CHAPTER 3

Planning, Implementing, and Troubleshooting DHCP

The Dynamic Host Configuration Protocol (DHCP) is one of those services that has proven itself as a valued solution on TCP/IP networks of all sizes and complexities. With the advent of DHCP, gone are the days administrators previously faced of manually providing and tracking IP addresses for hundreds or thousands (or even hundreds of thousands) of network clients. This chapter examines the DHCP service and how it is planned for and implemented in a Windows Server 2003 environment.

Although no exam objectives are directly addressed in this chapter, we felt the material presented here was still relevant enough to warrant coverage. Additionally, it's not out of the realm of possibilities that you will need to understand the information presented here on test day (and after) as you carry out your day-to-day administrative activities. Please do take the time to read through this chapter, as you stand a good chance of having at least one question on your exam that deals directly or indirectly with the planning, implementation, or troubleshooting of the DHCP service.

Outline

Introduction

TCP/IP is the de facto standard for computer networking and appears to have no challengers in the networking protocol arena. If you are going to work with Windows Server 2003, you should expect to work with TCP/IP. One of the keys to successfully working with TCP/IP is understanding the concept of TCP/IP addresses. The designers of TCP/IP wanted an identification scheme that was independent of any one computer or network equipment design, so they established a scheme of IP addresses.

If you've ever surfed the web, you have probably seen IP addresses (numbers such as 192.168.144.77). As you administer TCP/IP on a network, a considerable part of your time will be devoted to IP address assignment because IP addresses don't just magically get assigned to network hosts—they have to be provided through manual configuration or some other means. When a computer is added to a network, it needs an IP address to communicate on that network. When the computer moves to a new location, it likely will need a new IP address. If you are just starting out managing a large TCP/IP network, you might find the notion of managing all those addresses a bit daunting. If you move a DNS server to a new subnet, you might have to reconfigure every client computer. If you move a client computer to a new subnet, you might have to update its IP address. This does not endear you to road warriors who travel among several offices, especially those who are regional managers. If you manually manage IP addresses, almost any change to the network will require a visit to one or more computers to update TCP/IP configurations—not a happy prospect. Fortunately, the people who brought us DNS to replace the `hosts` file also came up with a solution to this dilemma.

DHCP was the Internet community's answer to dynamically distributing IP addresses. DHCP is open and standards-based, as defined by the Internet Engineering Task Force (IETF) in their Requests for Comments (RFCs) 2131 and 2132. (The IETF is the main standards organization for the Internet.) This chapter examines the basics of DHCP as it applies to you, the systems administrator, and how you can use it to make your life and your network better.

Understanding DHCP

Public IP addresses are registered with the Internet Assigned Numbers Authority (IANA) so that IANA can keep track of IP addresses that are being used on the Internet. In some cases, a network is not connected to the Internet and does not need to use registered public IP addresses. In other cases, the network is connected to the Internet with special hardware and software that can be configured to allow the network to use private addresses in conjunction with address translation, commonly referred to as Network Address Translation (NAT). By using NAT, you can (in simple terms) place an entire private network behind a single public IP address. As an example, the organization I work for has more than 5,000 hosts on its internal network. When I or anyone else visits a website on the Internet, we all appear to be coming from a single IP address. That's NAT in action!

NOTE

What are RFCs? RFCs are used to propose changes to existing standards and to help create new standards that specify the way the Internet and IP behave. If an RFC can garner enough interest, it might eventually become a standard. Topics of RFCs range from File Transfer Protocol (FTP; originally RFC 0114 but updated by RFC 0141, RFC 0172, and RFC 0171) to the *Hitchhiker's Guide to the Internet* (RFC 1118). The first RFC was posted in 1969 by Steve Crocker, and the topic of that document was host software. You can find listings of all the RFCs at a number of sites throughout the Internet. One place is www.rfc-editor.org.

Quite often, systems administrators use private (unregistered) addresses on their internal networks to ensure that there are enough readily available addresses for all users. This model works great on a network that is not tied directly to the Internet. However, with the shortage of Class A and Class B (and even Class C) IP addresses, some environments use small pools of registered addresses to service larger numbers of DHCP clients; the idea is that not every client computer needs access simultaneously. These environments require aggressive leasing policies to ensure that everyone can get an address.

In addition to IP addresses, DHCP can provide gateway addresses, DNS server addresses, and Windows Internet Name Service (WINS) server addresses—in essence, everything the client computer needs to participate in the network. This means that all available IP addresses can be stored in a central database, along with associated configuration information such as the subnet masks, gateways, and addresses of DNS servers.

DHCP

DHCP provides the mechanism for dynamically distributing IP addresses on a network—but it doesn't happen magically. Here's how a client computer gets an address:

1. After bootup, the client computer broadcasts a `DHCPDISCOVER` message that is intended for the DHCP server(s) on the network. If a router sits between the DHCP server and the client, it needs to be configured with the IP address of the DHCP server and also be configured to forward BOOTP. BOOTP is discussed in the next section, "BOOTP."
2. Each DHCP server that receives the `DHCPDISCOVER` message responds with a DHCP offer message. That message includes an IP address that is appropriate for the subnet where the client computer is attached. The DHCP server determines the appropriate address by looking at the source subnet for the broadcast `DHCPDISCOVER` message.
3. The client computer considers the offer messages and selects one (usually the first offer it receives). It sends a request (`DHCPREQUEST`) to use the address to the DHCP server that originated the offer. If there are multiple DHCP servers, they need to be carefully configured. It is easy to inadvertently configure servers and end up with them conflicting, so if you have multiple DHCP servers on a network, they should not be capable of

offering duplicate IP addresses. Because DHCP servers do not communicate with one another, they have no way of telling whether another DHCP server has already issued an address.

4. The DHCP server acknowledges the request and grants the client computer a lease to use the address.
5. The client computer uses the IP address to bind to the network. If the IP address is associated with any configuration parameters, the parameters are incorporated into the client computer's TCP/IP configuration.
6. For the first renewal of the IP address, when 50% of the configured lease time has elapsed, the client sends another `DHCPREQUEST` message to the DHCP server that granted its lease, asking to renew and extend its current lease. All subsequent lease renewal is at 75%.
7. If the DHCP server is reachable, it responds with a `DHCPACK` message to the client, renewing and extending the DHCP lease as requested.
8. If the DHCP server is not reachable, the client continues trying to reach it until 87.5% of the lease time has elapsed. At this point, the client attempts to renew its lease with any DHCP server that responds. If this is unsuccessful, the client starts the process of acquiring a new DHCP lease.

TIP

DHCP solitude Be sure to remember that DHCP servers do not communicate with one another; therefore, they have no way of telling whether another DHCP server has already issued an address. For this reason, you will never create identical DHCP scopes on multiple DHCP servers.

The first step of this process indicates that DHCP clients request their addresses by using broadcast messages. If you are familiar with routing, particularly TCP/IP routing, you are probably familiar with the fact that one of the benefits of routing is that the router segregates broadcast domains. In other words, broadcasts do not generally cross routers. Does that mean that DHCP works only on the local segment and you need 50 DHCP servers for 50 subnets? No, that is not the case—not if you configure your routers or other Windows Server 2003 computers to act as DHCP relay agents.

Configuring a router or server as a DHCP relay agent causes it to begin using BOOTP. BOOTP was the precursor to DHCP, and it was the first protocol used to assign IP addresses dynamically. BOOTP was specially designed to pass across a router, and it continues to be used to allow DHCP broadcasts to propagate across routers. You'll learn about the installation and configuration of DHCP relay agents later in this chapter, in the section "Configuring and Implementing a DHCP Relay Agent."

BOOTP

Before we discuss installing and configuring the DHCP service in Windows Server 2003, a brief discussion about BOOTP is necessary. A number of DHCP's features had their beginnings in BOOTP. BOOTP was originally designed in 1985 by Bill Croft and John Gilmore to automate the configuration of network devices. To use BOOTP, the systems administrator must create a table with a list of client computers, their IP addresses, and their network configurations. When a client computer comes on to the network, it broadcasts a request that the BOOTP server receives. The BOOTP server looks up the client computer in the table and responds with the configuration information stored in the table, allowing the client computer to communicate on the network.

Because BOOTP worked well, it was used extensively in the early 1990s in conjunction with diskless workstations. (A BOOTP chip was a common option on a network interface card [NIC], and many networks thrived on BOOTP.) The downside of BOOTP was that it provided only the configuration information entered in the table. The administrator still needed to configure the table. The limitations of BOOTP effectively prevented any automation of these tasks, so it was eventually replaced with DHCP. BOOTP and DHCP packets look virtually identical, and DHCP even takes advantage of the BOOTP forwarder functionality of many routers and switches. DHCP offers the automation features BOOTP lacked.

Now that we've completed the history lesson, you should have a pretty good understanding of the theory of DHCP. Before moving on to the workings of DHCP in Windows Server 2003, let's examine the new DHCP features that Windows Server 2003 provides.

What's New with Windows Server 2003 DHCP

DHCP is not a new service in Windows Server 2003, but it has undergone some changes from both Windows 2000 and Windows NT 4.0. The following list summarizes some of the major changes in DHCP in Windows Server 2003, as compared to Windows 2000 Server and Windows NT 4.0:

- **DHCP integration in DNS**—Windows Server 2003 DHCP servers can trigger dynamic updates in the DNS database for all clients to which it leases IP addresses. Windows 2000 and newer clients can automatically update their DNS records if they are authorized to do so. Legacy clients can have their records updated by the DHCP server if it is authorized to do so.
- **Rogue DHCP server detection**—Unauthorized, or *rogue*, DHCP servers can cause a wide variety of problems, including denial of service (DoS) to clients. To prevent such problems, Windows Server 2003 provides for authorizing DHCP servers and detecting and shutting down unauthorized servers. Active Directory is required for the detection of rogue DHCP servers to occur.

- **Superscope and multicast scope support**—Superscopes enable you to group several standard DHCP scopes into a single administrative group without causing any service disruption to network clients. Multicast scopes enable you to lease Class D IP addresses to clients for participation in multicast transmissions, such as streaming video and audio transmissions. Multicast scopes are discussed in more detail in the section "Understanding Multicasting and Multicast Scopes," later in this chapter.
- **Local security groups for DHCP management**—Two new local administrative security groups are created when the DHCP service is installed: DHCP Users and DHCP Administrators. The DHCP Users group can be used to provide read-only console access to the server to enable group members to view but not modify DHCP data. The DHCP Administrators group provides full administrative control of the DHCP service without granting its members full administrative control over the entire server.
- **Improved monitoring and reporting**—DHCP is a critical network service that must be kept running. The key to discovering problems early is monitoring, so Windows Server 2003 provides a full set of performance-monitoring counters that can be used to monitor DHCP server performance.
- **Custom DHCP option classes**—User- and vendor-specified option classes can be used to distribute specific options to the clients that need them. For example, you can use option classes to distribute a specific default gateway or parent domain name to one group of computers on a network.
- **In-console backup and restore**—For the first time ever, Windows Server 2003 provides the administrator with the capability to perform DHCP scope backups and restorations from within the DHCP console itself.

Now that we've briefly examined the improvements made in the DHCP service in Windows Server 2003, we need to spend some time examining four of the more basic parts of planning for a new DHCP implementation.

Planning for DHCP

Unless you want to go back to manually assigning and tracking IP addresses for all clients on your network, DHCP is going to be a very important network service for you. As such, it requires some time spent evaluating the needs of the current and future environment you support. When properly planned and implemented up front, DHCP typically continues to function as intended for many years into the future.

Planning a DHCP Infrastructure Type

Before you can get down to the task of planning how many DHCP servers you'll need, where you'll put them, or how you'll configure the scopes and options, you need to first understand what type of network infrastructure you have and how DHCP will fit into it. In general, organizations make use of three basic types of network infrastructures: centralized, distributed, and mixed. Your DHCP design also typically makes use of one of these three models.

Centralized Infrastructures

The most common model used today is the centralized infrastructure model. In this model, your DHCP servers (along with most other network services) are located in a central location. Clients at remote locations or on other subnets (or other broadcast domains) need to use a DHCP relay agent to contact a DHCP server. Almost all modern routers in use today can be configured as a DHCP relay agent, thus passing the DHCP broadcast traffic from the remote subnet to the subnet where the DHCP servers are located.

As an example, an organization I've had experience with has multiple subnets configured for their campus, one for each building where clients are located. These subnets were implemented through VLANs, and all of the VLANs were trunked together to form a single broadcast domain. Because no routers are required to pass traffic from one subnet (VLAN) to another, no DHCP relay agents are required anywhere on the network. In this example, the organization has two DHCP servers configured in their data centers to provide DHCP for the entire network.

Distributed Infrastructures

In the distribution infrastructure model, each subnet (or VLAN) has its own DHCP server located locally. This model does have the advantage of keeping DHCP traffic off WAN links, which are almost always slower and less reliable than a LAN. Of course, the disadvantage to this distributed infrastructure is that you must have many more DHCP servers on your network, so you have more areas of concern to manage and monitor.

As an example, another organization I've had experience with also has multiple subnets configured on their network through VLANs, but their network is very distributed and each VLAN maps directly to a single remote location. Each remote site has a WAN link for access to the main location, and each location has a router and switch (or multiple switches) at that location to support local and remote traffic. In this scenario, the local core switches themselves provide DHCP service to the site instead of using Windows Server 2003 DHCP servers, so the extra cost of using this model is fairly low. Your experiences with distributed infrastructures might be very different, however.

Mixed Infrastructures

As you might have guessed, a mixed infrastructure combines features of the centralized and distributed infrastructure models. Using the mixed infrastructure model, you can plan for DHCP server placement on a location-by-location basis that makes the most sense for each location. When using the mixed infrastructure model, you will likely still have two or more DHCP servers in your central data center, but you'll also have one or more DHCP servers locally in remote locations where you have large client populations, for example.

Planning a DHCP Server Placement Strategy

You've probably heard before that you should use either the 70/30 or the 80/20 rule when planning and implementing DHCP on your network. But what exactly do these rules mean? Is it even correct to assume that using one of these rules is always the correct answer? As you no doubt know by now, there are no absolutes in network design—only best practices that have typically been proven to yield consistently high quality results when implemented properly. As such, you cannot just blindly follow either the 70/30 or the 80/20 rule in your DHCP design. In this section, we examine some items you'll want to consider when planning the placement of DHCP servers on your network.

The DHCP Rules

The real question you have to answer before deciding on a DHCP server rule is whether you will have multiple DHCP servers on multiple subnets. If so, you should consider using either the 70/30 or the 80/20 rule. These rules break up your DHCP scope ranges so that 70% (or 80%) of the available IP addresses in a scope range are configured on the DHCP server on the local subnet, with the remaining 30% (or 20%) of the available IP addresses in a scope range configured on a DHCP server located on a different subnet. Different subnets are typically broken up by switches or routers, and each subnet is a single broadcast domain, so this design strategy works well. DHCP is a broadcast-based system; by default, clients will find the DHCP server on their local subnet and obtain a lease, if available, from that local DHCP server.

On the other hand, if you will be placing your DHCP servers on the same subnet, you will want to follow the 50/50 rule, with each DHCP server containing half of the available IP addresses in the scope range. This model also works well in large organizations that have multiple VLANs and use VLAN trunking and a subnet mask that creates a single large broadcast domain. Although this is not a common design on the network side, when it is done properly, it can work well. When using the 50/50 rule for DHCP servers, you typically have more IP addresses available within your organization than are needed; either DHCP server will be capable of servicing the entire organization if the other fails.

The rules we've discussed here seem to imply using only two DHCP servers, which, in most organizations is adequate, but you can extend this logic to four, six, eight, or more DHCP servers. It's obviously easier to work with DHCP servers in pairs of two, but you should use the number that is best for your organization.

Creating Standby Servers

If you choose to follow one of the rules we discussed previously—80/20, 70/30 or 50/50—you might not need to worry about having a standby server configured. If you use a single DHCP server for your organization, you should seriously consider configuring and implementing a hot standby DHCP server. This standby DHCP server should be installed and configured identically to your production DHCP server, including all scopes and options, but will not provide DHCP leases until you manually configure it to do so.

You can either configure and enable all scopes and options but not authorize the DHCP server in Active Directory, or authorize the DHCP server in Active Directory but not enable any scopes to stage the standby server for when it is needed. As a practical matter, it is simpler (and quicker) to have all the scopes configured and enabled, but have the server itself not authorized in Active Directory. Note that although a standby server ensures that you can continue to provide DHCP if the primary DHCP server becomes unavailable, this is a manual method that requires an administrator to enable the standby DHCP server to function and provide leases to clients. For that reason, you should consider the standby server model as a nonpreferred one and instead use multiple DHCP servers to provide services, as discussed previously.

Clustering DHCP Servers

DHCP in Windows Server 2003 is a clustering-aware application; therefore, you can implement and configure DHCP servers in a cluster arrangement for maximum fault tolerance and failover. When you implement DHCP in a cluster, you do not need to use the 70/30 or 80/20 rules. In this implementation, you can opt to use the 50/50 rule for maximum fault tolerance or just place the entire scope range on a single DHCP virtual server. Clustering, which is discussed in more detail in Chapter 10, "Planning, Implementing, and Maintaining Highly Available Servers," does have some very high hardware and software resource requirements, however, so it is not the right or best solution for every organization.

Planning for DHCP Reservations

Although it is perfectly acceptable—and preferred—for most client workstations to use DHCP and get a randomly assigned IP address, sometimes you will want to use DHCP to assign the same IP address to a specific network object every time. Enter the DHCP reservation. A DHCP reservation is configured in a specific DHCP zone by entering the MAC address of network adapter installed in the client (printer, workstation, network hardware) that you want to have the same DHCP assigned IP address every time. Using reservations allows the client to be configured for DHCP, but still get a static IP address and other information being passed by the DHCP server as part of that scope where the reservation was configured.

Although it sounds like you might want to use DHCP reservations for every client on your network that requires a static IP address, this is not always the case. It's still best practice to always assign a static IP address to any Windows server that will be providing a network service such

as DNS, WINS, DHCP, Exchange, SQL or Active Directory. In fact, services such as DNS and DHCP will actually "complain" about the network adapters installed in the server being configured for DHCP and not having a static network address. Most organizations that actually make use of DHCP reservations tend to use them for workstations that need the same IP address all the time or for printers on the network. In reality, most organizations still configure networked printers with a static IP address.

Planning for DHCP Options

A DHCP scope is not just a range of IP addresses that can be handed out to requesting clients—it's also a full suite of TCP/IP configuration information that the clients need to communicate effectively on the network. When you create your DHCP scopes, you can configure common DHCP scope options—be sure that you do, or your clients will likely not be able to communicate effectively.

Table 3.1 presents some of the most commonly used DHCP scope options configured.

TABLE 3.1 Common DHCP Scope Options

Code	Option Name	Option Description
3	Router	Specifies a list of IP addresses for routers on the client's subnet
4	Time Server	Specifies a list of RFC 868 time servers available to the client
6	DNS Servers	Specifies a list of DNS servers available to the client
15	DNS Domain Name	Specifies the domain name that the client should use when resolving host names via DNS
27	All Subnets Are Local	Specifies whether the client can assume that all subnets of the IP network to which the client is connected use the same MTU as the subnet of the network to which the client is directly connected
28	Broadcast Address	Specifies the broadcast address in use on the client's subnet
44	WINS/NBNS Servers	Specifies a list of RFC 1001/1002 NBNS servers, listed in order of preference
46	WINS/NBT Node Type	Allows NetBT clients, which can be configured as described in RFC 1001/1002

DHCP has a provision for configuring manufacturer-specific DHCP options. You can select these options by opening the DHCP management console and selecting the scope for which to configure options, as described later in Step by Step 3.3. Selecting the Advanced tab enables you to select Microsoft Options from the drop-down list in the Vendor Class window. Table 3.2 shows the manufacturer options that Microsoft defines.

TABLE 3.2 Microsoft-Specific DHCP Options

Code	Option Name	Description
1	Microsoft Disable NetBIOS	This option can be used to selectively enable or disable NetBT for DHCP-enabled computers running Windows.
2	Microsoft Release DHCP Lease on Shutdown	This option can be used to control whether DHCP-enabled computers running Windows send a release for their current DHCP lease to the DHCP server when shutdown occurs.
3	Microsoft Default Router Metric Base	This value is a specified router metric base to be used for all default gateway routes.

You can configure DHCP options at four different levels for each DHCP server:

- **Server options**—These are DHCP options that are applied, by default, to all scopes on the DHCP server.
- **Scope options**—These are DHCP options that are applied only to the specific scope on the DHCP server. When a scope option conflicts with a server option, the scope option wins and that value is made a part of the scope. If the conflicting scope option is later removed, the server option once again becomes effective in the scope.
- **Class options**—These are DHCP options that are applied only to clients identified as members of specified user or vendor classes.
- **Reservation options**—These are DHCP options that are applied only to a single specific computer.

Now that we've done some initial planning for an implementation of the DHCP service in Windows Server 2003, we can talk about installing and implementing it on the network. After DHCP is installed and configured, we'll take some time to examine how it can be secured and also how you'll go about troubleshooting it.

Installing and Implementing DHCP

The first question many managers ask when presented with a request to install Windows Server 2003 DHCP is this: "Can't we just use our existing DHCP?" The answer to this question is both yes and no. If you are maintaining a legacy domain and WINS network, Windows Server 2003 can receive DHCP information from any DHCP server with which Windows NT 4.0 or Windows 2000 Server works. However, if you want to take advantage of the features of Active Directory and possibly migrate away from the legacy WINS architecture, you need the Windows Server 2003 DHCP service.

The following sections discuss how to install and configure DHCP for a network.

Installing the DHCP Server Service

When you install Windows Server 2003, you can install DHCP as one of the optional services. To prepare for Exam 70-293, you need to know how to install DHCP on an existing server that does not already have DHCP installed.

NOTE

A DHCP server cannot also be a DHCP client If you currently have a server configured as a DHCP client, the DHCP installation prompts you to enter a static IP address for the server.

Before you install DHCP, you must configure the server with a static IP address. When the DHCP server's network adapter is configured with a static IP address, you can install the DHCP service on the server. To install the DHCP service on your server, perform the steps described in Step by Step 3.1.

STEP BY STEP

3.1 Installing the DHCP Service

1. Select Start, Settings, Control Panel, Add or Remove Programs.
2. On the Add or Remove Programs page, click Add/Remove Windows Components to open the Windows Components Wizard.
3. Select Networking Services, as shown in Figure 3.1.

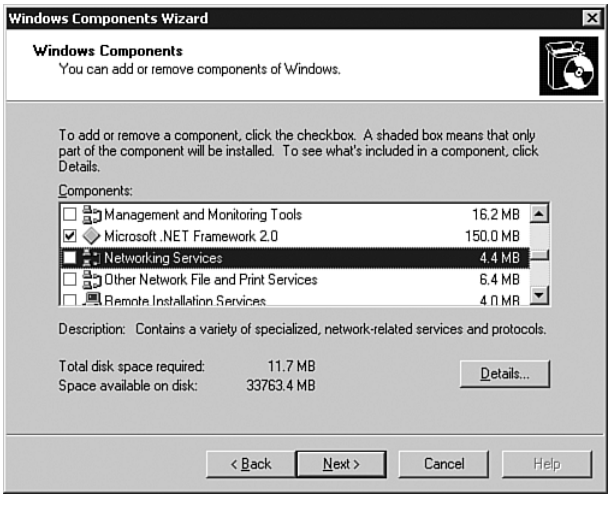

FIGURE 3.1 DHCP is located in the Networking Services group in the Windows Components Wizard.

4. Click the Details button to open the Networking Services window, shown in Figure 3.2.
5. Select Dynamic Host Configuration Protocol (DHCP) and click OK.

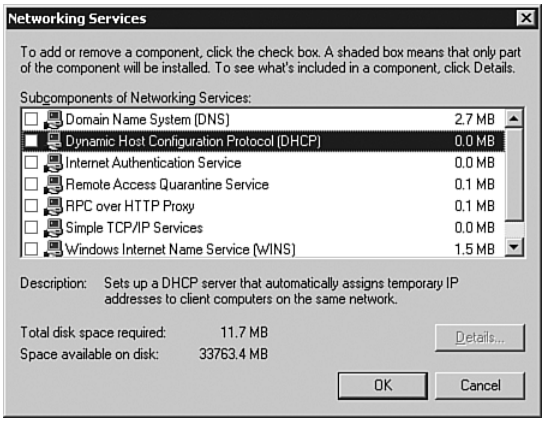

FIGURE 3.2 You select the Dynamic Host Configuration Protocol (DHCP) option to install the DHCP server.

6. Back in the Windows Components Wizard page, click Next to begin the installation.
7. If you are prompted to supply the location of your Windows Server 2003 CD-ROM or installation files, provide the correct location. Windows installs the DHCP service files on your computer.
8. When prompted that installation is complete, click Finish to close the Windows Components Wizard.

After you've installed the DHCP service, you need to begin configuring the DHCP server so that it can service network clients. Before you can begin the configuration process, you need to understand the types of DHCP scopes in Windows Server 2003.

Understanding DHCP Scopes

A *scope* is a range of IP addresses that are available for dynamic assignment to hosts on a given subnet. The scope for a particular subnet is determined by the network address of the broadcast DHCP request. In addition to address information, a scope can include a set of configuration parameters to be assigned to client computers when the address is assigned. This list of configuration parameters can include DNS servers, WINS servers, default gateways, the subnet mask, a NetBIOS scope ID, IP routing information, and WINS proxy information.

You should make the scope as large as you can. Later in the scope-creation process, you can exclude addresses and define reservations for particular addresses that exist within the scope.

NOTE

At least one scope After you install the DHCP service, you must define at least one scope on the server. Otherwise, the service will not respond to DHCP requests.

Understanding DHCP Superscopes

The *superscope* type of scope was introduced to the Windows NT product family with Service Pack 2 for Windows NT 4.0. A superscope enables you to support a supernetted or multinetted network with a Windows Server 2003 DHCP server.

A supernetted network is a network that has multiple network addresses or subnets running on the same segment. This configuration is common in a network environment with more than 254 hosts on a subnet and in an environment in which certain hosts need to be isolated from the rest of the logical network for security or routing reasons. Superscopes support a local multinet or a multinet that is located across a router and configured to use the BOOTP forwarder service.

Understanding Multicasting and Multicast Scopes

Multicasting is the act of transmitting a message to a select group of recipients. This is in contrast to the concept of a *broadcast*, in which traffic is sent to every host on the network, or a *unicast*, in which the connection is a one-to-one relationship and there is only one recipient of the data.

Let's look at an example using an email message. If you send an email message to your manager, that email is a unicast message. If you send an email message to every user on the system, you have sent a broadcast. If you send an email message to a mailing list, you have sent a multicast message, which falls between a unicast message and a broadcast message. Teleconferencing and videoconferencing use the concept of multicasting, as does broadcast audio, in which the connection is from one source computer to a selected group of destination computers. At this time, only a few applications take advantage of multicasting, but with the growing popularity of multicast applications, we might see more multicast applications in the future.

The following are a few terms you need to understand before we discuss the Windows Server 2003 multicast capabilities:

- **Multicast DHCP (MDHCP)**—An extension to the DHCP standard that supports dynamic assignment and configuration of IP multicast addresses on TCP/IP–based networks.
- **Multicast forwarding table**—The table used by an IP router to forward IP multicast traffic. An entry in the IP multicast forwarding table consists of the multicast group address, the source IP address, a list of interfaces to which the traffic is forwarded (that is, the *next-hop interfaces*), and the single interface on which the traffic must be received to be forwarded (that is, the *previous-hop interface*).
- **Multicast group**—A group of member TCP/IP hosts configured to listen for and receive datagrams sent to a specified destination IP address. The destination address for the group is a shared IP address in the Class D address range (224.0.0.0 to 2239.255.255.255).
- **Multicast scope**—A scope of IP multicast addresses in the range 239.0.0.0 to 239.254.255.255. Multicast addresses in this range can be prevented from propagating in either direction (send or receive) through the scope-based multicast boundaries.

Windows Server 2003 makes use of the concept of a multicast scope. The DHCP service has been extended to allow the assignment of multicast addresses in addition to unicast (single-computer) addresses. A proposed IETF standard (RFC 2730, "Multicast Address Dynamic Client Allocation Protocol [MADCAP]") defines multicast address allocation. MADCAP (also known as MDHCP in Microsoft lingo) would enable administrators to dynamically allocate multicast addresses to be assigned in the same fashion as unicast addresses. The Windows Server 2003 DHCP multicasting capability also supports *dynamic membership*, which allows individual computers to join or leave a multicast group at any time. This is similar to registering to receive an Internet broadcast or joining and leaving an email mailing list. Group membership is not limited by size, and computers are not restricted to membership in any single group.

How do client computers join and leave a multicast group? The answer is via MDHCP and the MDHCP application programming interface (API). Client computers using MDHCP must be configured to use the MDHCP API. MDHCP assists in simplifying and automating configuration of multicast groups on a network, but it is not required for the operation of multicast groups or for the DHCP service. Multicast scopes provide only address configuration and do not support or use other DHCP-assignable options. MDHCP address configuration for client computers should be done independently of how the client computers are configured to receive their primary IP addresses. Computers using either static or dynamic configuration through a DHCP server can also be MDHCP clients.

TIP

Class D IP addresses for the multicast scope Remember that, along with a primary IP address, a computer receives a multicast address, which is for multicasts only and uses the Class D IP addresses specified in the multicast scope. Multicast addresses are not used for regular network traffic such as web traffic or other IP-based applications.

Now that you know the different types of scopes supported in Windows Server 2003, you can move forward to creating scopes on a DHCP server.

Creating a DHCP Scope

Now that you are familiar with the different types of scopes, you can create one. To create a standard DHCP scope, you perform the steps described in Step by Step 3.2.

TIP

Preparing before performing Before you actually start to create a DHCP scope, you should ensure that you have gathered all the required information. You typically need the starting and ending IP addresses, the subnet mask, the DNS server IP address, and the gateway IP addresses.

STEP BY STEP

3.2 Creating a DHCP Scope

1. Open the DHCP console by selecting Start, Programs, Administrative Tools, DHCP.
2. Right-click the DHCP server and select New Scope from the context menu.
3. Click Next to dismiss the opening page of the New Scope Wizard.
4. On the first page of the wizard, the Scope Name page, enter a name and description for the new scope, as shown in Figure 3.3. You should make this name something that will enable you to easily identify this scope if you have multiple scopes on the DHCP server. When you're done entering the information, click Next to continue.

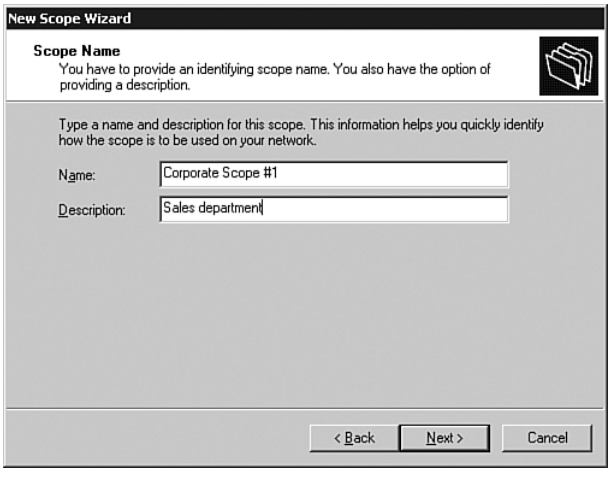

FIGURE 3.3 You should enter an intuitive name and description for the new scope.

5. On the next page of the wizard, the IP Address Range page, enter the IP address range and subnet mask that you need for the network, as shown in Figure 3.4. You can define the subnet mask by using the standard octet method (for example, 255.255.255.0) or by using the more router-centric mask length field (for example, 24 bits). When you're done entering the information, click Next to continue.
6. On the next page of the wizard, the Add Exclusions page (see Figure 3.5), you can configure a range of IP addresses that will not be leased to client computers. These are typically addresses assigned to application servers, routers, printers, or other infrastructure equipment that requires static addresses. You can have multiple excluded IP addresses or ranges for each scope. When you're done entering the information, click Next to continue.

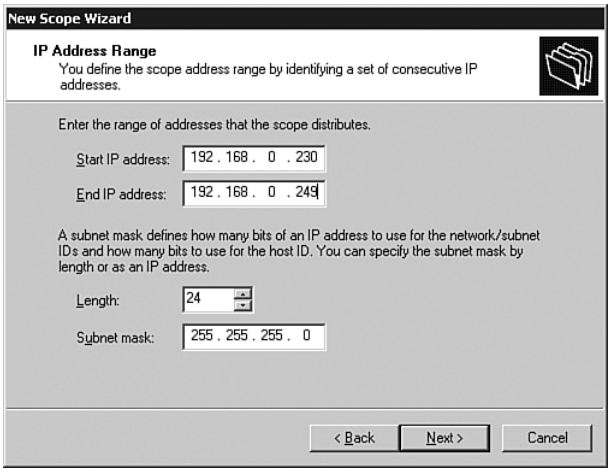

FIGURE 3.4 Configuring the IP address range and subnet mask information defines the scope boundaries.

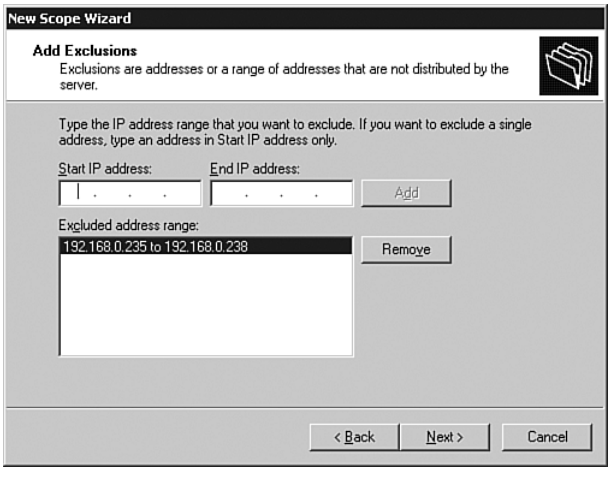

FIGURE 3.5 Configuring IP address exclusions enables you to prevent addresses within the scope from being leased.

7. On the next page of the wizard, the Lease Duration page, you can configure the amount of time for which a DHCP lease is valid, as shown in Figure 3.6. The default setting is 8 days and can be changed to any value between 1 minute and almost 1,000 days (999 days, 23 hours, 59 seconds, to be exact). For the average network, the default setting of 8 days is sufficient. In a network that has a large number of computers connecting at various locations, such as portable computers on wireless connections, you might want to reduce the lease duration. Conversely, in a network with clients that do not change location, you might consider increasing the lease duration to cut down on DHCP traffic on the network. When you're done entering the information, click Next to continue.

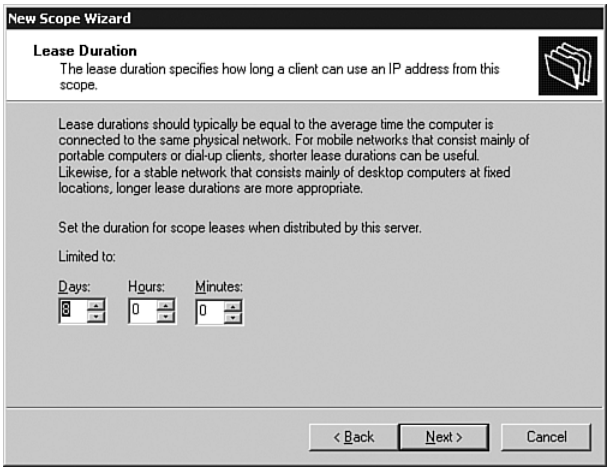

FIGURE 3.6 You should configure the lease duration that seems appropriate for the network.

8. On the next page of the wizard, the Configure DHCP Options page, you have the choice to configure additional options for your scope now or later. It is usually best to configure these options at the time of scope configuration, so you should do that now. Select Yes, I Want to Configure These Options Now and click Next to continue.

9. On the next page of the wizard, the Router (Default Gateway) page, enter the default gateway for the network or the subnet that the scope serves, as shown in Figure 3.7. When you're done entering the information, click Next to continue.

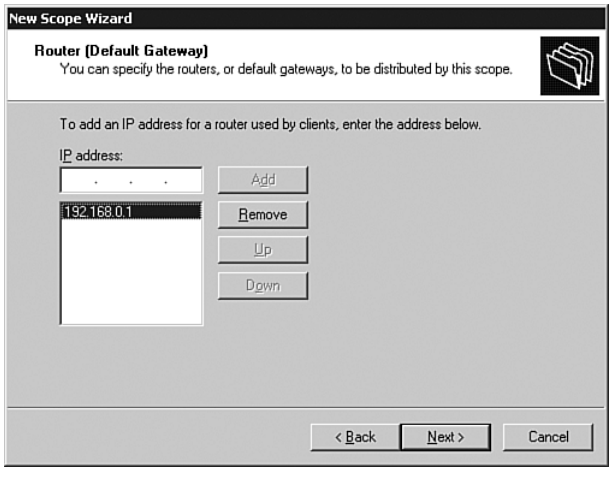

FIGURE 3.7 If you configure multiple gateways, you need to ensure that you place them in preferred order from top to bottom.

10. On the next page of the wizard, the Domain Name and DNS Servers page, configure the parent domain that all DHCP clients should be made part of, as well as any number of DNS servers you require, as shown in Figure 3.8. It is recommended that you enter at least two DNS servers for your clients to use. If you need to resolve a server name to an IP address, you can enter the server's name and then click the Resolve button. When you're done entering the information, click Next to continue.

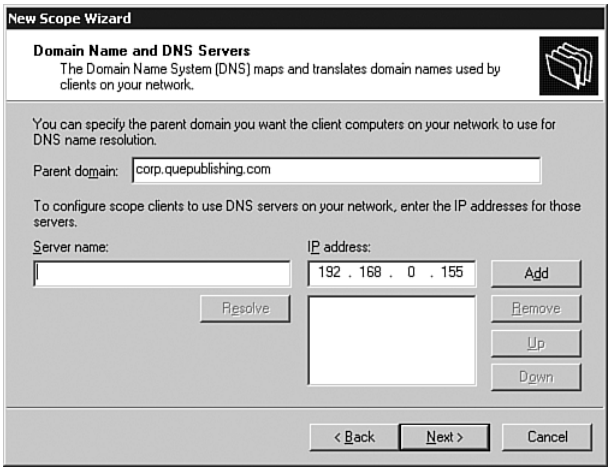

FIGURE 3.8 If you configure multiple DNS servers, you should ensure that you place them in preferred order from top to bottom.

11. On the next page of the wizard, the WINS Servers page, enter the IP addresses of the network's WINS servers, as shown in Figure 3.9. WINS servers are used to convert NetBIOS names to IP addresses for legacy clients on the network. As on the Domain Name and DNS Servers page, you can use the Resolve button to resolve a host name to an address. If a network is purely Windows 2000 or better, you do not need to have a WINS server on the network because Windows 2000, Windows XP, and Windows Server 2003 use DNS by default for all name resolutions. If you need WINS servers on a network, it is recommended that you enter at least two of them here. When you're done entering the information, click Next to complete the scope-creation process.

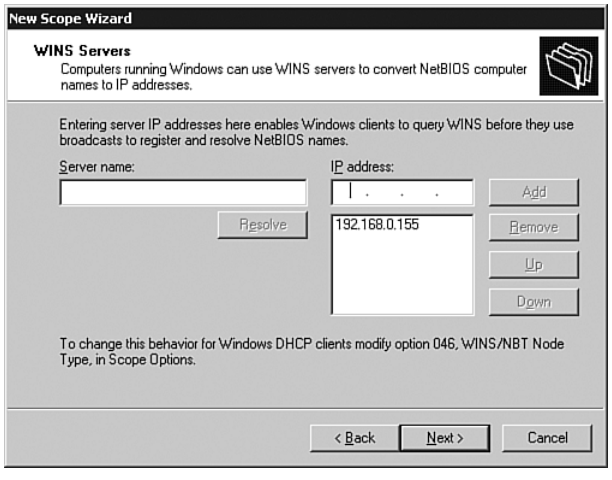

FIGURE 3.9 WINS servers are not required for networks that use only Windows 2000, Windows XP, or Windows Server 2003 computers.

12. On the next page of the wizard, the Activate Scope page (see Figure 3.10), you have the option to active the configured scope now or later. In most cases, you want to activate the scope right away. Select Yes, I Want to Activate This Scope Now and click Next to activate the configured scope.

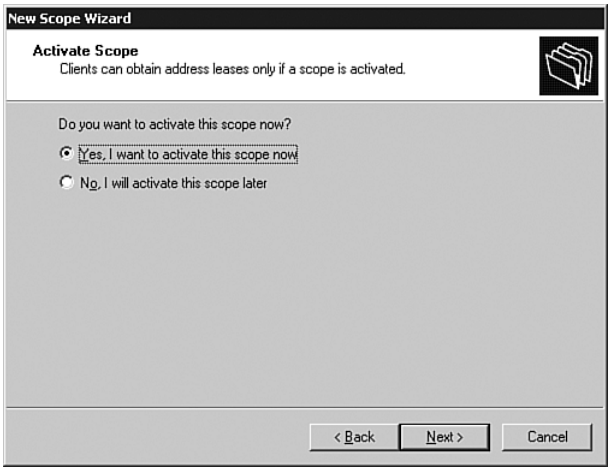

FIGURE 3.10 You typically want to activate the scope immediately after configuring it.

13. Click Finish to close the New Scope Wizard. Note that the DHCP won't issue any IP address from your new scope unless it has already been authorized in Active Directory. We discuss this a bit later in this chapter.

NOTE

Configuring scope ranges Common practice when configuring a new DHCP scope is to configure it and leave out enough addresses to cover all servers and other infrastructure devices that require statically assigned IP information without needing all the other options provided in a DHCP scope, such as DNS servers, WINS servers, and default gateways. For example, you might configure a scope of 192.168.0.10 to 192.168.0.200, with the remaining IP addresses available for servers, routers, switches, and other infrastructure equipment on that subnet. This practice keeps you from forgetting a configured reservation and ending up with duplicate IP addresses.

TIP

When to use the New Multicast Scope option Creating a new scope and creating a new multicast scope are two different tasks. If you get a question on the exam regarding the procedure for creating a multicast scope, remember that you need to start the process by selecting New Multicast Scope, not New Scope.

Configuring Scope Properties

After you've created a scope, you might want to modify its properties. To modify a scope's properties, you perform the steps described in Step by Step 3.3.

NOTE

Changing scope properties It's worth pointing out that you cannot change every option a scope has. For example, if you need to change the subnet mask that DHCP clients are receiving as part of their DHCP lease, you need to create a new DHCP scope reflecting this change and then remove the existing DHCP scope. Clients will then get the new information when they renew their lease the next time.

STEP BY STEP

3.3 Configuring a DHCP Scope's Properties

1. Right-click the scope and select Properties from the context menu.
2. The Properties dialog box opens, as shown in Figure 3.11.

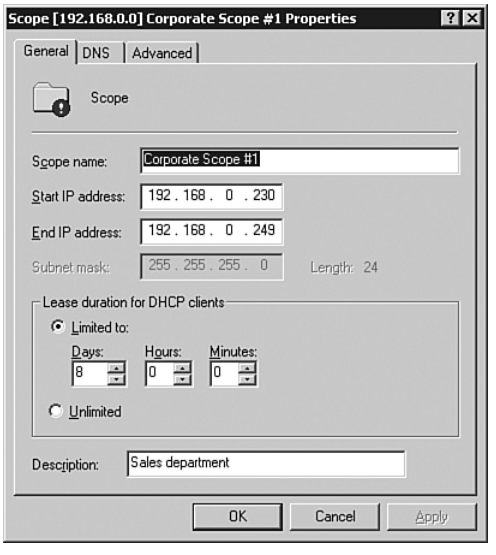

FIGURE 3.11 You can use the Scope Properties dialog box to change scope properties after you create a scope.

3. On the General tab, change the scope name, IP address range, lease duration, and scope description, if you want to.
4. If you want to change the options on the DNS tab, do so now. The options on the DNS tab are discussed later in this chapter, in the section "Configuring DHCP for DNS Integration."
5. On the Advanced tab, select options related to BOOTP clients, as shown in Figure 3.12. If you have BOOTP clients on your network, select either the BOOTP Only option or the Both option, depending on your network configuration. The default setting is DHCP Only. Click OK to close the Scope Properties dialog box after you make your changes.

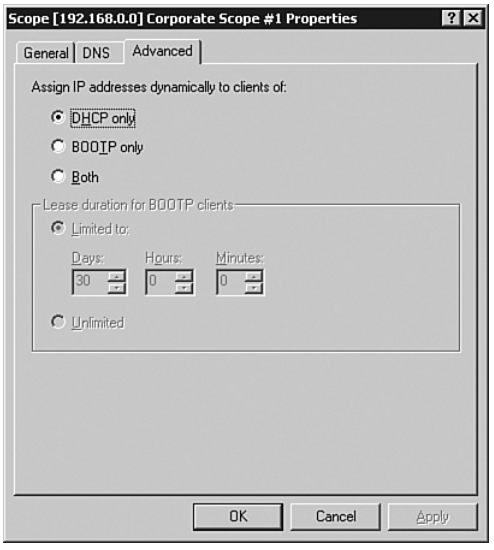

FIGURE 3.12 You can configure the scope to service BOOTP clients on the Advanced tab of the Scope Properties dialog box.

6. To view the address pool and configured exclusion ranges, click the Address Pool node of the DHCP console, as shown in Figure 3.13.

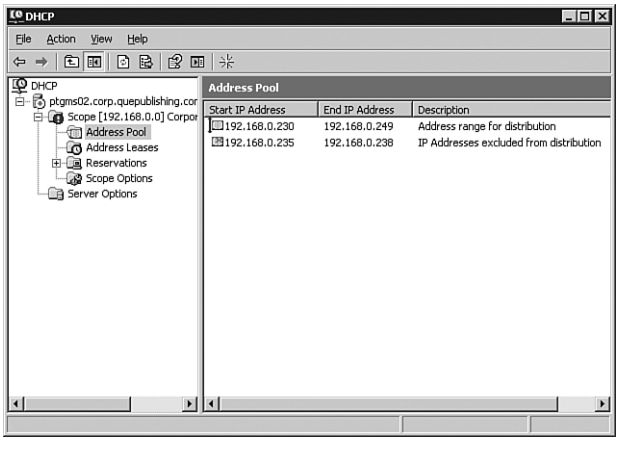

FIGURE 3.13 You can quickly view all configured scope ranges and exclusion ranges from the Address Pool node.

7. To add a new exclusion range, right-click Address Pool and select New Exclusion Range from the context menu. The Add Exclusion window appears (see Figure 3.14). Click Add after you enter your new exclusion range.

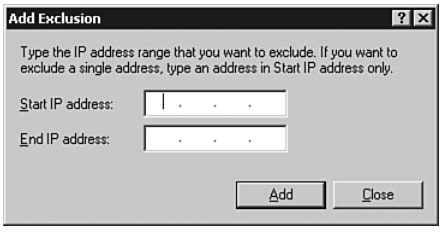

FIGURE 3.14 You can add a new exclusion range to a configured DHCP scope by using the Add Exclusion dialog box.

8. To view the addresses that have been leased, click the Address Leases node, as shown in Figure 3.15. (Of course, no leases are shown here until you authorize the DHCP server, as discussed later in this chapter, in the section "Authorizing a DHCP Server in Active Directory.")

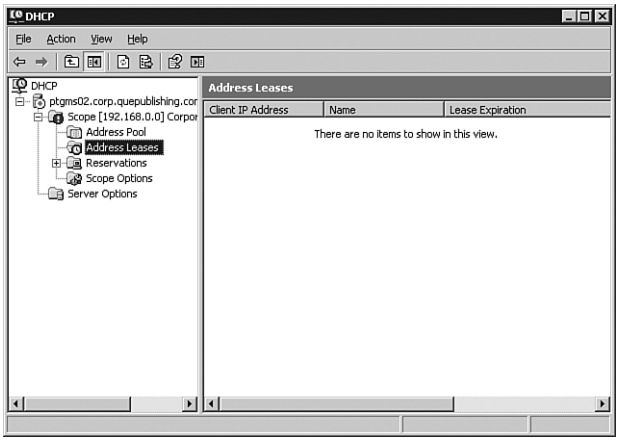

FIGURE 3.15 You can view all active scope leases from the Address Leases node.

9. If you want to manually revoke an active client lease, right-click it in the right pane of the Address Leases node and select Delete from the context menu.
10. To view the configured reservations, click the Reservations node of the DHCP console.
11. You can configure a new address reservation by right-clicking Reservations and selecting New Reservation from the context menu. You can configure a reservation for any device for which you want to have a DHCP-assigned IP address that never expires. Configure the reservation as shown in Figure 3.16 and click Add to add it. Click Close to close the New Reservation input box when you're done configuring reservations for this scope. After you've configured a reservation, you can see it in the Reservations node of the DHCP console, as shown in Figure 3.17.
12. You can view existing scope options by clicking the Scope Options node, as shown in Figure 3.18.
13. To configure a new scope option, right-click the Scope Options node and select Configure Options from the context menu. Configure the options in the Scope Options window (see Figure 3.19). Table 3.1 listed the common DHCP options available for configuration. Table 3.2 listed the Microsoft-specific DHCP options that are available for configuration.

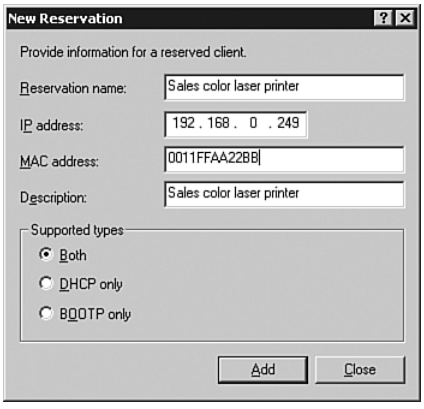

FIGURE 3.16 You can configure a new DHCP reservation, which is typically done for printers and other static infrastructure devices.

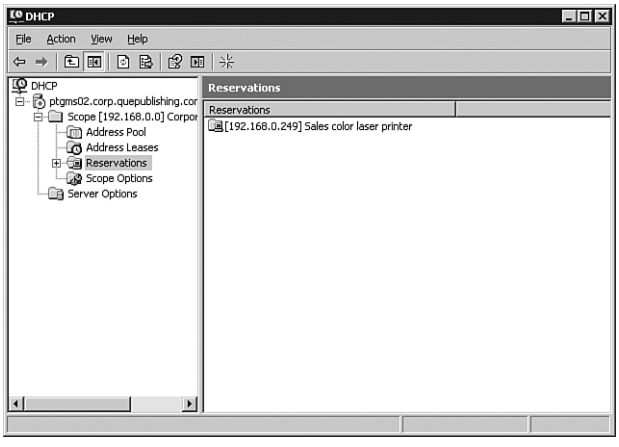

FIGURE 3.17 You can view all scope reservations from the Reservations node.

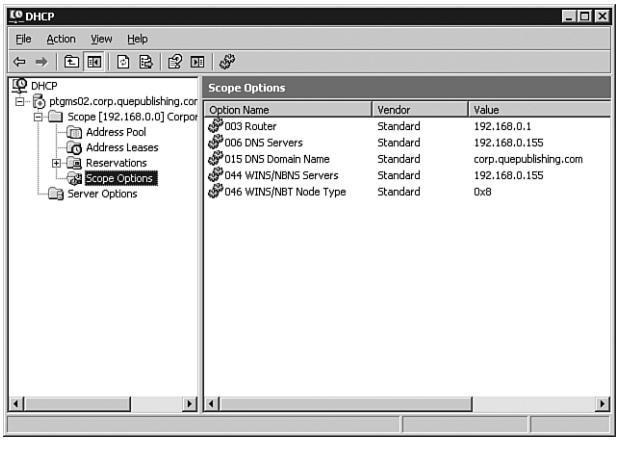

FIGURE 3.18 The Scope Options node lists all currently configured scope options.

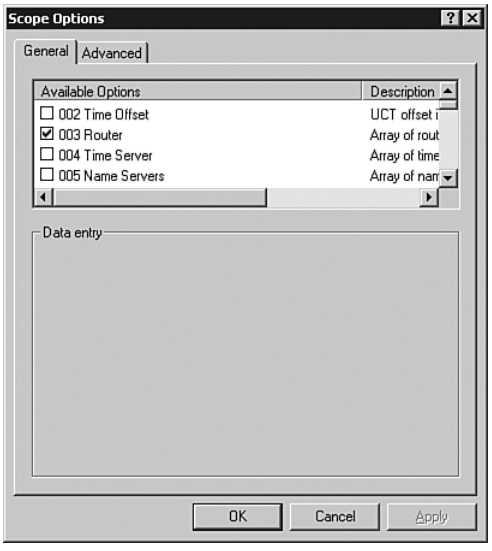

FIGURE 3.19 You can configure extra scope options from the Scope Options dialog box.

TIP

Configuring server options You can configure server-wide DHCP options as mentioned in Step by Step 3.3. To configure server DHCP options that apply to all scopes on the DHCP server, right-click the Server Options node in the DHCP console and select Configure Options from the context menu.

Authorizing a DHCP Server in Active Directory

For security reasons, a new DHCP server must be authorized in Active Directory before it can assign IP addresses by an administrator with Enterprise Admin credentials. This prevents unauthorized DHCP servers from running on the network. One of the nastiest things a troublemaker can do is put up a rogue DHCP server and have it issue addresses that conflict with infrastructure devices' addresses. The nice thing about this feature is that if you are running Windows 2000 or better client computers and they are using Active Directory, the computers will not accept DHCP addresses from an unauthorized server. To authorize a DHCP server in Active Directory, you perform the steps described in Step by Step 3.4.

STEP BY STEP

3.4 Authorizing a DHCP Server in Active Directory

1. Open the DHCP console by selecting Start, Programs, Administrative Tools, DHCP.
2. Right-click the DHCP server and select Authorize from the context menu.

3. The authorization process might take some time, depending on network conditions. Refresh the DHCP console by pressing F5. You should see the window shown in Figure 3.20. When authorization is complete, the status is shown as Active and the server is ready to issue addresses when it receives DHCP requests. Note also that the status arrow on the server itself is now pointing up instead of down, as before.

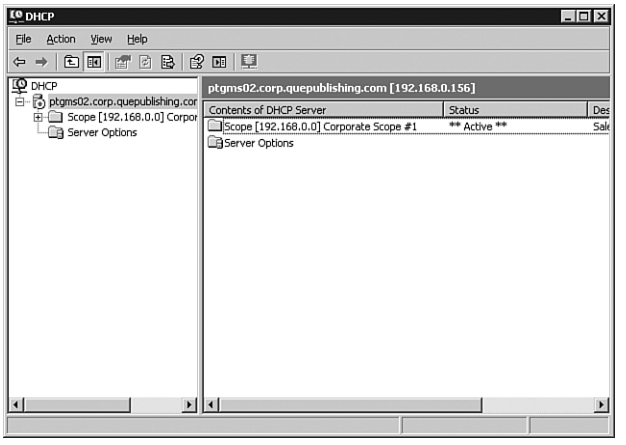

FIGURE 3.20 When a DHCP server is authorized, DHCP server scope information appears in the right pane of the DHCP console window.

Windows Server 2003 and Windows 2000 Server DHCP servers that are not authorized do not provide DHCP services to network clients. These unauthorized servers also check every 5 minutes to see if their authorization status has changed, thus allowing them to begin servicing clients.

You have now installed, configured, and authorized a Windows Server 2003 DHCP server. We next examine configuring DHCP for DNS integration.

Configuring DHCP for DNS Integration

One of the keys to effectively implementing an Active Directory environment is the capability for Windows 2000 and Windows XP workstations using DHCP to be automatically registered in DNS. You can set the following settings for DNS integration (see Step by Step 3.5):

- **Dynamically Update DNS A and PTR Records Only If Requested by the DHCP Clients**—This is the default behavior of the Windows Server 2003 DHCP server. It causes the DHCP server to register and update client information with the authoritative DNS server of the zone in which the DHCP server is located, according to the DHCP client's request. The DHCP client can request the way in which the DHCP server performs updates of its host (A) and pointer (PTR) resource records. If possible, the DHCP server accommodates the client's request for handling updates to its name and IP address information in DNS. This selection requires you to select the Enable Dynamic DNS Updates According to the Settings Below option.

- **Always Dynamically Update DNS A and PTR Records**—When this option is selected, the DHCP server always updates the client's fully qualified domain name (FQDN), IP address, and both A and PTR resource records, regardless of whether the client has requested to perform its own updates. This selection requires you to select the Enable Dynamic DNS Updates According to the Settings Below.
- **Discard A and PTR Records When Lease Is Deleted**—This option, which is selected by default, instructs the DHCP server to cause the DNS server to delete the client's A and PTR records when the lease has expired or otherwise has been deleted. This selection requires you to select the Enable Dynamic DNS Updates According to the Settings Below option.
- **Dynamically Update DNS A and PTR Records for DHCP Clients That Do Not Request Automatic Updates**—This option allows legacy clients, such as Windows NT 4.0 and Windows 9x clients, to participate in DNS dynamic updates. This selection requires you to select the Enable Dynamic DNS Updates According to the Settings Below option.

NOTE

New Group Policy object options Although it is beyond the scope of Exam 70-293, you can also configure the DNS options discussed here from Group Policy. The options are located in Computer Configuration, Administrative Templates, Network, DNS Client node.

Because the DHCP server controls DNS dynamic updating, you need to perform all the applicable DNS configuration from the DHCP console. The DHCP server automatically updates any DNS server configured as part of the server's TCP/IP network properties. It is important to be sure that the primary DNS server is configured as one of the DNS servers because any updates sent to it are propagated to the rest of the DNS servers for that domain. However, the DNS server in question must support DDNS. The Windows Server 2003 DNS server supports these updates, as do a number of other DNS servers.

To configure a DHCP server for DNS integration, you perform the steps described in Step by Step 3.5.

STEP BY STEP

3.5 Configuring DHCP for DNS Integration

1. Open the DHCP console by selecting Start, Programs, Administrative Tools, DHCP.
2. Right-click the DHCP server and select Properties from the context menu. Select the DNS tab of the DHCP Server Properties dialog box, shown in Figure 3.21.

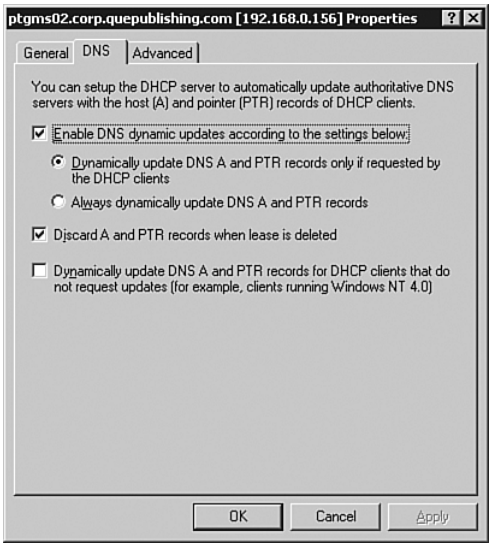

FIGURE 3.21 You can configure DDNS options on the DNS tab.

3. To enable DHCP integration with DNS, ensure that the Enable Dynamic DNS Updates According to the Settings Below check box is selected.
4. Select to have the DHCP server update A and PTR records when requested or to always update A and PTR records.
5. To help keep the DNS database clean and consistent, allow the DHCP server to cause expired leases to lead to A and PTR record deletion.
6. If there are legacy clients on the network, ensure that dynamic updating is configured for them.
7. If you are using secure dynamic updates, consider configuring a dedicated network user account for dynamic updating. You can enter the account credentials by switching to the Advanced tab of the DHCP Server Properties dialog box, as shown in Figure 3.22.
8. Click the Credentials button to open the DNS Dynamic Update Credentials window, as shown in Figure 3.23.
9. Enter the domain user account name, domain, and password in the DNS Dynamic Update Credentials dialog box. Click OK to accept the credentials or Cancel to avoid entering credentials at this time.
10. Click OK to close the DHCP Server Properties dialog box.

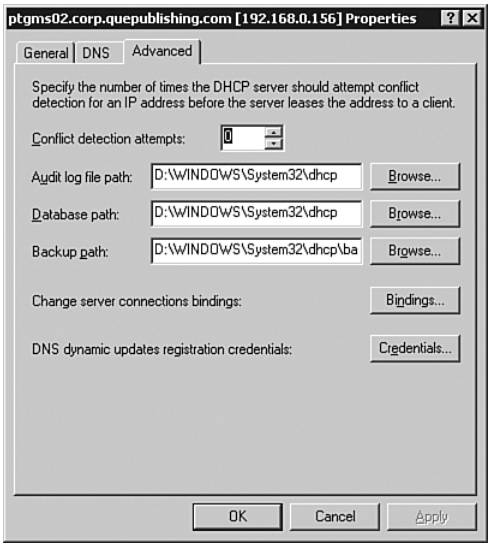

FIGURE 3.22 Click the Credentials button to enter the account username and password for DDNS.

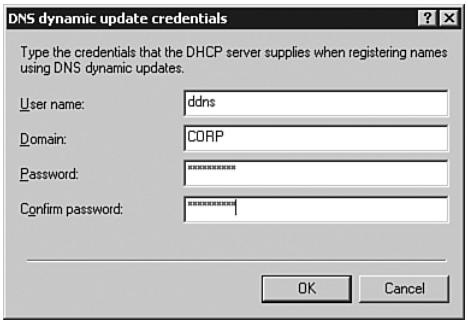

FIGURE 3.23 Enter the dynamic updates account credentials in the DNS Dynamic Update Credentials dialog box.

DHCP option code 81 is required to make dynamic updates work. Let's look at two examples that explain the basic dynamic update process.

The first example looks at a Windows 2000 Professional client computer that has requested a DHCP lease from a Windows Server 2003 DHCP server configured with the default options:

1. During the DHCP lease-negotiation process, the Windows 2000 Professional client sends a `DHCPREQUEST` message. By default, the client includes DHCP option 81 in this message, informing the DHCP server that it is requesting that the DHCP server register its PTR record in DNS. The client is responsible for registering its A record on its own.

2. The DHCP server replies with a DHCPACK message, granting the requested DHCP lease. This message includes DHCP option 81. With the default DHCP server settings, the DHCP server informs the client that it will register the PTR record and that the client is responsible for registering the A record in DNS.
3. The client registers its A record, and the DHCP server registers the client's PTR record in DNS.

The second example looks at a Windows NT 4.0 Workstation client computer that has requested a DHCP lease from a Windows Server 2003 DHCP server configured with the default options:

1. During the DHCP lease-negotiation process, the Windows NT 4.0 Workstation client sends a DHCPREQUEST message. DHCP option 81 is not included in this message.
2. The server returns a DHCPACK message to the client, granting its DHCP lease request.
3. The DHCP server updates the DNS server with the client's A and PTR records.

TIP

DHCP and DNS It is important to remember that Windows 2000 and Windows XP client computers update the A records in DNS without any assistance from the DHCP server. The only client computers for which DHCP updates DNS are older legacy clients.

CAUTION

DDNS updates and domain controllers To perform DDNS updates, you should not configure the DHCP service on a computer that is also a domain controller. If a DHCP server exists on a domain controller, the DHCP server has full control over all DNS objects stored in Active Directory because the account under which it is running (the domain controller computer account) has this privilege. This creates a security risk that should be avoided. You should not install the DHCP server service that is configured to perform DDNS updates on a domain controller; instead, you should install it on a member server if you're performing DDNS updates.

As an alternative, you can use a new feature in Windows Server 2003 DHCP. This feature enables you to create a dedicated domain user account that all DHCP servers will use when performing DDNS updates.

Configuring and Implementing a DHCP Relay Agent

Today most networks that use DHCP are routed. As discussed previously, DHCP messages are broadcast messages. By default, nearly all routers do not pass broadcast traffic, in the interest of reducing overall network traffic levels. Fortunately, you can get around this design limitation by configuring a DHCP relay agent to pass BOOTP messages across routers.

You can set up a DHCP relay agent in three basic configurations. The first involves entering the IP address or addresses of the DHCP server(s) into the router itself, instructing it to pass DHCP messages to a specified IP address for action. The second method involves using the Windows Server 2003 Routing and Remote Access Service (RRAS) component as a router (in place of a hardware-based router) and configuring the DHCP relay agent within it. The third solution, and the one that we examine in this section, uses a Windows Server 2003 computer located on a subnet without a DHCP server to act as a DHCP relay agent. This option requires RRAS components, but it does not involve creating or configuring a router, as the second solution would. What's important to understand is that the server providing the DHCP relay agent service does not have to be dedicated to that purpose; it could be a file server, a print server, or any other type of Windows Server 2003 (or Windows 2000 Server) server on that subnet. Figure 3.24 shows how this arrangement would look on a network.

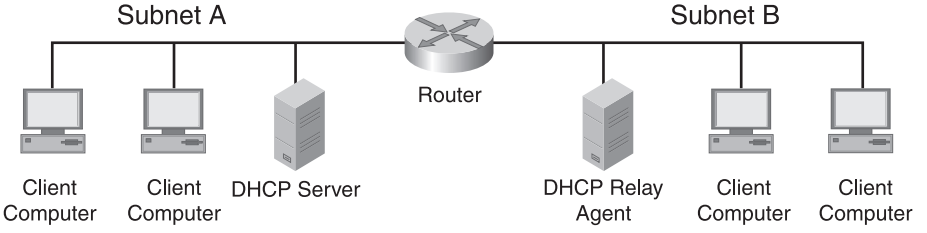

FIGURE 3.24 The DHCP relay agent allows clients on the other side of a router to communicate with the DHCP server.

TIP

DHCP relay agent Recall that the DHCP relay agent is needed only to help pass DHCP traffic across a router that otherwise could not pass that traffic. As such, the server acting as the relay agent is not the same server providing DHCP and is located on the subnet on the *other side* of the router in question. Referring back to Figure 3.24, the DHCP server is located on subnet A, whereas the DHCP relay agent is located on subnet B.

In Step by Step 3.6, you enable the DHCP relay agent on a Windows Server 2003 computer. This exercise assumes that you have not previously configured and enabled RRAS on the computer.

STEP BY STEP

3.6 Configuring a DHCP Relay Agent

1. Select Start, Programs, Administrative Tools, Routing and Remote Access to open the Routing and Remote Access console, shown in Figure 3.25. (If you've previously configured and enabled RRAS, you can skip to Step 7.)

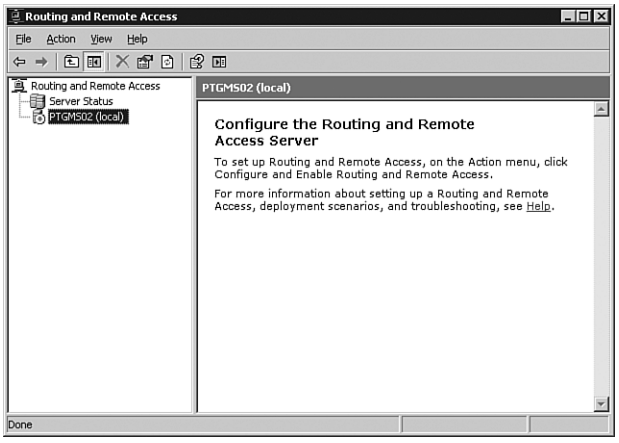

FIGURE 3.25 The Routing and Remote Access console is initially empty.

2. Right-click the server name and select Configure and Enable Routing and Remote Access from the context menu. The Routing and Remote Access Server Setup Wizard appears. Click Next to dismiss the opening page.
3. On the Configuration page of the wizard, shown in Figure 3.26, select the Custom Configuration option and click Next to continue.

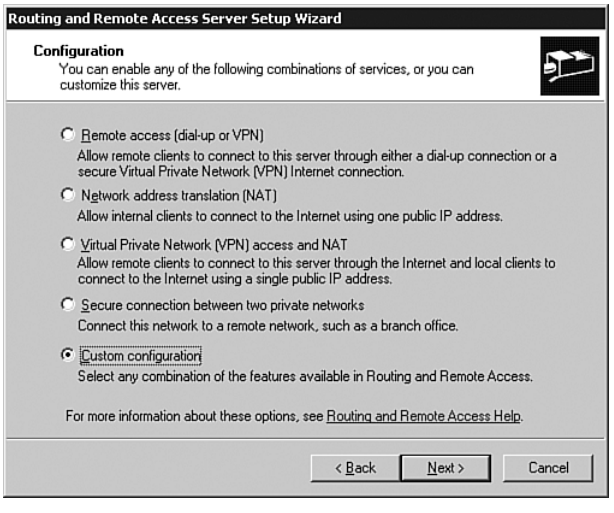

FIGURE 3.26 You need to specify a custom configuration to perform basic DHCP relay agent setup.

4. On the Custom Configuration page of the wizard, shown in Figure 3.27, select the LAN Routing option and click Next to continue.

FIGURE 3.27 The LAN Routing option is the bare minimum you need to support later installation of the DHCP relay agent.

5. When the summary page is displayed, review your selections and click Finish to continue.
6. You are prompted to start RRAS. Click Yes to start the service.
7. Back at the Routing and Remote Access console, expand the following nodes: Routing and Remote Access, *ServerName*, IP Routing, and General, as shown in Figure 3.28.

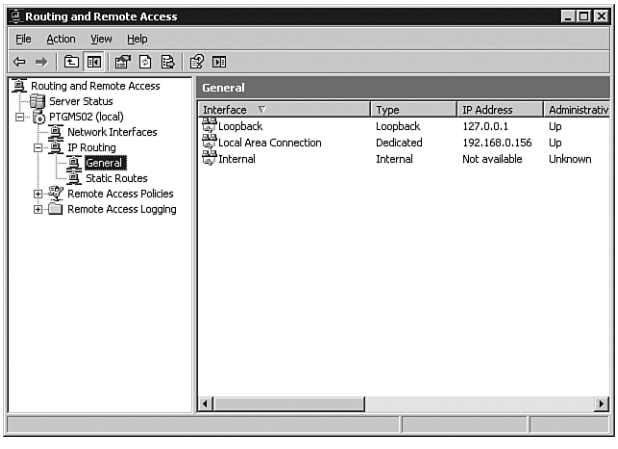

FIGURE 3.28 You need to add the DHCP relay agent from the General node.

8. Right-click the General node and select New Routing Protocol from the context menu. This opens the New Routing Protocol dialog box.
9. From the New Routing Protocol dialog box, shown in Figure 3.29, select DHCP Relay Agent. Click OK to confirm your configuration.

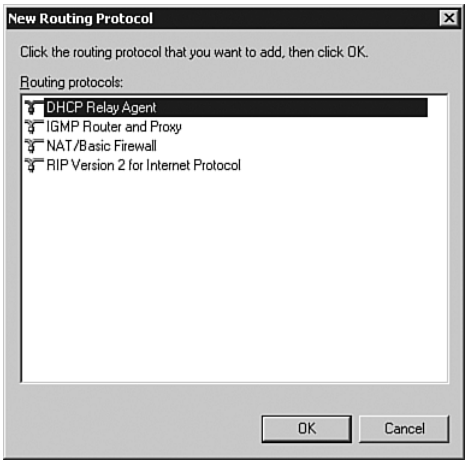

FIGURE 3.29 You can add the DHCP relay agent in addition to standard IP routing protocols.

10. To select a network interface for the DHCP relay agent to run on, right-click the DHCP Relay Agent node in the RRAS console and select New Interface from the context menu.
11. On the New Interface for DHCP Relay Agent page, shown in Figure 3.30, select the network interface that you want to be available for the DHCP relay agent. Click OK to continue. The DHCP Relay Properties dialog box, shown in Figure 3.31, opens.

FIGURE 3.30 Select one or more installed network adapters for use by the DHCP relay agent.

12. In the DHCP Relay Properties dialog box, configure the required values for hop-count threshold and boot threshold. The default value for each of them is 4. Click OK to confirm your settings.
13. The last configuration you need to perform is to assign the DHCP server IP addresses to which the DHCP relay agent forwards DHCP messages. Right-click the DHCP Relay Agent node in the RRAS console and select Properties to open the DHCP Relay Agent Properties dialog box, shown in Figure 3.32. Enter one or more remote DHCP servers in the list and click OK to confirm your settings.

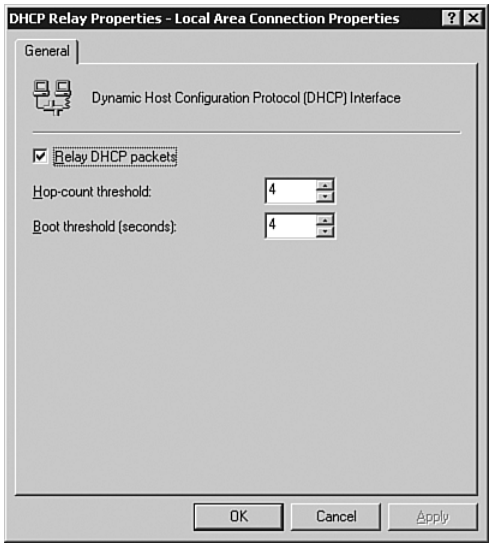

FIGURE 3.31 You need to configure the maximum hop count and length of delay time for the DHCP relay agent.

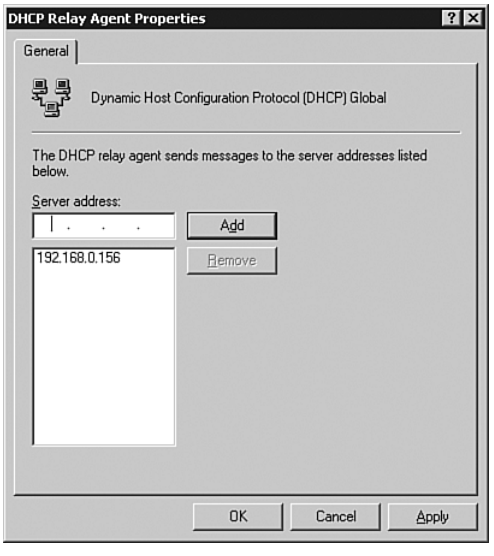

FIGURE 3.32 Provide one or more remote DHCP servers to which the DHCP relay agent can forward DHCP messages.

TIP

DHCP relay agent options The Hop-Count Threshold option enables you to configure a value for the maximum number of DHCP relay agents that are allowed to handle DHCP-relayed traffic. The maximum value is 16 hops, meaning that you can have only 16 DHCP relay agents (typically on different connected subnets) between a client and a DHCP server.

The Boot Threshold option enables you to specify how long the DHCP relay agent waits before forwarding DHCP messages. By configuring DHCP relay agents with different values, you can establish one that should respond first and then one or more DHCP relay agents that should forward DHCP messages, if required.

Configuring Security for DHCP

Although no administrative tasks outwardly appear to help secure your DHCP infrastructure, you can follow some best practices and take other actions to provide a more secure (and, thus, more reliable) DHCP implementation in your environment. We briefly examine them here:

- **Use the 80/20, 70/30, or 50/50 address-allocation rule**—By using one of these configurations, you can ensure that leases will still be made available to clients requesting them if a single server is under a DoS attack or otherwise becomes unavailable.
- **Create and use DHCP server clusters**—By enabling a DHCP server cluster, you remove a single server as a single point of failure (SPOF). By having two (or more) servers in a cluster acting as a single DHCP entity, a failure of a single server (or multiple servers, depending on your configuration) will not result in a failure to provide leases to clients.
- **Examine the DHCP audit logs regularly**—Ensure that audit logging is enabled, as shown in Figure 3.33. The audit logs are stored in the location defined on the Advanced tab, which was shown in Figure 3.22. The location is `%systemroot%\system32\dhcp\` by default.
- **Harden servers**—You can get detailed information and assistance on hardening Windows Server 2003 servers from the "Windows Server 2003 Security Guide."

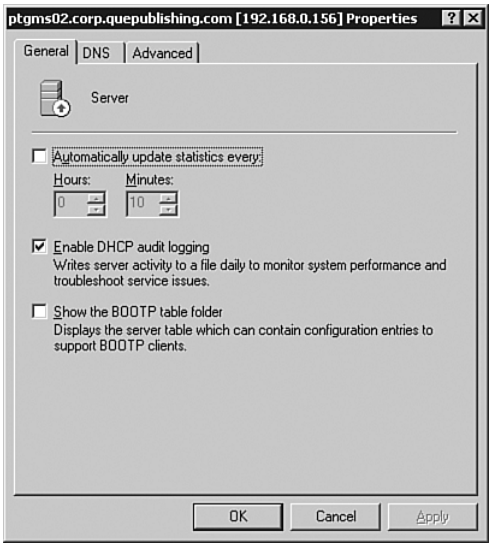

FIGURE 3.33 DHCP audit logging is enabled from the General tab of the DHCP server Properties dialog box.

Troubleshooting DHCP

Although DHCP is typically one of the easiest of the common network services to configure and maintain, from time to time, you might encounter problems. More often than not, the DHCP-related problems that arise stem from a misconfiguration in a scope, unauthorized DHCP servers on the network, or network connectivity problems. You might also find information that has changed in some way, but the change has not been reflected in your DHCP configuration, as in the case of DHCP reservations (which are tied to MAC addresses) or a DHCP server's IP address change. The following sections examine some troubleshooting tasks you can do to quickly determine the cause of DHCP woes and get this vital network service back into proper operation.

Troubleshooting DHCP Server Authorization Problems

As discussed previously, one of the first indicators you might see of an unauthorized or rogue DHCP server is an unexpected increase in the number of `DHCPNACK` messages. You can monitor this statistic over time by using the Performance console. The Performance console includes several counter objects that you can use to monitor and troubleshoot your DHCP server:

- **Acks/Sec**—This counter monitors the number of `DHCPACK` messages sent per second by the DHCP server to client computers. The DHCP server uses the `DHCPACK` messages to acknowledge requests for an address. An increase in this number indicates that a large number of client computers are probably trying to renew their leases with the DHCP server. This could be because of a short lease time configuration or because a number of new computers are entering the network.
- **Active Queue Length**—This counter monitors the current length of the internal message queue of the DHCP server. This number represents the number of unprocessed messages received by the server. A large number here could indicate an unusually large amount of network traffic or a heavy load on the server.
- **Conflict Check Queue Length**—This counter monitors the current length of the conflict check queue for the DHCP server. Before a Windows Server 2003 DHCP server issues an address, it checks whether any IP address conflicts exist. The conflict check queue holds the messages not responded to while the DHCP server performs address conflict detection. A large value here could indicate heavy lease traffic at the server. You might also want to check the Conflict Detection Attempts parameter, which could be set too high.
- **Declines/Sec**—This counter monitors the number of `DHCPDECLINE` messages that the DHCP server receives per second from client computers. This counter indicates that the DHCP client computer has declined the IP address issued by the server. You see this number rise when client computers start having address conflict problems, and it could indicate a network problem, computers with static addresses also being part of a scope, or a rogue DHCP server on the network.
- **Discovers/Sec**—This counter monitors the number of `DHCPDISCOVER` messages received per second by the server. The `DHCPDISCOVER` message is the initial request a client computer sends when it first enters the network and looks for a DHCP server to issue an address. A sudden increase in this counter could indicate that a large number of client computers are attempting to initialize and obtain an IP address lease from the server at the same time. You might see this first thing in the morning, when users power on their PCs, or after a power failure, when all the PCs might be powered on at about the same time.
- **Duplicates Dropped/Sec**—This counter monitors the number of duplicate packets per second dropped by the DHCP server. Duplicate packets on a network are never a good sign, and they can indicate that DHCP clients are timing out before the server can respond. This can be caused by client computers timing out too fast or the server not responding quickly enough.
- **Informs/Sec**—This counter monitors the number of `DHCPINFORM` messages received per second by the DHCP server. `DHCPINFORM` messages are used when the DHCP server queries the directory service for the enterprise root and when dynamic updates are being done on behalf of client computers by the DNS server. This is part of the DDNS integration, and an unusual increase in this number could indicate a large number of addresses being issued.

- **Milliseconds Per Packet (Avg)**—This counter monitors the average time, in milliseconds, the DHCP server takes to process each packet it receives. This is a very subjective number that depends on the server configuration; therefore, having a baseline for this number is a good idea. A sudden increase in this counter could indicate a disk problem or an increased load on the server.
- **Nacks/Sec**—This counter monitors the number of DHCP negative acknowledgment (`DHCPNACK`) messages sent per second by the DHCP server to client computers. A `DHCPNACK` message indicates that the server cannot fulfill the DHCP request. A very high value for this counter could indicate a network problem or a misconfiguration of client computers or the server. Watch for a deactivated scope as a possible culprit.
- **Offers/Sec**—This counter monitors the number of `DHCPOFFER` messages that the DHCP server sends per second to client computers. A `DHCPOFFER` message is the message the server returns to the client computer after the client computer sends a `DHCPDISCOVER` message, and it indicates that the server is offering to issue an address to that client computer. A sudden increase in this value could indicate heavy traffic or a heavy load on the server.
- **Packets Expired/Sec**—This counter monitors the number of packets per second that expire and are dropped by the DHCP server. This situation is caused by a packet remaining in the server's internal message queue too long. A large number for this counter indicates that the server either is taking too long to process some packets or is causing other packets to wait in queue, or that the traffic on the network is too heavy for the DHCP server to handle. It is important to note that high numbers for this counter can indicate pure network traffic problems and not necessarily DHCP-related problems.
- **Packets Received/Sec**—This counter monitors the number of message packets received per second by the DHCP server. A large number indicates heavy DHCP message traffic to the server. These message packets might be requests for addresses, renewals, or releases.
- **Releases/Sec**—This counter monitors the number of `DHCPRELEASE` messages that the DHCP server receives per second from client computers. A `DHCPRELEASE` message is sent only when the client computer manually releases an address, such as when the `ipconfig /release` command is used or the Release All button in the `winipcfg` utility is used at the client computer. Because most users do not manually release their addresses, this number should be low in all but the most unusual network environments.
- **Requests/Sec**—This counter monitors the number of `DHCPREQUEST` messages that the DHCP server receives per second from client computers. These messages are the requests that the client computer sends to request an IP address after it has found a server that can issue addresses. An increase in this number indicates that a large number of client computers are probably trying to renew their leases with the DHCP server. This could be caused by a short lease time configuration or by a number of new computers entering the network.

Configuring the Performance console to monitor and collect data about a DHCP server is a simple process, as outlined in Step by Step 3.7.

STEP BY STEP

3.7 Monitoring DHCP Performance

1. Select Start, Program, Administrative Tools, Performance to open the Performance console.
2. Click System Monitor, as shown in Figure 3.34.

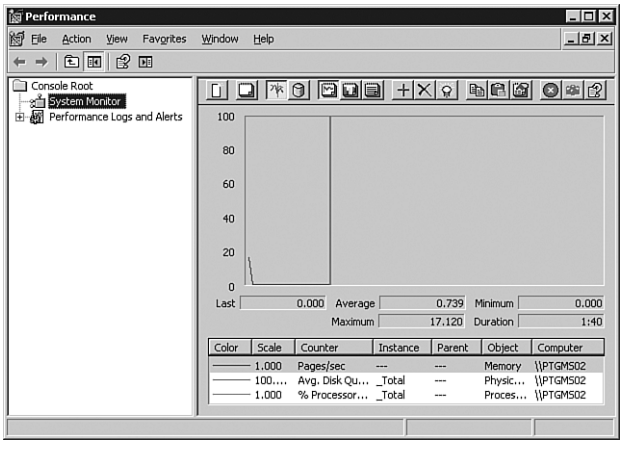

FIGURE 3.34 You can view server performance statistics by using the Performance console.

3. To create an entry in System Monitor, click the + icon. The Add Counters dialog box shown in Figure 3.35 opens, enabling you to begin adding counters.

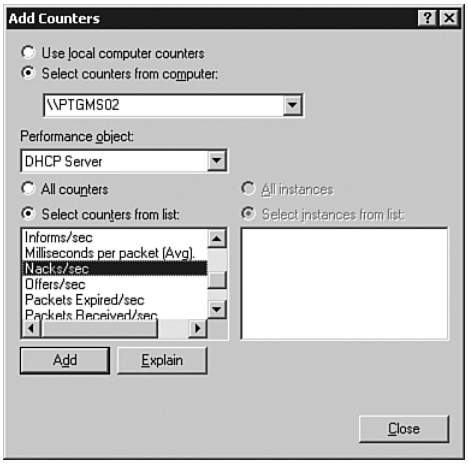

FIGURE 3.35 You can add counters to begin monitoring DHCP server statistics.

4. Select the DHCP Server performance object in the Performance object drop-down list box. You then see the list of counters available for selection that relate to the DHCP service. If you need to know what a counter means, select the counter and click the Explain button.
5. When you have decided what counter you want to monitor, click Add. You can add multiple counters either by selecting each counter and clicking Add or by holding down the Ctrl key while you select all the counters you want to monitor and then clicking Add. Click Close when you are finished. Your counters are graphed like those shown in Figure 3.36.

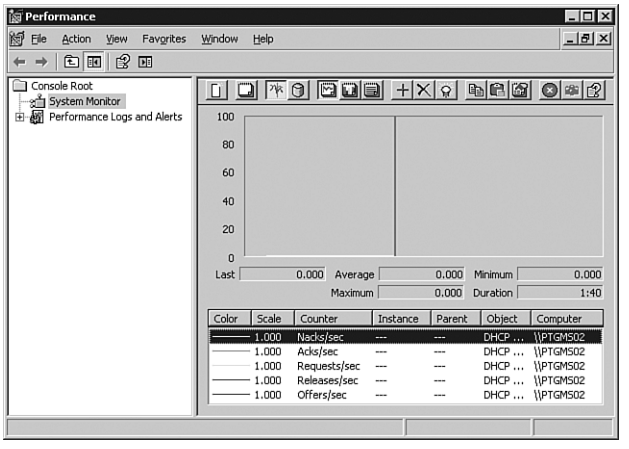

FIGURE 3.36 You can monitor DHCP server statistics in real time.

NOTE

Creating server baselines If you create baselines on servers, you can compare the performance at any given time to a known value. This can be very useful in performing troubleshooting, and it also helps when configurations are being modified. To create a baseline, you create a counter log from the Counter Logs option of the Performance Logs and Alerts node, shown in Figure 3.35. The configuration and use of a counter log is nearly identical to the creation and use of System Monitor, as described in Step by Step 3.7.

If you notice a trend of higher-than-normal `DHCPNACK` messages, you need to determine the source. The most common cause is a rogue DHCP server that has been set up on the network. You can also examine the DHCP lease properties of clients to determine whether any of them have different information than what you have configured in your DHCP scopes.

It's important to remember that Windows 2000 and Windows XP clients in an Active Directory environment that are configured to use DHCP do not accept leases from unauthorized DHCP servers. Older clients accept these leases and can contribute to the number of `DHCPNACK` messages when they attempt to renew their DHCP leases.

You can also examine the DHCP server daily audit logs, located in the `%systemroot%\sysytem32\dhcp` folder, to look for rogue-detection events. The DHCP audit logs are discussed in the next section.

Using the DHCP Logs

The DHCP server daily audit logs are often overlooked as a valuable source of information. You have learned how to enable the audit logs; now let's look at what they contain. Unlike the logs the Windows 2000 Server DHCP service produces, the Windows Server 2003 daily audit logs are natively in text format; you open them simply by double-clicking them. A sample of what you might expect to find in a log is displayed here:

```
ID,Date,Time,Description,IP Address,Host Name,MAC Address
00,04/27/06,20:08:38,Started,,,,
55,04/27/06,20:08:39,Authorized(servicing),,lab1.area51partners.com,,
24,04/27/06,20:44:10,Database Cleanup Begin,,,,
25,04/27/06,20:44:10,0 leases expired and 0 leases deleted,,,,
25,04/27/06,20:44:10,0 leases expired and 0 leases deleted,,,,
24,04/27/06,21:44:12,Database Cleanup Begin,,,,
25,04/27/06,21:44:12,0 leases expired and 0 leases deleted,,,,
25,04/27/06,21:44:12,0 leases expired and 0 leases deleted,,,,
11,04/27/06,19:39:46,Renew,192.168.0.231,
    xpclient01.corp.quepublishing.com,00E07DC13E70,
31,04/27/06,19:39:46,DNS Update Failed,
    192.168.0.231,xpclient01.corp.quepublishing.com,-1,
10,04/27/06,19:43:07,Assign,192.168.0.230,
    iMac01.corp.quepublishing.com,00306509D772,
30,04/27/06,19:44:14,DNS Update Request,192.168.0.231,
    xpclient01.corp.quepublishing.com,,
31,04/27/06,19:44:14,DNS Update Failed,192.168.0.231,
    xpclient01.corp.quepublishing.com,-1,
30,04/27/06,19:47:03,DNS Update Request,192.168.0.231,
    xpclient01.corp.quepublishing.com,,
11,04/27/06,19:47:03,Renew,192.168.0.231,
    xpclient01.corp.quepublishing.com,00E07DC13E70,
30,04/27/06,19:47:03,DNS Update Request,
    192.168.0.231,xpclient01.corp.quepublishing.com,,
11,04/27/06,19:47:03,Renew,192.168.0.231,
    xpclient01.corp.quepublishing.com,00E07DC13E70,
32,04/27/06,19:47:03,DNS Update Successful,192.168.0.231,
    xpclient01.corp.quepublishing.com,,
32,04/27/06,19:47:03,DNS Update Successful,192.168.0.231,
    xpclient01.corp.quepublishing.com,,
```

As you can see from this example, the DHCP server cleans up the database hourly. You can also see that two clients requested leases. One of them, an Apple iMac, requested and was

assigned the IP address 192.168.0.230, with no further actions. Another client, a Windows XP Professional computer, requested and received the IP address 192.168.0.231, with several failed DNS updates (evidenced by ID 31). After the DNS dynamic update account was properly configured, the DHCP server was able to make the DNS dynamic updates and generate an ID of 32. Table 3.3 explains the ID codes used in the DHCP daily audit logs.

TABLE 3.3 The DHCP Daily Audit Log ID Codes

ID	Description
00	The log was started.
01	The log was stopped.
02	The log was temporarily paused due to low disk space.
10	A new IP address was leased to a client.
11	A client renewed a lease.
12	A client released a lease.
13	An IP address was found to be in use on the network.
14	A lease request could not be satisfied because the scope's address pool was exhausted.
15	A lease was denied.
16	A lease was deleted.
17	A lease was expired.
20	A BOOTP address was leased to a client.
21	A dynamic BOOTP address was leased to a client.
22	A BOOTP request could not be satisfied because the scope's address pool for BOOTP was exhausted.
23	A BOOTP IP address was deleted after a check was made to see that it was not in use.
24	The IP address cleanup operation has begun.
25	IP address cleanup statistics are provided.
30	A DNS update request to the named DNS server was made.
31	The DNS update failed.
32	The DNS update was successful.
50+	These IDs are used for Rogue Server Detection information.

In addition to the DHCP daily audit logs, events related to the DHCP service are generated and placed in the system log, as shown in Figure 3.37.

As you can see in Figure 3.38, a DHCP server on the network has not been authorized in Active Directory. The system log contains many useful log events about all aspects of a server, and this is an area you should review often.

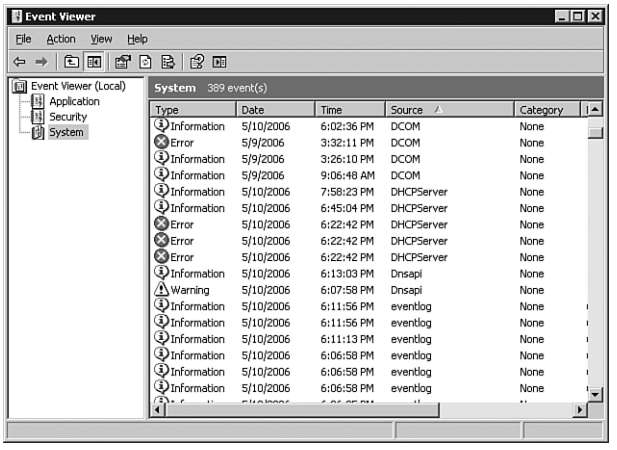

FIGURE 3.37 The system log contains events related to the DHCP service.

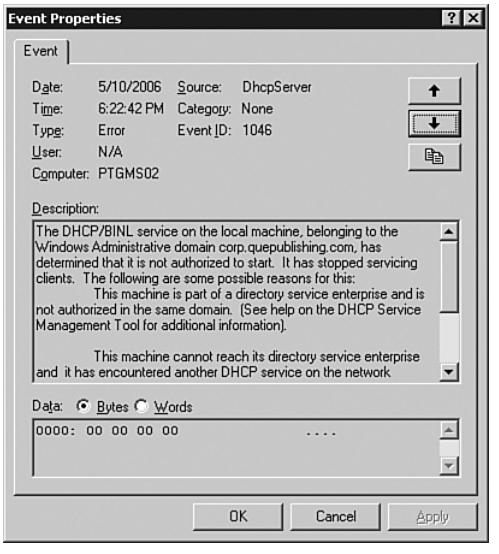

FIGURE 3.38 An unauthorized DHCP server cannot start the DHCP service.

Troubleshooting DHCP Reservations

For the most part, the only problem that prevents a DHCP reservation from functioning properly is a misconfigured MAC address. If you have a misconfigured DHCP reservation, it should show up in the Address Leases node of your DHCP server with the status Reservation (Inactive). Reservations that are configured properly show the status Reservation (Active). If you look back at Figure 3.16, you'll see that the reservation we created had a bad MAC address and, thus, was the cause of the problem in Figure 3.39.

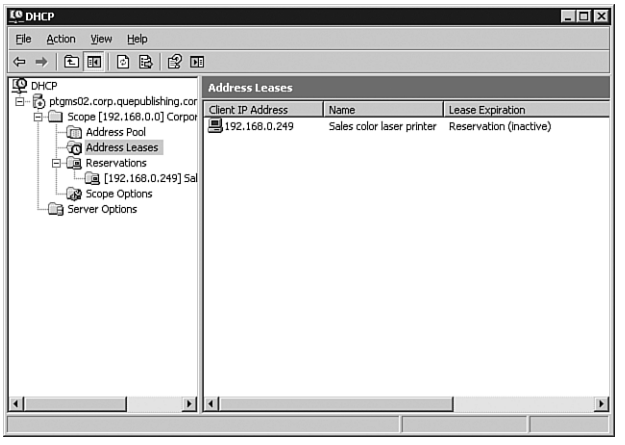

FIGURE 3.39 A DHCP reservation that is not active usually indicates a misconfiguration.

To verify that a reservation is configured properly, you can compare the MAC address of the component that is to have a reserved DHCP address (a print server, for example) to the MAC address entered in the reservation Properties dialog box. The vast majority of the time, this will reveal the source of the problem.

Troubleshooting the DHCP Relay Agent

The DHCP relay agent, like a DHCP reservation, typically doesn't present a problem. However, in some cases, relay services are not being provided to network clients. Some of the most common problems that you might encounter with the DHCP relay agent include the following:

- The network interface on the DHCP relay agent server that is connected to the subnet where the DHCP clients are located has not been selected for use with the DHCP relay agent. You can verify whether the interface has been added or add it from the DHCP Relay Agent node of the DHCP console. You should also verify that the Relay DHCP Packets check box is selected on all adapters that have been selected for use.
- An incorrectly entered DHCP server IP address on the DHCP Relay Agent Properties dialog box (refer back to Figure 3.32) prevents the successful relay of packets. You can verify and correct this problem from the properties dialog box of the DHCP Relay Agent node of the DHCP console.
- Remote DHCP servers might not be reachable because of network or server problems. In this case, you need to troubleshoot basic network connectivity, as discussed in Chapter 1, "Planning, Implementing, and Troubleshooting a TCP/IP Network Infrastructure". You should troubleshoot the server status as discussed in this chapter.
- DHCP traffic might be being filtered. In this case, you need to ensure that no IP filters exist for UDP ports 67 and 68 at any point between the DHCP servers and the remote DHCP clients.

Chapter Summary

In this chapter, we've examined how to implement, manage, and troubleshoot DHCP in Windows Server 2003. Some points of interest to take away from this chapter include the following:

- Windows Server 2003 DHCP supports three types of scopes: standard scopes, superscopes, and multicast scopes. A superscope is a grouping of one or more standard DHCP scopes, whereas a multicast scope is used for special Class D IP addresses for multicasting to clients.
- DHCP servers must be authorized in Active Directory to service clients. Windows Server 2003 DHCP servers that have not been authorized cannot offer leases to DHCP clients.
- DHCP can be integrated with DNS to provide dynamic updating of DNS A and PTR records for DHCP clients. This keeps the DNS database accurate and up-to-date as DHCP assigns leases to client computers.
- You can perform monitoring and troubleshooting on a DHCP server by using the DHCP counters in the Performance console.

Key Terms

- BOOTP
- DHCP
- DHCP client
- DHCP reservation
- DHCP server
- DNS
- Exclusion
- Lease
- Multicast scope
- Registered IP address
- RFCs
- Scope
- Supernetted network
- Superscope
- TCP/IP
- Unicast address

Apply Your Knowledge

In this chapter, you learned what DHCP is and how it works to make IP address assignment easier, quicker, and more accurate. In the following exercises, you will practice some of the concepts and methods discussed in this chapter.

Exercises

3.1 Creating a DHCP Scope

This exercise guides you through the process of creating a standard DHCP scope. This exercise requires you to have a Windows Server 2003 computer with the DHCP service installed.

Estimated time: 20 minutes

1. Open the DHCP console by selecting Start, Programs, Administrative Tools, DHCP.
2. Right-click the DHCP server and select New Scope from the context menu.
3. Click Next to dismiss the opening page of the New Scope Wizard.
4. On the Scope Name page, enter the name **`SCOPE1`** and an appropriate description for the new scope. Click Next to continue.
5. On the IP Address Range page, enter the IP address range **`10.0.0.2`**–**`10.0.0.100`**, and the subnet mask **`255.255.255.0`**. Click Next to continue.
6. On the Add Exclusions page, enter the IP address ranges **`10.0.0.5`**–**`10.0.0.10`** and **`10.0.0.15`**–**`10.0.0.20`** as exclusions. Click Next to continue.
7. On the Lease Duration page, you can leave the default setting of 8 days. Click Next to continue.
8. Select to configure advanced options and click Next to continue.
9. On the Router (Default Gateway) page, enter the default gateway IP address **`10.0.0.1`**. Click Next to continue.
10. On the Domain Name and DNS Servers page, enter the IP addresses **`10.0.0.250`** and **`10.0.0.251`** for the DNS servers. Specify the parent domain as **`testlab.local`**. Click Next to continue.
11. On the WINS Servers page, enter the IP addresses of the WINS servers if you have legacy clients that still need WINS services. Enter the IP addresses **`10.0.0.250`** and **`10.0.0.251`** for the WINS servers. Click Next to continue.
12. Opt to activate the scope now and click Finish to complete the wizard.

3.2 Creating a Superscope

This exercise shows you how to manage multiple scopes by creating a superscope. You must have completed Exercise 3.1 for this exercise to work.

Estimated time: 20 minutes

1. Open the DHCP console by selecting Start, Programs, Administrative Tools, DHCP.
2. Right-click the DHCP server and select New Scope from the context menu.
3. Create a second scope, using the IP address range 10.0.0.102 to 10.0.0.200, using the same default gateway, DNS servers, and WINS servers as detailed in Exercise 3.1, with no exclusions. Name the scope **SCOPE2**.
4. Right-click the DHCP server and select New Superscope from the context menu.
5. Click Next to dismiss the opening page of the New Superscope Wizard.
6. On the Superscope Name page, enter **SUPERSCOPE1** and click Next to continue.
7. On the Select Scopes page, select SCOPE1 and SCOPE2 by holding down the Ctrl key and clicking both scopes. Click Next to continue.
8. Verify your configuration on the Completing the New Superscope Wizard page. Click Next to complete the superscope-creation process.
9. The Completing the New Superscope Wizard dialog box summarizes the selections you made throughout the wizard. Click Finish to create the superscope.

3.3 Configuring a DHCP Relay Agent

This exercise walks you through the process of creating and configuring a DHCP relay agent for a network.

Estimated time: 15 minutes

1. Open the Routing and Remote Access console.
2. Expand the console nodes so that you can access the IP Routing, General node.
3. Right-click the General node and select New Routing Protocol.
4. Select the DHCP relay agent.
5. Right-click the DHCP Relay Agent node and select New Interface from the context menu to select the interface to be used for the DHCP relay agent.
6. Configure your required values for hop-count threshold and boot threshold.
7. Right-click the DHCP Relay Agent node and select Properties. Enter one or more remote DHCP servers in the list and click OK to confirm your settings.

3.4 Authorizing a DHCP Server in Active Directory

This exercise walks you through authorizing a DHCP server in Active Directory. This exercise requires that you have an Active Directory environment with an installed DHCP server.

Estimated time: 5 minutes

1. Open the DHCP console by selecting Start, Programs, Administrative Tools, DHCP.
2. Right-click the DHCP server and select Authorize from the context menu.
3. The authorization process might take some time, depending on network conditions. Refresh the DHCP console by pressing F5. The DHCP server status is shown as Active when the authorization is complete. The server is then ready to issue addresses when it receives DHCP requests.

3.5 Configuring DHCP for DNS Integration

This exercise walks you through configuring a DHCP server for DNS integration. This exercise requires that you have an Active Directory environment with an installed DHCP server and DNS server. To complete this exercise, you must have completed Exercise 3.4.

Estimated time: 15 minutes

1. Open the DHCP console by selecting Start, Programs, Administrative Tools, DHCP.
2. Right-click the DHCP server and select Properties from the context menu. Switch to the DNS tab of the DHCP Server Properties dialog box.
3. To enable DHCP integration with DNS, ensure that the Enable Dynamic DNS Updates According to the Settings Below check box is selected.
4. Select either to have the DHCP server update A and PTR records when requested or to always update A and PTR records.
5. To help keep your DNS database clean and consistent, you should allow the DHCP server to cause expired leases to lead to A and PTR record deletion.
6. If you have legacy clients on the network, ensure that dynamic updating is configured for them as well.
7. If you are using secure dynamic updates, you should consider configuring a dedicated network user account for the dynamic updating. You can enter the account credentials by switching to the Advanced tab.
8. Click the Credentials button on the Advanced tab to open the DNS Dynamic Update Credentials dialog box.
9. Enter the domain user account name, domain, and password.

Review Questions

1. You are the systems administrator for Exponent Mathematicians, and you have been asked to implement DHCP on a multinetted network segment. What should you do to ensure that you do this successfully?

2. You are the administrator of the DHCP server for the Get Bux pawn shop chain. You are getting complaints from users that they keep getting address-conflict messages when they turn on their computers. What DHCP counter might help you identify the problem?

3. You are the administrator for Fly Away Travel. When administering Fly Away's DHCP server, you notice that the number of DHCP requests is very high for the number of users on the network. Where is the first place you should look for a server-related problem?

4. You're the administrator of the DHCP server for Little Faith Enterprises. You notice that the DHCP server is running sluggishly during peak hours. When you check the Performance utility, you notice that the DHCP Conflict Check Queue Length counter is very high. What could be causing the DHCP server to be running slowly?

5. You're the administrator of the DHCP server for Little Faith Enterprises. You have just installed the DHCP service and created your first scope by using the New Scope Wizard. You are trying to provide DHCP addresses to a group of users that are two router hops away. What do you still need to do?

Exam Questions

1. You are the systems administrator for Wild Widgets, Inc. You are training a new employee on the use of the DHCP service in Windows Server 2003. She asks you how the client computer requests and receives an address from the server. Which of the following answers is correct?

   - ❍ **A.** The client computer broadcasts a `DHCPDISCOVER` message. The DHCP server offers an IP address. The client computer accepts the address and uses it to communicate on the network.

   - ❍ **B.** The client computer broadcasts a `DHCPDISCOVER` message. The DHCP server offers an IP address. The client computer accepts the address and sends a request to use that address back to the DHCP server. The client computer uses the address to communicate on the network.

   - ❍ **C.** The client computer broadcasts a `DHCPDISCOVER` message. The DHCP server offers an IP address. The client computer accepts the address and sends a request to use that address back to the DHCP server. The DHCP server acknowledges the request and grants the client computer a lease to use the address. The client computer uses the address to connect to the network.

   - ❍ **D.** The client computer broadcasts a `DHCPDISCOVER` message. The DHCP server offers an IP address. The client computer accepts the address and sends a request to use that address back to the DHCP server. The DHCP server acknowledges the request and grants the client computer a lease to use the address. The client computer responds with an acknowledgment of the lease and uses the address to connect to the network.

2. You are the system administrator for Phil's Phill-up Stations, a chain of gas stations. As part of the network, you maintain a Windows Server 2003 DHCP server to dynamically assign addresses. You have three superscopes set up, and within each superscope are four scopes. One day, you start experiencing problems with one of the scopes issuing bad addresses. You check the server and suspect that there is a database problem. How can you verify that the database is intact?

   - ❍ **A.** Open the DHCP console. Select the scope in question and select Action, Reconcile Scope.
   - ❍ **B.** Open the DHCP console. Select the superscope that contains the scope in question and then select Action, Reconcile All Scopes.
   - ❍ **C.** Open the DHCP console. Select the DHCP server that contains the scope in question and then select Action, Reconcile All Scopes.
   - ❍ **D.** Open the DHCP console. Select the DHCP server that contains the scope in question and then select Action, Reconcile DHCP Database.

3. You are the LAN administrator for Get Stuffed Taxidermy, and you are responsible for maintaining the company's Windows Server 2003 DHCP server. While doing your daily system checks, you notice that the number of `DHCPDISCOVER` packets spiked at 9:00 this morning. What could cause the Discovers/Sec counter to spike at 9:00 a.m.?

   - ❍ **A.** A network problem
   - ❍ **B.** The DHCP service being restarted
   - ❍ **C.** A large number of computers entering the network at approximately the same time
   - ❍ **D.** A rogue DHCP server issuing duplicate addresses

4. You are the systems administrator for Hank's Harmonicas, Ltd. Your Active Directory–based network consists of all Windows Server 2003 server computers and Windows 98, Windows 2000 Professional, and Windows XP Professional client computers. This morning, one of the users of a Windows 98 computer called you and said that she could no longer connect to network resources. Upon further investigation, you discover that several other Windows 98 clients are experiencing the same problem. You determine that the cause of the problem is an incorrectly configured DHCP lease. What is the most likely reason that only your Windows 98 clients are exhibiting this problem?

   - ❍ **A.** The DHCP service in Windows 98 is not as stable as that in Windows 2000 or Windows XP, and this sometimes results in corrupted lease information.
   - ❍ **B.** An unauthorized DHCP server has been set up on the network.
   - ❍ **C.** A misconfigured DHCP server has been set up on the network.
   - ❍ **D.** The Windows 98 clients were unable to renew their DHCP lease and have thus assumed APIPA IP addresses instead.

5. You are the lead systems administrator for Little Faith Enterprises, and a customer has asked you to install the DHCP service on her Windows Server 2003 computer, get one scope configured, and issue addresses. What minimum steps do you need to take to accomplish this?

   - ❍ **A.** Install the DHCP service from the Windows Components Wizard. After the service is installed, authorize it in Active Directory. Next, create the scope. Finally, configure the DNS integration.
   - ❍ **B.** Install the DHCP service from the Windows Components Wizard. After the service is installed, create the scope and then configure the DNS integration.
   - ❍ **C.** Install the DHCP service from the Windows Components Wizard. After the service is installed, create the scope. Create a superscope and add the scope to it. Authorize the server in Active Directory.
   - ❍ **D.** Install the DHCP service from the Windows Components Wizard. After the service is installed, create the scope. Authorize the server in Active Directory.

6. You are the systems administrator for the Hittem Boxing Glove Corporation. The corporation is running a routed network with a centrally located Windows Server 2003 DHCP server. The server is capable of issuing addresses to users on the local segment, but it cannot issue addresses to any of the sites that are across a router. What is the most probable cause of this problem?

   - ❍ **A.** The DHCP forwarder service is not enabled on the DHCP server.
   - ❍ **B.** The BOOTP forwarder service is not enabled on the DHCP server.
   - ❍ **C.** The DHCP forwarder service is not enabled on the routers.
   - ❍ **D.** The BOOTP forwarder service is not enabled on the routers.

7. You manage the Windows Server 2003 DHCP servers for the Really Big Screwdriver Corporation. You are running in a purely Windows Server 2003 environment with all Windows XP Professional clients, and you need to make sure that workstations are registered properly in DNS for Active Directory integration. How should you configure DNS integration?

   - ❍ **A.** Set DNS integration to automatically update DHCP client information in DNS.
   - ❍ **B.** Set DNS integration to discard A and PTR records when a lease is deleted.
   - ❍ **C.** Set DNS integration to enable updates for DNS clients that do not support dynamic updates.
   - ❍ **D.** Set DNS integration to enable DNS keepalives.

8. You are the systems administrator for UR Write publishing, a bookseller. Your Windows Server 2003 DHCP server issues a block of 40 addresses to 120 salespeople on the Sales network. These users are frequently in and out of the office, so no more than 40 users are ever on the network at one time. What do you need to do to ensure that users get addresses when needed?

   - ❍ **A.** Set the DHCP lease duration to 60 minutes.
   - ❍ **B.** Set the DHCP lease duration to 5 days.

- ❍ **C.** Configure a reservation for each user.
- ❍ **D.** Configure an exclusion for each user.

9. You are the distributed computing administrator for Talk to Me Telephone. The company has Windows Server 2003 installed, with the DHCP service running. Mixed in with the DHCP client computers, the company still has some old workstations on the network with BOOTP chips on their Ethernet cards. You need to add support for BOOTP for these computers. How do you ensure that support?

- ❍ **A.** Add the BOOTP service to the server.
- ❍ **B.** In the Advanced tab of the scope Properties dialog box, configure the server to issue addresses to BOOTP clients.
- ❍ **C.** In the Advanced tab of the server Properties dialog box, configure the server to issue addresses to both DHCP and BOOTP clients.
- ❍ **D.** In the Advanced tab of the scope Properties dialog box, configure the server to issue addresses to both DHCP and BOOTP clients.

10. You manage the Windows Server 2003 DHCP servers for the Really Big Hammer Corporation. It is a mixed environment, with Windows 2000, Windows XP, and Windows 98 workstations. You need to make sure workstations are registered properly in DNS for Active Directory integration. What do you need to do?

- ❍ **A.** Set DNS integration to automatically update DHCP client information in DNS.
- ❍ **B.** Set DNS integration to discard A and PTR records when a lease is deleted.
- ❍ **C.** Set DNS integration to enable updates for DNS clients that do not request dynamic updates.
- ❍ **D.** Set DNS integration to enable DNS keepalives.

11. You are the systems administrator for BT Editing Unlimited. You have a 50-host network and are running a Windows Server 2003 DHCP server to assign IP addresses. You also have five IP-based printers with static IP addresses. Your assistant administrator has been working on the DHCP server and has made some changes. Now your users cannot print to one of the printers. What is most likely the problem?

- ❍ **A.** The scope from which the printers were receiving their IP addresses has been deleted.
- ❍ **B.** The existing scope has been modified so that it overlaps the addresses reserved for the printers.
- ❍ **C.** The existing scope has been modified so that it overlaps the addresses reserved for the printers, and a workstation has been assigned the same address as one of the printers.
- ❍ **D.** The DHCP service was inadvertently stopped.

12. You are the systems administrator for the Little Faith Department Store. You are responsible for maintaining the company's Windows Server 2003 DHCP server. The company recently added a new router and routed a segment to the network. Now that segment must be added to the DHCP server. The address of the router port is 10.10.25.1, and the router is subnetted with a Class C subnet mask. You need to provide 40 addresses, starting at 10.10.25.20. What needs to occur for you to get DHCP working on that segment?

- ❍ **A.** You need to install and configure an additional DHCP server on that segment to provide DHCP services.
- ❍ **B.** You need to add to the DHCP server a scope that contains the addresses from 10.10.25.20 through 10.10.25.59. The scope needs a subnet mask of 255.255.255.0. You need to configure the BOOTP forwarder for the new segment's router, using the address of the DHCP server. You need to activate the scope.
- ❍ **C.** You need to add to the DHCP server a scope that contains the addresses from 10.10.25.20 through 10.10.25.60. The scope needs a subnet mask of 255.255.255.0. You need to configure the BOOTP forwarder for the new segment's router, using the address of the DHCP server. You need to activate the scope.
- ❍ **D.** You need to add to the DHCP server a scope that contains the addresses from 10.10.25.20 through 10.10.25.60. The scope needs a subnet mask of 255.255.255.0. You need to configure the BOOTP forwarder for the new segment's router, using the address of the DHCP server. You do not need to activate the scope because that happens automatically when the scope is created.

13. You are the network manager for IntCo Manufacturing. You are running in a mixed environment, and you are using a Windows Server 2003 DHCP service to support three network segments. Your client computers consist of Windows 2000 Professional, Windows NT Workstation, and Windows 98 SE workstations. What do you need to do to ensure that all the client computers can receive DHCP addresses?

- ❍ **A.** Configure a scope for each network segment. Configure each client computer to receive IP addresses dynamically. Configure the DHCP service for backward compatibility.
- ❍ **B.** Configure a scope for each network segment. Configure each client computer to receive IP addresses dynamically. For the Windows NT Workstation client computers, ensure that the DHCP update from Service Pack 6 has been installed.
- ❍ **C.** Configure a scope for each network segment. Configure each client computer to receive IP addresses dynamically. Configure the DHCP service for mixed mode.
- ❍ **D.** Configure a scope for each network segment. Configure each client computer to receive IP addresses dynamically.

14. You are the systems administrator for BT Editing, and you are running a purely Windows Server 2003 network, using Active Directory and the Windows Server 2003 DHCP service. A user in another department has installed a DHCP server on a UNIX server. How do you prevent your client computers from receiving DHCP addresses from that server?

    - ❍ **A.** Disable the unauthorized server in Active Directory.
    - ❍ **B.** Make sure all your domain client computers are running Windows 2000 or higher.
    - ❍ **C.** Reconfigure BOOTP on the router.
    - ❍ **D.** Go to each client computer and enter the address of the production DHCP server in the Internet Protocol (TCP/IP) Properties dialog box.

15. You are the systems administrator for Area 51 Partners, a consulting firm that is not involved in any way, shape, or form with alien activity in Nevada. You have a customer who would like to ensure that only authorized DHCP servers can make dynamic updates to the DNS database. What will you configure for the customer to make this happen? (Choose all that apply.)

    - ❍ **A.** Create a new domain user account called DNSDYNUPD.
    - ❍ **B.** Enter the credentials for the DNSDYNUPD account in the scope options for your DHCP server.
    - ❍ **C.** Enter the credentials for the DNSDYNUPD account in the DNS Dynamic Update Credentials dialog box for your DHCP server.
    - ❍ **D.** Add the DNSDYNUPD account to the Enterprise Administrators group.

Answers to Review Questions

1. To successfully implement DHCP in a multinetted environment, you should consider using a superscope to ease the management of the scopes for each of the multinetted networks. For more information, see the section “Understanding DHCP Superscopes.”
2. You should check the Declines/Sec counter in the Performance console for the DHCP object. The number of DHCPDECLINE messages received per second by the DHCP server from client computers can be used to see whether the DHCP client computer has declined the IP address issued by the server. You see this number rise when client computers start having address conflict problems, and it could indicate a network problem, computers with static addresses also being part of a scope, or a rogue DHCP server being on the network. For more information, see the section “Troubleshooting DHCP Server Authorization Problems.”
3. You should check the length of the DHCP lease. If the lease has been set to a very short duration, client computers would need to request addresses frequently. For more information, see the section “Creating a DHCP Scope.”

4. Either a lot of DHCP requests are occurring during peak hours or the Conflict Detection Attempts parameter is set too high. If that parameter is enabled, the Windows Server 2003 DHCP service issues an address and checks whether any IP address conflicts exist. This can put a lot of additional overhead on the server and drive up the DHCP conflict check queue length. For more information, see the section "Troubleshooting DHCP Server Authorization Problems."

5. First, you need to authorize the DHCP server in Active Directory. The DHCP server cannot provide addresses until that occurs. You also need to configure the BOOTP forwarder on any routers between the DHCP server and the client workstations so that the routers know where to forward DHCP messages. For more information, see the section "Authorizing a DHCP Server in Active Directory."

Answers to Exam Questions

1. **C**. The client computer cannot use the address until the DHCP server grants the lease. After the DHCP server acknowledges the DHCP request and grants the lease, the client computer can use the address. Before a client computer can actually use an offered address, it must request to do so and receive an acknowledgment from the offering DHCP server; thus, answers A, B, and D are incorrect. No additional step is required in the process. For more information, see the section "DHCP."

2. **C**. You need to reconcile all the scopes on the server. Answer A is almost correct because you can reconcile a single scope, but the correct command is Reconcile, not Reconcile Scope. You cannot reconcile scopes at the superscope level, as stated in answer B. The command in answer D does not exist.

3. **C**. The `DHCPDISCOVER` packet is sent when a computer first requests an address. The most likely reason for the Discovers/Sec counter to spike would be a large number of concurrent requests occurring, which could happen when a large number of client workstations request addresses at the same time. A network problem would have the opposite effect because no `DHCPDISCOVER` packets would reach the server; thus, answer A is incorrect. A DHCP service restart or a rogue DHCP server couldn't affect the number of `DHCPDISCOVER` packets because the packets are generated by client PCs; thus, answers B and D are incorrect. For more information, see the section "Troubleshooting DHCP Server Authorization Problems."

4. **B**. In this scenario, the most likely cause for the problem is that an unauthorized DHCP server has been set up on the network. Windows 2000 and Windows XP clients in an Active Directory domain do not take DHCP leases from DHCP servers that have not been authorized in Active Directory. The DHCP service in Windows 98 would not likely cause this sort of problem; thus, answer A is incorrect. A misconfigured DHCP server that was authorized would give bad DHCP lease information to all clients, not just to Windows 98 clients; thus, answer C is incorrect. In addition, if clients were unable to reach a DHCP server, the Windows 2000 and Windows XP clients would also assign themselves APIPA IP addresses; thus, answer D is incorrect. For more information, see the section "Troubleshooting DHCP Server Authorization Problems."

5. **D**. If the task is to install the DHCP service and get it issuing addresses, you do not need to configure DNS, but you do need to authorize the server in Active Directory; thus, answers A and B are incorrect. Even though you learned how to create a superscope in this chapter, you do not need a superscope for the server to function; thus, answer C is incorrect.

6. **D**. To issue addresses using DHCP across a router, the router needs to have the BOOTP forwarder service enabled and configured; thus, answer C is incorrect. DHCP relay is configured on a router or a Windows Server 2003 computer running Routing and Remote Access; thus, answer A is incorrect. There is no such thing as the BOOTP forwarder server; thus, answer B is incorrect. For more information, see the section "Configuring and Implementing a DHCP Relay Agent."

7. **A**. In a purely Windows 2000, Windows XP, and Windows Server 2003 environment, you need to configure DHCP to automatically update DNS to ensure that the client computers appear on the network correctly. Setting the DNS integration to discard lookups after a lease is deleted also works with a purely Windows 2000 network, but it has nothing to do with the computers registering properly; thus, answer B is incorrect. Windows 2000, Windows XP, and Windows Server 2003 all support dynamic updates; thus, answer C is incorrect. Keepalives are associated with HTTP sessions, not DNS; thus, answer D is incorrect. For more information, see the section "Configuring DHCP for DNS Integration."

8. **A**. To ensure that addresses are available, the DHCP lease needs to be set to a short interval; thus, answer B is incorrect. Reservations won't help since you have too few leases already; thus, answer C incorrect. There was no mention of a need for exclusions and, thus, no need to configure them; therefore, answer D is incorrect. For more information, see the section "Creating a DHCP Scope."

9. **D**. You need to configure the scope to issue addresses to both DHCP and BOOTP clients; thus, answers A, B, and C are incorrect. For more information, see the section "Creating a DHCP Scope."

10. **C**. Because the non–Windows 2000 (or non–Windows XP) machines lack the capability to directly update the DNS server themselves, you need the DHCP server to make the updates to DNS. Using DNS integration to enable updates for DNS client computers that do not support dynamic updates enables the DHCP server to perform this service. The options mentioned in answers A and B do not exist; thus, they are incorrect. Keepalives are associated with HTTP sessions, not DNS; thus, answer D is incorrect. For more information, see the section "Configuring DHCP for DNS Integration."

11. **C**. The address from the printer has probably been issued to another computer. Because the printers use static addresses, the only change to the DHCP server that could have affected printing would be another host having the same address. Deleting the scope would cause problems, but not likely right away; thus, answer A is incorrect. Answer B is close, but just creating an overlapping scope is not a problem until the overlapping addresses are assigned. As with deleting the scope, stopping the DHCP service would causes problems, but not unless a client needed a new address; thus, answer D is incorrect.

12. **B**. A single DHCP server can serve multiple segments, so you do not need an additional server. To get 40 addresses, the range must be from 10.10.25.20 to 10.10.25.59, which is an inclusive range. Also, the last step of the New Scope Wizard is to authorize the new scope. The actions listed in answer A are not enough to perform the required task; thus, answer A is incorrect. Answers C and D each provide 41 addresses; in addition, answer D has you not activating the scope, which you must do to use the scope. Therefore, answers C are D are incorrect.

13. **D**. You do not need to make any special configurations to the DHCP service; it can communicate with non–Windows 2000 or non–Windows XP client computers without problems. Thus, answers A and C are incorrect. You also do not need to update any of the client computers. Windows NT and Windows 98 are capable of using DHCP without needing updates applied; thus, answer B is incorrect. You just need to configure the appropriate scope and configure the client computers to use that scope.

14. **B**. Because a UNIX server cannot be enabled in Active Directory, Windows 2000 (and Windows XP) client computers do not accept DHCP addresses from the server. Answer A is not correct because you cannot disable a server that isn't joined to the Active Directory domain. Changing the BOOTP configuration on the router might prevent remote users from receiving addresses, but local users would still be vulnerable; thus, answer C is incorrect. In answer D, there is nowhere to enter the address of the DHCP server. For more information, see the section "Authorizing a DHCP Server in Active Directory."

15. **A, C**. Windows Server 2003 enables you to use a preconfigured domain user account to perform DNS dynamic updates. This ensures that only authorized DHCP servers are performing dynamic updates and that all DHCP servers can update and modify DNS entries. In addition, this prevents problems previously associated with allowing a DHCP server running on a domain controller to perform DNS dynamic updates. The best course of action is to create a dedicated domain user account for this purpose. The account information to be used for dynamic updates is configured at the server level; thus, answer B is incorrect. The account used for dynamic updates does not need to be a member of the Enterprise Administrators group; thus, answer D is incorrect. For more information, see the section "Configuring DHCP for DNS Integration."

Suggested Readings and Resources

1. Davies, Joseph, and Thomas Lee. *Microsoft Windows Server 2003 TCP/IP Protocols and Services Technical Reference*. Redmond, WA: Microsoft Press, 2003.

2. Stevens, W. Richard. *TCP/IP Illustrated, Volume 1: The Protocols*. Boston: Addison-Wesley, 1994.

3. "Deploying Network Services." http://technet2.microsoft.com/WindowsServer/en/Library/119050c9-7c4d-4cbf-8f38-97c45e4d01ef1033.mspx.

4. "Technical Overview of Windows Server 2003 Networking and Communications." www.microsoft.com/windowsserver2003/techinfo/overview/netcomm.mspx.

5. "Windows Server 2003 Reviewer's Guide." www.microsoft.com/windowsserver2003/techinfo/overview/reviewersguide.mspx.

6. "Dynamic Host Configuration Protocol (DHCP) Operations Topics." http://technet2.microsoft.com/windowsserver/en/operations/dhcp.mspx.

7. "Windows Server 2003 Security Guide." www.microsoft.com/technet/security/prodtech/windowsserver2003/W2003HG/SGCH00.mspx.