Module 6

Implementing Dynamic Host Configuration Protocol

Module Overview

Dynamic Host Configuration Protocol (DHCP) plays an important role in the Windows Server® 2012 infrastructure. It is the primary means of distributing important network configuration information to network clients, and it provides configuration information to other network-enabled services, including Windows® Deployment Services (Windows DS) and Network Access Protection (NAP). To support and troubleshoot a Windows Server–based network infrastructure, it is important that you understand how to deploy, configure, and troubleshoot the DHCP server role.

Installing a DHCP Server Role

Using DHCP can help simplify client computer configuration. This lesson describes the benefits of DHCP, explains how the DHCP protocol works, and discusses how to control DHCP in a Windows Server 2012 network with Active Directory® Domain Services (AD DS).

Benefits of Using DHCP

The DHCP protocol simplifies configuration of IP clients in a network environment. If you do not use DHCP, each time you add a client to a network, you need to configure it with information about the network on which you installed it, including the IP address, the network's subnet mask, and the default gateway for access to other networks.

DHCP reduces the complexity and amount of administrative work by using automatic IP configuration

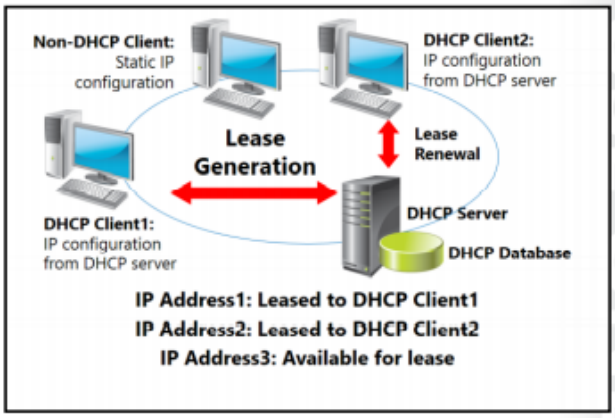
Automatic IP Configuration	Manual IP Configuration
IP addresses are supplied automatically	IP addresses are entered manually
Correct configuration information is ensured	IP address could be entered incorrectly
Client configuration is updated automatically	Communication and network issues can result
A common source of network problems is eliminated	Frequent computer moves increase administrative effort

When you need to manage many computers in a network, managing them manually can become a time-consuming process. Many corporations manage thousands of computer devices, including handhelds, desktop computers, and laptops. It is not feasible to manually manage the network IP configurations for organizations of this size.

With the DHCP server role, you can help to ensure that all clients have appropriate configuration information, which helps to eliminate human error during configuration. When key configuration information changes in the network, you can update it using the DHCP server role without having to change the information directly on each computer.

How DHCP Allocates IP Addresses

DHCP allocates IP addresses on a dynamic basis, otherwise known as a *lease*. Although you can set the lease duration to Unlimited, you typically set the duration for not more than a few hours or days. The default lease time for wired clients is eight days, and for wireless clients it is three days.



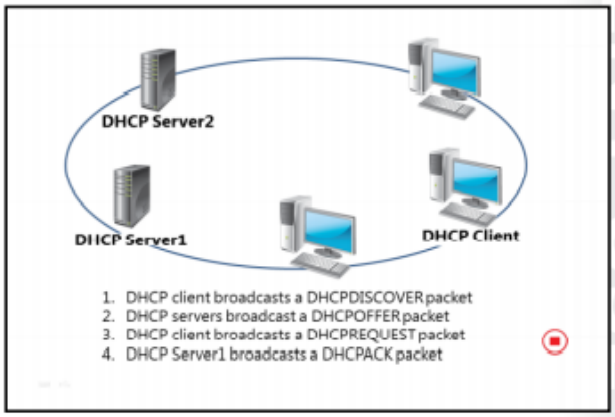
DHCP uses IP broadcasts to initiate communications. Therefore, DHCP servers are limited to communication within their IP subnet. This means that in many networks, there is a DHCP server for each IP subnet.

By default, all Microsoft operating systems are configured to obtain an IP address automatically. For a computer to be considered a DHCP client, it must be configured to obtain an IP address automatically. In a network where a DHCP server is installed, DHCP clients respond to DHCP broadcasts.

If a computer is configured with an IP address by an administrator, than that computer has a static IP address and is considered a non-DHCP client, and does not communicate with a DHCP server.

How DHCP Lease Generation Works

DHCP uses a four-step lease-generation process to assign an IP address to clients. Understanding how each step of this process works helps you troubleshoot problems when clients cannot obtain an IP address.



The following are the four steps of the DHCP lease-generation process:

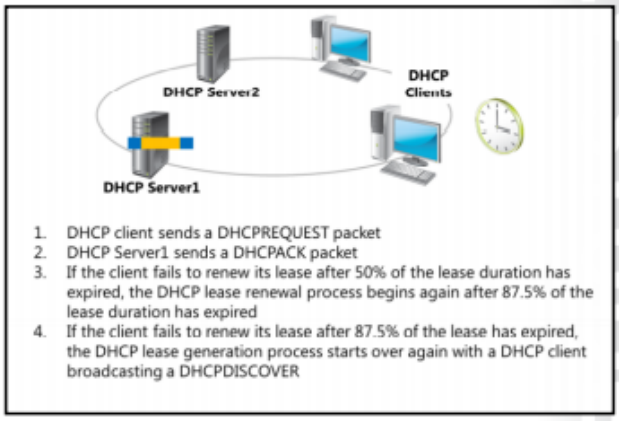
1. The DHCP client broadcasts a DHCPDISCOVER packet to every computer in the subnet. The only computers that respond are computers that have either the DHCP server role or computers or routers that are running a DHCP relay agent. In the latter case, the DHCP relay agent forwards the message to the DHCP server with which it is configured.
2. A DHCP Server responds with a DHCPOFFER packet. This packet contains a potential address for the client.

3. The client receives the DHCPOFFER packet. It might receive packets from multiple servers. If it does, it usually selects the server that made the fastest response to its DHCPDISCOVER, which typically is the DHCP server closest to the client. The client then broadcasts a DHCPREQUEST that contains a server identifier. This informs the DHCP servers that receive the broadcast which server's DHCPOFFER the client has chosen to accept.

4. The DHCP servers receive the DHCPREQUEST. Servers that the client have not accepted use this message as the notification that the client declines that server's offer. The chosen server stores the IP address client information in the DHCP database and responds with a DHCPACK message. If the DHCP server cannot provide the address that was offered in the initial DHCPOFFER, the DHCP server sends a DHCPNAK message.

How DHCP Lease Renewal Works

When the DHCP lease reaches 50 percent of the lease time, the client automatically attempts to renew the lease. This process occurs in the background. It is possible for a computer to have the same DHCP-assigned IP address for a long time if the computer is not restarted, as it will renegotiate the lease periodically.



To attempt to renew the IP address lease, the client sends a unicast DHCPREQUEST message. The server that leased the IP address originally sends a DHCPACK message back to the client. This message contains any new parameters that have changed since the original lease was created. Note that these packets are not broadcast, because the client at this point has an IP address it can use for unicast communications.

If the DHCP client cannot contact the DHCP server, then the client waits until 87.5 percent of the lease time expires. If the renewal is unsuccessful, or in other words 100 percent of the lease time has expired, then the client computer attempts to contact the configured default gateway. If the gateway does not respond, the client considers itself to be on a new subnet and enters the Discovery phase, where it attempts to obtain an IP configuration from any DHCP server, as previously described.

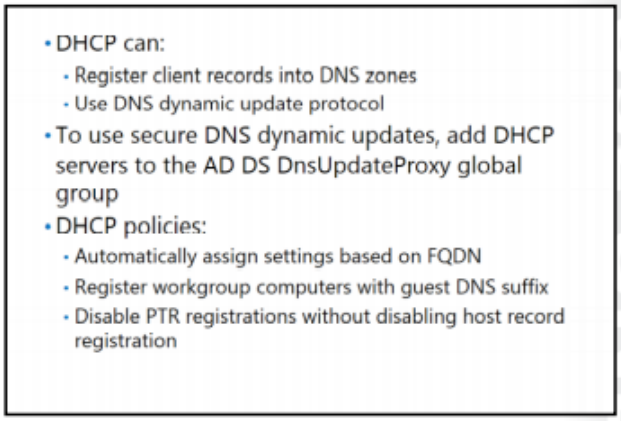
Because client computers might be moved while they are turned off, for example a laptop computer that is plugged into a new subnet, client computers also attempt renewal during the startup process, or when the computer detects a network change. If renewal is successful, the lease period is reset.

DHCP Server Failover Protocol

The DHCP role on Windows Server 2012 supports a new feature named the *DHCP Server Failover protocol*. This protocol enables synchronization of lease information between multiple DHCP servers. It also increases DHCP service availability. If one DHCP server is not available, the other DHCP servers continue to service clients in the same subnet.

How DHCP Interacts with DNS

DHCP servers are primarily used to give client computers IP addresses dynamically. DNS servers are mainly used to find an IP address based on the given name or to find a name based on a given IP address. Starting with Windows 2000, DNS clients can register their records through the DNS dynamic update protocol.



Additionally, you can configure a DHCP server to register and update client names and IP addresses with a DNS server when those DHCP clients belong to that DNS zone. DHCP option code 81 returns a client's Fully Qualified Domain Name (FQDN) to the DHCP server, which can then dynamically update the individual client's resource record back to the DNS server by using the DNS dynamic update protocol.

DNS Dynamic Update Protocol

Depending on how you configure the DNS dynamic update function on the DNS server, using the DNS dynamic update protocol might not be secure. Instead, you can configure the secure DNS dynamic update functionality. The DNS server accepts updates only from clients that are authorized to make DNS dynamic updates to the objects they represent in AD DS. When using DHCP servers and DNS servers that are set for secure DNS dynamic updates, you can add the DHCP server's computer account to the AD DS DnsUpdateProxy global group. Membership in this group ensures that the DHCP server can perform secure DNS dynamic updates for a client's resource records.

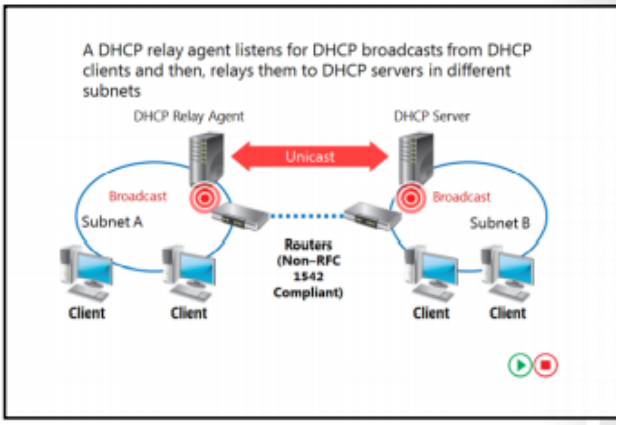
DHCP Policies

You can create DHCP policies In Windows Server 2012. Policy-based assignment allows the DHCP server to evaluate requests for IP addresses against policies that you define. The policies apply to a specific scope using a defined processing order and can be inherited from the server. When the request matches the conditions of a policy the DHCP server provides specific settings to the client. You can use DHCP policies to configure conditions based on the FQDN of the clients, and to register workgroup computers with a guest DNS suffix.

Previous to Windows Server 2012 R2, if you wanted to prevent a DNS reverse lookup record in DHCP, also known as pointer records registration (PTR), you had to disable both host and PTR record registration for DHCP clients. In Windows Server 2012 R2, you can allow a DHCP server to register a client's host record, but not the PTR record.

What Is a DHCP Relay Agent?

When initially attempting to get an IP address, DHCP clients use IP broadcasts to initiate communications Because of this, DHCP servers and clients can only communicate within their IP subnet. This means that in many networks, there is a DHCP server for each IP subnet. If there are a large number of subnets, it might be expensive to deploy servers for every subnet. A single DHCP server might service collections of smaller subnets.

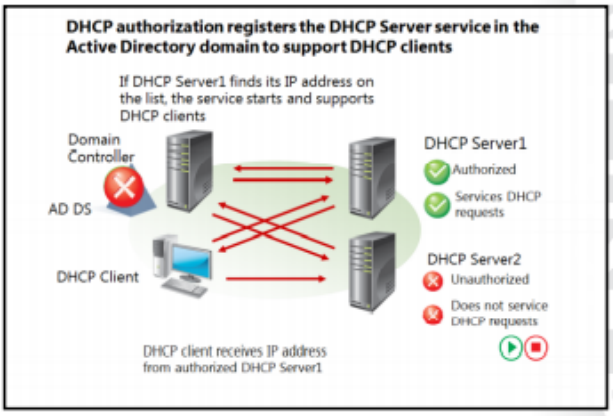


For the DHCP server to respond to a DHCP client request, it must be able to receive DHCP requests. You can enable this by configuring a DHCP relay agent on each subnet. A *DHCP relay agent* is a computer or router that listens for DHCP broadcasts from DHCP clients and then relays them to DHCP servers in different subnets.

With the DHCP relay agent, the DHCP broadcast packets can be relayed into another IP subnet across a router. Then, you can configure the DHCP relay agent in the subnet that requires IP addresses. Additionally, you can configure the agent with the IP address of the DHCP server. The agent can then capture the client broadcasts and forward them to the DHCP server in another subnet. You also can relay DHCP packets into other subnets using a router that is compatible with RFC 1542.

DHCP Server Authorization

DHCP allows a client computer to acquire configuration information about the network in which it starts. DHCP communication typically occurs before any authentication of the user or computer; and because the DHCP protocol is based on IP broadcasts, an incorrectly-configured DHCP server in a network can provide invalid information to clients. To avoid this, the server must be authorized. *DHCP authorization* is the process of registering the DHCP Server service in the Active Directory domain to support DHCP clients.



Active Directory Requirements

You must authorize the Windows Server 2012 DHCP server role in AD DS before it can begin leasing IP addresses. It is possible to have a single DHCP server providing IP addresses for subnets that contain multiple AD DS domains. Because of this, an Enterprise Administrator account must authorize the DHCP server.

Standalone DHCP Server Considerations

A standalone DHCP server is a computer that is running Windows Server 2012, that is not part of an AD DS domain, and that has the DHCP server role installed and configured. If the standalone DHCP server detects an authorized DHCP server in the domain, it does not lease IP addresses and then automatically shuts down.

Unauthorized DHCP Servers

Many network devices have built-in DHCP server software. As such, many routers can act as a DHCP server, but often these servers do not recognize DHCP-authorized servers, and might lease IP addresses to clients. In this situation you must perform an investigation to detect unauthorized DHCP servers, whether they are installed on devices or on non-Microsoft servers. Once you detect unauthorized DHCP servers, you should disable the DHCP service or functionality on them. You can find the IP address of the DHCP server by issuing the **ipconfig /all** command on the DHCP client computer.

Module 6

Lab: Implementing DHCP

Exercise 1: Implementing DHCP

▶ Task 1: Install the Dynamic Host Configuration Protocol (DHCP) server role

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In Server Manager, click **Add roles and features**.
3. In the Add Roles and Features Wizard, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, select the **DHCP Server** check box.
7. In the Add Roles and Features Wizard, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **DHCP Server** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. On the **Installation progress** page, wait until the "Installation succeeded on lon-svr1.adatum.com" message appears, and then click **Close**.

▶ Task 2: Configure the DHCP scope and options

1. In the Server Manager Dashboard, click **Tools**, and then click **DHCP**.
2. In the DHCP console, expand and then right-click **lon-svr1.adatum.com**, and then click **Authorize**.
3. In the DHCP console, right-click **lon-svr1.adatum.com**, and then click **Refresh**.

   Notice that the icons next to IPv4 IPv6 changes color from red to green, which means that the DHCP server has been authorized in Active Directory® Domain Services (AD DS).
4. In the DHCP console, in the navigation pane, click **lon-svr1.adatum.com**, expand and right-click **IPv4**, and then click **New Scope**.
5. In the New Scope Wizard, click **Next**.
6. On the **Scope Name** page, in the **Name** box, type **Branch Office**, and then click **Next**.
7. On the **IP Address Range** page, complete the page using the following information, and then click **Next**:
   - Start IP address: **172.16.0.100**
   - End IP address: **172.16.0.200**
   - Length: **16**
   - Subnet mask: **255.255.0.0**
8. On the **Add Exclusions and Delay** page, complete the page using the following information:
   - Start IP address: **172.16.0.190**
   - End IP address: **172.16.0.200**
9. Click **Add**, and then click **Next**.
10. On the **Lease Duration** page, click **Next**.
11. On the **Configure DHCP Options** page, click **Next**.
12. On the **Router (Default Gateway)** page, in the **IP address** box, type **172.16.0.1**, click **Add**, and then click **Next**.
13. On the **Domain Name and DNS Servers** page, click **Next**.
14. On the **WINS Servers** page, click **Next**.
15. On the **Activate Scope** page, click **Next**.
16. On the **Completing the New Scope Wizard** page, click **Finish**.

▶ Task 3: Configure the client to use DHCP, and then test the configuration

1. Sign in to **20410C-LON-CL1** as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the **Start** page, type **Control Panel**, and then press Enter.
3. In Control Panel, under Network and Internet, click **View Network Status and Tasks**.
4. In the Network and Sharing Center window, click **Change adapter settings**.
5. In the Network Connections window, right-click **Ethernet**, and then click **Properties**.
6. In the Ethernet Properties window, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
7. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select the **Obtain an IP address automatically** radio button, select the **Obtain DNS server address automatically** radio button, click **OK**, and then click **Close**.
8. Right-click the **Start** button, and then click **Command Prompt**.
9. In the Command Prompt window, at the command prompt, type the following, and then press Enter:

```
ipconfig /renew
```

10. To test the configuration and verify that LON-CL1 has received an IP address from the DHCP scope, at a command prompt, type the following, and then press Enter:

```
ipconfig /all
```

Note: This command returns information such as IP address, subnet mask, and DHCP enabled status, which should be **Yes**.

▶ Task 4: Configure a lease as a reservation

1. In the Command Prompt window, at a command prompt, type the following, and then press Enter:

```
ipconfig /all
```

2. Write down the Physical Address of LON-CL1 network adapter.
3. Switch to LON-SVR1.
4. In the Server Manager dashboard, click **Tools**, and then click **DHCP**.

5. In the DHCP console, expand **lon-svr1.adatum.com**, expand **IPv4**, expand **Scope [172.16.0.0] Branch Office**, select and then right-click **Reservations**, and then click **New Reservation**.
6. In the New Reservation window:
   - In the Reservation Name field, type **LON-CL1**.
   - In the IP address field, type **172.16.0.155**.
   - In the MAC address field, type the physical address you wrote down in step 2.
   - Click **Add**, and then click **Close**.
7. Switch to **LON-CL1**.
8. In the Command Prompt window, at a command prompt, type the following, and then press Enter:

```
ipconfig /release
```

   This causes LON-CL1 to release any currently leased IP addresses.
9. At a command prompt, type the following, and then press Enter:

```
ipconfig /renew
```

   This causes LON-CL1 to lease any reserved IP addresses.
10. Verify that the IP address of LON-CL1 is now **172.16.0.155**.

Results: After completing this exercise, you should have implemented DHCP, configured DHCP scope and options, and configured a DHCP reservation.

▶ Prepare for the optional exercise

If you are going to complete the optional lab, revert the 20410C-LON-CL1 and 20410C-LON-SVR1 virtual machines by performing the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410C-LON-CL1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 1 through 3 for 20410C-LON-SVR1.
5. Start 20410C-LON-SVR1.

Exercise 2: Implementing a DHCP Relay Agent (Optional Exercise)

▶ Task 1: Install a DHCP relay agent

1. Sign in to LON-RTR as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In Server Manager, click **Tools**, and then click **Routing and Remote Access**.
3. Add the DHCP relay agent to the router by performing the following steps:
   a. In the navigation pane, expand **LON-RTR (local)**, expand **IPv4**, right-click **General**, and then click **New Routing Protocol**.
   b. In the Routing protocols list, click **DHCP Relay Agent**, and then click **OK**.

▶ Task 2: Configure a DHCP relay agent

1. In the navigation pane, right-click **DHCP Relay Agent**, and then click **New Interface**.
2. In the New Interface for DHCP Relay Agent dialog box, click **Ethernet 2**, and then click **OK**.
3. In the DHCP Relay Agent Properties – Ethernet 2 Properties dialog box, click **OK**.
4. Right-click **DHCP Relay Agent**, and then click **Properties**.
5. In the DHCP Relay Agent Properties dialog box, in the Server address box, type **172.16.0.11**, click **Add**, and then click **OK**.
6. Close **Routing and Remote Access**.

▶ Task 3: Test the DHCP relay agent with a client

Note: To test how a client receives an IP address from the DHCP relay agent in another subnet, you need to create another DHCP scope.

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. In the **Desktop**, right-click the **PowerShell** icon and select **Run as administrator**.
3. At a Windows PowerShell command prompt, type the following, pressing Enter after each line:

```
Add-WindowsFeature  -IncludeManagementTools dhcp

netsh dhcp add securitygroups

Restart-service dhcpserver

Add-DhcpServerInDC  LON-SVR1  172.16.0.11

Add-DhcpServerv4Scope -Name "Branch Office 2" -StartRange 10.10.0.100 -EndRange
10.10.0.200 -SubnetMask 255.255.0.0

Add-Dhcpserverv4ExclusionRange -ScopeID 10.10.0.0 -StartRange 10.10.0.190 -EndRange
10.10.0.200

Set-DhcpServerv4OptionValue -Router 10.10.0.1

Set-DhcpServerv4Scope -ScopeID 10.10.0.0 -State Active
```

4. To test the client, switch to **LON-CL2**.
5. On the Start screen, type **Control Panel**, and then press Enter.
6. Under Network and Internet, click **View network status and tasks**.
7. In the Network and Sharing Center window, click **Change Adapter Settings**, right-click **Ethernet,** and then click **Properties**.

8. In the Ethernet Properties window, click **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.
9. In the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box, click **Obtain an IP address automatically**, click **Obtain DNS server address automatically**, click **OK**, and then click **Close**.
10. Right-click the Start button and then click Command Prompt.
11. In the Command Prompt window, at a command prompt, type the following, and then press Enter:

```
ipconfig /renew
```

12. Verify that IP address and DNS server settings on LON-CL2 are obtained from DHCP Server scope **Branch Office 2**, installed on **LON-SVR1**.

Note: The IP address should be in the following range: **10.10.0.100/16** to **10.10.0.200/16**.

Results: After completing this exercise, you should have implemented a DHCP relay agent.

▶ Prepare for the next module

After you finish the lab, revert the virtual machines back to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the Virtual Machines list, right-click **20410C-LON-DC1**, and then click **Revert**.
3. In the Revert Virtual Machine dialog box, click **Revert**.
4. Repeat steps 2 and 3 for 20410C-LON-SVR1, 20410C-LON-RTR, and 20410C-LON-CL2.