems also include DHCP client capabilities, which activate by default. If you install Windows XP on a new computer, for example, and connect it to a network, during the computer's first boot sequence it transmits messages requesting an IP address assignment to any DHCP servers on the network. DHCP servers can assign IP addresses and subnet masks, and they can also provide other configuration settings, including default gateway addresses and Domain Name System (DNS) server addresses.

To set up a Windows Server 2003 DHCP server:

1. Install the service on the computer.
2. Configure it by specifying a range of IP addresses for the DHCP server to assign, called a scope.
3. Optionally, configure a variety of DHCP options that provide the other TCP/IP configuration parameters your computers need, such as the list of DNS servers available to the client.
4. Activate the scope and, if you are using the Active Directory directory service on your network, authorize the DHCP server in the Active Directory database.

Understanding DHCP Allocation Methods

The Windows Server 2003 DHCP server can assign IP addresses using three different allocation methods, which are as follows:

- **Dynamic allocation** Assigns an IP address to a client computer from a scope, for a specified length of time. DHCP servers using dynamic allocation only lease addresses to clients. Each client must periodically renew the lease to continue using the address. If the client allows the lease to expire, the address is returned to the scope for reassignment to another client.

  Note Dynamic allocation is the default method for the Windows Server 2003 DHCP server, and it is particularly suitable for networks where IP addresses are in short supply or for networks on which you frequently move computers from one subnet to another.

- **Automatic allocation** Permanently assigns an IP address to a client computer from a scope. Once the DHCP server assigns the address to the client, the only way to change it is to manually reconfigure the computer. Automatic allocation is suitable for networks where you do not often move computers to different subnets. It reduces network traffic by eliminating the periodic lease renewal messages.
needed for dynamic allocation. In the Windows Server 2003 DHCP server, automatic allocation is essentially dynamic allocation with an indefinite lease.

- **Manual allocation** Permanently assigns a specific IP address to a specific computer on the network. In the Windows Server 2003 DHCP server, manually allocated addresses are called reservations. You use manually allocated addresses for computers that must have the same IP address at all times, such as Internet Web servers that have their IP addresses associated with their host names in the DNS namespace. Although you can just as easily configure such computers manually, DHCP reservations prevent the accidental duplication of permanently assigned IP addresses.

**Planning a DHCP Deployment**

To configure the TCP/IP clients on your computers using DHCP, you must specify in your network infrastructure plan how many DHCP servers you intend to deploy and where to locate them. DHCP clients rely on broadcast transmissions to locate and contact DHCP servers. This means that a DHCP client can only communicate directly with a DHCP server on the same LAN. Fortunately, this does not mean you have to install a DHCP server on every one of your LANs. Most routers are equipped with DHCP relay-agent capabilities you can use to support multiple networks with one DHCP server.

A **DHCP relay agent** is a module you configure with the IP addresses of DHCP servers on other networks. The relay agent listens for broadcast transmissions from DHCP clients, and when it receives them, it forwards the messages to the DHCP servers on another network. The relay agent then functions as the intermediary between the DHCP client and server during the entire configuration process.

Although one DHCP server can configure thousands of clients, most network designers deploy several servers for fault tolerance purposes. However, when you have multiple Windows Server 2003 DHCP servers on your network, you must configure them with separate IP address scopes. DHCP servers do not work together. Each server has its own scopes, from which it allocates IP addresses. If you configure two DHCP servers with scopes that contain the same IP address ranges, you will end up with duplicate IP addresses on your network.

You can configure two DHCP servers with scopes to service the same subnet, however. Microsoft recommends that you distribute the IP addresses for a subnet in an 80:20 ratio. Configure one server with a scope containing 80 percent of the addresses available for the subnet, and then configure a second server with the remaining 20 percent of the addresses for that subnet. This provides a fault-tolerance mechanism in case one of the servers fails for an extended length of time.
Practice: Installing and Configuring the DHCP Service

In this practice, you install, authorize, and configure the DHCP service on Server01. You also create a scope and configure a range of addresses for the scope.

**Caution** For this exercise, ensure that Server01 is on an isolated network (or no network at all) so that it doesn’t conflict with IP addressing strategy already in place.

**Exercise 1: Installing and Authorizing the DHCP Server**

In this exercise, you install and authorize the DHCP Server service on Server01.

1. Log on to Server01 as Administrator.

2. Click the Start menu, point to Control Panel, and then click Add Or Remove Programs. The Add Or Remove Programs window appears.

3. In the left frame, click Add/Remove Windows Components. The Windows Components Wizard appears.

4. In the Components box, scroll down and click Networking Services, but do not click or change the status of the check box to the left of this option.

**Note** Windows Server 2003 has already selected the Networking Services check box because you’ve already installed some networking services on Server01.

5. Click Details. The Networking Services dialog box appears.
   In the Subcomponents Of Networking Services box, select the Dynamic Host Configuration Protocol (DHCP) check box.

6. Click OK. The Windows Components page reappears.

7. Click Next. The Configuring Components page shows a progress indicator as the changes you requested are made. The Completing The Windows Components Wizard page appears.

8. Click Finish.

9. Close the Add Or Remove Programs window.

10. Click the Start menu, point to All Programs, point to Administrative Tools, and then click DHCP. The DHCP console appears and Server01.contoso.com [10.0.0.1] is listed in the console tree.

11. In the console tree, expand Server01.contoso.com [10.0.0.1]. A red down-arrow appears to the left of Server01.contoso.com [10.0.0.1].
Lesson 4  Assigning IP Addresses

12. Click Server01.contoso.com [10.0.0.1] and, from the Action menu, select Authorize. The red down-arrow remains until you create at least one scope. Leave the DHCP console open to complete the next exercise.

Exercise 2: Creating and Configuring a DHCP Scope

In this exercise, you create and configure a DHCP scope on Server01.

1. Verify that Server01.contoso.com [10.0.0.1] is highlighted, and then from the Action menu, select New Scope. The New Scope Wizard appears.

2. Click Next. The Scope Name page appears.

3. In the Name text box, type **Scope01**.

4. In the Description text box, type **Training network**, and then click Next. The IP Address Range page appears.

5. Type **10.0.0.1** in the Start IP Address text box, and type **10.0.0.254** in the End IP Address text box.

6. In the Subnet Mask text box, notice that the server automatically changes the mask to **255.0.0.0**.

7. Check the value in the Length spin box. Notice that the server automatically enters 24 for the subnet mask length. This means that 24 bits of the IP address are allocated to the network address. Eight bits remain for allocating host addresses on the network.

8. Click Next. The Add Exclusions page appears.

9. In the Start IP Address text box, type **10.0.0.1**.

10. In the End Address text box, type **10.0.0.1**.

11. Click Add.

12. Notice that 10.0.0.1 To 10.0.0.11 appears in the Excluded Address Range box.

13. Click Next. The Lease Duration page appears. Read the information on this page, and notice that the default lease duration is 8 days.

14. Click Next to accept the default lease duration. The Configure DHCP Options page appears, asking if you would like to configure the most common DHCP options now.

15. Select the No, I Will Configure These Options Later option button, and then click Next. The Completing The New Scope Wizard page appears.

16. Read the instructions on this screen, and then click Finish. An icon representing the new scope appears in the DHCP console.

Notice that Server01.contoso.com now contains a green up-arrow. This is because you have authorized the server and created a scope. The red down-arrow to the left of the
scope indicates you have not yet activated the scope. You will activate the scope in a later procedure.

Leave the DHCP console open to complete the next exercise.

Exercise 3: Configuring Scope Options

In this exercise, you configure DHCP so that it sends the preferred DNS and DNS domain name to the DHCP client upon registration. This procedure is similar to setting server options, which apply to all DHCP clients using this server, and setting individual client options.

1. In the console tree, expand Scope01, click Scope Options, and then from the Action menu, click Configure Options. The Scope Options dialog box appears.

2. In the General tab, scroll down and select the 006 DNS Servers check box, which enables the options in the Data Entry group box.

3. In the Server Name text box, type server01 and then click Resolve. The IP address 10.0.0.1 appears in the IP Address text box.

4. Click Add.

5. Scroll down in the Available Options box, and select the 015 DNS Domain Name checkbox.

6. In the String Value text box, type contoso.com and then click OK. The DHCP server will now deliver the DNS data to DHCP client computers within this scope along with their IP addresses.

7. Select Server01.contoso.com [10.0.0.1] and, from the Action menu, select Activate. The scope is now activated.

8. Close the DHCP console.

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 type of DHCP address allocation would you typically use for an Internet Web server? Why?
2. What configuration tasks must you perform on a newly installed Windows XP workstation to activate the DHCP client?

3. What is the function of a DHCP relay agent?

Lesson Summary

- You can configure the TCP/IP clients on your network manually, or you can use DHCP servers to automatically allocate IP addresses and other configuration parameters to your computers as needed.

- A DHCP server using manual allocation assigns specific IP addresses to specific clients permanently. Administrators typically use manual allocation for Internet servers and other computers that require static IP addresses.

- A DHCP server using permanent allocation assigns IP addresses from a pool to DHCP clients, which retain them until an administrator manually reconfigures them.

- A DHCP server using dynamic allocation assigns IP addresses to DHCP clients from a pool, and then reclaims them when a specified lease period expires.

- DHCP relay agents forward the DHCP broadcast messages generated by clients to DHCP servers on other networks. This enables a single DHCP server to furnish IP addresses for an entire internetwork.
Lesson 5: Troubleshooting TCP/IP Addressing

Using the TCP/IP protocol suite on your network tends to be more problematic than using other protocols, in large part because of the need to individually configure each computer. Most isolated TCP/IP communications problems are related to the client configuration process in some way, and a large part of the TCP/IP troubleshooting process is recognizing the effects of various configuration errors.

After this lesson, you will be able to
■ Determine whether a network communications problem is related to TCP/IP
■ Understand how TCP/IP client configuration problems can affect computer performance
■ List the reasons why a DHCP client might fail to obtain an IP address from a DHCP server

Estimated lesson time: 20 minutes

Isolating TCP/IP Problems

When a computer experiences a network communications problem, there are obviously many possible sources of error. The difficulty could lie in the TCP/IP protocol stack, it could be a problem with the data-link layer protocol, or it could even be a hardware problem such as a broken cable or a faulty network interface adapter. Before you begin troubleshooting possible TCP/IP problems, you should make sure the trouble is in fact related to the TCP/IP stack.

One sure way to test whether a network communications problem is related to TCP/IP is to try using a different protocol on the computer. NetBIOS Extended User Interface (NetBEUI) is the best choice for this type of test because it is a single, monolithic protocol and requires no configuration. However, Windows Server 2003 no longer includes the NetBEUI protocol, so you can use the IPX protocols for testing, in the form of the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol module, instead.

To do this, you install the NetBEUI or IPX protocol module in the Network Connections tool and then unbind the Internet Protocol (TCP/IP) module in the Advanced Settings dialog box. (To access the Advanced Settings dialog box, right-click Network Connections in the Control Panel menu, click Open to display the Network Connections window, and then select Advanced Settings from the Advanced menu in the Network Connections window, as shown in Figure 2-7.) At this point, you’ve activated the alternative protocol and deactivated the TCP/IP module. If the computer is still unable to communicate with the other computers on the network, you know the problem is not related to TCP/IP. You should start looking at the networking hardware and the computer’s data-link layer protocol drivers. If the computer can communicate using the alternative protocol but it can’t by using TCP/IP, you know there is a TCP/IP-related problem, most likely related to the protocol’s configuration.
Troubleshooting Client Configuration Problems

The most obvious source of problems on a TCP/IP network is the existence of duplicate IP addresses. When two computers have the same IP address, packets end up in the wrong place and message transactions are interrupted. Fortunately, the Windows operating systems check for the existence of a duplicate address each time the computer starts. If Windows detects a duplicate IP address, it disables the TCP/IP protocol stack on the newly started computer and displays an error message specifying the hardware address of the system with which the computer is in conflict. The computer that is the original owner of the duplicate address continues to function normally. When you reconfigure the other computer with a different, nonconflicting IP address, the TCP/IP stack becomes active again on that computer.

Incorrect Subnet Masks

As you learned earlier in this chapter, the function of the subnet mask is to let the computer know which bits of the computer’s IP address identify the host and which bits identify the network on which the host is located. If two computers have different subnet masks, their network addresses are different, and the computers see them as being on different subnets even if they have correct IP addresses. Computers that are on different subnets cannot communicate with each other except through a router, so if you have a computer that can’t communicate with the other systems on the network, the problem might be that the computer’s subnet mask is incorrect.
Chapter 2 Planning a TCP/IP Network Infrastructure

To view the subnet mask and all the other TCP/IP configuration settings at once on a computer running Windows 2000, Windows XP, or Windows Server 2003, you can use the Ipconfig.exe program. Display a Command Prompt window, type **IPCONFIG /all** on the command line, and press Enter to generate a display like the following:

```
Windows IP Configuration
    Host Name . . . . . . . . . . . .: CZ7
    Primary DNS Suffix . . . . . . .: adatum.com
    Node Type . . . . . . . . . . . .: Hybrid
    IP Routing Enabled. . . . . . . .: No
    WINS Proxy Enabled. . . . . . . .: No
    DNS Suffix Search List. . . . . . .: adatum.com
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . .:
    Description . . . . . . . . . . . .: Intel(R) PRO/100 VE Network Connection
    Physical Address . . . . . . . . .: 00-D0-59-83-B1-52
    DHCP Enabled. . . . . . . . . . .: No
    IP Address. . . . . . . . . . . .: 192.168.2.7
    Subnet Mask . . . . . . . . . . .: 255.255.255.0
    Default Gateway . . . . . . . . .: 192.168.2.99
    DNS Servers . . . . . . . . . . .: 192.168.2.10
                192.168.86.15
    Primary WINS Server . . . . . . .: 192.168.2.10
```

Incorrect Default Gateway Addresses

If a TCP/IP computer is able to communicate with other systems on the same LAN but is unable to communicate with systems on other LANs, there is likely a problem with the computer's default gateway. The default gateway is the router that a computer uses whenever it has to communicate with a computer on another network. The routing table of a TCP/IP computer contains specific network addresses and information on how to reach them. If the computer must send traffic to a system on one of the networks listed in the table, the computer uses that table entry to route the packets properly. If the computer has traffic to send to a system on a network that is not listed in the table, the computer sends the traffic to the default gateway.

If a TCP/IP computer does not have a default gateway address in its configuration, it can communicate with the other systems on the LAN (because no router is needed), but it can't communicate with other networks. In the same way, if the default gateway address is incorrect and doesn't point to a router, or points to a router that is not functioning properly, no internetwork communication can occur. If you find that one of your computers is impaired in this way, you should check the Default Gateway setting in the Internet Protocol (TCP/IP) Properties dialog box if your computer uses a static IP address (see Figure 2-8), or by using the IPCONFIG /all command if the computer has obtained its address from a DHCP server. If the default gateway address is correct, you should check the functionality of the default gateway itself to make sure that it is running and routing traffic.
Name Resolution Failures

A common cause of TCP/IP communication problems is a failure to successfully resolve names into IP addresses. TCP/IP network communication is based on IP addresses. Every message packet generated by a TCP/IP computer contains a destination IP address and a source IP address. IP addresses are difficult for human beings to use and remember, however. As a result, the TCP/IP developers devised services like DNS and the Windows Internet Name Service (WINS), which enable people to use friendly names for computers instead of IP addresses.

Name resolution is the process by which a computer converts a name into an IP address. In the case of DNS names, for example, the computer sends the name to a DNS server, which replies with the IP address associated with the name. The computer can then initiate communications using the IP address rather than the name.

If a TCP/IP computer fails to communicate with another computer, it might be because the name resolution has failed. This means that the two computers are both functioning properly; they just don’t have the IP addresses they need to communicate. To test for a name resolution failure, try to communicate with the destination computer using its IP address instead of its name. For example, if you are trying to contact a Web server using the uniform resource locator (URL) http://www.adatum.com/home.html and you cannot connect, try using the server’s IP address instead of its name, as in the URL http://10.112.65.34/home.html. If the connection succeeds, the problem lies in the name resolution.
Windows computers can use either DNS or WINS for name resolution. If your network uses the Active Directory directory service, it relies on DNS for name resolution. DNS name resolution is also required for Internet connectivity. To resolve DNS names into IP addresses, the computer must have the IP address of a functioning DNS server as part of its TCP/IP configuration. If the DNS server address is incorrect, or if the DNS server itself is malfunctioning, name resolution cannot occur and TCP/IP communication attempts that use names will fail. The Internet Protocol (TCP/IP) Properties dialog box (see Figure 2-8) enables you to specify a preferred DNS server address and an alternate DNS server address. The latter provides fault tolerance if the preferred server is unreachable or malfunctioning. You can check the validity of the addresses in a computer's TCP/IP configuration by using the Nslookup.exe program from the command prompt to send a name resolution request to those specific servers. If the Nslookup test fails, either the address does not point to a valid DNS server or the DNS server itself is malfunctioning.

If you are running WINS on your network, your computers must have the IP address of one or more WINS servers specified in the WINS tab of the Advanced TCP/IP Settings dialog box (see Figure 2-9). WINS is one of several NetBIOS name resolution mechanisms that Windows computers can use, so an incorrect WINS server address or even the failure of a WINS server to resolve names might not be as immediately evident as a DNS problem. Windows computers can resolve the NetBIOS names of systems on the local LAN even without WINS (by using broadcast transmissions as a fallback). However, if the WINS server addresses are incorrect or the servers are not functioning, the computer cannot resolve the NetBIOS names of computers on other LANs (because broadcasts are limited to the local network).

![Figure 2-9 The WINS tab of the Advanced TCP/IP Settings dialog box](image-url)
Note

Name resolution is an important issue on a Windows network, and an important part of network infrastructure planning. For more information on name resolution, see Chapter 4, “Planning a Name Resolution Strategy.”

Troubleshooting DHCP Problems

If you are using DHCP servers to automatically configure the TCP/IP clients in your network’s computers, there are still problems that can arise with the DHCP clients and the DHCP server. Some of these problems and their solutions are described in the following sections.

Failure to Contact a DHCP Server

When you configure your Windows computers to obtain their IP addresses and other TCP/IP configuration settings from a DHCP server, you may sometimes find that the DHCP server has apparently assigned an incorrect IP address to a computer. No matter what address scope you have configured the DHCP server to use, a client might have an address that begins with 169.254. This is not an address that the DHCP server has assigned. Rather, the computer has failed to contact the DHCP server on the network and has assigned itself an IP address using a Windows feature called Automatic Private IP Addressing (APIPA).

APIPA is designed to enable Windows computers on a small LAN to configure their own IP addresses. For example, if you connect a few computers to build a home network, there is no need to manually configure the IP addresses because APIPA automatically assigns a unique address in the same Class B subnet to each computer on the network. This is fine for a home or small business network, but it is not acceptable on your carefully planned large network installation.

When a DHCP client resorts to using APIPA to obtain an IP address, it is because the DHCP messages the computer has broadcasted on the network have gone unanswered. There are several reasons why this might happen. First, the computer might be unable to communicate with the network at all because of a hardware or data-link layer protocol problem. You can test that theory by installing another network/transport layer protocol on the computer. If no network communications are possible with the alternative protocol, it is time to start looking at the computer’s networking hardware and data-link layer protocol drivers.

Tip

After you determine that the problem is due to the client hardware or software configuration and then correct the problem, you must delete the APIPA-supplied address from the system’s TCP/IP configuration before it can send another request to the DHCP server.
The client’s failure to obtain an IP address from the DHCP server might also result from a problem at the server end of the connection. If this is the case, you will see the same problem on multiple client computers. The DHCP server might be experiencing a hardware or software problem of its own, preventing it from communicating with the network. You can use the same alternative protocol test to determine if this is the case.

The DHCP requests that clients transmit to servers are broadcast messages; they must be because the client does not yet have the IP address needed to send a unicast message. Broadcasts are limited to the local network, so if the DHCP server is not on the same LAN as the client, it cannot receive the request directly. You must use a DHCP relay agent for a DHCP server to support clients on other networks, and this introduces another potential source of communication problems. DHCP relay agents are built into the routers that connect networks or are supplied by the RRAS service in Windows Server 2003, and you must configure them with the addresses of the DHCP servers on the other networks. This is so that the relay agent can receive the broadcasts from DHCP clients and send them to the DHCP servers on the other networks as unicasts. If you have forgotten to configure the relay agent, or if you have configured it with an incorrect DHCP server address, the clients’ attempts to contact the DHCP server will fail.

**Failure to Obtain an IP Address**

In some cases, DHCP clients might be able to communicate with the network but are still failing to obtain IP address assignments from DHCP servers. This could be because of an incorrect scope on the server or because of an error in the server’s own TCP/IP configuration. You should check the scope itself first, to be sure that you have created it correctly and that you have activated it. Also be sure that the DHCP Server service is running on the server computer and that the DHCP server is authorized by Active Directory (if you are using Active Directory on your network).

Using regular scopes, a DHCP server can only supply IP addresses to subnets of which the server itself is a member. For example, if you create a scope to supply your DHCP clients with IP addresses on the 192.168.67.0/24 subnet, the DHCP server must have an IP address in that subnet itself.

**Note** DHCP servers must have manually configured IP addresses. They cannot obtain their addresses from another DHCP server or supply one to themselves.

When the DHCP server is servicing clients on the local network, having an IP address on the same subnet is usually not a problem. However, if you have multiple IP subnets on a single physical network, or if the DHCP server is providing addresses to distant networks using relay agents, you must create scopes for networks other than the one to which the DHCP server is connected. To enable the server to supply addresses to the clients on other subnets, you can either configure the DHCP server with multiple IP
addresses, one in each subnet for which you have created a scope, or you can combine the scopes for the various subnets into a superscope. A superscope is an administrative grouping of existing scopes supporting multiple IP subnets on the same physical network, which you can activate and deactivate collectively.

**Failure to Obtain Correct DHCP Options**

When you configure a DHCP server, creating a scope enables the server to assign IP addresses to clients and supply them with a correct subnet mask. For all other TCP/IP configuration parameters, such as default gateway and DNS server addresses, you must configure the server to deliver DHCP options along with the IP address. DHCP options are specific configuration parameter settings that the server can deliver along with the IP address and subnet mask. The DHCP server in Windows Server 2003 enables you to configure DHCP options for specific scopes or for the entire server. For example, if you want all your DHCP clients, no matter what subnet they are on, to use the same DNS server, you should create a server option. For the default gateway address (called the 003 Router option by DHCP), you should use scope options because the computers on each scope need a different gateway address.

If your DHCP clients are receiving IP addresses but are not receiving their DHCP options properly, you should first check to see whether you have mistakenly created a scope option instead of a server option, or whether you have created a scope option for the wrong scope. It is also possible the client does not support a particular option that you have configured the server to provide. Microsoft’s DHCP server is designed to support clients running many different operating systems and contains many options that are exclusive to non-Windows clients.

**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. When a TCP/IP computer can communicate with the local network but not with computers on other networks, which of the following configuration parameters is probably incorrect?
   a. IP address
   b. Subnet mask
   c. Default gateway
   d. Preferred DNS server
2. How do you determine whether name resolution failure is the cause of a network communication problem?

3. Why must a DHCP client use broadcast transmissions to request an IP address from a DHCP server?
   - Because the DHCP server can only receive broadcasts
   - Because the DHCP client does not yet have an IP address
   - Because the DHCP server can service requests only from computers on the same LAN
   - Because the DHCP client must inform all the other clients on the network of its intention to request an IP address

Lesson Summary

- An incorrect subnet mask makes the computer appear to be on a different network, preventing LAN communications.
- A missing or incorrect default gateway address prevents communication with other networks.
- A missing or incorrect DNS or WINS server address can prevent the computer from resolving other systems' names.
- When a Windows Server 2003 DHCP client fails to make contact with a DHCP server, the client computer uses APIPA to assign itself an IP address.
- Most DHCP communication problems that are not the result of hardware or driver errors are caused by incorrect configuration of the DHCP client, server, or relay agent.

Case Scenario Exercise

You are the network infrastructure design specialist for Litware Inc., a manufacturer of specialized scientific software products, and you have already created a basic network design for their new office building, as described in the Case Scenario Exercise in Chapter 1. The office building is a three-story brick structure built in the late 1940s, which has since been retrofitted with several different types of network cabling by various tenants. In your original design, each floor of the building has a separate Ethernet LAN, as follows:

- **First Floor** Ten individual offices, each with a single computer using 100Base-TX Fast Ethernet
- **Second Floor** Fifty-five cubicles, each with a single computer using 10Base-T Ethernet
Third Floor  A laboratory setting with network connections for up to 100 computers using 100Base-FX Fast Ethernet

The three LANs are all connected to a backbone network that is running 1000Base-T Gigabit Ethernet and using dedicated computers running Windows Server 2003 as routers. In addition to connecting the LANs, the backbone network is connected to the corporate headquarters network in another city using a hardware router and a T-1 line. A second T-1 line to the corporation's ISP is connected to the backbone using an Internet access router.

The Litware home office has also recently notified you that you must modify the network design because they have now decided to use the new facility to house the corporation's Internet Web servers. To accommodate this addition, you add another LAN to the design, located in the building's locked basement. The basement LAN consists of six Web servers running Windows Server 2003, connected by 100Base-TX Fast Ethernet and running on Category 5 unshielded twisted pair (UTP) cable. One of the computers running Windows Server 2003 also has a 1000Base-T Gigabit Ethernet adapter installed in it, enabling it to route traffic to the backbone.

Because the Web servers must be visible from the Internet so that potential customers can access them, they must have IP addresses that are registered with the IANA. The home office has informed you that the corporation has obtained the registered Class C network address 207.46.230.0 from its ISP. The company has already subnetted the address using a 3-bit subnet identifier. All the subnets are already in use by other company offices except for the last one, which is available for your use.

For the three remaining LANs, you have decided to use unregistered IP addresses. The computers on these networks will be able to access the Internet using the NAT capabilities of the Internet access router on the backbone. Your IP addressing plan calls for using a single private network address, 172.19.0.0/22, with one (and only one) subnet allocated to each of the four unregistered LANs.

Given this information, answer the following questions about your IP addressing plan:

1. What subnet mask should you use for the Web server computers on the basement LAN?

2. How many subnets are there on the 207.46.230.0/27 network in total, and how many hosts can there be on each subnet?
3. What is the range of registered IP addresses available for your use?

4. How many routers are there on the building’s networks? How many of the routers are computers running Windows Server 2003, and how many are hardware devices?

5. Which of the following IP address classes can you not use when selecting a network address for your unregistered LANs? (Choose all that apply.)
   a. Class A
   b. Class B
   c. Class C
   d. Class D

6. For each answer you selected in question 5, explain why you cannot use an address in that class for your unregistered LANs.

7. Assuming that you will use a network address in the Class B private address range designated by the IANA, what is the maximum number of subnet identifier bits you can use and still have a sufficient number of host identifier bits to support the computers on each of your networks?

8. Using the network address specified earlier, how many subnet identifier bits are you using for your unregistered network address?

9. What subnet mask must you use for the unregistered LANs on your network?
10. List the IP address ranges for the first four subnets created from your unregistered network address.

---

**Troubleshooting Lab**

You are deploying DHCP on a newly constructed network consisting of four horizontal LANs connected to a backbone network. Each of the five LANs is a separate IP subnet. You have installed the Microsoft DHCP Server service on one Windows Server 2003 computer that is connected to the backbone network, and you have installed and configured a DHCP relay agent on each of the four routers connecting the backbone to the horizontal LANs. After configuring the DHCP server by creating the appropriate scopes and options, you start the client computers.

For each of the problem scenarios below, specify which listed conditions (a, b, c, or d) could be the cause of the difficulty.

- **a.** One of the DHCP relay agents is improperly configured.
- **b.** One of the scopes on the DHCP server has not been activated.
- **c.** One of the cables connecting a client to its hub has been accidentally cut.
- **d.** The Router (default gateway) option on the DHCP server is configured as a server option, not a scope option.

1. All of the computers successfully obtain IP addresses from the DHCP server except one, which has an IP address of 169.254.0.1.
2. All of the computers on one of the five horizontal LANs fail to obtain IP addresses from the DHCP server.
3. All of the computers on the backbone LAN fail to obtain IP addresses from the DHCP server.
4. The computers on four of the five LANs are able to communicate with the local network only.
Chapter Summary

- Computers that are visible from the Internet must have IP addresses that are registered with the IANA.
- Computers on private networks typically use unregistered IP addresses to protect them from unauthorized access and to conserve the IP address space.
- Computers with unregistered IP addresses can access the Internet as clients using a NAT router or a proxy server.
- Large networks typically consist of multiple LANs connected by routers, network layer devices that enable communication between the networks while maintaining separate broadcast and collision domains.
- A switch is a data-link layer device that intelligently forwards traffic to specified destinations. Switches can replace many routers in your network infrastructure design, creating a more efficient and economical network.
- If you require registered IP addresses for your network, you must obtain them from your ISP. For an unregistered network, you can use any addresses in the private address ranges designated by the IANA.
- You can create subnets using any network address by using some host identifier bits to create a subnet identifier. You can calculate subnet masks and IP addresses by using the binary values of the numbers, incrementing them as needed, and then converting the results back into decimals.
- You can configure the TCP/IP clients on your network manually, or you can use DHCP servers to automatically allocate IP addresses and other configuration parameters to your computers as needed.
- Most DHCP communication problems that are not the result of hardware or driver errors are caused by incorrect configuration of the DHCP client, server, or relay agent.

Exam Highlights

Before taking the exam, review the following key topics and terms 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

- Every computer on a TCP/IP network must have a unique IP address. Computers visible to the Internet must have registered addresses. Computers accessing the Internet through NAT routers or proxy servers can use unregistered addresses.

- Routers are network layer devices that connect networks into an internetwork while keeping their collision domains and broadcast domains separate.

- Switches are data-link layer devices that connect networks into one large network. Although switching all but eliminates collisions from an Ethernet installation, the network still consists of one large broadcast domain.

- To subnet a network, you borrow some bits from the host identifier and use them to create a subnet identifier. You can then split a network address into separate subnets, each of which is a separate entity on a TCP/IP network.

- Most TCP/IP communications problems are the result of incorrect configuration settings on the TCP/IP client. The problems can result from typographical errors during a manual client configuration or from incorrect configuration of a DHCP server or relay agent.

Key Terms

Network address translation (NAT) A router function that enables client computers on a private network with unregistered IP addresses to access Internet resources without exposing themselves to possible intrusion from the Internet.

Proxy server An application layer software component that relays transmissions between unregistered client computers on a private network and the Internet. Proxy servers can also regulate client access to specific Internet resources and cache Internet information for rapid access by other clients.

Collision domain A group of computers connected so that any two systems transmitting packets at the same time will cause a collision. Computers connected to a shared Ethernet hub, for example, are said to be in the same collision domain. Connecting two LANs with a router creates an internetwork with two separate collision domains.

Broadcast domain A group of computers connected so that a broadcast message transmitted by any system will reach all other connected computers. Computers connected by hubs or switches form a single broadcast domain. Connecting two LANs with a router creates an internetwork with two separate broadcast domains.
Lesson 1 Practice

For each of the following types of computers, specify whether it should have a registered or an unregistered IP address, or both, and why.

1. A corporate Web server providing product information to Internet clients around the world
   Registered, because for clients on the Internet to send requests to the server, the server must have a registered IP address

2. A NAT router enabling clients on a private network to access Internet servers
   Both, because the NAT router must be connected to the private network to communicate with the clients, and it must connect to the Internet so that it can communicate with the Web servers

3. An intranet Web server on a private network used to provide human resources information to employees
   Unregistered, because although the computer is a Web server, the clients are also located on the private network and the server does not have to be visible to the Internet

4. A client computer that accesses Web servers on the Internet using a NAT router
   Unregistered, because the NAT router is responsible for communicating with the Internet servers requested by the client

5. A proxy server providing Internet Web access to clients on a private network
   Registered, because the proxy server is responsible for sending the clients’ requests to the Web servers on the Internet

Lesson 1 Review

1. Which of the following statements about NAT routers and proxy servers are true? Choose all answers that are correct.
   a. NAT routers and proxy servers must have two IP addresses.
   b. A NAT router can provide Internet access to any client application on the private network.
   c. Proxy servers can cache information they receive from Internet servers.
   d. The Windows Server 2003 operating system includes a proxy server.

   b and c

2. What are the two primary reasons why you should use unregistered IP addresses for Internet client computers?

   To conserve the public IP address space and to protect the private network from unauthorized access by Internet predators.
3. Which of the following best describes the function of a subnet mask?
   a. A subnet mask indicates whether an IP address is registered or unregistered.
   b. A subnet mask specifies the sizes of the network and host identifiers in an IP address.
   c. A subnet mask is a value assigned by the IANA to uniquely identify a specific network on the Internet.
   d. A subnet mask enables an IP address to be visible from the Internet.

Lesson 2 Practice

Exercise 1: Internetwork Design with a Single Broadcast Domain and Multiple Collision Domains

In the following diagram, add the components needed to connect the LANs to an internetwork that consists of a single broadcast domain and several collision domains.

![Diagram of network design with a single broadcast domain and multiple collision domains]
Exercise 2: Internetwork Design with Multiple Broadcast and Collision Domains

In the following diagram, add the components needed to connect the LANs in an internetwork that consists of five broadcast domains and five collision domains.

Lesson 2 Review

1. Replacing the hubs and routers on an internetwork with switches creates a network that has which of the following?
   a. One broadcast domain and one collision domain
   b. One broadcast domain and multiple collision domains
   c. One collision domain and multiple broadcast domains
   d. Several collision domains and several broadcast domains

b
2. Specify the OSI reference model layer at which each of the following devices operates.
   a. A switch
   b. A router
   c. A hub
   a. Data-link, b. Network, c. Physical

3. Which of the following Windows Server 2003 TCP/IP configuration parameters specifies the address of a router?
   a. Preferred DNS server
   b. Subnet mask
   c. Default gateway
   d. IP address
   c

4. When you replace the routers on an internetwork with switches that include no VLAN or layer 3 capabilities, which of the following is a possible reason for poor network performance?
   a. Excessive collisions
   b. Excessive broadcast traffic
   c. Excessive number of workstations on the LAN
   d. Excessive number of collision domains
   b

Lesson 3 Practice

For each of the following IP address assignments, specify the number of bits in the subnet identifier, the number of possible IP addresses in each subnet, the subnet mask for the IP addresses, and the IP address ranges for the first and last subnet.

10.0.0.0/19

1. Number of bits in subnet identifier: 11
2. Number of possible IP addresses in each subnet: 8,190
3. Subnet mask: 255.255.224.0
4. First subnet: 10.0.32.1 to 10.0.63.254
5. Last subnet: 10.255.224.1 to 10.255.255.254
Chapter 2 Planning a TCP/IP Network Infrastructure

192.168.214.0/29

1. Number of bits in subnet identifier: 5
2. Number of possible IP addresses in each subnet: 6
3. Subnet mask: 255.255.255.248
5. Last subnet: 192.168.214.249 to 10.255.214.254

172.28.0.0/20

1. Number of bits in subnet identifier: 4
2. Number of possible IP addresses in each subnet: 4,094
3. Subnet mask: 255.255.240.0
4. First subnet: 172.28.16.1 to 172.28.31.254
5. Last subnet: 172.28.240.1 to 172.28.255.254

Lesson 3 Review

1. Which of the following is the correct formula for calculating the number of subnets or hosts you can create with a given number of bits represented by $x$?
   a. $x^2 + 2$
   b. $2^x + 2$
   c. $2^x - 2$
   d. $x^2 - 2$

c
2. What is the correct subnet mask to use on a Class B network with a 10-bit subnet identifier?
   a. 255.192.255.255
   b. 255.255.255.192
   c. 255.255.192.0
   d. 255.192.0.0

b

3. How many hosts can you create on a subnet with 9 bits available for the host identifier?

510
4. In the IP address assignment 10.54.113.0/24, what does the number 24 represent?
   a. The number of bits in the subnet identifier
   b. The number of bits in the host identifier
   c. The number of bits in the combined subnet and host identifiers
   d. The number of bits in the combined network and subnet identifiers

5. Which IP address class provides the largest number of hosts per subnet?
   Class A

Lesson 4 Review

1. Which type of DHCP address allocation would you typically use for an Internet Web server? Why?
   Manual allocation because the Web server must be permanently assigned a specific IP address.

2. What configuration tasks must you perform on a newly installed Windows XP workstation to activate the DHCP client?
   None. The DHCP client on a Windows computer is activated by default.

3. What is the function of a DHCP relay agent?
   A DHCP relay agent enables DHCP clients to obtain IP address assignments from DHCP servers located on other networks by relaying the clients’ broadcast transmissions to specific server addresses.

Lesson 5 Review

1. When a TCP/IP computer can communicate with the local network but not with computers on other networks, which of the following configuration parameters is probably incorrect?
   a. IP address
   b. Subnet mask
   c. Default gateway
   d. Preferred DNS server

2. How do you determine whether name resolution failure is the cause of a network communication problem?
   By using an IP address to establish the connection instead of a name.
2-62  Chapter 2  Planning a TCP/IP Network Infrastructure

3. Why must a DHCP client use broadcast transmissions to request an IP address from a DHCP server?
   a. Because the DHCP server can only receive broadcasts
   b. Because the DHCP client does not yet have an IP address
   c. Because the DHCP server can service requests only from computers on the same LAN
   d. Because the DHCP client must inform all the other clients on the network of its intention to request an IP address

   b

Case Scenario Exercise

Based on the information provided in the Case Scenario Exercise, answer the following questions:

1. What subnet mask should you use for the Web server computers on the basement LAN?
   255.255.255.224

2. How many subnets are there on the 207.46.230.0/27 network in total, and how many hosts can there be on each subnet?
   6 subnets, with 30 hosts on each

3. What is the range of registered IP addresses available for your use?
   207.46.230.193 to 207.46.230.222

4. How many routers are there on the building’s networks? How many of the routers are computers running Windows Server 2003, and how many are hardware devices?
   There are six routers in total: two are hardware devices and four are computers running Windows Server 2003.

5. Which of the following IP address classes can you not use when selecting a network address for your unregistered LANs? (Choose all that apply.)
   a. Class A
   b. Class B
   c. Class C
   d. Class D

   c and d
6. For each answer you selected in question 5, explain why you cannot use an address in that class for your unregistered LANs.

You cannot use a Class C address because there is no way for a subnetted Class C address to support the 100 computers required on the third floor with a single subnet. You cannot use a Class D address because this address class is reserved for multicast addresses.

7. Assuming that you will use a network address in the Class B private address range designated by the IANA, what is the maximum number of subnet identifier bits you can use and still have a sufficient number of host identifier bits to support the computers on each of your networks?

9

8. Using the network address specified earlier, how many subnet identifier bits are you using for your unregistered network address?

6

9. What subnet mask must you use for the unregistered LANs on your network?

255.255.252.0

10. List the IP address ranges for the first four subnets created from your unregistered network address.

172.19.4.1 to 172.19.7.254
172.19.8.1 to 172.19.11.254
172.19.12.1 to 172.19.15.254
172.19.16.1 to 172.19.19.254
Troubleshooting Lab

For each of the problem scenarios below, specify which listed conditions (a, b, c, or d) could be the cause of the difficulty, based on the information provided in the Troubleshooting Lab.

1. All the computers successfully obtain IP addresses from the DHCP server except one, which has an IP address of 169.254.0.1.
   - (c)

2. All the computers on one of the five horizontal LANs fail to obtain IP addresses from the DHCP server.
   - (a)

3. All the computers on the backbone LAN fail to obtain IP addresses from the DHCP server.
   - (b)

4. The computers on four of the five LANs are able to communicate with the local network only.
   - (d)