System i

Networking
Dynamic Host Configuration Protocol

Version 6 Release 1

System i

Networking
Dynamic Host Configuration Protocol

Version 6 Release 1

Note

Before using this information and the product it supports, read the information in "Notices," on page 57.

This edition applies to version 6, release 1, modification 0 of IBM i5/OS (product number 5761-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

Contents

Dynamic Host Configuration Protocol

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.

PDF file for DHCP

You can view and print a PDF file of this information.

To view or download the PDF version of this document, select DHCP (about 1399 KB).

Saving PDF files

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

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe® Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Related reference

"Related information for DHCP" on page 54
IBM Redbooks® and Web sites contain information that relates to the DHCP topic collection. You can view or print any of the PDF files.

DHCP concepts

Dynamic Host Configuration Protocol (DHCP) provides an automated method for dynamic client configuration. Here are some DHCP-related concepts to help you better understand DHCP.

DHCP client/server interaction

The interaction between Dynamic Host Configuration Protocol (DHCP) clients and servers enables a client to obtain its IP address and corresponding configuration information from a DHCP server.

This process occurs through a series of steps, illustrated in the following figure.

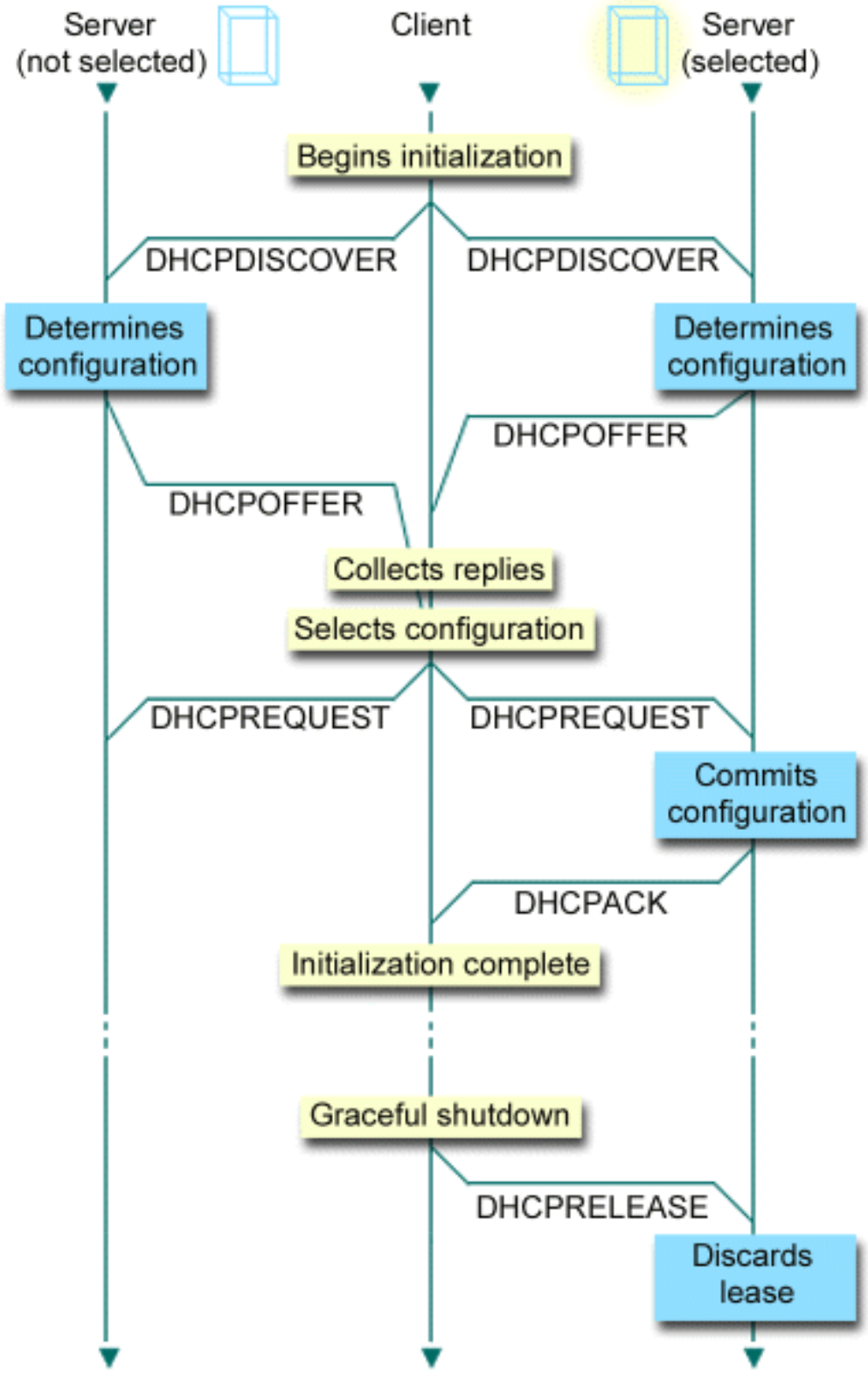


Figure 1. DHCP client-server interaction

Client requests DHCP information: DHCPDISCOVER

First, the client sends out a DHCPDISCOVER message requesting an IP address. The DHCPDISCOVER message contains an identifier unique to the client (typically the MAC

address). The message might 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 DHCPDISCOVER packets to DHCP servers on attached networks.

DHCP server offers information to client: DHCPOFFER
Any DHCP server that receives the DHCPDISCOVER message might send a DHCPOFFER message in response. The DHCP server might not send a DHCPOFFER 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 a DHCPOFFER 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 DHCPOFFER messages from the DHCP servers that responded to the DHCPDISCOVER messages. The client compares the offers with the settings that it requested, and then selects the server that it wants to use. It sends a DHCPREQUEST 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 DHCPREQUEST message, the server marks the address as leased. Servers that are 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 might 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 end 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 DHCPREQUEST 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 might 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. When the lease has expired, the client must start over with the DHCPDISCOVER process.

Client ends the lease: DHCPRELEASE
The client ends the lease by sending a DHCPRELEASE message to the DHCP server. The server will then return the client's IP address to the available address pool.

Related concepts

"Relay agents and routers" on page 5
You can use Dynamic Host Configuration Protocol (DHCP) relay agents and routers to efficiently and securely transfer data throughout the network.

"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 can use the IP address it has been assigned. The duration of the lease time can be changed according to your specific requirement.

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 can use the IP address it has been assigned. The duration of the lease time can be changed according to your specific requirement.

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 can use an IP address. A lease prevents unused clients

from taking up IP addresses when there are more clients than addresses. It also enables 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 can continue to use the IP address and configuration information until the lease expires. If the lease is still active, the client and server do not need to go through the DHCPDISCOVER and DHCPREQUEST process. When the lease has expired, the client must start over with the DHCPDISCOVER process.

If the server is unreachable, the client can continue to use the assigned address until the lease expires. In the previous 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 starts.

Determining lease duration

The default lease time for the DHCP server is 24 hours. When setting the lease time on your DHCP server, consider your goals, usage patterns of your site, and service arrangements for your DHCP server. Use the following questions to help you decide on an appropriate lease time.

Do you have more users than addresses?
If so, the lease time must be short so that clients do not need 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 might cause problems. The shorter the lease, the heavier traffic the server and network load from the renewal request 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 twice the server outage time, 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, and checking their e-mail typically only once or twice a day, you might want a relatively short lease time. In this case, it might not be necessary to have a single IP address set aside for every client. By limiting the lease time, you can use fewer IP addresses to support the mobile clients.

Alternatively, if you have an office environment where most of the employees have primary workstations in a fixed location, a lease time of 24 hours might be more appropriate. It might also be necessary in this environment to have an IP address available for each client that connects to

the network during business hours. In this case, if you specify a shorter lease time, the DHCP server negotiates the lease renewal much more frequently with the clients, which causes excess network traffic.

How much does your network configuration change?

If your network topology changes quite frequently, you might 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 restarting 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 can configure DHCP to use infinite leases, that is, 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 after they receive the infinite lease. After an infinite lease is assigned to a client, that address cannot be assigned to another client. Therefore, if you want to assign that client a new IP address or lease the client's IP address to another client later, problems might occur.

You might have clients in your network, such as a file server, that will always receive the same IP address. Rather than using an infinite lease, assign a specific address to the client and give it a long lease time. The client still must lease it for a given amount of time and renew the lease, but the DHCP server reserves 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 DHCP server gives the new file server that same address. If you have given it an infinite lease, then the DHCP server cannot give out the address again unless the lease is explicitly deleted.

Related concepts

"Network topology considerations" on page 41
When planning for your Dynamic Host Configuration Protocol (DHCP) setup, you must consider several factors, such as your network topology, the devices on the network (for example, routers), and how you want to support your clients in DHCP.

Related reference

"DHCP client/server interaction" on page 1
The interaction between Dynamic Host Configuration Protocol (DHCP) clients and servers enables a client to obtain its IP address and corresponding configuration information from a DHCP server.

Relay agents and routers

You can use Dynamic Host Configuration Protocol (DHCP) relay agents and routers to efficiently and securely transfer data throughout the network.

Initially, DHCP clients broadcast their DHCPDISCOVER packets because they do not know what network they are connected to. In some networks, the DHCP server might not be on the same LAN as the client. Therefore, it is necessary to forward the client's broadcast DHCP packets to the LAN where the DHCP server is located. Some routers are configured to forward DHCP packages. If your router supports DHCP packet forwarding, your router forwards the DHCP packets to the LAN where the DHCP server is located. However, many routers do not support forwarding packets that have a destination IP address of the broadcast address (DHCP packets). In this case, the LAN must have a Bootstrap protocol (BOOTP)/DHCP relay agent to forward the DHCP packets to the LAN that has the DHCP server. See "Example: DHCP and PPP profile on different System i models" on page 38 for a sample network using a relay agent and a router.

In either case, because the DHCP server is on a separate network, your clients must have the IP address of the router that connects your clients' network to the network that has the DHCP server specified in the router option (option 3).

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” on page 41.

Related concepts

“Network topology considerations” on page 41
When planning for your Dynamic Host Configuration Protocol (DHCP) setup, you must consider several factors, such as your network topology, the devices on the network (for example, routers), and how you want to support your clients in DHCP.

Related tasks

“Configuring the DHCP server and BOOTP/DHCP relay agent” on page 44
Use the following information to work with the DHCP server and the BOOTP/DHCP relay agent, such as configuring, starting, or stopping the DHCP server or the BOOTP/DHCP relay agent.

Related reference

“DHCP client/server interaction” on page 1
The interaction between Dynamic Host Configuration Protocol (DHCP) clients and servers enables a client to obtain its IP address and corresponding configuration information from a DHCP server.

DHCP client support

You can use a DHCP server to manage each client in your network individually, rather than managing all of the clients as a large group (subnet).

This DHCP setup method allows only the clients identified by the DHCP server to receive IP address and configuration information.

People often think about using DHCP to distribute IP addresses from an address pool to a subnet of clients. When you use subnets, any client that requests DHCP information from the network might receive an IP address from the address pool, unless they are explicitly excluded by the DHCP administrator. However, the DHCP server can also limit DHCP service to only specific clients.

The DHCP server can limit service at the individual client level or by the type of client (Bootstrap protocol (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 its client ID (typically 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 that they receive, you can set up 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 must 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.

Related concepts

“BOOTP” on page 7
The Bootstrap Protocol (BOOTP) is a host configuration protocol that was used before the Dynamic Host Configuration Protocol (DHCP) was developed. BOOTP support is a subset of DHCP.

"Network topology considerations" on page 41
When planning for your Dynamic Host Configuration Protocol (DHCP) setup, you must consider several factors, such as your network topology, the devices on the network (for example, routers), and how you want to support your clients in DHCP.

BOOTP

The Bootstrap Protocol (BOOTP) is a host configuration protocol that was used before the Dynamic Host Configuration Protocol (DHCP) was developed. BOOTP support is a subset of DHCP.

In BOOTP, clients are identified by their MAC addresses and are assigned a specific IP address. Essentially, each client in your network is mapped to an IP address. BOOTP does not have 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 set up and use DHCP without affecting 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 turn on the BOOTP support for the entire system or for 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 reusable 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 addresses to the BOOTP client from the address pool. After 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 might want to consider converting your BOOTP clients to DHCP for easier host configuration management.

Related concepts

"DHCP client support" on page 6
You can use a DHCP server to manage each client in your network individually, rather than managing all of the clients as a large group (subnet).

BOOTP

"Network topology considerations" on page 41
When planning for your Dynamic Host Configuration Protocol (DHCP) setup, you must consider several factors, such as your network topology, the devices on the network (for example, routers), and how you want to support your clients in DHCP.

Dynamic updates

You can configure a Dynamic Host Configuration Protocol (DHCP) server to work with a Domain Name System (DNS) server to dynamically update the client information in the DNS when DHCP assigns the client an IP address.

DNS is a distributed database system for managing host names and their associated IP addresses. With DNS, users can locate hosts using simple names, such as www.example.com, rather than 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 that 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 is 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 System i® model, different System i models, or other systems that are capable of dynamic updates.

Related concepts

Domain Name System

"Network topology considerations" on page 41
When planning for your Dynamic Host Configuration Protocol (DHCP) setup, you must consider several factors, such as your network topology, the devices on the network (for example, routers), and how you want to support your clients in DHCP.

"Problem: DNS records are not being updated by DHCP" on page 53
The System i DHCP server is capable of dynamically updating DNS resource records. The DHCP server uses name resolution functions and programming interfaces to determine the appropriate dynamic DNS server to update. You can use this information when troubleshooting dynamic update errors.

Related tasks

"Configuring DHCP to send dynamic updates to DNS" on page 49
The Dynamic Host Configuration Protocol (DHCP) server can be configured 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.

Configuring DNS to receive dynamic updates

Related reference

Domain Name System resource records

DHCP options lookup

Dynamic Host Configuration Protocol (DHCP) has many configuration options that can be sent to clients when they request information from the DHCP server. You can use a lookup tool to see all of the DHCP options.

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 in the following table. You might also configure customized options using the DHCP Options display in System i Navigator.

Table 1. Standard DHCP options

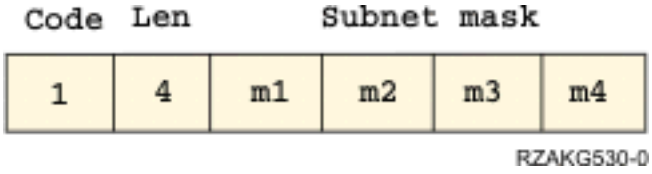
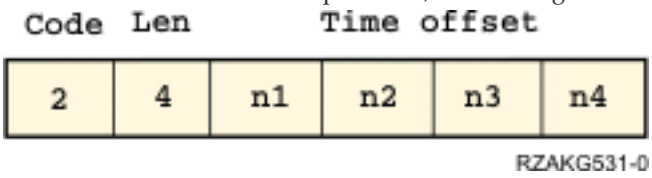
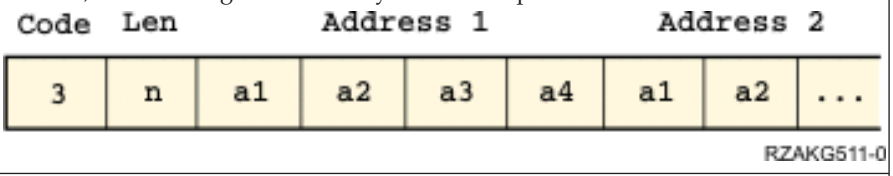
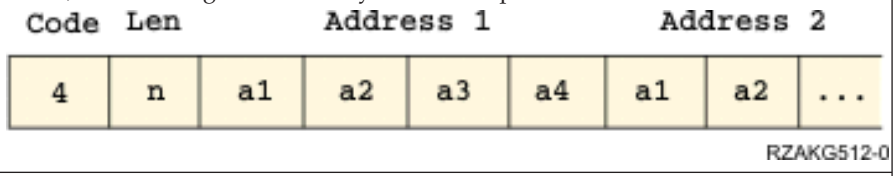
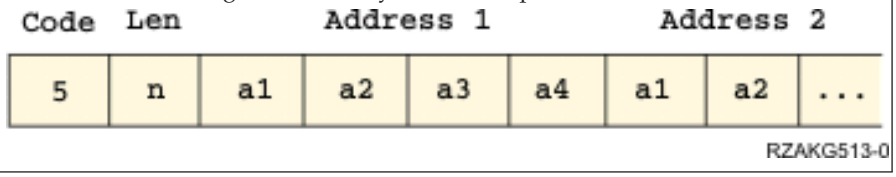
Option number	Option	Description
1	Subnet mask	The subnet mask option specifies the client's subnet mask as per Request for Comments (RFC) 950. If both the subnet mask and the router option are specified in a DHCP reply, the subnet mask option must be specified first. The code for the subnet mask option is 1, and its length is 4 octets. 
2	Time offset	The time offset field specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). The offset is expressed as a two's complement 32-bit integer. A positive offset indicates a location east of the zero meridian and a negative offset indicates a location west of the zero meridian. The code for the time offset option is 2, and its length is 4 octets. 
3	Router	The router option specifies a list of IP addresses for routers on the client's subnet. Routers should be listed in order of preference. The code for the router option is 3. The minimum length for the router option is 4 octets, and the length must always be a multiple of 4. 
4	Time server	The time server option specifies a list of RFC 868 time servers available to the client. Servers should be listed in order of preference. The code for the time server option is 4. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
5	Name server	The name server option specifies a list of IEN 116 name servers available to the client. Servers should be listed in order of preference. The code for the name server option is 5. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 

Table 1. Standard DHCP options (continued)

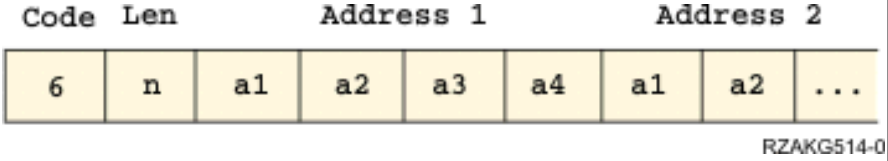
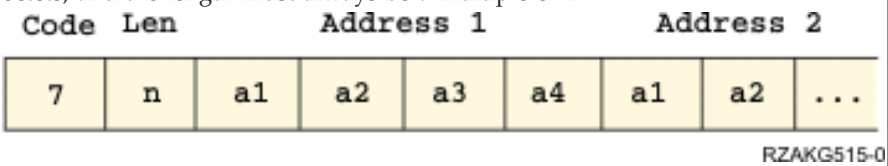
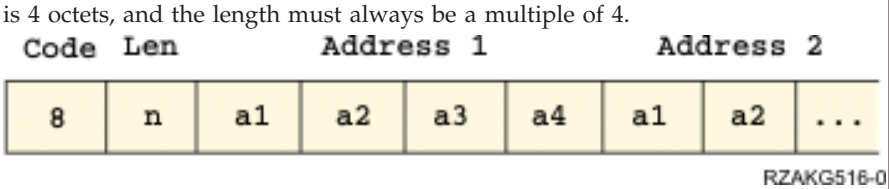
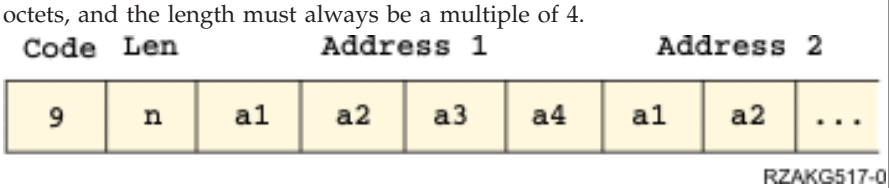
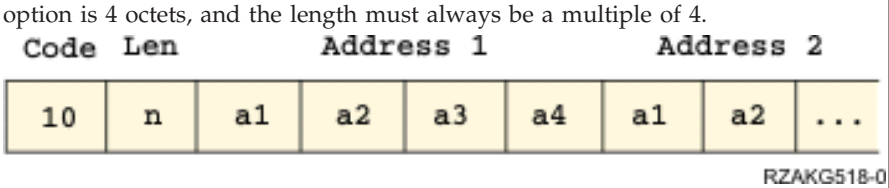
Option number	Option	Description
6	Domain Name Server	The domain name server option specifies a list of Domain Name System (STD 13, RFC 1035) name servers available to the client. Servers should be listed in order of preference. The code for the domain name server option is 6. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
7	Log server	The log server option specifies a list of MIT-LCS UDP log servers available to the client. Servers should be listed in order of preference. The code for the log server option is 7. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
8	Cookie server	The cookie server option specifies a list of RFC 865 cookie servers available to the client. Servers should be listed in order of preference. The code for the cookie server option is 8. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
9	LPR server	The LPR server option specifies a list of RFC 1179 line printer servers available to the client. Servers should be listed in order of preference. The code for the LPR server option is 9. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
10	Impress server	The Impress server option specifies a list of Imagen Impress servers available to the client. Servers should be listed in order of preference. The code for the Impress server option is 10. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 

Table 1. Standard DHCP options (continued)

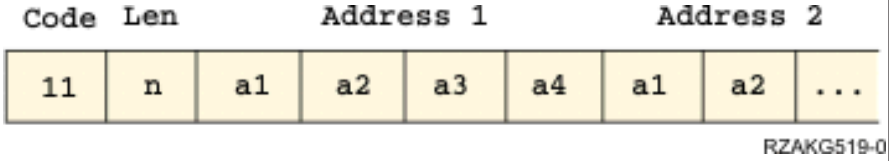
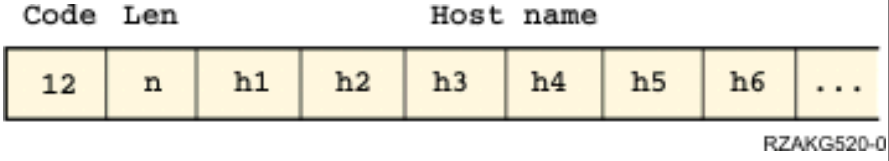
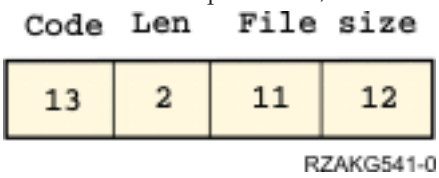
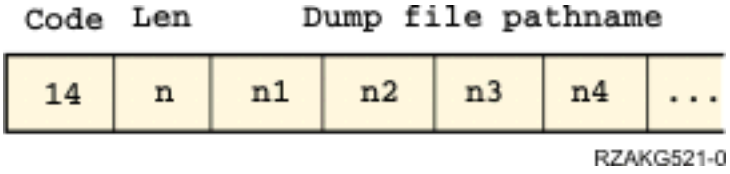
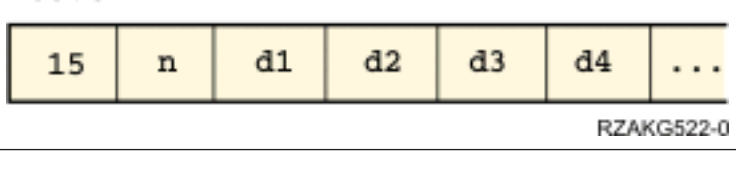
Option number	Option	Description
11	Resource location server	This option specifies a list of RFC 887 Resource Location servers available to the client. Servers should be listed in order of preference. The code for this option is 11. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
12	Host name	This option specifies the name of the client. The name might or might not be qualified with the local domain name (see section 3.17 for the preferred way to retrieve the domain name). See RFC 1035 for character set restrictions. The code for this option is 12, and its minimum length is 1. 
13	Boot file size	This option specifies the length in 512-octet blocks of the default boot image for the client. The file length is specified as an unsigned 16-bit integer. The code for this option is 13, and its length is 2. 
14	Merit dump file	This option specifies the path-name of a file to which the client's core image should be dumped in the event the client crashes. The path is formatted as a character string consisting of characters from the NVT ASCII character set. The code for this option is 14. Its minimum length is 1. 
15	Domain name	This option specifies the domain name that client should use when resolving hostnames through the Domain Name System. The code for this option is 15. Its minimum length is 1. 

Table 1. Standard DHCP options (continued)

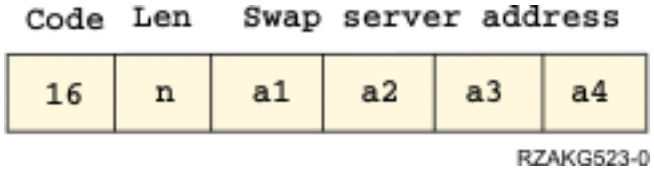
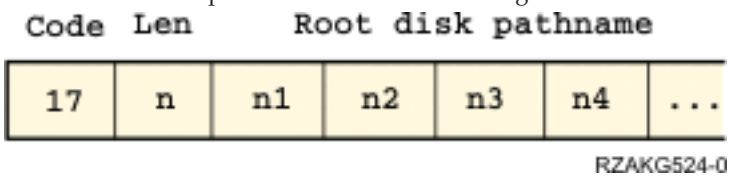
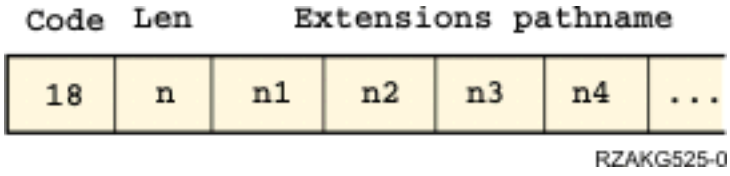
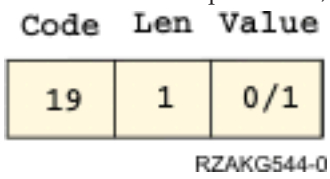
Option number	Option	Description
16	Swap server	This specifies the IP address of the client's swap server. The code for this option is 16, and its length is 4. 
17	Root path	This option specifies the path-name that contains the client's root disk. The path is formatted as a character string consisting of characters from the NVT ASCII character set. The code for this option is 17. Its minimum length is 1. 
18	Extensions path	A string to specify a file, retrievable via TFTP, which contains information that can be interpreted in the same way as the 64-octet vendor-extension field within the BOOTP response, with the following exceptions: • The length of the file is unconstrained • All references to Tag 18 (that is, instances of the BOOTP Extensions Path field) within the file are ignored. The code for this option is 18. Its minimum length is 1. 
19	IP forwarding	This option specifies whether the client should configure its IP layer for packet forwarding. A value of 0 means disable IP forwarding, and a value of 1 means enable IP forwarding. The code for this option is 19, and its length is 1. 

Table 1. Standard DHCP options (continued)

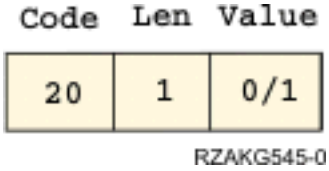
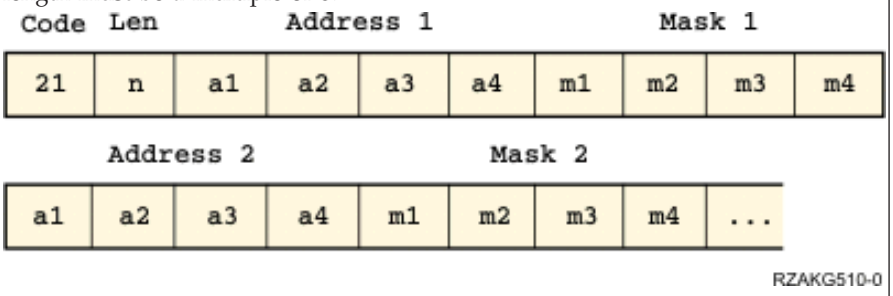
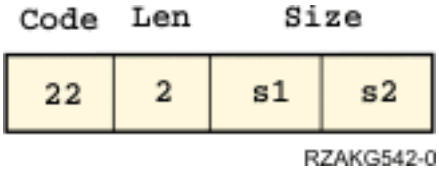
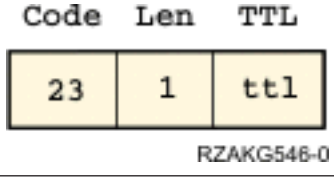
Option number	Option	Description
20	Non-Local source routing	This option specifies whether the client should configure its IP layer to allow forwarding of datagrams with non-local source routes. A value of 0 means disallow forwarding of such datagrams, and a value of 1 means allow forwarding. The code for this option is 20, and its length is 1. 
21	Policy filter	This option specifies policy filters for non-local source routing. The filters consist of a list of IP addresses and masks which specify destination/mask pairs with which to filter incoming source routes. Any source routed datagram whose next-hop address does not match one of the filters should be discarded by the client. The code for this option is 21. The minimum length of this option is 8, and the length must be a multiple of 8. 
22	Maximum datagram reassembly size	This option specifies the maximum size datagram that the client should be prepared to reassemble. The size is specified as a 16-bit unsigned integer. The minimum value legal value is 576. The code for this option is 22, and its length is 2. 
23	Default IP time to live	This option specifies the default time-to-live that the client should use on outgoing datagrams. The TTL is specified as an octet with a value between 1 and 255. The code for this option is 23, and its length is 1. 

Table 1. Standard DHCP options (continued)

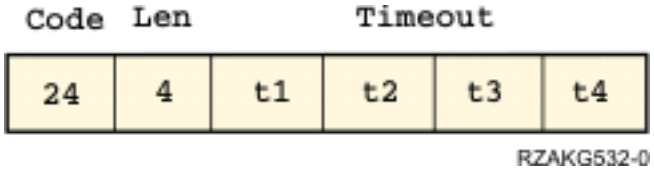
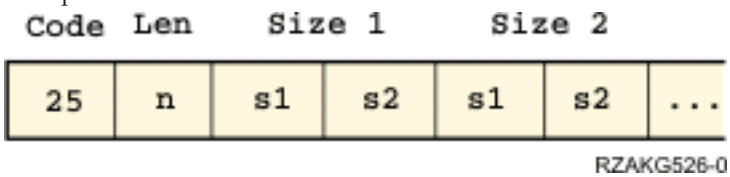
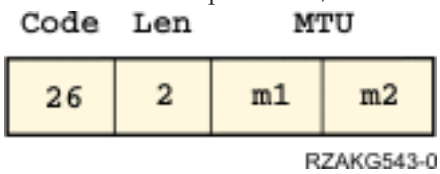
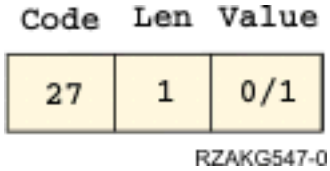
Option number	Option	Description
24	Path MTU aging timeout	This option specifies the timeout (in seconds) to use when aging Path MTU values discovered by the mechanism defined in RFC 1191. The timeout is specified as a 32-bit unsigned integer. The code for this option is 24, and its length is 4. 
25	Path MTU plateau table	This option specifies a table of MTU sizes to use when performing Path MTU Discovery as defined in RFC 1191. The table is formatted as a list of 16-bit unsigned integers, ordered from smallest to largest. The minimum MTU value cannot be smaller than 68. The code for this option is 25. Its minimum length is 2, and the length must be a multiple of 2. 
26	Interface MTU	This option specifies the MTU to use on this interface. The MTU is specified as a 16-bit unsigned integer. The minimum legal value for the MTU is 68. The code for this option is 26, and its length is 2. 
27	All subnets are local	This option specifies whether the client can assume that all subnets of the IP network to which the client is connected use the same MTU as the subnet of that network to which the client is directly connected. A value of 1 indicates that all subnets share the same MTU. A value of 0 means that the client should assume that some subnets of the directly connected network might have smaller MTUs. The code for this option is 27, and its length is 1. 

Table 1. Standard DHCP options (continued)

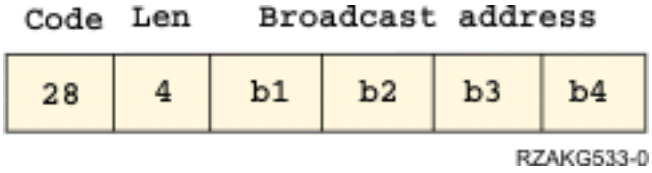
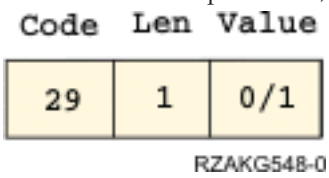
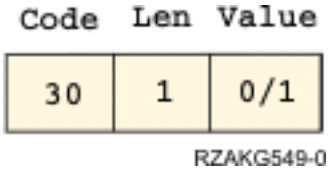
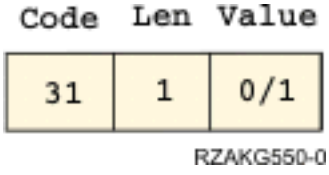
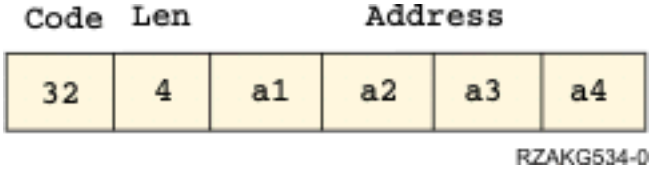
Option number	Option	Description
28	Broadcast address	This option specifies the broadcast address in use on the client's subnet. Legal values for broadcast addresses are specified in section 3.2.1.3 of RFC 2132. The code for this option is 28, and its length is 4. 
29	Perform mask discovery	This option specifies whether the client should perform subnet mask discovery using ICMP. A value of 0 indicates that the client should not perform mask discovery. A value of 1 means that the client should perform mask discovery. The code for this option is 29, and its length is 1. 
30	Mask supplier	This option specifies whether the client should respond to subnet mask requests using ICMP. A value of 0 indicates that the client should not respond. A value of 1 means that the client should respond. The code for this option is 30, and its length is 1. 
31	Perform router discovery	This option specifies whether the client should solicit routers using the Router Discovery mechanism defined in RFC 1256. A value of 0 indicates that the client should not perform router discovery. A value of 1 means that the client should perform router discovery. The code for this option is 31, and its length is 1. 
32	Router solicitation address option	This option specifies the address to which the client should transmit router solicitation requests. The code for this option is 32, and its length is 4. 

Table 1. Standard DHCP options (continued)

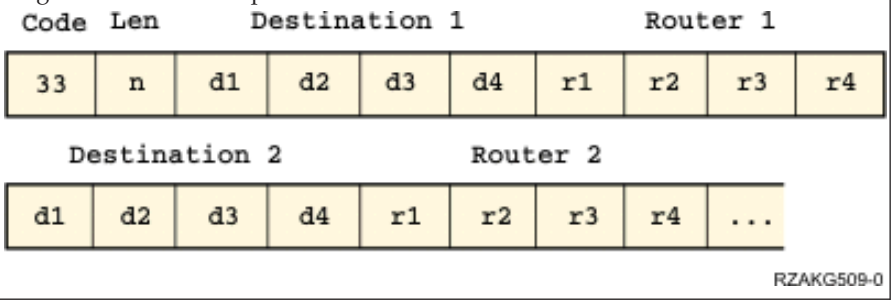
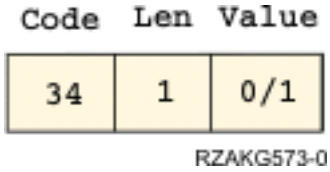
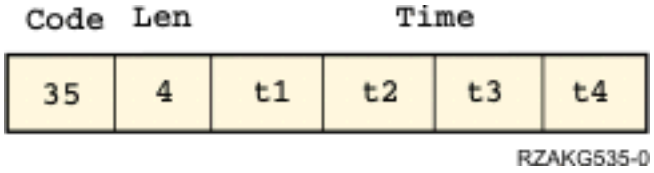
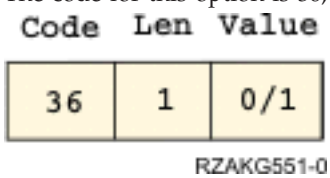
Option number	Option	Description
33	Static route	This option specifies a list of static routes that the client should install in its routing cache. If multiple routes to the same destination are specified, they are listed in descending order of priority. The routes consist of a list of IP address pairs. The first address is the destination address, and the second address is the router for the destination. The default route (0.0.0.0) is an illegal destination for a static route. The code for this option is 33. The minimum length of this option is 8, and the length must be a multiple of 8. 
34	Trailer encapsulation	This option specifies whether the client should negotiate the use of trailers (RFC 893) when using the ARP protocol. A value of 0 indicates that the client should not attempt to use trailers. A value of 1 means that the client should attempt to use trailers. The code for this option is 34, and its length is 1. 
35	ARP cache timeout	This option specifies the timeout in seconds for ARP cache entries. The time is specified as a 32-bit unsigned integer. The code for this option is 35, and its length is 4. 
36	Ethernet encapsulation	This option specifies whether the client should use Ethernet Version 2 (RFC 894) or IEEE 802.3 (RFC 1042) encapsulation if the interface is an Ethernet. A value of 0 indicates that the client should use RFC 894 encapsulation. A value of 1 means that the client should use RFC 1042 encapsulation. The code for this option is 36, and its length is 1. 

Table 1. Standard DHCP options (continued)

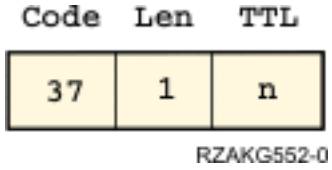
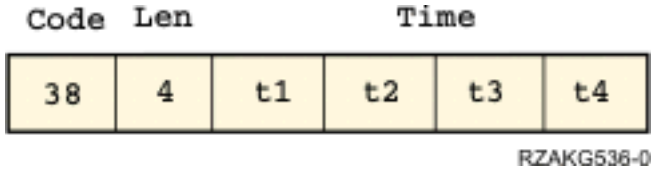
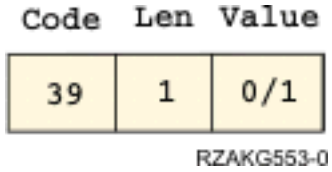
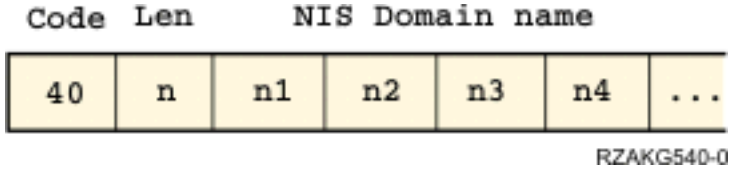
Option number	Option	Description
37	TCP default TTL	This option specifies the default TTL that the client should use when sending TCP segments. The value is represented as an 8-bit unsigned integer. The minimum value is 1. The code for this option is 37, and its length is 1. 
38	TCP keep-alive interval	This option specifies the interval (in seconds) that the client TCP should wait before sending a keepalive message on a TCP connection. The time is specified as a 32-bit unsigned integer. A value of zero indicates that the client should not generate keepalive messages on connections unless specifically requested by an application. The code for this option is 38, and its length is 4. 
39	TCP keep-alive garbage	This option specifies whether the client should send TCP keepalive messages with an octet of garbage for compatibility with older implementations. A value of 0 indicates that a garbage octet should not be sent. A value of 1 indicates that a garbage octet should be sent. The code for this option is 39, and its length is 1. 
40	Network information service domain	This option specifies the name of the client's NIS domain. The domain is formatted as a character string consisting of characters from the NVT ASCII character set. The code for this option is 40. Its minimum length is 1. 

Table 1. Standard DHCP options (continued)

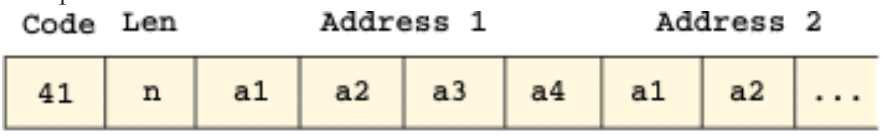
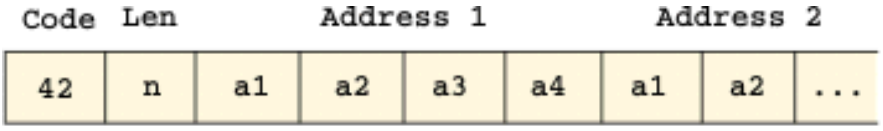
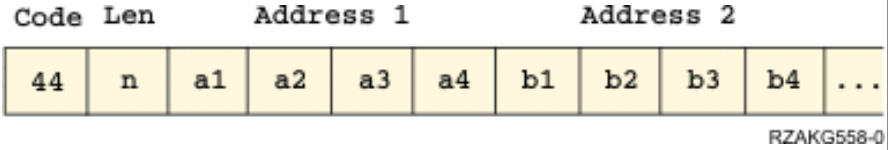
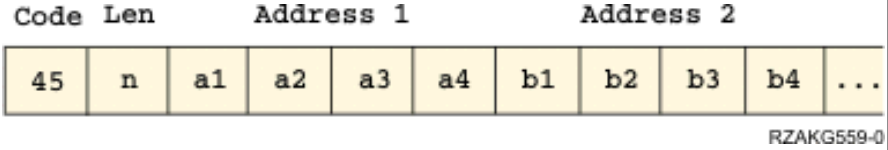
Option number	Option	Description
41	Network information servers	This option specifies a list of IP addresses indicating NIS servers available to the client. Servers should be listed in order of preference. The code for this option is 41. Its minimum length is 4, and the length must be a multiple of 4. 
42	Network time protocol servers option	This option specifies a list of IP addresses indicating NTP servers available to the client. Servers should be listed in order of preference. The code for this option is 42. Its minimum length is 4, and the length must be a multiple of 4. 
44	NetBIOS over TCP/IP name server	The NetBIOS name server (NBNS) option specifies a list of RFC 1001/1002 NBNS name servers listed in order of preference. The code for this option is 44. The minimum length of the option is 4 octets, and the length must always be a multiple of 4. 
45	NetBIOS over TCP/IP datagram distribution server	The NetBIOS datagram distribution server (NBDD) option specifies a list of RFC 1001/1002 NBDD servers listed in order of preference. The code for this option is 45. The minimum length of the option is 4 octets, and the length must always be a multiple of 4. 

Table 1. Standard DHCP options (continued)

Option number	Option	Description
46	NetBIOS over TCP/IP node type	The NetBIOS node type option allows NetBIOS over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002. The value is specified as a single octet which identifies the client type as follows: Value — Node type 0x1 — B-node 0x2 — P-node 0x4 — M-node 0x8 — H-node RZAKG554-0 In the above chart, the notation '0x' indicates a number in base-16 (hexadecimal). The code for this option is 46. The length of this option is always 1. Code | Len | Node type 46 | 1 | see above RZAKG555-0
47	NetBIOS over TCP/IP scope	The NetBIOS scope option specifies the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002. The code for this option is 47. The minimum length of this option is 1. Code | Len | NetBIOS scope 47 | n | s1 | s2 | s3 | s4 | ... RZAKG528-0
48	X Window System Font server	This option specifies a list of X Window System Font servers available to the client. Servers should be listed in order of preference. The code for this option is 48. The minimum length of this option is 4 octets, and the length must be a multiple of 4. Code | Len | Address 1 | Address 2 48 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG560-0
49	X Window System display manager	This option specifies a list of IP addresses of systems that are running the X Window System Display Manager and are available to the client. Addresses should be listed in order of preference. The code for the this option is 49. The minimum length of this option is 4, and the length must be a multiple of 4. Code | Len | Address 1 | Address 2 49 | n | a1 | a2 | a3 | a4 | a1 | a2 | ... RZAKG561-0

Table 1. Standard DHCP options (continued)

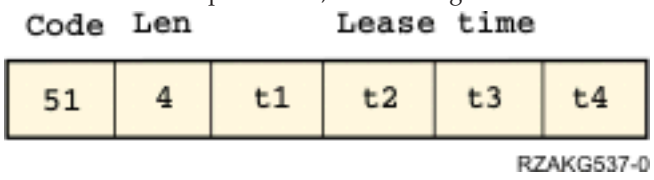
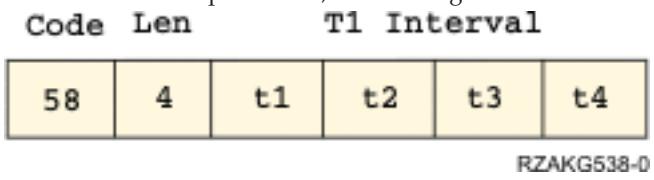
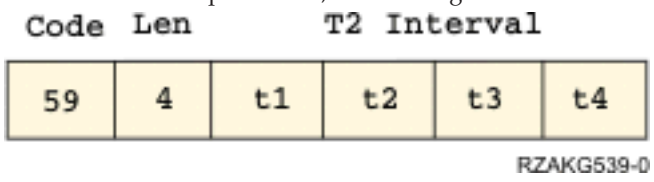
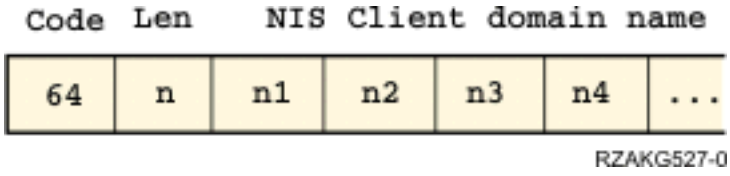
Option number	Option	Description
51	IP address lease time	This option is used in a client request (DHCPDISCOVER or DHCPREQUEST) to allow the client to request a lease time for the IP address. In a server reply (DHCPOFFER), a DHCP server uses this option to specify the lease time it is willing to offer. The time is in units of seconds, and is specified as a 32-bit unsigned integer. The code for this option is 51, and its length is 4. 
58	Renewal (T1) time value	This option specifies the time interval from address assignment until the client transitions to the RENEWING state. The value is in units of seconds, and is specified as a 32-bit unsigned integer. The code for this option is 58, and its length is 4. 
59	Rebinding (T2) time value	This option specifies the time interval from address assignment until the client transitions to the REBINDING state. The value is in units of seconds, and is specified as a 32-bit unsigned integer. The code for this option is 59, and its length is 4. 
62	NetWare/IP domain name	Specifies the Netware/IP domain name.
63	NetWare/IP	Specifies the NetWare sub-options you want. The range is 1 to 255. Use option 62 to specify the NetWare/IP domain name.
64	NIS domain name	This option specifies the name of the client's NIS+ domain. The domain is formatted as a character string consisting of characters from the NVT ASCII character set. The code for this option is 64. Its minimum length is 1. 

Table 1. Standard DHCP options (continued)

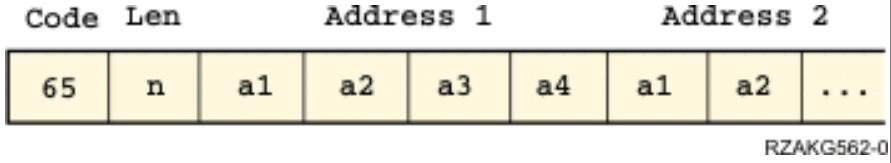
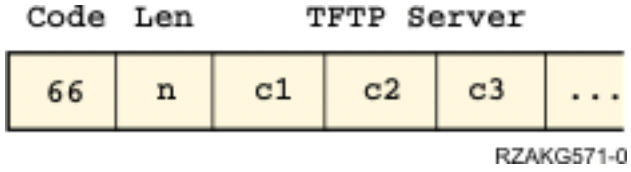
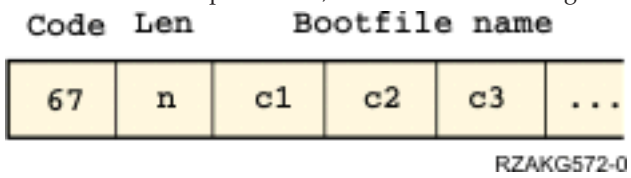
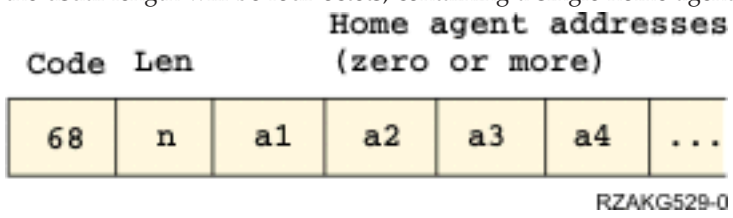
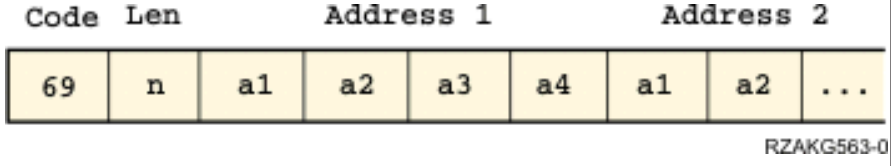
Option number	Option	Description
65	NIS servers	This option specifies a list of IP addresses indicating NIS+ servers available to the client. Servers should be listed in order of preference. The code for this option is 65. Its minimum length is 4, and the length must be a multiple of 4. 
66	Server name	This option is used to identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options. The code for this option is 66, and its minimum length is 1. 
67	Boot file name	This option is used to identify a bootfile when the 'file' field in the DHCP header has been used for DHCP options. The code for this option is 67, and its minimum length is 1. 
68	Home address	This option specifies a list of IP addresses indicating mobile IP home agents available to the client. Agents should be listed in order of preference. The code for this option is 68. Its minimum length is 0 (indicating no home agents are available) and the length must be a multiple of 4. It is expected that the usual length will be four octets, containing a single home agent's address. 
69	SMTP servers	The SMTP server option specifies a list of SMTP servers available to the client. Servers should be listed in order of preference. The code for the SMTP server option is 69. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 

Table 1. Standard DHCP options (continued)

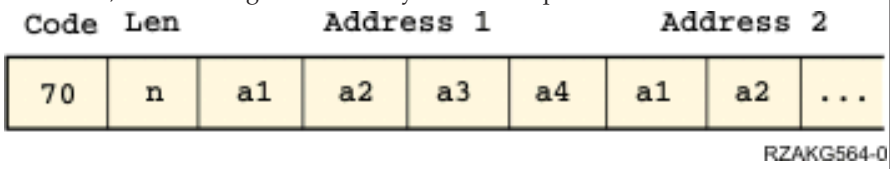
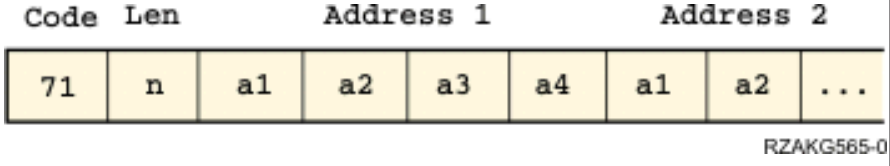
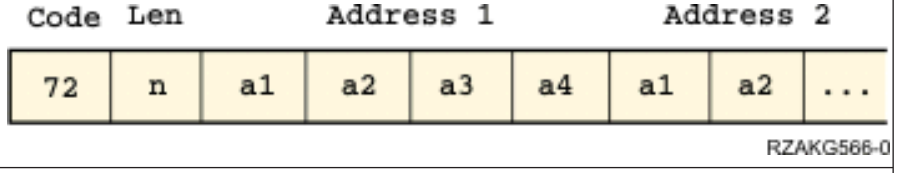
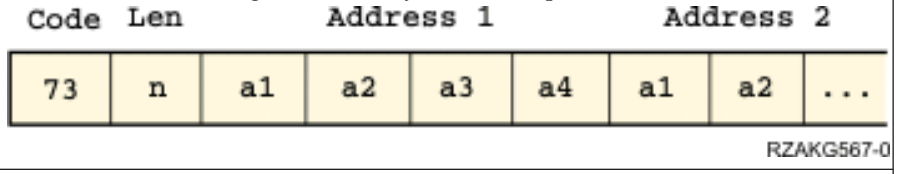
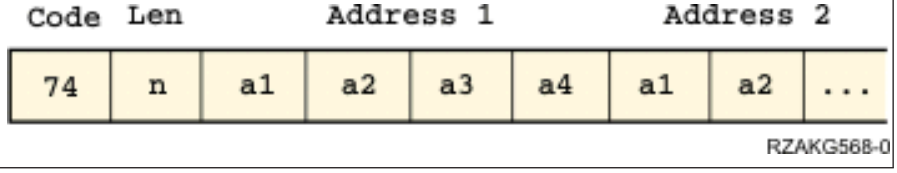
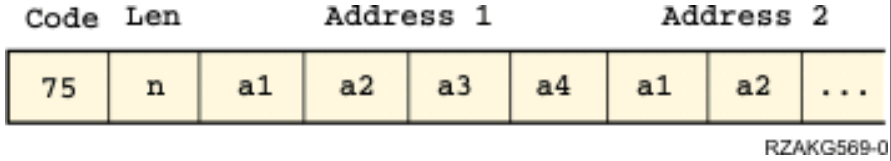
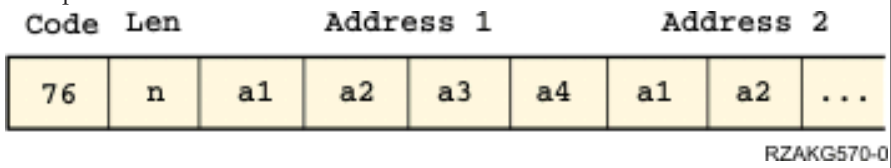
Option number	Option	Description
70	POP3 server	The POP3 server option specifies a list of POP3 available to the client. Servers should be listed in order of preference. The code for the POP3 server option is 70. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
71	NNTP server	The NNTP server option specifies a list of NNTP available to the client. Servers should be listed in order of preference. The code for the NNTP server option is 71. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
72	WWW server	The WWW server option specifies a list of WWW available to the client. Servers should be listed in order of preference. The code for the WWW server option is 72. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
73	Finger server	The Finger server option specifies a list of Finger available to the client. Servers should be listed in order of preference. The code for the Finger server option is 73. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
74	IRC server	The IRC server option specifies a list of IRC available to the client. Servers should be listed in order of preference. The code for the IRC server option is 74. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 

Table 1. Standard DHCP options (continued)

Option number	Option	Description
75	StreetTalk server	The StreetTalk server option specifies a list of StreetTalk servers available to the client. Servers should be listed in order of preference. The code for the StreetTalk server option is 75. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
76	STDA server	The StreetTalk Directory Assistance (STDA) server option specifies a list of STDA servers available to the client. Servers should be listed in order of preference. The code for the StreetTalk Directory Assistance server option is 76. The minimum length for this option is 4 octets, and the length must always be a multiple of 4. 
77	User class	Specifies the class name of which the host is a member. You must have previously defined this class to the DHCP server during DHCP server configuration.
78	Directory agent	Specifies the IP address of the directory agent if clients use Service Location Protocol to transact messages.
79	Service scope	Specifies the scope of the directory agent that uses Service Location Protocol to respond to service request messages.
80	Naming authority	Specifies the naming authority for the directory agent if clients use Service Location Protocol to transact messages. The naming authority specifies the syntax for schemes that are used in URLs.

Related information

DHCP Options and BOOTP Vendor Extensions

Examples: DHCP

By reviewing diagrams and examples of how different networks are set up, you can determine which is the best choice for your installation.

Looking at how someone else has used a technology is often the best way to learn about that technology. The following examples show how DHCP works, how it is incorporated into different network setups, and how to tie in some of the V5R4 functions. It is a great place to start whether you are a beginner to DHCP or an experienced DHCP administrator.

Related concepts

"Network topology considerations" on page 41
When planning for your Dynamic Host Configuration Protocol (DHCP) setup, you must consider several factors, such as your network topology, the devices on the network (for example, routers), and how you want to support your clients in DHCP.

Example: Simple DHCP subnet

This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server in a simple LAN with four PC clients and a LAN-based printer.

In this example, the System i model 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.

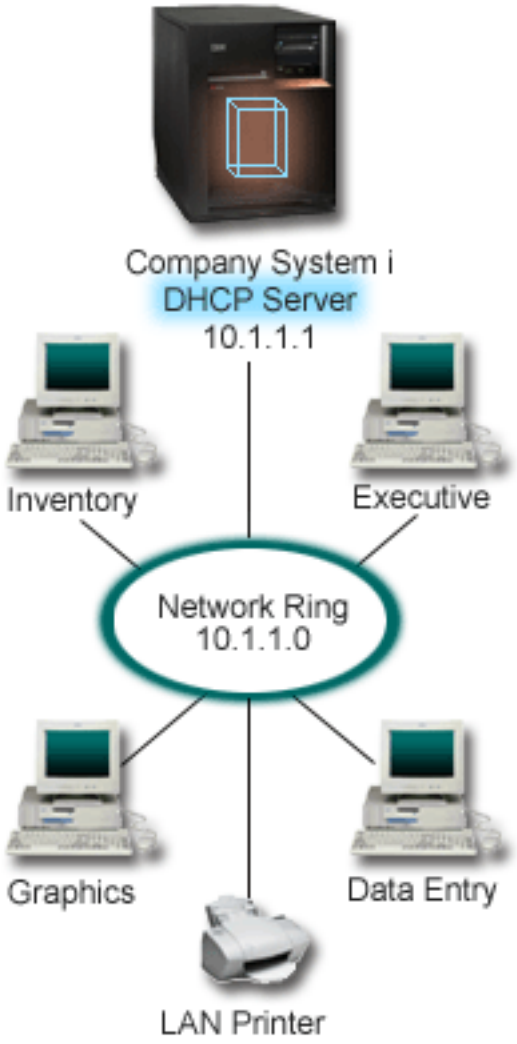


Figure 2. Simple LAN setup for System i model

With so few PC clients, administrators can easily type the information that is related to each PC's IP address and maintain this information. (They only need to visit four PCs in this case.) Now imagine that the four PCs become 200 PCs. Setting up each PC's IP information now becomes a time-consuming task that might result in accuracy errors too. DHCP can simplify the process of assigning IP information to clients. If the subnet 10.1.1.0 has hundreds of clients, an administrator only needs to create a single DHCP policy on the system. This policy distributes IP information to each client.

When PC clients send out their DHCPDISCOVER signals, the server responds with the appropriate IP information. In this example, the company also has a LAN-based printer that obtains its IP information from the DHCP server. But because PC clients depend on the printer's IP address remaining the same, the network administrator must account for that in the DHCP policy. One solution is to assign a constant

IP address to the printer. You can use the DHCP server to define a client, like the LAN printer, in the DHCP policy 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. 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 the system		10.1.1.1 (Domain name server)
Is the system performing DNS updates?		No
Is the system supporting BOOTP clients?		No

Table 3. 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 4. Client for printer

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

Related reference

"Example: Multiple TCP/IP subnets"
This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server with two LANs connected by a DHCP-enabled router.

"Example: DHCP and multihoming" on page 28
This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server for a LAN that is connected to the Internet by an Internet router.

Example: Multiple TCP/IP subnets

This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server with two LANs connected by a DHCP-enabled router.

This example is similar to the Simple DHCP subnet example except that there is now an additional TCP/IP subnet. Suppose that the office and data entry clients are on different floors of an office building and are 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 a System i DHCP server connected to two LANs using a router between the networks. The figure intentionally has a limited number of clients so as not to become cluttered. An actual enterprise generally has considerably more clients on each subnet.

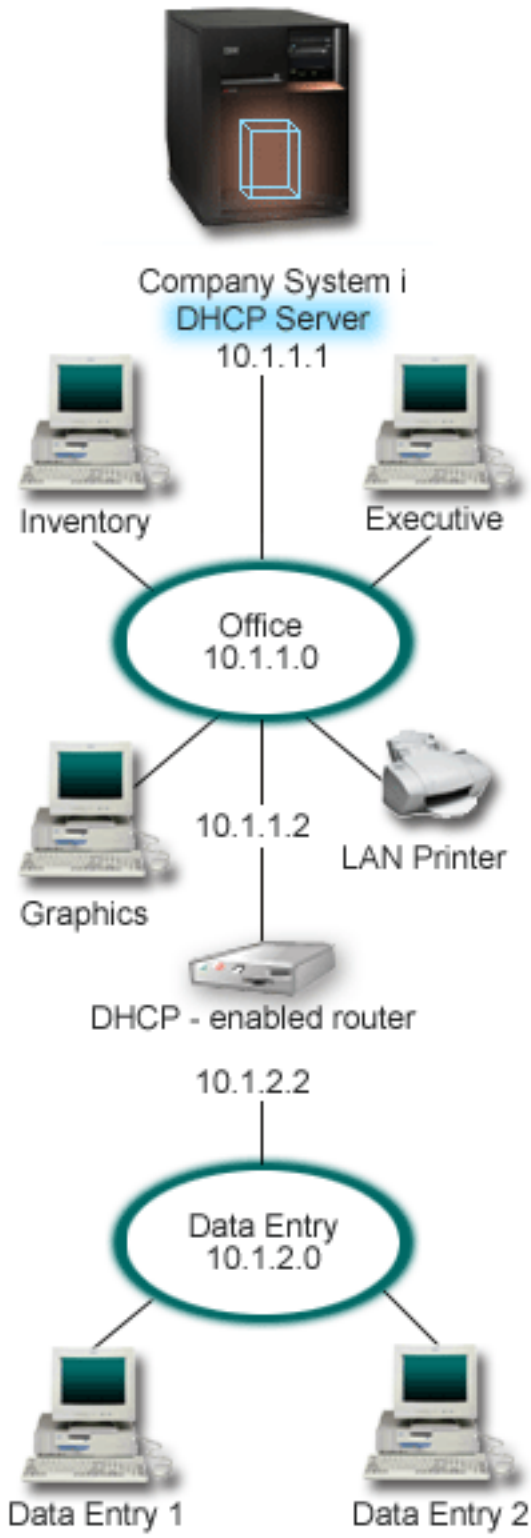


Figure 3. Multiple LANs connected through a router

The router that connects the two networks must be enabled to pass DHCPDISCOVER 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 needs two subnet definitions--one for the data entry subnet and the other for the office

subnet. At a minimum, the differences between the subnets are their IP subnets and router addresses. The data entry subnet needs to receive a router address of 10.1.2.2 to communicate with the office subnet.

Planning the DHCP setup for multiple LANs

Table 5. 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 the system		10.1.1.1 (Domain name server)
Is the system performing DNS updates?		No
Is the system supporting BOOTP clients?		No

Table 6. 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	10.1.1.2
	inherited options	Options from Global configuration
Subnet addresses not assigned by server		10.1.1.2 (Router)

Table 7. 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	10.1.2.2
	Inherited options	Options from Global configuration
Subnet addresses not assigned by server		10.1.2.2 (Router)

Related reference

"Example: Simple DHCP subnet" on page 24
This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server in a simple LAN with four PC clients and a LAN-based printer.

Example: DHCP and multihoming

This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server for a LAN that is connected to the Internet by an Internet router.

This example is much like the Simple DHCP subnet example. In this example, the data entry clients are only communicating among themselves and the System i model. They obtain their IP information dynamically from the System i DHCP server.

However, a new version of their data entry application requires that the network communicates with the Internet, and the company decides to provide Internet access through an Internet router as shown in the following figure. In addition to the router, the administrator also adds another interface with an IP

address to communicate with the Internet. When multiple IP addresses are assigned to the same adapter, the system is multihoming.

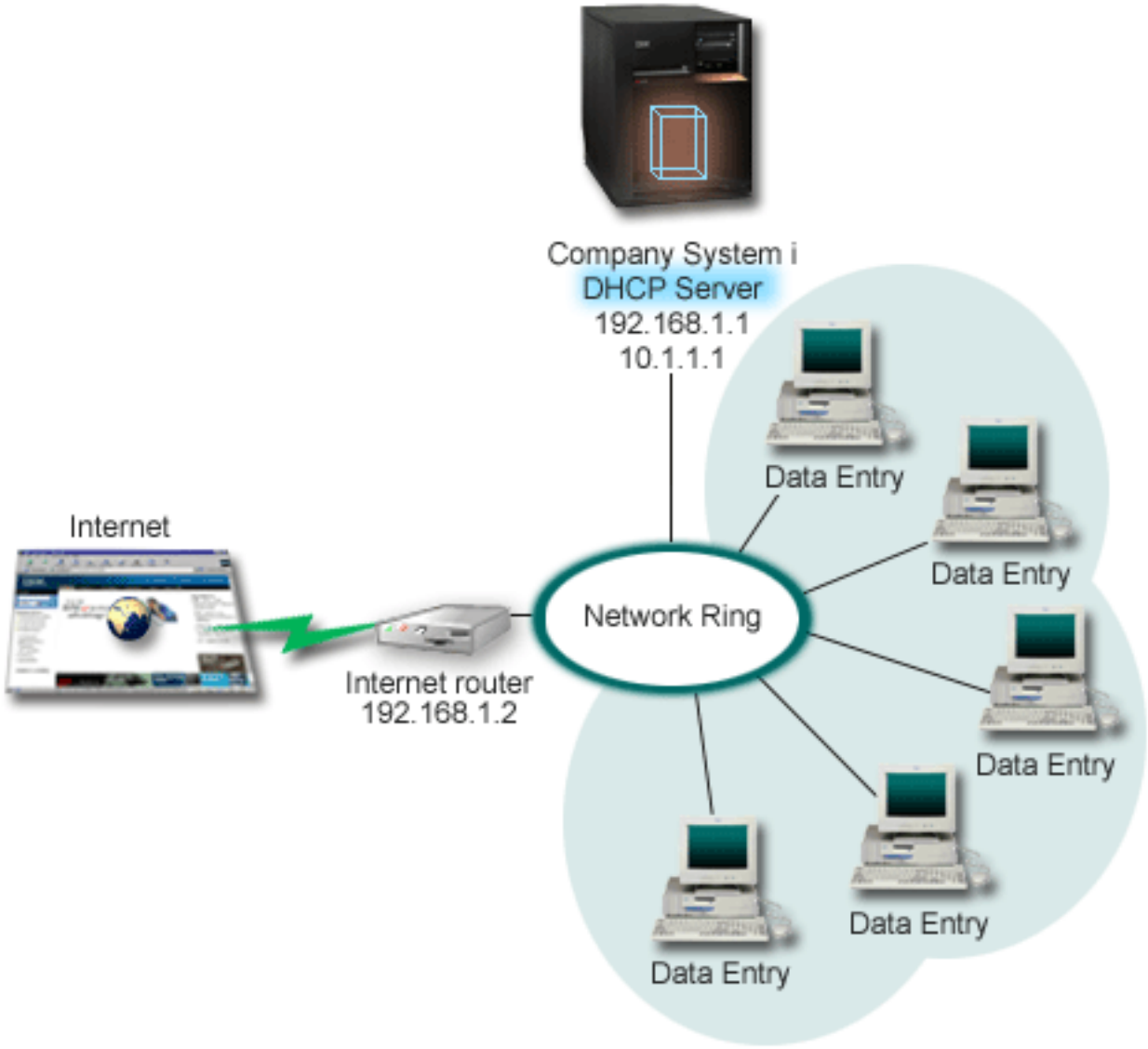


Figure 4. Using DHCP with multiple IP addresses assigned to the same adapter

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

When configuring the DHCP setup, take into account that the System i model is known by two different IP addresses. To understand how to set up DHCP correctly for this scenario, it is helpful to understand what happens when a client sends out a DHCPDISCOVER packet.

When a client sends out a DHCPDISCOVER packet, it is broadcasted on the ring. Therefore, the System i DHCP server cannot determine which IP address the packet is intended for. If this packet is marked with the 10.1.1.1 interface IP (the one used for DHCP), your clients receive their IP information as expected.

But it is possible that the packet can actually get marked with the 192.168.1.1 address (the one connected to the Internet). If the packet is received on the 192.168.1.1 interface, your data entry client does not receive any IP information.

To set up DHCP in this situation, you must create not only the data entry DHCP subnet, but also a subnet 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), and then exclude that same IP address. With the two subnets defined, you combine the two (or more) subnets into a subnet group. If the DHCPDISCOVER packet gets marked with the 192.168.1.1 interface, the data entry subnet still issues valid IP information.

To make this scenario work, the data entry subnet must pass its clients their router address for access to the Internet. In this case, the router address is the System i 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 also need to use network address translation (NAT) for your data entry clients to communicate with the Internet.

Using subnet groups to eliminate this marking problem is not limited to only multihoming examples. Any time multiple interfaces are connected to the same network, you might encounter the same problem. The following figure illustrates how the System i model can have two physical connections to the data entry network. This network configuration requires a similar DHCP group policy as the multihoming setup because DHCPDISCOVER packets might conceivably be answered by the 192.168.1.1 interface.

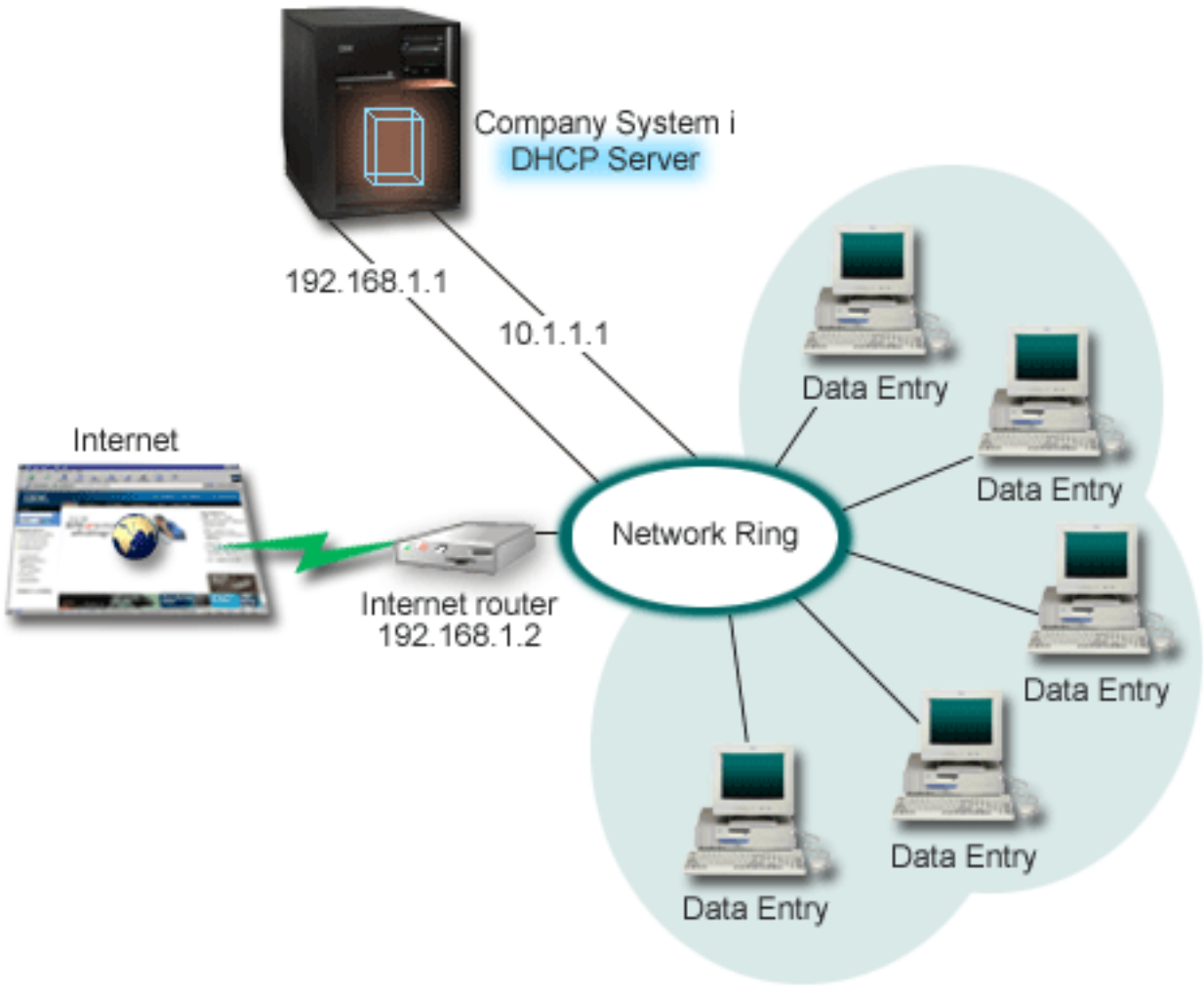


Figure 5. Using DHCP with multiple interfaces connected to the same network

Planning the DHCP setup for multihoming

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

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

Table 9. Subnet for Data Entry clients

Object		Value
Subnet name		Data Entry
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

Table 9. Subnet for Data Entry clients (continued)

Object	Value
Subnet addresses not assigned by server	10.1.1.1 (Router, DNS server)

Table 10. 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 11. Subnet group for all incoming DHCPDISCOVER 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

Related reference

"Example: Simple DHCP subnet" on page 24
This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server in a simple LAN with four PC clients and a LAN-based printer.

Example: DNS and DHCP on the same System i

This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server with dynamic Domain Name System (DNS) updates on a simple LAN.

The following illustration depicts how the System i model 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 mapping a network drive to its host name.

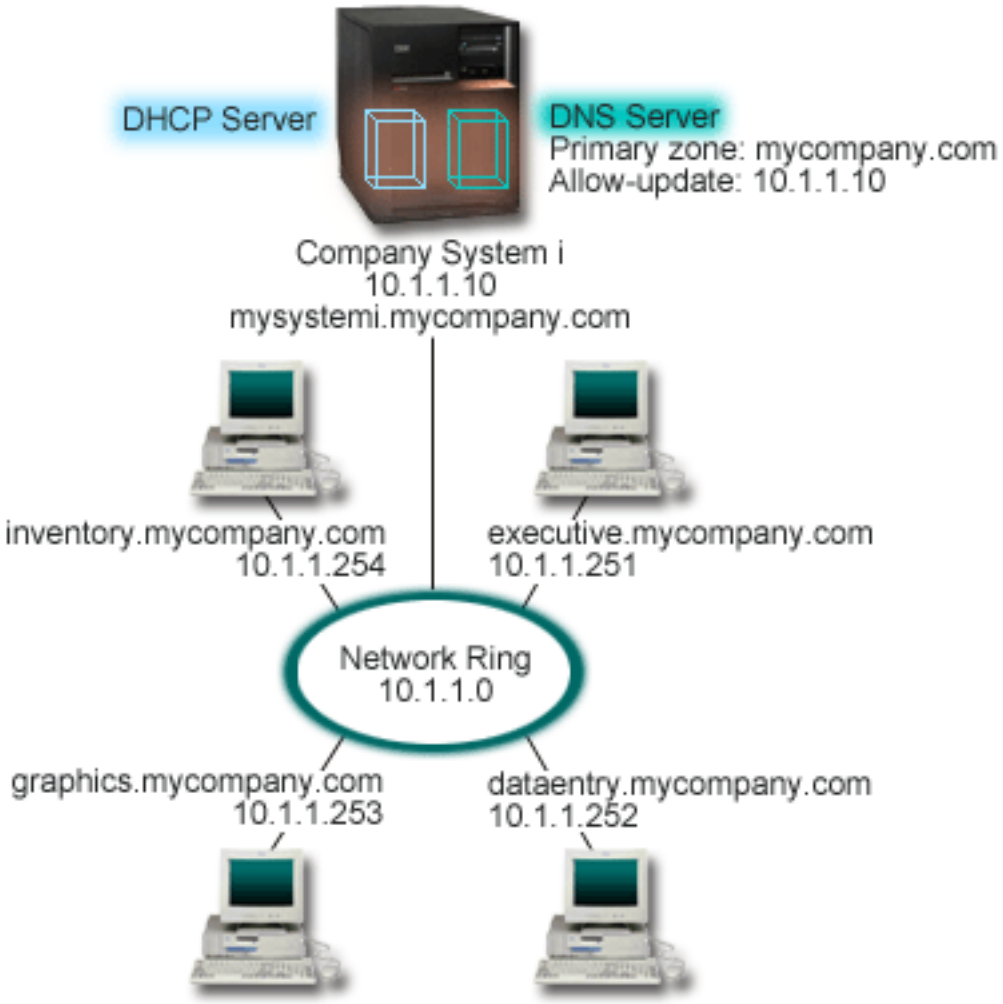


Figure 6. Dynamic DNS and DHCP

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 changes because it is assigned by DHCP, then its dependent clients are unable to map a network drive to its host name because the DNS records contain the file server's previous IP address.

With the current DNS server, 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 are updated dynamically. This allows 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 is written to identify that the record was written by DHCP. You can choose to let DHCP 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 System i in the DNS topic collection.

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 12. 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 system performing DNS updates?		Yes -- Both A and PTR records
Is the system supporting BOOTP clients?		No

Table 13. 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 System i in the DNS topic collection.

Example: DNS and DHCP on different System i models

This example explains how to set up Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) on two different System i models to perform dynamic updates over a simple LAN.

The following illustration depicts a small subnet network with DNS and DHCP running on separate System i models. The system running DNS is configured the same as when DNS and DHCP are on the same System i model. However, there are some additional steps to configure the DHCP server to send dynamic updates.

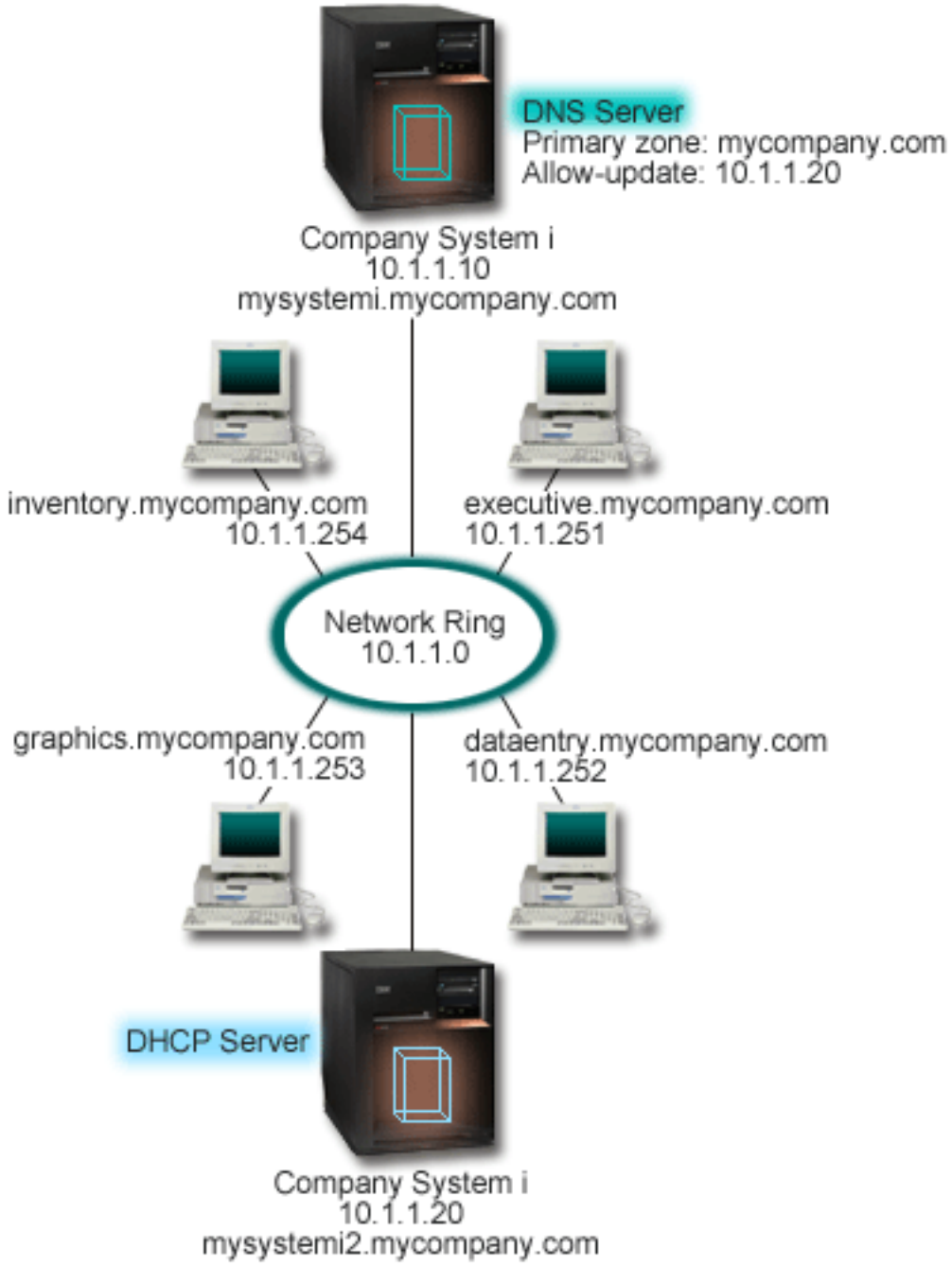


Figure 7. DNS and DHCP on different System i models

Planning the DHCP setup when using Dynamic DNS

Refer to "Example: DNS and DHCP on the same System i" on page 32 for examples of the global configuration options and subnet settings.

Other setup:

Installing i5/OS® Domain Name System (Option 31).

Install i5/OS Domain Name System (Option 31) on the System i model that will be running DHCP, in this case, mysystemi2. This option contains the dynamic update API that manages the resource record update process. Refer to DNS system requirements for installation instructions.

Authorizing 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 send the file and place it in the appropriate directory path.

To create a Dynamic Update Key on both System i models, follow these steps:

1. In System i Navigator, expand ***your system*** → **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 that you want to use to generate a secret key.
5. Repeat the preceding steps so that the same key is defined on both the System i model running DNS and the System i model running DHCP.

Related concepts

Domain Name System requirements

Related information

Update DNS API

Example: PPP and DHCP on a single System i

This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server for a LAN and a remote dial-in client.

Remote clients, such as dial-in clients, often require access to a company's network. Dial-in clients can gain access to a System i model with Point-to-Point Protocol (PPP) . To access the network, the dial-in client needs IP information just like any directly attached network client. A System i DHCP server can distribute IP address information to a PPP dial-in client just like any other directly attached client. The following figure shows a remote client that must dial into the company's network to do some work.

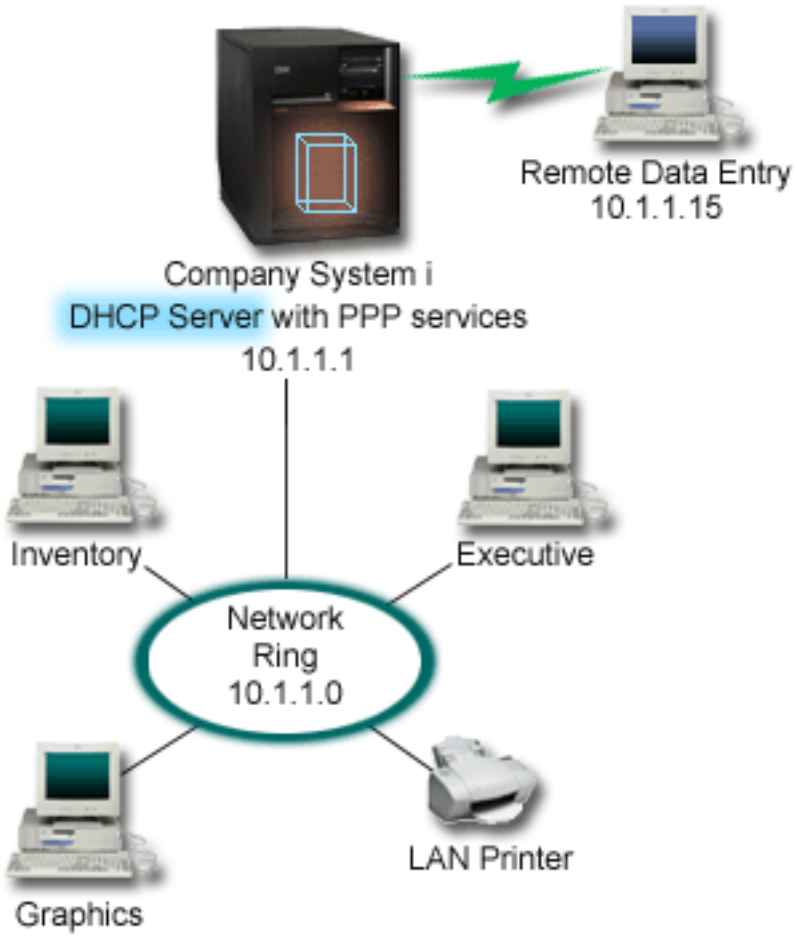


Figure 8. PPP and DHCP on a single System i model

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

In this example, a single DHCP subnet policy covers 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, 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 System i model will not pass the IP packets. You must set IP forwarding on in both the profile and the stack.

Also, the local interface IP address in the PPP profile must be an IP address that falls within the subnet definition in the DHCP server. In this example, the PPP profile local interface IP address must be 10.1.1.1. This address must 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 14. 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 system performing DNS updates?		No
Is the system supporting BOOTP clients?		No

Table 15. 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 System i 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 System i Navigator.
  2. Select to use DHCP for the IP address assignment method under the TCP/IP Settings Properties of the Receiver Connection Profile in System i Navigator.
- Allow remote system to access other networks (IP forwarding) under the TCP/IP Settings Properties of the Receiver Connection Profile in System i Navigator.
- Enable IP datagram forwarding under the Settings Properties of the TCP/IP Configuration in System i Navigator.

Related reference

"Example: DHCP and PPP profile on different System i models"
This example explains how to set up two System i models as the network Dynamic Host Configuration Protocol (DHCP) server and the BOOTP/DHCP relay agent for two LANs and remote dial-in clients.

Example: DHCP and PPP profile on different System i models

This example explains how to set up two System i models as the network Dynamic Host Configuration Protocol (DHCP) server and the BOOTP/DHCP relay agent for two LANs and remote dial-in clients.

The example about PPP and DHCP on a single System i model shows how to use PPP and DHCP on a single system to permit dial-in clients access to a network. If you are concerned with the physical layout of your network or with security, it might be better to have the PPP and DHCP servers separated or to have a dedicated PPP server without DHCP services. The following figure represents a network that has dial-in clients with the PPP and DHCP policies on different servers.

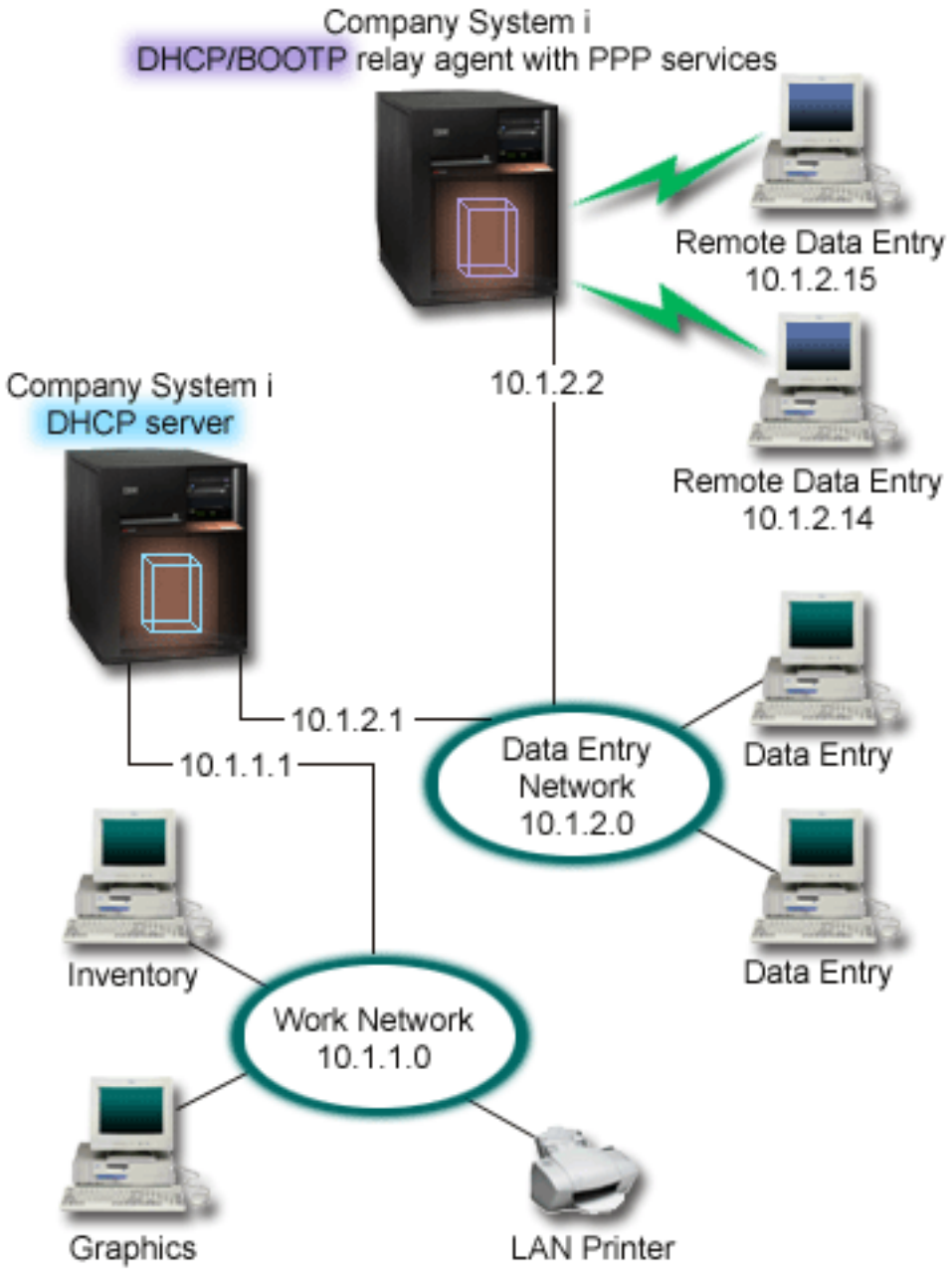


Figure 9. DHCP and PPP profile on different System i models

The remote data entry clients dial into the System i PPP server. The PPP profile on that server must have a remote IP address method of DHCP, such as the one used in the example of PPP and DHCP on a single System i model. The PPP profile and the TCP/IP stack properties on the PPP server must have IP forwarding. Furthermore, because this server is acting as a DHCP relay agent, the BOOTP/DHCP relay agent must be on. This allows the System i Remote Access server to pass on DHCPDISCOVER packets to the DHCP server. The DHCP server then responds and distributes 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, the DHCP server gives out IP addresses ranging 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 System i DHCP server must also have IP forwarding enabled.

Also, the local interface IP address in the PPP profile must be an IP address that falls within the subnet definition in the DHCP server. In this example, the PPP profile Local Interface address must be 10.1.2.2. This address must 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 16. 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 system performing DNS updates?		No
Is the system supporting BOOTP clients?		No

Table 17. 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 18. 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 a System i platform 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 System i Navigator
2. Select to Use DHCP for the IP address assignment method under the TCP/IP Settings Properties of the Receiver Connection Profile in System i Navigator

- Allow remote system to access other networks (IP forwarding) under the TCP/IP Settings Properties of the Receiver Connection Profile in System i 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 System i Navigator (to allow the remote clients to communicate with the data entry network)

Related reference

"Example: PPP and DHCP on a single System i" on page 36
This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server for a LAN and a remote dial-in client.

Planning for DHCP

Setting up Dynamic Host Configuration Protocol (DHCP) can be a time-consuming and error-prone process if you do not take time to plan how to configure your DHCP server. To configure your DHCP server more efficiently, consider network setup and security concerns beforehand.

Related reference

"Configuring DHCP" on page 44
Here are instructions for setting up your DHCP server and clients, and for configuring DHCP to send dynamic updates to Domain Name System (DNS).

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 with the network, it is important that you secure your System i model from outside clients. If your DHCP server is on a System i model that is part of a trusted internal network, you might be able to use IP filtering and network address translation to further secure it from any unauthorized parties. If your DHCP server is on a System i model that is attached to an untrusted network, such as the Internet, refer to the System i and Internet security topic.

Related concepts

IP filtering and network address translation

Security

Network topology considerations

When planning for your Dynamic Host Configuration Protocol (DHCP) setup, you must consider several factors, such as your network topology, the devices on the network (for example, routers), and how you want to support your clients in DHCP.

Understanding your network topology

One of the most important aspects of planning a DHCP implementation is understanding you 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 whether DHCP can work with your DNS or PPP servers. Depending on the complexity of your network, you might even want to sketch your network topology on a piece of scrap paper. You must 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 might 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 might need to set up a few DHCP/BOOTP relay agents or enable your routers to forward DHCP packets to make it work.

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 might 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 others 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 can 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 might not be able to service all the requests from new clients, which might, 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 can document which network address ranges you want the DHCP server to manage. You must identify which devices have a manually configured IP address (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 you want to assign specific IP addresses to certain clients. You might want to reserve a specific address and configuration parameters for a specific client on a particular subnet, such as a file server. Or, you might 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 addresses to the BOOTP clients from the address pool. After 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 is a good option if you have a large number of BOOTP clients in your network.

Another option is to migrate your 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 might 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 must identify other servers in your network, such as the Domain Name System (DNS) server, that your clients might 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 have specified the same router, for example, for every client in your network, you must change the configuration for every client when the router has changed. However, if you have specified the router at the global level (all of the clients will inherit this configuration information), you only need to change the information once and the information is changed for all clients.

Some of your clients might have unique TCP/IP configuration requirements that require the 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 might need a longer lease time than all the other clients. Or, maybe only one client, such as a file server, needs a dedicated IP address. Identifying those clients and the unique information they require beforehand will help you when you start configuring the DHCP server.

For a quick reference to all of the configuration options, refer to “DHCP options lookup” on page 8.

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 might want to consider adding a DNS server when you add the DHCP server. You can read the DNS topic in the information center 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 those remote clients 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 System i” on page 36 or “Example: DHCP and PPP profile on different System i models” on page 38. These examples also explain how to set up the network to use PPP and DHCP together for your remote clients.

Related concepts

“Examples: DHCP” on page 23
By reviewing diagrams and examples of how different networks are set up, you can determine which is the best choice for your installation.

“Relay agents and routers” on page 5
You can use Dynamic Host Configuration Protocol (DHCP) relay agents and routers to efficiently and securely transfer data throughout the network.

“DHCP client support” on page 6
You can use a DHCP server to manage each client in your network individually, rather than managing all of the clients as a large group (subnet).

“Leases” on page 3
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 can use the IP address it has been assigned. The duration of the lease time can be changed according to your specific requirement.

“BOOTP” on page 7
The Bootstrap Protocol (BOOTP) is a host configuration protocol that was used before the Dynamic Host Configuration Protocol (DHCP) was developed. BOOTP support is a subset of DHCP.

“Dynamic updates” on page 7
You can configure a Dynamic Host Configuration Protocol (DHCP) server to work with a Domain Name System (DNS) server to dynamically update the client information in the DNS when DHCP assigns the client an IP address.

Domain Name System

Configuring DHCP

Here are instructions for setting up your DHCP server and clients, and for configuring DHCP to send dynamic updates to Domain Name System (DNS).

Related reference

“Planning for DHCP” on page 41
Setting up Dynamic Host Configuration Protocol (DHCP) can be a time-consuming and error-prone process if you do not take time to plan how to configure your DHCP server. To configure your DHCP server more efficiently, consider network setup and security concerns beforehand.

Configuring the DHCP server and BOOTP/DHCP relay agent

Use the following information to work with the DHCP server and the BOOTP/DHCP relay agent, such as configuring, starting, or stopping the DHCP server or the BOOTP/DHCP relay agent.

Related concepts

“Relay agents and routers” on page 5
You can use Dynamic Host Configuration Protocol (DHCP) relay agents and routers to efficiently and securely transfer data throughout the network.

Configuring or viewing the DHCP server

You can use the DHCP server configuration function to create a new DHCP configuration or view the existing DHCP configuration.

About this task

To access the DHCP server configuration, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP** → **DHCP**.
2. Right-click **DHCP**, and then select **Configuration**.

Results

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.

Creating a shortcut to the DHCP configuration window

Follow these steps if you look at the DHCP configuration frequently and want to create a shortcut to the DHCP configuration window on your desktop.

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP** → **DHCP**.
2. Right-click **DHCP**, and then select **Create Shortcut**.

Starting or stopping the DHCP server

After the DHCP server is configured, follow these steps to start or stop the DHCP server.

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

Configuring the DHCP server to be started automatically

To configure the DHCP server to be started automatically, follow these steps.

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP** → **DHCP**.
2. Right-click **DHCP**, and then select **Configuration**.
3. Right-click **DHCP Server** and select **Properties**.
4. Select the **Start when TCP/IP is started** check box.
5. Click **OK**.

Accessing the DHCP server monitor

The Dynamic Host Configuration Protocol (DHCP) server monitor is provided to monitor active lease information for an IBM® System i DHCP server. You can use this graphical interface to view which IP addresses are leased, how long they have been leased, and when they will be available to lease again.

About this task

To access the DHCP server monitor, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP** → **DHCP**.
2. Right-click **DHCP**, and then select **Monitor**.

Configuring the BOOTP/DHCP relay agent

i5/OS provides a DHCP/BOOTP relay agent that can be used to forward DHCP packets to a DHCP server on a different network.

About this task

To set up the DHCP/BOOTP relay agent, follow these steps:

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP** → **BOOTP/DHCP relay agent**.
2. Right-click **BOOTP/DHCP relay agent**, and then select **Configuration**.
3. Specify the interface that the relay agent will receive the DHCP packets from, and the destination where the packets should be forwarded, and click **OK**.

Starting or stopping the BOOTP/DHCP relay agent

After the DHCP/BOOTP relay agent is configured, you can start or stop it by following these steps.

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP** → **BOOTP/DHCP relay agent**.
2. Right-click **BOOTP/DHCP relay agent**, and then select **Start** or **Stop**.

Configuring the BOOTP/DHCP relay agent to be started automatically

To configure the BOOTP/DHCP relay agent to be started automatically when TCP/IP is started, follow these steps.

About this task

1. In System i Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP** → **BOOTP/DHCP relay agent**.
2. Right-click **BOOTP/DHCP relay agent**, and then select **Properties**.
3. Select the **Start when TCP/IP is started** check box and click **OK**.

Configuring clients to use DHCP

After the Dynamic Host Configuration Protocol (DHCP) server is configured, clients must be configured as well to request their configuration information from the DHCP server.

About this task

The following information describes the steps to configure your Windows® clients to request their configuration information from the DHCP server. In addition, it describes how the clients can view their own DHCP lease information.

Enabling DHCP for Windows Me clients

The Dynamic Host Configuration Protocol (DHCP) function for Windows Me clients can be enabled or disabled from a graphical interface that the Windows Me operating system provides.

About this task

To enable DHCP, follow these steps:

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

Checking the DHCP lease for Windows Me clients:

Windows Me clients have a utility that displays the client's MAC address and DHCP lease information. You can also use it to release and renew DHCP leases.

About this task

To check the DHCP lease for the client, complete the following steps:

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

Results

Note: This utility does not dynamically update the displayed information, so it is necessary to rerun the utility to view updated status.

Enabling DHCP for Windows 2000 clients

The Dynamic Host Configuration Protocol (DHCP) function for Windows 2000 clients can be enabled or disabled from a graphical interface that the Windows 2000 operating system provides.

About this task

To enable DHCP, follow these 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 then select **Properties**.
4. On the **General** tab, select **Obtain an IP address from a DHCP server**.
5. Click **OK**.

Checking the MAC address and DHCP lease:

Windows 2000 and Windows XP clients have a utility that displays the client's MAC address and DHCP lease information. You can also use this utility to release and renew DHCP leases.

About this task

To check the DHCP lease for a Windows 2000 or a Windows XP client, follow these steps:

1. Open a Command Prompt window.
2. Run **IPCONFIG /ALL**.

Results

Note: This utility does not dynamically update the displayed information, so it will be necessary to rerun 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.

If you want the DHCP server to update DNS A records on behalf of the client, configure the DHCP clients of Microsoft® Windows 2000 and Windows XP. This configuration might simplify your DNS administration because DNS updates will then originate from the DHCP server for all clients, rather than some clients updating their own records.

Updating DNS A records:

You can follow these steps to enable Windows 2000 or Windows XP to use the DHCP server to update DNS A records on behalf of the client.

1. On the **Start** Menu, complete either of the following steps according to your Windows environment.
   - Windows XP: Select **Control Panel** → **Network Connections**.

- Windows 2000: Select **Settings** → **Network and Dial-up Connections**.

2. Right-click the appropriate connection name and select **Properties**.
3. Select **TCP/IP Protocol**, and then select **Properties**.
4. Click **Advanced**. On the **DNS** tab, make sure **Register this connection's addresses in DNS** is unchecked.
5. Click **OK** on the Advanced TCP/IP Settings panel.
6. Click **OK** on the Internet Protocol (TCP/IP) Properties panel.
7. Click **OK**.

Enabling DHCP for Windows XP clients

You can enable or disable the Dynamic Host Configuration Protocol (DHCP) function for Windows XP clients from a graphical interface that the Windows XP operating system provides.

About this task

To enable DHCP, follow these steps:

1. On the **Start** Menu, select **Control Panel** → **Network Connections**.
2. Right-click the appropriate connection name and select **Properties**.
3. Select **TCP/IP Protocol**, and then select **Properties**.
4. On the **General** tab, select **Obtain an IP address automatically**.
5. Click **OK**.

Checking the MAC address and DHCP lease:

Windows 2000 and Windows XP clients have a utility that displays the client's MAC address and DHCP lease information. You can also use this utility to release and renew DHCP leases.

About this task

To check the DHCP lease for a Windows 2000 or a Windows XP client, follow these steps:

1. Open a Command Prompt window.
2. Run **IPCONFIG /ALL**.

Results

Note: This utility does not dynamically update the displayed information, so it will be necessary to rerun 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.

If you want the DHCP server to update DNS A records on behalf of the client, configure the DHCP clients of Microsoft Windows 2000 and Windows XP. This configuration might simplify your DNS administration because DNS updates will then originate from the DHCP server for all clients, rather than some clients updating their own records.

Updating DNS A records:

You can follow these steps to enable Windows 2000 or Windows XP to use the DHCP server to update DNS A records on behalf of the client.

1. On the **Start** Menu, complete either of the following steps according to your Windows environment.
   - Windows XP: Select **Control Panel** → **Network Connections**.
   - Windows 2000: Select **Settings** → **Network and Dial-up Connections**.

2. Right-click the appropriate connection name and select **Properties**.
3. Select **TCP/IP Protocol**, and then select **Properties**.
4. Click **Advanced**. On the **DNS** tab, make sure **Register this connection's addresses in DNS** is unchecked.
5. Click **OK** on the Advanced TCP/IP Settings panel.
6. Click **OK** on the Internet Protocol (TCP/IP) Properties panel.
7. Click **OK**.

Configuring DHCP to send dynamic updates to DNS

The Dynamic Host Configuration Protocol (DHCP) server can be configured 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.

About this task

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 record updates to occur, Domain Name System (Option 31 of i5/OS) must be installed on this server. The DHCP server uses programming interfaces provided by Option 31 to perform dynamic updates. The DNS server can be running on a separate System i model 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 panel 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.

Related concepts

"Dynamic updates" on page 7
You can configure a Dynamic Host Configuration Protocol (DHCP) server to work with a Domain Name System (DNS) server to dynamically update the client information in the DNS when DHCP assigns the client an IP address.

Disabling DNS dynamic updates

By disabling the Domain Name System (DNS) dynamic updates function, the responsibility of managing the DNS server is returned to the administrator. Disabling DNS dynamic updates might be suitable for networks where hosts rarely change locations, where growth and change are infrequent, and when stricter DNS server administration is required.

About this task

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 then 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. Click **OK**.

Results

Follow these steps for all connections that you want to have the DNS records update delegated to the DHCP server.

Managing leased IP addresses

You can use the Dynamic Host Configuration Protocol (DHCP) configuration tool to specify the IP address pool that DHCP manages and the lease time for those address pools. You can use the DHCP server monitor to see which of the IP addresses are currently being leased.

The DHCP server monitor is provided to monitor active lease information for a System i DHCP server. You can use this graphical interface to view which IP addresses are leased, how long they have been leased, and when they are available to lease again.

You can also use the DHCP server monitor 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. Use the active lease information to determine if you can delete any leases to make the IP addresses available to other clients. For example, you might 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 can only perform this operation when you are certain that the client will no longer attempt to use the address. The DHCP server does 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 might end up with duplicate IP address assignments on your network.

Related concepts

“Problem: Duplicate IP address assignments on the same network” on page 52
An IP address must be unique across your network. The Dynamic Host Configuration Protocol (DHCP) server cannot assign a single IP address to more than one client.

Troubleshooting DHCP

Follow these guidelines when troubleshooting DHCP problems.

About this task

If your problem is not listed here, review the “Planning for DHCP” on page 41 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 topic for directions to access server log data and trace information.

Related reference

Using communications trace to solve communication problems

Gathering detailed DHCP error information

There are a couple of ways to find out the error details behind the problem that you are encountering.

About this task

First, look at the DHCP server job log, using the follow steps:

1. In System i Navigator, expand ***your system*** → **Network** → **Servers** → **TCP/IP** → **DHCP**.
2. Right-click **DHCP**, and then select **Server Jobs**.

Results

If there are no messages in the DHCP server job log, it might be necessary to collect the information from the System i communication trace or the internal program trace of the DHCP server. The 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.

Tracing the DHCP server

The DHCP log file is used to record the DHCP server logging information. Viewing the DHCP log file can help you locate where the problem is and the reasons that cause the problem.

About this task

To trace the DHCP server, follow these steps:

1. In System i Navigator, expand ***your system*** → **Network** → **Servers** → **TCP/IP** → **DHCP**.
2. Right-click **DHCP**, and then select **Configuration**.
3. Right-click **DHCP Server** and select **Properties**.
4. Select the **Logging** properties tab.
5. Check the **Enable Logging** check box.
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. Click **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 then select **Properties** → **Logging**.
12. Deselect **Enable Logging** to turn off logging.
13. Click **OK**.
14. Right-click **DHCP Server**, and then select **Update Server** to restart the DHCP server.
15. View the DHCP log file in QIBM/UserData/OS400/DHCP/dhcpsd.log. Do one of the following steps:
    - In System i Navigator, expand ***your system*** → **File Systems** → **Integrated File System** → **Root** → ***the file's directory***.
    - From a character-based interface, use the Work with Object Links (WRKLNK) command and select option 5 (Display).

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

Problems might occur if the clients cannot receive an IP address or the configuration information. An IP address is leased to a client through a four-step process between the client and the Dynamic Host Configuration Protocol (DHCP) server.

All four steps must take place before the client receives an IP address. Refer to the "DHCP client/server interaction" on page 1 topic for details about the four-step process.

Here are some common reasons for this problem.

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" on page 41.

The DHCPDISCOVER 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 DHCPDISCOVER message to the DHCP server. For more information, refer to "Relay agents and routers" on page 5. 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 System i model is multihomed, you might need to add a subnet group to the DHCP configuration. For more detail about configuring DHCP for a multihomed system, see "Example: DHCP and multihoming" on page 28. This example describes what needs to be done to the DHCP configuration so that the client's broadcast message is received by the system.

The DHCP server does not have any available addresses for the client in the address pool.
You can use the DHCP server monitor to see which addresses are currently being used by the DHCP server. "Managing leased IP addresses" on page 50 provides more details about using the DHCP server monitor. If the DHCP server has run out of available addresses, you might 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 must be unique across your network. The Dynamic Host Configuration Protocol (DHCP) server cannot 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 monitor to view which IP addresses that the server has detected are in use but were not assigned by the DHCP server. These addresses will have a USED status and an UNKNOWN_TO_IBMDHCP client identifier.

Here are some common reasons for this problem.

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 receives the IP address from one of the DHCP servers, and the other client receives the same IP address from the other DHCP server. Multiple DHCP servers can serve the same subnet or network, but they must 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 typically 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 might 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.

Related concepts

"Managing leased IP addresses" on page 50
You can use the Dynamic Host Configuration Protocol (DHCP) configuration tool to specify the IP address pool that DHCP manages and the lease time for those address pools. You can use the DHCP server monitor to see which of the IP addresses are currently being leased.

Problem: DNS records are not being updated by DHCP

The System i DHCP server is capable of dynamically updating DNS resource records. The DHCP server uses name resolution functions and programming interfaces to determine the appropriate dynamic DNS server to update. You can use this information when troubleshooting dynamic update errors.

Check the following points when the DNS records are not being updated dynamically.

Verify which subnets and the type of resource records (A, PTR, or both 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.

Verify that i5/OS Domain Name System, Option 31, is installed on the System i model that is running DHCP.
The DHCP server uses programming interfaces provided by the i5/OS Domain Name System feature, Option 31. The DNS that is being dynamically updated does not need to reside on the same system as the DHCP server.

Verify the DHCP server is authorized to send updates to the DNS server.
Check the DNS configuration to verify that 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 System i model where DHCP resides by using the Change TCP/IP Domain (CHGTCPDMN) command. Verify that these DNS servers can resolve the domain that is being updated. To do this, run the Name Server Lookup (NSLOOKUP) tool from the System i model where DHCP is running to resolve a name (or IP address) 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 does not attempt to update a dynamic DNS without an 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), Option 15 (Domain Name), or both options in the DHCPREQUEST message from the client.
3. Option 12 (Host Name) in the DHCPREQUEST message from the client, Option 15 (Domain Name) configured in the DHCP server, or both of these options. 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 might 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 system 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 does not update the DNS A resource record. This prevents

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).

Related concepts

"Dynamic updates" on page 7
You can configure a Dynamic Host Configuration Protocol (DHCP) server to work with a Domain Name System (DNS) server to dynamically update the client information in the DNS when DHCP assigns the client an IP address.

Problem: DHCP job log has DNS030B messages with error code 3447

Error code 3447 means that the Dynamic Host Configuration Protocol (DHCP) server times out while waiting for a response from the Domain Name System (DNS) server. This might be due to network or connection problems between the System i DHCP server and the 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 server attempts to update DNS resource records each time a lease is renewed, the resource records might 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 might 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 server attempts to update the resource record at the next lease renewal request. So, you can wait until that occurs. Or, many clients attempt to renew or reacquire an IP address when they are turned on. You might want to try to restart the client, which can cause the DHCP server to attempt to update the DNS resource records again.

If none 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 you make manual updates. So, other dynamic updates from the DHCP server are lost during this downtime. However, you can use the dynamic update utilities that are provided by some client and BIND DNS server implementations to update the resource record. Although 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.

Related information for DHCP

IBM Redbooks and Web sites contain information that relates to the DHCP topic collection. You can view or print any of the PDF files.

IBM Redbooks

AS/400® TCP/IP Autoconfiguration: DNS and DHCP Support  (5181 KB)

This IBM Redbooks publication describes the Domain Name System (DNS) server and Dynamic Host Configuration Protocol (DHCP) server support that are included in i5/OS. The information in this Redbooks publication helps you install, tailor, configure, and troubleshoot the DNS and DHCP support through examples.

DHCP RFCs

Requests for Comments (RFCs) are written definitions of protocol standards and proposed standards used for the Internet. The following RFCs might 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)

Related reference

"PDF file for DHCP" on page 1
You can view and print a PDF file of this information.

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming interface information

This DHCP publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

| AS/400
| i5/OS
| IBM
| IBM (logo)
| Redbooks
| System i

| Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks
| of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA