Windows 2000 Server

Chapter 4 - Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard that reduces the complexity and administrative overhead of managing network client IP address configuration. Microsoft® Windows® 2000 Server provides the DHCP service, which enables a computer to function as a DHCP server and configure DHCP-enabled client computers on your network. DHCP runs on a server computer, enabling the automatic, centralized management of IP addresses and other TCP/IP configuration settings for your network's client computers. The Microsoft DHCP service also provides integration with the Active Directory™ directory service and Domain Name System (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.

Related Information in the Resource Kit

- For information about deploying DHCP with IP Security, see "Internet Protocol Security" in the *Microsoft Windows 2000 Server Resource Kit TCP/IP Core Networking Guide*.
- For more information about DHCP options, see "DHCP Options" in this book.
- For more information about DHCP message formats, see "DHCP Message Formats" in this book.
- For more information about setting DHCP registry settings, see the "Technical Reference to the Windows 2000 Registry" (Regentry.chm) on the Windows 2000 Resource Kit CD.

What Is DHCP?

DHCP simplifies the administrative management of IP address configuration by automating address configuration for network clients. The DHCP standard provides for the use of DHCP servers, which are defined as any computer running the DHCP service. The DHCP server automatically allocates IP addresses and related TCP/IP configuration settings to DHCP-enabled clients on the network.

Every device on a TCP/IP-based network must have a unique IP address in order to access the network and its resources. Without DHCP, IP configuration must be done manually for new computers, computers moving from one subnet to another, and computers removed from the network.

By deploying DHCP in a network, this entire process is automated and centrally managed. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it logs on to the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

The DHCP service for Microsoft Windows 2000 Server is based on Internet Engineering Task Force (IETF) standards. DHCP specifications are defined in Requests for Comments (RFCs) published by the IETF and other working groups. RFCs are an evolving series of reports, proposals for protocols, and protocol standards used by the Internet community. The following RFCs specify the core DHCP standards that Microsoft supports with its DHCP service:

- RFC 2131: Dynamic Host Configuration Protocol (obsoletes RFC 1541)
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

DHCP Terminology

Table 4.1 lists common DHCP terms that are used throughout this chapter.

Table 4.1 DHCP Terminology

Term	Description
DHCP server	Any computer running the Windows 2000 DHCP service.
DHCP client	Any computer that has DHCP settings enabled.
Scope	The full, consecutive range of possible IP addresses for a network. DHCP services can be offered to scopes, which typically define a single physical subnet on a network. DHCP servers primarily use scopes to manage network distribution and assignment of IP addresses and any related configuration parameters.
Superscope	An administrative grouping of scopes that are used to support multiple, logical IP subnets on the same physical subnet. Superscopes contain a list of member scopes (or child scopes) that can be activated as a collection.
Exclusion range	Ensures that any IP address listed in that range is not offered by the DHCP server to any DHCP clients.
Address pool	Available IP addresses form an address pool within the scope. Pooled addresses are available for dynamic assignment by the DHCP server to DHCP clients.
Lease	The length of time, specified by the DHCP server, a client computer can use a dynamically assigned IP address. When a lease is made to a client, the lease is considered active. Before the lease expires, the client renews its lease with the DHCP server. A lease becomes inactive when it either expires or is deleted by the server. The lease duration determines when the lease expires and how often the client needs to renew its lease with the DHCP server.
Reservation	Creates a permanent address lease assignment from the DHCP server to the client. Reservations ensure that a specified hardware device on the subnet can always use the same IP address. This is useful for computers such as remote access gateways, WINS, or DNS servers that must have a static IP address.
Option types	Other client configuration parameters a DHCP server can assign when offering an IP address lease to a client. Typically, these option types are enabled and configured for each scope. Most options are predefined through RFC 2132, but you can use DHCP Manager to define and add custom option types as needed.
Option class	A way for the DHCP server to further submanage option types provided to clients. Option classes can be configured on your DHCP servers to offer specialized client support. When an option class is added to the server, clients of that class can be provided class-specific option types for their configuration.

How DHCP Works

DHCP is based on a client/server model, as illustrated in Figure 4.1.

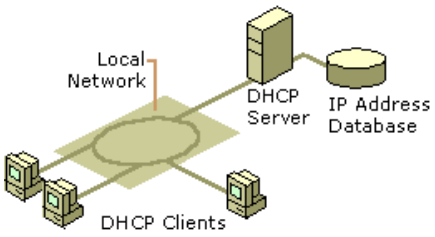


Figure 4.1 The Basic DHCP Model

The network administrator establishes one or more DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer. The DHCP server stores the configuration information in a database, which includes:

- Valid TCP/IP configuration parameters for all clients on the network.
- Valid IP addresses, maintained in a pool for assignment to clients, as well as reserved addresses for manual assignment.
- Duration of the lease offered by the server—the length of time for which the IP address can be used before a lease renewal is required.

A DHCP-enabled client, upon acceptance of a lease offer, receives:

- A valid IP address for the network it is joining.
- Additional TCP/IP configuration parameters, referred to as DHCP options.

Benefits of DHCP

Deploying DHCP on your enterprise network provides the following benefits:

- **Safe and reliable configuration.** DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, as well as address conflicts caused by a currently assigned IP address accidentally being reissued to another computer.
- **Reduced network administration.**
  - TCP/IP configuration is centralized and automated.
  - Network administrators can centrally define global and subnet-specific TCP/IP configurations.
  - Clients can be automatically assigned a full range of additional TCP/IP configuration values by using DHCP options.
  - Address changes for client configurations that must be updated frequently, such as remote access clients that move around constantly, can be made efficiently and automatically when the client restarts in its new location.
  - Most routers can forward DHCP configuration requests, eliminating the requirement of setting up a DHCP server on every subnet, unless there is another reason to do so.

New Features

The Windows 2000 DHCP service provides the following new features:

- Enhanced performance monitoring and server reporting capabilities

  New System Monitor counters have been added to Windows 2000 Server to specifically monitor DHCP server performance on your network. Additionally, DHCP Manager now provides enhanced server reporting through graphical display of current states for servers, scopes, and clients. For example, icons visually represent whether a server is disconnected, or if it has leased over 90 percent of its available addresses.

- Expanded support for multicast scopes and superscopes

  Multicast scopes now allow multicast-aware applications to lease Class D–type IP addresses (224.0.0.0 to 239.255.255.255) for participation in multicast groups.

- Support for user-specific and vendor-specific DHCP options

  This allows the separation and distribution of options for clients with similar or special configuration needs. For example, you might assign all DHCP-enabled clients on the same floor of your building to the same option class. You could use this class (configured with the same DHCP Class ID value) to distribute other option data during the lease process, overriding any scope or global default options.

- Integration of DHCP with DNS

  A DHCP server can enable dynamic updates in the DNS namespace for any DHCP clients that support these updates. Scope clients can then use DNS with dynamic updates to update their computer name–to–IP address mapping information whenever changes occur to their DHCP-assigned address.

- Rogue DHCP server detection

  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.

- Dynamic support for BOOTP clients

  Dynamic BOOTP is an extension of the BOOTP protocol, which permits the DHCP server to configure BOOTP clients without having to use explicit, fixed-address configuration. This feature reduces administration of large BOOTP networks by allowing automatic distribution of IP address much the same way that DHCP does.

- Read-only console access to DHCP Manager

  This feature provides a special-purpose local group, the DHCP Users group, which is automatically added when the DHCP service is installed. By adding members to this group, you can provide read-only access to information related to the DHCP service on the server computer. Using DHCP Manager, users in this group can view, but not modify, information and properties stored on the specified DHCP server.

DHCP Client Support

The term *client* is used to describe a networked computer that requests and uses the DHCP services offered by a DHCP server. Any Windows-based computer, or other network-enabled device that supports the ability to communicate with a DHCP server (in compliance with RFC 2132), can be configured as a DHCP client.

DHCP client support is provided for computers running under any of the following Microsoft operating systems:

- Microsoft® Windows NT® Workstation (all released versions)
- Microsoft® Windows NT® Server (all released versions)
- Microsoft® Windows® 98
- Microsoft® Windows® 95
- Microsoft® Windows® for Workgroups version 3.11 (with the Microsoft 32-bit TCP/IP VxD installed)
- Microsoft® Network Client version 3.0 for MS-DOS (with the real-mode TCP/IP driver installed)
- LAN Manager version 2.2c

IP Auto-Configuration

Windows 2000–based clients can automatically configure an IP address and subnet mask if a DHCP server is unavailable at system start time. This feature, Automatic Private IP Addressing (APIPA), 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 auto-configure 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 auto-configures 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 auto-configuration 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 auto-configured 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.

If the DHCP client had previously obtained a lease from a DHCP server:

1. If the client's lease is still valid (not expired) at system start time, the client will try to renew its lease.
2. If, during the renewal attempt, the client fails to locate any DHCP server, it will attempt to ping the default gateway listed in the lease, and proceed in one of the following ways:
   - If the ping is successful, the DHCP client assumes that it is still located on the same network where it obtained its current lease, and continue to use the lease. By default, the client will then attempt, in the background, to renew its lease when 50 percent of its assigned lease time has expired.
   - If the ping fails, the DHCP client assumes that it has been moved to a network where DHCP services are not available. The client then auto-configures its IP address as described previously. Once the client is auto-configured, every 5 minutes it attempts to locate a DHCP server and obtain a lease.

Local Storage

Microsoft DHCP supports local storage, allowing clients to store DHCP information on their own hard disks. Local storage is useful because when the client system starts, it first attempts to renew the lease of the same IP address. Local storage also means that a client can be shut down and restarted using its previously leased address and configuration, even if the DHCP server is unreachable or offline at the time the client computer is restarted. Local storage also enables the ability to perform IP auto-configuration.

DHCP Lease Process

A DHCP-enabled client obtains a lease for an IP address from a DHCP server. Before the lease expires, the DHCP server must renew the lease for the client or the client must obtain a new lease. Leases are retained in the DHCP server database approximately one day after expiration. This grace period protects a client's lease in case the client and server are in different time zones, their internal clocks are not synchronized, or the client is off the network when the lease expires.

DHCP Messages

Table 4.2 describes the DHCP messages exchanged between client and server. This is necessary before proceeding with an explanation of how the DHCP lease process works. For more information about each message field, see "DHCP Message Formats" in this book.

Table 4.2 DHCP Messages

Message Type	Description
DHCPDiscover	The first time a DHCP client computer attempts to log on to the network, it requests IP address information from a DHCP server by broadcasting a DHCPDiscover packet. The source IP address in the packet is 0.0.0.0 because the client does not yet have an IP address. The message is either 342 or 576 bytes long—older versions of Windows use a longer message frame.
DHCPOffer	Each DHCP server that receives the client DHCPDiscover packet responds with a DHCPOffer packet containing an unleased IP address and additional TCP/IP configuration information, such as the subnet mask and default gateway. More than one DHCP server can respond with a DHCPOffer packet. The client will accept the first DHCPOffer packet it receives. The message is 342 bytes long.
DHCPRequest	When a DHCP client receives a DHCPOffer packet, it responds by broadcasting a DHCPRequest packet that contains the offered IP address, and shows acceptance of the offered IP address. The message is either 342 or 576 bytes long, depending on the length of the corresponding DHCPDiscover message.
DHCPAcknowledge (DHCPAck)	The selected DHCP server acknowledges the client DHCPRequest for the IP address by sending a DHCPAck packet. At this time the server also forwards any optional configuration parameters. Upon receipt of the DHCPAck, the client can participate on the TCP/IP network and complete its system startup. The message is 342 bytes long.
DHCPNak	If the IP address cannot be used by the client because it is no longer valid or is now used by another computer, the DHCP server responds with a DHCPNak packet, and the client must begin the lease process again. Whenever a DHCP server receives a request for an IP address that is invalid according

	to the scopes that it is configured with, it sends a DHCPNak message to the client.
DHCPDecline	If the DHCP client determines the offered configuration parameters are invalid, it sends a DHCPDecline packet to the server, and the client must begin the lease process again.
DHCPRelease	A DHCP client sends a DHCPRelease packet to the server to release the IP address and cancel any remaining lease.
DHCPInform	DHCPInform is a new DHCP message type, defined in RFC 2131, used by computers on the network to request and obtain information from a DHCP server for use in their local configuration. When this message type is used, the sender is already externally configured for its IP address on the network, which may or may not have been obtained using DHCP. This message type is not currently supported by the DHCP service provided in earlier versions of Windows NT Server and may not be recognized by third-party implementations of DHCP software.

How the Lease Process Works

The first time a DHCP-enabled client starts and attempts to join the network, it automatically follows an initialization process to obtain a lease from a DHCP server. Figure 4.2 shows the lease process.

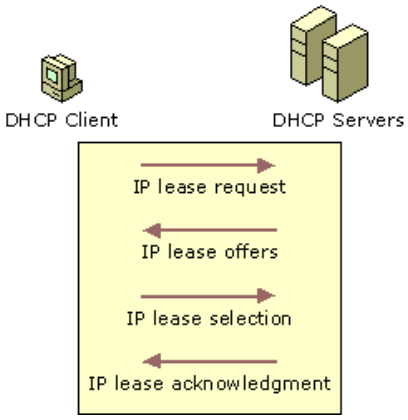


Figure 4.2 The DHCP Lease Process

1. The DHCP client requests an IP address by broadcasting a DHCPDiscover message to the local subnet.
2. The client is offered an address when a DHCP server responds with a DHCPOffer message containing an IP address and configuration information for lease to the client. If no DHCP server responds to the client request, the client can proceed in two ways:
   - If it is a Windows 2000–based client, and IP auto-configuration has not been disabled, the client self-configures an IP address for its interface.
   - If the client is not a Windows 2000–based client, or IP auto-configuration has been disabled, the client network initialization fails. The client continues to resend DHCPDiscover messages in the background (four times, every 5 minutes) until it receives a DHCPOffer message from a DHCP server.
3. The client indicates acceptance of the offer by selecting the offered address and replying to the server with a DHCPRequest message.
4. The client is assigned the address and the DHCP server sends a DHCPAck message, approving the lease. Other DHCP option information might be included in the message.
5. Once the client receives acknowledgment, it configures its TCP/IP properties using any DHCP option information in the reply, and joins the network.

In rare cases, a DHCP server might return a negative acknowledgment to the client. This can happen if a client requests an invalid or duplicate address. If a client receives a negative acknowledgment (DHCPNak), the client must begin the entire lease process again.

DHCP Client States in the Lease Process

DHCP clients cycle through six different states during the DHCP lease process, as illustrated in Figures 4.3 and 4.4. Figure 4.4 illustrates the DHCP lease process for clients that are renewing a lease.

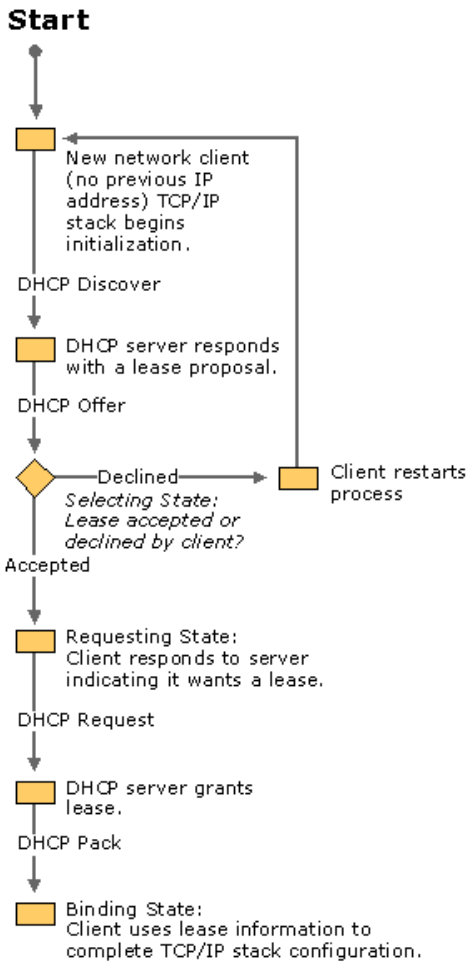


Figure 4.3 DHCP Client States During the Lease Process

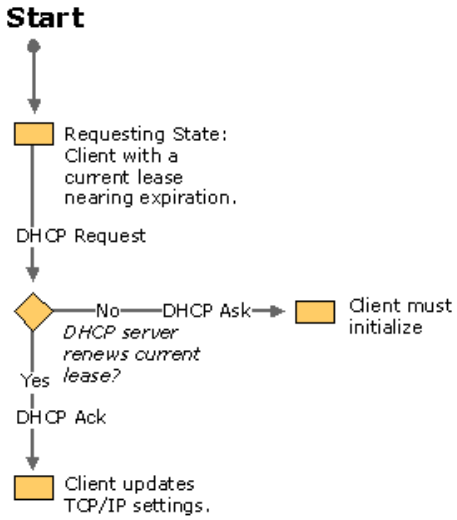


Figure 4.4 DHCP Client States During the Lease Renewal Process

When the DHCP client and DHCP server are on the same subnet, the DHCPDiscover, DHCPOffer, DHCPRequest, and DHCPAck messages are sent via media access control and IP-level broadcasts.

In order for DHCP clients to communicate with a DHCP server on a remote network, the connecting router or routers must support the forwarding of DHCP messages between the DHCP client and the DHCP server using a BOOTP/DHCP Relay Agent. For more information, see “Supporting BOOTP Clients” and “Managing Relay Agents” later in this chapter.

Initializing

This state occurs the first time the TCP/IP protocol stack is initialized on the DHCP client computer. The client does not yet have an IP address to request from the DHCP servers. This state also occurs if the client is denied the IP address it is requesting or the IP address it previously had was released. Figure 4.5 shows the Initialization state.

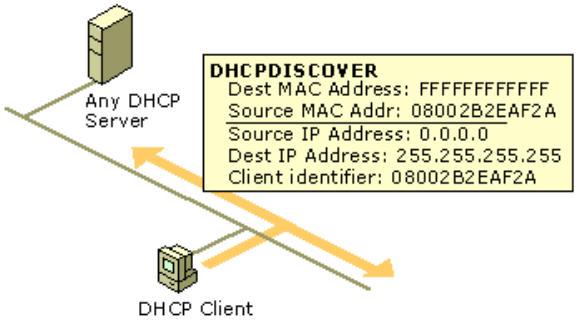


Figure 4.5 The Initialization State

When the DHCP client is in this state, its IP address is 0.0.0.0. To obtain a valid address, the client broadcasts a DHCPDiscover message from UDP port 68 to UDP port 67, with a source address of 0.0.0.0 and a destination of 255.255.255.255 (the client does not yet know the address of any DHCP servers). The DHCPDiscover message contains the DHCP client's media access control address and computer name.

Selecting

Next, the client moves into the Selecting state, where it chooses a DHCPOffer. All DHCP servers that receive a DHCPDiscover message and have a valid IP address to offer the DHCP client respond with a DHCPOffer message sent from UDP port 68 to UDP port 67. The DHCPOffer is sent via the media access control and IP broadcast because the DHCP client does not yet have a valid IP address that can be used as a destination. The DHCP server reserves the IP address to prevent it from being offered to another DHCP client.

The DHCPOffer message contains an IP address and matching subnet mask, a DHCP server identifier (the IP address of the offering DHCP server), and a lease duration. Figure 4.6 shows the Selecting state.

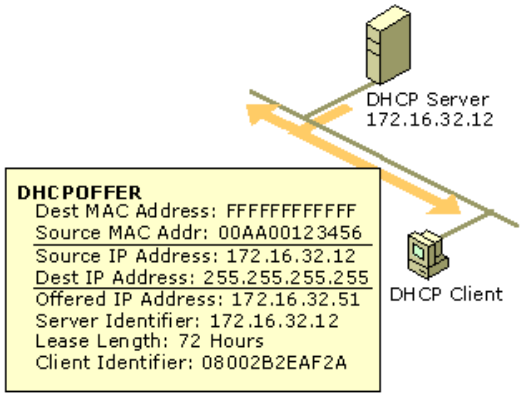
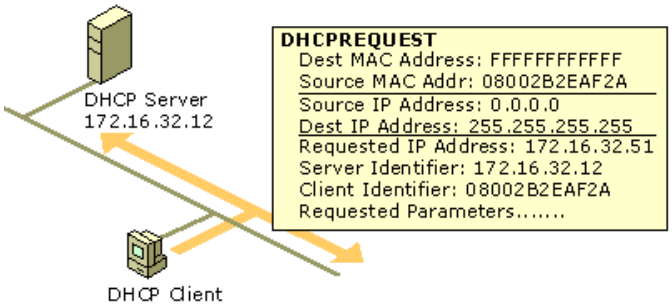


Figure 4.6 The Selecting State

The DHCP client waits for a DHCPOffer message. If a DHCP client does not receive a DHCPOffer message from a DHCP server on startup, it will retry four times (at intervals of 2, 4, 8, and 16 seconds, plus a random amount of time between 0 and 1,000 milliseconds). If a DHCP client does not receive a DHCPOffer after four attempts, it waits 5 minutes, then retries at 5-minute intervals.

Requesting

After a DHCP client has received a DHCPOffer message from a DHCP server, the client moves into the Requesting state. The DHCP client knows the IP address it wants to lease, so it broadcasts a DHCPRequest message to all DHCP servers. The client must use a broadcast because it still does not have an assigned IP address. Figure 4.7 shows the Requesting state.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.7 The Requesting State

If the IP address of the client was known (that is, the computer restarted and is trying to lease its previous address), the broadcast is looked at by all of the DHCP servers. The DHCP server that can lease the requested IP address responds with either a successful acknowledgment (DHCPAck) or an unsuccessful acknowledgment (DHCPNak). The DHCPNak message occurs when the IP address requested is not available or the client has been physically moved to a different subnet that requires a different IP address. After receiving a DHCPNak message, the client returns to the Initializing state and begins the lease process again.

If the IP address of the client was just obtained with a DHCPDiscover or DHCPOffer exchange with a DHCP server, the client puts the IP address of that DHCP server in the DHCPRequest. The specified DHCP server responds to the request, and any other DHCP servers retract their DHCPOffer. This ensures that the IP addresses that were offered by the other DHCP servers go back to an available state for another DHCP client.

Binding

The DHCP server responds to a DHCPRequest message with a DHCPAck message. This message contains a valid lease for the negotiated IP address, and any DHCP options configured by the DHCP administrator. Figure 4.8 shows the Binding state.

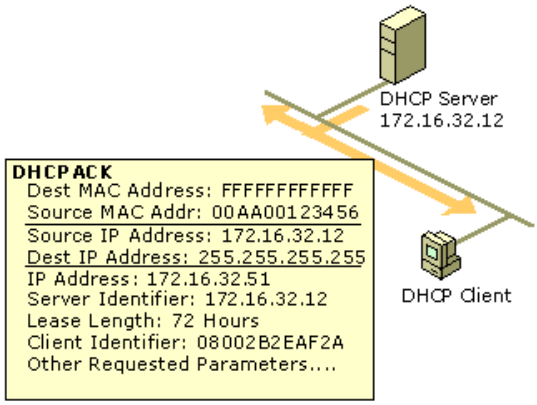


Figure 4.8 The Binding State

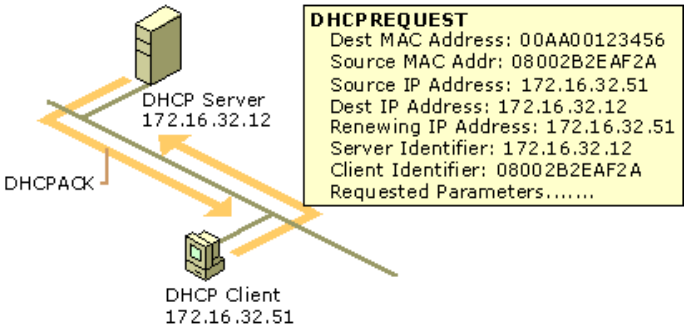
The DHCPAck message is sent by the DHCP server using an IP broadcast. When the DHCP client receives the DHCPAck message, it completes initialization of the TCP/IP stack. It is now considered a bound DHCP client that can use TCP/IP to communicate on the network.

The IP address remains allocated to the client until the client manually releases the address, or until the lease time expires and the DHCP server cancels the lease.

Renewing

IP addressing information is leased to a client, and the client is responsible for renewing the lease. By default, DHCP clients try to renew their lease when 50 percent of the lease time has expired. To renew its lease, a DHCP client sends a DHCPRequest message to the DHCP server from which it originally obtained the lease.

The DHCP server automatically renews the lease by responding with a DHCPAck message. This DHCPAck message contains the new lease as well as any DHCP option parameters. This ensures that the DHCP client can update its TCP/IP settings in case the network administrator has updated any settings on the DHCP server. Figure 4.9 illustrates the Renewing state.



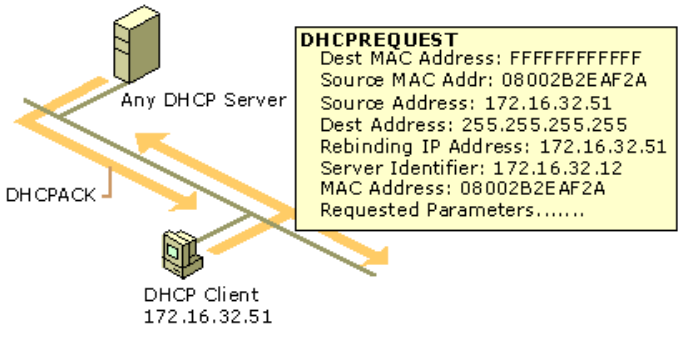
If your browser does not support inline frames, click here to view on a separate page.

Figure 4.9 The Renewing State

Once the DHCP client has renewed its lease, it returns to the Bound state. Renewal messages (DHCPRequest and DHCPAck) are sent by media access control and IP-level unicast traffic.

Rebinding

If the DHCP client is unable to communicate with the DHCP server from which it obtained its lease, and 87.5 percent of its lease time has expired, it will attempt to contact any available DHCP server by broadcasting DHCPRequest messages. Any DHCP server can respond with a DHCPAck message, renewing the lease, or a DHCPNak message, forcing the DHCP client to initialize and restart the lease process. Figure 4.10 shows the Rebinding state.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.10 The Rebinding State

If the lease expires or a DHCPNak message is received, the DHCP client must immediately discontinue using its current IP address. If

this occurs, communication over TCP/IP stops until a new IP address is obtained by the client.

Restarting a DHCP Client

When a client that previously leased an IP address restarts, it broadcasts a DHCPRequest message instead of a DHCPDiscover message. The DHCPRequest message contains a request for the previously assigned IP address.

If the requested IP address can be used by the client, the DHCP server responds with a DHCPAck message.

If the IP address cannot be used by the client because it is no longer valid, is now used by another client, or is invalid because the client has been physically moved to a different subnet, the DHCP server responds with a DHCPNak message. If this occurs, the client restarts the lease process.

If the client fails to locate a DHCP server during the renewal process, it attempts to ping the default gateway listed in the current lease, with the following results:

- If a ping of the default gateway succeeds, the DHCP client assumes it is still located on the same network where it obtained its current lease, and the client continues to use the current lease. By default, the client attempts, in the background, to renew its current lease when 50 percent of its assigned lease time has expired.
- If a ping of the default gateway fails, the DHCP client assumes that it has been moved to a different network, where DHCP services are not available (such as a home network). By default, the client auto-configures its IP address as described previously, and continues (every five minutes in the background) trying to locate a DHCP server and obtain a lease.

Lease Renewals

The renewal process occurs when a client already has a lease, and needs to renew that lease with the server. To ensure that addresses are not left in an assigned state when they are no longer needed, the DHCP server places an administrator-defined time limit, known as a lease duration, on the address assignment.

Halfway through the lease period, the DHCP client requests a lease renewal, and the DHCP server extends the lease. If a computer stops using its assigned IP address (for example, if a computer is moved to another network segment or is removed), the lease expires and the address becomes available for reassignment.

The renewal process occurs as follows:

1. The client sends a request to the DHCP server, asking for a renewal and extension of its current address lease. The client sends a directed request to the DHCP server, with a maximum of three retries at 4, 8, and 16 seconds.
   - If the DHCP server can be located, it typically sends a DHCP acknowledgment message to the client. This renews the lease.
   - If the client is unable to communicate with its original DHCP server, the client waits until 87.5 percent of its lease time elapses. Then the client enters a rebinding state, broadcasting (with a maximum of three retries at 4, 8, and 16 seconds) a DHCPDiscover message to any available DHCP server to update its current IP address lease.
2. If a server responds with a DHCPOffer message to update the client's current lease, the client renews its lease based on the offering server and continues operation.
3. If the lease expires and no server has been contacted, the client must immediately discontinue using its leased IP address. The client then proceeds to follow the same process used during its initial startup to obtain a new IP address lease.

Managing Lease Durations

When a scope is created, the default lease duration is set to eight days, which works well in most cases. However, because lease renewal is an ongoing process that can affect the performance of DHCP clients and your network, it might be useful to change the lease duration. Use the following guidelines to decide how best to modify lease duration settings for improving DHCP performance on your network:

- If you have a large number of IP addresses available and configurations that rarely change on your network, increase the lease duration to reduce the frequency of lease renewal queries between clients and the DHCP server. This reduces network traffic.
- If there are a limited number of IP addresses available and if client configurations change frequently or clients move often on the network, reduce the lease duration. This increases the rate at which addresses are returned to the available address pool for reassignment.
- Consider the ratio between connected computers and available IP addresses. For example, if there are 40 systems sharing a Class C address (with 254 available addresses), the demand for reusing addresses is low. A long lease time, such as two months, would be appropriate in such a situation. However, if 230 computers share the same address pool, demand for available addresses is greater, and a lease time of a few days or weeks is more appropriate.
- Use infinite lease durations with caution. Even in a relatively stable environment, there is a certain amount of turnover among clients. At a minimum, roving computers might be added and removed, desktop computers might be moved from one office to another, and network adapter cards might be replaced. If a client with an infinite lease is removed from the network, the DHCP server is not notified, and the IP address cannot be reused. A better option is a very long lease duration, such as six months. This ensures that addresses are ultimately recovered.

Managing Scopes

A scope must be defined and activated before DHCP clients can use the DHCP server for dynamic TCP/IP configuration. A DHCP scope is an administrative collection of IP addresses and TCP/IP configuration parameters that are available for lease to DHCP clients. The network administrator creates a scope for each logical or physical subnet.

A scope has the following properties:

- A scope name, assigned when the scope is created.
- A range of possible IP addresses from which to include or exclude addresses used in DHCP lease offers.
- A unique subnet mask, which determines the subnet for a given IP address.
- Lease duration values.

Each subnet can have a single DHCP scope with a single continuous range of IP addresses. To use several address ranges within a single scope or subnet, you must first define the scope and then set exclusion ranges.

Exclusion Ranges

When you create a new scope, addresses of existing statically configured computers should be immediately excluded from the range. By using exclusion ranges, an administrator can exclude IP address ranges within a scope so those addresses are not offered to clients.

Because Windows 2000 Server requires that a computer running the DHCP service have its IP address statically configured, be sure that the server computer has its IP address either outside of, or excluded from, the range of the scope.

Excluded IP addresses can be active on your network, but only by manually configuring these addresses at computers that do not use

DHCP to obtain an address. Exclusion ranges should be used for computers or devices that must have a static IP address, such as printer servers, firewalls, or routers.

Reservations

An administrator can reserve IP addresses for permanent lease assignment to specified computers or devices on the network. Reservations ensure that a specified hardware device on a subnet can always use the same IP address. Reservations should be made for DHCP-enabled devices that must always have the same IP address on your network, such as print servers, firewalls, or routers. For more information, see “Managing Reservations” later in this chapter.

Deleting Entries

There may be times when a scope needs to be modified in order to delete the lease of a DHCP client. The main reason for doing so is to remove a lease that conflicts with an IP address exclusion range or a reserved address that you want to specify. Deleting a lease has the same effect as if the client’s lease expired—the next time the client system starts, it must go through the process of requesting a lease. There is nothing, however, to prevent the client from obtaining a new lease for the same IP address.

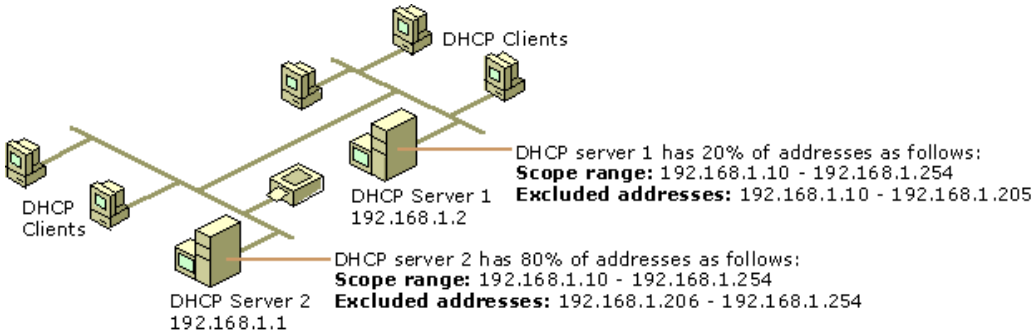
To prevent this, you must make the address unavailable before the client can request another lease by removing it from the scope and setting a reservation or exclusion. Delete scope entries only for clients that are no longer using the assigned DHCP lease or that are to be moved immediately to a new address. Deleting an active client could result in duplicate IP addresses on the network because deleted addresses are automatically reassigned to new clients.

After you delete a client’s lease from the scope and set a reservation or exclusion, you should always run **ipconfig /release** at a command prompt on the client computer, to force the client to free its IP address with a DHCPRelease message.

80/20 Rule

You will probably install more than one DHCP server so that the failure of any individual server will not prevent DHCP clients from starting. However, DHCP does not provide a way for DHCP servers to cooperate in ensuring that assigned addresses are unique. Therefore, you must carefully divide the available address pool among the DHCP servers to prevent duplicate address assignment.

For balancing DHCP server usage, use the 80/20 rule to divide scope addresses between DHCP servers. Figure 4.11 is an example of the 80/20 rule.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.11 80/20 Rule Model

DHCP Server 2 is configured to lease most (about 80 percent) of the available addresses. DHCP Server 1 is configured to lease the remaining addresses (about 20 percent).

This scenario allows the local DHCP server (DHCP Server 2) to respond to requests from local DHCP clients most of the time. The remote or backup DHCP server (DHCP Server 1) assigns addresses to clients on the other subnet only when the local server is not available or is out of addresses. This same rule can be used in a multiple-subnet scenario to ensure the availability of a DHCP server when a client requests a lease.

Managing Reservations

By using reservations, you can reserve specific IP addresses for permanent use by a DHCP-enabled computer or device.

If multiple DHCP servers are each configured with scopes that cover a range of addresses that must be reserved, the reservation ranges must be specified on each DHCP server. Otherwise, those addresses could be given out by another DHCP server.

If you want to change a reserved address for a client, the client’s existing address reservation must be removed before the new reservation can be added. DHCP option information can be changed while still keeping the reserved IP address.

Reserving a scope IP address does not automatically force a client currently using that address to stop using it. If you are reserving a new address for a client, or an address that is different from the client’s current one, you should verify that the address has not already been leased. If the address is already in use, the client using the address must release it by issuing a DHCPRelease request. To achieve this, run **ipconfig /release** at a command prompt.

Reserving an address does not force the client for whom the reservation is made to immediately move to using the reserved address. The client must issue a renewal request to move to the newly reserved address. To achieve this, run **ipconfig /renew** at a command prompt.

For Windows 95 or Windows 98–based clients, use the Winipcfg.exe program to force the release or renewal of the reserved address. For clients using MS-DOS or other operating systems, restart the clients to force the change.

Once a release or renewal is complete, the reserved client is leased the newly reserved IP address for its permanent use.

Superscopes

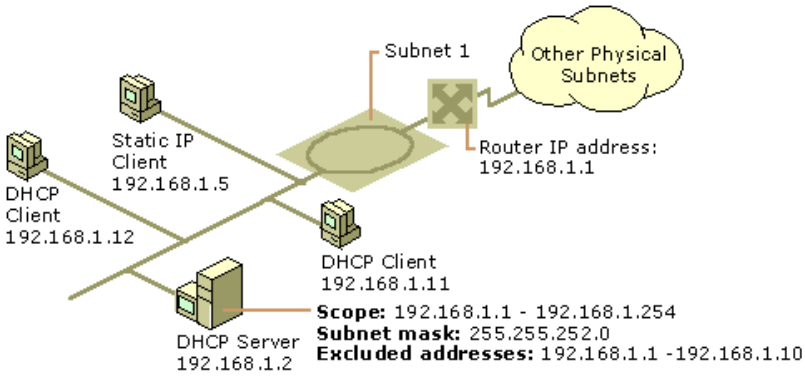
A superscope allows a DHCP server to provide leases from more than one scope to clients on a single physical network. Before you can create a superscope, you must use DHCP Manager to define all scopes to be included in the superscope. Scopes added to a superscope are called member scopes. Superscopes can resolve DHCP service issues in several different ways; these issues include situations in which:

- Support is needed for DHCP clients on a single physical network segment—such as a single Ethernet LAN segment—where multiple logical IP networks are used. When more than one logical IP network is used on a physical network, these configurations are also known as multinets.
- The available address pool for a currently active scope is nearly depleted and more computers need to be added to the physical network segment.

- Clients need to be migrated to a new scope.
- Support is needed for DHCP clients on the other side of BOOTP relay agents, where the network on the other side of the relay agent has multiple logical subnets on one physical network. For more information, see “Supporting BOOTP Clients” later in this chapter.

Versions of the DHCP service prior to Windows NT 4.0 with Service Pack 2 cannot create superscopes. One solution for this situation is to add additional network adapters to the server, and to address each of the network adapters to a given logical IP subnet. This involves additional and otherwise unnecessary hardware, and only works on segments local to the DHCP server.

A standard network with one DHCP server on a single physical subnet is limited to leasing addresses to clients on the physical subnet. Figure 4.12 shows Subnet A before a superscope is implemented.

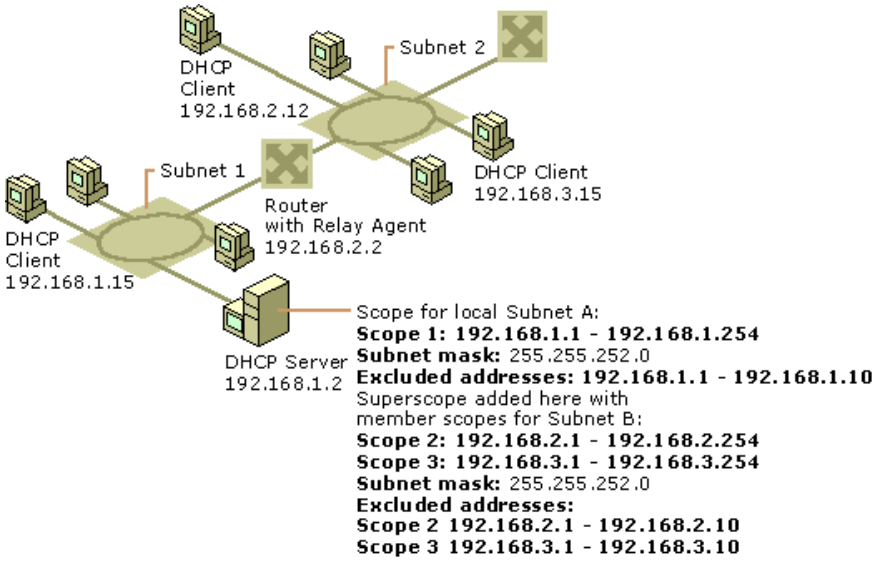


If your browser does not support inline frames, click here to view on a separate page.

Figure 4.12 DHCP Servers Using Single Scopes

To include the multinets on Subnet B in the range of addresses leased by the DHCP server shown in Figure 4.12, you can create a superscope that includes member Scopes 2 and 3 for Subnet B in addition to the scope for Subnet A.

Figure 4.13 shows the superscope configuration.

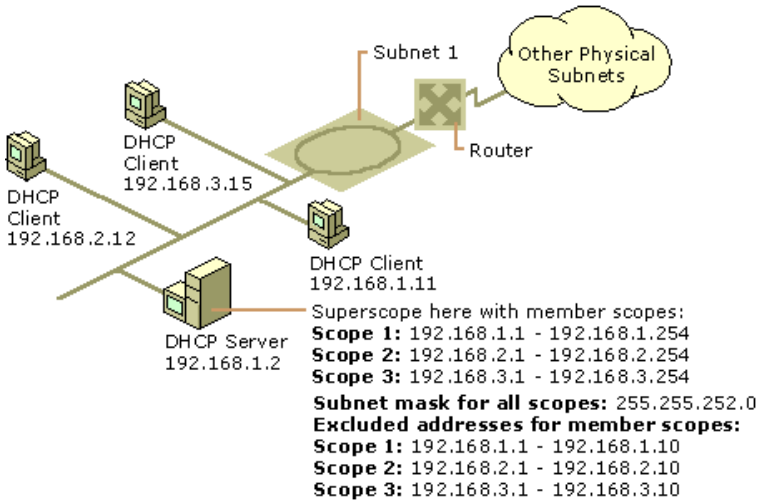


If your browser does not support inline frames, click here to view on a separate page.

Figure 4.13 DHCP Servers Using Superscopes

To include multinets on remote networks in the range of addresses leased by the DHCP server, you can configure a superscope to include member Scope 1, Scope 2, and Scope 3.

Figure 4.14 shows the scope configuration that includes the multinets on remote networks.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.14 DHCP Servers Using Superscopes for Remote Networks

Table 4.3 shows how two DHCP servers, both located on the same physical subnet, are each configured with a single scope.

Table 4.3 DHCP Scope for Servers A and B

DHCP Server Name	Starting IP Scope Address	Ending IP Scope Address
DHCP Server A	211.111.111.1	211.111.111.255
DHCP Server B	222.222.222.1	222.222.222.255

If DHCP Server A manages a different scope of addresses from DHCP Server B, and neither has any information about addresses managed by the other, a problem arises if a client previously registered with Server A, for example, releases its name during a proper shutdown and later reconnects to the network after a restart and tries to lease an address from Server B.

If Server B receives a DHCPRequest packet from the client to renew use of an address before Server A does, Server B (which does not contain any of Server A's IP addresses) rejects the request and sends a DHCPNak packet to the client. The client must then renegotiate a DHCP lease by broadcasting a DHCPDiscover packet onto the local subnet. Server B can send a DHCPOffer packet offering the client an address, which it can accept by returning a DHCPRequest for that address to Server B for approval, which occurs when Server B returns a DHCPAck packet to the client.

Nothing in this example prevents a client from having its request to renew an address rejected every time it connects to the network. In the process of rejecting and obtaining an address lease, the client might be offered an address that places it on a different subnet for which the client is not configured. By using superscopes on both DHCP servers, you can avoid both of these problems, and addresses are managed predictably and effectively.

Table 4.4 describes the same situation, but using superscopes. Both servers are located on the same physical subnet, and each is configured to allow multiple servers to provide addresses for a multinet.

Table 4.4 Superscope: DHCP Servers A and B

DHCP Server	Starting IP Scope Address	Ending IP Acope Address	Exclusions in the Scope
DHCP-ServerA	211.111.111.1	211.111.111.254	
DHCP-ServerA	222.222.222.1	222.222.222.254	222.222.222.1 to 222.222.222.254
DHCP-ServerB	222.222.222.1	222.222.222.254	
DHCP-ServerB	211.111.111.1	211.111.111.254	211.111.111.1 to 211.111.111.254

By configuring superscopes as described in this table, DHCP Servers A and B each recognize IP addresses assigned by the other. This prevents either server from negatively acknowledging attempts by DHCP clients to renew their IP address or to obtain an address from the same logical range of addresses. This works because DHCP Server B has knowledge of the scope in DHCP Server A via the superscope defined in DHCP Server B. Thus, if a DHCP client attempts to renew and its address belongs to one of the member scopes in DHCP Server B's superscope, Server B ignores the request.

> **Warning** When an IP address range that is too large for the subnet mask is specified, the administrator is given the option (by the DHCP Create Scope wizard) of creating a superscope. However, this might tax DHCP server resources. For example, if the new superscope includes more than 10,000 scopes, it might overload the server. In such cases, superscopes should be created manually with a smaller subset of scopes, or a smaller IP address range should be specified when using the wizard.

Removing Scopes

Scopes should be removed when a subnet is no longer in use or when you need to renumber your network to use a different IP address range.

You must deactivate a scope before removing it. This enables clients using the scope to renew their lease in a different scope. Otherwise, clients lose their leases and possibly network access (if they cannot auto-configure).

To ensure that all clients migrate smoothly to a new scope, you should deactivate the old scope for at least half of the lease time, or until you have manually renewed all clients, to remove them from the inactive scope. For more information about deactivating scopes, see Windows 2000 Server Help.

Preventing Address Conflicts

Windows 2000 has both server-side and client-side conflict detection to prevent duplicate IP addresses on your network.

Server Conflict Detection

The DHCP server detects conflicts by pinging an IP address before offering that address to clients. If the ping is successful (a response is received from a computer), a conflict is registered and that address is not offered to clients requesting a lease from the server. The DHCP server pings only addresses that have not been successfully and previously leased. If a client receives a lease on an IP address that it already had or is requesting a renewal, the DHCP server does not send a ping.

If conflict detection is enabled, an administrator-defined number of pings are sent. The server waits 1 second for a reply. Because the time required for a client to obtain a lease is equal to the number of pings selected, choose this value carefully as it directly impacts the overall performance of the server. In general, one ping should be sufficient.

A DHCP server receiving a reply to any of the pings (meaning there is a conflict) attaches a BAD_ADDRESS value to that IP address in the scope, and will try to lease the next available address. If the duplicate address is removed from the network, the BAD_ADDRESS value attached to the IP address can be deleted from the scope's list of active leases, and the address returned to the pool. Addresses are marked as BAD_ADDRESS for the length of the lease for which the scope is configured.

If your network includes legacy DHCP clients, enable conflict detection on the DHCP server. By default, the DHCP service does not perform any conflict detection. In general, conflict detection should be used only as a troubleshooting aid when you suspect there are duplicate IP addresses in use on your network. The reason for this is that, for each additional conflict detection attempt that the DHCP service performs, additional seconds are added to time needed to negotiate leases for DHCP clients.

Client Conflict Detection

Windows 2000 or 98-based client computers also check to determine if an address is already in use before completing address configuration with the DHCP server. If the client detects a conflict, it sends a DHCPDecline message to the DHCP server. The DHCP server attaches a BAD_ADDRESS value to the IP address in the scope, as detailed in "Server-Side Conflict Detection." The client begins the lease process again, and is offered the next available address in the scope.

For networks that include clients that are not running Windows 2000 or 98, server-side conflict detection should be enabled.

Managing DHCP Options

DHCP options can be configured for specific values and enabled for assignment and distribution to DHCP clients based on either server, scope, class or client-specific levels. The most specific take precedence over the least specific. In most cases, the client values provided are taken from the **DHCP Options Properties** dialog box on the DHCP server. These properties can be configured and set for an entire scope or for a single reserved scope client.

Although these options are not required for use by DHCP, assign and configure these options to automate client TCP/IP configuration when you have a sizable number of Microsoft-based DHCP client computers in active operation on your network. Options can also be used for DHCP communication between the server computer and client computers.

Options can be managed using different levels assigned for each managed DHCP server, including:

- Default global options

  These options are applied globally for all scopes and classes defined at each DHCP server and any clients that it services. Active global option types always apply unless they are overridden by other scope, class, or reserved client settings for the option type.

- Scope options

  These options are applied to any clients that obtain a lease within that particular scope. Active scope option types always apply to all computers obtaining a lease in a given scope unless they are overridden by class or reserved client settings for the option type.

- Class options

  These options are applied to any clients that specify that particular DHCP Class ID value when obtaining a scope lease. Active class option types always apply to all computers configured as members in a specified DHCP option class unless they are overridden by a reserved client setting for the option type.

- Reserved client options

  These options apply to any appropriate, reserved, client computer—any computer that has a reservation in the scope for its IP address. Where reserved client option types are active, settings for these option types override all other possible defaults (server, scope, or class assigned option settings for the option type).

In general, options are applied at each DHCP server at the server or scope level. To precisely manage or customize option settings, specify either a user or vendor class assignment that overrides the broader server or scope option defaults. For special requirements, such as clients with special functions, narrow the spectrum even further by assigning options for reserved clients.

Options can also be used to separate and distribute appropriate options for clients with similar or special configuration needs. For example, DHCP-enabled clients on the same floor can be assigned membership in the same option class (that is, configured with the same DHCP Class ID value). This class can then be used to distribute additional or varied option data during the lease process, overriding any scope or globally provided default options.

Many of these option types are predefined in Windows 2000 DHCP. Other standard DHCP option types can be added as needed to support any other DHCP client software that recognizes or requires the use of these additional option types. All DHCP options supported by the Windows 2000 DHCP service are defined in RFC 2132, although most DHCP clients use or support only a small subset of the available RFC-specified option types. This feature enables custom applications for enterprise networks to be introduced quickly. Equipment from multiple vendors on a network can also use different option numbers for different functions. The vendor class and vendor options are described in RFC 2132.

The Microsoft-based DHCP server usually allocates 312 bytes for DHCP options. That is more than enough for most option configurations. Some other DHCP servers and clients support option overlay, in which unused space in other standard DHCP message header fields within the DHCP packet can be overlaid to store and carry additional options. Microsoft DHCP service does not support this feature. If you attempt to use more than 312 bytes, some option settings will be lost. In that case, you should delete any unused or low-priority options. Table 4.5 contains a list of default DHCP options used by Microsoft Windows 2000 DHCP clients.

Table 4.5 Default DHCP Options

Code	Option name	Meaning
1	Subnet mask	Specifies the subnet mask of the client subnet. This option is defined in the DHCP Manager **Create Scope** or **Scope Properties** dialog box. It cannot be set directly in the **DHCP Options** dialog box.
3	Router	Specifies a list of IP addresses for routers on the client's subnet. Multihomed computers can have only one list per computer, not one per network adapter.
6	DNS servers	Specifies a list of IP addresses for DNS name servers available to the client.

15	Domain name	Specifies the DNS domain name that the client should use for DNS computer name resolution.
44	WINS/NBNS servers	Specifies a list of IP addresses for NetBIOS name servers (NBNS).
46	WINS/NBT node type	Allows configurable NetBIOS over TCP/IP (NetBT) clients to be configured as described in RFC 1001/1002, where 1 = b-node, 2 = p-node, 4 = m-node, and 8 = h-node. On multihomed computers, the node type is assigned to the entire computer, not to individual network adapters.
47	NetBIOS scope ID**(1)**	Specifies a text string that is the NetBIOS over TCP/IP scope ID for the client, as specified in RFC 1001/1002.
51	Lease time	Specifies the time, in seconds, from address assignment until the client's lease on the address expires. Lease time is specified in the DHCP Manager **Create Scope** or **Scope Properties** dialog box, and can be set directly in the **DHCP Options** dialog box.
58	Renewal (T1) time value	Specifies the time in seconds from address assignment until the client enters the Renewing state. Renewal time is a function of the lease time option, which is specified in the DHCP Manager **Create Scope** or **Scope Properties** dialog box and can be set directly in the **DHCP Options** dialog box.
59	Rebinding (T2) time value	Specifies the time, in seconds, from address assignment until the client enters the Rebinding state. Rebinding time is a function of the lease time option, which is specified in the DHCP Manager **Create Scope** or **Scope Properties** dialog box andcan be set directly in the **DHCP Options** dialog box.

(1) Option 47 (NetBIOS scope ID) is provided for backward compatibility. Don't use this option unless you already employ NetBIOS scope IDs in your environment.

> **Note** If you are using Microsoft DHCP service to configure computers that should use the services of a WINS server for name resolution, be sure to use option 44, WINS Servers, and option 46, Node Type. These DHCP options automatically configure the DHCP client as an h-node computer that directly contacts WINS servers for NetBIOS name registration and name query instead of using only broadcasts.

DHCP Option Parameters

DHCP servers can be configured to provide optional data that fully configures TCP/IP on a client. Some of the most common DHCP option types configured and distributed by the DHCP server during leases include default gateway, router, DNS, and WINS parameters.

Clients can be configured with:

- Information options. You can explicitly configure these option types and any associated values provided to clients.
- Protocol options. You can implicitly configure these option types used by the DHCP service based on server and scope property settings.

You can use DHCP Manager to configure these properties and set them for an entire scope or for a single, reserved, client scope. The LAN Manager for OS/2 client does not support DHCP or WINS.

Information Options

Table 4.6 lists the most common types of DHCP information option types that can be configured for DHCP clients. Typically, these option types can be enabled and configured for each scope that you configure on a DHCP server.

Table 4.6 Common Information Option Types

Code	Description
3	Router
6	DNS server
15	DNS domain name
44	WINS server (NetBIOS name server)
45	NetBIOS datagram distribution server (NBDD)
46	WINS/NetBIOS node type
47	NetBIOS scope ID

Clients can receive these values to set their TCP/IP configurations, during the period of the lease.

Internal Protocol Options

Table 4.7 shows internal protocol option types that DHCP clients can be configured to use when communicating with a DHCP server to obtain or renew a lease.

Table 4.7 Common Internal Protocol Option Types

Code	Description
51	Lease time
53	DHCP message type
55	Special option type used to communicate a parameter request list to the DHCP server
58	Renewal time value (T1)
59	Rebind time value (T2)

In most cases, the actual values provided to clients with these option types are taken from the DHCP service property settings on the DHCP server.

Options for Remote Access Clients

When a remote access client obtains an IP address lease from a remote access server, run Winipcfg.exe (for Windows 95) or Ipconfig.exe (for Windows 2000 or Windows NT) to display information about the lease.

When a remote access server assigns an IP address to a remote access client, either from its own static address pool or from its cached DHCP address pool, there is no effective lease time for the IP address because it is released when the client disconnects.

However, remote access clients can still receive additional TCP/IP configuration information from the remote access server: WINS server assignments and DNS server assignments can be delegated to the client when it connects. These settings are delegated directly from the remote access server's settings. If a remote access server has WINS or DNS servers as configured entries in its dial-up connection properties, these settings are passed on to remote access clients that are DHCP-enabled.

Table 4.8 lists the DHCP option types that Windows-based clients support, which are assigned to the clients through a dial-up network connection with a remote access server.

Table 4.8 DHCP Options Used by Remote Access, Windows-Based, DHCP-Enabled Clients

Option	Description
IP Address	The remote access server proactively obtains an IP address from the DHCP server and builds a cached pool of DHCP leased addresses. The remote access server then distributes these cached IP addresses to the remote access client on demand and manages each lease. This is the only information from the DHCP server that the remote access client receives.
WINS server	Values provided with the option type are taken from the remote access server dial-up connection properties if the remote access server is configured with WINS server addresses. The client acquires the list of WINS servers that are configured on the remote access server.
DNS server	Values provided with the option type are taken from the remote access server dial-up connection properties if the remote access server is configured with DNS server addresses. The client acquires the first DNS server address listed in the remote access server's DNS server search list.
Subnet Mask	The subnet mask corresponds to the default subnet mask associated with the standard address class type (Class A, B, or C) of the given IP address.
NetBIOS Scope ID	NetBIOS scope ID information is not passed to the client. If you need to modify this setting, you must change it directly on the client.
Node Type	Node Type is not taken from the DHCP lease but can change on the remote access client, depending on WINS information. If the remote access server has no locally defined WINS servers, a b-node remote access client remains a b-node client. If the remote access server has locally defined WINS servers, a b-node remote access client switches to h-node for the duration of the connection. Windows 95 clients do not automatically switch between node types if the remote access server supplies WINS addresses. In these cases, you must manually switch the node type.

Option Classes

This feature allows quick introduction of custom applications for enterprise networks. DHCP option classes provide a way to easily configure network clients with the parameters necessary to meet the special requirements of custom applications. Equipment from multiple vendors on a network can also use different option numbers for different functions. The option types used to support vendor classes—the vendor class identifier and the vendor-specific option—are defined in the Internet DHCP options standard reference, RFC 2132.

For Windows 2000 Server, there are two types of option classes: vendor-defined and user-defined. These classes can be configured on your servers to offer specialized client support in the following ways:

- Add and configure vendor-defined classes for submanaging DHCP options assigned to clients identified by vendor type.
- Add and configure user-defined classes for submanaging DHCP options assigned to clients identified by a common need for a similar DHCP option configuration.

After options classes are defined on a DHCP server, scopes on the server must be configured to assign options for specific user-defined and vendor-defined option classes.

Vendor Classes

Vendor-defined option classes can be used by DHCP clients to identify the client's vendor type and configuration to the DHCP server when obtaining a lease. For a client to identify its vendor class during the lease process, the client needs to include the vendor class ID option (option code 60) when it requests or selects a lease from a DHCP server.

The vendor class identifier information is a string of character data interpreted by the DHCP servers. Vendors can choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client. For example, the identifier might encode the client's hardware or software configuration. Most vendor types are derived from standard reserved hardware and operating system- type abbreviation codes listed in RFC 1700.

When vendor options are specified, the server performs the following additional steps to provide a lease to the client:

1. The server checks to see that the vendor class identified by the client request is a recognized class defined on the server.

   If the vendor class is recognized, the server checks to see if any additional DHCP options are configured for this class in the active scope.

   If the vendor class is not recognized, the server ignores the vendor class identified in the client request, and returns options allocated to the default vendor class (includes all DHCP Standard Options).
2. If the scope contains options configured specifically for use with clients in this vendor-defined class, the server returns those options using the vendor-specific option type (option code 43) as part of its acknowledgment message.

In most cases, the default vendor class—DHCP Standard Options—provides a default vendor class for grouping any Microsoft DHCP clients or other DHCP clients that do not specify a vendor class ID. In some cases, you might define additional vendor classes for other DHCP clients, such as printers or some types of UNIX clients. When you add other vendor classes for these purposes, be sure that the vendor class identifier you use to configure the class at the server matches the identifier used by clients for your third-party vendor.

User Classes

User classes allow DHCP clients to differentiate themselves by specifying what type of client they are, such as a remote access or desktop computer. For Windows 2000 computers, you can define specific user class identifiers to convey information about a client's software configuration, its physical location in a building, or about its user preferences. For example, an identifier can specify that DHCP

clients are members of a user-defined class called “2nd floor, West,” which has need for a special set of router, DNS, and WINS server settings. An administrator can then configure the DHCP server to configure different option types depending on the type of client receiving the lease.

Windows 2000 user classes can be used in the following ways:

- DHCP client computers can include the DHCP user class option when sending DHCP request messages to the DHCP server. This can specifically identify the client as part of a user class on the server.
- DHCP servers running the Microsoft DHCP service can recognize and interpret the DHCP user class option from clients and provide additional options (or a modified set of DHCP options) based on the client’s user class identity.

For example, shorter leases should be assigned to remote access clients. Desktop clients on the same network might require special settings, such as CAD platforms. These variations could also include WINS and DNS server settings.

If user-defined option classes are not specified, default settings (such as server options or scope options) are assigned.

A user-defined class can be either a default or custom user class. Microsoft provides three default user classes, as described in Table 4.9.

Table 4.9 Default User Classes Provided by Microsoft DHCP

Class Type	Class ID String	Description
Default User Class	(Unspecified)	Used by the DHCP service to classify clients that do not further specify an identity or type. This class is typically used by most DHCP clients. Clients are assigned to this class under the following conditions: • DHCP clients that have no concept of a user class or a user class ID. This is true for most DHCP clients prior to Windows 2000. • Windows 2000 clients configured with a class ID unknown to the DHCP server (for example, the server has not defined this class).
Default Routing and Remote Access class	RRAS.Microsoft	Used by the Microsoft DHCP service to classify clients making a PPP-type connection through a remote access server. Typically, this class includes most dial-up networking clients that use DHCP to obtain a lease: • remote access clients that have no concept of a Routing and Remote Access user class or a Routing and Remote Access user class ID. See the section titled “DHCP and Routing and Remote Access” later in this chapter for details on the interaction between server with the Routing and Remote Access feature and a DHCP server and how DHCP servers identify Routing and Remote Access clients.
Default BOOTP class	BOOTP	Used by the Microsoft DHCP service to classify any clients recognized as BOOTP clients.

Using the Microsoft default user classes can be useful for isolating configuration details specific for clients with special needs, such as older clients or clients that use BOOTP or Routing and Remote Access. For example, you might want to include and assign special BOOTP option types (such as option codes 66 and 67) for clients that are BOOTP type, or shorten the lease time for remote access clients.

You might also add and configure custom user classes for use by DHCP clients running Windows 2000. For custom user classes, you must specify a custom identifier that must correspond with a user class defined on the DHCP server computer.

Currently, the user class option field permits only one ASCII text string to be used for identifying clients. This means each client computer can only be identified as a member of a single user class by the DHCP server. If you need to, you can use additional user classes and make new hybrids from your other user classes. For example, if you have two user classes, one called “mobile” with short lease times assigned and another called “engineer” with an option assigned to configure a high-performance server for its clients, you could make a new hybrid class called “mobile-engineer” that would lease clients that have overlapping configuration needs specified in each class.

Configuring Options

The following steps can help you determine at what level to configure and assign DHCP options for clients on your network:

- Add or define new, custom option types only if you have new software or applications that requires a nonstandard DHCP option.
- If your network is large, be conservative and selective when assigning global options. These options apply to *all* clients of a DHCP server computer.
- Use scope-level options for most options that clients are assigned. In most networks, the scope level is typically the preferred level for assigning options.
- Use class options if you have a large network or groups of clients with diverse needs that are able to support membership in option classes (such as Windows 2000 clients).
- Use reserved client options only for clients that have special requirements—for example, if your intranet has a DNS server that performs forwarding for resolving Internet DNS names not authoritatively managed on your network. In this case, you need to add the IP address of an external DNS server on your DNS server computer. You can configure your DNS server as a reserved client in DHCP and set this address as another reserved client option.

Options Precedence

The DHCP service uses a bottom-up hierarchy in determining which option to enforce. This simplifies DHCP management and allows a flexible administration that can range from server-wide default settings to individualized client settings when needed for special circumstances.

Following are the basic rules of how options are used:

- Active global options always apply unless overridden by scope, class, or reserved options.
- Active scope options always apply to any computers obtaining a lease from that scope, unless overridden by class or reserved options.
- Active class options always apply to any computers configured as members of that class, unless overridden by a reserved option.
- Reserved options override all other possible options.
- Statically configured values on a client override any DHCP options of any type or level.

Multicast DHCP

Multicast DHCP, now referred to as MADCAP (Multicast Address Dynamic Client Allocation Protocol), is now included with the Windows 2000 DHCP service, and is used to support dynamic assignment and configuration of IP multicast addresses on TCP/IP-based networks.

Ordinarily, you use DHCP scopes to provide client configurations by allocating ranges of IP addresses from the Class A, B, or C address classes. By using these scopes and ranges of addresses, your clients are configured to use unicast for point-to-point communication between two networked computers.

With Windows 2000 Server, the DHCP service offers MADCAP support in the form of multicast scopes. You configure a multicast scope as you would a regular DHCP scope, but multicast scopes provide scope ranges of Class D multicast IP addresses. These addresses are reserved for multicast operation using directed transmission from one point to multiple points.

Background on Multicasting

A group of TCP/IP computers can use a multicast IP address to send directed communication to all computers with which they share the use of the group address. Multicast addresses are shared by many computers.

When the destination address for an IP datagram is a multicast address, the packet is forwarded to all members of that multicast group, which is a set of zero or more computers identified by that multicast address.

Dynamic Membership

Multicast addresses support dynamic membership, allowing individual computers to join or leave the multicast group at any time. Group membership is not limited by size, and computers are not restricted to membership in any single group. In addition, any computer that uses TCP/IP can send datagrams to any multicast group. A multicast group is similar to a group e-mail address in its usage. When an IP multicast address is used as the destination address for an IP datagram, the datagram is forwarded to all members of the multicast group identified by the address.

Multicast Address Ranges

You can permanently reserve multicast group addresses or temporarily assign and use them. A permanent group is made by permanently reserving a Class D IP address (224.0.0.0 to 239.255.255.255) with the Internet Assigned Numbers Authority (IANA). The reserved address then becomes a well-known address, indicating a specific multicast group that exists regardless of whether group member computers are present on the network. For multicast IP addresses not permanently reserved with the IANA, all Class D addresses that remain unreserved can then be used dynamically to assign and form temporary multicast groups. These temporary groups can exist as long as one or more computers on the network are configured with the group's address and actively share in its use.

Supporting MADCAP

Clients using MADCAP must be configured to use the MADCAP API. For more information on writing or programming applications that use this API, see the developer resources made available through the Microsoft Solution Developers Network (MSDN).

MADCAP assists in simplifying and automating configuration of multicast groups on your 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.

MADCAP address configuration for clients should be done independently of how the clients are configured to receive their primary IP address. Computers that use either static or dynamic configuration through a DHCP server can be MADCAP clients.

The Windows 2000 DHCP service supports both DHCP and MADCAP, although these services function separately. Clients of one are not dependent on the use or configuration of the other.

- Clients that are manually configured or use DHCP to obtain a unicast IP address lease can also use MADCAP to obtain multicast IP address configuration.
- Clients that do not support MADCAP service or are unable to contact and obtain multicast configuration from a MADCAP server can be configured in other ways so that they participate in either permanent or temporary multicast groups on the network.
- In all TCP/IP networks, each computer requires a unique primary computer IP address (that is not shared or duplicated) from one of the standard address classes used for building the network (Class A, B, or C range). You must assign this required primary computer IP address before you can configure a computer to support and use secondary IP addresses such as multicast IP addresses.
- When multicast address configuration is used, a MADCAP server can dynamically perform this configuration for clients that support the MADCAP protocol.

DHCP Database

Windows 2000 DHCP servers use the performance-enhanced Exchange Server Storage engine version 4.0.

The DHCP service database is a dynamic database that is updated as DHCP clients are assigned or as they release their TCP/IP configuration parameters. Because the DHCP database is not a distributed database like the WINS server database, maintaining the DHCP service database is less complex.

Database Management

The following describes the administrative tasks for managing your DHCP database. To avoid high cost of ownership, these are performed by Windows 2000 automatically, but can also be done manually by the network administrator.

Record Management

There is no built-in limit to the number of records that a DHCP server can store. The size of the database depends on the number of DHCP clients on the network. The DHCP database grows over time as a result of clients starting and stopping on the network. Over time, as some DHCP client entries become obsolete and are deleted, some unused space remains.

Storage Space Management

To recover unused space, the DHCP database must be compacted. Windows 2000 dynamically compacts the database in an automatic background process during idle time after a database update. Although dynamic compacting greatly reduces the need for performing offline compaction, it does not fully eliminate it. Offline compaction reclaims the space more efficiently and should be performed at least once a month for large, busy networks with 1,000 or more DHCP clients. For smaller networks, manual compaction might be required only every few months.

Because the dynamic database compaction occurs in the background while the database is in use, you do not need to stop the DHCP server. However, for manual compacting, the DHCP server must be taken offline.

Database Backup

The DHCP database and related registry entries are automatically backed up at a specific interval. You can modify the default interval by changing the value of the **BackupInterval** entry in the following registry subkey:

HKEY_LOCAL_COMPUTER\SYSTEM\CurrentControlSet

Caution Do not use a registry editor to edit the registry directly unless you have no alternative. The registry editors bypass the standard safeguards provided by administrative tools. These safeguards prevent you from entering conflicting settings or settings that are likely to degrade performance or damage your system. Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows 2000. To configure or customize Windows 2000, use the programs in Control Panel or Microsoft Management Console (MMC) whenever possible.

DHCP Service Database Files

When you install the DHCP service, the files shown in Table 4.10 are automatically created in the *%SystemRoot%*\System32\Dhcp directory.

Table 4.10 Database Files and Descriptions

File	Description
J50.log and J50*xxxx*.log	A log of all transactions done with the DHCP database. This file is used by DHCP to recover data if necessary. To increase speed and efficiency of data storage, the Jet database writes current transactions to log files rather than to the database directly. Therefore, the most current view of the data is the database plus any transactions in the log files. These files are also used for recovery if the DHCP service is stopped in an unexpected manner. If the service is stopped in an unexpected manner, the log files are automatically used to recreate the correct state of the DHCP database. Log files are always a certain size; however, they can grow quickly in number on a very busy DHCP server. It is inevitable that DHCP will write more transactions to a log than the size of the log can accommodate. When a log file becomes filled, it is renamed to indicate that it is an older log and not in use. A new transaction log is created with the J*n*.log filename (where *n* is a decimal number), such as J50.log. The naming format of the previous log file will be Jet*xxxxx*.log, where each *x* denotes a hexadecimal number from 0 to F. Previous log files are maintained in the same folder as the current log files. The log files are processed (all log entries written to the database) and deleted when a successful backup occurs or when the DHCP server is shut down gracefully. Therefore, if many J*n*.log files have accumulated, frequent backups should be scheduled to maintain the logs. After the entries have been processed, it is possible to manually delete the log files; however, this prevents a successful recovery of the database if it is needed. Because of this, it is important that the log files not be manually deleted or removed from the system until a backup has been performed.
J50.chk	A checkpoint file that indicates the location of the last information successfully written from the transaction logs to the database. It is also used for recovery purposes—that is, the checkpoint file indicates where the recovery or replaying of data should begin. This checkpoint file is updated every time data is written to the database file (DHCP.mdb).
Dhcp.mdb	The DHCP service database file that contains two tables: the IP-address-Owner-ID mapping table and the name–to–IP address mapping table.
Dhcptmp.mdb	A temporary file that is created by a DHCP server. This file is used by the database as a swap file during index maintenance operations and may remain in the *%SystemRoot%*\System32\DHCP directory after a crash.
Res*x*.log	These are reserved log files that are kept for emergency purposes. They are used if the server runs out of disk space. If a server attempts to create another transaction log file and there is insufficient disk space, the server flushes any outstanding transactions into these reserved log files. The service then shuts down and logs an event to the event log.

DHCP uses the Jet database format for storing its data. Jet produces J*n*.log and other files in the *%SystemRoot%*\System32\DHCP folder to increase the speed and efficiency of data storage.

Caution The J50.log, J50*xxxxx*.log, Dhcp.mdb, Dhcptmp.mdb, and Res*x*.log files should not be removed or tampered with in any manner.

Supporting BOOTP Clients

The Bootstrap Protocol (BOOTP) is a computer configuration protocol developed before DHCP. DHCP improves on BOOTP and resolves specific limitations BOOTP had as a computer configuration service. RFC 951 defines BOOTP.

BOOTP was intended to configure diskless workstations with limited boot capabilities, while DHCP was intended to configure frequently relocated networked computers (such as portables) that have local hard drives and full boot capabilities.

Because of the relationship between BOOTP and DHCP, both protocols share some defining characteristics. The common elements include:

- The format structure used to exchange client/server messages.

  BOOTP and DHCP use nearly identical request messages (sent by clients) and reply messages (sent by servers). Messages in either of these protocols use a single User Datagram Protocol (UDP) datagram of 576 bytes to enclose each protocol message. Message headers are the same for both BOOTP and DHCP with one exception: The final message header field used to carry optional data. For BOOTP, this optional field is called the vendor-specific area and is limited to 64 octets. For DHCP, this area is called the options field and can carry up to 312 octets of DHCP options information.

  Because DHCP and BOOTP messages use nearly identical format types and packet structures, and typically use the same well-known service ports, BOOTP or DHCP relay agent programs usually treat BOOTP and DHCP messages as essentially the same message type, without differentiating between them.

- Use of well-known UDP ports for client/server communication.

  Both BOOTP and DHCP use the same reserved protocol ports for sending and receiving messages between servers and clients. Both BOOTP and DHCP servers use UDP port 67 to listen for and receive client request messages. BOOTP and DHCP clients typically reserve UDP port 68 for accepting message replies from either a BOOTP server or DHCP server.

- IP address distribution as an integral part of configuration service.

  Although both BOOTP and DHCP allocate IP addresses to clients during startup, they use different methods of allocation. BOOTP typically provides fixed allocation of a single IP address for each client, permanently reserving this address in the BOOTP server

database. DHCP typically provides dynamic, leased allocation of available IP addresses, reserving each DHCP client address temporarily in the DHCP service database.

- The downloading of the image file by the BOOTP client is performed using the Trivial File Transfer Protocol (TFTP).

  Clients contact TFTP servers to perform file transfer of their boot image. Because Windows 2000 does not provide a TFTP file service, you need a third-party TFTP server to support BOOTP clients that must boot from an image file (usually diskless workstations). You also need to configure your DHCP server to provide supported BOOTP/DHCP options.

The implementation of BOOTP support described in this section assumes that the DHCP service is already installed and correctly configured for DHCP clients.

For more information about BOOTP, see RFCs 1532, 2131, and 2132. Support for BOOTP is also available with Windows NT Server 4.0 with Service Pack 2 and later.

Differences Between BOOTP and DHCP

Despite these similarities, there are significant differences in the ways BOOTP and DHCP perform client configuration:

- BOOTP supports a limited number of client configuration parameters called vendor extensions, while DHCP supports a larger and extensible set of client configuration parameters called options.
- BOOTP uses a two-phase bootstrap configuration process in which clients contact BOOTP servers to perform address determination and boot file name selection, and clients contact Trivial File Transfer Protocol (TFTP) servers to perform file transfer of their boot image. DHCP uses a single-phase boot configuration process whereby a DHCP client negotiates with a DHCP server to determine its IP address and obtain any other initial configuration details it needs for network operation.
- BOOTP clients do not rebind or renew configuration with the BOOTP server except when the system restarts, while DHCP clients do not require a system restart to rebind or renew configuration with the DHCP server. Instead, clients automatically enter the Rebinding state at set timed intervals to renew their leased address allocation with the DHCP server. This process occurs in the background and is transparent to the user.

BOOTP Clients Requesting IP Address Information Only

Previously, BOOTP client support through the DHCP server required an explicit client reservation to be made for each BOOTP client.

With new support for dynamic BOOTP, a pool of addresses can be designated—similar to the way a scope is used for DHCP clients—to dynamically manage IP address assignment for BOOTP clients. The DHCP service can later reclaim addresses used in the dynamic BOOTP address pool, after first verifying that a specified lease time has elapsed and that each address is not still in use by the BOOTP client.

To configure your DHCP server to assign and distribute IP address information to BOOTP clients, you must configure a BOOTP address pool within a DHCP scope on the server.

Another option to the dynamic BOOTP address pool is to add a client reservation for each BOOTP client within your DHCP scopes. A reservation builds an association between the BOOTP client's media access control address (encoded in its physical hardware) and its leased IP address. When a reserved client requests the reservation of an IP address, the DHCP service returns the appropriate reserved IP address in the lease response based on the client's media access control address included in the BOOTP request message.

BOOTP Clients Requesting Boot File Information

To configure the DHCP service to provide boot file information to BOOTP clients, you must do the following:

1. Create a client address reservation for each BOOTP client within an active DHCP scope.

   BOOTP addresses must be reserved by an IP address reservation that you make for each BOOTP client. When you make client reservations, enter the BOOTP client's physical or media access control address, as assigned in LAN adapter hardware for the **Unique identifier** in the **Add Reservation** dialog box. BOOTP clients use this address when they start and send a BOOTP request. In the same dialog box, under **Allowed client types**, you should click either **BOOTP only** or **Both** when you create each BOOTP client reservation.

2. Create BOOTP entries for each client-specific platform in the BOOTP table on the DHCP server.

Information stored in the BOOTP table is returned to any requesting BOOTP clients on the network that broadcast a BOOTP request message. If at least one BOOTP entry has been added to the BOOTP table, the DHCP service replies to BOOTP client requests. If no BOOTP entries are configured, the DHCP service ignores BOOTP request messages.

The reply message returned by the DHCP service indicates the name and location of another server on the network (a TFTP server) that the client can then contact to retrieve its boot image file.

DHCP Options Supported for BOOTP Clients

BOOTP clients that do not specify the DHCP option code 55 (the Options Request List parameter) can still retrieve the following options from DHCP servers running Windows NT Server 4.0 or later. Table 4.11 lists the DHCP options available for BOOTP clients.

Table 4.11 DHCP Options for BOOTP Clients

Code	Description
1	Subnet Mask
3	Router
4	Time Server
5	Name Server
9	LPR Server
12	Computer Name
15	Domain Name
17	Root Path
42	NTP Servers
44	WINS Server
45	NetBIOS over TCP/IP Datagram Distribution Server

46	NetBIOS over TCP/IP Node Type
47	NetBIOS over TCP/IP Scope
48	X Window System Font Server
49	X Window System Display Manager
69	SMTP Server
70	POP3 Server

In order to obtain other options, the client must specify option 55 in the BOOTP request. Windows 2000 DHCP servers return the options in the order listed above and return as many options as can fit in a single datagram response.

Important When configuring client reservations for use with BOOTP clients, remember that DHCP options can apply equally to DHCP and BOOTP clients. Therefore, it is imperative that you correctly configure your scopes.

Configuring the BOOTP Table

Each record in the BOOTP table contains the three fields that contain information that is returned to the BOOTP client:

- **Boot Image.** Identifies the generic file name (such as “unix”) of the requested boot file, based on the BOOTP client’s hardware type.
- **File Name.** Identifies the full path of the boot file (such as “/etc/vmunix”) returned to the client by the BOOTP server, using TFTP.
- **File Server.** Identifies the name of the TFTP server used to source the boot file.

To add entries in the BOOTP table, use DHCP Manager.

Planning for DHCP

DHCP implementation is so closely linked to the Windows Internet Name Service (WINS) and the Domain Name System (DNS) that network administrators will benefit from combining all three when planning deployment.

If you use DHCP servers for Microsoft network clients, you must use a name resolution service. Windows 2000 networks use the DNS service to support Active Directory (in addition to general name resolution). Networks supporting Windows NT 4.0 and earlier clients must use WINS servers. Networks supporting a combination of Windows 2000 and Windows NT 4.0 clients should implement both WINS and DNS.

Best Practices

Before you install Microsoft DHCP servers on your network, consider these best practices:

Use the 80/20 design rule

Using more than one DHCP server on the same subnet provides increased fault tolerance for servicing DHCP clients located on the subnet. With two DHCP servers, if one server goes down, the other server can be made to take its place and continue to lease new addresses or renew existing clients. This also helps balance server usage.

Use superscopes for multiple DHCP server environments

On each subnet in a LAN environment, with different scopes on each server, it is recommended that you use superscopes. Using superscopes as a way to share information about all scopes in the subnets on each of the DHCP servers resolves problems, such as a negative acknowledgment being sent to a client erroneously.

When started, each DHCP client sends a limited broadcast of the DHCPDiscover message to its local subnet to try 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.

For example, if two DHCP servers—Server1 and Server2—are configured with different scope ranges of available addresses, a DHCP client can be leased by either server depending on which server responds first to the client’s initial broadcast request to find a server at startup. Later, the DHCP server originally used by the client to obtain its lease may be temporarily unavailable during the client renewal state (by default, the client attempts renewal after 50 percent of its lease has elapsed).

If renewal fails, the client delays any attempt to renew its lease until it enters the Rebinding state (by default, the client enters the Rebinding state after 87.5 percent of its lease has elapsed). In the Rebinding state, the client broadcasts to the subnet to obtain a valid IP configuration for its continued use on the network. At this point, if a different DHCP server (that is, a DHCP server other than the one that first leased the client) responds to the client broadcast first, it sends a DHCPNak (a negative acknowledgment) message in reply. This happens because the client’s current address is not known to the other server and recognized as a valid IP address for the subnet. This DHCPNak situation for the client can occur even if the original DHCP server that leased the client is available on the network.

To avoid these problems when using more than one DHCP server on the same subnet, use a new superscope configured similarly at all DHCP servers. The superscope should include all valid scopes for the subnet as member scopes. For configuring member scopes at each server, addresses must only be made available at a single DHCP server on the subnet. For all other DHCP servers on the subnet, use exclusion ranges when configuring the corresponding scope.

When a superscope is created, all DHCP servers are configured with member scopes that exclude addresses they do not service. When a server receives a renewal request, it checks to see if the client’s IP address belongs to one of the scopes it is aware of:

- If it belongs to one of these scopes, and the address falls in a range that has been excluded on that server, the server ignores the renewal request.
- If the server cannot find any scopes that include this IP address, the server sends a DHCPNack in response to the request, indicating this address should not be used on that subnet.
- If the server is unavailable, the client times out and waits until the rebinding time (T2) interval occurs, usually when 87.5 percent of the lease time has expired. If the server is still unavailable at that time, the client keeps using its current IP address until the lease expires. The client then begins broadcasting a DHCPDiscover message to obtain a new lease. If the client’s original DHCP server (the server from which it obtained its lease) is still unavailable, another DHCP server on the subnet handles the client request, and allocates an IP address and lease to the client.

Deactivate scopes only when removing a scope permanently from service.

Once you activate a scope and place it into service, it should not be deactivated until you are ready to retire the scope and its included range of addresses from use on your network. This is because once a scope is deactivated, the DHCP server no longer accepts those scope addresses as valid addresses. This can be useful when your intention is to permanently retire a scope from use. Otherwise, deactivating a scope can cause undesired DHCPNak messages to be sent to clients leased in the scope.

If your intent is only to effect temporary deactivation of scope addresses, edit or modify exclusion ranges in an active scope so you don’t cause undesired DHCPNak problems that appear after a scope is deactivated.

Use conflict detection on DHCP servers only under unusual circumstances.

For Windows 2000, DHCP client computers that obtain an IP address use a gratuitous ARP request to perform client-based conflict detection before completing configuration and use of an offered IP address. If a client running Windows 2000 is configured to use DHCP and detects a conflict, it sends a DHCPDecline message to the DHCP server. Windows 95-based Microsoft TCP/IP clients typically do not perform conflict detection in this way.

If your network includes Windows 95-based DHCP clients, you should only use server-side conflict detection provided by the DHCP service. To enable conflict detection, increase the number of ping attempts that the DHCP service performs for each address before leasing that address to a client.

Note that for each additional conflict detection attempt the DHCP service performs, additional seconds are added to the time needed to negotiate leases for DHCP clients.

Reservations should be created on all DHCP servers that can potentially service the reserved client.

You can use a client reservation to assure 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 on each of your other DHCP servers. This allows other servers to honor the address reservation made for the client.

In this situation, all reachable DHCP servers for the reserved client should be configured as described earlier, using a superscope with similar scope ranges of addresses. Although the client reservation will be acted upon only by the DHCP server where the reserved address is available, you can create the same reservation on other DHCP servers that exclude this address.

For server performance, consider 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 for the best performance, consider RAID solutions when purchasing hardware for your server computer to improve disk access time.

When evaluating performance of your DHCP servers, you should view DHCP as part of making a full performance evaluation of the server as a whole. By monitoring system hardware performance in the most demanding areas of utilization (that is, CPU, memory, disk input/output) you will obtain the best assessment of when a DHCP server is overloaded or in need of upgrades.

Note that for Windows 2000 Server, the DHCP service includes several new System Monitor counters that can be used to monitor service. For more information, see “Overview of Performance Monitoring” in the Microsoft Windows 2000 Server Resource Kit Server Operations Guide.

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.

Reduce lease times for DHCP clients that use Routing and Remote Access for dial-up networking.

If the Routing and Remote Access service is used on your network to support dial-up clients, you can adjust the lease time on scopes that service these clients to use a lease time reduced from the default for a scope of eight days. For Windows 2000, one recommended way to support remote access clients in your scopes is to add and configure the built-in Microsoft user class provided for identifying remote access clients.

Increase the lease duration of scope leases for large, stable, fixed networks if available address space is plentiful.

For small networks (for example, one physical LAN not using routers), the default lease duration of eight days is a typical period. For larger routed networks, consider increasing the length of scope leases to a longer period of time, such as 7 to 21 days. This can reduce DHCP-related network broadcast traffic, particularly if client computers generally remain in fixed locations and scope addresses are plentiful (at least 20 percent or more of the addresses are still available).

Integrate DHCP with other services, such as WINS and DNS.

Either WINS or DNS (or possibly both) are 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 either routers which are capable of relaying BOOTP and DHCP message traffic, or use relay agents and set appropriate timers to prevent undesired forwarding and relay of BOOTP and DHCP message traffic.

If you have multiple physical networks connected through routers, the routers must be capable of relaying BOOTP and DHCP traffic. In routed networks that use subnets to divide network segments, planning options for DHCP services must observe some specific requirements for a full implementation of DHCP services to function. These requirements include the following:

- One DHCP server must be located on at least one subnet in the routed network.
- For a DHCP server to support clients on other remote subnets separated by routers, a router or remote computer must be used as a DHCP and BOOTP relay agent to support forwarding of DHCP traffic between subnets.

If you do not have such routers, you can set up the DHCP Relay Agent component on at least one computer running Windows 2000 Server (or Windows NT Server) in each routed subnet. The relay agent relays DHCP- and BOOTP-type message traffic between the DHCP-enabled clients on a local physical network and a remote DHCP server located on another physical network. When using relay agents, be sure to set and increase the initial time that relay agents wait before relaying DHCP messages to servers. For more information, see the section titled “Relay Agent Deployment” later in this chapter.

For DNS with dynamic updates performed by the DHCP server, use the default client preference settings.

For Windows 2000 Server, the DHCP service performs dynamic updates for DHCP clients based on how clients request updates be done. This setting provides the best use of the DHCP service to perform dynamic updates on behalf of its clients as follows:

- Client computers running Windows 2000 explicitly request that the DHCP service only update pointer (PTR) resource records used in DNS for the reverse lookup and resolution of the client’s IP address to its name. These clients update their address (A) resource records for themselves.
- Clients running earlier Windows versions cannot make an explicit request for dynamic update preference. For these clients, the DHCP service can be configured to update both the PTR and the A resource records for the client.

Follow the recommended process for moving a DHCP service database from old server computer hardware to new hardware.

For information on moving DHCP service data to another server computer, such as in the case of hardware failure or disaster recovery, see the Microsoft Knowledge Base.

DHCP Service Installation

Before you install a DHCP server, 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.
- The DHCP option types and the option values that will be predefined for the DHCP clients.

DHCP Server Location

Use the physical characteristics of your LAN or WAN infrastructure and not the logical groupings defined by Windows 2000 domains and your Active Directory structure. When subnets are connected by routers that support BOOTP relay agents, DHCP servers are not required on every subnet.

Also, DHCP servers can be administered remotely from a computer running Windows 2000 and DHCP Manager.

Resources

Compile a list of requirements, including:

- The number and types of computers that need to be supported.
- Interoperability with existing systems, including your requirements for mission-critical accounting, personnel, and similar information systems.
- Hardware support and related software compatibility, including routers, switches, and other types of servers.
- Network monitoring software, such as Net Monitor (provided with Windows 2000).

Process Isolation

Isolate the areas of the network where processes must continue uninterrupted, and then target these areas for the last stages of implementation.

Logical Subnet Planning

Review the geographic and physical structure of the network to determine the best plan for defining logical subnets as segments of the intranet.

Test Phases

Define the components in the new system that require testing, and then develop a phased plan for testing and adding components. For example, the plan could define the order of types of computers to be phased in, including Windows 2000 servers and workstations, Microsoft remote access servers and clients, Windows for Workgroups computers, and MS-DOS clients.

- Create a pilot and a second test phase, including tuning the DHCP and WINS server-client configuration for efficiency. This task includes determining strategies for backup servers and for partitioning the address pool at each server for local vs. remote clients.
- Document all architecture and administration issues for network administrators.
- Always run estimates of normal workloads during your testing scenarios, to gain accurate performance information and feedback.

Supporting Additional Subnets

For the DHCP service to support additional subnets on your network, you must first determine if the routers used to connect adjoining subnets can support relaying of BOOTP and DHCP messages. If routers cannot be used for DHCP and BOOTP relay, you can set up either of the following for each subnet:

- A computer running either Windows 2000 Server or Windows NT Server 4.0 configured to use the DHCP Relay Agent component. This computer simply forwards messages back and forth between clients on the local subnet and a remote DHCP server, using the IP address of the remote server. The DHCP Relay Agent service is available only on computers running Windows 2000 Server or Windows NT Server 4.0.
- A computer running Windows 2000 Server configured as a DHCP server for the local subnet. This server computer must contain and manage scope and other address-configurable information for the local subnet it serves.

DHCP Traffic

DHCP traffic does not use significant network bandwidth during normal periods of usage. Typical DHCP traffic does not exceed 1 percent of overall network traffic. However, there are two phases of DHCP client configuration that generate some network traffic load. These phases are IP address lease and IP address renewal.

When a client initializes TCP/IP for the first time (and is configured as a DHCP client), its first step is to acquire an IP address using DHCP. This process, as described earlier, results in a conversation between the DHCP client and server consisting of four packets, the first of which is the client computer broadcasting a DHCPDiscover packet in an attempt to locate a DHCP server.

As shown in the initial lease process earlier in this chapter, the entire process of acquiring an IP address lease through DHCP takes a total of four packets, each varying between 342 and 590 bytes in size. This process, on a clean network (when no other network traffic is using bandwidth), takes less than 1 second (about 300 milliseconds) on 10BaseT media. Results depend on media type in use.

DHCP conversations generally occur in the following instances:

- When a DHCP client initializes for the first time (all four frames are sent).
- When an automatic renewal occurs, which is done every one-half lease life (four days by default, or every 96 hours). This communication takes two packets (DHCPRequest and DHCPAck) and lasts approximately 200 milliseconds.
- When a client is moved to a new subnet (DHCPRequest, DHCPNak, then the four frames).
- When a DHCP client replaces its network adapter (all four frames are sent).
- Whenever a client manually refreshes or releases its address by using the Ipconfig utility.

If you want to reduce the amount of traffic generated by DHCP, it is possible to adjust the lease duration for IP address leases. This is done by using DHCP Manager, and adjusting **Lease Duration**.

Upgrading the DHCP Database for Windows 2000

When upgrading a Windows NT Server version 3.51 (or earlier) release for Windows 2000, the DHCP database must be converted to the new database format. The Windows 2000 database uses an improved database engine that is faster and compacts automatically to prevent fragmentation and consequent growth of the database. The database conversion procedure happens automatically as part of an upgrade installation.

When the DHCP service first starts after an upgrade to Windows 2000, it detects that the database needs to be converted. It then starts a conversion process by running a program called Jetconv.exe. The DHCP service stops and the conversion begins. Jetconv.exe finds and converts the databases for all of the installed services (DHCP and, if installed, WINS) to the new Windows 2000 database format.

After the DHCP database is converted successfully, the DHCP service is automatically restarted.

> **Note** Prior to upgrading to Windows 2000, bring any Windows NT 3.51 or 4.0 databases for the DHCP server up to a consistent state. Do this by terminating the services, either by using the **Service** utility in Control Panel or by using the **net stop service** command. This is recommended because it prevents the Jetconv.exe conversion from failing due to an inconsistent

Windows NT 3.51 or 4.0 database.

The conversion requires approximately the same amount of free disk space as the size of the original database and log files. You should have at least 5 MB free for the log files for each database.

The conversion process preserves the original database and log files in a subdirectory named 351db (if from Windows NT 3.51) or 40db (if from Windows NT 4.0) under the same directory where the original database and log files were located. On a DHCP server, this is the *%SystemRoot%*\System32\Dhcp*version*db directory. The administrator can later remove these files to reclaim the disk space.

The database conversion can take anywhere from a minute to an hour depending on the size of the database. The user must not restart the services while the databases are being converted. To check the status of the conversion, use Event Viewer to watch the application event log of the Jetconv.exe process.

In case this automatic procedure of converting databases fails for some reason (as can be determined from the event logs), the database that could not be converted can be converted manually using *%SystemRoot%*\System32*upgversiondb*.exe.

The new database engine uses log files named by using the prefix J50.

Warning You cannot convert the new database back to the previous database format. The converted database does not work with Windows NT 3.51 or earlier versions of DHCP services.

Configuring DHCP

The primary tool that you use to manage DHCP servers is DHCP Manager—a Microsoft Management Console (MMC) component that is added to the **Administrative Tools** menu when you install the DHCP service.

After you install a DHCP server, you can use DHCP Manager to:

- Define scopes, superscopes, and multicast scopes, including exclusion and reservation ranges.
- Activate scopes or superscopes.
- Monitor scope leasing activity.
- Define custom, default DHCP option types.
- Configure user-defined or vendor-defined option classes.
- Define other DHCP server properties, such as audit logging or BOOTP tables.

DHCP Manager also provides enhanced server performance monitoring, predefined DHCP option types, dynamic update support for clients using earlier versions of DHCP, and detection of unauthorized (rogue) DHCP servers on your network.

You can also define:

Enhanced Monitoring and Statistical Reporting

Enhanced monitoring and statistical reporting provide notification when the number of IP addresses available for lease is below a user-defined threshold. For example, an alert can be triggered when 90 percent of IP addresses in a particular scope have been assigned. A second alert can be triggered when the pool of IP addresses is exhausted.

User-Specified and Vendor-Specified Option Classes

The DHCP service for Windows 2000 allows user-specified and vendor-specified options to be defined as an alternative to the potentially lengthy process of obtaining IETF approval for a new standard option.

Integration of DHCP with DNS

DHCP servers can enable dynamic updates in the DNS namespace for any of its clients that support these updates. This feature allows scope clients to use dynamic updates to update their computer name–to–address mapping information (which is stored in zones on the DNS server) when changes occur to their DHCP-assigned address.

Rogue DHCP Server Detection

The DHCP service for Windows 2000 is designed to prevent rogue DHCP servers from creating address assignment conflicts. This solves problems that can occur because of unauthorized DHCP servers assigning improper or unintended IP addresses to clients elsewhere on the network.

Preventing Rogue DHCP Servers

The process of authorizing DHCP servers is useful or needed for DHCP servers running Windows 2000 Server. Where this scheme is used, authorization is neither used nor needed if the following conditions exist:

- If DHCP servers are running earlier versions of Windows NT Server, such as versions 3.51 or 4.0.
- If DHCP servers are running other DHCP server software.

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.

Most commonly, there will be only one enterprise root and therefore only a single point for directory authorization of the DHCP servers. However, there is no restriction on authorizing DHCP servers for more than one enterprise root.

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 a rogue DHCP server starts, it can begin leasing incorrect IP addresses to clients or negatively acknowledging DHCP clients attempting to renew their current address lease.

Either of these misconfiguration problems can produce further problems for DHCP-enabled clients. For example, clients that obtain a configuration lease from the unauthorized server can then fail to locate valid domain controllers, preventing clients from successfully logging on to the network.

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.

This support uses an additional object type (the DhcpServer object) to the base directory schema. This provides for the following enhancements:

- A list of IP addresses available for the computers that you authorize to operate as DHCP servers on your network.
- Detection of rogue DHCP servers and prevention of their starting or running on your network.

Note For the directory authorization process to work properly, it is necessary that the first Windows 2000 DHCP server introduced onto your network participate in the Active Directory service. This requires that the server be installed in a domain (as either a domain controller or a member server), and not in a workgroup. When you are either planning for or actively deploying Active Directory services, do not elect to install your first DHCP server as a workgroup server. You must have enterprise

administrator rights to authorize a DHCP server in the Active Directory.

How DHCP Servers Are Authorized

The authorization process for DHCP server computers in Active Directory depends on the 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:

- **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.
- **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 database.
- **Stand-alone Server.** The computer is not operating as a domain controller or a members 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 or start providing DHCP service to clients. When a DHCP server is authorized, the server computer is added to the list of authorized DHCP servers maintained in the directory service database.

How Unauthorized Servers Are Detected

The DHCP implementation under Windows 2000 Server provides detection of both authorized and unauthorized DHCP servers in two ways:

- The use of information messaging between DHCP servers using the DHCPInform message.
- The addition of several new vendor-specific option types, used for communicating information about the directory service enterprise root.

The Windows 2000 DHCP service uses the following process to detect other DHCP servers currently running on the reachable network and determine if they are authorized to provide service.

When the DHCP service starts, it sends a DHCPInform request message to the reachable network, using the local limited broadcast address (255.255.255.255), to locate the directory service enterprise root on which other DHCP servers are installed and configured.

This message includes several vendor-specific option types that are known and supported by other DHCP servers running Windows 2000 Server. When received by other DHCP servers, these option types provide for the query and retrieval of information about the directory service enterprise root.

When queried, other DHCP servers reply with DHCPAck messages to acknowledge and answer with directory service enterprise root information. In this way, the initializing DHCP server collects and compiles a list of all currently active DHCP servers on the reachable network, along with the root of the directory service enterprise used by each server.

Typically, only one single enterprise root is detected: the same one for all DHCP servers that are reachable and that respond to acknowledge the initializing server. However, if additional enterprise roots are detected, each root is queried in turn to see if the computer is authorized for DHCP service for those other enterprises discovered during this phase.

After a list is built of all DHCP servers running on the network, the next step in the detection process depends on whether a directory service is available from the local computer.

If the directory service is not available (such as where the initializing DHCP server is installed in a confined network environment used for testing), the initializing server can start if no other DHCP servers are discovered on the network that are part of any enterprise. When this condition is met, the server successfully initializes and begins serving DHCP clients.

However, the server continues every 5 minutes to collect information about other DHCP servers running on the network, using DHCPInform as it did at startup. Each time, it checks to see whether the directory service is available. If a directory service is found, the server makes sure it is authorized by following the procedure, depending on whether the server is a member server or a stand-alone server.

- For member servers (a server joined to some domain that is part of the enterprise), the DHCP server queries the directory service for the DHCP server list of addresses that are authorized.
- If the server finds its IP address in the authorized list, it initializes and starts providing DHCP service to clients. If it does not find itself in the authorized list, it does not initialize, and stops providing DHCP services.
- For stand-alone servers (a server not joined to any domain or part of an existing enterprise), the DHCP server queries the directory service with the root of the enterprise returned by each of the other DHCP servers to see if it can find itself on the authorized list with any of the reported enterprises.

  The server initializes and starts providing DHCP services to clients only if the server finds its IP address in the authorized list for each of the enterprise roots reported by other DHCP servers. If it does not find itself in the authorized list for each of the reported enterprise roots, it does not initialize, and the DHCP service is stopped.

Clustering DHCP Servers

Windows Clustering allows two servers to be managed as a single system. The Windows 2000 (Advanced Server only) clustering service can be used for DHCP servers to provide higher availability, easier manageability, and greater scalability.

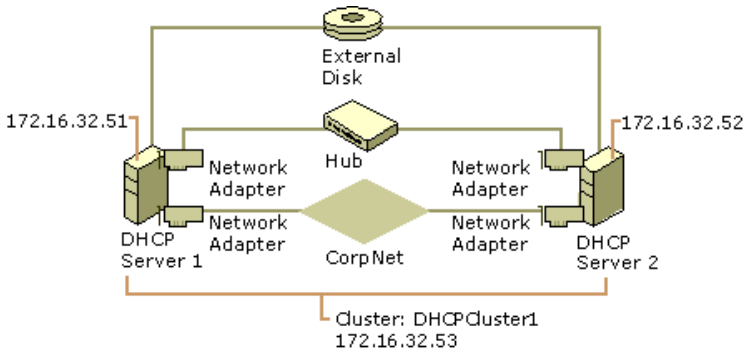
Windows Clustering can automatically detect the failure of an application or server and quickly restart it on a surviving server, with users only experiencing a momentary pause in service. With Windows Clustering, administrators can quickly inspect the status of all cluster resources and easily move workloads around onto different servers within the cluster. This is useful for manual load balancing and for performing rolling updates on the servers without taking important data and applications offline.

Windows Clustering allows DHCP servers to be virtualized so that if one of the clustered nodes crashes, the namespace and all the services are transparently reconstituted to the second node. This means no changes are visible to the client, which sees the same IP address for the clustered DHCP servers.

Without clustering, network administrators might split scopes between servers, so if one server goes down, at least half of the available addresses remain available. Clustering uses IP addresses efficiently by removing the need to split scopes. A database stored on a remote disk tracks address assignment and other activity so that if the active cluster node goes down, the second node becomes the DHCP server, with complete knowledge of what has been assigned and access to the complete scope of addresses. Only one node at a time runs as a DHCP server, with the Windows 2000 clustering database providing transparent transition when needed.

Example of Clustered DHCP Servers

Figure 4.15 is a generic example of clustered DHCP servers. DHCP Server 1 is the active DHCP server, and DHCP Server 2 is the backup DHCP server.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.15 Clustered DHCP Servers

In Figure 4.15:

- DHCP Server 1 and DHCP Server 2 have Windows 2000 DHCP and Windows Clustering services installed.
- Each DHCP server has a unique server name and IP address.
- Each DHCP server has two network interfaces—one for the cluster identity and the connection to the enterprise network and the second for server-to-server communication. This is a private link only for cluster communication. The wire runs directly between the two servers.
- Both DHCP servers are configured with identical scopes. However, on Server 2, the scopes are not activated because Server 2 is not currently functioning as the active DHCP server. DHCP Server 2 can function as a hot spare, ready in the event of a shutdown of DHCP Server 1.
- To facilitate clustering and the sharing of resources, the DHCP servers are connected to an external disk system that holds the DHCP database and log files. This allows DHCP Server 2 to access the DHCP database files if it needs to take over as the active DHCP server. The clustering service installed on each DHCP server prevents one server from trying to exclusively claim the external disk and prevent sharing of the disk system between the DHCP servers.
- The cluster itself has a unique name and IP address, so that DHCP clients can use the cluster name and IP address to connect to the cluster and request DHCP services. This prevents rejected DHCP client requests if one of the DHCP servers is turned off. For example, if the client was configured with a specific DHCP server name and IP address instead of the cluster address, the client would not receive DHCP services. However, by configuring the DHCP clients with the cluster name and IP address, the client is able to communicate with the active DHCP server in the cluster.

Before implementing a similar scenario, consider the following recommendations:

- On each DHCP server in the cluster (whether backup or primary), install the DHCP service before you install the clustering service.
- Keep the second DHCP server turned off until the first server has the clustering service installed and is configured with a new cluster name and address. When the second server is turned on (and configured with DHCP and clustering services), it joins the existing cluster.
- The cluster name and IP address must be statically configured—they cannot be configured dynamically by another DHCP server.
- If a DHCP cluster is using an external disk system to store the DHCP database files, the DatabasePath and BackupDatabasePath registry entries must be configured on both DHCP servers in the cluster. The registry entries are located in

  HKLM\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters

  These registry entries must specify the path to the external disk system.
- Permissions: Any backup DHCP servers in the cluster will not be able to successfully take over DHCP tasks if the appropriate security permissions have not been enabled. Administrators must create a new domain security group to which the servers belong. This group must have permissions of Full Control for the DNS zone object in Active Directory where DHCP clients have their A and PTR records registered and updated. Alternatively, administrators can add the second server to the DNSUpdateProxyGroup for the domain. Otherwise, name resolution failures will result.
- Use the 80/20 rule when implementing clustered DHCP servers to provide additionally enhanced “failover” (hot-spare) services. The combination of clustering DHCP servers and using the 80/20 rule to manage scopes between the clustered server enables an enhanced failover solution. See the sections “80/20 Rule” and “Best Practices” for details in specifying scopes using the 80/20 rule.

For more information, see “Windows Clustering” in the *Microsoft® Windows® 2000 Distributed Systems Guide*.

DHCP Scenarios

The following sections discuss common DHCP deployment scenarios and issues.

DHCP in Small Networks

A single DHCP server can be used on a small LAN that does not include routers and subnetting. An example layout of a small network is shown in Figure 4.16.

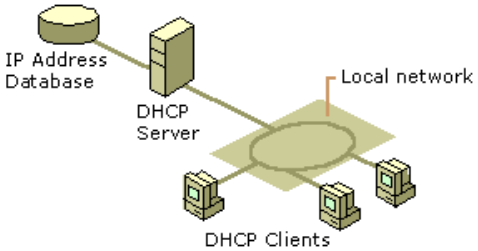


Figure 4.16 A Single Local Network Using Automatic TCP/IP Configuration with DHCP

Before installing a DHCP server computer on a small network, you need to identify:

- The hardware and storage requirements for the DHCP server.

- Which computers can be configured as DHCP clients for dynamic TCP/IP configuration and which computers should be manually configured with static TCP/IP configuration parameters, including static IP addresses.
- The predefined DHCP option types and their values.

DHCP in Large Networks

For an enterprise network, you should:

- Plan the physical subnets of the network and relative placement of DHCP servers. This includes planning for placement of DHCP (and WINS) servers among subnets in a way that reduces b-node broadcasts across routers.
- Specify the DHCP option types and their values to be predefined per scope for the DHCP clients. This can include planning for scopes based on the needs of particular groups of users. For example, for a unit that frequently moves computers to different locations, shorter lease durations can be defined for the related scopes. This approach collects IP addresses that are changed frequently and disposed of, and returns them to the pool of available addresses that can be used for new lease offerings.
- Recognize the impact that slower links have on your WAN environment. Place DHCP, WINS, and DNS servers to maximize response time and minimize low-speed traffic.

As one example of planning for a large enterprise network, the segmenting of the WAN into logical subnets can match the physical structure of the internetwork. Then one IP subnet can serve as the backbone, and off this backbone each physical subnet maintains a separate IP subnet address.

DHCP in Routed Networks

In routed networks that use subnets to divide network segments, administrators must observe some specific requirements for a full implementation of DHCP services to function. These requirements include one of the following:

- One DHCP server must be located on at least one subnet in the routed network.
- For a DHCP server to support clients on other remote subnets separated by routers, a router or remote computer must be used as a DHCP/BOOTP relay agent to support forwarding of DHCP traffic between subnets.

Figure 4.17 illustrates an example of a routed network with a DHCP server and DHCP clients.

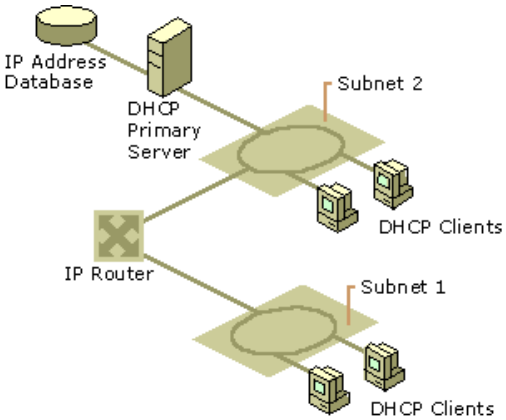


Figure 4.17 An Internetwork Using Automatic TCP/IP Configuration with DHCP

As explained earlier, routers that implement the DHCP/BOOTP relay agent can be used to route traffic between DHCP servers and clients located on different subnets. The relay agent on the router forwards requests from local DHCP clients to the remote DHCP server and subsequently relays the DHCP server responses back to the DHCP clients.

Relay Agent Deployment

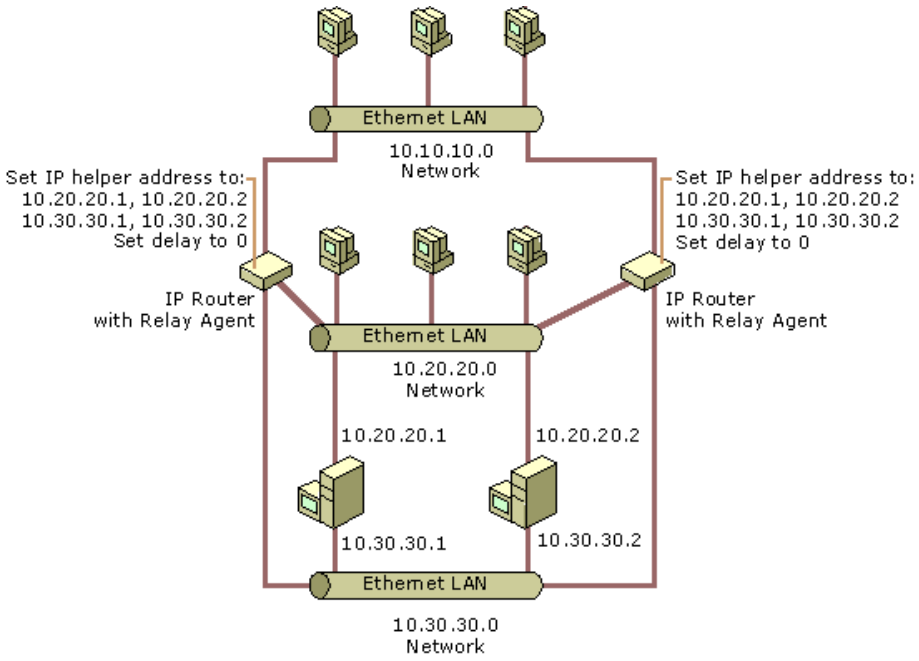
When you have multiple DHCP servers, Microsoft recommends that you place your DHCP servers on different subnets to achieve a degree of fault tolerance, rather than having all the DHCP servers in one subnet. The servers should not have common IP addresses in their scopes (each server should have a unique pool of addresses).

If the DHCP server in the local subnet shuts down, requests are relayed to a remote subnet. The DHCP server at that location can respond to DHCP requests if it maintains a scope of IP addresses for the requesting subnet. If the remote server has no scope defined for the requesting subnet, it cannot provide IP addresses even if it has available addresses for other scopes. If each DHCP server has a pool of addresses for each subnet, it can provide IP addresses for remote clients whose own DHCP server is offline.

There are several relay agent configuration options available if you plan to incorporate a relay agent into your DHCP/BOOTP-enabled network. These include using third-party routers, Windows 2000 Routing and Remote Access, and the DHCP Relay Agent component provided in Windows NT Server 4.0. For more information about how relay agents work, see the section “Managing Relay Agents” later in this chapter.

Recommended General Configuration

Figure 4.18 shows a recommended relay agent implementation, which provides for the best network performance.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.18 Windows 2000 Recommended Relay Agent Configuration

This figure illustrates a general configuration for relay agents. For specific scenarios, see the following sections and illustrations.

Windows 2000 Server Routing and Remote Access Relay Agents

Figure 4.19 shows the Windows 2000 Server Routing and Remote Access configuration. In this example, the Windows 2000 server is acting as an IP router between Subnet 1 and 2, as well as a relay agent between the DHCP server on Subnet 1 and the DHCP clients on Subnet 2.

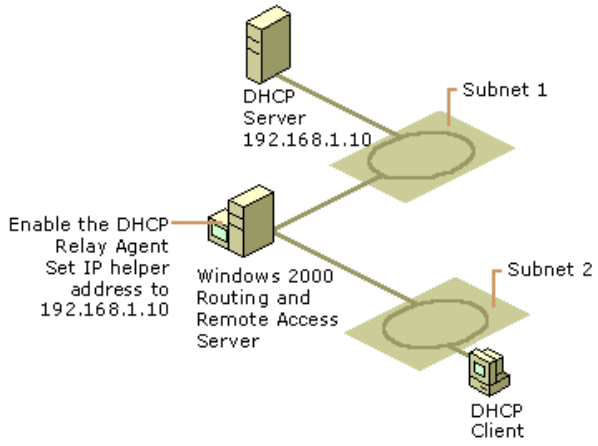


Figure 4.19 Windows 2000 Remote Access Server as a Relay Agent

The DHCP Relay Agent on the Windows 2000 server must be configured with the IP address of the DHCP server to relay DHCP requests between Subnet 1 and Subnet 2.

Windows NT Server 4.0 Relay Agents

Figure 4.20 shows a standard router configuration.

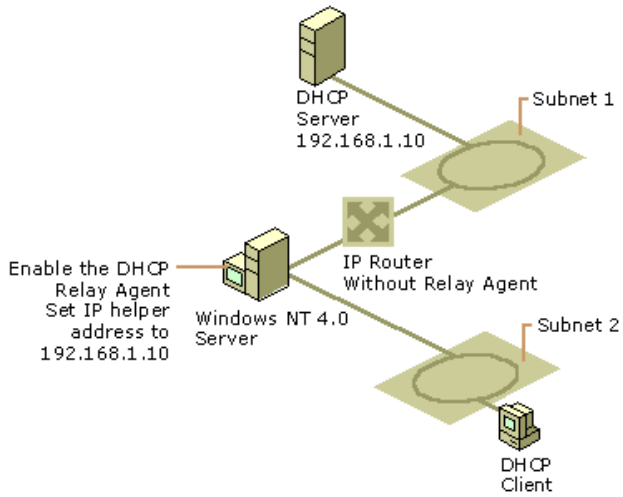


Figure 4.20 Standard Router as a Relay Agent

This example shows how a standard IP router can be implemented on a network, in combination with a Windows NT Server 4.0 relay agent relaying DHCP requests between Subnet 1 and Subnet 2.

DHCP and Routing and Remote Access

The DHCP service can be deployed along with Routing and Remote Access to dynamically provide remote access clients with IP addresses during a dial-up connection. When Routing and Remote Access and DHCP are used together on the same server computer, the information provided during dynamic configuration is provided differently from that provided under the normal DHCP configuration for LAN-based clients.

When a remote access server provides dynamic configuration for dial-up clients, the remote access server first performs the following steps before the client is assigned DHCP lease information:

- When the remote access server starts with the **Use DHCP to assign remote TCP/IP addresses** option, it makes advance requests to the DHCP server to obtain DHCP client addresses for dial-up clients, and caches these addresses.
- The number of client addresses that are requested in advance is equal to the number of Routing and Remote Access ports set to receive calls, plus one additional address.

For example, if the remote access server has two analog modem ports and two ISDN adapter ports that are set to receive calls, the remote access server requests a total of five IP addresses from the DHCP server. The first four are for assigning to remote access clients that dial into the Routing and Remote Access ports. The fifth address is reserved for the remote access server computer, to configure and use as its own IP address when processing connections for dial-up clients.

When the remote access server uses this type of proactive caching of DHCP address leases for dial-up clients, it records the following information for each lease response it obtains from the DHCP server:

- The IP address of the DHCP server.
- The client's leased IP address (for later distribution to the remote access client).
- The time at which the lease was obtained.
- The time at which the lease expires.
- The length of the lease.

All other DHCP option information returned by the DHCP server (such as server global, scope, or reserved client options) is discarded. When the client dials into the remote access server and requests an IP address (that is, **Server Assigned IP Address** is selected), the remote access server uses one of these cached leases to provide the remote access client dynamic IP address configuration. When the IP address is provided to the remote access client, the client is unaware that the IP address has been obtained through this intermediate communication between the DHCP server and remote access server. The remote access server maintains the lease on behalf of the client. Therefore, the only information that the client receives from the DHCP lease is the IP address.

DHCP and WINS

WINS is a naming service used to register and resolve name-to-address mappings for NetBIOS clients on TCP/IP-based networks.

Because NetBIOS naming is a required feature for networking that is supported in all previous versions of Windows, install and use WINS if you are operating the Windows 2000 DHCP service in a network environment that includes DHCP clients running under any of the following earlier Microsoft operating systems:

- Windows for Workgroups 3.11
- Windows 95
- Windows NT Advanced Server 3.1
- Windows NT 3.5*x*
- Windows NT 4.0
- MS-DOS client for Microsoft Networks

In many cases, it is not necessary to add WINS servers beyond the number of servers that are planned for DHCP server usage. In many cases, the same server computer can work effectively as both the WINS and DHCP server for a single internet on your network.

Where a single server is configured as both a WINS server and a DHCP server, it can:

- Administer a defined scope or superscope range of IP addresses for your network.
- Serve as the default gateway to provide IP forwarding between adjoining physical networks.

  To set the same default gateway for all DHCP clients located across subnets, assign DHCP option code 3 by using the server computer's IP address as the value in configuring the DHCP scope options.
- Serve as the primary WINS server for adjoining physical networks.

To set the WINS server for all DHCP clients located across subnets, assign DHCP option code 44 (a list of IP addresses for WINS servers) and use the server computer's IP address as the value.

To ensure that WINS is used first by all DHCP clients for NetBIOS name resolution (before broadcast name resolution is tried), assign option code 46 (WINS/NBT node type) to identify the WINS node type as h-node (hybrid node).

Adding Fault Tolerance to DHCP/WINS Service

To create a more fault-tolerant installation for DHCP and WINS, you can set up two server computers running Windows 2000 Server to act as backup service providers for each other. Table 4.12 shows the functions of each server (Server1 and Server2) when configured in this way.

Table 4.12 DHCP/WINS servers

Computer Name	WINS Server Status	DHCP Server Status
Server1	Primary WINS	Secondary DHCP
Server2	Secondary WINS	Primary DHCP

If you want to create a primary and backup relationship between DHCP servers, you can partition the address pool so that each server provides addresses to remote clients. One recommended practice is to allocate approximately 75 percent of the available IP address pool for your network to the primary DHCP server and the remaining 25 percent of your address pool to the backup DHCP server.

When defining a shared scope between two DHCP servers, you must ensure that the scope is configured to be disjointed (with no overlap) for each server, to avoid duplicating IP addresses in lease offerings for both servers.

Additional Recommendations

When using DHCP and WINS together on your network, consider the following options for interoperation:

Use additional DHCP scope options.

Use DHCP options to assign WINS node types (option type 46) and to identify WINS servers for use by DHCP clients (option type 44). In some cases, this can involve adjusting these option types for each physical subnet where DHCP and WINS are implemented.

Assign a length of time for DHCP lease durations comparable to the time WINS uses for renew intervals.

By default, DHCP leases are eight days in length and the WINS renew interval is six days. If lease lengths for DHCP differ widely from WINS renew intervals, the effect on your network can be an increase in lease-management traffic and might cause a WINS registration for both services. If you shorten or lengthen the DHCP lease time for clients, modify the WINS renew interval accordingly.

Configure all installed connections as routable interfaces.

Windows 2000 does not guarantee the binding order for NetBIOS when more than one connection is present and active. All multihomed WINS servers should have their primary IP addresses assigned to each network connection. When configuring a replication partner with the multihomed server as a push or pull partner, you can ensure that the partner always connects to the same adapter on the multihomed server by configuring the partner to refer to the multihomed server using the specific IP address to which you want the partner to connect. If the partner is configured to refer to the name of the multihomed server instead of a specific IP address, when the replication partner resolves the name to an IP address, it may end up sending WINS packets to the multihomed server using any of its IP addresses.

DHCP and DNS

Domain Name System (DNS) servers provide name resolution for network clients. DNS maintains (among other things) information that links a computer's fully qualified domain name (FQDN) to its assigned IP address(es).

While 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 nor provide a mapping from the new IP address to the computer name (FQDN).

In Windows 2000, DHCP servers and clients can register with DNS to provide this update service if the DNS server supports DNS with dynamic updates. The Windows 2000 DNS service supports dynamic updates. For more information, see the chapter "Windows 2000 DNS" in this book

A Windows 2000 DHCP server can register with a DNS server and update pointer (PTR) and address (A) resource records on behalf of its DHCP-enabled clients using the DNS dynamic update protocol.

The ability to register both A and PTR type records lets a DHCP server act as a proxy for clients using Microsoft 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 resource records 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 DHCPRequest 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, do the following steps:

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.

Wherever possible, upgrade or replace older, static-based DNS servers with DNS servers supporting updates. Dynamic updates are supported by the Microsoft DNS service, included in Windows 2000.

Additional Recommendations

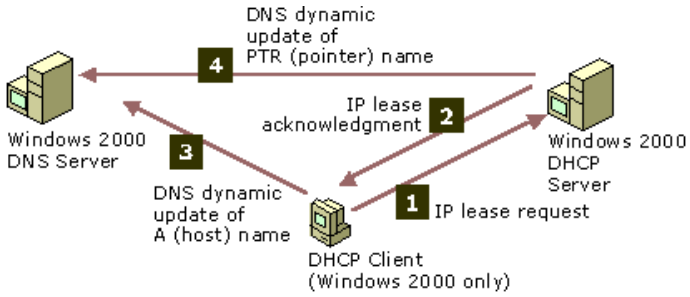
When using DNS and WINS together, consider the following options for interoperation:

- 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. For more information, see “Windows Internet Name Service” and “Windows 2000 DNS” in this book.

Windows-Based DHCP Clients and DNS with Dynamic Updates

Windows 2000 DHCP clients and earlier versions of Windows DHCP client interact with DNS in different ways. The DHCP server can be configured to always register the DHCP client for both the forward (A-type records) and reverse (PTR-type records) lookups with DNS. Windows 2000 DHCP clients update their own dynamic forward lookup names.

Figure 4.21 shows how Windows 2000 DHCP clients interact with dynamic updates:



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.21 Windows 2000 DHCP Clients and Dynamic Updates

1. The Windows 2000 DHCP client makes an IP lease request.
2. The DHCP server grants an IP lease.
3. The Windows 2000 DHCP client updates its forward (A) name with the DNS server.
4. The DHCP server updates the DNS reverse (PTR) name for the client using the dynamic update protocol.

Earlier versions of Windows DHCP clients do not interact directly with DNS server that perform dynamic updates. Figure 4.22shows how the forward and reverse lookup names are updated by a DHCP server:

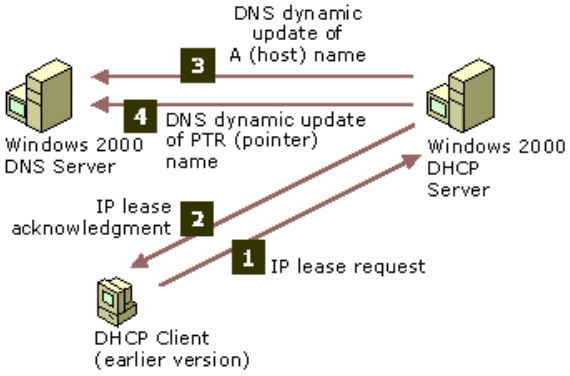


Figure 4.22 Older DHCP Clients and Dynamic Updates

1. The DHCP client makes an IP lease request.
2. The DHCP server grants an IP lease.
3. The DHCP server automatically generates the client’s FQDN by appending the domain name defined for the scope to the client name obtained from the DHCPRequest message sent by the older client.
4. Using the dynamic update protocol, the DHCP server updates the DNS forward (A) name for the client.
5. Using the dynamic update protocol, the DHCP server updates the DNS reverse (PTR) name for the client.

DHCP and Automatic Private IP Addressing

Windows 2000 and Windows 98 provide Automatic Private IP Addressing (APIPA), a service for assigning unique IP addresses on small office/home office (SOHO) networks without deploying the DHCP service. Intended for use with small networks with fewer than 25 clients, APIPA enables Plug and Play networking by assigning unique IP addresses to computers on private local area networks.

APIPA uses a reserved range of IP addresses (169.254.*x*.*x*) and an algorithm to guarantee that each address used is unique to a single computer on the private network.

APIPA works seamlessly with the DHCP service. APIPA yields to the DHCP service when DHCP is deployed on a network. A DHCP server can be added to the network without requiring any APIPA-based configuration. APIPA regularly checks for the presence of a DHCP server, and upon detecting one replaces the private networking addresses with the IP addresses dynamically assigned by the DHCP server.

Multihomed DHCP Servers

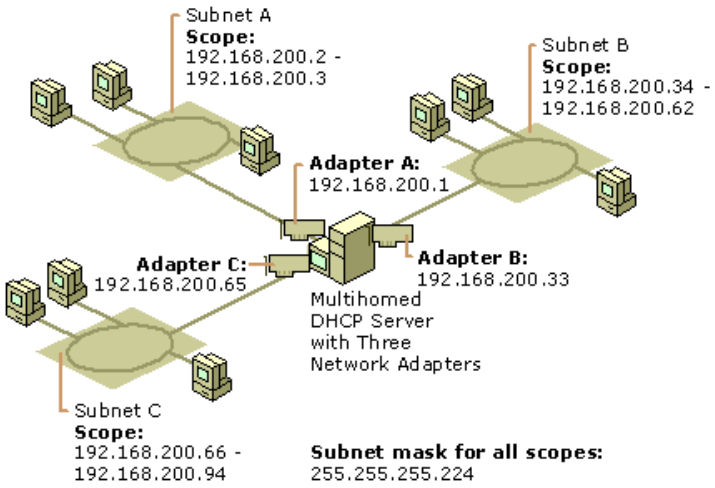
For a server computer to be multihomed, each network connection must attach the computer to more than one physical network. This requires that additional hardware (in the form of multiple installed network adapters) be used on the computer.

A computer running Windows 2000 Server can function as a multihomed DHCP server. The DHCP server binds to the first IP address configured on each network connection (that is, each physical adapter interface) in use on the server. By default, the service binding depends on whether the connection is dynamically or statically configured for TCP/IP. If statically, the connection is enabled in the binding to listen to and provide service to DHCP clients. If dynamically, it is disabled in service bindings and does not provide service to DHCP clients. Dynamic configuration methods include the use of either another DHCP server to obtain a leased IP configuration or self-configuring an address through the use of the APIPA feature provided in Windows 2000. For more information, see “DHCP and Automatic Private IP Addressing” earlier in this chapter.

Server scopes use the primary IP address for each multihomed network connection to communicate with the DHCP clients. To verify the primary IP address for each of the connections used in a multihomed server configuration, you can review the Internet Protocol (TCP/IP) properties for each connection listed in the Network and Dial-up Connections folder on the server.

Configuring a Multihomed DHCP Server

Figure 4.23 is an example of a multihomed DHCP server with three network adapters installed. Each adapter is configured to lease addresses on separate physical subnets.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4.23 Multihomed DHCP Server Configuration

The multihomed DHCP server has three adapters installed and configured statically with a single IP address for each. Because the IP addressing for the DHCP server also uses an adjusted or custom subnet mask value (255.255.255.224), that value is applied for all the IP addresses that are configured at the server and for other computers in use on the same network. Here, a Class C range of IP addresses, 192.168.200.1 to 192.168.200.254, is used.

Each of the three adapters connects the server to three different physical subnets (Subnets A, B and C). To achieve the intended results of having the DHCP server provide leased configuration service to all clients in each of the respective subnets, two configuration details are essential and must be verified during deployment plans:

1. The server must use a statically configured IP address within the same range of valid IP addresses for the physical network on which it is servicing clients.
2. The server must have each of its valid subnet IP addresses excluded from the scope used to offer leases to clients.

For example, if no special subnetting was used in this environment, the selection of DHCP server IP addresses is not as critical because the IP network and IP subnet are the same. When the default subnet mask value (255.255.255.255) for this example network is applied and in use, all 254 possible computer IDs are considered part of one single unified subnet.

If, however, a custom subnet mask of 255.255.255.224 is applied, the network ID and subnet ID are not the same. When the subnet ID is not the same as the network ID, make sure the DHCP server is provided an IP address assignment within the same subnet it is meant to service.

For instance, with the mask set to 255.255.255.224 at all computers, the first 3 bit places of the last notated octet (224) are taken from the full 8 bit places that would normally comprise the full computer ID section. These bits are used by IP for physical subnet identification. This leaves the remaining 8 bit places to be used as the actual or reduced computer ID field.

In this way, the example network shown above requires of the three subnets in use that they have a maximum of eight (or 2^3) potentially different subnet IDs. Likewise, each of these subnets can, in turn, only support up to 32 (or 2^5) potential computer IDs.

Because of the use of subnetting, Subnet A in this example consists of the first 32 address values in the network, from 0 to 31. Because no computer IDs consisting of all 0s or all 1s in the computer ID field can be assigned for use to computers, the useful range of total available IP addresses for each subnet drops from 32 to 30.

Of the remaining 30 addresses, the DHCP server needs to use one. The remaining 29 can be configured in a regular DHCP scope and used for assigning leases to subnet clients. The choice of which address to use for the DHCP server is at the administrator’s preference, as well as the decision to either include the DHCP server’s statically assigned IP address within the scope defined for use in each subnet.

The multihomed server’s IP addresses (192.169.200.1, 192.168.200.33, 192.168.200.65) are configured using the first IP address available for use in each of the three subnets. For the configuration shown, these addresses are excluded from the defined boundaries of each of the scopes created for use with these subnets.

Alternatively, you can set up your scopes to include these addresses within the defined boundaries of the scope. If you do, you need to create address exclusions to exclude these server IP addresses from each of the respective scopes.

If more than a single IP address is statically configured for a network connection, the Windows 2000 DHCP Server service permits only the first configured IP address to be used in the context of enabling or disabling service bindings.

Managing Relay Agents

A relay agent is a small program that relays a certain type of message to other hosts on a network. In TCP/IP networking, routers are used to interconnect hardware and software on different subnets and forward IP packets between the subnets.

To support and use the DHCP service across multiple subnets, routers connecting each subnet should comply with the DHCP/BOOTP relay agent capabilities described in RFC 1542. To comply with RFC 1542 and provide relay agent support, each router must be able to recognize BOOTP and DHCP protocol messages and process (relay) them appropriately. Because routers interpret DHCP messages as BOOTP messages (such as a UDP message sent through the same UDP port number and containing shared message structure), a router with BOOTP–relay agent capability typically relays DHCP packets and any BOOTP packets sent on the network.

In most cases, routers support DHCP/BOOTP relay. If your routers do not, contact your router manufacturer or supplier to find out if a software or firmware upgrade is available to support this feature.

Alternatively, if a router cannot function as a DHCP/BOOTP relay agent, each subnet must have either its own DHCP server or another computer that can function as a relay agent on that subnet.

In cases where it is impractical or impossible to configure routers to support DHCP/BOOTP relay, you can configure a computer running Windows 2000 or Windows NT Server 4.0 to act as a relay agent by installing the DHCP Relay Agent service. A DHCP relay agent is a hardware device or software program that can pass DHCP/BOOTP broadcast messages from one subnet to another subnet according to the RFC 2131 specification for DHCP. DHCP/BOOTP relay agents act as proxies, forwarding messages from one subnet to the next. By default, DHCP is a broadcast-based protocol, so without relay agents and the ability to pass DHCP and BOOTP messages across routers, every subnet on a network must have its own DHCP server.

How Relay Agents Work

Figure 4.24 shows how Client C on Subnet 2 obtains a DHCP address lease from DHCP Server 1 on Subnet 1.

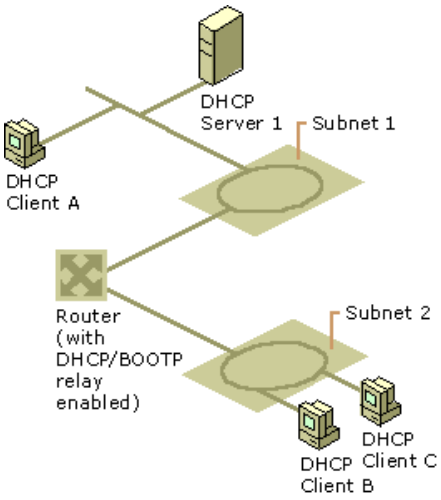


Figure 4.24 Using a Relay Agent

1. DHCP Client C broadcasts a DHCP/BOOTP discover message (DHCPDiscover) on Subnet 2, as a User Datagram Protocol (UDP) datagram using the well-known UDP server port of 67 (the port number reserved and shared for BOOTP and DHCP server communication).
2. The relay agent, in this case a DHCP/BOOTP relay-enabled router, examines the gateway IP address field in the DHCP/BOOTP message header. If the field has an IP address of 0.0.0.0, the agent fills it with the relay agent or router's IP address and forwards the message to the remote Subnet 1, where the DHCP server is located.
3. When DHCP Server 1 on remote Subnet 1 receives the message, it examines the gateway IP address field for a DHCP scope that can be used by the DHCP server to supply an IP address lease.
4. If DHCP Server 1 has multiple DHCP scopes, the address in the gateway IP address field (giaddr) identifies the DHCP scope from which to offer an IP address lease.

   For example, if the giaddr field has an IP address of 201.2.45.2, the DHCP server checks its available set of address scopes for a scope range of addresses that matches the Class C IP network that includes the gateway address of the computer. In this case, the DHCP server checks to see which scope includes addresses between 201.2.45.1 and 201.2.45.254. If a scope exists that matches this criterion, the DHCP server selects an available address from the matched scope to use in an IP address lease offer response to the client.
5. When DHCP Server 1 receives the DHCPDiscover message, it processes the message and sends an IP address lease offer (DHCPOffer) directly to the relay agent identified in the gateway IP address field (giaddr).
6. The router relays the address lease offer (DHCPOffer) to the DHCP client.

   The client's IP address is still unknown, so it has to be a broadcast on the local subnet. Similarly, a DHCPRequest message is relayed from client to server, and a DHCPAck message is relayed from server to client, according to RFC 1542.

Troubleshooting

This section contains methods for determining the cause of DHCP-related communication problems, and tools that can verify DHCP statistics and operations.

Many DHCP problems involve incorrect or missing configuration details. To help prevent the most common types of problems, review "Best Practices" for deploying and managing your DHCP servers.

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.

Using Ipconfig and Winipcfg

Ipconfig is a TCP/IP utility that you can use at the command prompt. You can use the **ipconfig** command to get information about the configured TCP/IP parameters on local or remote computers on the network.

For more information on how to use the **ipconfig** command, type **ipconfig /?** at a command prompt.

Winipcfg is a similar utility for Windows 95 and Windows 98 clients.

Troubleshooting DHCP Clients

The most common DHCP client problem is a failure to obtain an IP address or other configuration parameters from the DHCP server during startup. When a client fails to obtain configuration, answer the following questions in order to quickly identify the source of the problem.

DHCP client does not have an IP address configured or has an IP address configured as 0.0.0.0.

The client was not able to contact a DHCP server and obtain an IP address lease, either because of a network hardware failure or because the DHCP server is unavailable.

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.

DHCP client has an auto-configured IP address that is incorrect for its current network.

The Windows 2000 or Windows 98 DHCP client could not find a DHCP server and has used the Automatic Private IP Addressing (APIPA) feature to configure its IP address. In some larger networks, disabling this feature might be desirable for network administration.

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.

Next, 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.

Also, try releasing or renewing the client's address lease, and check the TCP/IP configuration settings on automatic addressing.

The 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.

For 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.

The 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 client's default gateway address, clients running Windows NT or Windows 2000 do not use the incorrect address. However, DHCP clients running Windows 95 use the incorrect address.

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

DHCP clients are unable to get IP addresses from the server.

This problem can be caused the following:

- 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:

  a. 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.

  b. 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.

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

  d. Use a default gateway on the network connection of the DHCP server in such a way that it is not using the same IP address as the router that supports the remote subnet where the clients are located.

  e. 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.

  f. Make sure there is only one logical route between the DHCP server and the remote subnet clients.

- Multiple DHCP servers exist on the same local area network (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

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 or the failure of clients to obtain configuration from a working server. When a server fails to provide leases to its clients, the failure most often is discovered by clients in one of three ways:

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

Common Problems

The following error conditions indicate potential problems with the DHCP server:

- The administrator can't connect to a DHCP server by using DHCP Manager. The message that appears might be "The RPC server is unavailable."
- DHCP clients cannot renew the leases for their IP addresses. The message that appears on the client computer is "The DHCP client could not renew the IP address lease."

- The DHCP client service or Microsoft DHCP service is stopped and cannot be restarted.

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 under an account with Administrator rights.
2. At the command prompt, type **net start dhcpserver**, and 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 provided with Multi-Protocol Routing (MPR) does not provide a TCP/IP address from a remote DHCP server.

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.

Install the DHCP service and the DHCP Relay Agent component on separate computers.

The 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 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\CurrentControlSet\Services\DHCPServer \Parameters**IgnoreBroadcastFlag**

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.

The DHCP server fails to issue address leases for a new scope

A new scope has been added at the DHCP server for the purposes 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 lease 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.

  If you cannot change the primary IP address assigned on the DHCP server's network adapter card, use superscopes to effect scope migration for DHCP clients on your network. Superscope support was added for Windows NT Server 4.0 with Service Pack 2 and is available for Windows 2000 Server. Superscopes provide ease and assistance in migrating DHCP scope clients. To effectively migrate clients from an old scope to a new scope using a superscope:

  a. Define the new scope.
  b. Assign and configure options for the new scope.
  c. Define a superscope and add the new scope and the old scope (that is, the scope that corresponds to the primary or first IP address assigned to the DHCP server on its **TCP/IP Properties** tab).
  d. Activate the superscope.
  e. Leave the original scope active and exclude all the addresses within that scope.

  After renumbering in this manner using superscopes, the DHCP server, upon receiving a renewal request:

  a. Checks to see if the client's IP address belongs to a scope it is aware of. Since the superscope includes the old scope, the server finds the scope and checks to see that this IP address has been marked as excluded.
  b. The server checks if the client lease exists in its database. Since this server previously allocated the lease to this client, it sends a DHCPNack in response to the renewal request.
  c. The client is forced to request a new address (the client broadcasts a DHCPDiscover message).

d. The server responds to the DHCPDiscover with a lease from the new scope.

The second step in this process (when the server checks the existence of the lease in its database), is what differentiates a renumbering scenario from a using multiple servers on the same subnet:

- If the server finds the lease in its database, it sends a DHCPNack to the renewal request.
- If the server does not find the lease, it ignores the renewal request.

For more information about using superscopes, see the section "Superscopes."

Note To migrate to the new scope, you can either deactivate the old scope or exclude all the addresses in the old scope. The server interprets both methods identically.

- 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 a 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 on 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.

DHCP System Monitor Counters

Table 4.13 provides a list of the DHCP system monitor counters and their meaning:

Table 4.13 DHCP System Monitor Counters

Name	Description
Packets Received/sec	The number of message packets received per second by the DHCP server. A large number indicates heavy DHCP-related message traffic to the server.
Duplicates Dropped/sec	The number of duplicated packets per second dropped by the DHCP server. A large number indicates clients are probably timing out too fast or the server is not responding very fast.
Packets Expired/sec	The number of packets per second that expire and are dropped by the DHCP server. Packets expire because they are in the server's internal message queue for too long. A large number here indicates that the server is either taking too long to process some packets while other packets are queued, or traffic on the network is too high for the DHCP server to handle.
Milliseconds per packet (Avg.)	The average time, in milliseconds, used by the DHCP server to process each packet it receives. This number can vary depending on the server hardware and its I/O subsystem. A sudden or unreasonable increase may indicate trouble, possibly with the I/O subsystem getting slower or because of some intrinsic processing overhead on the server computer.
Active Queue Length	The current length of the internal message queue of the DHCP server. This number equals the number of unprocessed messages received by the server. A large number may indicate heavy server traffic.
Conflict Check Queue Length	The current length of the conflict check queue for the DHCP server. This queue holds messages not responded to while the DHCP server performs address conflict detection. A large value here may indicate heavy lease traffic at the server or that **Conflict Detection Attempts** has been set too high.
Discovers/sec	The number of DHCPDiscover messages received per second by the server. A sudden or abnormal increase indicates that a large number of clients are probably attempting to initialize and obtain an IP address lease from the server, such as when a number of client computers are started at one time.
Offers/sec	The number of DHCPOffer messages sent per second by the DHCP server to clients. A sudden or abnormal increase in this number indicates heavy traffic on the server.
Requests/sec	The number of DHCPRequest messages received per second by the DHCP server from clients. A sudden or abnormal increase in this number indicates that a large number of clients are probably trying to renew their leases with the DHCP server. This may indicate scope lease times are too short.
Informs/sec	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 clients by the DNS server.
Acks/sec	The number of DHCPAck messages sent per second by the DHCP server to clients. A sudden or abnormal increase in this number indicates that a large number of clients are being renewed by the DHCP server. This may indicate scope lease times are too short.
Nacks/sec	The number of DHCP negative acknowledgment messages sent per second by the DHCP server to clients. A very high value might indicate potential network trouble, either misconfiguration of clients or the server. Where servers can be misconfigured, one possible cause is a deactivated scope. For clients, a very high value could be caused by computers (such as laptop portables or other mobile devices) moving between subnets.
Declines/sec	The number of DHCPDecline messages received per second by the DHCP server from clients. A high value indicates that several clients have found their address to be in conflict, possibly indicating network trouble. In this situation, it may help to enable conflict detection on the DHCP server. If used on the server, conflict detection should only be used temporarily. Once the situation returns to normal, it should be turned off.
Releases/sec	The number of DHCPRelease messages received per second by the DHCP server from clients. This number is only generated when clients manually release their address, such as when the **ipconfig /release** command

	is used at the client computer. Because clients rarely release their address, this counter should not be high for most networks and configurations.

DHCP Manager Statistical Data

The DHCP service, which supports Simple Network Management Protocol (SNMP) and Management Information Base (MIBs) object types, provides a graphical display of statistical data. This helps administrators monitor system status, such as the number of available versus depleted addresses, or the number of leases processed per second. Additional statistical information includes the number of messages and offers processed, as well as the number of requests, acknowledgments, declines, NACKS, and releases received.

Also viewable by DHCP Manager is the total number of scopes and addresses on the server, the number used, and the number available. These statistics can be provided for a particular scope, or at the server level, which shows the aggregate of all scopes managed by that server.

DHCP Audit Logging

The Windows 2000 DHCP service includes several new logging features and server parameters that provide enhanced auditing capabilities.

The audit logging behavior discussed in this section applies only to the DHCP service provided with Windows 2000 Server. It replaces the previous DHCP logging behavior used in earlier versions of Windows NT Server, which do not perform audit checks and use only a single log file named Dhcpsrv.log for logging service events.

The formatted structure of DHCP service logs and the level of reporting maintained for audited logging are the same as in earlier versions of the Windows DHCP service. For more information on the structure of the logs, you can review the header section of each log in a text-editing program such as Notepad.

You can now specify the following features:

- The directory path in which the DHCP service stores audit log files.
- A maximum size restriction (in MB) for the total amount of disk space available for all the audit log files created and stored by the DHCP service.
- An interval for disk checking that is used to determine how many times the DHCP server writes audit log events to the log file before checking for available disk space on the server.
- A minimum size requirement (in MB) for server disk space that is used during disk checking to determine if sufficient space exists for the server to continue audit logging.

Through the **DHCP Properties** dialog boxes, you can specify:

- The directory path in which the DHCP server stores audit log files.
- A maximum size restriction (in megabytes) for the total amount of disk space available for all audit log files created and stored by the DHCP service.
- An interval for disk checking that is used to determine how many times the DHCP server writes audit log events to the log file before checking for available disk space on the server.
- A minimum size requirement (in megabytes) for server disk space that is used during disk checking to determine if sufficient space exists for the server to continue audit logging.

See the online documentation for procedural information about specifying these parameters.

Naming Audit Log Files

The name of the audit log file is based on the current day of the week, as determined by the server's current date and time.

For example, when the DHCP server starts, if the current date and time is Saturday, January 1, 1900, at 12:00:00 A.M. then the server's audit log file is named DhcpSrvLog.Sat.

Starting a Daily Audit Log

When the DHCP server starts or whenever a new day of the week occurs (when local time on the computer is 12:00 A.M.), the server writes a header message in the audit log file, indicating that logging started. Depending on whether the audit log file is a new or existing file, the following actions occur next:

- If the audit log file has existed without modification for more than 24 hours, it is overwritten.
- If the file has existed but was modified within the previous 24 hours, the file is not overwritten. New logging activity is appended to the existing file.

Disk Checks

After audit logging starts, the DHCP server performs disk checks at regular intervals to ensure the ongoing availability of server disk space and that the current audit log file does not become too large or that log-file growth is not occurring too rapidly.

The DHCP server performs a full disk check whenever either of the following conditions occurs:

- A set number of events are logged.
- The date changes on the server computer.

The interval that is used to determine the frequency of periodic disk checks is set for *n* number of logged events, where *n* is specified by the value of the registry entry **DhcpLogDiskSpaceCheckInterval**.

Each time a disk check is completed, the DHCP service checks to see if the server disk space is full. The disk is considered full if either of the following conditions is true:

- Disk space on the server computer is lower than the required minimum amount for DHCP audit logging. This is determined by the configured value of the **DhcpLogMinSpaceOnDisk** entry. The default is **20 MB**.
- The current audit log file is larger than one-seventh (1/7) of the maximum allotted space or size for the combined total of all audit logs currently stored on the server. This is determined by a value obtained by dividing the value of the **DhcpLogFilesMaxSize** entry by 7—the maximum number of potential audit log files that can be stored on the server computer. For example, if the **DhcpLogFilesMaxSize** entry is set to its default value of **7**, the largest size that the current audit file could reach is 1 MB.

If the disk is full, the DHCP server closes the current file and ignores further requests to log audit events until either 12:00 A.M. or until disk status is improved and the disk is no longer full.

Even if audit log events are ignored because of a full-disk condition, the DHCP server continues checking every *n* number of attempted log events to see if disk conditions on the server computer have improved. The number is set in the **DhcpLogDiskSpaceCheckInterval** entry. If subsequent disk checks determine that the required amount of server disk space is

available, the DHCP service reopens the current day's log file and resumes logging.

Ending a Daily Audit Log

At 12:00 A.M. local time on the server computer, the DHCP server closes the existing log and moves to the log file for the next day of the week. For example, if the day of the week changes at 12:00 A.M. from Wednesday to Thursday, the log file named DhcpSrvLog.wed is closed and the file named DhcpSrvLog.thu is opened and used for logging events.

Restoring Server Data

Restoring the DHCP server database can be useful if the database either becomes corrupted or lost. When this happens, Windows 2000 Server provides a progressive set of recovery and repair options for restoration of DHCP data on the server computer.

In troubleshooting data corruption problems, use the following steps to detect corruption and restore DHCP service.

- First, confirm that the source of data loss or corruption is with the DHCP server and perform preliminary diagnosis or repairs, such as compaction of the DHCP server database. Also, it is a good idea to verify that corruption is not related to other problems or conditions with hardware or software changes. Where data loss occurs, verify the server computer disk drives are operating properly. In most cases, database corruption first appears in the form of Jet database error messages in the System event log.
- Second, where repair fails, you can use simple recovery of the DHCP server from your available options for server backup. DHCP Manager provides a simple backup option to effectively back up the DHCP server database. You can also have other options for obtaining a backup copy of the database for use during restoration, such as from a recent tape backup of the server computer disk drives.
- Third, when simple data recovery options are not available or are tried but unsuccessful, you can also try advanced data recovery methods provided with the DHCP console and Windows 2000 Server to recover specific information related to individual scopes stored in the DHCP server database.

If you determine that the DHCP services are running on both the client and server computers but the error conditions described earlier under "Troubleshooting DHCP Servers" persist, then the DHCP database is not available or has become corrupted. If a DHCP server fails for any reason, you can restore the database from a backup copy.

To restore a DHCP database

1. Before starting, make a copy of the DHCP server database files.
2. In the *%SystemRoot%*\System32\Dhcp directory, delete the J50.log, J50*xxxxx*.log, and Dhcp.tmp files.
3. Copy an uncorrupted backup version of the Dhcp.mdb (from your manual or automatic database backup media) to the *%SystemRoot%*\System32\Dhcp directory.
4. Restart the Microsoft DHCP server.

Detecting DHCP Jet Data Corruption

Table 4.14 lists the possible DHCP service messages that might appear in the System event log when the DHCP server database becomes corrupted:

Table 4.14 Corrupt Jet Database Messages

Event ID	Source	Description
1014	DhcpServer	The Jet database returned the following Error: –510.
1014	DhcpServer	The Jet database returned the following Error: –1022.
1014	DhcpServer	The Jet database returned the following Error: –1850.

Typically, Jet errors can be resolved by manual offline compaction of the database using the Jetpack utility. In cases where Jetpack.exe fails to repair the database, restoration of the DHCP server database as described in the following sections can be used to recover the server database and restore DHCP service at the server computer.

To recover a corrupted DHCP database, you can use the following options for restoring the database:

- **Simple recovery.** Restore the database from a backup copy of the database file, Dhcp.mdb.

  This method is recommended as the preferred method of recovery because it involves less risk of losing information previously configured and stored by the DHCP server and is much simpler to perform.
- **Advanced recovery.** The registry can be modified to force creation of a new database file. This method can be useful as an additional method for data recovery when simple restoration of the database is not possible. However, this should be done with extreme caution. For more information about restoring a corrupted DHCP database, see the Microsoft Knowledge Base link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources/default.asp. Search the Knowledge Base using the keywords *DHCP*, database, and recovery.

Simple Recovery: Restoring from Backup

If the DHCP server database becomes corrupted or is lost, simple recovery is possible by replacing the server database file (Dhcp.mdb), located in the *%SystemRoot%*\System32\Dhcp folder, with a backup copy of the same file. You can then perform a simple file copy to overwrite the current corrupted database with a backup copy of the same file.

If DHCP Manager has been used previously to enable backup, you can obtain the backup copy of the server database file located in the *%SystemRoot%*\System32\Dhcp\Backup folder. As an option, you can also choose to restore the Dhcp.mdb file from a tape backup or other backup media.

Before restoring the database file from backup, the DHCP service must first be stopped. Once you have copied the backup file to the *%SystemRoot%*\System32\Dhcp folder from your preferred backup source, you can restart the DHCP service.

To stop the DHCP server service, type the following at a command prompt:

net stop dhcpserver

Once the DHCP service has been stopped, the following procedure can be used to safely restore a backup copy of the database from either backup media or the DHCP service backup folder.

First, move the files from your existing DHCP folder to a different folder location, such as \Olddhcp. Be careful to keep the DHCP folder structure intact. For example, type the following set of commands at a command prompt to perform this step:

md c:\Olddhcp

move %*SystemRoot*%\system32\DHCP*.* C:\Olddhcp

Next, remove the corrupted server database file. This can also be done at the command prompt:

del %*SystemRoot*%\system32\DHCP\Dhcp.mdb

You can then copy the backup database file into the DHCP service folder. The path to be used when performing the actual copy operation varies (as shown in Table 4.15), depending on the specific server version of Windows running on the computer where the DHCP database file is being restored.

Table 4.15 Location of DHCP Database Files

Server version	Copy command usage
Windows NT Server 3.51	**copy %*SystemRoot*%\system32\dhcp\backup\jet\dhcp.mdb %*SystemRoot*%\system32\dhcp\dhcp.mdb**
Windows NT Server 4.0	**copy %*SystemRoot*%\system32\dhcp\backup\jet\new\dhcp.mdb %*SystemRoot*%\system32\dhcp\dhcp.mdb**
Windows 2000 Server	**copy %*SystemRoot*%\system32\dhcp\backup\jet\new\dhcp.mdb %*SystemRoot*%\system32\dhcp\dhcp.mdb**

Once the backup database file has been copied to the correct DHCP folder location for your server computer, you can restart the DHCP service.

To restart the service, type the following at the command prompt:

```
net start dhcpserver
```

The previous procedure should allow the DHCP service to start, but if scope information is missing, it might be necessary to use a backup copy of your registry to reconfigure the values necessary for restoring your scope and client reservation information.

Rebuilding a Stopped DHCP Server

If the hardware for the DHCP server is malfunctioning or other problems prevent you from running Windows 2000, you must rebuild the DHCP database on another computer.

To rebuild a DHCP server

1. If you can start the original DHCP server by using the **net start DHCP** command, use the **copy** command to make backup copies of the files in the *%SystemRoot%*\System32\Dhcp directory. If you cannot start the computer at all, you must use the last backup version of the DHCP database files.
2. Install Windows 2000 Server to create a new DHCP server using the same hard drive location and *%SystemRoot%* directory. That is, if the original server stored the DHCP files on *%SystemRoot%* \System32\Dhcp, then the new DHCP server must use this same path to the DHCP files.
3. Make sure the Microsoft DHCP service on the new server is stopped, and then use a registry editor to restore the DHCP keys from backup files.
4. Copy the DHCP backup files to the *%SystemRoot%*\System32\Dhcp directory.
5. Restart the new, rebuilt DHCP server.

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.

Compacting the DHCP Server Database

Windows 2000 and Windows NT Server 4.0 are designed to automatically compact the DHCP server database. However, if you are using Windows NT Server version 3.51 or earlier, the database might need to be compacted after DHCP has been running for awhile to improve performance. You should compact the DHCP database whenever it approaches 30 MB.

You can use the Jetpack.exe utility provided with Windows NT Server 3.5 and 3.51 to compact a DHCP database. Jetpack.exe is a command-line utility that is run in the Windows NT Server command window. The utility is found in the *%SystemRoot%*\System32 directory.

The Jetpack.exe syntax is:

```
Jetpack.exe database_name temp_database_name
```

For example:

```
CD %SystemRoot%\SYSTEM32\DHCP
JETPACK DHCP.MDB TMP.MDB
```

In the preceding example, Tmp.mdb is a temporary database that is used by Jetpack.exe. Dhcp.mdb is the DHCP server database file.

When Jetpack.exe is started, it performs the following tasks:

1. Copies database information to a temporary database file called Tmp.mdb.
2. Deletes the original database file, Dhcp.mdb.
3. Renames the temporary database file to the original file name.

To compact the DHCP database

1. Open the DHCP Manager console.
2. Select the applicable DHCP server.
3. Click **Action**, point to **All Tasks**, and click **Stop**. (Alternatively, you can type **net stop DHCP** at the command prompt.)
4. At the command prompt, type **jetpack** to run the Jetpack program.
5. Restart the DHCP service by using the **Services** dialog box.

Using Reconcile to Salvage Scopes

Before using the Reconcile feature to fully recover DHCP scope client information from the registry, the server computer needs the following:

- All DHCP server registry keys must be either restored or exist and remain intact from previous service operation on the server computer.
- A fresh version of the DHCP server database file must be regenerated in the *%SystemRoot%*\System32\Dhcp folder on the server computer.

When the registry and database meet these criteria, you can restart the DHCP service. At this point, you might notice that, upon opening the DHCP console, scope information is present but there are no active leases displayed. To regain your active leases for each scope, you use the Reconcile feature to recover each scope. Use the following steps for Windows 2000 Server to perform reconciliation and recovery of scope data.

1. In DHCP Manager, click a scope to select and expand it.
2. Click the Active Leases folder.
3. Right-click and select **Task**, and then click **Reconcile**.
4. When the **Reconciling Database** dialog window appears, click **OK**.

This process can be repeated for each scope to add client lease and reservation information from the registry back into the list of active leases for each scope previously configured for the DHCP server.

After using the Reconcile feature, you might notice that, when viewing properties for individual clients shown in the list of active leases, client information is displayed incorrectly. This information is corrected and updated in DHCP Manager as scope clients renew their leases.

If your DHCP server is running under Windows NT Server 4.0, Service Pack 2 or later, enable address conflict detection after using this recovery method. This is recommended since the backup may have been performed on an older database or from a slightly out-of-date system registry. For more information about when to use and how to enable conflict detection, see the “Server Conflict Detection” section in this chapter and the Microsoft Knowledge Base.

Although the Reconcile feature can be used to recover scope information in the event of disaster recovery for a DHCP server, it is not intended as a replacement for other traditional backup measures. Implement other methods (such as backing up to a tape drive) to provide further safe offline storage and duplicate archives of your DHCP database.

Analyzing Server Log Files

Because Windows 2000 Server uses audit logging when writing DHCP server log files, DHCP server logging is not resource-intensive. It can be left enabled because it uses a limited amount of disk space on server hard drives.

DHCP Server Log File Format

DHCP server logs are comma-delimited text files with each log entry representing a single line of text. The fields and their order as they appear in each log file entry are:

ID Date, Time, Description, IP Address, Computer Name, MAC Address

Each of these fields is described in further detail in Table 4.16.

Table 4.16 Log File Fields

Field	Description
ID	A DHCP server event ID code.
Date	The date at which this entry was logged on the DHCP server.
Time	The time at which this entry was logged on the DHCP server.
Description	A description of this DHCP server event.
IP Address	The IP address of the DHCP client.
Computer Name	The computer name of the DHCP client.
MAC Address	The media access control address used by the client’s network adapter hardware.

DHCP Server Log Event Codes

The DHCP server log also uses special event ID codes to specifically indicate information about the type of service event logged.

Table 4.17 describes these event ID codes.

Table 4.17 Event ID Codes

Event 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 lease was renewed by a client.
12	A lease was released by a client.
13	An IP address was found 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.
20	A BOOTP address was leased to a client.

Additional Resources

For more information about using DHCP, refer to the following books:

- *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture* Third Edition by Douglas Comer, 1995, Englewood Cliffs, NJ: Prentice Hall.
- *Managing a Microsoft Windows NT Network* by Microsoft Corporation, 1999, Redmond, WA: Microsoft Press.
- *Mastering TCP/IP For NT Server* by M. Minasi, T. Lammle, and M. Lammle, 1997, Alameda, CA: Sybex.
- *Optimizing Network Traffic* by Microsoft Corporation, 1999, Redmond, WA: Microsoft Press.
- *TCP/IP Unleashed* by T. Parker, 1996, Indianapolis, IN: Sams Publishing.
- *TCP/IP Illustrated, Volume 1: The Protocol* by W.R. Stevens, 1994, Reading, MA: Addison-Wesley.
- *Windows NT TCP/IP Network Administration* by C. Hunt, and R.B. Thompson, 1998, Sebastopol, CA: O'Reilly and Associates.
