CHAPTER 19

# Introduction to Dynamic Host Configuration

All hosts seeking Internet access must have an IP address. As Internet administrator, you must perform the following for every new user and for every user whose computer was moved to another subnet:

1. Choose a legal IP address.
2. Assign the address to the individual workstation.
3. Define workstation configuration parameters.
4. Update the DNS database, mapping the workstation name to the IP address.

These activities are time consuming and error prone, hence the Dynamic Host Configuration Protocol (DHCP). DHCP frees you from the burden of individually assigning IP addresses. It was designed by the Internet Engineering Task Force (IETF) to reduce the amount of configuration required when using TCP/IP. DHCP allocates IP addresses to hosts. It also provides all the parameters that hosts require to operate and exchange information on the Internet network to which they are attached.

DHCP localizes TCP/IP configuration information. It also manages allocating TCP/IP configuration data by automatically assigning IP addresses to systems configured to use DHCP. Thus, you can ensure that hosts have Internet access without having to configure each host individually.

### See Also

How DHCP Works
Cisco Network Registrar DHCP Implementations, page 19-4
DNS Update, page 19-7
DHCP Failover, page 19-8
Client-Classes, page 19-12

# How DHCP Works

DHCP makes dynamic address allocation possible by shifting workstation configuration to global address pools at the server level. DHCP is based on a client/server model. The client software runs on the workstation and the server software runs on the DHCP server.

### See Also

Sample DHCP User, page 19-2
Typical DHCP Administration, page 19-2
Leases, page 19-3
Scopes and Policies, page 19-3

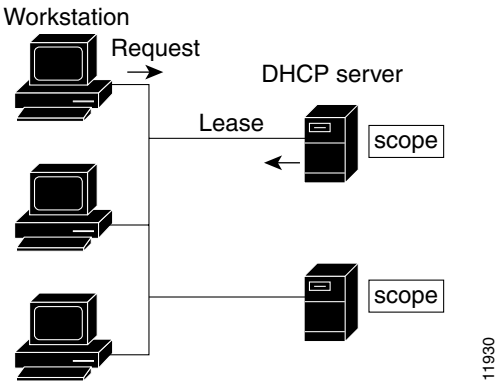
# Sample DHCP User

After Beth's workstation (bethpc) is configured with DHCP, these actions occur when she first starts up:

1. Her workstation automatically requests an IP address from a DHCP server on the network.
2. The DHCP server offers her a lease that is an IP address with the configuration data necessary to use the Internet. Nobody else uses the leased address, and it is valid only for her workstation.
3. Before the address lease expires, bethpc renews it, thereby extending the expiration time. It continues to use the lease right up to its expiration or if it cannot reach the server.
4. If Beth relocates to another department and her workstation moves to a different subnet, her current address expires and becomes available for others. When Beth starts her workstation at its new location, it leases an address from an appropriate DHCP server on the subnet (see Figure 19-1).

As long as the DHCP server has the correct configuration data, none of the workstations or servers using DHCP will ever be configured incorrectly. Therefore, there is less chance of incurring network problems from incorrectly configured workstations and servers that are difficult to trace.

***Figure 19-1 Hosts Request an IP Address***




The example shows the DHCP protocol with a set of DHCP servers that provide addresses on different subnets. To further simplify the administration of address pools, network routers are often configured as DHCP relay agents to forward client messages to a central DHCP server. This server is configured with address pools for a group of subnets.

# Typical DHCP Administration

To use DHCP, you must have at least one DHCP server on the network. After you install the server:

- Define a scope of IP addresses that the DHCP server can offer to DHCP clients. You no longer need to keep track of which addresses are in use and which are available.
- Configure a secondary server to share the distribution or handle leases if the first DHCP server goes down. This is known as DHCP failover, and is described further in the "DHCP Failover" section on page 19-8.

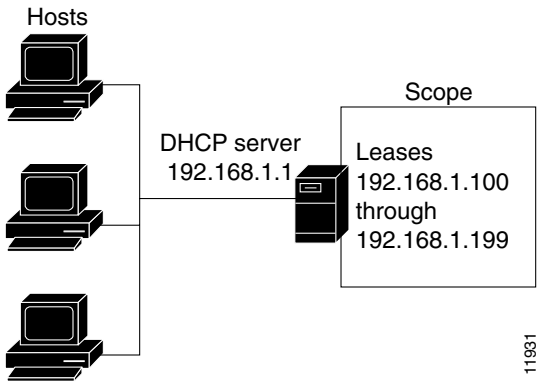
# Leases

One of the most significant benefits of DHCP is that it can dynamically configure workstations with IP addresses and associate leases with the assigned addresses. DHCP uses a lease mechanism that offers an automated, reliable, and safe method for distributing and reusing addresses in networks, with little need for administrative intervention. As system administrator, you can tailor the lease policy to meet the specific needs of your network.

Leases are grouped together in an address pool, called a scope, which defines the set of IP addresses available for requesting hosts. A lease can be reserved (the host always receives the same IP address) or dynamic (the host receives the next available, unassigned lease in the scope). The DHCP server of the site is configured to lease addresses 192.168.1.100 through 192.168.1.199 (see Figure 19-2).

If you plan not to have more network devices than configured addresses for the scope, you can define long lease times, such as one to two weeks, to reduce network traffic and DHCP server load.

***Figure 19-2 DHCP Hosts Requesting Leases from a DHCP Server***




# Scopes and Policies

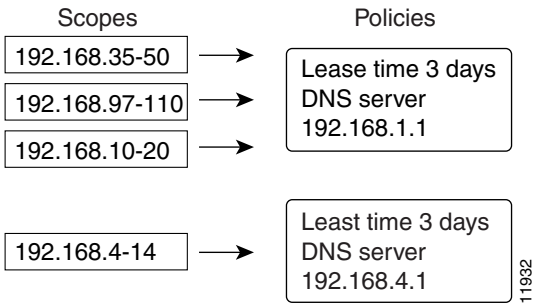
A scope contains a set of addresses for a subnet, along with the necessary configuration parameters. You must define at least one scope for each subnet for which you want dynamic addressing.

A policy includes lease times and other configuration parameters that a DHCP server communicates to clients. Use policies to configure DHCP options that the DHCP server supplies to a client upon request. Policies ensure that the DHCP server supplies all the correct options for scopes without having to do so separately for each scope (see Figure 19-3 on page 19-4).

The difference between scopes and policies is that scopes contain server information about addresses, such as which address is leasable and whether to ping clients before offering a lease. Policies contain client configuration data, such as the lease duration and address of the local DNS server.

Policies are especially useful if you have multiple scopes on a server. You can create policies that apply to all or selected scopes. The Cisco Network Registrar policy hierarchy is a way to define policies from least to most specific. For example, you usually specify a router option for each policy, which means that you would need a policy for each scope. Scope-specific policies like this can be defined in a scope-embedded policy. More general policies, such as those referring to lease times, can be applied in a system-wide policy (see the "Configuring DHCP Policies" section on page 21-1). You can also write extensions to handle policy assignments (see the "Using Extensions to Affect DHCP Server Behavior" section on page 23-11).

*Figure 19-3 Scopes and Policies*




# Cisco Network Registrar DHCP Implementations

The Cisco Network Registrar DHCP server provides a reliable method for automatically assigning IP addresses to hosts on your network. You can define DHCP client configurations, and use the Cisco Network Registrar database to manage assigning client IP addresses and other optional TCP/IP and system configuration parameters. The TCP/IP assignable parameters include:

- IP addresses for each network adapter card in a host.
- Subnet masks for the part of an IP address that is the physical (subnet) network identifier.
- Default gateway (router) that connects the subnet to other network segments.
- Additional configuration parameters you can assign to DHCP clients, such as a domain name.

Cisco Network Registrar automatically creates the databases when you install the DHCP server software. You add data as you define DHCP scopes and policies.

The Cisco Network Registrar DHCP server also supports allocating addresses in virtual private networks (VPNs) and subnets to pool manager devices for on-demand address pools. These features are described in the following sections.

### See Also

DHCP and IPv6
Virtual Private Networks
Subnet Allocation and DHCP Address Blocks, page 19-6

# DHCP and IPv6

For details on the Cisco Network Registrar implementation of DHCPv6, see Chapter 26, “Managing DHCPv6 Addresses.”

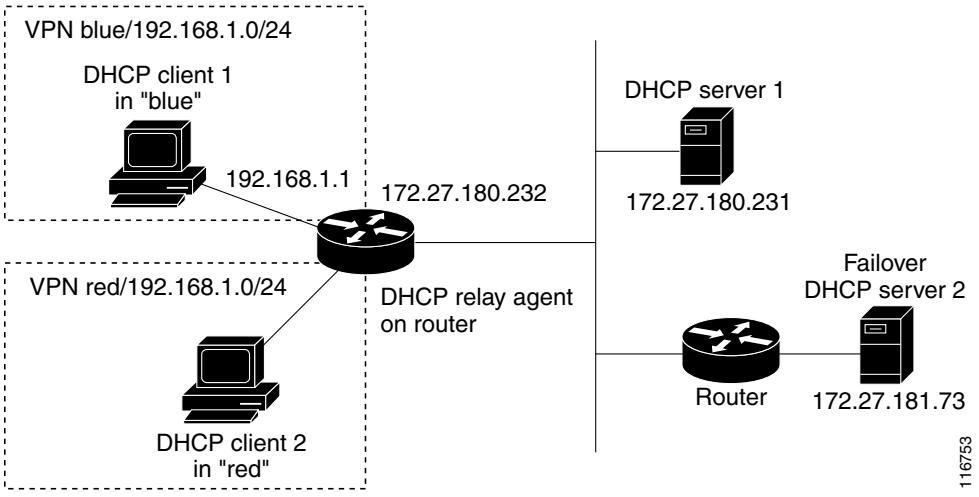
# Virtual Private Networks

Virtual private networks (VPNs) allow the possibility that two pools in separate networks can have the same address space, with these two pools having overlapping private network addresses. This can save address resources without having to use valuable public addresses. These VPN addresses, however, require a special designator to distinguish them from other overlapping IP addresses. Cisco Network Registrar DHCP servers that are not on the same VPN as their clients can now allocate leases and addresses to these clients, and can distinguish the addresses from one VPN to another.

Through changes made to the Cisco Network Registrar DHCP server and Cisco IOS DHCP Relay Agent, the DHCP server can service clients on multiple VPNs. A VPN distinguishes a set of DHCP server objects, making them independent of otherwise identical objects in other address spaces. You can define multiple VPNs containing the same addresses. You create a VPN based on the VPN identifier configured in the Cisco IOS Relay Agent.

Figure 19-4 shows a typical VPN-aware DHCP environment. The DHCP Relay Agent services two distinct VPNs, blue and red, with overlapping address spaces. The Relay Agent has the interface address 192.168.1.1 on VPN blue and is known to DHCP Server 1 as 172.27.180.232. The server, which services address requests from DHCP Client 1 in VPN blue, can be on a different network or network segment than the client, and can be in a failover configuration with DHCP Server 2 (see the "DHCP Failover" section on page 19-8). The Relay Agent can identify the special, distinguished route of the client address request to the DHCP server, as coordinated between the Relay Agent and Cisco Network Registrar administrators. The DHCP servers can now issue leases based on overlapping IP addresses to the clients on both VPNs.

***Figure 19-4 Virtual Private Network DHCP Configuration***



# Subnet Allocation and DHCP Address Blocks

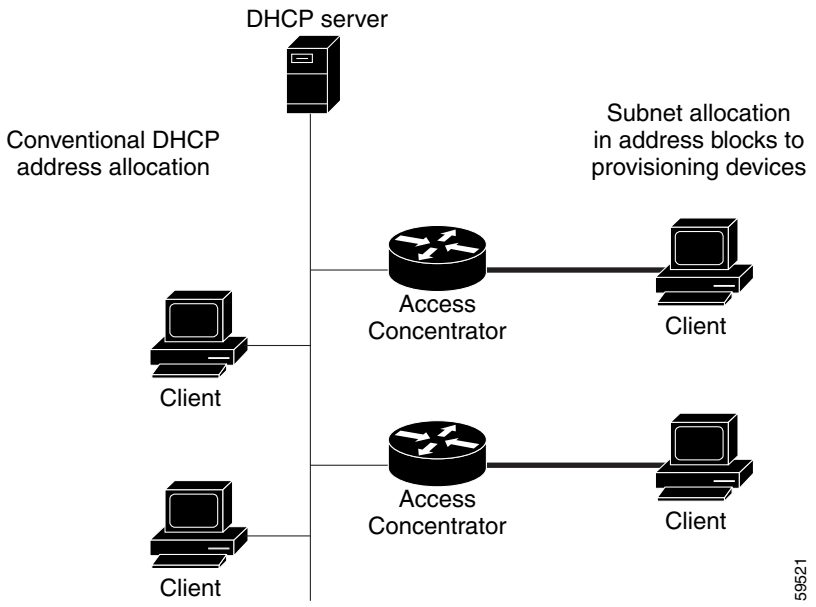
Cisco Network Registrar supports creating on-demand address pools as a network infrastructure for address provisioning and VPNs. Traditionally, the DHCP server is limited to interact with individual host devices. Through subnet allocation, the server can interact with VPN routers and other provisioning devices to provision entire IP subnets. This Cisco Network Registrar feature enhances the on-demand address pool capability currently supported by the Cisco IOS Relay Agent.

Cisco Network Registrar supports explicitly provisioned subnets. You must explicitly configure the DHCP server address space and subnet allocation policies before the server can allocate pools or leases. You can thereby configure a server as a pool manager to manage subnets and delegate them to client devices.

You manage DHCP subnet allocation using DHCP server address block objects in Cisco Network Registrar. A DHCP address block is a range of contiguous IP addresses delegated to the DHCP server for assignment. The server expects to subdivide these addresses into pools so that it or other servers or devices can allocate them. DHCP address blocks are parents to subnets. These DHCP address blocks are distinct from the address blocks you can create using Cisco Network Registrar, which are static. DHCP address blocks cannot include static address ranges or lease reservations.

Figure 19-5 shows a sample environment where a DHCP server allocates entire subnets to access concentrators or other provisioning devices, in addition to servicing individual clients. The traditional client/server relationship is shown on the left of the diagram, while the subnet allocation to access concentrators is shown on the right of the diagram. Dialup customers, for example, connect to the service provider network at two ISP gateways (routers), which connect to the management network segment where the DHCP server resides. The gateways provision addresses to their connected clients based on the subnet requested from the DHCP server.

***Figure 19-5 Sample DHCP Subnet Allocation Configuration***



# DNS Update

Although DHCP frees you from the burden of distributing IP addresses, it still requires updating the DNS server with DHCP client names and addresses. DNS update automates the task of keeping the names and addresses current. With the Cisco Network Registrar DNS update feature, the DHCP server can tell the corresponding DNS server when a name-to-address association occurs or changes. When a client gets a lease, Cisco Network Registrar tells the DNS server to add the host data. When the lease expires or when the host gives it up, Cisco Network Registrar tells the DNS server to remove the association.

In normal operation, you do not have to manually reconfigure DNS, no matter how frequently clients' addresses change through DHCP. Cisco Network Registrar uses the hostname that the client workstation provides. You also can have Cisco Network Registrar synthesize names for clients who do not provide them, or use the client lookup feature to use a preconfigured hostname for the client.

### See Also

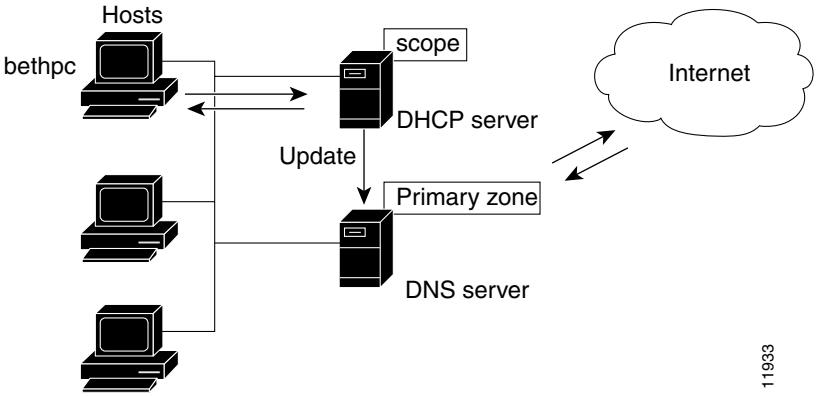
Effect on DNS of Obtaining Leases
Effect on DNS of Releasing Leases
Effect on DNS of Reacquiring Leases, page 19-8

## Effect on DNS of Obtaining Leases

For ExampleCo, the administrator creates a scope on the DHCP server and allocates 100 leases (192.168.1.100 through 192.168.1.199). Each workstation gets its owner name. The administrator also configures the DHCP server to use DNS update and associates it with the correspondingly configured DNS server. The administrator does not need to enter the names in the DNS server database.

Monday morning, Beth (user of bethpc) tries to log in to a website without having an address. When her host starts up, it broadcasts an address request (see Figure 19-6).

***Figure 19-6 DNS Update at ExampleCo Company***




The DHCP server then:

1. Gives bethpc the next available (unassigned) IP address (192.168.1.125).
2. Updates her DNS server with the hostname and address (bethpc 192.168.1.125).

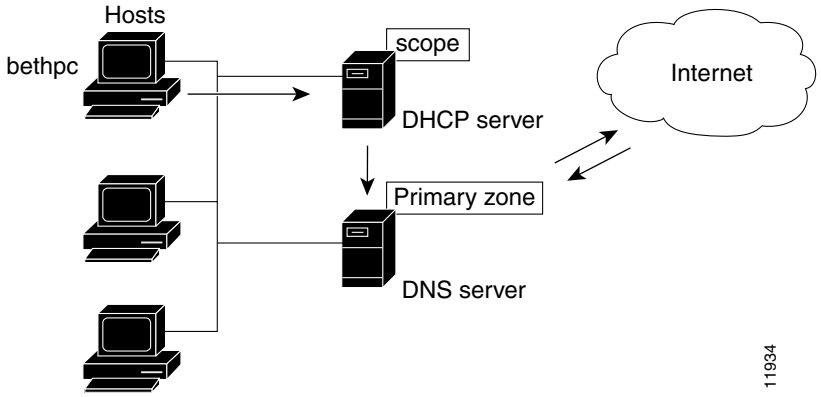
Beth can now access the website. In addition, programs that need to translate the name of Beth's machine to her IP address, or the other way around, can query the DNS server.

## Effect on DNS of Releasing Leases

Later that day, Beth learns that she needs to travel out of town. She turns off her host, which still has a leased address that is supposed to expire after three days. When the lease is released, the DHCP server:

1. Acknowledges that the IP address is now available for other users (see Figure 19-7 on page 19-8).
2. Updates the DNS server by removing the hostname and address. The DNS server no longer stores data about bethpc or its address.

***Figure 19-7 Relinquishing a Lease***




## Effect on DNS of Reacquiring Leases

When Beth returns from her trip to start up her host again:

1. Her workstation broadcasts for an IP address.
2. The DHCP server checks if the host is on the correct network. If so, the server issues an address. If not, the server on the correct network issues the address.
3. The DHCP server updates the DNS server again with the host and address data.

# DHCP Failover

Because DHCP provides for multiple servers (see RFC 2131), you can configure these servers so that if one cannot provide leases to requesting clients, another one can take over. Cisco Network Registrar provides the DHCP failover feature, where two servers operate as redundant partners. Existing DHCP clients can keep and renew their leases without needing to know or care which server is responding to their requests.

### See Also

How Failover Works
Failover States and Transitions
Allocating Addresses Through Failover, page 19-11

# How Failover Works

Failover is based on a partner server relationship. The partners must have identical scopes, leases, policies, and client-classes. After the servers start up, each contacts the other. The main server provides its partner with a private pool of addresses and updates its partner with every client operation. If the main server fails, then the partner takes over offering and renewing leases, using its private pool. When the main server becomes operational again, it reintegrates with its partner without administrative intervention. These servers are in a relationship known as a failover pair.

The failover protocol keeps DHCP operational if:

- **The main server fails**—The partner takes over services during the time the main server is down. The servers cannot generate duplicate addresses, even if the main server fails before updating its partner.
- **Communication fails**—A partner can operate correctly even though it cannot tell whether it was the other server or the communication with it that failed. The servers cannot issue duplicate addresses, even if they are both running and each can communicate with only a subset of clients.

Failover configurations are usually in a simple, back office, or symmetrical fashion. Once configured:

1. The partners connect.
2. The main server supplies data about all existing leases to its partner.
3. The backup server requests a pool of backup addresses from the main server.
4. The main server replies with a percentage of available addresses from each scope to its partner.
5. The backup server ignores all DHCPDISCOVER requests, unless it senses that the main server is down. In normal operations, it handles only DHCPRENEW and DHCPREBINDING requests. A DHCPDISCOVER request is a broadcast to locate available servers.
6. The main server updates its partner with the results of all client operations.

You can automatically synchronize the servers in a failover pair. The two servers dynamically rebalance the available leases; if the main server hands out a large portion of its available leases, it can reclaim leases from its partner.

**Note** Always configure failover on the same interface that the server uses to serve client traffic.

# Failover States and Transitions

During normal operation, the failover partners transition between states. They stay in their current state until all the actions for the state transition are completed and, if communication fails, until the conditions for the next state are fulfilled. The states and their transitions are described in Table 19-1.

*Table 19-1 Failover States and Transitions*

| State | Server Action |
|---|---|
| STARTUP | Tries to contact its partner to learn its state, then transitions to another state after a short time, typically seconds. |
| NORMAL | Can communicate with its partner. The main and backup servers act differently in this state:<br>• The main server responds to all client requests using its pool. If its partner requests a backup pool, the main server provides it.<br>• The backup server only responds to renewal and rebinding requests. It requests a backup pool from the main server. |
| COMMUNICATIONS-INTERRUPTED | Cannot communicate with its partner, whether it or the communication with it is down. The servers cycle between this state and NORMAL state as the connection fails and recovers, or as they cycle between operational and nonoperational. During this time, the servers cannot give duplicate addresses.<br>During this state, you usually do not need to intervene and move a server into the PARTNER-DOWN state. However, this is not practical in some cases. A server running in this state is not using the available pool efficiently. This can restrict the time a server can effectively service clients.<br>A server is restricted in COMMUNICATIONS-INTERRUPTED state:<br>• It cannot reallocate an expired address to another client.<br>• It cannot offer a lease or renewal beyond the maximum client lead time (MCLT) longer than the current lease time. The MCLT is a small additional time added that controls how much the client lease expiration is ahead of what the backup server thinks it is.<br>• A backup server can run out of addresses to give new clients, because it normally has only a small pool, while the main server has most of them.<br>The server is limited only by the number of addresses allocated to it and the arrival rate of DHCPDISCOVER or INIT-REBOOT packets for new clients. With a high new client arrival or turnover rate, you may need to move the server into PARTNER-DOWN state more quickly. |
| PARTNER-DOWN | Acts as if it were the only operating server, based on one of these facts:<br>• The partner notified it during its shutdown.<br>• The administrator put the server into PARTNER-DOWN state.<br>• The safe period expired and the partner automatically went into this state. |

*Table 19-1 Failover States and Transitions (continued)*

| State | Server Action |
|---|---|
| PARTNER-DOWN (continued) | In this state, the server ignores that the other server might still operate and could service a different set of clients. It can control all its addresses, offer leases and extensions, and reallocate addresses. The same restrictions to servers in COMMUNICATIONS-INTERRUPTED state do not apply.<br><br>Either server can be in this state, but only one should be in it at a time so that the servers do not issue duplicate addresses and can properly resynchronize later on. Until then, an address is in a pending-available state. |
| POTENTIAL-CONFLICT | Might be in a situation that does not guarantee automatic reintegration, and is trying to reintegrate with its partner. The server might determine that two clients (who might not be operating) were offered and accepted the same address, and tries to resolve this conflict. |
| RECOVER | Has no data in its stable storage, or is trying to reintegrate after recovering from PARTNER-DOWN state, from which it tries to refresh its stable storage. A main server in this state does not immediately start serving leases again. Because of this, do not reload a server in this state. |
| RECOVER-DONE | Can transition from RECOVER or PARTNER-DOWN state, or from COMMUNICATIONS-INTERRUPTED into NORMAL state. |
| PAUSED | Can inform its partner that it will be out of service for a short time. The partner then transitions to COMMUNICATIONS-INTERRUPTED state and begins servicing clients. |
| SHUTDOWN | Can inform its partner that it will be out of service for a long time. The partner then transitions to PARTNER-DOWN state to take over completely. |

# Allocating Addresses Through Failover

To keep your failover pair operating in spite of a network partition, in which both can communicate with clients but not with each other, you must allocate more addresses than are needed to run a single server. Configure the main server to allocate a percentage of the currently available (unassigned) addresses in each scope address pool to its partner. These addresses become unavailable to the main server. The partner uses them when it cannot talk to the main server and does not know if it is down.

How many additional addresses are needed? There is no single percentage for all environments. It depends on the arrival rate of new DHCP clients and the reaction time of your network administration staff. The backup server needs enough addresses from each scope to satisfy the requests of all new DHCP clients that arrive during the period in which the backup does not know if the main server is down.

Even during PARTNER-DOWN state, the backup server waits for the lease expiration and the maximum client lead time (MCLT), a small additional time buffer, before reallocating any leases. When these times expire, the backup server offers:

- Leases from its private pool of addresses.
- Leases from the main server pool of addresses.
- Expired leases to new clients.

During the day, if the administrative staff can respond within two hours to a COMMUNICATIONS INTERRUPTED state to determine if the main server is working, the backup server needs enough addresses to support a reasonable upper bound on the number of new DHCP clients that might arrive during those two hours.

During off hours, if the administrative staff can respond within 12 hours to the same situation, and considering that the arrival rate of previously unheard from DHCP clients is also less, the backup server then needs enough addresses to support a reasonable upper bound on the number of DHCP clients that might arrive during those 12 hours.

Consequently, the number of addresses over which the backup server requires sole control would be the greater of the numbers of addresses given out during peak and nonpeak times, expressed as a percentage of the currently available (unassigned) addresses in each scope.

# Client-Classes

Assigning classes to clients is an important adjunct to DHCP addressing and addresses quality of service issues. You can use the Cisco Network Registrar client and client-class facility to provide differentiated services to users that are connected to a common network. You can group your user community based on administrative criteria, and then ensure that each user receives the appropriate class of service.

Although you can use the Cisco Network Registrar client-class facility to control any configuration parameter, the most common uses are for:

- **Lease periods**—How long a set of clients should keep their addresses.
- **IP address ranges**—From which lease pool to assign clients addresses.
- **DNS server addresses**—Where clients should direct their DNS queries.
- **DNS hostnames**—What name to assign clients.
- **Denial of service**—Whether unauthorized clients should be offered leases.

One way to use the client-class facility is to allow visitors access to some, but not all, of your network. For example, when Joe, a visitor to ExampleCo, tries to attach his laptop to the example.com network, Cisco Network Registrar recognizes the laptop as being foreign. ExampleCo creates one class of clients known as having access to the entire network, and creates another visitor class with access to a subnet only. If Joe needs more than the standard visitor access, he can register his laptop with the Cisco Network Registrar system administrator, who adds him to a different class with the appropriate service.

The following sections describe how DHCP normally processes an address assignment, and then how it would handle it with the client-class facility in effect.

## See Also

DHCP Processing Without Client-Classes
DHCP Processing with Client-Classes, page 19-13
Defining Scopes for Client-Classes, page 19-14
Choosing Networks and Scopes, page 19-15

# DHCP Processing Without Client-Classes

To understand how you can apply client-class processing, it is helpful to know how the DHCP server handles client requests. The server can perform three tasks:

- Assign an IP address.
- Assign the appropriate DHCP options (configuration parameters).
- Optionally assign a fully qualified domain name (FQDN) and update the DNS server with that name.

The DHCP server:

1. Assigns an address to the client from a defined scope—To choose an address for the client, the DHCP server determines the client subnet, based on the request packet contents, and finds an appropriate scope for that subnet.

   If you have multiple scopes on one subnet or several network segments, which is known as multinetting, the DHCP server may choose among these scopes in a round-robin fashion, or you can change the priority of the scope choice by using the DHCP server address allocation priority feature (see the "Configuring Multiple Scopes Using Allocation Priority" section on page 20-12). After the server chooses a scope, it chooses an available (unassigned) address from that scope:

   a. It assigns DHCP option values from a defined policy. Cisco Network Registrar uses policies to group options. There are two types of policies: scope-specific and system default. For each DHCP option the client requests, the DHCP server searches for its value in a defined sequence.

   b. If the scope-specific policy contains the option, the server returns its value to the client and stops searching.

   c. If not found, the server looks in the system default policy, returns its value, and stops searching.

   d. If neither policy contains the option, the server returns no value to the client and logs an error.

   e. The server repeats this process for each requested option.

2. With DNS update in effect, the server assigns an FQDN to the client. If you enabled DNS update, Cisco Network Registrar enters the client name and address in the DNS host table. See the "DNS Update" section on page 19-7. The client name can be:

   - Its name as specified in the client lease request (the default value).
   - Its MAC address (hardware address; for example, 00:d0:ba:d3:bd:3b).
   - A unique name using the default prefix *dhcp* or a specified prefix.

# DHCP Processing with Client-Classes

When you enable the client-class facility for your DHCP server, the request processing performs the same three tasks of assigning IP addresses, options, and domain names as described in the "DHCP Processing Without Client-Classes" section on page 19-13, but with added capability. The DHCP server:

1. **Considers the client properties and client-class inclusion before assigning an address**—As in regular DHCP processing, the DHCP server determines the client subnet. The server then checks if there is a client-class defined or a MAC address for this client in its database. If there is:

   a. A client-class defined by a client-class lookup ID expression, the client is made a member of this client-class.

   b. No MAC address, it uses the default client. For example, the default client could have its client-class name set to Guest, and that client-class could limit (using options and address selection) what network operations such clients are permitted.

c. No MAC address and no default client, the server handles the client through regular DHCP processing.

d. No client-specifier, but a MAC address, the MAC address is converted into a client-specifier. An unknown client is mapped to the default client, if the default client is defined.

The scopes must have addresses on client-accessible subnets. That is, they must have a selection tag that associates them with a client-class. To assign the same clients to different address pools, you must use separate scopes.

For example, a scope would either have a selection tag of Employee or Guest, but not both. In this case, there are two scopes for each subnet; one with the selection tag Employee, and the other with Guest. Each scope has a different associated policy and address range that provides the appropriate access rights for the user group.

2. **Checks for client-class DHCP options**—In regular DHCP processing, the server checks the scope-specific and system default DHCP options. With client-class, it also first checks the client-specific and client-class-specific options.
3. **Provides additional FQDN assignment options**—Beyond the usual name assignment process of using the hostname the client requests, the server can:
   - Provide an explicit hostname that overrides it.
   - Drop the client-requested hostname and not replace it.
   - Synthesize a hostname from the client MAC address.

# Defining Scopes for Client-Classes

The motivating factor for using client-classes is often to offer an address from one or another address pool to a client. Another motivating factor might be to provide clients with different option values or lease times. Offering clients addresses from separate pools requires defining more than one scope.

To get more than one scope on a subnet, they must come from the same network segment. Networks are not configured directly in Cisco Network Registrar, but are inferred from scope configurations. Scopes become related (end up in the same network):

- **Implicitly**—Two scopes have the same network number and subnet mask. These scopes naturally end up on the same network without explicit configuration.
- **Explicitly**—One scope is marked as a secondary to another. This is required when the scope marked as a secondary has a network and subnet mask unrelated to the primary. An example is putting a set of 10.0.0.0 network addresses on a normal, routable network segment.

When the Cisco Network Registrar DHCP server reads the scope configuration from its database, it places every scope in a network, and logs this information. Scopes with the same network number and subnet mask end up on the same network, while a secondary scope ends up on the primary scope network.

# Choosing Networks and Scopes

When a DHCP packet arrives, the server determines the address from which it came by:

- Gateway address (*giaddr*), if there was one, for packets sent through a BOOTP relay.
- Interface address of the interface on which the broadcast packet arrived, if the DHCP client is on a network segment to which the DHCP server is also directly connected.

In all cases, the DHCP server determines a network from the gateway or interface address. Then, if the network has multiple scopes, the server determines from which scope to allocate an address to the DHCP client. It always looks for a scope that can allocate addresses to this type of client. For example, a DHCP client needs a scope that supports DHCP, and a BOOTP client needs one that supports BOOTP. If the client is a DHCP client and there are multiple scopes that support DHCP, each with available (unassigned) addresses, the DHCP server allocates an IP address from any of those scopes, in a round-robin manner, or by allocation priority.

Selection tags and client-classes let you configure the DHCP server to allocate IP addresses from:

- One or more scopes on a network to one class of clients.
- A different set of scopes to a different class of clients.

In the latter case, the gateway or interface address determines the network. The client-class capability, through the mechanism of the selection tags, determines the scope on the network to use.