Chapter 10

Implementing Dynamic Host Configuration Protocol (DHCP)

About This Chapter

In this chapter, you learn how to use the Dynamic Host Configuration Protocol (DHCP) to automatically configure Transmission Control Protocol/Internet Protocol (TCP/IP) and eliminate some common configuration problems. During the lessons, you install and configure a DHCP server, test the DHCP configuration, and then obtain an Internet Protocol (IP) address from a DHCP server.

Before You Begin

To complete the lessons in this chapter, you must have

- Installed Microsoft Windows 2000 Server with TCP/IP

Lesson 1: Introducing and Installing DHCP

DHCP automatically assigns IP addresses to computers. DHCP overcomes the limitations of configuring TCP/IP manually. This lesson gives you an overview of DHCP and how it works.

After this lesson, you will be able to

- Describe the difference between manual and automatic configuration of TCP/IP
- Identify TCP/IP configuration parameters that can be assigned by a DHCP server
- Describe IP Lease Requests and Offers
- Install DHCP in Windows 2000

Estimated lesson time: 20 minutes

DHCP Overview

DHCP is an extension of the Boot Protocol (BOOTP). BOOTP enables diskless clients

to start up and automatically configure TCP/IP. DHCP centralizes and manages the allocation of TCP/IP configuration information by automatically assigning IP addresses to computers configured to use DHCP. Implementing DHCP eliminates some of the configuration problems associated with manually configuring TCP/IP.

As illustrated in Figure 10.1, each time a DHCP client starts, it requests IP addressing information from a DHCP server, including the IP address, the subnet mask, and optional values. The optional values may include a default gateway address, Domain Name System (DNS) address, and Windows Internet Name Service (WINS) server address.

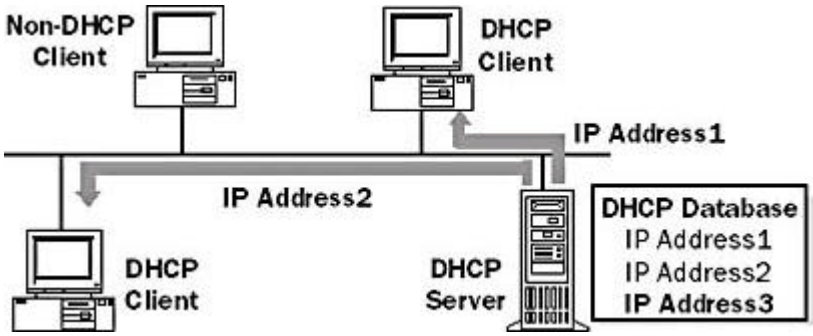

Figure 10.1 *How a DHCP client interacts with a DHCP server*

When a DHCP server receives a request, it selects IP addressing information from a pool of addresses defined in its database and offers it to the DHCP client. If the client accepts the offer, the IP addressing information is leased to the client for a specified period of time. If there is no available IP addressing information in the pool to lease to a client, the client cannot initialize TCP/IP.

Manual vs. Automatic Configuration

To understand why DHCP is beneficial in configuring TCP/IP on client computers, it is useful to contrast the manual method of configuring TCP/IP with the automatic method using DHCP.

Configuring TCP/IP Manually

Configuring TCP/IP manually means that users can easily pick a random IP address instead of getting a valid IP address from the network administrator. Using incorrect addresses can lead to network problems that can be very difficult to trace to the source.

In addition, typing the IP address, subnet mask, or default gateway can lead to problems ranging from trouble communicating if the default gateway or subnet mask is wrong to problems associated with a duplicate IP address.

Another limitation of configuring TCP/IP manually is the administrative overhead on internetworks where computers are frequently moved from one subnet to another. For example, when a workstation is moved to a different subnet, the IP address and default gateway address must be changed for the workstation to communicate from its new location.

Configuring TCP/IP Using DHCP

Using DHCP to automatically configure IP addressing information means that users no longer need to acquire IP addressing information from an administrator to configure TCP/IP. The DHCP server supplies all of the necessary configuration information to all of the DHCP clients. Many difficult-to-trace network problems are eliminated by using DHCP.

TCP/IP configuration parameters that can be assigned by the DHCP server include

- IP addresses for each network adapter in a client computer
- Subnet masks that are used to identify the IP network portion from the host portion of the IP address
- Default gateways (routers) that are used to connect a single network segment to others
- Additional configuration parameters that can optionally be assigned to DHCP clients (such as IP addresses for DNS or WINS servers a client may use)

How DHCP Works

DHCP uses a four-phase process to configure a DHCP client, as shown in Table 10.1. If a computer has multiple network adapters, the DHCP process occurs separately over each adapter. A unique IP address will be assigned to each adapter in the computer. All DHCP communication is done over User Datagram Protocol (UDP) ports 67 and 68.

Most DHCP messages are sent by broadcast. For DHCP clients to communicate with a DHCP server on a remote network, the IP routers must support forwarding DHCP broadcasts. DHCP configuration phases are shown in Table 10.1.

Table 10.1 *Four Phases of DHCP Client Configuration*

Phase	Description
IP lease discover	The client initializes a limited version of TCP/IP and broadcasts a request for the location of a DHCP server and IP addressing information.
IP lease offer	All DHCP servers that have valid IP addressing information available send an offer to the client.
IP lease request	The client selects the IP addressing information from the first offer it receives and broadcasts a message requesting to lease the IP addressing information in the offer.
IP lease acknowledgment	The DHCP server that made the offer responds to the message, and all other DHCP servers withdraw their offers. The IP addressing information is assigned to the client and an acknowledgment is sent. The client finishes initializing and binding the TCP/IP protocol. Once the automatic configuration process is complete, the client can use all TCP/IP services and utilities for normal network communications and connectivity to other IP hosts.

IP Lease Discover and Offer

As illustrated in Figure 10.2, in the first two phases, the client broadcasts for a DHCP server and a DHCP server offers an IP address to the client.

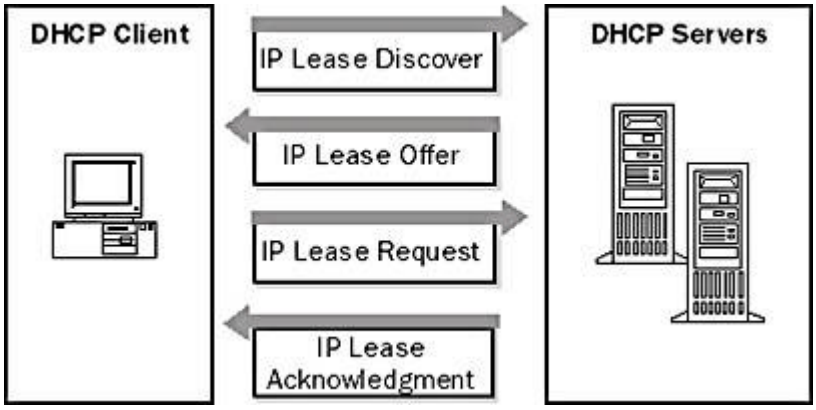

Figure 10.2 *IP lease discover and offer*

IP Lease Discover

During the boot process of a client, it requests to lease an IP address by broadcasting a request to all DHCP servers. Because the client does not have an IP address or know the IP address of a DHCP server, it uses 0.0.0.0 as the source address and 255.255.255.255 as the destination address.

The request for a lease is sent in a DHCPDISCOVER message. This message also contains the client's hardware address and computer name so that DHCP servers know which client sent the request.

The IP lease process is used when one of the following occurs:

- TCP/IP is initialized for the first time as a DHCP client
- The client requests a specific IP address and is denied, possibly because the DHCP server dropped the lease
- The client previously leased an IP address but released the lease and now requires a new lease

IP Lease Offer

All DHCP servers that receive the request and have a valid configuration for the client broadcast an offer with the following information:

- The client's hardware address
- An offered IP address
- Subnet mask
- Length of the lease

- A server identifier (the IP address of the offering DHCP server)

A broadcast is used because the client does not yet have an IP address. As illustrated in Figure 10.3, the offer is sent as a DHCPOFFER message. The DHCP server reserves the IP address so that it will not be offered to another DHCP client. The DHCP client selects the IP address from the first offer it receives.

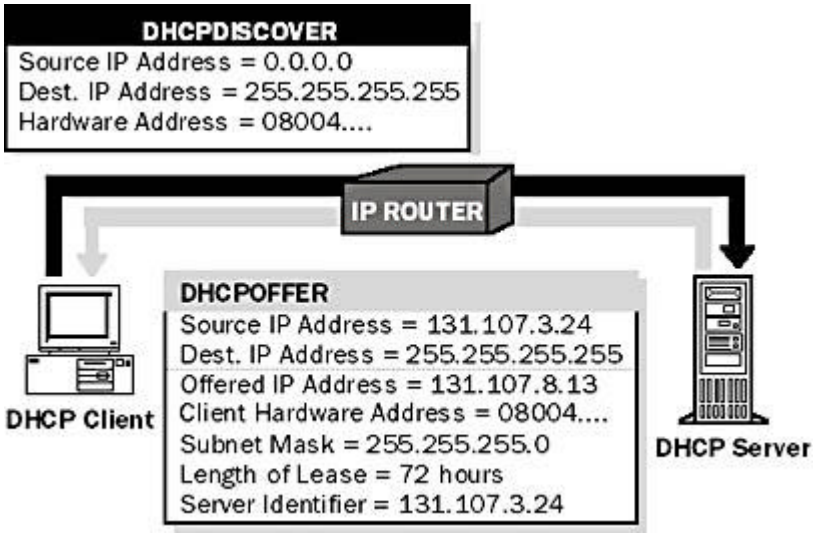

Figure 10.3 *Sending a DHCPOFFER message*

When No DHCP Servers Are Online

The DHCP client waits 1 second for an offer. If an offer is not received, the client will not be able to initialize and it will rebroadcast the request three times (at 9-, 13-, and 16-second intervals, plus a random length of time between 0 and 1000 milliseconds). If an offer is not received after four requests, the client will retry every 5 minutes.

Windows 2000-based clients can automatically configure an IP address and subnet mask if a DHCP server is unavailable at system start time. This is a new feature of Windows 2000 called Automatic Private IP Addressing (APIPA). This is useful for clients on small private networks, such as a small business office, a home office, or a remote access client. The Windows 2000 DHCP client service goes through the following process to autoconfigure the client:

1. The DHCP client attempts to locate a DHCP server and obtain an address and configuration.

2. If a DHCP server cannot be found or does not respond, the DHCP client autoconfigures its IP address and subnet mask using a selected address from the Microsoft-reserved Class B network, 169.254.0.0, with the subnet mask 255.255.0.0.

   The DHCP client tests for an address conflict to make sure that the IP address it has chosen is not already in use on the network. If a conflict is found, the client selects another IP address. The client will retry autoconfiguration for up to 10 addresses.

3. Once the DHCP client succeeds in self-selecting an address, it configures its network interface with the IP address. The client then continues, in the

background, to check for a DHCP server every 5 minutes. If a DHCP server is found later, the client abandons its autoconfigured information. The DHCP client then uses an address offered by the DHCP server (and any other provided DHCP option information) to update its IP configuration settings.

IP Lease Request and Acknowledgment

In the last two phases, the client selects an offer and the DHCP server acknowledges the lease.

IP Lease Request

After the client receives an offer from at least one DHCP server, it broadcasts to all DHCP servers that it has made a selection by accepting an offer.

The broadcast is sent in a DHCPREQUEST message and includes the server identifier (IP address) of the server whose offer was accepted. All other DHCP servers then retract their offers so that their IP addresses are available for the next IP lease request.

IP Lease Acknowledgment (Successful)

The DHCP server with the accepted offer broadcasts a successful acknowledgment to the client in the form of a DHCPACK message. This message contains a valid lease for an IP address and possibly other configuration information. When the DHCP client receives the acknowledgment, TCP/IP is completely initialized and is considered a bound DHCP client. Once bound, the client can use TCP/IP to communicate on the internetwork.

IP Lease Acknowledgment (Unsuccessful)

An unsuccessful acknowledgment (DHCPNACK) is broadcast if the client is trying to lease its previous IP address and the IP address is no longer available. It is also broadcast if the IP address is invalid because the client has been physically moved to a different subnet. When the client receives an unsuccessful acknowledgment, it returns to the process of requesting an IP lease.

Installing a DHCP Server

Before you install a DHCP server, you should identify the following:

- The hardware and storage requirements for the DHCP server
- Which computers you can immediately configure as DHCP clients for dynamic TCP/IP configuration and which computers you should manually configure with static TCP/IP configuration parameters, including static IP addresses
- The DHCP option types and their values to be predefined for DHCP clients

Before you install DHCP, answer the following questions:

- **Will all of the computers become DHCP clients?** If not, consider that non-DHCP clients have static IP addresses, and static IP addresses must be excluded from the DHCP server configuration. If a client requires a specific address, the

IP address needs to be reserved.

- **Will a DHCP server supply IP addresses to multiple subnets?** If so, consider that any routers connecting subnets act as DHCP relay agents. If your routers are not acting as DHCP relay agents, at least one DHCP server is required on each subnet that has DHCP clients. The DHCP server could be a DHCP relay agent or a router that has BOOTP enabled.

- **How many DHCP servers are required?** Consider that a DHCP server does not share information with other DHCP servers. Therefore, it is necessary to create unique IP addresses for each server to assign to clients.

- **What IP addressing options will clients obtain from a DHCP server?** The IP addressing options determine how to configure the DHCP server, and whether the options should be created for all of the clients in the internetwork, clients on a specific subnet, or individual clients. The IP addressing options might be:

    - Default gateway
    - DNS server
    - NetBIOS over TCP/IP name resolution
    - WINS server
    - NetBIOS scope ID

- **To install a DHCP server**

1. Open Windows Components Wizard by clicking Start, pointing to Settings, and clicking Control Panel.

   When Control Panel opens, double-click Add/Remove Programs, then click Add/Remove Windows Components.

2. Under Components, scroll to and click Networking Services.

3. Click Details.

4. Under Subcomponents Of Networking Services, select Dynamic Host Configuration Protocol (DHCP), click OK, then click Next.

   If prompted, type the full path to the Windows 2000 distribution files and click Continue. Required files will be copied to your hard disk.

5. Click Finish to close the Windows Components Wizard.

   NOTE

   It is strongly recommended that you manually configure the DHCP server computer to use a static IP address. The DHCP server cannot be a DHCP client. It must have a static IP address, subnet mask, and default gateway address.

Ipconfig

Ipconfig is a command-line tool that displays the current configuration of the installed IP stack on a networked computer. It can display a detailed configuration report for all interfaces, including any configured wide area network (WAN) miniports, such as those used for remote access or virtual private network (VPN) connections. A sample report is illustrated in Figure 10.4.

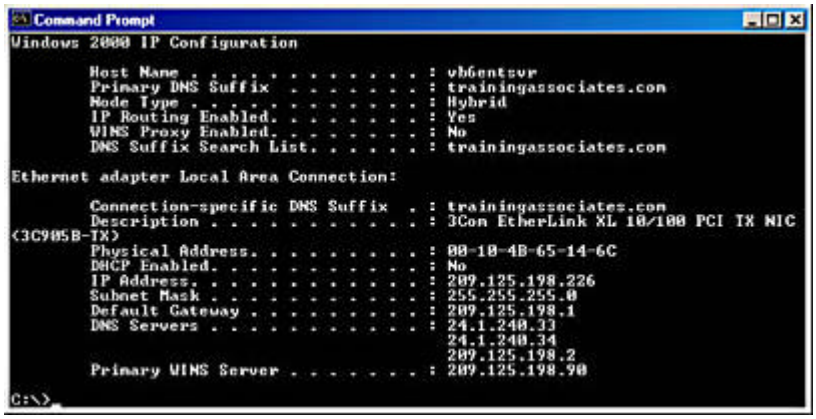

Figure 10.4 *Report displayed for Ipconfig /all*

Ipconfig Switches

The Ipconfig command is of particular use on systems running DHCP, allowing users to determine which TCP/IP configuration values have been configured by DHCP. Table 10.2 explains the switches used with the Ipconfig command.

Table 10.2 *Ipconfig Command-Line Switches*

Switch	Effect
/all	Produces a detailed configuration report for all interfaces
/flushdns	Removes all entries from the DNS name cache
/registerdns	The DNS domain name for client resolutions
/displaydns	Displays the contents of the DNS resolver cache
/release <adapter>	Releases the IP address for a specified interface
/renew <adapter>	Renews the IP address for a specified interface
/showclassid <adapter>	Displays all the DHCP class IDs allowed for the adapter specified
/setclassid <adapter> <classID to set>	Changes the DHCP class ID for the adapter specified
/?	Displays the items in this table

NOTE

Output can be redirected to a file and pasted into other documents.

- **To verify, release, or renew a client address lease**

1. At a DHCP-enabled client computer running Windows 2000, open a command prompt.

2. Use the Ipconfig command-line utility to verify, release, or renew the lease of the client with a DHCP server, as follows:

   To verify the current DHCP and TCP/IP configuration, type **ipconfig /all**.

   To release a DHCP client lease, type **ipconfig /release**.

   To renew a DHCP client lease, type **ipconfig /renew**.

The Ipconfig utility is also supported for use in Windows NT. For Windows 95 and Windows 98 clients, use Winipcfg, the Windows IP configuration program, to perform these same tasks. To run Winipcfg on supporting clients, type **winipcfg** at either an MS-DOS command prompt or in the Run command window. When using Winipcfg to release or renew leases, click Release or Renew to perform these respective tasks.

DHCP Relay Agent

A relay agent is a small program that relays DHCP/BOOTP messages between clients and servers on different subnets. The DHCP Relay Agent component provided with the Windows 2000 router is a BOOTP relay agent that relays DHCP messages between DHCP clients and DHCP servers on different IP networks. For each IP network segment that contains DHCP clients, either a DHCP server or a computer acting as a DHCP relay agent is required.

- **To add the DHCP Relay Agent**

1. Click Start, point to Programs, point to Administrative Tools, then click Routing And Remote Access.

2. In the console tree, click Server name\IP Routing\General.

3. Right-click General, then click New Routing Protocol.

4. In the Select Routing Protocol dialog box, click DHCP Relay Agent, then click OK.

Lesson Summary

DHCP was developed to solve configuration problems by centralizing IP configuration information for allocation to clients. DHCP uses a four-phase process to configure a DHCP client. The phases are, in order: lease discover, lease offer, lease request, and lease acknowledgment. In addition to verifying a computer's IP configuration, you can use the Ipconfig utility to renew options, lease time, and relinquish a lease.

[Previous] [Next]

Lesson 2: Configuring DHCP

In this lesson, you will learn how to configure DHCP on a Windows 2000-based server.

After this lesson, you will be able to

- Identify the benefits of using DHCP on a network
- Configure a DHCP server and clients

Estimated lesson time: 10 minutes

Using DHCP on a Network

Configuring DHCP servers for a network provides the following benefits:

- The administrator can assign and specify global and subnet-specific TCP/IP parameters centrally for use throughout the entire network.
- Client computers do not require manual TCP/IP configuration.

  When a client computer moves between subnets, its old IP address is freed for reuse. The client reconfigures its TCP/IP settings automatically when the computer is restarted in its new location.
- Most routers can forward DHCP and BOOTP configuration requests, so DHCP servers are not required on every subnet in the network.

How Clients Use DHCP Servers

A computer running Windows 2000 becomes a DHCP client if Obtain An IP Address is selected in its TCP/IP properties, as illustrated in Figure 10.5.

When a client computer is set to use DHCP, it accepts a lease offer and can receive from the server the following:

- Temporary use of an IP address known to be valid for the network it is joining
- Additional TCP/IP configuration parameters for the client to use in the form of options data

In addition, if conflict detection is configured, the DHCP server attempts to ping each available address in the scope prior to presenting the address in a lease offer to a client. This ensures that each IP address offered to clients is not already in use by another non-DHCP computer that uses manual TCP/IP configuration. Scopes are discussed in more detail later in this lesson.

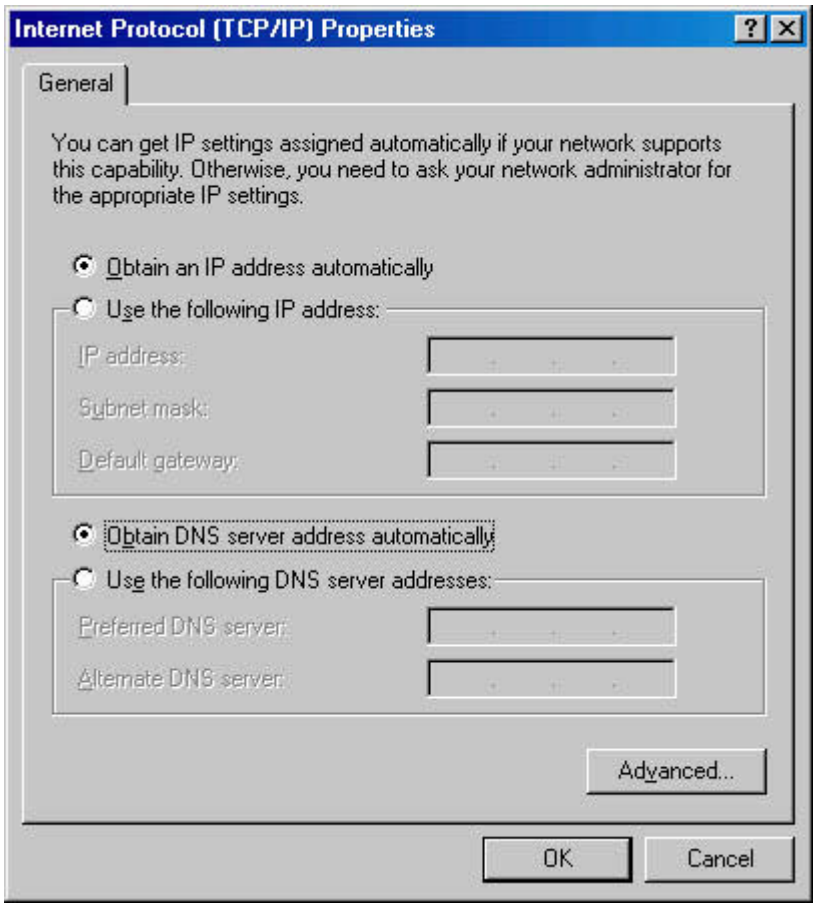

Figure 10.5 *Setting a client to obtain an IP address from a DHCP server*

How DHCP Servers Provide Optional Data

In addition to an IP address, DHCP servers can be configured to provide optional data to fully configure TCP/IP for clients. Some of the most common DHCP option types configured and distributed by the DHCP server during leases include

- Default gateways (routers), which are used to connect a network segment to other network segments
- Other optional configuration parameters to assign to DHCP clients, such as IP addresses for the DNS servers or WINS servers that the client can use in resolving network host names

Installing and Configuring a DHCP Server

The DHCP Server service must be running to communicate with DHCP clients. Once DHCP Server is installed and started, several options must be configured. The following are the general steps for installing and configuring DHCP:

- Install the Microsoft DHCP Server service.
- Authorize the DHCP server.
- A scope or pool of valid IP addresses must be configured before a DHCP server can lease IP addresses to DHCP clients.

- Global scope and client scope options can be configured for a particular DHCP client.

- The DHCP server can be configured to always assign the same IP address to the same DHCP client.

Authorizing a DHCP Server

When configured correctly and authorized for use on a network, DHCP servers provide a useful and intended administrative service. However, when a misconfigured or unauthorized DHCP server is introduced into a network, it can cause problems. For example, if an unauthorized DHCP server starts, it might begin either leasing incorrect IP addresses to clients or negatively acknowledging DHCP clients, attempting to renew current address leases. Either of these configurations can produce further problems for DHCP-enabled clients. For example, clients that obtain a configuration lease from the unauthorized server can fail to locate valid domain controllers, preventing clients from successfully logging on to the network.

To avoid these problems in Windows 2000, servers are verified as legal in the network before they can service clients. This avoids most of the accidental damage caused by running DHCP servers with incorrect configurations or correct configurations on the wrong network.

How DHCP Servers Are Authorized

The process of authorizing DHCP servers is useful or needed for DHCP servers running Windows 2000 Server. For the directory authorization process to work properly, it is assumed and necessary that the first DHCP server introduced onto your network participate in the Active Directory service. This requires that the server be installed as either a domain controller or a member server. When you are either planning for or actively deploying Active Directory services, it is important that you do not elect to install your first DHCP server computer as a stand-alone server. Windows 2000 Server provides some integrated security support for networks that use Active Directory. This avoids most of the accidental damage caused by running DHCP servers with wrong configurations or on the wrong networks.

The authorization process for DHCP server computers in Active Directory depends on the installed role of the server on your network. For Windows 2000 Server (as in earlier versions) there are three roles or server types for which each server computer can be installed:

1. **Domain controller.** The computer keeps and maintains a copy of the Active Directory service database and provides secure account management for domain member users and computers.

2. **Member server.** The computer is not operating as a domain controller but has joined a domain in which it has a membership account in the Active Directory service database.

3. **Stand-alone server.** The computer is not operating as a domain controller or a member server in a domain. Instead, the server computer is made known to the network through a specified workgroup name, which can be shared by other computers, but is used only for browsing purposes and not to provide secured logon access to shared domain resources.

If you deploy Active Directory, all computers operating as DHCP servers must be either domain controllers or domain member servers before they can be authorized in the directory service and provide DHCP service to clients.

- **To authorize a computer as a DHCP server in Active Directory**

1. Log on to the network using either an account that has enterprise administrative privileges or one that has been delegated authority to authorize DHCP servers for your enterprise.

   In most cases, it is simplest to log on to the network from the computer where you want to authorize the new DHCP server. This ensures that other TCP/IP configuration of the authorized computer has been set up correctly prior to authorization. Typically, you can use an account that has membership in the Enterprise Administrators group. The account you use must allow you to have Full control rights to the NetServices container object as it is stored in the enterprise root of the Active Directory service.

2. Install the DHCP service on this computer if necessary.

3. Click Start, point to Programs, point to Administrative Tools, then click DHCP.

4. On the Action menu, click Manage Authorized Servers, as illustrated in Figure 10.6.

   The Manage Authorized Servers dialog box appears.

5. Click Authorize.

6. When prompted, type the name or IP address of the DHCP server to be authorized, then click OK.

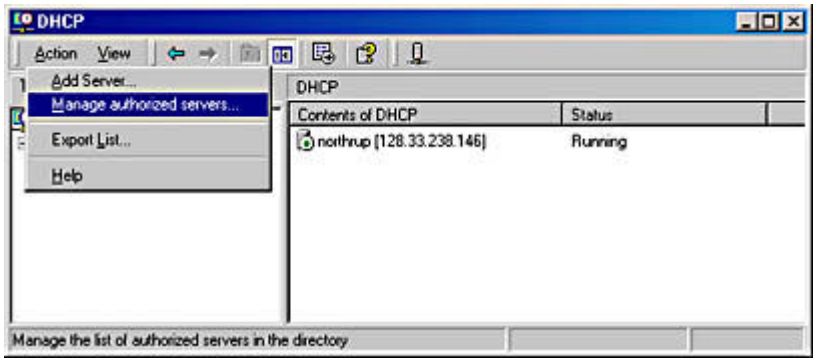

Figure 10.6 *Authorizing a DHCP server*

Protecting Against Unauthorized DHCP Servers

Active Directory is now used to store records of authorized DHCP servers. When a DHCP server comes up, the directory can now be used to verify the status of that server. If that server is unauthorized, no response is returned to DHCP requests. A network manager with the proper access rights has to respond. The domain administrator can assign access to the DHCP folder holding configuration data to allow only authorized personnel to add DHCP servers to the approved list.

The list of authorized servers can be created in Active Directory through the DHCP snap-in. When it first comes up, the DHCP server tries to find out if it is part of the directory domain. If it is, it tries to contact the directory to see if it is in the list of authorized servers. If it succeeds, it sends out DHCPINFORM to find out if there are other directory services running and makes sure that it is valid in others as well. If it cannot connect to the directory, it assumes that it is not authorized and does not respond to client requests. Likewise, if it does reach the directory but does not find itself in the authorized list, it does not respond to clients. If it does find itself in the authorized list, it starts to service client requests.

Creating a DHCP Scope

Before a DHCP server can lease an address to DHCP clients, you must create a scope. A scope is a pool of valid IP addresses available for lease to DHCP clients. After you have installed the DHCP service and it is running, the next step is to create a scope.

When creating a DHCP scope, consider the following points:

- You must create at least one scope for every DHCP server.
- You must exclude static IP addresses from the scope.
- You can create multiple scopes on a DHCP server to centralize administration and to assign IP addresses specific to a subnet. You can assign only one scope to a specific subnet.
- DHCP servers do not share scope information. As a result, when you create scopes on multiple DHCP servers, ensure that the same IP addresses do not exist in more than one scope to prevent duplicate IP addressing.
- Before you create a scope, determine starting and ending IP addresses to be used within it.

  Depending on the starting and ending IP addresses for your scope, the DHCP console suggests a default subnet mask useful for most networks. If you know a different subnet mask is required for your network, you can modify the value as needed.

- **To create a new scope**

1. Click Start, point to Programs, point to Administrative Tools, then click DHCP.
2. In the console tree, click the applicable DHCP server.
3. On the Action menu, click New Scope.
4. Follow the instructions in the New Scope Wizard.

   When you finish creating a new scope, you might need to complete additional tasks, such as activating the scope for use or assigning scope options.

After Scopes Are Added

After you define a scope, you can additionally configure the scope by performing the following tasks:

- **Set additional exclusion ranges.** You can exclude any other IP addresses that must not be leased to DHCP clients. You should use exclusions for all devices that must be statically configured. The excluded ranges should include all IP addresses that you assigned manually to other DHCP servers, non-DHCP clients, diskless workstations, or Routing and Remote Access and Point-to-Point (PPP) clients.

- **Create reservations.** You can choose to reserve some IP addresses for permanent lease assignment to specified computers or devices on your network. You should make reservations only for devices that are DHCP-enabled and that must be reserved for specific purposes on your network (such as print servers).

  If you are reserving an IP address for a new client or an address that is different from its current one, you should verify that the address has not already been leased by the DHCP server. Reserving an IP address in a scope does not automatically force a client currently using that address to stop using it. If the address is already in use, the client using the address must first release it by issuing a DHCP release message. To make this happen on a system running Windows 2000, at the command prompt type **ipconfig /release**. Reserving an IP address at the DHCP server also does not force the new client for which the reservation is made to immediately move to that address. In this case, too, the client must first issue a DHCP request message. To make this happen on a system running Windows 2000, at the command prompt type **ipconfig /renew**.

- **Adjust the length of lease durations.** You can modify the lease duration to be used for assigning IP address leases. The default lease duration is eight days. For most local area networks (LANs), the default value is acceptable but can be further increased if computers seldom move or change locations. Infinite lease times can also be set, but should be used with caution. For information about circumstances under which modifying this setting is most useful, see Managing Leases.

- **Configure options and classes to be used with the scope.** To provide full configuration for clients, DHCP options need to be configured and enabled for the scope. For more advanced discrete management of scope clients, you can add or enable user- or vendor-defined option classes.

Table 10.3 describes some of the available options in the Configure DHCP Options: Scope Properties dialog box and includes all of the options supported by Microsoft DHCP clients.

Table 10.3 *DHCP Scope Configuration Options*

Option	Description
003 Router	Specifies the IP address of a router, such as the default gateway address. If the client has a locally defined default gateway, that configuration takes precedence over the DHCP option.
006 DNS	Specifies the IP address of a DNS server.

Servers	
015 DNS Domain Name	The DNS domain name for client resolutions.
044 WINS/NBNS servers	The IP address of a WINS server available to clients. If a WINS server address is configured manually on a client, that configuration overrides the values configured for this option.
046 WINS/NBT node type	Specifies the type of NetBIOS over TCP/IP name resolution to be used by the client. Options are: 1 = B-node (broadcast); 2 = P-node (peer); 4 = M-node (mixed); 8 = H-node (hybrid)
044 WINS/NBNS servers	Specifies the IP address of a WINS server available to clients. If a WINS server address is manually configured on a client, that configuration overrides the values configured for this option.
047 NetBIOS Scope ID	Specifies the local NetBIOS scope ID. NetBIOS over TCP/IP will communicate only with other NetBIOS hosts using the same scope ID.

Implementing Multiple DHCP Servers

If your internetwork requires multiple DHCP servers, it is necessary to create a unique scope for each subnet. To ensure that clients can lease IP addresses in the event of a server failure, it is important to have multiple scopes for each subnet distributed among the DHCP servers in the internetwork. For example:

- Each DHCP server should have a scope containing approximately 75 percent of the available IP addresses for the local subnet.
- Each DHCP server should have a scope for each remote subnet containing approximately 25 percent of the available IP addresses for a subnet.

When a client's DHCP server is unavailable, the client can still receive an address lease from another DHCP server on a different subnet, assuming the router is a DHCP relay agent.

As illustrated in Figure 10.7, Server A has a scope for the local subnet with an IP address range of 131.107.4.20 through 131.107.4.150, and Server B has a scope with an IP address range of 131.107.3.20 through 131.107.3.150. Each server can lease IP addresses to clients on its own subnet.

Additionally, each server has a scope containing a small range of IP addresses for the remote subnet. For example, Server A has a scope for Subnet 2 with the IP address range of 131.107.3.151 through 131.107.3.200. Server B has a scope for Subnet 1 with the IP address range of 131.107.4.151 through 131.107.4.200. When a client on Subnet 1 is unable to lease an address from Server A, it can lease an address for its subnet from Server B, and vice versa.

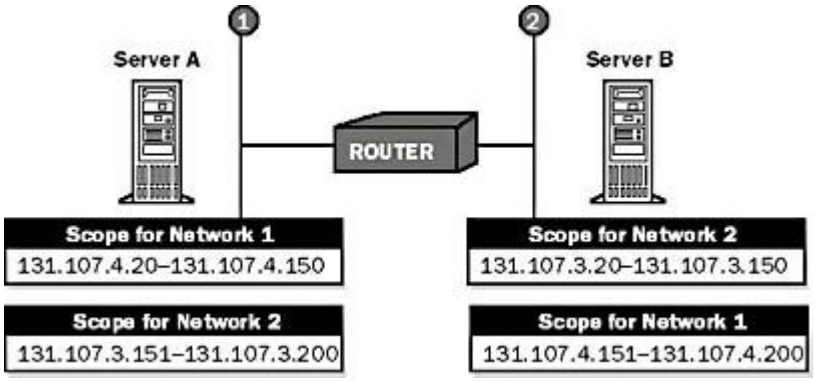

Figure 10.7 *Scope and IP address ranges for Server A and Server B*

Lesson Summary

A scope is a range of IP addresses that are available to be leased or assigned to clients. Multiple scopes and separate scopes for each subnet can be created to allow DHCP clients to obtain a valid IP address from any DHCP server. To implement DHCP, software is required on both the client and the server. Every DHCP server requires at least one scope.

[Previous] [Next]

Lesson 3: Integrating DHCP with Naming Services

With Windows 2000, a DHCP server can enable dynamic updates in the DNS name space for any of its clients that support these updates. Scope clients can then use DNS dynamic update protocol to update their host name-to-address mapping information (which is stored in zones on the DNS server) whenever changes occur to their DHCP-assigned address. In this lesson, you will learn how to integrate DHCP with DNS.

After this lesson, you will be able to

- Integrate DNS and DHCP
- Describe how Dynamic DNS updates work
- Identify how DHCP client updates are typically handled

Estimated lesson time: 25 minutes

DNS and DHCP

Although DHCP provides a powerful mechanism for automatically configuring client IP addresses, until recently DHCP did not notify the DNS service to update the DNS records on the client—specifically, updating the client name to an IP address, and IP address-to-name mappings maintained by a DNS server. Without a way for DHCP to interact with DNS, the information maintained by DNS for a DHCP client may be incorrect. For example, a client may acquire its IP address from a DHCP server, but the

DNS records would not reflect the IP address acquired or provide a mapping from the new IP address to the computer name (fully qualified domain name [FQDN]).

Registering for Dynamic DNS Updates

In Windows 2000, DHCP servers and clients can register with DNS, if the server supports Dynamic DNS updates. The Windows 2000 DNS service supports dynamic updates. A Windows 2000 DHCP server can register with a DNS server and update pointer (PTR) and address (A) resource records (RRs) on behalf of its DHCP- enabled clients using the Dynamic DNS update protocol. The ability to register both A and PTR type records lets a DHCP server act as a proxy for clients using Windows 95 and Windows NT 4.0 for the purpose of DNS registration. DHCP servers can differentiate between Windows 2000 and other clients. An additional DHCP option code (Option Code 81) enables the return of a client's FQDN to the DHCP server. If implemented, the DHCP server can dynamically update DNS to modify an individual computer's RRs with a DNS server using the dynamic update protocol. This DHCP option permits the DHCP server the following possible interactions for processing DNS information on behalf of DHCP clients that include Option Code 81 in the DHCP request message they send to the server:

- The DHCP server always registers the DHCP client for both the forward (A-type records) and reverse lookups (PTR-type records) with DNS.
- The DHCP server never registers the name-to-address (A-type records) mapping information for DHCP clients.
- The DHCP server registers the DHCP client for both forward (A-type records) and reverse lookups (PTR-type records) only when requested to by the client.

DHCP and static DNS service are not compatible for keeping name-to-address mapping information synchronized. This might cause problems with using DHCP and DNS together on a network if you are using older, static DNS servers, which are incapable of interacting dynamically when DHCP client configurations change.

- **To avoid failed DNS lookups for DHCP-registered clients when static DNS service is in effect**

1. If WINS servers are used on the network, enable WINS lookup for DHCP clients that use NetBIOS.
2. Assign IP address reservations with an infinite lease duration for DHCP clients that use DNS only and do not support NetBIOS.
3. Wherever possible, upgrade or replace older, static-based DNS servers with DNS servers supporting updates. Dynamic updates are supported by the Microsoft DNS, included in Windows 2000.

Additional Recommendations

When using DNS and WINS together, consider the following options for interoperation:

- If a large percentage of clients use NetBIOS and you are using DNS, consider using WINS lookup on your DNS servers. If WINS lookup is enabled on the

Microsoft DNS service, WINS is used for final resolution of any names that are not found using DNS resolution. The WINS forward lookup and WINS-R reverse lookup records are supported only by DNS. If you use servers on your network that do not support DNS, use DNS Manager to ensure that these WINS records are not propagated to DNS servers that do not support WINS lookup.

- If you have a large percentage of computers running Windows 2000 on your network, consider creating a pure DNS environment. This involves developing a migration plan to upgrade older WINS clients to Windows 2000. Support issues involving network name service are simplified by using a single naming and resource locator service (such as WINS and DNS) on your network.

Windows DHCP Clients and DNS Dynamic Update Protocol

In Windows 2000 Server, the DHCP Server service provides default support to register and update information for legacy DHCP clients in DNS zones. Legacy clients typically include other Microsoft TCP/IP client computers that were released prior to Windows 2000. The DNS/DHCP integration provided in Windows 2000 Server enables a DHCP client that is unable to dynamically update DNS RRs directly to have this information updated in DNS forward and reverse lookup zones by the DHCP server.

- **To allow dynamic updates for DHCP clients that do not support Dynamic DNS updates**

1. Click Start, point to Programs, point to Administrative Tools, then click DNS.
2. In the console tree, click the applicable zone.
3. On the Action menu, click Properties.
4. In the DNS Property tab, select Enable Updates For DNS Clients That Do Not Support Dynamic Update.
5. Select Only Secure Updates If Your Zone Type Is Active Directory-Integrated.

DHCP clients running Windows 2000 and earlier versions of Windows interact differently when performing the DHCP/DNS interactions previously described. The following sections explain how this process varies in different cases.

DHCP/DNS Update Interaction for Windows 2000 DHCP Clients

Windows 2000 DHCP clients interact with DNS dynamic update protocol as follows:

1. The client initiates a DHCP request message (DHCPREQUEST) to the server.
2. The server returns a DHCP acknowledgment message (DHCPACK) to the client, granting an IP address lease.
3. By default, the client sends a DNS update request to the DNS server for its own forward lookup record, a host (A) RR.

   Alternately, the server can perform this update to the DNS server on behalf of

the client if both the client and its configuration are modified accordingly.

4. The server sends updates for the DHCP client's reverse lookup record—a PTR RR—using the process defined by the DNS dynamic update protocol.

This process is illustrated in Figure 10.8.

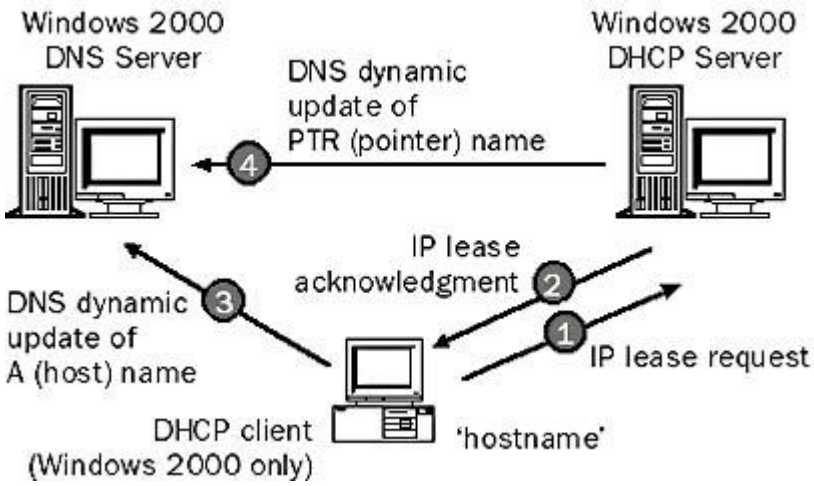

Figure 10.8 *A DHCP client interacting with the DNS dynamic update protocol*

DHCP/DNS Update Interaction for DHCP Clients Prior to Windows 2000

Earlier versions of Windows DHCP clients do not support the DNS dynamic update process directly and therefore cannot directly interact with the DNS server. For these DHCP clients, updates are typically handled as follows:

1. The client initiates a DHCP request message (DHCPREQUEST) to the server.

2. The server returns a DHCP acknowledgment message (DHCPACK) to the client, granting an IP address lease.

3. The server then sends updates to the DNS server for the client's forward lookup record, which is a host (A) RR.

4. The server also sends updates for the client's reverse lookup record, which is a PTR RR.

This process is illustrated in Figure 10.9.

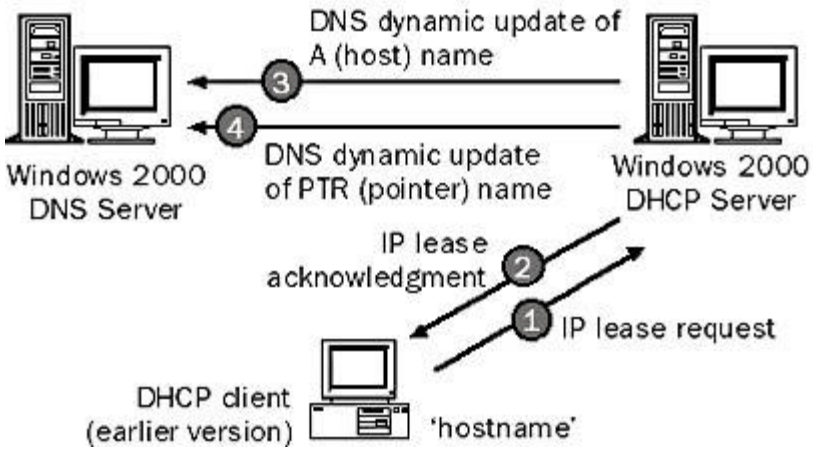

Figure 10.9 *DHCP/DNS interaction with older Windows clients*

Lesson Summary

With Windows 2000, a DHCP server can enable dynamic updates in the DNS name space for any of its clients that support these updates. With dynamic update, the primary server for a zone can also be configured to support updates that are initiated by another computer or device that supports dynamic update. For example, it can receive updates from workstations registering A and PTR RRs, or from DHCP servers.

[Previous] [Next]

Lesson 4: Using DHCP with Active Directory

Microsoft DHCP provides integration with the Active Directory service and DNS service, enhanced monitoring and statistical reporting for DHCP servers, vendor-specific options and user-class support, multicast address allocation, and rogue DHCP server detection.

After this lesson, you will be able to

- Describe how IP address and naming management is managed through DHCP and Active Directory integration
- Describe how DHCP servers are authorized

Estimated lesson time: 15 minutes

Windows 2000 Integrated IP Management

Windows 2000 Server naming and address services offer the flexibility to manage networks more easily and interoperate with other address and naming systems. As with Windows NT Server 4.0, Windows 2000 Server provides DHCP, DNS, and WINS services to continue to simplify address assignment and name resolution. New with Windows 2000 Server is support for Dynamic DNS, Active Directory integration of DHCP and DNS, and a DHCP relay agent.

Address Assignment and Naming Services

IP address and naming management is simplified through Active Directory integration. Customers can choose to use Active Directory to replicate and synchronize DNS naming throughout the corporate network. This eliminates the need to maintain a separate replication service for DNS. Integrated DHCP and Dynamic DNS services then utilize this directory-registered information to provide address assignment and naming services. As DHCP allocates addresses, DNS and Active Directory are dynamically updated. This lets administrators reassign IP addresses for end systems, and name resolution is updated automatically so they can be located easily.

Support for Legacy Servers

Interoperability with other DHCP and DNS services helps preserve investment in existing services. Customers have the option to use legacy IP address and naming management systems using the Windows 2000 Server DHCP, DHCP relay agent, and/or the DNS service. Standard zone transfer and referral support ensures that the Windows 2000 Server DNS interoperates with other DNS servers for enterprise and Internet address resolution. This lets customers use Active Directory integrated services for their network while maintaining interoperability with Internet and other corporate DNS systems. For example, a company can deploy Active Directory-integrated DNS and DHCP in a core part of its network while interoperating with legacy DNS servers. Over time, the Active Directory-based IP management infrastructure can be expanded while interoperability with external DNS services is preserved.

Windows 2000 DHCP is also dynamically integrated with Windows 2000 DNS in support of Active Directory. Earlier versions of DNS do not offer this support, and you should consider upgrading if you plan to deploy Active Directory or want to use network load balancing.

Rogue DHCP Server Detection Feature

The Windows 2000 DHCP service provides a rogue DHCP server detection feature. This prevents rogue (unauthorized) DHCP servers from joining an existing DHCP network in which Windows 2000 Server and Active Directory are deployed. A DHCP server object is created in Active Directory, which lists the IP addresses of servers that are authorized to provide DHCP services to the network. When a DHCP server attempts to start on the network, Active Directory is queried and the server computer's IP address is compared to the list of authorized DHCP servers. If a match is found, the server computer is authorized as a DHCP server and is allowed to complete the system startup. If a match is not found, the server is identified as rogue, and the DHCP service is automatically shut down.

Lesson Summary

IP address and naming management is simplified through Active Directory integration. As DHCP allocates addresses, DNS and Active Directory are dynamically updated. Interoperability with other DHCP and DNS services helps preserve investment in existing services because you can use legacy IP address and naming management systems with Windows 2000 Server DHCP servers. The authorization process for DHCP server computers in Active Directory depends on whether the server is a domain controller, member server, or stand-alone server. In addition, Active Directory is now

used to store records of authorized DHCP servers to protect against unauthorized DHCP servers. The list of authorized servers can be created in the Active Directory through the DHCP snap-in.

[Previous] [Next]

Lesson 5: Troubleshooting DHCP

The most common DHCP client problem is a failure to obtain an IP address or other configuration parameters from the DHCP server during startup. The most common DHCP server problems are the inability to start the server on the network in a Windows 2000 or Active Directory domain environment and the failure of clients to obtain configuration from a working server. In this lesson, you will learn how to troubleshoot DHCP clients and DHCP servers.

After this lesson, you will be able to

- Identify and solve DHCP client problems
- Identify and solve DHCP server problems

Estimated lesson time: 35 minutes

Preventing DHCP Problems

Many DHCP problems involve incorrect or missing configuration details. To help prevent the most common types of problems, you should do the following:

- **Use the 75/25 design rule for balancing scope distribution of addresses where multiple DHCP servers are deployed to service the same scope.** Using more than one DHCP server on the same subnet provides increased fault tolerance for servicing DHCP clients located on it. With two DHCP servers, if one server is unavailable, the other server can take its place and continue to lease new addresses or renew existing clients.

- **Use superscopes for multiple DHCP servers on each subnet in a LAN environment.** A superscope allows a DHCP server to provide leases from more than one scope to clients on a single physical network. When started, each DHCP client broadcasts a DHCP discover message (DHCPDISCOVER) to its local subnet to attempt to find a DHCP server. Because DHCP clients use broadcasts during their initial startup, you cannot predict which server will respond to a client's DHCP discover request if more than one DHCP server is active on the same subnet.

- **Deactivate scopes only when removing a scope permanently from service.** Once you activate a scope, it should not be deactivated until you are ready to retire the scope and its included range of addresses from use on your network. Once a scope is deactivated, the DHCP server no longer accepts those scope addresses as valid addresses.

- **Use server-side conflict detection on DHCP servers only when it is needed.** Conflict detection can be used by either DHCP servers or clients to determine

whether an IP address is already in use on the network before leasing or using the address.

- **Reservations should be created on all DHCP servers that can potentially service the reserved client.** You can use a client reservation to ensure that a DHCP client computer always receives lease of the same IP address at its startup. If you have more than one DHCP server reachable by a reserved client, add the reservation at each of your other DHCP servers.

- **For server performance, remember that DHCP is disk-intensive and purchase hardware with optimal disk performance characteristics.** DHCP causes frequent and intensive activity on server hard disks. To provide the best performance, consider RAID 0 or RAID 5 solutions when purchasing hardware for your server computer.

- **Keep audit logging enabled for use in troubleshooting.** By default, the DHCP service enables audit logging of service-related events. With Windows 2000 Server, audit logging provides for a long-term service monitoring tool that makes limited and safe use of server disk resources.

- **Integrate DHCP with other services, such as WINS and DNS.** WINS and DNS can both be used for registering dynamic name-to-address mappings on your network. To provide name resolution services, you must plan for interoperability of DHCP with these services. Most network administrators implementing DHCP also plan a strategy for implementing DNS and WINS servers.

- **Use the appropriate number of DHCP servers for the number of DHCP-enabled clients on your network.** In a small LAN (for example, one physical subnet not using routers), a single DHCP server can serve all DHCP-enabled clients. For routed networks, the number of servers needed increases, depending on several factors, including the number of DHCP-enabled clients, the transmission speed between network segments, the speed of network links, the IP address class of the network, and whether DHCP service is used throughout the enterprise network or only on selected physical networks.

Troubleshooting DHCP Clients

Most DHCP-related problems start as failed IP configuration at a client, so it is a good practice to start there. After you have determined that a DHCP-related problem does not originate at the client, check the system event log and DHCP server audit logs for possible clues. When the DHCP service does not start, these logs generally explain the source of the service failure or shutdown. Furthermore, you can use the Ipconfig TCP/IP utility at the command prompt to get information about the configured TCP/IP parameters on local or remote computers on the network.

The following sections describe common symptoms for DHCP client problems. When a client fails to obtain configuration, you can use this information to quickly identify the source of the problem.

Invalid IP Address Configuration

If a DHCP client does not have an IP address configured or has an IP address

configured as 168.254.x.x, that means that the client was not able to contact a DHCP server and obtain an IP address lease. This is either because of a network hardware failure or because the DHCP server is unavailable. If this occurs, you should verify that the client computer has a valid, functioning network connection. First, check that related client hardware devices (cables and network adapters) are working properly at the client.

Autoconfiguration Problems on the Current Network

If a DHCP client has an autoconfigured IP address that is incorrect for its current network, this means that the Windows 2000 or Windows 98 DHCP client could not find a DHCP server and has used the APIPA feature to configure its IP address. In some larger networks, disabling this feature is desirable for network administration. APIPA generates an IP address in the form of 169.254.x.y (where x.y is a unique identifier on the network that the client generates) and a subnet mask of 255.255.0.0. Note that Microsoft has reserved IP addresses from 169.254.0.1 through 169.254.255.254 and uses this range to support APIPA.

- **To fix an invalid autoconfigured IP address for your network**

1. First, use the PING command to test connectivity from the client to the server. Next, verify or manually attempt to renew the client lease. Depending on your network requirements, it might be necessary to disable APIPA at the client.

2. If the client hardware appears to be functioning properly, check that the DHCP server is available on the network by pinging it from another computer on the same network as the affected DHCP client. Furthermore, you can try releasing or renewing the client's address lease, and check the TCP/IP configuration settings on automatic addressing.

Missing Configuration Details

If a DHCP client is missing configuration details, the client might be missing DHCP options in its leased configuration, either because the DHCP server is not configured to distribute them or the client does not support the options distributed by the server. If this occurs on Microsoft DHCP clients, verify that the most commonly used and supported options have been configured at either the server, scope, client, or class level of option assignment. Check the DHCP option settings.

Sometimes a client has the full and correct set of DHCP options assigned, but its network configuration does not appear to be working correctly. If the DHCP server is configured with an incorrect DHCP router option (Option Code 3) for the Windows 98 or earlier client's default gateway address, you can

1. Change the IP address list for the router (default gateway) option at the applicable DHCP scope and server.

2. Set the correct value in the Scope Options tab of the Scope Properties dialog box.

   In rare instances, you might have to configure the DHCP client to use a specialized list of routers different from other scope clients. In such cases, you can add a reservation and configure the router option list specifically for the reserved client.

Clients running Windows NT or Windows 2000 do not use the incorrect address beause they support the dead gateway detection feature. This feature of the Windows 2000 TCP/IP protocol changes the default gateway to the next default gateway in the list of configured default gateways when a specific number of connections retransmits segments.

DHCP Servers Do Not Provide IP Addresses

If DHCP clients are unable to get IP addresses from the server, one of the following situations can cause this problem:

- **The IP address of the DHCP server was changed and now DHCP clients cannot get IP addresses.** A DHCP server can only service requests for a scope that has a network ID that is the same as the network ID of its IP address. Make sure that the DHCP server IP address falls in the same network range as the scope it is servicing. For example, a server with an IP address in the 192.168.0.0 network cannot assign addresses from scope 10.0.0.0 unless superscopes are used.

- **The DHCP clients are located across a router from the subnet where the DHCP server resides, and are unable to receive an address from the server.** A DHCP server can provide IP addresses to client computers on remote multiple subnets only if the router that separates them can act as a DHCP relay agent. Completing the following steps might correct this problem:

    1. Configure a BOOTP/DHCP relay agent on the client subnet (that is, the same physical network segment). The relay agent can be located on the router itself or on a Windows 2000 Server computer running the DHCP Relay service component.

    2. At the DHCP server, configure a scope to match the network address on the other side of the router where the affected clients are located.

    3. In the scope, make sure that the subnet mask is correct for the remote subnet.

    4. Do not include this scope (that is, the one for the remote subnet) in superscopes configured for use on the same local subnet or segment where the DHCP server resides.

- **Multiple DHCP servers exist on the same LAN.** Make sure that you do not configure multiple DHCP servers on the same LAN with overlapping scopes. You might want to rule out the possibility that one of the DHCP servers in question is a Small Business Server (SBS) computer. By design, the DHCP service, when running under SBS, automatically stops when it detects another DHCP server on the LAN.

Troubleshooting DHCP Servers

When a server fails to provide leases to its clients, the failure most often is discovered by clients in one of three ways:

1. The client might be configured to use an IP address not provided by the server.

2. The server sends a negative response back to the client, and the client displays an error message or popup indicating that a DHCP server could not be found.

3. The server leases the client an address but the client appears to have other network configuration-based problems, such as the inability to register or resolve DNS or NetBIOS names, or to perceive computers beyond its subnet.

The first troubleshooting task is to make sure that the DHCP services are running. This can be verified by opening the DHCP service console to view service status, or by opening Services And Applications under Computer Manager. If the appropriate service is not started, start the service. In rare circumstances, a DHCP server cannot start, or a Stop error might occur. If the DHCP server is stopped, complete the following procedure to restart it:

- **To restart a DHCP server that is stopped**

1. Start Windows 2000 Server, and log on as an administrator.

2. At the command prompt, type **net start dhcpserver**, then press Enter.

   NOTE

   Use Event Viewer in Administrative Tools to find the possible source of problems with DHCP services.

DHCP Relay Agent Service Is Installed But Not Working

The DHCP Relay Agent service is running on the same computer as the DHCP service. Because both services listen for and respond to BOOTP and DHCP messages sent using UDP ports 67 and 68, neither service works reliably if both are installed on the same computer. To solve this problem, install the DHCP service and the DHCP Relay Agent component on separate computers.

DHCP Console Incorrectly Reports Lease Expirations

When the DHCP console displays the lease expiration time for reserved clients for a scope, it indicates one of the following:

- If the scope lease time is set to an infinite lease time, the reserved client's lease is also shown as infinite.

- If the scope lease time is set to a finite length of time (such as eight days), the reserved client's lease uses this same lease time.

The lease term of a DHCP reserved client is determined by the lease assigned to the reservation. To create reserved clients with unlimited lease durations, create a scope with an unlimited lease duration and add reservations to that scope.

DHCP Server Uses Broadcast to Respond to All Client Messages

The DHCP server uses broadcast to respond to all client configuration request messages, regardless of how each DHCP client has set the broadcast bit flag. DHCP clients can set the broadcast flag (the first bit in the 16-bit flags field in the DHCP

message header) when sending DHCPDISCOVER messages to indicate to the DHCP server that broadcast to the limited broadcast address (255.255.255.255) should be used when replying to the client with a DHCPOFFER response.

By default, the DHCP server in Windows NT Server 3.51 and earlier versions ignored the broadcast flag in DHCPDISCOVER messages and broadcasted only DHCPOFFER replies. This behavior is implemented on the server to avoid problems that can result from clients not being able to receive or process a unicast response prior to being configured for TCP/IP.

Starting with Windows NT Server 4.0, the DHCP service still attempts to send all DHCP responses as IP broadcasts to the limited broadcast address, unless support for unicast responses is enabled by setting the value of the IgnoreBroadcastFlag registry entry to 1. The entry is located in:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DHCPServer\Parame
When set to 1, the broadcast flag in client requests is ignored, and all DHCPOFFER responses are broadcast from the server. When it is set to 0, the server transmission behavior (whether to broadcast or not) is determined by the setting of the broadcast bit flag in the client DHCPDISCOVER request. If this flag is set in the request, the server broadcasts its response to the limited local broadcast address. If this flag is not set in the request, the server unicasts its response directly to the client.

DHCP Server Fails to Issue Address Leases for a New Scope

A new scope has been added at the DHCP server for the purpose of renumbering the existing network. However, DHCP clients do not obtain leases from the newly defined scope. This situation is most common when you are attempting to renumber an existing IP network. For example, you might have obtained a registered class of IP addresses for your network, or you might be changing the address class to accommodate more computers or networks. In these situations, you want clients to obtain leases in the new scope instead of using the old scope to obtain or renew their leases. Once all clients are actively obtaining leases in the new scope, you intend to remove the existing scope.

When superscopes are not available or used, only a single DHCP scope can be active on the network at one time. If more than one scope is defined and activated on the DHCP server, only one scope is used to provide leases to clients. The active scope used for distributing leases is determined by whether the scope range of addresses contains the first IP address that is bound and assigned to the DHCP server's network adapter hardware. When additional secondary IP addresses are configured on a server using the Advanced TCP/IP Properties tab, these addresses have no effect on the DHCP server in determining scope selection or responding to configuration requests from DHCP clients on the network.

This problem can be solved in the following ways:

- Configure the DHCP server to use a superscope that includes the old scope and the new scope.

- Change the primary IP address (the address assigned in the TCP/IP Properties tab) on the DHCP server's network adapter to an IP address that is part of the same network as the new scope.

  For Windows NT Server 3.51, support for superscopes is not available. In this case, you must change the first IP address configured for the DHCP server's

network adapter to an address in the new scope range of addresses. If necessary, you can still maintain the prior address that was first assigned as an active IP address for the server computer by moving it to the list of multiple IP addresses maintained in the Advanced TCP/IP Properties tab.

Monitoring Server Performance

Because DHCP servers are of critical importance in most environments, monitoring the performance of servers can help in troubleshooting cases where server performance degradation occurs. For Windows 2000 Server, the DHCP service includes a set of performance counters that can be used to monitor various types of server activity. By default, these counters are available after the DHCP service is installed. To access these counters, you must use System Monitor (formerly Performance Monitor). The DHCP server counters can monitor

- All types of DHCP messages sent and received by the DHCP service
- The average amount of processing time spent by the DHCP server per message packet sent and received
- The number of message packets dropped because of internal delays on the DHCP server computer

Moving the DHCP Server Database

You may need to move a DHCP database to another computer. To do this, use the following procedure.

- **To move a DHCP database**

1. Stop the Microsoft DHCP service on the current computer.
2. Copy the \System32\Dhcp directory to the new computer that has been configured as a DHCP server.

   Make sure the new directory is under exactly the same drive letter and path as on the old computer. If you must copy the files to a different directory, copy DHCP.MDB, but do not copy the .log or .chk files.
3. Start the Microsoft DHCP service on the new computer. The service automatically starts using the .mdb and .log files copied from the old computer.

When you check DHCP Manager, the scope still exists because the registry holds the information on the address range of the scope, including a bitmap of the addresses in use. You need to reconcile the DHCP database to add database entries for the existing leases in the address bitmask. As clients renew, they are matched with these leases, and eventually the database is again complete.

- **To reconcile the DHCP database**

1. In DHCP Manager, on the Scope menu, click Active Leases.
2. In the Active Leases dialog box, click Reconcile.

Although it is not required, you can force DHCP clients to renew their leases in order to update the DHCP database as quickly as possible. To do so, type **ipconfig /renew** at the command prompt.

Lesson Summary

The most common DHCP client problem is a failure to obtain an IP address or other configuration parameters from the DHCP server during startup. The most common DHCP server problem is the inability to start the server on the network in a Windows 2000 or Active Directory domain environment. Most DHCP-related problems start as failed IP configuration at a client, so it is a good practice to start there.

[Previous] [Next]

Review

Answering the following questions will reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A, "Questions and Answers."

1. What is DHCP?
2. Describe the integration of DHCP with DNS.
3. What is a DHCP client?
4. What is IP autoconfiguration in Windows 2000?
5. Why is it important to plan an implementation of DHCP for a network?
6. What tool do you use to manage DHCP servers in Windows 2000?
7. What is the symptom of most DHCP-related problems?

Answers