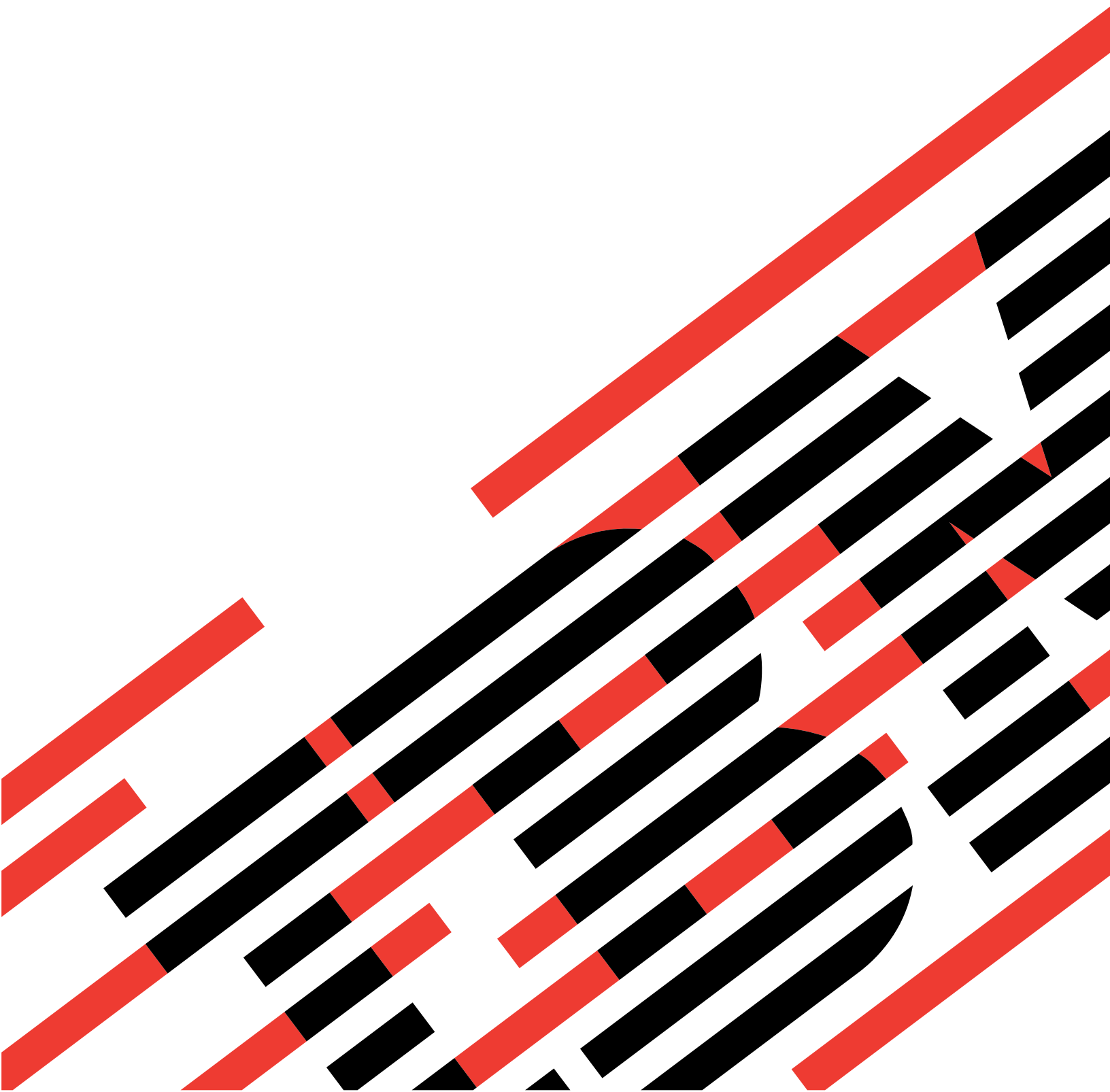


IBM

@server

iSeries
DHCP





@server

iSeries

DHCP

Contents

DHCP	1
What's new for V5R1	1
Print this topic	2
DHCP examples	2
Example: Simple DHCP subnet	3
Example: Multiple TCP/IP subnets	4
Example: DHCP and multihoming	6
Example: DNS and DHCP on the same iSeries server	9
Example: DNS and DHCP on different iSeries servers	11
Example: PPP and DHCP on a single iSeries server	13
Example: DHCP and PPP profile on different iSeries servers	15
DHCP concepts	18
DHCP client-server interaction	19
Leases	21
Relay agents and routers	23
DHCP client support	23
BOOTP	24
Dynamic updates	24
DHCP options lookup	25
Planning for DHCP	25
Network topology considerations	25
Configuring DHCP	28
Configuring the DHCP server	28
Configuring the clients to use DHCP	29
Configuring DHCP to send dynamic updates to DNS	31
Managing leased IP addresses	32
Troubleshooting DHCP	32
Problem: Clients are not receiving an IP address or their configuration information	33
Problem: Duplicate IP address assignments on the same network	34
Problem: DNS records are not being updated by DHCP	34
Problem: DHCP job log has DNS030B messages with errno1 of 3447	35
Other information about DHCP	36

DHCP

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard that uses a central server to manage IP addresses and other configuration details for an entire network. A DHCP server responds to requests from clients, dynamically assigning properties to them.

For information about new features of DHCP, see [What's new for V5R1](#). To print the DHCP topic as a single file, see [Print this topic](#).

Understanding DHCP

These topics are designed to help you understand DHCP fundamentals and plan to use DHCP on your iSeries(TM).

DHCP examples provides diagrams and explains how DHCP works.

DHCP concepts explains how DHCP interacts with clients and how it works in a network.

Planning for DHCP helps you determine how DHCP should be set up for your network.

Using DHCP

These topics are designed to help you create and manage your iSeries DHCP server.

Configuring DHCP

This topic provides instructions for setting up your DHCP server and clients, and for configuring DHCP to send dynamic updates to DNS.

Managing leased IP addresses

This topic introduces the DHCP Server Administration tool, which can help you to monitor and manage leases.

Troubleshooting DHCP

This topic provides instructions for viewing job log and trace data, and provides troubleshooting lists for common problems.

If the topics above do not provide the information you need, refer to [Other information about DHCP](#) for other reference sources.

What's new for V5R1

For Version 5 Release 1 (V5R1), the following features have been added to DHCP:

Dynamic DNS updates

In past releases, DNS records had to be maintained manually. With V5R1, you can configure your DHCP server to update resource records on your DNS server. DHCP can update reverse-lookup pointer (PTR) records and address mapping (A) records on behalf of its clients. This reduces maintenance for DNS administrators. For more information, refer to [Dynamic updates](#).

DHCP proxy client support

The DHCP server can be used to allocate IP addresses to Point-to-Point (PPP) clients. This allows you to more efficiently assign IP addresses from a pool to regular clients and PPP clients.

Improved unlisted client support

In past releases, the unlisted client support option had to be set to Yes or No at a global level. If No was selected, all clients that the administrator wanted to support had to be entered manually by client ID (such as MAC addresses). For V5R1, DHCP has been updated to offer new unlisted client support

options. You can choose to support unlisted clients using BOOTP, DHCP, or both. In addition, you can control unlisted client support by setting the preference at the global, subnet, and class levels.

New information


The DHCP topic is new to the Information Center for V5R1. DHCP examples help to introduce basic DHCP concepts. You may want to refer to the examples as you plan and configure DHCP for your iSeries. Troubleshooting information is available to help you debug your server configuration.

Print this topic

To view or download the PDF version, select DHCP (about 359 KB or 46 pages).

To save a PDF on your workstation for viewing or printing:

1. Open the PDF in your browser (click the link above).
2. In the menu of your browser, click **File**.
3. Click **Save As...**
4. Navigate to the directory in which you would like to save the PDF.
5. Click **Save**.

If you need Adobe Acrobat Reader to view or print these PDFs, you can download a copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

DHCP examples

Looking at how someone else has used a technology is often the best way to learn about that technology. Therefore, the following examples show how DHCP works, how it is incorporated into different network setups, and how to tie in some of the new V5R1 function. It is a great place to start if you are a beginner to DHCP or if you are an experienced DHCP administrator.

Example: Simple DHCP subnet

Describes setting up the iSeries server as a DHCP server in a simple LAN with a four PC clients and a LAN based printer.

Example: Multiple TCP/IP subnets

Describes setting up the iSeries server as a DHCP server for two LANs connected by a DHCP-enabled router.

Example: DHCP and multihoming

Describes setting up the iSeries server as a DHCP server for a LAN that is connected to the Internet by an Internet router.

Example: DNS and DHCP on the same iSeries server

Describes setting up the iSeries server as a DHCP server with dynamic DNS updates for a simple LAN.

Example: DNS and DHCP on different iSeries servers

Describes setting up DHCP and DNS on two different iSeries servers to perform dynamic updates over a simple LAN.

Example: PPP and DHCP on a single iSeries server

Describes setting up the iSeries server as a DHCP server for a LAN and a remote dial-in client.

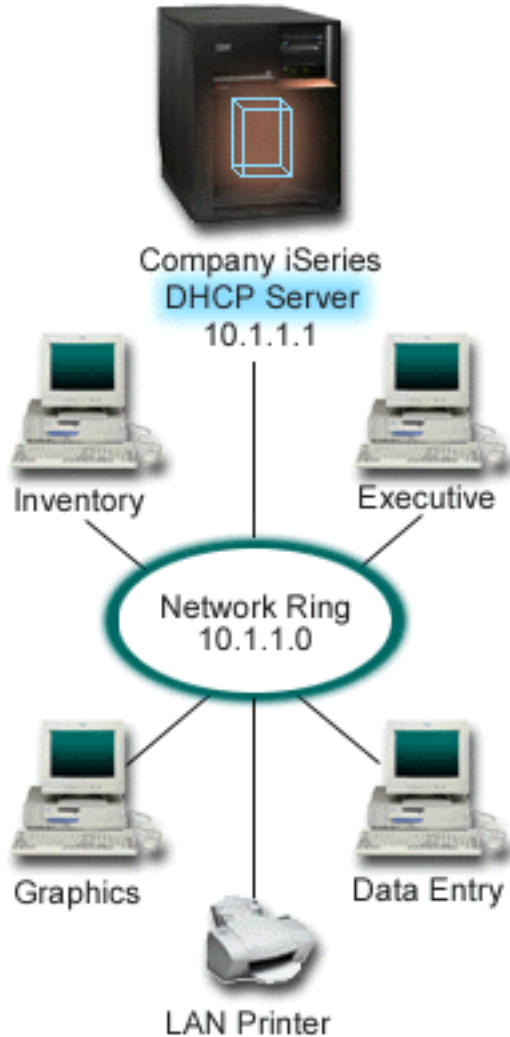
Example: DHCP and PPP profile on different iSeries servers

Describes setting up two iSeries servers as the network DHCP server and a DHCP/BOOTP relay agent for two LANs and remote dial-in clients.

Example: Simple DHCP subnet

The following figure illustrates a simple LAN with a iSeries server, four PC clients, and a LAN based printer. In this example, the iSeries server acts as a DHCP server for the 10.1.1.0 IP subnet. It is connected to the LAN with its 10.1.1.1 interface.

Figure 2-1. Simple LAN setup for iSeries server.



With so few PC clients, administrators could easily type in each PC's IP information statically. They would only need to visit four PCs in this case. Now imagine that the four PCs became 200 PCs. Setting up each PC's IP information would now become a time consuming task that could result in accuracy errors too. DHCP can simplify the process of assigning IP information to clients. If the subnet 10.1.1.0 had hundreds of clients, an administrator would only have to create a single DHCP policy on the iSeries server. This policy would distribute IP information to each client.

When the PC clients send out their DHCP DISCOVER signals, the iSeries server will respond with the appropriate IP information. In this example, the company also has a LAN based printer that obtains its IP information with DHCP too. But because the PC clients depend on the printer's IP address remaining the

same, the network administrator should account for that in the DHCP policy. One solution would be to assign a constant IP address to the printer. The DHCP server allows you to define a client in the DHCP policy like the LAN printer by its MAC address. In the DHCP client definition, you can then assign specific values such as IP addresses and router addresses to the intended client.

For a client to communicate with a TCP/IP network, it requires at least an IP address and subnet mask. The clients will get their IP address from the DHCP server, and the DHCP server passes additional configuration information (for example, their subnet mask) using the configuration options.

Planning the DHCP setup for a simple LAN

Table 2-1: Global configuration options (applies to all clients served by the DHCP server).

Object	Value
Configuration options	
option 1: Subnet mask	255.255.255.0
option 6: Domain name server	10.1.1.1
option 15: Domain name	mycompany.com
Subnet addresses not assigned by server	10.1.1.1 (Domain name server)
Is the server performing DNS updates?	No
Is the server supporting BOOTP clients?	No

Table 2-2: Subnet for PCs.

Object	Value
Subnet name	SimpleSubnet
Addresses to manage	10.1.1.2 - 10.1.1.150
Lease time	24 hours (default)
Configuration options	
Inherited options	Options from Global configuration

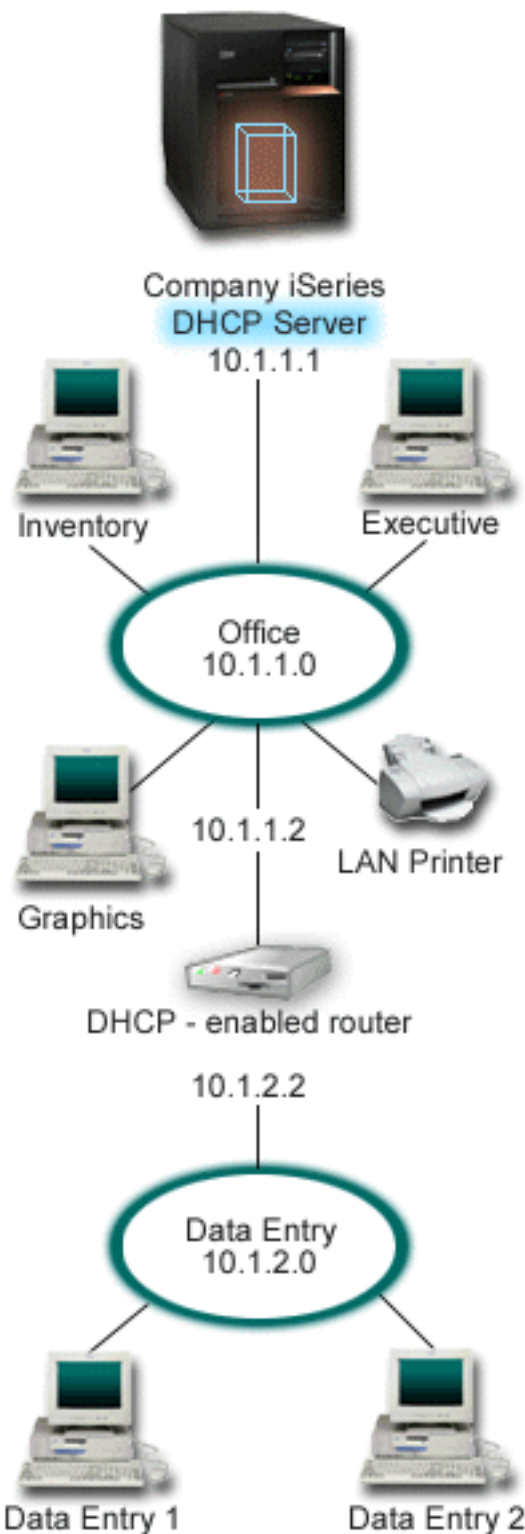
Table 2-3: Client for Printer.

Object	Value
Client Name	LANPrinter
Client Address	10.1.1.5
Configuration options	
Inherited options	Options from Global configuration

Example: Multiple TCP/IP subnets

This example is similar to the previous example, Simple DHCP subnet, except that there is now an additional TCP/IP subnet. Suppose the office and data entry clients are on different floors of a office building and separated with a router. If the network administrator wants all of the clients to receive their IP information through DHCP, this situation presents some unique differences from a simple DHCP subnet. The following figure shows an example network layout for an iSeries DHCP server connected to two LANs using a router between the networks. The figure intentionally has a limited number of clients as to not become cluttered. A real world situation would have considerably more clients on each subnet.

Figure 3-1. Multiple LANs connected through a router.



The router that connects the two networks must be enabled to pass DHCP DISCOVER packets. If it is not, the data entry clients will not be able to receive their IP information and access the network. Also, the DHCP policy would need two subnet definitions—one for the data entry and office subnets. At a minimum, the only difference between the subnets would be their IP subnets and router addresses. The data entry subnet would need to receive a router address of 10.1.2.2 to communicate with the office subnet.

Planning the DHCP setup for multiple LANs

Table 3-1: Global configuration options (applies to all clients served by the DHCP server).

Object	Value
Configuration options option 1: Subnet mask option 6: Domain name server option 15: Domain name	255.255.255.0 10.1.1.1 mycompany.com
Subnet addresses not assigned by server	10.1.1.1 (Domain name server)
Is the server performing DNS updates?	No
Is the server supporting BOOTP clients?	No

Table 3-2: Subnet for Office clients.

Object	Value
Subnet name	Office
Addresses to manage	10.1.1.3 - 10.1.1.150
Lease time	24 hours (default)
Configuration options option 3: Router Inherited options	10.1.1.2 Options from Global configuration
Subnet addresses not assigned by server	10.1.1.2 (Router)

Table 3-3: Subnet for Data Entry clients.

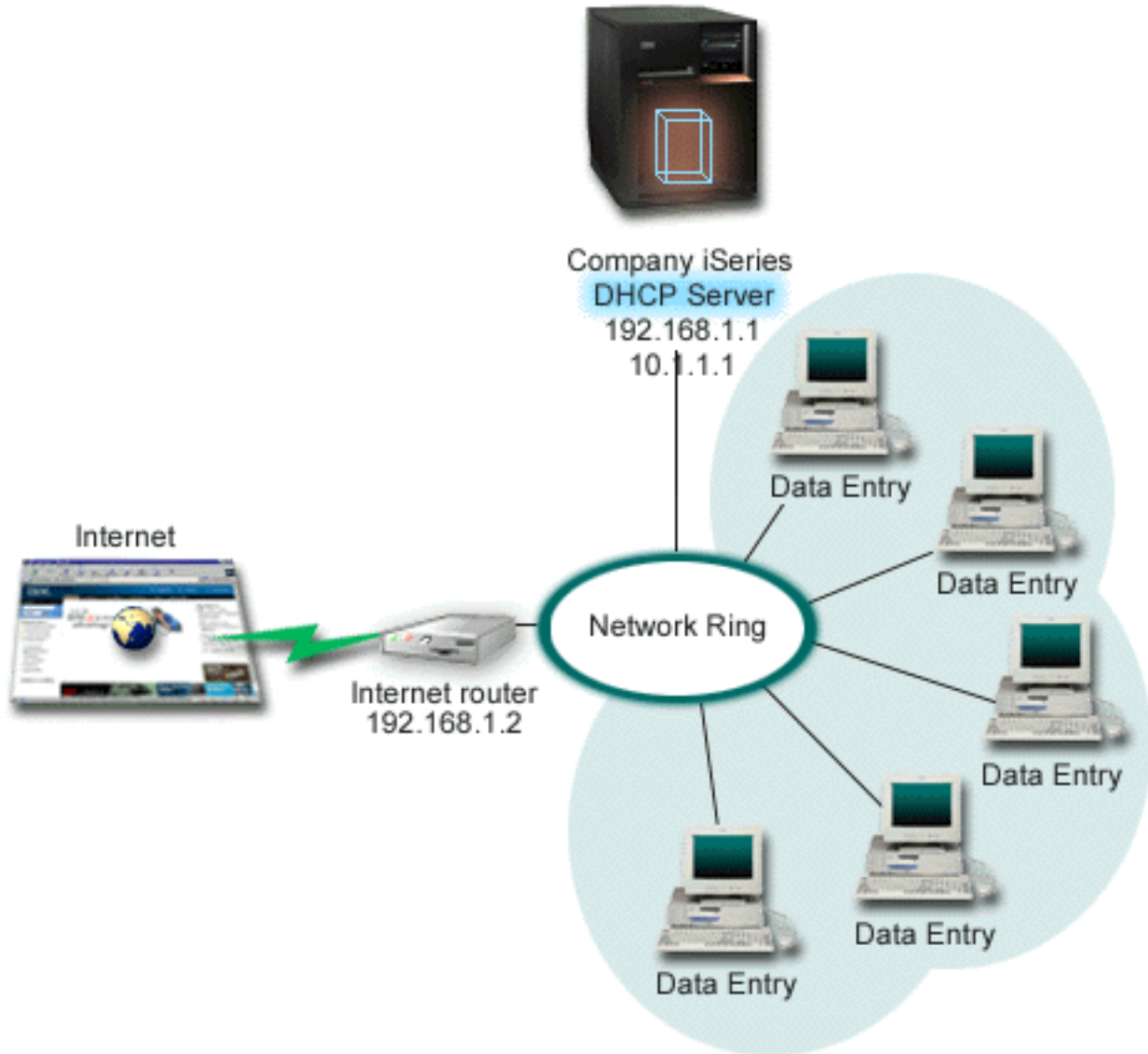
Object	Value
Subnet Name	DataEntry
Addresses to manage	10.1.2.3 - 10.1.2.150
Lease time	24 hours (default)
Configuration options option 3: Router Inherited options	10.1.2.2 Options from Global configuration
Subnet addresses not assigned by server	10.1.2.2 (Router)

Example: DHCP and multihoming

This example is much like the first example, Simple DHCP subnet. In this example, the data entry clients are only communicating amongst themselves and the iSeries server. They obtain their IP information dynamically from the iSeries' DHCP server.

However, a new version of their data entry application requires that the network communicates with the Internet, and the company decided to provide Internet access through an Internet router as shown below in Figure 4-1. In addition to the router, the administrator also added another interface with an IP address to communicate with the Internet. When multiple IP addresses are assigned to the same adapter, the iSeries is multihoming.

Figure 4-1. Using DHCP with multiple IP addresses assigned to the same adapter.



Note: Although this is a feasible way to connect your network to the Internet, it is not the most secure. It suits the purposes of this DHCP example, but you should consider the security implications when you configure your own DHCP server.

The DHCP setup must take into account that the iSeries server is known by two different IP addresses. To understand how to setup DHCP correctly for this scenario, it is helpful to understand what happens when a client sends out a DHCP DISCOVER packet.

When a client sends out a DHCP DISCOVER packet, it is broadcast on the ring. Therefore, iSeries cannot determine which IP address the packet was intended for. If this packet is marked with the 10.1.1.1 interface IP (the one used for DHCP), your clients would receive their IP information as expected. But it is possible that the packet could actually get marked with the 192.168.1.1 address (the one connected to the Internet). If the packet was received on the 192.168.1.1 interface, your data entry client would not receive any IP information.

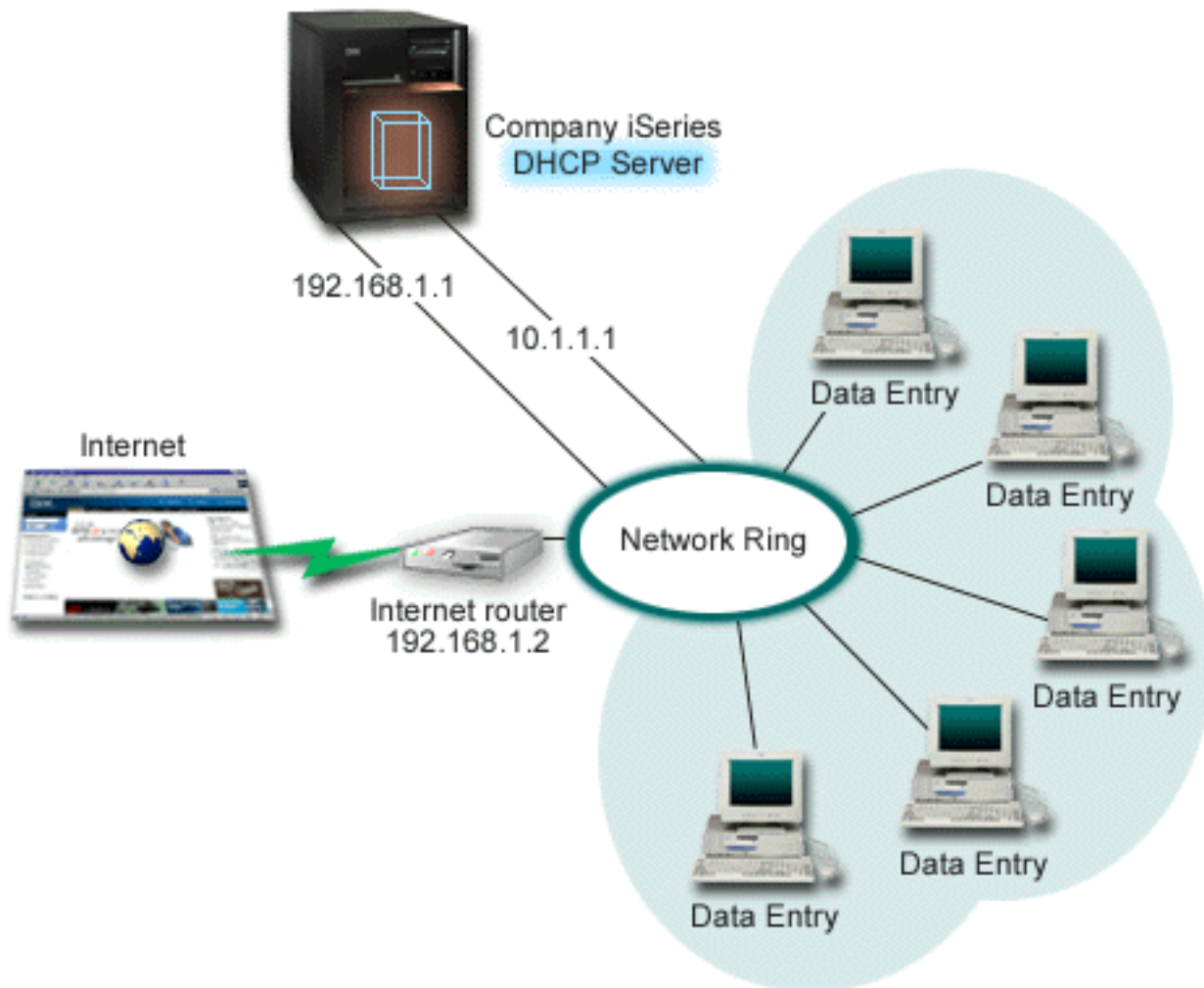
To set up DHCP in this situation, you need to not only create the data entry DHCP subnet but also one for the Internet network. The Internet policy consists of a subnet with no available addresses. The easiest way

to do this is to define the subnet with at least one IP address (like 192.168.1.1), then exclude that same IP address. With the two subnets defined, you now combine the two (or more) subnets into a subnet group. If the DISCOVER packet gets marked with the 192.168.1.1 interface, the data entry subnet will still issue valid IP information.

To make this scenario work, the policy for the Data Entry subnet must pass its clients their router address for access to the Internet. In this case, the router address is the iSeries interface of 10.1.1.1. You must also set IP Datagram forwarding to 'on' for the two interfaces to route packets to each other. This example uses reserved IP addresses to represent both internal and external IP addresses. If your network matches this scenario, you would need to also use NAT for your Data Entry clients to communicate with the Internet.

Using subnet groups to eliminate this marking problem is not only limited to multihoming examples. Any time multiple interfaces connect to the same network, you can encounter the same problem. The following figure illustrates how the iSeries server can have two physical connections to the data entry network. This network configuration would require a similar DHCP group policy as the multihoming setup, because DHCP DISCOVER packets could conceivably be answered by the 192.168.1.1 interface.

Figure 4-2. Using DHCP with multiple interfaces connected to the same network.



Planning the DHCP setup for multihoming

Table 4-1: Global configuration options (applies to all clients served by the DHCP server).

Object	Value
Is the server performing DNS updates?	No
Is the server supporting BOOTP clients?	No

Table 4-2: Subnet for Data Entry clients.

Object	Value
Subnet Name	DataEntry
Addresses to manage	10.1.1.2 - 10.1.1.150
Lease time	24 hours (default)
Configuration options	
option 1: Subnet mask	255.255.255.0
option 3: Router	10.1.1.1
option 6: Domain name server	10.1.1.1
option 15: Domain name	mycompany.com
Subnet addresses not assigned by server	10.1.1.1 (Router, DNS server)

Table 4-3: Subnet for Internet clients (empty Subnet).

Object	Value
Subnet Name	Internet
Addresses to manage	192.168.1.1 - 192.168.1.1
Subnet addresses not assigned by server	192.168.1.1 (All IP addresses available)

Table 4-4: Subnet group for all incoming DISCOVER packets.

Object	Value
Subnet Group Name	Multihomed
Subnets included in group	Subnet Internet Subnet DataEntry

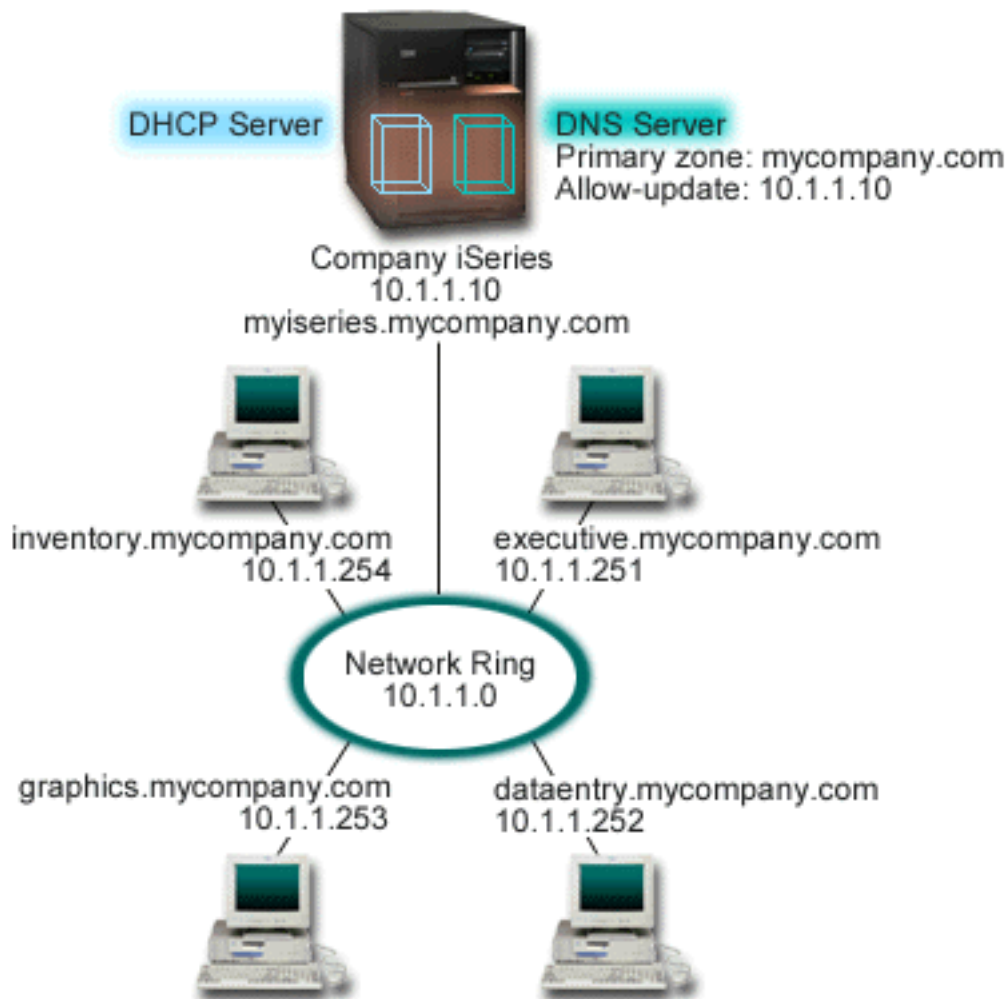
Other setup

- Set IP Datagram forwarding to 'on' for the two interfaces
- Set up NAT for the Data Entry clients

Example: DNS and DHCP on the same iSeries server

Figure 5-1 illustrates how the iSeries server can act as a DHCP and DNS server for a simple subnet. In this work environment, suppose that the inventory, data entry, and executive clients create documents with graphics from the graphics file server. They connect to the graphics file server by a network drive to its host name.

Figure 5-1. Dynamic DNS and DHCP.



Previous versions of DHCP and DNS were independent of each other. If DHCP assigned a new IP address to a client, the DNS records had to be manually updated by the administrator. In this example, if the graphics file server's IP address changed because it is assigned by DHCP, then its dependent clients would be unable to map a network drive to its host name because the DNS records would contain the file server's previous IP address.

With the new DNS server delivered in V5R1, you can dynamically update your DNS records in conjunction with intermittent address changes through DHCP. For example, when the graphics file server renews its lease and is assigned an IP address of 10.1.1.250 by the DHCP server, the associated DNS records would be updated dynamically. This would allow the other clients to query the DNS server for the graphics file server by its host name without interruption.

You can configure DHCP to update resource records on address mapping (A) records and reverse-lookup pointer (PTR) records on behalf of a client. The A record maps a client's host name to its IP address. The PTR record maps a client's IP address to its host name. For each record that is updated dynamically, an associated text (TXT) record will be written to identify that the record was written by DHCP. You can choose to allow DHCP to update both A and PTR records, or just PTR records. For more information about how to configure DNS to accept dynamic updates, refer to Example: DNS and DHCP on the same iSeries server in the DNS topic.

Note: If you set DHCP to update only PTR records, you must configure DNS to allow updates from clients

so that each client can update its A record. Not all DHCP clients support making their own A record update requests. Consult the documentation for your client platform before choosing this method.

To enable DNS updates, you must create a DNS key for your DHCP server. The DNS key authorizes the DHCP server to update the DNS records based on IP addresses it has distributed. Then, in the DHCP configuration, choose the scope level where you want DNS updates to occur. For example, if you want all subnets to perform DNS updates, set the updates at the Global level. If you want only one subnet to perform updates, then set only that subnet to update.

Planning the DHCP setup when using Dynamic DNS

Table 5-1: Global configuration options (applies to all clients served by the DHCP server).

Object	Value
Configuration options	
option 1: Subnet mask	255.255.255.0
option 6: Domain name server	10.1.1.10
option 15: Domain name	mycompany.com
Is the server performing DNS updates?	Yes — Both A and PTR records
Is the server supporting BOOTP clients?	No

Table 5-2: Subnet for Network Ring.

Object	Value
Subnet name	NetworkSubnet
Addresses to manage	10.1.1.250 - 10.1.1.254
Lease time	24 hours (default)
Configuration options	
Inherited options	Options from Global configuration

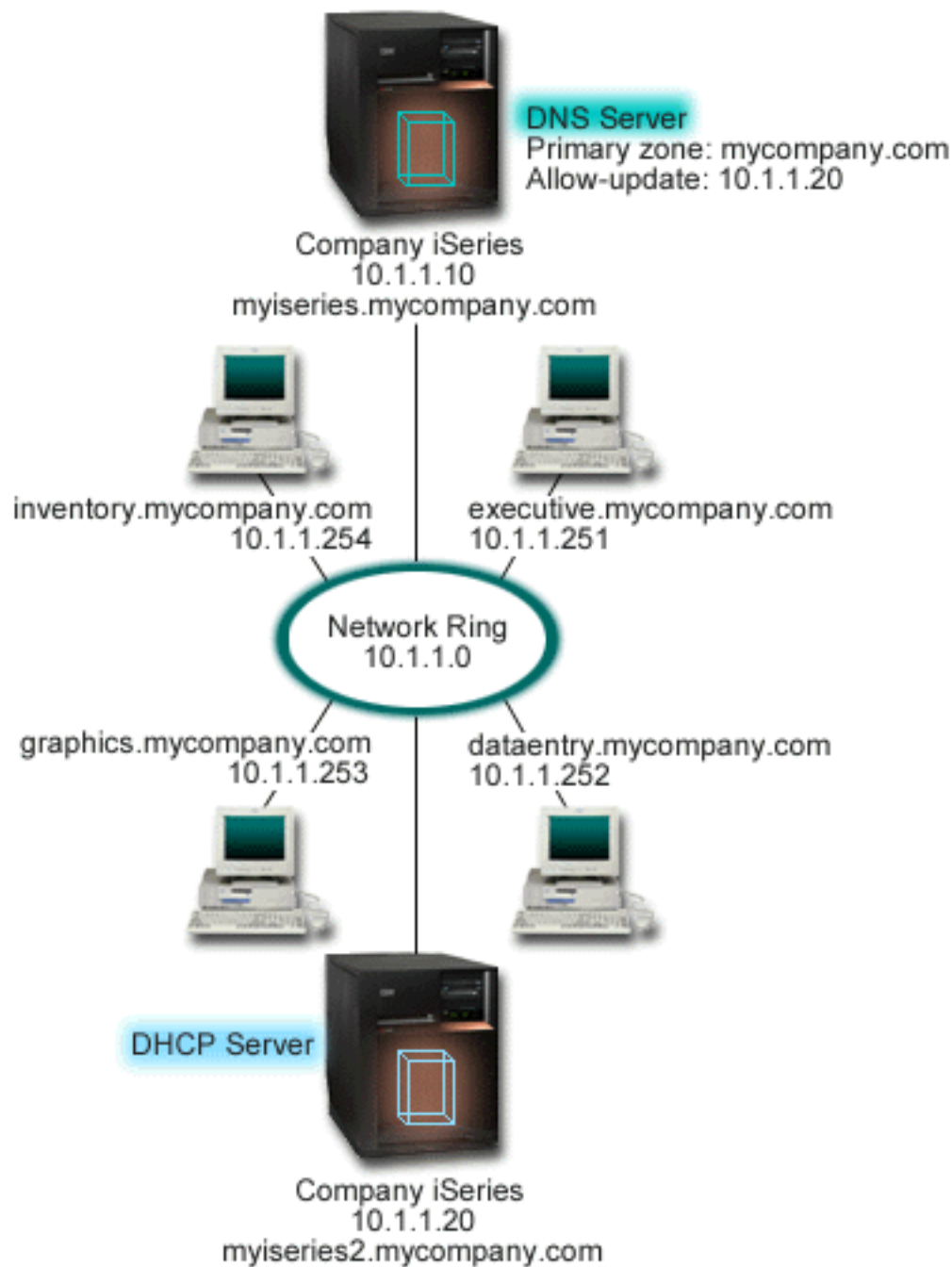
Other setup:

- Authorize DHCP to send updates to DNS.
Refer to Example: DNS and DHCP on the same iSeries server in the DNS topic.

Example: DNS and DHCP on different iSeries servers

The illustration below depicts a small subnet network with DNS and DHCP running on separate iSeries servers. The iSeries running DNS will be configured the same as when DNS and DHCP were on the same iSeries. However, there are some additional steps to configure the DHCP server to send dynamic updates.

Figure 6-1. DNS and DHCP on different iSeries servers



Planning the DHCP setup when using Dynamic DNS

- Refer to Example: DNS and DHCP on the same iSeries server for examples of the global configuration options and subnet settings.

Other setup:

- **Install OS/400 Option 31**

Install OS/400 Option 31 on the iSeries that will be running DHCP, in this case, myiseries2. This option contains the dynamic update API that manages the resource record update process. Refer to DNS system requirements for installation instructions.

- **Authorize DHCP to send updates to DNS.**

You must authorize the DHCP server to send updates to the DNS server. You can either repeat the process of defining the Dynamic Update Key, or you can send the file and place it in the proper directory path.

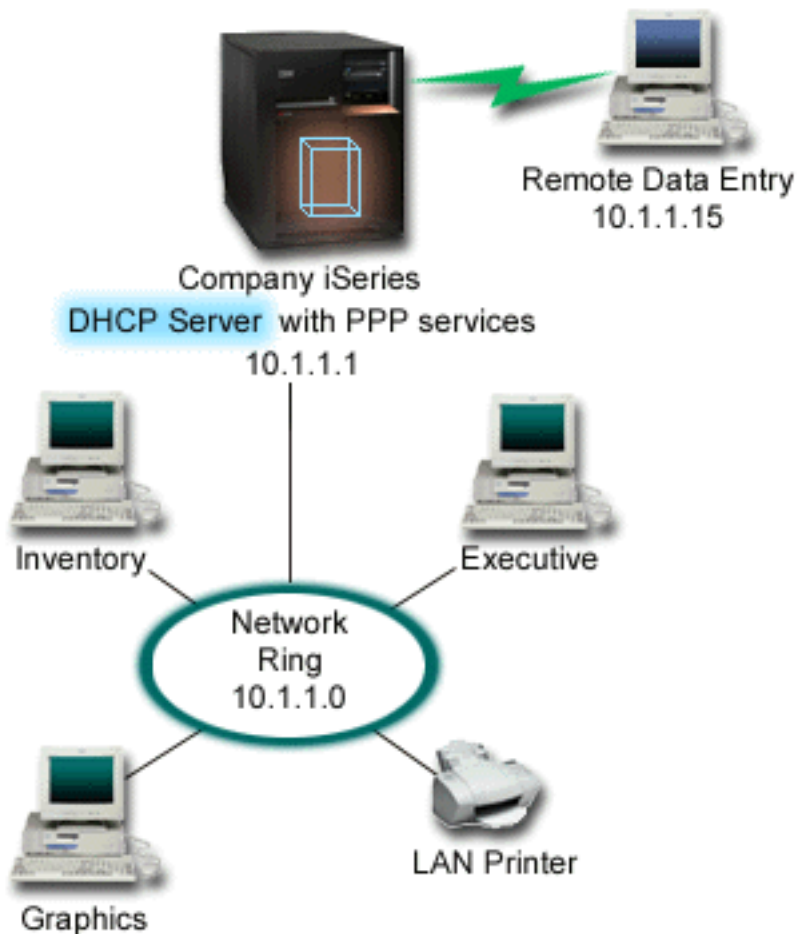
To create a Dynamic Update Key on both iSeries servers, follow these steps:

1. In **iSeries Navigator**, expand **your iSeries server** —> **Network** —> **Servers** —> **DNS**.
2. In the left pane, right-click **DNS** and select **Manage Dynamic Update Keys...**
3. On the **Managing Dynamic Update Keys** page, select **Add...**
4. On the **Add Dynamic Update Keys** page, complete the following fields:
 - **Key name:** Specify the name for the key, for example `mycompany.key`. The key name must be dot-terminated.
 - **Dynamic update zones:** Specify the zone names for which this key will be valid. You can specify more than one zone.
 - **Generate key:** Select the method you want to use to generate a secret key.
5. Repeat the steps above so that the same key is defined on both the iSeries running DNS and the iSeries running DHCP.

Example: PPP and DHCP on a single iSeries server

Remote clients such as dial-in clients often require access to a company's network. Dial-in clients can gain access to an iSeries server with PPP. To access the network, the dial-in client will need IP information just like any direct-attached network client. An iSeries DHCP server can distribute IP address information to a PPP dial-in client just like it is any other directly attached client. The following figure shows a remote employee that needs to dial into the company's network to do some work.

Figure 7-1. PPP and DHCP on a single iSeries server.



For the remote employee to successfully become part of the company's network, the iSeries server must use a combination of Remote Access Services and DHCP. The Remote Access Services function creates the dial-in capability for the iSeries server. If set up properly, once the worker establishes the dial-in connection, the PPP server tells the DHCP server to distribute TCP/IP information to the worker.

In this example, a single DHCP subnet policy would cover both the on-site network clients and the dial-in clients.

If you want your PPP profile to defer to the DHCP for IP distribution, you must do so in the PPP profile. In the TCP/IP settings of the receiver connection profile, you must set the Remote IP address assignment method from Fixed to DHCP. To allow the dial-in clients to communicate with other network clients like the LAN printer, you must also allow IP forwarding in the TCP/IP settings of the profile and the TCP/IP configuration (stack) properties. If you only set IP forwarding on in the PPP profile, the iSeries server will not pass the IP packets. You must set IP forwarding on in both the profile and stack.

Also, the Local Interface IP address in the PPP profile must be an IP address which falls within the subnet definition in the DHCP server. In this example, the PPP profile Local Interface address would be 10.1.1.1. This address should also be excluded from the DHCP server's address pool so that it is not assigned to a DHCP client.

Planning the DHCP setup for on-site and PPP clients

Table 7-1: Global configuration options (applies to all clients served by the DHCP server).

Object	Value
Configuration options	
option 1: Subnet mask	255.255.255.0
option 6: Domain name server	10.1.1.1
option 15: Domain name	mycompany.com
Is the server performing DNS updates?	No
Is the server supporting BOOTP clients?	No

Table 7-2: Subnet for both on-site and dial-in clients.

Object	Value
Subnet Name	MainNetwork
Addresses to manage	10.1.1.3 - 10.1.1.150
Lease time	24 hours (default)
Configuration options	
Inherited options	Options from Global configuration
Subnet addresses not assigned by server	10.1.1.1 (Local interface address specified in the TCP/IP Settings of the Receiver Connection Profile properties in iSeries Navigator)

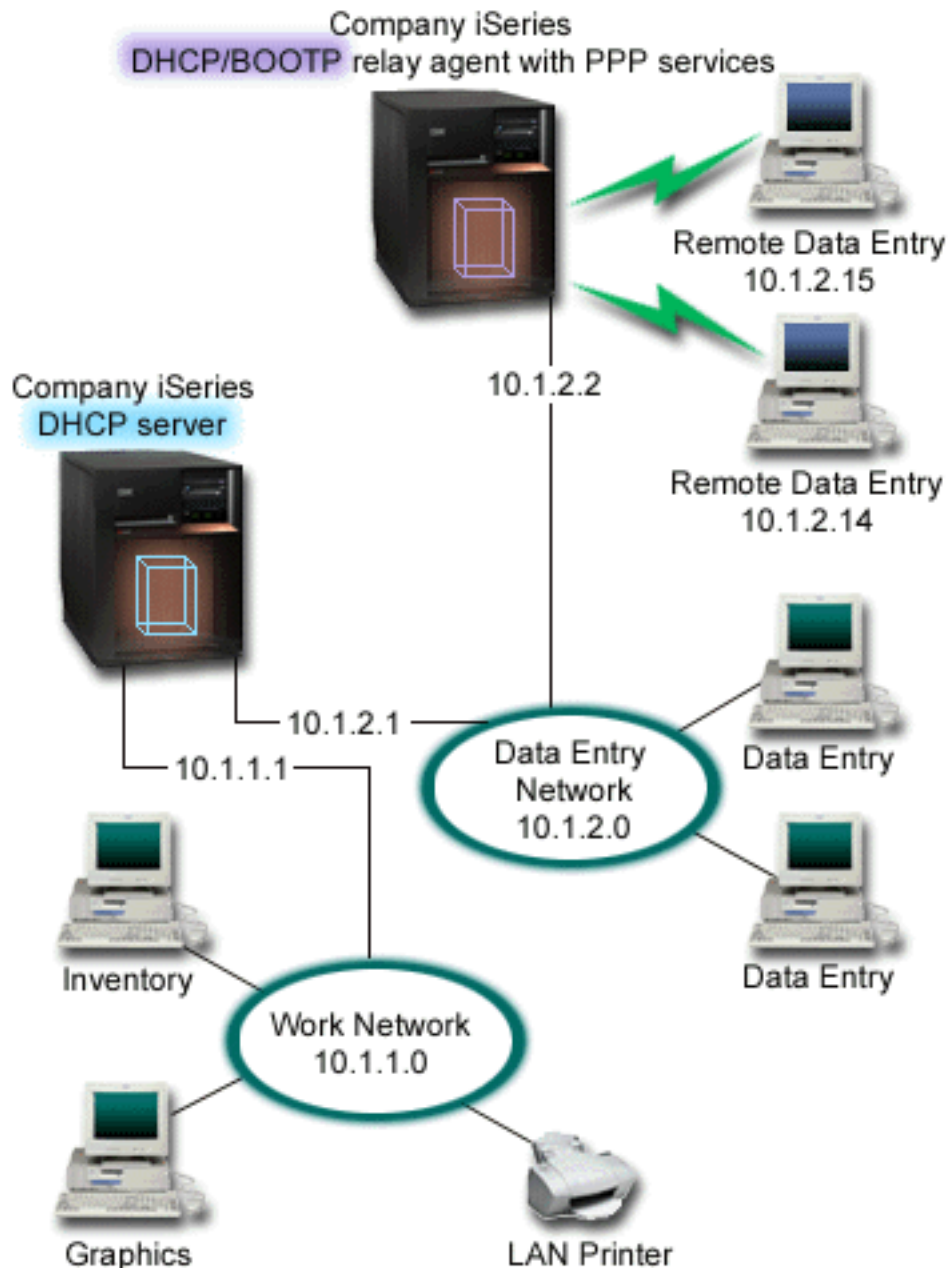
Other setup

- Set the Remote IP address method to DHCP in the PPP receiver connection profile
 1. Enable DHCP WAN client connection with a DHCP server or relay connection using the Services menu item for Remote Access Services in iSeries Navigator
 2. Select to Use DHCP for the IP address assignment method under the TCP/IP Settings Properties of the Receiver Connection Profile in iSeries Navigator
- Allow remote system to access other networks (IP forwarding) under the TCP/IP Settings Properties of the Receiver Connection Profile in iSeries Navigator
- Enable IP datagram forwarding under the Settings Properties of the TCP/IP Configuration in iSeries Navigator

Example: DHCP and PPP profile on different iSeries servers

The previous example, PPP and DHCP on a single iSeries server, shows how to use PPP and DHCP on a single iSeries server to permit dial-in clients access to a network. Whether it is the physical layout of your network or security concerns, it may be more desirable to have the PPP and DHCP servers separated or to have a dedicated PPP server without DHCP services. The following figure represents a network which has dial-in clients but the PPP and DHCP policies are on different servers.

Figure 8-1. DHCP and PPP profile on different iSeries servers.



The Remote Data Entry clients dial into the iSeries PPP server. The PPP profile on that server must have a remote IP address method of DHCP like in the previous example as well as IP Forwarding in the PPP profile and the TCP/IP stack properties. Furthermore, because this server is acting as a DHCP relay agent, the BOOTP/DHCP Relay Agent TCP/IP server must be on. This allows the iSeries Remote Access server to pass on DHCP DISCOVER packets to the DHCP server. The DHCP server will then respond and distribute TCP/IP information to the dial-in clients through the PPP server.

The DHCP server is responsible for distributing IP addresses to both the 10.1.1.0 and 10.1.2.0 networks. In the Data Entry network, it will give out IP addresses from 10.1.2.10 to 10.1.2.40 to either dial-in or directly-attached network clients. The data entry clients also need a router address (option 3) of 10.1.2.1 to communicate with the Work network and the iSeries DHCP server must also have IP forwarding enabled.

Also, the Local Interface IP address in the PPP profile must be an IP address which falls within the subnet definition in the DHCP server. In this example, the PPP profile Local Interface address would be 10.1.2.2. This address should also be excluded from the DHCP server's address pool so that it is not assigned to a DHCP client. The Local Interface IP address must be an address to which the DHCP server can send reply packets to.

Planning the DHCP setup for DHCP with a DHCP relay agent

Table 8-1: Global configuration options (applies to all clients served by the DHCP server).

Object	Value
Configuration options	
option 1: Subnet mask	255.255.255.0
option 6: Domain name server	10.1.1.1
option 15: Domain name	mycompany.com
Is the server performing DNS updates?	No
Is the server supporting BOOTP clients?	No

Table 8-2: Subnet for Work Network.

Object	Value
Subnet Name	WorkNetwork
Addresses to manage	10.1.1.3 - 10.1.1.150
Lease time	24 hours (default)
Configuration options	
Inherited options	Options from Global configuration
Subnet addresses not assigned by server	none

Table 8-3: Subnet for Data Entry Network.

Object	Value
Subnet Name	DataEntry
Addresses to manage	10.1.2.10 - 10.1.2.40
Lease time	24 hours (default)
Configuration options	
option 3: Router	10.1.2.1
Inherited options	Options from Global configuration
Subnet addresses not assigned by server	10.1.2.1 (Router) 10.1.2.15 (Remote Data Entry client's local interface IP address) 10.1.2.14 (Remote Data Entry client's local interface IP address)

Other setup on the iSeries running PPP

- Set up the BOOTP/DHCP Relay Agent TCP/IP server

Object	Value
Interface address	10.1.2.2
Relay packets to Server IP address	10.1.2.1

- Set the Remote IP address method to DHCP in the PPP receiver connection profile
 1. Enable DHCP WAN client connection with a DHCP server or relay connection using the Services menu item for Remote Access Services in iSeries Navigator
 2. Select to Use DHCP for the IP address assignment method under the TCP/IP Settings Properties of the Receiver Connection Profile in iSeries Navigator
- Allow remote system to access other networks (IP forwarding) under the TCP/IP Settings Properties of the Receiver Connection Profile in iSeries Navigator (to allow the remote clients to communicate with the Data Entry Network)
- Enable IP datagram forwarding under the Settings Properties of the TCP/IP Configuration in iSeries Navigator (to allow the remote clients to communicate with the Data Entry Network)

DHCP concepts

DHCP provides an automated method for dynamic client configuration. Clients that are DHCP enabled automatically obtain their own IP address and configuration parameters from the server. This process occurs through a series of steps.

DHCP client-server interaction

Describes the details of how a client gets the DHCP information from the server, the specific messages that are sent between the client and the server, and how leases are obtained and returned.

Leases

Describes what DHCP leases are and poses some questions to consider when determining the lease time for your DHCP clients.

Relay agents and routers

Describes when you might need to use a DHCP relay agent in your network and when a router would be sufficient. It will also describe using both a DHCP relay agent and a router to efficiently and securely transfer data throughout the network.

DHCP client support

Describes using DHCP to manage each client in your network individually, rather than managing all of the clients as a large group (subnet). This DHCP setup method only allows the clients identified by the DHCP server to receive IP address and configuration information.

BOOTP

Describes what BOOTP is, gives some history about BOOTP and DHCP, and talks about whether your DHCP server needs to support BOOTP clients.

DHCP dynamic updates

Describes using your DHCP server in conjunction with your DNS server to dynamically update the client information in the DNS when DHCP assigns the client an IP address.

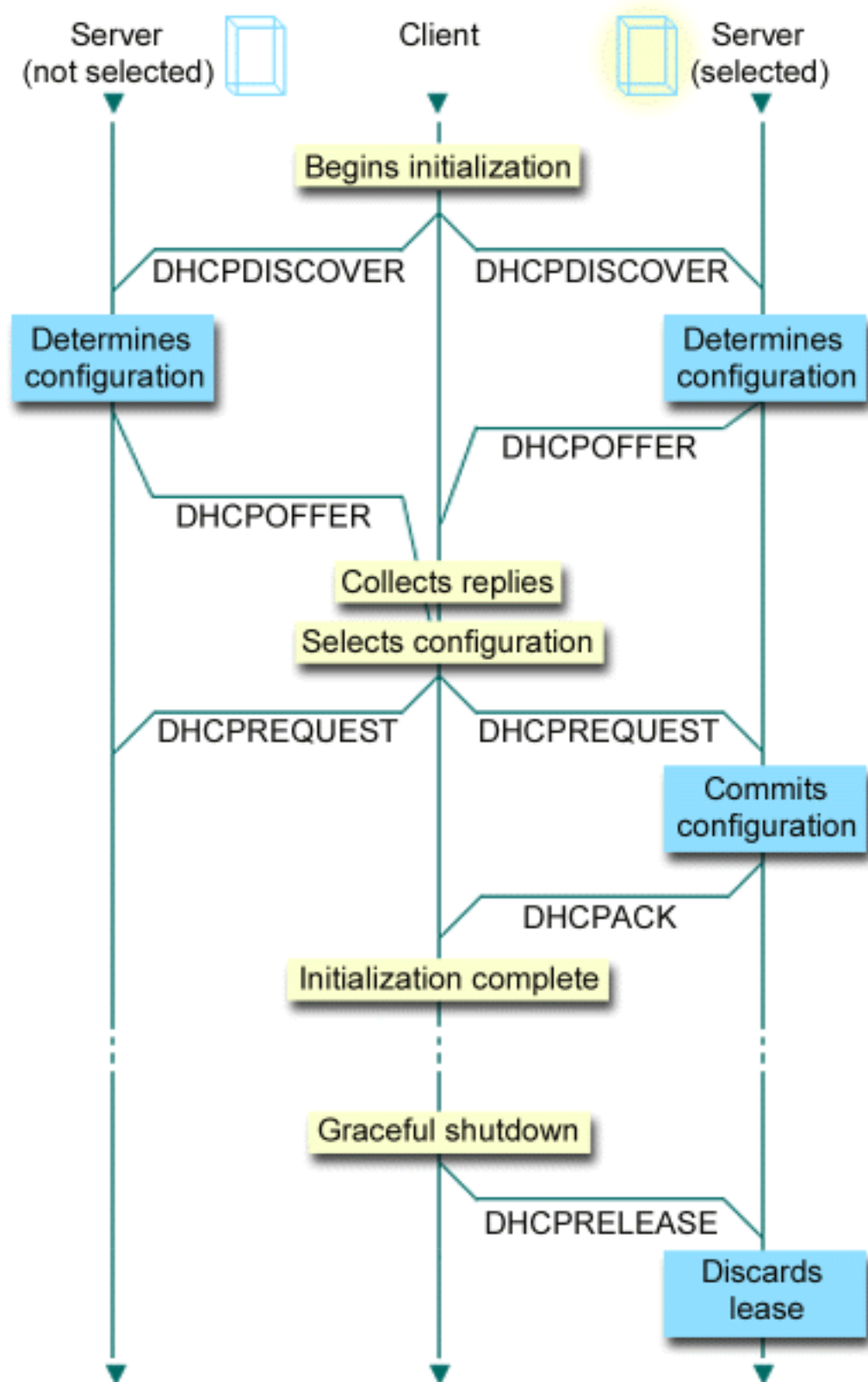
DHCP Options

DHCP has many configuration options that can be sent to the client when they request information from the DHCP server. This topic provides a lookup tool that describes all of the DHCP options.

DHCP client-server interaction

DHCP provides an automated method for dynamic client configuration. Clients that are DHCP enabled automatically obtain their own IP address and configuration parameters from the server. This process occurs through a series of steps, illustrated below.

Figure 1-1. DHCP client-server interaction.



Client requests DHCP information: DHCPDISCOVER

First, the client sends out a DISCOVER message requesting an IP address. The DISCOVER message contains an identifier unique to the client (usually the MAC address). The message may also contain other

requests, such as requested options (for example, subnet mask, domain name server, domain name, or static route). The message is sent out as a broadcast. If the network contains routers, those routers can be configured to forward DISCOVER packets to DHCP servers on attached networks.

DHCP server offers information to client: DHCPOFFER

Any DHCP server that receives the DISCOVER message may send an OFFER message in response. The DHCP server may not send an OFFER message back to the client for multiple reasons; the most common reasons are that all available addresses are currently leased, the subnet is not configured, or the client is not supported. If the DHCP server sends an OFFER message in response, the DHCPOFFER will contain an available IP address and any other configuration information that is defined in the DHCP setup.

Client accepts DHCP server offer: DHCPREQUEST

The client receives OFFER messages from the DHCP servers that responded to the DISCOVER. The client compares the offers with the settings it requested and then selects the server it wants to use. It sends a REQUEST message to accept the offer, indicating which server it selected. This message is broadcast to the entire network to let all DHCP servers know which server was selected.

DHCP server acknowledges the client and leases the IP address: DHCPACK

If a server receives a REQUEST message, the server marks the address as leased. Servers that were not selected will return offered addresses to their available pool. The selected server sends the client an acknowledgment (DHCPACK), which contains additional configuration information.

The client may now use the IP address and configuration parameters. It will use these settings until its lease expires or until the client sends a DHCPRELEASE message to the server to terminate the lease.

Client attempts to renew the lease: DHCPREQUEST, DHCPACK

The client starts to renew a lease when half of the lease time has passed. The client requests the renewal by sending a REQUEST message to the server. If the server accepts the request, it will send a DHCPACK message back to the client. If the server does not respond to the request, the client may continue to use the IP address and configuration information until the lease expires. As long as the lease is still active, the client and server do not need to go through the DHCPDISCOVER and DHCPREQUEST process. Once the lease has expired, the client must start over with the DHCPDISCOVER process.

Client terminates the lease: DHCPRELEASE

The client terminates the lease by sending a RELEASE message to the DHCP server. The server will then return the client's IP address to the available address pool.

Leases

When DHCP sends configuration information to a client, the information is sent with a lease time. This is the length of time that the client may use the IP address it has been assigned. During the lease time, the DHCP server cannot assign that IP address to any other clients. The purpose of a lease is to limit the length of time that a client may use an IP address. A lease prevents unused clients from taking up IP addresses when there are more clients than addresses. It also allows the administrator to make configuration changes to all of the clients on the network in a limited amount of time. When the lease expires, the client will request a new lease from DHCP. If the configuration data has changed, the new data will be sent to the client at that time.

Lease Renewal

The client starts to renew a lease when half of the lease time has passed. For example, for a 24 hour lease, the client will attempt to renew the lease after 12 hours. The client requests the renewal by sending a DHCPREQUEST message to the server. The renewal request contains the current IP address and configuration information of the client.

If the server accepts the request, it will send an DHCPACK message back to the client. If the server does not respond to the request, the client may continue to use the IP address and configuration information

until the lease expires. As long as the lease is still active, the client and server do not need to go through the DHCPDISCOVER and DHCPREQUEST process. Once the lease has expired, the client must start over with the DHCPDISCOVER process.

If the server is unreachable, the client may continue to use the assigned address until the lease expires. In the above example, the client has 12 hours from when it first tries to renew the lease until the lease expires. During a 12-hour outage, new users cannot get new leases, but no leases will expire for any computer turned on at the time that the outage commences.

Determining Lease Duration

The default lease time for the DHCP server is 24 hours. The duration for which you set the lease time on your DHCP server depends on several factors. You will need to consider your goals, your site's usage patterns, and service arrangements for your DHCP server. The following questions can help you to decide on an appropriate lease time:

Do you have more users than addresses?

If so, the lease time should be short so clients do not have to wait for unused leases to expire.

Do you have a minimum amount of time that you need to support?

If your typical user is on for an hour at minimum, that suggests an hour lease at minimum.

How much DHCP message traffic can your network handle?

If you have a large number of clients or slow communication lines over which the DHCP packets will run, network traffic may cause problems. The shorter the lease, the higher the server and network load from the renewal request traffic on your network.

What kind of service plan do you have in place, and to what extent can your network handle an outage?

Consider any routine maintenance, and the potential impact of an outage. If the lease time is at least double the server outage, then running clients who already have leases will not lose them. If you have a good idea of your longest likely server outage, you can avoid such problems.

What type of network environment is the DHCP server in? What does a typical client do?

Consider what the clients do on the network that the DHCP server is servicing. For example, if you have an environment where the clients are primarily mobile, connecting to the network at varying times, usually only once or twice a day to check their e-mail, you may want a relatively short lease time. In this case, it may not be necessary to have a single IP address set aside for each and every client. By limiting the lease time, you could use fewer IP addresses to support the mobile clients.

On the other hand, if you have an office environment where most of the employees have primary workstations in a fixed location, a lease time of 24 hours may be more appropriate. It may also be necessary in this environment to have an IP address available for each client that would connect to the network during business hours. In this case, if you specified a shorter lease time, the DHCP server would be negotiating the lease renewal much more frequently with the client, causing excess network traffic.

How much does your network configuration change?

If your network topology changes quite frequently, you may want to stay away from longer leases. Long leases can be disadvantageous in cases where you need to change a configuration parameter. The length of the lease can mean the difference between having to go to every affected client and rebooting it, or merely waiting a certain amount of time for the leases to be renewed.

If your network topology rarely changes and you have enough IP addresses in your address pool, you could configure DHCP to use infinite leases — leases that never expire. However, infinite leases are not recommended. If you use an infinite lease, the IP address is leased to the client indefinitely. These clients do not need to go through any lease renewal process once they receive the infinite lease. Once an infinite

lease is assigned to a client, that address cannot be assigned to another client. Therefore, there can be problems with infinite leases if you want to assign that client a new IP address or lease the client's IP address to another client later.

You may have clients in your network, such as a file server, that will always receive the same IP address. Rather than using an infinite lease, you should assign a specific address for the client and give it a long lease time. The client still has to lease it for a given amount of time and renew the lease, but the server will reserve the IP address for that client only. Then, if you get a new file server, for example, you can just change the client identifier (MAC address) and the server will give the new file server that same address. If you had given it an infinite lease, then the DHCP server cannot give out the address again unless the lease is explicitly deleted.

Relay agents and routers

Initially, DHCP clients broadcast their DISCOVER packets because they do not know what network they are connected to. In some networks, the DHCP server may not be on the same LAN as the client. Therefore, it is necessary to forward the client's broadcasted DHCP packets to the LAN where the DHCP server is. Some routers are configured to forward DHCP packages. If your router supports DHCP packet forwarding, that is all you need. However, many routers do not forward packets that have a destination IP address of the broadcast address (DHCP packets). In this case, if the router cannot forward DHCP packets, then the LAN must have a BOOTP/DHCP Relay agent to forward the DHCP packets to the LAN with the DHCP server. Refer to Example: DHCP and PPP profile on different iSeries servers for a sample network using a relay agent and a router.

In either case, since the DHCP server is on a separate network, your clients will need to have the router option (option 3) defined that specifies the IP address of the router that connects their network to the network with the DHCP server.

In these scenarios, if you do not use a BOOTP/DHCP relay agent, you will need to add a DHCP server to the other LAN to serve those clients. To help you decide how many DHCP servers to have in your network, refer to Network topology considerations.

DHCP client support

Usually people think about using DHCP to hand out IP addresses from an address pool to a subnet of clients. Any client that requests DHCP information from the network may receive an IP address from the address pool when you use subnets, unless they are explicitly excluded by the DHCP administrator. However, the DHCP server is also capable of the inverse — limiting DHCP service to only specific clients.

The DHCP server can limit service at both the individual client level and by the type of client (BOOTP or DHCP). To limit service at the individual client level, you must identify each network client individually in your DHCP configuration. Each client is identified by their client ID (usually their MAC address). Only the clients that are identified in the DHCP configuration will be served an IP address and configuration information from the DHCP server. If a client is not listed in the DHCP configuration, it is refused service by the DHCP server. This method prevents unknown hosts from obtaining an IP address and configuration information from the DHCP server.

If you want even more control over your network clients and the configuration information they receive, you can setup your DHCP clients to receive a static IP address rather than receiving an IP address from an address pool. If you set up the client to receive a defined IP address, that client should be the only client that can receive that IP address to avoid address overlap. If you use dynamic IP address allocation, the DHCP server will manage IP address assignment for the clients.

On a broader level, the DHCP server can limit service to a client based on the type of client — BOOTP or DHCP. The DHCP server can refuse service to BOOTP clients. For more information about BOOTP clients, refer to BOOTP.

BOOTP

The Bootstrap protocol (BOOTP) is a host configuration protocol that was used before DHCP was developed. BOOTP support is a slimmed down version of DHCP. In BOOTP, clients are identified by their MAC address and are assigned a specific IP address. Essentially, each client in your network is mapped to an IP address. There is no dynamic address assignment, each network client must be identified in the BOOTP configuration, and the clients can only receive a limited amount of configuration information from the BOOTP server.

Because DHCP is based on BOOTP, the DHCP server can support BOOTP clients. If you are currently using BOOTP, you can setup and use DHCP without any impacts to your BOOTP clients. To support BOOTP clients successfully, you must specify the IP address of the bootstrap server and the boot file name option (option 67), and BOOTP support must be turned on for the entire server or various subnets.

Using DHCP to support BOOTP clients is preferred over using a BOOTP server. Even when you use DHCP to support your BOOTP clients, each BOOTP client is essentially being mapped to a single IP address, and that address is therefore not re-usable by another client. The advantage, however, of using DHCP in this case is that there is no need to configure a one-to-one mapping of BOOTP clients to IP addresses. The DHCP server will still dynamically assign an IP address to the BOOTP client from the address pool. Once the IP address is assigned to the BOOTP client, it is permanently reserved for use by that client until you explicitly delete the address reservation. Eventually, you may want to consider converting your BOOTP clients to DHCP for easier host configuration management.

For more information about using BOOTP, see the BOOTP topic.

Dynamic updates

Domain Name System (DNS) is a distributed database system for managing host names and their associated IP addresses. DNS allows users to locate hosts using simple names, such as "www.jktoys.com", rather than by using the IP address (xxx.xxx.xxx.xxx).

In the past, all DNS data was stored in static databases. All DNS resource records had to be created and maintained by the administrator. Now, DNS servers running BIND 8 can be configured to accept requests from other sources to update zone data dynamically.

You can configure your DHCP server to send update requests to the DNS server each time it assigns a new address to a host. This automated process reduces DNS server administration in rapidly growing or changing TCP/IP networks, and in networks where hosts change locations frequently. When a client using DHCP receives an IP address, that data is immediately sent to the DNS server. Using this method, DNS can continue to successfully resolve queries for hosts, even when their IP addresses change.

You can configure DHCP to update address mapping (A) records, reverse-lookup pointer (PTR) records, or both on behalf of a client. The A record maps the client's DNS name to its IP address. The PTR record maps a host's IP address to its host name. When a client's address changes, DHCP can automatically send an update to the DNS server so other hosts in the network can locate the client through DNS queries at its new IP address. For each record that is updated dynamically, an associated text (TXT) record will be written to identify that the record was written by DHCP.

Note: If you set DHCP to update only PTR records, you must configure DNS to allow updates from clients so that each client can update its A record.

Dynamic zones are secured by creating a list of authorized sources that are allowed to send updates. DNS verifies that incoming request packets are coming from an authorized source before updating the resource records.


Dynamic updates can be performed between DNS and DHCP on a single iSeries server, different iSeries servers, or to other servers that are capable of dynamic updates. Refer to the following topics for more information about configuring dynamic updates for your iSeries:

- Configuring DHCP to send dynamic updates
- Configuring DNS to receive dynamic updates

DHCP options lookup

DHCP options define additional configuration data that the DHCP server passes along to clients in addition to an IP address. Typical options include subnet mask, domain name, router IP addresses, domain name server IP addresses, and static routes.

Standard DHCP options, based on definitions in RFC 2132: DHCP Options and BOOTP Vendor

Extensions  are described below. You may also configure customized options using the DHCP **Options** page.

<LABEL for="selectnameid1">Select an option from the table or enter a one-word lookup below: <LABEL>

<LABEL for="selectnameid2">Or a one-word lookup <LABEL>

Select an option to view its description.

Planning for DHCP

Setting up DHCP can be a time-consuming and error-prone process if you have not taken the time to plan how your DHCP server should be configured. By taking time to think about your network setup and security concerns in advance, you can configure your DHCP server more efficiently. The following topics pose some important questions that you should consider before you configure DHCP in your network.

Network topology considerations

You can plan for the majority of the DHCP setup just by looking at your network topology, the devices on the network (for example, routers), and how you want to support your clients in DHCP.

Security considerations

The DHCP protocol is not capable of verifying that clients requesting IP addresses are authorized to do so. Because of the nature of DHCP's interaction to the network, it is important that you secure your iSeries from outside clients. If your DHCP server is on an iSeries that is part of a trusted internal network, you may be able to use Packet rules (filtering and NAT) to further secure it from any unauthorized parties. If your DHCP server is on an iSeries that is attached to an untrusted network, such as the Internet, refer to Secureway: iSeries and the Internet. For more security references, refer to the Information Center Security topic.

Network topology considerations

Understanding your network topology

One of the most important aspects of planning a DHCP implementation is understanding your network layout or topology. When you understand your network topology, you will be able to quickly identify the IP address ranges for DHCP, the configuration information that each client needs, the devices that need to be configured to forward DHCP messages, and if DHCP can work with your DNS or PPP servers. Depending on the complexity of your network, you may even want to sketch your network topology on a piece of scrap paper. You should include all of the LANs, the devices that connect the LANs, and the IP addresses for devices and clients (for example, a printer) that need a defined IP address. You may want to look at some of the DHCP examples to help you sketch out your network topology.

Determining the number of DHCP servers

Even with a complex network, you can still manage all of your network clients using only one DHCP server. Depending on your network topology, you may need to set up a few DHCP/BOOTP relay agents or

enable your routers to forward DHCP packets to make it work. For more information about DHCP/BOOTP relay agents and routers in your network, refer to Relay agents and routers.

Using only one DHCP server for your entire network will centralize host configuration management for all of your clients. However, there are cases where you may want to consider using multiple DHCP servers in your network.

To avoid a single point of failure, you can configure two or more DHCP servers to serve the same subnet. If one server fails, the other can continue to serve the subnet. Each of the DHCP servers must be accessible either by direct attachment to the subnet or by using a DHCP/BOOTP relay agent.

Because two DHCP servers cannot serve the same addresses, address pools defined for a subnet must be unique across DHCP servers. Therefore, when using two or more DHCP servers to serve a particular subnet, the complete list of addresses for that subnet must be divided among the servers. For example, you could configure one server with an address pool consisting of 70% of the available addresses for the subnet and the other server with an address pool consisting of the remaining 30% of the available addresses.

Using multiple DHCP servers decreases the probability of having a DHCP-related network access failure, but it does not guarantee against it. If a DHCP server for a particular subnet fails, the other DHCP server may not be able to service all the requests from new clients which may, for example, exhaust the server's limited pool of available addresses.

If you are considering multiple DHCP servers, remember that multiple DHCP servers cannot share any of the same addresses. If you use more than one DHCP server in your network, each server must be configured with their own unique IP address ranges.

Identifying the IP addresses that your DHCP server should manage

Using your network topology, you should start documenting which network address ranges you want the DHCP server to manage. You should identify which devices have a manually configured IP addresses (for example, the router's IP address) that you want to exclude from the DHCP's address pool.

In addition, you will want to consider whether these addresses should be assigned dynamically by the DHCP server or if you want to assign a specific IP address to certain clients. You may want to reserve a specific address and configuration parameters for a specific client on a particular subnet, such as a file server. Or, you may want to map all of your clients to a specific IP address. Refer to DHCP client support for more information about assigning IP addresses dynamically versus statically.

Determining the lease time for the IP addresses

The default lease time for the DHCP server is 24 hours. The duration for which you set the lease time on your DHCP server depends on several factors. You will need to consider your goals, your site's usage patterns, and service arrangements for your DHCP server. For more information to help you determine the lease time for your DHCP clients, refer to Leases.

Supporting BOOTP clients

If you are currently using a BOOTP server, consider that the DHCP server can replace the BOOTP server on your network with little or no impact to your BOOTP clients. There are three options for you if you have BOOTP clients currently on your network.

The easiest option is to configure your DHCP server to support BOOTP clients. When you use DHCP to support your BOOTP clients, each BOOTP client is essentially being mapped to a single IP address, and that address is therefore not re-usable by another client. The advantage, however, of using DHCP in this case is that there is no need to configure a one-to-one mapping of BOOTP clients to IP addresses. The DHCP server will still dynamically assign an IP address to the BOOTP client from the address pool. Once the IP address is assigned to the BOOTP client, it is permanently reserved for use by that client until

you explicitly delete the address reservation. This would be a good option if you have a large number of BOOTP clients in your network. For more information about BOOTP clients, refer to BOOTP.

Another option is to migrate your iSeries BOOTP server configuration to the DHCP server. A DHCP client will be created for each BOOTP client listed in the BOOTP server configuration. In this option, it is recommended that you reconfigure your clients to be DHCP clients. However, when you migrate your BOOTP configuration to DHCP, the DHCP address assignments will work for either a BOOTP or DHCP client. This might be a good option to transition your BOOTP clients to DHCP. Your BOOTP clients will still be supported during the process of reconfiguring them to DHCP.

Eventually, you may want to do the third option: change each BOOTP client to DHCP and configure DHCP to dynamically assign them addresses. Essentially, this option removes BOOTP entirely from the network.

Identifying the configuration information for the network clients

Using your network topology layout, you can clearly see the devices (for example, routers) that must be identified in the DHCP configuration. In addition, you should identify other servers in your network, such as the Domain Name System (DNS) server, that your clients may need to know about. You can either specify this information for the entire network, a specific subnet, or a specific client regardless of the subnet.

If you have devices that apply to many clients, you will want to specify them at the highest level possible (for example, at the Global level for the entire network, or at the subnet level for a specific subnet). This will minimize the changes you will need to make to the DHCP configuration when the device changes. If you had specified the same router, for example, for every client in your network, you would need to change the configuration for every client when the router has changed. However, if you had specified the router at the global level (all of the clients will inherit this configuration information), you would only need to change the information once and the information would be changed for all clients.

Some of your clients may have unique TCP/IP configuration requirements that requires information to be configured at the client level. DHCP can recognize those clients and provide the unique configuration data to them. This is not only true for the configuration options, but also for the lease time and IP address. For example, a client may need a longer lease time than all of the other clients. Or, maybe only one client, such as a file server, needs a dedicated IP address. Identifying those clients up front and what unique information they require will help you when you start configuring the DHCP server.

For a quick reference to all of the configuration options, refer to DHCP options.

Using dynamic DNS with your DHCP server

If you are currently using a DNS server to manage all of your client's host names and IP addresses, you will definitely want to reconfigure your DNS server to accept dynamic updates from DHCP. If you use Dynamic DNS, the clients will not notice any interruption or changes in the DNS service when you switch over to DHCP. For more information about using DHCP with your DNS server, refer to Dynamic updates.

If you are not currently using a DNS server, you may want to consider adding a DNS server when you add the DHCP server. You can read the DNS Information Center topic to find out more about DNS benefits and requirements.

Using DHCP for your remote clients

If you have any remote clients that connect to your network using PPP, you can set up DHCP to dynamically assign an IP address to them when they connect to the network. To see some examples of networks where this might be useful, see Example: PPP and DHCP on a single iSeries Server or Example: DHCP and PPP profile on different iSeries servers. These examples also explain how to set up the network to use PPP and DHCP together for your remote clients.

Configuring DHCP

The following topics explain how to successfully set up DHCP in your network. You may want to read about Planning for DHCP before you start configuring DHCP on your network.

Configuring the DHCP server

Explains what software you need to use to configure the iSeries DHCP server. It also includes instructions to work with the DHCP configuration, use the DHCP Server Administration Program, and set up a DHCP/BOOTP relay agent.

Configuring the clients to use DHCP

Describes the steps to configure your Windows and OS/2 clients to request their configuration information from the DHCP server.

Configuring DHCP to send dynamic updates to DNS

Describes the steps to configure your DHCP and DNS servers to dynamically update DNS resource records when the DHCP server leases an IP address to a client.

Configuring the DHCP server

The following information explains how to work with the DHCP configuration, use the DHCP Server Administration Program, and set up a DHCP/BOOTP relay agent.

DHCP server configuration

You will need to use the DHCP server configuration function to create a new DHCP configuration or view the existing DHCP configuration. To access the DHCP server configuration:

1. In **iSeries Navigator**, expand **your iSeries server** → **Network** → **Servers** → **TCP/IP** → **DHCP**.
2. Right-click **DHCP** and select **Configuration**.

If you are creating a new DHCP configuration, you will use a wizard that helps you set up the DHCP server. This wizard asks you some of the basic configuration questions and steps you through the process of creating a subnet. After you have completed the wizard, you can change and improve the configuration to your network's needs.

If your DHCP server is already configured, the DHCP server configuration function will display the current configuration, including all of the subnets and clients that can be managed from the DHCP server and the configuration information that will be sent to the clients.

Once the DHCP server is configured, you can start or stop the DHCP server:

1. In **iSeries Navigator**, expand **your iSeries server** → **Network** → **Servers** → **TCP/IP** → **DHCP**.
2. Right-click **DHCP** and select **Start** or **Stop**.

In addition, you can configure the DHCP server to be started automatically by the iSeries server when TCP/IP is started:

1. In **iSeries Navigator**, expand **your iSeries server** → **Network** → **Servers** → **TCP/IP** → **DHCP**.
2. Right-click **DHCP** and select **Configuration**.
3. Right-click **DHCP Server** and select **Properties**.
4. Check the **Start when TCP/IP is started** checkbox.
5. Select **OK**.


If you look at the DHCP configuration frequently, you may want to create a shortcut to the DHCP configuration window on your desktop:

1. In **iSeries Navigator**, expand **your iSeries server** → **Network** → **Servers** → **TCP/IP** → **DHCP**.

2. Right-click **DHCP** and select **Create Shortcut**.

DHCP Server Administration Program

The DHCP Server Administration tool is provided to monitor active lease information for an IBM iSeries DHCP server. This graphical interface allows you to view which IP addresses are leased, how long they have been leased, and when they will be available to lease out again. In addition, you can view additional client and server statistics, such as when a client last leased an IP address, or the number of BOOTP clients the server is supporting.

For more information about the tool and its software requirements, see the Technical Studio topic DHCP Server Administration Program .

DHCP/BOOTP Relay agent

iSeries server provides a DHCP/BOOTP Relay agent that can be used to forward DHCP packets to a DHCP server on a different network. For more information about when to use a Relay agent or router, refer to Relay agents and routers.

To set up the iSeries DHCP/BOOTP Relay agent:

1. In **iSeries Navigator**, expand **your iSeries server** → **Network** → **Servers** → **TCP/IP** → **BOOTP/DHCP Relay Agent**.
2. Right-click **BOOTP/DHCP Relay Agent** and select **Configuration**.
3. Specify the interface that the relay agent will receive the DHCP packets from and the destination of where the packets should be forwarded.
4. Select **OK**.

Once the DHCP/BOOTP relay agent is configured, you can start or stop it:

1. In **iSeries Navigator**, expand **your iSeries server** → **Network** → **Servers** → **TCP/IP** → **BOOTP/DHCP Relay Agent**.
2. Right-click **BOOTP/DHCP Relay Agent** and select **Start** or **Stop**.

In addition, you can configure the BOOTP/DHCP Relay Agent to be started automatically by the iSeries server when TCP/IP is started:

1. In **iSeries Navigator**, expand **your iSeries server** → **Network** → **Servers** → **TCP/IP** → **BOOTP/DHCP Relay Agent**.
2. Right-click **BOOTP/DHCP Relay Agent** and select **Properties**.
3. Check the **Start when TCP/IP is started** checkbox.
4. Select **OK**.

Configuring the clients to use DHCP

Once the DHCP server is configured, each client must be configured to use DHCP. The following information describes the steps to configure your Windows and OS/2 clients to request their configuration information from the DHCP server. In addition, it describes how the clients can view their own DHCP lease information.

Windows 95/98/ME clients

To enable DHCP:

1. On the **Start Menu**, select **Settings** → **Control Panel**.
2. Double-click **Network** and select the **Protocols** tab.
3. Select **TCP/IP Protocol** and select the **Properties** button.

4. On the **IP Address** tab, select the **Obtain an IP address from a DHCP server** radio button.
5. Select **OK**.

Windows 95/98/ME clients have a utility that displays the client's MAC address and DHCP lease information. It also allows you to release and renew DHCP leases. To check the DHCP lease for the client:

1. Open an **MS-DOS Command Prompt**.
2. Run **WINIPCFG**.

Note: this utility does not dynamically update the displayed information, so it will be necessary to re-run the utility to view updated status.

Windows NT clients

To enable DHCP:

1. On the **Start Menu**, select **Settings** —> **Control Panel**.
2. Double-click **Network** and select the **Protocols** tab.
3. Select **TCP/IP Protocol** and select **Properties**.
4. On the **IP Address** tab, select **Obtain an IP address from a DHCP server**.
5. Select **OK**.

Windows 2000 clients

To enable DHCP:

1. On the **Start Menu**, select and **Settings** —> **Network and Dial-up Connections**.
2. Right-click the appropriate connection name and select **Properties**.
3. Select **TCP/IP Protocol** and select **Properties**.
4. On the **General** tab, select **Obtain an IP address from a DHCP server**.
5. Select **OK**.

Windows NT and Windows 2000 clients also have a utility that displays the client's MAC address and DHCP lease information. To check the DHCP lease for a Windows NT and Windows 2000 client:

1. Open an **MS-DOS Command Prompt**.
2. Run **IPCONFIG /ALL**.

Note: This utility does not dynamically update the displayed information, so it will be necessary to re-run the utility to view updated status. You can use the same utility with different parameters to release and renew a lease (IPCONFIG /RELEASE and IPCONFIG /RENEW). Run IPCONFIG /? from an MS-DOS Command Prompt to see all of the possible parameters for the command.

Windows 2000 DHCP clients need to be configured if you want the DHCP server to update DNS A records on behalf of the client. You may want to delegate updates to the DHCP server if your network has standard legacy Microsoft Windows clients like Windows 95 and NT, since these clients currently do not update DNS A records. This may simplify your DNS administration because DNS updates will originate from the DHCP server for all clients, rather than having some clients update their own records.

To disable DNS dynamic updates from the client perform the following steps:

1. On the **Start Menu**, select **Settings** —> **Network and Dial-up Connections**.
2. Right-click the appropriate connection name and select **Properties**.
3. Select **TCP/IP Protocol** and select **Properties**.
4. Select **Advanced**.
5. On the **DNS** tab, deselect the "Register this connection's addresses in DNS" and "Use this connections DNS suffix in DNS registration" options.
6. Select **OK**.

This should be done for all connections that you want to have the DNS records update delegated to the DHCP server.

OS/2 Warp 4 clients

To enable DHCP:

1. Select **TCP/IP Configuration**.
2. Select the **Obtain IP address automatically** radio button.
3. Select **OK**.

The client can be started manually from an OS/2 window by entering DHCPDCD. You can also update the client configuration file (mptn\etc\dhcpdcfg) to allow the client to request DHCP options.

Warp also has a utility for tracking leases. From an OS/2 window, enter DHCPMON, or select the DHCP monitor icon in the TCP/IP folder. The client can be terminated by entering DHCPMON -t. Note: this does not issue a DHCP release, it simply shuts the DHCP client down so that it no longer renews a lease.

You can also view the client's DHCP log file to view the client/server interaction and to see the options passed back by the server. The file name is configurable in the client config file. Some systems have a log in the root directory with file name of dhcpdc.log. In addition, previously obtained lease and option information is stored by the client in the file mptn\etc\dhcpc.db. If you ever need to restart the client "from scratch" you should erase the mptn\etc\dhcpc.db file.

Configuring DHCP to send dynamic updates to DNS

You can configure your DHCP server to send update requests to the DNS server each time it assigns a new address to a host. This automated process reduces DNS server administration in rapidly growing or changing TCP/IP networks, and in networks where hosts change locations frequently. When a client using DHCP receives an IP address, that data is immediately sent to the DNS server. Using this method, DNS can continue to successfully resolve queries for hosts, even when their IP addresses change. For more information, refer to Dynamic updates.

For record updates to occur, Option 31 must be installed on this iSeries. The DHCP server uses programming interfaces provided by Option 31 to perform dynamic updates. The DNS server can be running on a separate iSeries that is capable of performing dynamic updates. For information about verifying that Option 31 is installed, refer to DNS system requirements.

To configure DHCP properties to allow the DHCP server to perform dynamic DNS updates, follow these steps:


1. Expand **Network** —> **Servers** —> **TCP/IP**.
2. In the right pane, right-click **DHCP** and select **Configuration**.
3. In the left pane of the **DHCP Server Configuration** window, right-click **Global** and select **Properties**.
4. Select the **Options** tab.
5. Select **option 15: Domain name** from the **Selected options** list. If option 15 does not appear in the **Selected options** list, select 15: Domain name from the **Available options** list and click **Add**.
6. In the **Domain Name** field, specify the domain name the client uses when resolving host names using DNS.
7. Select the **Dynamic DNS** tab.
8. Select **DHCP server updates both A records and PTR records** or **DHCP server updates PTR records only**.
9. Set **Append domain name to host name** to **Yes**.
10. Click **OK** to close the **Global Properties** page.

Managing leased IP addresses

The DHCP configuration tool helps you set up the DHCP server, the clients it will serve, and the information that is sent to the clients. In the DHCP configuration tool, you specify the IP address pool that DHCP will manage and the lease times for those address pools. If you want to see which of the IP addresses are currently being leased, you need to use the DHCP Server Administration tool.

The DHCP Server Administration tool is provided to monitor active lease information for an IBM iSeries DHCP server. This graphical interface allows you to view which IP addresses are leased, how long they have been leased, and when they will be available to lease out again. In addition, you can view additional client and server statistics, such as when a client last leased an IP address.

You can also use the DHCP Server Administration tool to reclaim IP addresses that are no longer being used. If the DHCP address pool has been exhausted, you can look through the active lease information to determine if there are any leases that you may want to delete, making the IP address available to other clients. For example, you may have a client that is no longer on the network, but still has an active IP address lease. You can delete the active IP address lease for this client. You should only perform this operation when you are certain that the client will no longer attempt to use the address. The DHCP server will not notify the clients when you delete their active IP address lease. If you delete an active lease for a client that is still on the network without releasing the IP address from the client, you may end up with duplicate IP address assignments on your network.

For more information about the tool and its software requirements, see the Technical Studio topic DHCP Server Administration Program .

Troubleshooting DHCP

The following information is provided to help you troubleshoot problems that you may have with your DHCP server. If your problem is not listed below, review the Planning for DHCP topic to verify that you have taken everything into consideration for your DHCP configuration.

Select a problem description from the following list, or read Gathering detailed DHCP error information for directions to access server log data and trace information.

Problem: Clients are not receiving an IP address or their configuration information

Problem: Duplicate IP address assignments on the same network

Problem: DNS records are not being updated by DHCP

Problem: DHCP job log has DNS030B messages with errno1 of 3447

Gathering detailed DHCP error information

There are a couple of ways to find out the error details behind the problem you are encountering. First, you should look at the DHCP server job log:

1. In **iSeries Navigator**, expand **your iSeries server** —> **Network** —> **Servers** —> **TCP/IP** —> **DHCP**.
2. Right-click **DHCP** and select **Server Jobs**.

If there are no messages in the DHCP server job log, it may be necessary to collect the information from the iSeries Communication Trace or the DHCP server's internal program trace. The iSeries Communication Trace helps determine whether the client requests are reaching the DHCP server and whether the DHCP server is responding to the client. If the client requests are reaching the DHCP server, but the server is not responding, use the DHCP server internal program trace function. To trace the DHCP server,

1. In **iSeries Navigator**, expand **your iSeries server** → **Network** → **Servers** → **TCP/IP** → **DHCP**.
2. Right-click **DHCP** and select **Configuration**.
3. Right-click **DHCP Server** and select **Properties**.
4. Select the **Logging** properties tab.
5. Check the **Enable Logging** checkbox.
6. Verify that the **Log file name** is **dhcpsd.log**.
7. Check all of the **Log** categories except Trace and Statistics (trace and statistics logs are used only by the support line).
8. Select **OK**.
9. Right-click **DHCP Server** and select **Update Server** to restart the DHCP server if the server is already started.
10. Recreate the problem.
11. Right-click **DHCP Server** and select **Properties** → **Logging**.
12. Deselect **Enable Logging** to turn off logging.
13. Select **OK**.
14. Right-click **DHCP Server** and select **Update Server** to restart the DHCP server.
15. View the DHCP log file in 'QIBM/UserData/OS400/DHCP/dhcpsd.log'. In **iSeries Navigator**, expand **your iSeries server** → **File Systems** → **Integrated File System** → **Root** → **the file's directory**. Or, from a character-based interface, use the **wrklnk** command and select option **5=Display**.

Problem: Clients are not receiving an IP address or their configuration information

An IP address is leased to a client through a four-step process between the client and the DHCP server. All four steps must take place before the client receives an IP address. Refer to DHCP client-server interaction for details about the four-step process.

Some common reasons for this problem include:

The client is connected to a subnet that is not configured in the DHCP server.

Check the DHCP configuration and verify that all subnets managed by the DHCP server are listed in the configuration. If you are unsure about which subnets should be managed by the DHCP server, refer to Network topology considerations.

The DHCP DISCOVER message from the client cannot reach the DHCP server.

If the DHCP server does not have an IP address on the client's subnet, there must be a router or DHCP/BOOTP relay agent that can forward the client's DHCP DISCOVER message to the DHCP server. For more information, refer to Relay agents and routers. In addition to receiving the broadcast message, the server needs to be able to send reply packets back to the client's subnet.

If your iSeries is multihomed, you may need to add a Subnet Group to the DHCP configuration. For more detail on configuring DHCP for a multihomed server, see Example: DHCP and multihoming. This example describes what needs to be done to the DHCP configuration so that the client's broadcast message is received by the server.

The DHCP server does not have any available addresses for the client in the address pool.

You can use the DHCP Server Administration tool to see which addresses are currently being used by the DHCP server. Managing leased IP addresses provides more details about using the DHCP Server Administration tool. If the DHCP server has run out of available addresses, you may need to add more IP addresses to the address pool, shorten the lease time, or delete permanent leases that are no longer required.

Problem: Duplicate IP address assignments on the same network

An IP address should be unique across your network. The DHCP server will not assign a single IP address to more than one client. Under certain conditions, the DHCP server will attempt to verify that an address is not currently in use before it assigns it to a client. When the DHCP server detects that an address is being used when it should not be, it will temporarily mark that address as used and will not assign that address to any client. You can use the DHCP Server Administration tool to view which IP addresses the server has detected are in use but were not assigned by the DHCP server. These addresses will have a USED status and a UNKNOWN_TO_IBMDHCP client identifier. For more information about the tool, refer to Managing leased IP addresses.

Some common reasons for this problem include:

Multiple DHCP servers are configured to assign the same IP address.

If two DHCP servers are configured to assign the same IP address to clients, then it is possible for two different clients to receive the same IP address. One of the clients will receive the IP address from one of the DHCP servers, and another client will receive the same IP address from the other DHCP server. Multiple DHCP servers can serve the same subnet or network, but they should not be configured with the same address pool or overlapping address pools.

A client has been manually configured with an IP address which is managed by DHCP.

The DHCP server usually attempts to verify whether an IP address is currently in use before assigning it to a client. However, there is no guarantee that the manually configured client is currently connected to the network or available to respond when the DHCP server is verifying the IP address. So, the DHCP server may assign the IP address to a DHCP client. When the manually configured client connects to the network, you will have duplicate IP addresses on your network. IP addresses that are managed by DHCP should not be used to manually configure the network setup for a client. If a client needs to be manually configured with an IP address, that IP address should be excluded from the DHCP server's address pool.

Problem: DNS records are not being updated by DHCP

The iSeries DHCP server is capable of dynamically updating DNS resource records. Refer to Dynamic updates for details about this capability. The DHCP server uses normal name resolution functions and programming interfaces to determine the appropriate dynamic DNS server to update. You can use this to your advantage when determining the source of dynamic update errors.

Some things to check when the DNS records are not being updated dynamically:

Verify which subnets and the type of resource records (A and/or PTR records) are being updated.

Check the DHCP configuration and verify that the client's subnet is set up to dynamically update resource records and which type of record is being updated.

OS/400 Option 31 (Domain Name System) must be installed on the iSeries server running DHCP.

The DHCP server uses programming interfaces provided by OS/400 Option 31 (Domain Name System). The DNS that is being dynamically updated does not need to reside on the same iSeries server as the DHCP server.

Verify the DHCP server is authorized to send updates to the DNS server.

Check the DNS configuration to verify the DNS zone is configured to allow dynamic updates and that the DHCP server is included in the Access Control List.

Verify that the DNS servers can resolve the client's domain.

Display the list of DNS servers on the iSeries server where DHCP resides using the CHGTCPDMN command. Verify that these DNS servers can resolve the domain that is being updated. To do this, run NSLOOKUP from the iSeries server where DHCP is running to resolve a name (or IP address) that exists in the domain that is failing to be updated. The DHCP server must be able to derive the fully qualified domain name (FQDN) of the client to update its DNS record. The DHCP server will not attempt to update

a dynamic DNS without a FQDN (the host name and domain name of the client). The DHCP server derives the FQDN of the client using the following sequence:

1. Option 81 (Client FQDN) in the DHCPREQUEST message from the client.
2. Option 12 (Host Name) and/or Option 15 (Domain Name) in the DHCPREQUEST message from the client.
3. Option 12 (Host Name) in the DHCPREQUEST message from the client and/or Option 15 (Domain Name) configured in the DHCP server.

In this case, to derive the FQDN, the DHCP server must be configured to append the domain name to the host name (specified on the **Properties** → **Dynamic DNS** tab for the global level, subnet, class, or client).

The TXT record may not match the corresponding DNS record.

The DHCP server can be configured to check the existing DNS resource records to determine which DHCP client they are associated with. The DHCP server accomplishes this by writing a corresponding TXT record with each A and PTR record that it updates in the DNS. If the server is configured to verify the client ID before performing the DNS update, then the TXT record data must match the client ID of the client that received the address from the DHCP server. If it does not match, the DHCP server will not update the DNS A resource record. This is done to prevent overwriting existing records. However, the DHCP server can be configured to ignore the existing records and perform DNS updates regardless of the data in the TXT record (specified on the **Properties** → **Dynamic DNS** tab for the global level, subnet, class, or client).

Problem: DHCP job log has DNS030B messages with errno1 of 3447

The error code 3447 means that the DHCP server timed out waiting for a response from the DNS server while attempting to update the DNS records. This could be due to network or connection problems between the iSeries DHCP server and DNS server.

This message will be accompanied by a TCP5763 message which contains the type of DNS resource record and detailed data for the resource record that the DHCP server attempted to update.


Because the DHCP iSeries server attempts to update DNS resource records each time a lease is renewed, the resource records may already be present in the zone configuration file from the initial IP address lease or a prior lease renewal. Check the DNS zone configuration data using a tool such as NSLOOKUP. You may find that the resource record is already present with the correct data and that no action is necessary.







If the resource record is not present in DNS there are several ways to update the resource record. The DHCP iSeries server will attempt to update the resource record at the next lease renewal request. So, you could wait until that occurs. Or, many clients attempt to renew or reacquire an IP address when they are powered on. You may want to try to reboot the client which could cause the DHCP server to attempt to update the DNS resource records again.

If neither of these options work for you, you can update the DNS resource records manually. This method is not recommended because the dynamic zone must not be running when manual updates are made. So, other dynamic updates from the DHCP server will be lost during this down-time. However, there are dynamic update utilities provided by some client and BIND DNS server implementations. You could use the dynamic update utility to update the resource record. While similar in process to manually updating the zone (an administrator must enter the resource record data to be updated), dynamic update utilities allow the zone to be updated while the zone is active.


Other information about DHCP

DHCP RFCs

Requests for Comments (RFCs)  are written definitions of protocol standards and proposed standards used for the Internet. The following RFCs may be helpful for understanding DHCP and related functions:

- RFC 2131: Dynamic Host Configuration Protocol (obsoletes RFC 1541) 
- RFC 2132: DHCP Options and BOOTP Vendor Extensions 
- RFC 951: The Bootstrap Protocol (BOOTP) 
- RFC 1534: Interoperation Between DHCP and BOOTP 
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol 
- RFC 2136: Dynamic Updates in the Domain Name System (DNS UPDATE) 

IBM Manuals and Redbooks

- AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support 
This redbook describes the Domain Name System (DNS) server and Dynamic Host Configuration Protocol (DHCP) server support that are included in OS/400. The information in this redbook helps you install, tailor, configure, and troubleshoot the DNS and DHCP support through examples.
Note: This redbook has not been updated to include the new BIND 8 features, including dynamic updates, that are available for V5R1. However, it is a good reference for general DNS and DHCP concepts.



Printed in U.S.A.