Solaris DHCP Administration Guide

Beta

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900
U.S.A.

Part No: 806–5529–10
July 2001

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REPONDRE A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.

Contents

Tables

Figures

Examples

Preface

This *Solaris DHCP Administration Guide* is an update of the DHCP information provided in the *System Administration Guide, Volume 3*, relevant to the Solaris 8 7/01 release.

This manual provides conceptual information about the DHCP protocol and how the Solaris DHCP implementation works. It also provides information for planning, configuring, and administering your DHCP service.

Who Should Use This Book

This book is intended for administrators who are responsible for the DHCP service on systems running the Solaris 8 release. To use this book, you should have 1 to 2 years of UNIX® system administration experience.

How This Book Is Organized

This book consists of the following chapters:

Chapter 1 introduces the Dynamic Host Configuration Protocol (DHCP), explains the concepts underlying the protocol, and describes the advantages of using it in your network.

Chapter 2 describes what you need to do before setting up DHCP service on your network.

Chapter 3 includes procedures for configuring the DHCP server and placing networks and their associated IP addresses under DHCP management.

Chapter 4 describes tasks useful in administering the Solaris DHCP service.

Chapter 5 provides information to help you solve problems you might encounter when configuring a Solaris DHCP server or client, or problems in using DHCP after configuration is complete.

Chapter 6 provides useful information regarding the relationships between Solaris DHCP files and the commands that use the files.

Ordering Sun Documents

Fatbrain.com, an Internet professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at `http://www1.fatbrain.com/documentation/sun`.

Accessing Sun Documentation Online

The docs.sun.com^{SM} Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is `http://docs.sun.com`.

Typographic Conventions

The following table describes the typographic changes used in this book.

TABLE P–1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`

`AaBbCc123`	What you type, contrasted with on-screen computer output	`machine_name%` **`su`**
		`Password:`

AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type **`rm`** *filename*.
AaBbCc123	Book titles, new words, or terms, or words to be emphasized.	Read Chapter 6 in *User's Guide*. These are called *class* options. You must be *root* to do this.

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–2 Shell Prompts

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

CHAPTER 1

Overview of DHCP

This chapter introduces the Dynamic Host Configuration Protocol (DHCP), explains the concepts underlying the protocol, and describes the advantages of using it in your network.

This chapter contains the following information:

About the DHCP Protocol

The DHCP protocol enables host systems in a TCP/IP network to be configured automatically for the network as they boot. DHCP uses a client/server mechanism. Servers store and manage configuration information for clients, and provide that information upon a client’s request. The information includes the client’s IP address and information about network services available to the client.

DHCP evolved from an earlier protocol, BOOTP, which was designed for booting over a TCP/IP network. DHCP uses the same format as BOOTP for messages between client and sever, but includes more information in the messages. The additional information is the network configuration data for the client.

A primary benefit of DHCP is its ability to manage IP address assignments through leasing, which allows IP addresses to be reclaimed when not in use and reassigned to other clients. This enables a site to use a smaller pool of IP address than would be needed if all clients were assigned a permanent address.

Advantages of Using Solaris DHCP

DHCP relieves the system or network administrator of some of the time-consuming tasks involved in setting up a TCP/IP network and the daily management of that network. Note that Solaris DHCP works only with IPv4.

Solaris DHCP offers the following advantages:

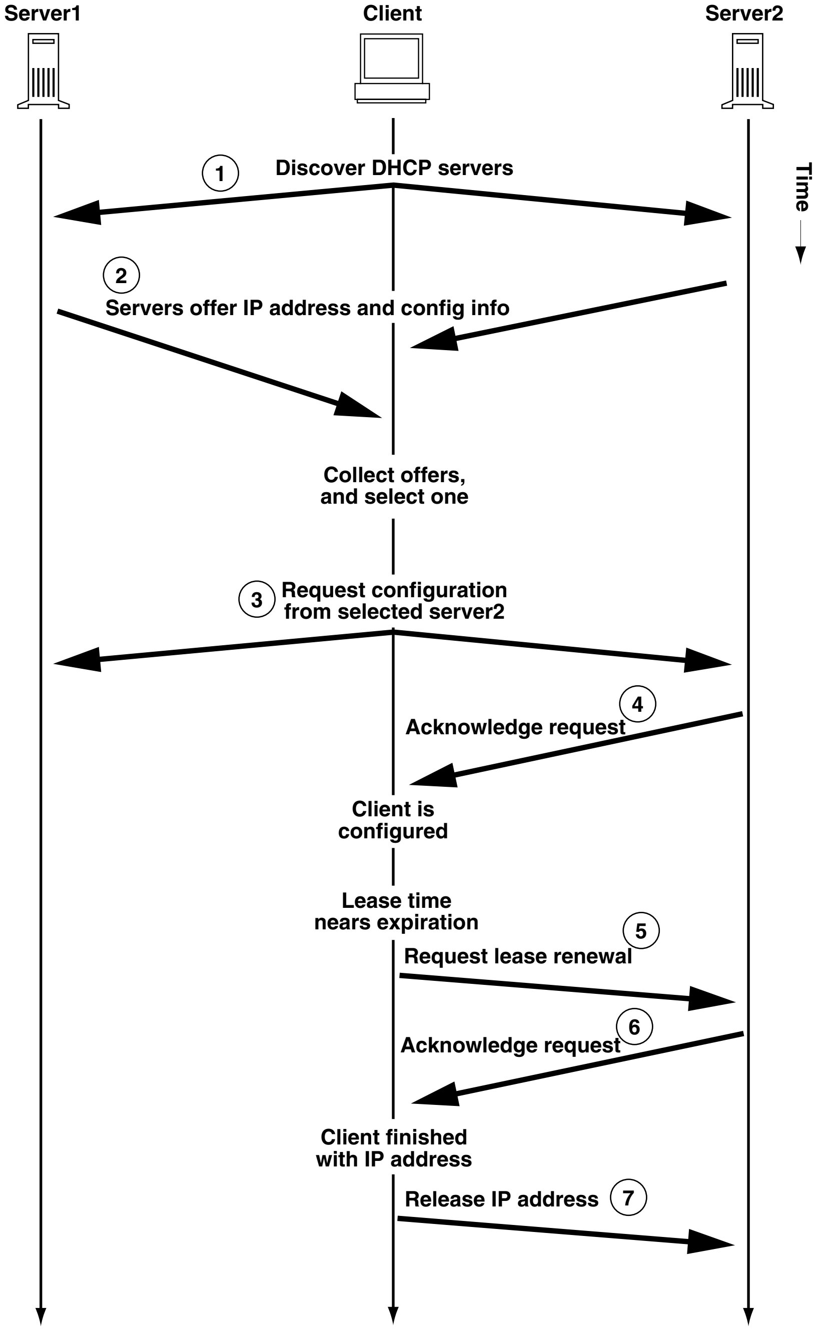
- **IP address management** – A primary advantage of DHCP is easier management of IP addresses. In a network without DHCP, an administrator must manually assign IP addresses, being careful to assign unique IP addresses to each client and configure each client individually. If a client moves to a different network, the administrator must make manual modifications for that client. When DHCP is enabled, the DHCP server manages and assigns IP addresses without administrator intervention. Clients can move to other subnets without manual reconfiguration because they obtain, from a DHCP server, new client information appropriate for the new network.
- **Centralized network client configuration** – A network administrator can create a tailored configuration for certain clients, or certain types of clients, and keep the information in one place, the DHCP data store. The administrator does not need to log in to a client to change its configuration. The administrator can make changes for multiple clients just by changing the information in the data store.
- **Support of BOOTP clients** – Both BOOTP servers and DHCP servers listen and respond to broadcasts from clients. The DHCP server can respond to requests from BOOTP clients as well as DHCP clients. BOOTP clients receive an IP address and the information needed to boot from a server.
- **Support of local and remote clients** – BOOTP provides for the relaying of messages from one network to another. DHCP takes advantage of the BOOTP relay feature in several ways. Most network routers can be configured to act as BOOTP relay agents to pass BOOTP requests to a server that is not on the client's network. DHCP requests can be relayed in the same manner because, to the router, they are indistinguishable from BOOTP requests. The Solaris DHCP server can also be configured to behave as a BOOTP relay agent, if a router that supports BOOTP relay is not available.
- **Network booting** – Clients can use DHCP to obtain the information needed to boot from a server on the network, instead of using RARP (Reverse Address Resolution Protocol) and `bootparams`. The DHCP server can give a client all the information it needs to function, including IP address, boot server, and network configuration information. Because DHCP network boot requests can be relayed across subnets, you can deploy fewer boot servers in your network when you use DHCP network booting. RARP booting requires that each subnet has a boot server.
- **Large network support** - Networks with millions of DHCP clients can use Solaris DHCP. The DHCP server uses multithreading to process many client requests simultaneously and supports data stores optimized to handle large amounts of

data. Data store access is handled by separate processing modules, and sites can add support for any database they want to use for their DHCP data.

How DHCP Works

The DHCP server must first be installed and configured by a system administrator. During configuration, the administrator enters information about the network that clients will need to operate on the network. After this information is in place, clients are able to request and receive network information.

The sequence of events for DHCP service is shown in the following diagram. The numbers in circles correlate to the numbered items in the description following the diagram.



Server1
Client
Server2
1
Discover DHCP servers
Time
2
Servers offer IP address and config info
Collect offers, and select one
3
Request configuration from selected server2
4
Acknowledge request
Client is configured
Lease time nears expiration
5
Request lease renewal
6
Acknowledge request
Client finished with IP address
Release IP address
7

FIGURE 1–1 Sequence of Events for DHCP Service

LEGEND:

1. The client discovers a DHCP server by broadcasting a discover message to the limited broadcast address (255.255.255.255) on the local subnet. If a router is present and configured to behave as a BOOTP relay agent, the request is passed to other DHCP servers on different subnets. The client's broadcast includes its unique ID, which in the Solaris DHCP implementation, is derived from the client's Media Access Control (MAC) address. On an Ethernet network, the MAC address is the same as the Ethernet address.

   DHCP servers that receive the discover message can determine the client's network by looking at the following information:

   - Which network interface did the request come in on? This tells the server that the client is either on the network to which the interface is connected, or that the client is using a BOOTP relay agent connected to that network.
   - Does the request include the IP address of a BOOTP relay agent? When a request passes through a relay agent, the relay agent inserts its address in the request header. When the server detects a relay agent address, it knows that the network portion of the address indicates the client's network address because the relay agent must be connected to the client's network.
   - Is the client's network subnetted? The server consults the `netmasks` table to find the subnet mask used on the network indicated by the relay agent's address or the address of the network interface that received the request. Once the server knows the subnet mask used, it can determine which portion of the network address is the host portion, and then select an IP address appropriate for the client. (See `netmasks`(4) for information on `netmasks`.)

2. After they determine the client's network, DHCP servers select an appropriate IP address and verify that the address is not already in use. The DHCP servers then respond to the client by broadcasting an offer message that includes the selected IP address and information about services that can be configured for the client. Each server temporarily reserves the offered IP address until it can determine if the client will use it.

3. The client selects the best offer (based on the number and type of services offered) and broadcasts a request that specifies the IP address of the server that made the best offer. The broadcast ensures that all the responding DHCP servers know the client has chosen a server, and those servers not chosen can cancel the reservations for the IP addresses they had offered.

4. The selected server allocates the IP address for the client, stores the information in the DHCP data store, and sends an acknowledgement (ACK) to the client. The acknowledgement message contains the network configuration parameters for the client. The client uses `ping` to test the IP address to make sure no other system is using it, then continues booting to join the network.

5. The client monitors the lease time, and when a set period of time has elapsed, the client sends a new message to the chosen server to increase its lease time.

6. The DHCP server that receives the request extends the lease time if it still adheres to the local lease policy set by the administrator. If the server does not respond within 20 seconds, the client broadcasts a request so that one of the other DHCP servers can extend the lease.
7. When the client no longer needs the IP address, it notifies the server that it is releasing the IP address. This can happen during an orderly shutdown and can also be done manually.

Solaris DHCP Server

The Solaris DHCP server runs as a daemon in the Solaris operating environment on a host system. The server has two basic functions:

- **Managing IP addresses** – The server controls a range of IP addresses, and allocates them to clients, either permanently or for a defined period of time. The DHCP server uses a lease mechanism to determine how long a client can use a nonpermanent address. When the address is no longer in use, it is returned to the pool and can be reassigned. The server maintains information about the binding of IP addresses to clients in its DHCP network tables, ensuring that no address is used by more than one client.
- **Providing network configuration for clients** – The server assigns an IP address and provides other information for network configuration, such as a hostname, broadcast address, network subnet mask, default gateway, name service, and potentially much more information. The network configuration information is obtained from the server's `dhcptab` database.

The Solaris DHCP server can also be configured to perform the following additional functions:

- **Responding to BOOTP client requests** – The server listens for broadcasts from BOOTP clients discovering a BOOTP server and provides them with an IP address and boot parameters. The information must have been configured statically by an administrator. The DHCP server can perform as a BOOTP server and DHCP server simultaneously.
- **Relaying requests** – The server relays BOOTP and DHCP requests to appropriate servers on other subnets. The server cannot provide DHCP or BOOTP service when configured as a BOOTP relay agent.
- **Providing network booting support for DHCP clients** – The server can provide DHCP clients with information needed to boot over the network: IP address, boot parameters, and network configuration information.
- **Updating DNS tables for clients that supply a host name** – For clients that provide a Hostname option and value in their requests for DHCP service, the server can attempt DNS updates on their behalf.

DHCP Server Management

As superuser, you can start, stop, and configure the DHCP server with the DHCP Manager, or with command-line utilities described in "DHCP Command-Line Utilities" on page 27. Generally, the DHCP server is configured to start automatically when the system boots, and stop when the system is shut down. You should not need to start and stop the server manually under normal conditions.

DHCP Data Store

All the data used by the Solaris DHCP server is maintained in a data store, which might be stored as plain text files, NIS+ tables, or binary-format files. While configuring the DHCP service, the administrator chooses the type of data store to be used. The section "Choosing the Data Store" on page 44 describes the differences between the data stores. Data stores can be converted from one format to another using DHCP Manager or the `dhcpconfig` command.

You can also move data from one DHCP server's data store to another with export and import utilities that work with the data stores, even if the servers are using different data store formats. The entire content of a data store, or just some of the data within it, can be exported and imported using DHCP Manager or the `dhcpconfig` command.

Note – Any database or file format can be used for DHCP data storage if you want to develop your own code module to provide an interface between Solaris DHCP (server and management tools) and the database. *Solaris DHCP Service Developer's Guide* contains information for doing this.

Within the Solaris DHCP data store are two types of tables, the contents of which you can view and manage by using either the DHCP Manager or command-line utilities. The data tables are:

- `dhcptab` table – Table of configuration information that can be passed to clients.
- **DHCP network tables** – Tables that contain information about the DHCP and BOOTP clients that reside on the network specified in the table name. For example, the network 134.20.0.0 would have a table whose name includes `134_20_0_0`.

The `dhcptab` Table

The `dhcptab` table contains all the information that clients can obtain from the DHCP server. The DHCP server scans the `dhcptab` each time it starts. The file name of the `dhcptab` varies according to the data store used. For example, the `dhcptab` created by the NIS+ data store `SUNWnisplus` is `SUNWnisplus1_dhcptab`.

The DHCP protocol defines a number of standard items of information that can be passed to clients. These items are referred to as parameters, symbols, or options. Options are defined in the DHCP protocol by numeric codes and text labels, but without values. Some commonly used standard options are shown in the following table.

TABLE 1–1 Sample DHCP Standard Options

Code	Label	Description
1	Subnet	Subnet mask IP address
3	Router	IP address for router
6	DNSserv	IP address for DNS server
12	Hostname	Text string for client host name
15	DNSdmain	DNS domain name

Some options are automatically assigned values when the administrator provides information during server configuration. The administrator can also explicitly assign values to other options at a later time. Options and their values are passed to the client to provide configuration information. For example, the option/value pair, `DNSdmain=Georgia.Peach.COM`, sets the client's DNS domain name to `Georgia.Peach.COM`.

Options can be grouped with other options in containers known as macros, which makes it easier to pass information to a client. Some macros are created automatically during server configuration, and contain options that were assigned values during configuration. Macros can also contain other macros.

The format of the `dhcptab` table is described in `dhcptab`(4) man page. In DHCP Manager, all the information shown in the Options and Macros tabs comes from the `dhcptab` table. See "About Options" on page 30 for more information about options, and "About Macros" on page 30 for more information about macros.

Note that the `dhcptab` table should not be edited manually. You should use either the `dhtadm` command or DHCP Manager to create, delete, or modify options and macros.

DHCP Network Tables

A DHCP network table maps client identifiers to IP addresses and the configuration parameters associated with each address. The format of the network tables is described in the `dhcp_network`(4) man page. In DHCP Manager, all the information shown in the Addresses tab is acquired from the network tables.

DHCP Manager

DHCP Manager is a graphical tool you can use to perform all management duties associated with DHCP services, and you must be root when you run it. You can use it to manage the server itself as well as the data the server uses. You can use DHCP Manager with the server in the following ways:

- Configure and unconfigure the DHCP server
- Start, stop, and restart the DHCP server
- Disable and enable DHCP service
- Customize server settings

DHCP Manager allows you to manage the IP addresses, network configuration macros, and network configuration options in the following ways:

- Add and delete networks under DHCP management
- View, add, modify, delete, and release IP addresses under DHCP management
- View, add, modify, and delete network configuration macros
- View, add, modify, and delete nonstandard network configuration options

DHCP Manager allows you to manage the DHCP data stores in the following ways:

- Convert data to a new data store format
- Move DHCP data from one DHCP server to another by exporting it from the first server and importing it on the second server

DHCP Manager includes extensive online help for procedures you can perform with the tool.

DHCP Command-Line Utilities

All DHCP management functions can be performed using command-line utilities. You can run them if you are logged in as root, or as a user assigned to the DHCP Management profile. See "Setting Up User Access to DHCP Commands" on page 74.

The following table lists the utilities and describes the purpose of each utility.

TABLE 1–2 DHCP Command-Line Utilities

Command	Description and Purpose
`in.dhcpd`	The DHCP service daemon. It provides command-line arguments that allow you to set several runtime options.

TABLE 1–2 DHCP Command-Line Utilities *(Continued)*

Command	**Description and Purpose**
`dhcpconfig`	Used to configure and unconfigure a DHCP server. This utility enables you to perform many of the functions of DHCP Manager from the command line. It is primarily intended for use in scripts for sites that want to automate some configuration functions. `dhcpconfig` collects information from the server system's network topology files to create useful information for the initial configuration.
`dhtadm`	Used to add, delete, and modify configuration options and macros for DHCP clients. This utility lets you edit the `dhcptab` indirectly, which ensures the correct format of the `dhcptab`. You should not directly edit the `dhcptab`.
`pntadm`	Used to manage the DHCP network tables. You can use this utility to add and remove IP addresses and networks under DHCP management, modify the network configuration for specified IP addresses, and display information about IP addresses and networks under DHCP management.

Role-Based Access Control for DHCP Commands

Security for the `dhcpconfig`, `dhtadm`, and `pntadm` commands is determined by role-based access control (RBAC) settings. By default, the commands can be run only by root. If you want to be able to use the commands under another user name, you must assign the user name to the DHCP Management profile as described in "Setting Up User Access to DHCP Commands" on page 74.

DHCP Server Configuration

You configure the DHCP server the first time you run DHCP Manager on the system where you want to run the DHCP server. DHCP Manager server configuration dialogs prompt you for essential information needed to enable and run the DHCP server on one network. Some default values are obtained from existing system files. If you have not configured the system for the network, there will be no default values. DHCP Manager prompts for the following information:

- Role of the server, either DHCP server or BOOTP relay agent
- Data store type (files, binary files, NIS+, or something specific to your site)
- Data store configuration parameters, which vary according to the data store type you selected
- Naming service to use to update host records, if any (`/etc/hosts`, NIS+, or DNS)

- Length of lease time and whether clients should be able to renew leases
- DNS domain name and IP addresses of DNS servers
- Network address and subnet mask for the first network you want to be configured for DHCP service
- Network type, either LAN or point-to-point
- Router discovery or the IP address of a particular router
- NIS domain name and IP address of NIS servers
- NIS+ domain name and IP address of NIS+ servers

You can also configure the DHCP server using the `dhcpconfig` command. This utility gathers information from existing system files automatically in order to provide a useful initial configuration. Therefore, you must ensure that the files are correct before running `dhcpconfig`. See the `dhcpconfig`(1M) man page for information about the files `dhcpconfig` uses to obtain information.

IP Address Allocation

The Solaris DHCP server supports the following types of IP address allocation:

- **Manual allocation** – The server provides a specific IP address chosen by the administrator for a specific DHCP client. The address cannot be reclaimed or assigned to any other client.
- **Automatic, or permanent, allocation** – The server provides an IP address that has no expiration time, making it permanently associated with the client until the administrator changes the assignment or the client releases the address.
- **Dynamic allocation** – The server provides an IP address to a requesting client, with a lease for a specific period of time. When the lease expires, the address is taken back by the server and can be assigned to another client. The period of time is determined by the lease time configured for the server.

Network Configuration Information

The administrator determines what information to provide to DHCP clients. When you configure the DHCP server you provide essential information about the network. Later, you can add more information you want to provide to clients.

The DHCP server stores network configuration information in the `dhcptab` database, in the form of option/value pairs and macros. Options are keywords for network data you want to supply to clients. Values are assigned to options and passed to clients in DHCP messages. For example, the NIS server address is passed by way of an option called `NISservs` that has a value (a list of IP addresses) assigned by the DHCP server. Macros provide a convenient way to group together any number of options that you want to supply to clients. You can use the DHCP Manager to create macros to group options and assign values to the options. If you prefer a nongraphical tool, you can use `dhtadm`, the DHCP configuration table management utility, to work with options and macros.

About Options

In Solaris DHCP, an option is a piece of network information to be passed to a client. The DHCP literature also refers to options as symbols or tags. An option is defined by a numeric code and a text label. An option receives a value when it is used in the DHCP service.

The DHCP protocol defines a large number of standard options for commonly specified network data: `Subnet`, `Router`, `Broadcast`, `NIS+dom`, `Hostname`, and `LeaseTim` are a few examples. A complete list of standard options is shown in the `dhcp_inittab` man page. You cannot modify the standard option keywords in any way, but you can assign values to the options that are relevant to your network when you include the options in macros.

You can create new options for data that is not represented by the standard options. Options you create must be classified in one of three categories:

- **Extended** – Reserved for options that have become standard DHCP options, but are not yet included in the DHCP server implementation. You might use this if you know of a standard option that you want to use, but do not want to upgrade your DHCP server.
- **Site** – Reserved for options that are unique to your site. The system administrator creates these options.
- **Vendor** – Reserved for options that should apply only to clients of a particular class, such as hardware or vendor platform. The Solaris DHCP implementation includes a number of vendor options for Solaris clients. For example, the option `SrootIP4` is used to specify the IP address of a server that a client that boots from the network should use for its root file system.

Chapter 4 includes procedures for creating, modifying, and deleting options.

About Macros

In the Solaris DHCP service, a macro is a collection of network configuration options and the values assigned to them by the system administrator. Macros are created to group options together to be passed to specific clients or types of clients. For example, a macro intended for all clients of a particular subnet might contain option/value pairs for subnet mask, router IP address, broadcast address, NIS+ domain, and lease time.

Macro Processing by the DHCP Server

When the DHCP server processes a macro, it places the network options and values defined in the macro in a DHCP message to a client. The server processes some macros automatically for clients of a particular type.

In order for the server to process a macro automatically, the name of the macro must comply with one of the categories shown in the following table.

TABLE 1–3 Macro Categories for Automatic Processing

Macro Category	Description
Client class	The macro name matches a class of client, indicated by the client machine type and/or operating system. For example, if a server has a macro named `SUNW.Ultra-1`, any client whose hardware implementation is `SUNW,Ultra-1` automatically receives the values in the `SUNW.Ultra-1` macro.
Network address	The macro name matches a DHCP-managed network IP address. For example, if a server has a macro named `125.53.224.0`, any client connected to the 125.53.224.0 network automatically receives the values in the `125.53.224.0` macro.
Client ID	The macro name matches some unique identifier for the client, usually derived from an Ethernet or MAC address. For example, if a server has a macro named `08002011DF32`, the client with the client ID `08002011DF32` (derived from the Ethernet address `8:0:20:11:DF:32`) automatically receives the values in the macro named `08002011DF32`.

A macro with a name that does not use one of the categories listed in Table 1–3 can be processed only if one of the following is true:

- Macro is mapped to an IP address.
- Macro is included in another macro that is processed automatically.
- Macro is included in another macro that is mapped to an IP address.

Note – When you configure a server, a macro that is named to match the server's name is created by default. This server macro is *not* processed automatically for any client because it is not named with one of the name types that cause automatic processing. When you later create IP addresses on the server, the IP addresses are mapped to use the server macro by default.

Order of Macro Processing

When a DHCP client requests DHCP services, the DHCP server determines which macros match the client. The server processes the macros, using the macro categories to determine the order of processing, from the more general to the specific. The macros are processed in the following order:

1. Client class macros – the most general category
2. Network address macros – more specific than Client class
3. Macros mapped to IP addresses – more specific than Network address
4. Client ID macros – the most specific category, pertaining to one client

A macro that is included in another macro is processed as part of the containing macro.

If the same option is included in more than one macro, the value set for that option in the macro with the most specific category is used because it is processed last. For example, if a Network address macro contained the lease time option with a value of 24 hours, and a Client ID macro contained the lease time option with a value of 8 hours, the client would receive a lease time of 8 hours.

Solaris DHCP Client

The term "client" is sometimes used to refer to a physical machine that is performing a client role on the network. However, the DHCP client described here is a software entity. The Solaris DHCP client is a daemon (`dhcpagent`) that runs in the Solaris operating environment on a system that is configured to receive its network configuration from a DHCP server. DHCP clients from other vendors can also use the services of the Solaris DHCP server. However, this section describes only the Solaris DHCP client.

Notice that the description assumes one network interface. The section "DHCP Client Systems With Multiple Network Interfaces" on page 38 discusses issues important for hosts that have two or more network interfaces.

DHCP Client Installation

The Solaris DHCP client is installed and enabled on a system during installation of the Solaris operating environment when you specify that you want to use DHCP to configure network interfaces. You do not need to do anything else on the Solaris client to use DHCP.

If you want a system that is already running the Solaris operating environment to use DHCP to obtain network configuration information, see "Configuring and Unconfiguring a Solaris DHCP Client" on page 68.

DHCP Client Startup

The `dhcpagent` daemon obtains configuration information that is needed by other processes involved in booting the system. For this reason, the system startup scripts start `dhcpagent` early in the boot process and wait until the network configuration information from the DHCP server arrives.

The presence of the file `/etc/dhcp.`*interface* (for example, `/etc/dhcp.hme0` on a Sun Enterprise Ultra™ system) indicates to the startup scripts that DHCP is to be used on the specified interface. Upon finding a `dhcp.`*interface* file, the startup scripts start the `dhcpagent` daemon.

After startup, `dhcpagent` waits until it receives instructions to configure a network interface. The startup scripts issue the `ifconfig` *interface* `dhcp start` command, which instructs `dhcpagent` to start DHCP as described in "How DHCP Works" on page 21. If commands are contained within the `dhcp.`*interface* file, they are appended to the `dhcp start` option of `ifconfig`. See the `ifconfig`(1M) man page for more information about options used with the `dhcp` option.

How Solaris DHCP Client Manages Network Configuration Information

After the information packet is obtained from a DHCP server, `dhcpagent` configures the network interface and brings it up, controlling the interface for the duration of the lease time for the IP address. The `dhcpagent` daemon maintains the configuration data in an internal table held in memory. The system startup scripts use the `dhcpinfo` command to extract configuration option values from the `dhcpagent` daemon's table. The values are used to configure the system and enable it to join the network.

The agent waits passively until a period of time elapses, usually half the lease time, and then requests an extension of the lease from a DHCP server. If the `dhcpagent` daemon finds that the interface is down or the IP address has changed, it does not control the interface until it is instructed by the `ifconfig` command to do so. If the `dhcpagent` daemon finds that the interface is up and the IP address hasn't changed, it sends a request to the server for a lease renewal. If the lease cannot be renewed, the `dhcpagent` daemon takes down the interface at the end of the lease time.

DHCP Client Management

The Solaris DHCP client does not require management under normal system operation. It automatically starts when the system boots, renegotiates leases, and stops when the system shuts down. You cannot manually start and stop the `dhcpagent` daemon. However, you can use the `ifconfig` command as superuser on the client system to affect the client's management of the network interface if necessary.

`ifconfig` Command Options Used With DHCP Client

The `ifconfig` command enables you to:

- **Start the DHCP client** – The command `ifconfig` *interface* `dhcp start` initiates the interaction between the DHCP client and DHCP server to obtain an IP address and a new set of configuration options. This might be useful when you change information that you want a client to use immediately, such as when you add IP addresses or change the subnet mask.
- **Request network configuration information only** – The command `ifconfig` *interface* `dhcp inform` causes `dhcpagent` to issue a request for network configuration parameters, with the exception of the IP address. This is useful for situations where the network interface has a valid IP address, but the client system needs updated network options. For example, this might be useful if you do not use DHCP to manage IP addresses, but do use it to configure hosts on the network.
- **Request a lease extension** – The command `ifconfig` *interface* `dhcp extend` causes `dhcpagent` to issue a request to renew the lease. This happens automatically, but you might want to use this command if you change the lease time and want clients to use the new lease time immediately rather than waiting for the next attempt at lease renewal.
- **Release the IP address** – The command `ifconfig` *interface* `dhcp release` causes `dhcpagent` to relinquish the IP address used by the network interface. This happens automatically when the lease expires. You might want to issue this command if the lease time is long and you need to take down the network interface for an extended period of time or you want to remove the system from the network.
- **Drop the IP address** – The command `ifconfig` *interface* `dhcp drop` causes `dhcpagent` to take down the network interface without informing the DHCP server that it is doing so. This enables the client to use the same IP address when it reboots.
- **Ping the network interface** – The command `ifconfig` *interface* `dhcp ping` lets you test to see if the interface is under the control of DHCP.
- **View DHCP configuration status of the network interface** – The command `ifconfig` *interface* `dhcp status` displays the current state of the DHCP client. The display indicates the following:
  - If an IP address has been bound to the client

- Number of requests sent, received, and declined
- If this is the primary interface
- Times when the lease was obtained, when it expires, and when attempts to renew it will or did start For example:

```
# ifconfig hme0 dhcp status
Interface  State         Sent  Recv  Declined  Flags
hme0       BOUND            1     1         0   [PRIMARY]
(Began, Expires, Renew) = (08/16/2000 15:27, 08/18/2000 13:31, 08/17/2000 15:24)
```

DHCP Client Parameter File

The file `/etc/default/dhcpagent` on the client system contains tunable parameters for the `dhcpagent` daemon. You can use a text editor to change several parameters that affect client operation. The file is well documented so you should refer to the file for more information, as well as referring to the `dhcpagent` man page.

DHCP Client Shutdown

When the system running the DHCP client shuts down normally, the `dhcpagent` daemon writes the current configuration information to the file `/etc/dhcp/`*interface*`.dhc`. The lease is dropped rather than released, so the DHCP server does not know that the IP address is not in active use.

If the lease is still valid when the system reboots, the DHCP client sends an abbreviated request to use the same IP address and network configuration information it had used before the system rebooted. If the DHCP server permits this, the client can use the information that it wrote to disk when the system shut down. If the server does not permit the client to use the information, the client initiates the DHCP protocol sequence described previously and obtains new network configuration information.

DHCP Client Systems and Name Services

Solaris systems support the following name services: DNS, NIS, NIS+, and a local file store (`/etc/hosts`). Each name service requires some configuration before it is usable. The name service switch configuration file (see `nsswitch.conf`(4)) must also be set up appropriately to indicate the name services to be used.

Before a DHCP client system can use a name service, you must configure the system as a client of the name service.

The following table summarizes issues related to each name service and DHCP, and includes links to documentation that can help you set up clients for each name service.

TABLE 1–4 Name Service Client Setup Information for DHCP Client Systems

Name Service	Client Setup Notes

NIS	If you are *installing* the Solaris operating environment on a client system by using Solaris DHCP, you can use a configuration macro that contains the `NISservs` and `NISdmain` options to pass the IP addresses of NIS servers and the NIS domain name to the client. The client then automatically becomes a NIS client.
	If a DHCP client system is already running the Solaris operating environment, the NIS client is not automatically configured on that system when the DHCP server sends NIS information to the client.
	If the DHCP server is configured to send NIS information to the DHCP client system, you can see the values given to the client if you use the `dhcpinfo` command on the client as follows:
	`# /sbin/dhcpinfo NISdmain`
	`# /sbin/dhcpinfo NISservs`
	Use the values returned for the NIS domain name and NIS servers when you set up the system as a NIS client.
	You set up a NIS client for a Solaris DHCP client system in the standard way, as documented in “Configuring NIS Service” in *Solaris Naming Setup and Configuration Guide*.
	Note – You can write a script that uses `dhcpinfo` and `ypinit` to automate NIS client configuration on DHCP client systems.

NIS+	If the DHCP client system receives a nonreserved IP address (the address may not always be the same), you must set up the NIS+ client for a DHCP client system in a nonstandard way, which is documented in “Setting Up DHCP Clients as NIS+ Clients” on page 131. This procedure is necessary because NIS+ uses security measures to authenticate requests for service. The security measures depend upon the IP address. If the DHCP client system has been manually assigned an IP address (the client’s address is always the same), you can set up the NIS+ client in the standard way, which is documented in “Configuring NIS+ Clients” in *Solaris Naming Setup and Configuration Guide*
`/etc/inet/hosts`	You must set up the `/etc/inet/hosts` file for a DHCP client system that is to use `/etc/inet/hosts` for its name service. The DHCP client system’s host name is added to its own `/etc/inet/hosts` file by the DHCP tools. However, you must add the host name manually to the `/etc/inet/hosts` files of other systems in the network. If the DHCP server system uses `/etc/inet/hosts` for name resolution, you must also add the client’s host name manually on the system.

TABLE 1–4 Name Service Client Setup Information for DHCP Client Systems *(Continued)*

Name Service	Client Setup Notes
DNS	If the DHCP client system receives the DNS domain name through DHCP, the client system's `/etc/resolv.conf` file is configured automatically. To actually use DNS on systems that use `/etc/inet/hosts` files, you must modify the `/etc/nsswitch.conf` file to add `dns` to the `hosts` line, as shown in "Default nsswitch.files File" in *Solaris Naming Setup and Configuration Guide* If the client system uses NIS or NIS+ for local name resolution, you should be aware of the following: ■ NIS – If the NIS server allows DNS forwarding (which it does by default), the NIS client system can also use DNS. No further DNS client setup is needed in this case. If the NIS server does not allow DNS forwarding, the client system can use DNS by becoming a DNS client as described in "Setting Up DNS Clients" in *Solaris Naming Setup and Configuration Guide*. Note that if the client receives the DNS domain name from the DHCP server, the `/etc/resolv.conf` file needed for a DNS client is configured automatically, so you need only be concerned with the `nsswitch.conf` file. ■ NIS+ – The NIS+ client system can be configured to also use DNS if you edit the `nsswitch.conf`file as described in "Modifying the /etc/nsswitch.conf File" in *Solaris Naming Setup and Configuration Guide*.

Client Host Name Registration

If you let the DHCP server generate host names for the IP addresses you place in the DHCP service, the DHCP server can register those host names in NIS+, `/etc/inet/hosts`, or DNS name services. Host name registration cannot be done in NIS because NIS does not provide a protocol to allow programs to update and propagate NIS maps.

Note – The DHCP server can update DNS with generated host names only if the DNS server and DHCP server are running on the same system.

If a DHCP client provides its host name and the DNS server is configured to allow dynamic updates from the DHCP server, the DHCP server can update DNS on the client's behalf, even if the DNS and DHCP servers are running on different systems. See "Enabling Dynamic DNS Updates by DHCP Server" on page 82 for more information about enabling this feature.

The following table summarizes client host name registration for DHCP client systems with the various name services.

TABLE 1–5 Client Host Name Registration in Name Services

	Who Registers Host Name	
Name Service	**DHCP Generated Host Name**	**DHCP Client Supplied Host Name**
NIS	NIS Administrator	NIS Administrator
NIS+	DHCP tools	DHCP tools
`/etc/hosts`	DHCP tools	DHCP tools
DNS	DHCP tools, if the DNS server runs on the same system as the DHCP server. DNS Administrator, if the DNS sever runs on a different system.	DHCP server, if configured for dynamic DNS updates. DNS Administrator, if DHCP server is not so configured.

Note that Solaris DHCP clients can request particular host names in DHCP requests if configured to do so as described in "How to Enable a Solaris Client to Request Specific Host Name" on page 84. Please consult the documentation for non-Solaris clients to determine if the capability is supported.

DHCP Client Systems With Multiple Network Interfaces

The DHCP client daemon can manage several different interfaces on one system simultaneously, each with its own IP address and lease time. If more than one network interface is configured for DHCP, the client issues separate requests to configure them and maintains a separate set of network configuration options for each interface. However, although the parameters are stored separately, some of the parameters are global in nature, applying to the system as a whole, rather than to a particular network interface.

Options such as hostname, NIS domain name, and timezone are global parameters and should have the same values for each interface, but these values may differ due to errors in the information entered by the DHCP administrator. To ensure that there is only one answer to a query for a global parameter, only the parameters for the primary network interface are requested. You can insert the word `primary` in the `/etc/dhcp.`*interface* file for the interface you want to be treated as the primary interface.

CHAPTER 2

Planning for DHCP Service

You can use DHCP services in a network you are creating or in a network that exists. If you are setting up a network, see "IP Address Management Topics" in *System Administration Guide, Volume 3* before you attempt to set up DHCP services. If the network exists, continue in this chapter.

This chapter describes what you need to do before you set up DHCP service on your network. The information is intended for use with DHCP Manager, although you can also use the command-line utility `dhcpconfig` to set up DHCP service.

This chapter contains the following information:

Preparing Your Network for DHCP

Before you set up your network to use DHCP, you must first collect information and make decisions about how you will configure the server(s). First:

- Map out your network topology to determine which servers are the best candidates for DHCP servers, and how many servers you will need.
- Update your system files and `netmasks` table to reflect network topology accurately. If your DHCP server is to support clients on remote networks, you must also be sure the `netmasks` table entries for those networks are up to date. (See the `netmasks`(4) man page for more information.
- Choose the data storage method you want to use: text files, binary files, or NIS+.

- Define a lease policy.
- Determine how router information should be obtained by clients.

Mapping Your Network Topology

If you have not already done so, you should map the physical structure or layout of your network. Indicate the location of routers and clients, and the location of servers that provide network services. This map of your network topology can help you determine which server to use for DHCP services, and what configuration information the DHCP server can provide to clients.

See "Planning Your TCP/IP Network" in *System Administration Guide, Volume 3* for more information about planning your network.

The DHCP configuration process can look up some network information from the server's system and network files. "Updating System Files and Netmask Tables" on page 41 discusses these files. However, you might want to give clients other service information, which you must enter into the server's databases. As you examine your network topology, record the IP addresses of any servers you want your clients to know about. The following are some examples of network services you may have on your network that the DHCP configuration does not discover:

- Time server
- Log server
- Print server
- Install server
- Boot server
- Swap server
- X Window font server
- TFTP server

Network Topology to Avoid

DHCP does not work well in network environments where more than one IP network shares the same network hardware media, either through the use of multiple network hardware interfaces or multiple logical interfaces. When multiple IP networks run across the same physical LAN, a DHCP client's request arrives on all network hardware interfaces. This makes the client appear to be attached to all of the IP networks simultaneously.

DHCP must be able to determine the address of a client's network in order to assign an appropriate IP address to the client. If more than one network is present on the hardware media, the server cannot determine the client's network and cannot assign an IP address.

You can use DHCP on one of the networks, but not more than one. If this does not suit your needs, you must reconfigure the networks. Suggestions for reconfiguration include:

- Use variable length subnet masks (VLSM) to make better use of the IP address space you have, so you do not need to run multiple LANs on the same physical network. See RFC-1519 for more information on VLSM and Classless Inter-Domain Routing (CDIR).
- Configure the ports on your switches to assign devices to different physical LANs. This preserves the mapping of one LAN to one IP network required for Solaris DHCP. See the documentation for the switch for information about port configuration.

Determining the Number of DHCP Servers

The data store option you choose has a direct effect on the number of servers you must have to support your DHCP clients. The following table shows the maximum number of DHCP/BOOTP clients that can be supported by one DHCP server for each data store.

TABLE 2–1 Estimated Maximum Number of Clients

Data Store	Maximum Number of Clients
Text files	10,000
NIS+	40,000
Binary files	100,000

This maximum number is a general guideline, not an absolute number. A DHCP server's client capacity depends greatly on the number of transactions it must process per second. Lease times and usage patterns have a large effect on the number of clients that a server can support. For example, if leases are set to 12 hours and users turn their systems off at night and on at the same time the next morning, the server must handle transaction peaks each morning as many clients request leases simultaneously. The DHCP server can support fewer clients in such an environment compared to an environment with longer leases, or an environment that consists of constantly connected devices such as cable modems.

The section "Choosing the Data Store" on page 44 compares data store options.

Updating System Files and Netmask Tables

During the configuration process, DHCP Manager or the `dhcpconfig` utility scans various system files on your server for information it can use to configure the server.

You must be sure the information in the system files is current before you run DHCP Manager or dhcpconfig to configure your server. If you notice errors after you configure the server, use DHCP Manager or dhtadm to modify the macros on the server.

The following table lists some of the information gathered during DHCP server configuration, and the sources for the information. Be sure this information is set correctly on the server before you configure DHCP on it. If you make changes to the system files after you configure the server, you should reconfigure the service to pick up the changes.

TABLE 2–2 Information for DHCP Configuration

Information	Source	Comments
Time zone	System date, time zone settings	The date and time zone are initially set during the Solaris installation. You can change the date by using the date command and change the time zone by editing the /etc/TIMEZONE file, which sets the TZ variable.
DNS parameters	/etc/resolv.conf	The DHCP server uses the /etc/resolv.conf file to look up DNS parameters such as DNS domain name and DNS server addresses. See “Setting Up DNS Clients” in *Solaris Naming Setup and Configuration Guide* for more information about resolv.conf.
NIS or NIS+ parameters	System domain name, nsswitch.conf, NIS, NIS+	The DHCP server uses the domainname command to obtain the domain name of the server system, and the nsswitch.conf file to determine where to look for domain-based information. If the server system is a NIS or NIS+ client, the DHCP server queries NIS or NIS+ services to get NIS/NIS+ server IP addresses.
Default router	System routing tables, user prompt	The DHCP server searches the network routing tables to find the default router for clients attached to the local network. For clients not on the same network, the DHCP server must prompt the administrator for the information.

TABLE 2–2 Information for DHCP Configuration *(Continued)*

Information	Source	Comments
Subnet mask	Network interface, `netmasks` table	The DHCP server looks to its own network interfaces to determine the netmask and broadcast address for local clients. If the request had been forwarded by a relay agent, the server looks up the subnet mask in the `netmasks` table on the relay agent's network.
Broadcast address	Network interface, `netmasks` table	For the local network, the DHCP server obtains the broadcast address by querying the network interface. For remote networks, the server uses the BOOTP relay agent's IP address and the remote network's netmask to calculate the broadcast address for the network.

Making Decisions for Server Configuration

This section discusses some of the decisions to make before you configure the first DHCP server on your network. The topics parallel the dialogs in the DHCP Manager's Configuration Wizard, but the information is also useful if you decide to use the `dhcpconfig` utility to configure the server.

Selecting a Server for DHCP

With your network topology in mind, you can use the following guidelines to select a host on which to set up a DHCP server.

The server must:

- Run the Solaris 2.6, Solaris 7, or Solaris 8 operating environment. You must install the Solaris 8 7/01 operating environment if you need to support a large number of clients.
- Be accessible to all the networks that have clients that will use DHCP, either directly on the network or through a BOOTP relay agent.
- Be configured to use routing.
- Have a correctly configured `netmasks` table that reflects your network topology.

Choosing the Data Store

You can choose to store the DHCP data in text files, binary files, or the NIS+ directory service. The following table summarizes the features of each type of data store, and recommends the environment to which each is best suited.

TABLE 2–3 Comparison of Data Stores

Data Store Type	Performance	Maintenance	Sharing	Recommended Environment
Binary files	High performance, high capacity.	Low-maintenance, no database servers required. Contents must be viewed with DHCP Manager or `dhtadm` and `pntadm`. Regular file backups suggested.	Containers cannot be shared among DHCP servers.	Midsize to large environments with many networks with thousands of clients per network. Useful for small to medium ISPs.
NIS+	Moderate performance and capacity, dependent upon NIS+ service's performance and capacity	DHCP server system must be configured as a NIS+ client. Requires NIS+ service maintenance. Contents must be viewed with DHCP Manager or `dhtadm` and `pntadm`. Regular backups with `nisbackup` suggested.	DHCP data is distributed in NIS+, multiple servers can access the same containers.	Small to midsize environments with up to 5000 clients per network.
Text files	Moderate performance, low capacity.	Low-maintanence, no database servers required. ASCII format is readable without DHCP Manager, `dhtadm`, or `pntadm`. Regular file backups suggested.	Containers can be shared among DHCP servers if DHCP data is stored on one file system that is exported though an NFS mount point.	Small environments with a few hundred to a thousand clients per network, less than 10,000 total clients.

Traditional NIS (as opposed to NIS+) is not offered as a data store option because it does not support fast incremental updates. If your network uses NIS, you should use text files or binary files for your data store.

Setting a Lease Policy

A lease specifies the amount of time the DHCP server grants permission to a DHCP client to use a particular IP address. During the initial server configuration, you must specify a site-wide lease policy to indicate the lease time and whether clients can renew their leases. The server uses the information you supply to set option values in the default macros it creates during configuration. You can set different lease policies for specific clients or type of clients, by setting options in configuration macros you create.

The lease time is specified as a number of hours, days, or weeks for which the lease is valid. When a client is assigned an IP address (or renegotiates a lease on an IP address it is already assigned), the lease expiration date and time is calculated by adding the number of hours in the lease time to the timestamp on the client's DHCP acknowledgment. For example, if the timestamp of the DHCP acknowledgment is September 16, 2001 9:15 A.M., and the lease time is 24 hours, the lease expiration time is September 17, 2001 9:15 A.M. The lease expiration time is stored in the client's DHCP network record, viewable in DHCP Manager or with `pntadm`.

The lease time value should be relatively small, so that expired addresses are reclaimed quickly, but large enough so that if your DHCP service becomes unavailable, the clients continue to function until the system(s) that run the DHCP service can be repaired. A rule of thumb is to specify a time that is two times the predicted down time of a server. For example, if it generally takes four hours to obtain and replace a defective part and reboot the server, you should specify a lease time of eight hours.

The lease negotiation option determines whether or not a client can renegotiate its lease with the server before the lease expires. If lease negotiation is allowed, the client tracks the time that remains in its lease, and when half the lease time is used, the client requests the DHCP server to extend its lease to the original lease time. It is useful to disable lease negotiation in environments where there are more systems than IP addresses, so the time limit is enforced on the use of IP addresses. If there are enough IP addresses, you should enable lease negotiation so you do not force a client to take down its network interface and obtain a new lease, which can interrupt the client's TCP connections (such as NFS and telnet sessions). You can enable lease negotiation site-wide during the server configuration, and for particular clients or types of clients through the use of the `LeaseNeg` option in configuration macros.

Note – Systems that provide services on the network should retain their IP addresses, and should not be subject to short-term leases. You can use DHCP with such systems if you assign them reserved (manual) IP addresses, rather than IP addresses with permanent leases. This enables you to detect when the system's IP address is no longer in use.

Determining Routers for DHCP Clients

Clients use routers for any network communication beyond their local network, and they must know the IP addresses of these routers in order to use them.

When you configure a DHCP server, you must provide the IP address of a router the clients can use or, if you use DHCP Manager, you can specify that clients should find routers themselves with the router discovery protocol.

If clients on your network support router discovery, you should use router discovery protocol, even if there is only one router. Discovery enables a client to adapt easily to router changes in the network. For example, if a router fails and is replaced by one with a new address, clients can discover the new address automatically without having to obtain a new network configuration to get the new router address.

Making Decisions for IP Address Management

This section discusses the decisions you need to make when you configure IP addresses to be managed by DHCP. The topics parallel the dialogs of DHCP Manager's Address Wizard, but can also be used to make decisions if you use the `dhcpconfig` utility.

As part of the DHCP service setup, you determine several aspects of the IP addresses that the server is to manage. If your network needs more than one DHCP server, you must decide how to divide responsibility for the addresses so you can assign some to each server. Before you begin to configure your server you must decide on the following:

- Number or range of IP addresses that the server should manage
- Whether you want the server to automatically generate host names for clients and the prefix to use for generated host names
- What configuration macro to use to assign clients' network configuration
- Whether IP address leases are dynamic or permanent

Number and Ranges of IP Addresses

During the initial server configuration, DHCP Manager allows you to add one block, or range, of IP addresses under DHCP management by specifying the total number of addresses and the first address in the block. DHCP Manager adds a list of contiguous addresses from this information. If you have several blocks of noncontiguous addresses, you can add the others by running DHCP Manager's Address Wizard again, after the initial configuration.

Before you configure your IP addresses, know how many addresses are in the initial block of addresses you want to add and the IP address of the first address in the range.

Client Host Name Generation

The dynamic nature of DHCP means that an IP address is not permanently associated with the host name of the system that is using it. The DHCP management tools can generate a client name to associate with each IP address if you select this option. The client names consist of a prefix, or root name, plus a dash and a number assigned by the server. For example, if the root name is `charlie`, the client names will be `charlie-1`, `charlie-2`, `charlie-3`, and so on.

By default, generated client names begin with the name of the DHCP server that manages them. This is useful in environments that have more than one DHCP server because you can quickly see in the DHCP network tables which clients any given DHCP server manages. However, you can change the root name to any name you choose.

Before you configure your IP addresses, decide if you want the management tools to generate client names, and if so, what root name to use for the names.

The generated client names can be mapped to IP addresses in `/etc/inet/hosts`, DNS, or NIS+ if you specify this at configuration. See "Client Host Name Registration" on page 37 for more information.

Default Client Configuration Macros

In Solaris DHCP, a macro is a collection of network configuration options and their assigned values. The DHCP server uses macros to determine what network configuration information to send to a DHCP client.

When you configure the DHCP server, the management tools gather information from system files and directly from you through prompts or command-line options you specify. With this information, the management tools create the following macros:

- Network address macro, named to match the IP address of the client network. The macro contains information needed by any client that is part of the network, such as subnet mask, network broadcast address, default router or router discovery token, and NIS/NIS+ domain and server if the server uses NIS/NIS+. Other options applicable to your network might be included.
- Locale macro, named `Locale`. The macro contains the offset (in seconds) from Universal Time to specify the time zone.
- Server macro, named to match the server's host name. The macro contains information about the lease policy, time server, DNS domain, and DNS server, and possibly other information that the configuration program was able to obtain from system files. This macro includes the `Locale` macro.

The network address macro is automatically processed for all clients located on that network. The locale macro is included in the server macro, so it is processed when the server macro is processed.

When you configure IP addresses for the first network, you must select a client configuration macro to be used for all DHCP clients using the addresses you are configuring. By default, the server macro is selected because it is contains information needed by all clients that use this server. Clients receive the options contained in the network address macro before those in the server macro. See "Order of Macro Processing" on page 32 for more information about the order in which macros are processed.

Dynamic and Permanent Lease Type

The lease type determines if the lease policy applies to the addresses you are configuring. During initial server configuration, DHCP Manager allows you to select either dynamic or permanent leases for the addresses you are adding. If you configure with the `dhcpconfig` command, leases are dynamic.

When an address has a dynamic lease, the DHCP server can manage the address by allocating it to a client, extending the lease time, detecting when it is no longer in use, and reclaiming it. When an address has a permanent lease, the DHCP server can only allocate it to a client, after which the client owns the address until the client explicitly releases it. When the address is released, the server can assign it to another client. The address is not subject to the lease policy as long as it is configured with a permanent lease type.

When you configure a range of IP addresses, the lease type you select applies to all the addresses in the range. To get the most benefit from DHCP, you should use dynamic leases for most of the addresses. You can later modify individual addresses to make them permanent if necessary, but the total number of permanent leases should be kept to a minimum.

Reserved Addresses and Lease Type

Addresses can be reserved by manually assigning them to particular clients. A reserved address can have a permanent or dynamic lease associated with it. When a reserved address is assigned a permanent lease:

- The address can be allocated only to the client that is bound to the address
- The DHCP server cannot allocate the address to another client
- The address cannot be reclaimed by the DHCP server

If a reserved address is assigned a dynamic lease, the address can be allocated only to the client that is bound to the address, but the client must track lease time and negotiate for a lease extension as if the address were not reserved. This allows you to track when the client is using the address by looking at the network table.

You cannot create reserved addresses for all the IP addresses during the initial configuration because they are intended to be used sparingly for individual addresses.

Planning for Multiple DHCP Servers

If you want to configure more than one DHCP server to manage your IP addresses, consider the following guidelines:

- Divide the pool of IP addresses so that each server is responsible for a range of addresses and there is no overlap of responsibility.
- Choose NIS+ as your data store, if available. If not, choose text files and specify a shared directory for the absolute path to the data store. The binary files data store cannot be shared.
- Configure each server separately so that address ownership is allocated correctly and that server-based macros can be automatically created.
- Set up the servers to scan the options and macros in the `dhcptab` table at specified intervals so they each are using the latest information. You can do this by using DHCP Manager to schedule automatic reading of `dhcptab` as described in "Customizing DHCP Service Performance Options" on page 84.
- Be sure all clients can access all DHCP servers so that the servers can support one another. If a client has a valid IP address lease, and is either trying to verify its configuration or extend the lease, but the server that owns the client's address is not reachable, another server can respond to the client after the client has attempted to contact the primary server for 20 seconds. If a client requests a specific address, and the server that owns the address is not available, one of the other servers handles the request. The client receives a different address from the one requested.

Planning for Remote Network Configuration

After the initial configuration, you can place IP addresses in remote networks under DHCP management. However, because the system files are not local to the server, DHCP Manager and dhcpconfig cannot look up information to provide default values, so you must provide the information. Before you attempt to configure a remote network, be sure you know the following information:

- Remote network's IP address.
- Subnet mask of the remote network – This can be obtained from the netmasks table in the name service. If the network uses local files, look in /etc/netmasks on a system in the network. If the network uses NIS+, use the command niscat netmasks.org_dir. If the network uses NIS, use the command ypcat -k netmasks.byaddr. Make sure the netmasks table contains all the topology information for all the subnets you want to manage.
- Network type – Do the clients connect to the network through a local area network (LAN) connection or point-to-point protocol (PPP)?
- Routing – Can the clients use router discovery? If not, you must determine the IP address of a router they can use.
- NIS domain and NIS servers, if applicable.
- NIS+ domain and NIS+ servers, if applicable.

See "Adding, Modifying, and Removing DHCP Networks" on page 87 for the procedure for adding DHCP networks.

Selecting the Tool for Configuring DHCP

After you have gathered information and made decisions as outlined in the previous sections, you are ready to configure a DHCP server. You can use the graphical DHCP Manager or the command-line utility dhcpconfig to configure a server. DHCP Manager lets you select options and enter data that is then used to create the dhcptab and network tables used by the DHCP server. The dhcpconfig utility supports an interactive mode that prompts you for information, but relies on system and network files for additional data used to create the dhcptab and network tables. The noninteractive mode of dhcpconfig requires you to use command-line options to specify data. Note that the interactive version of dhcpconfig is scheduled for removal in a future Solaris release.

DHCP Manager Features

DHCP Manager, a Java-based graphical tool, provides a DHCP Configuration Wizard, which starts automatically the first time you run DHCP Manager on a system that is not configured as a DHCP server. The DHCP Configuration Wizard provides a series of dialog boxes that prompt you for the essential information required to configure a server: data store format, lease policy, DNS/NIS/NIS+ servers and domains, and router addresses. Some of the information is obtained by the wizard from system files, and you only need to confirm that the information is correct, or correct it if necessary.

When you progress through the dialog boxes and approve the information, and the DHCP server daemon starts on the server system, you are prompted to start the Add Addresses Wizard to configure IP addresses for the network. Only the server's network is configured for DHCP initially, and other server options are given default values. You can run DHCP Manager again after the initial configuration is complete to add networks and modify other server options.

`dhcpconfig` Features

In interactive mode, the `dhcpconfig` utility prompts you for information and then adds macros to the `dhcptab` and creates DHCP network tables. It prompts you for server startup options such as the interval for reading the `dhcptab`, the timeout value for DHCP service offers, and so on. It obtains other information from the system files discussed in "Updating System Files and Netmask Tables" on page 41. You cannot view the information it obtains from system files, so it is important that the system files be updated before you run `dhcpconfig` in interactive mode.

Note – The interactive mode is scheduled to be removed in a future Solaris release. DHCP Manager is the recommended tool for interactive use.

In noninteractive mode, the `dhcpconfig` command supports a list of options that allow you to configure and unconfigure a DHCP server, as well as convert to a new data store and import/export data to and from other DHCP servers. The command can be used in scripts. Please see the `dhcpconfig` man page for more information.

Comparison of DHCP Manager and `dhcpconfig`

The following table summarizes the differences between the two server configuration tools.

TABLE 2–4 Comparison of DHCP Manager and the dhcpconfig Command

Feature	DHCP Manager	dhcpconfig Interactive	dhcpconfig With Options
Network information gathered from system.	Allows you to view the information gathered from system files, and change it if needed.	You cannot see what information dhcpconfig is gathering. You must look at the dhcptab and network tables after they are created.	You specify the network information with command-line options.
Configuration experience for user.	Speeds the configuration process by omitting prompts for nonessential server options by using default values for them. Allows you to change nonessential options after initial configuration.	Prompts for all server options during configuration process. To change the options later, you must use dhtadm and pntadm commands.	Fastest configuration process, but user must specify values for many options.

The next chapter includes procedures you can use to configure your server with both DHCP Manager and the dhcpconfig utility.

CHAPTER 3

Configuring DHCP Service

When you configure DHCP service on your network, you configure and start the first DHCP server. Other servers can be added later, and may access the same data from a shared location if the data store supports shared data. This chapter includes procedures to enable you to configure the DHCP server and place networks and their associated IP addresses under DHCP management. It also explains how to unconfigure a server.

This chapter also provides instructions for procedures that use both DHCP Manager and the `dhcpconfig` utility in separate sections. This chapter contains the following information:

- "Configuring and Unconfiguring a DHCP Server Using DHCP Manager" on page 53
- "Configuring and Unconfiguring a DHCP Server Using `dhcpconfig` Commands" on page 59
- "Configuring and Unconfiguring a DHCP Server Using Interactive `dhcpconfig`" on page 61
- "Configuring and Unconfiguring a Solaris DHCP Client" on page 68

Configuring and Unconfiguring a DHCP Server Using DHCP Manager

This section includes procedures to help you configure and unconfigure a DHCP server with DHCP Manager. Note that you must be running an X Window system such as CDE to use DHCP Manager.

When you run DHCP Manager on a server not configured for DHCP, the following screen is displayed to allow you to specify whether you want to configure a DHCP server or a BOOTP relay agent.

FIGURE 3–1 Choose Server Configuration Dialog Box

Configuring DHCP Servers

When you configure a DHCP server, DHCP Manager starts the DHCP Configuration Wizard, which prompts you for information needed to configure the server. The initial screen of the wizard is shown in the following figure.

FIGURE 3–2 DHCP Configuration Wizard’s Initial Screen

When you finish answering the wizard prompts, DHCP Manager creates the items listed in the following table.

TABLE 3–1 Items Created During DHCP Server Configuration

Item	Description	Contents
Service configuration file, `/etc/inet/dhcpsvc.conf`	Records keywords and values for server configuration options.	Data store type and location, options used with `in.dhcpd` to start the DHCP daemon when system boots.
`dhcptab` table	DHCP Manager creates a `dhcptab` table if it does not already exist.	Macros and options with assigned values.
`Locale` macro, optional	Contains the local time zone’s offset in seconds from Universal Time (UTC).	`UTCoffst` option

TABLE 3–1 Items Created During DHCP Server Configuration *(Continued)*

Item	Description	Contents
Server macro, named to match server's node name	Contains options whose values were determined by input from the administrator who configured the DHCP server. Options apply to all clients that use addresses owned by the server.	The `Locale` macro, plus the following options: ■ `Timeserv`, set to point to the server's primary IP address ■ `LeaseTim`, and `LeaseNeg` if you selected negotiable leases ■ `DNSdmain` and `DNSserv`, if DNS is configured ■ `Hostname`, which *must not* be assigned a value. The presence of this option indicates that the hostname must be obtained from the name service.
Network address macro, whose name is the same as the network address of client's network	Contains options whose values were determined by input from the administrator who configured the DHCP server. Options apply to all clients that reside on the network specified by the macro name.	The following options: ■ `Subnet` ■ `Router` or `RDiscvyF` ■ `Broadcst`, if the network is a LAN ■ `MTU` ■ `NISdmain` and `NISservs`, if NIS is configured ■ `NIS+dom` and `NIS+serv`, if NIS+ is configured
Network table for the network.	Empty table is created until you create IP addresses for the network.	None, until you add IP addresses.

▼ How to Configure a DHCP Server (DHCP Manager)

1. **Select the system you want to use as a DHCP server.**

   Use the guidelines in "Making Decisions for Server Configuration" on page 43.

2. **Make decisions about your data store, lease policy, and router information.**

   Use the guidelines in "Making Decisions for Server Configuration" on page 43.

3. **Become superuser on the server system.**

4. **Type the following command:**

   ```
   #/usr/sadm/admin/bin/dhcpmgr &
   ```

5. **Choose the option Configure as DHCP Server.**

This starts the DHCP Configuration Wizard, which helps you configure your server.

6. **Select options or type requested information based on the decisions you made in the planning phase.**

   If you have difficulty, click Help in the wizard window to open your web browser and display help for the DHCP Configuration Wizard.

7. **Click Finish to complete the server configuration when you have finished entering the requested information.**

8. **At the Start Address Wizard window, click Yes to configure addresses for the server.**

   The Address Wizard enables you to specify which addresses to place under the control of DHCP.

9. **Answer the prompts based on decisions made in the planning phase.**

   See "Making Decisions for IP Address Management" on page 46 for more information. If you have difficulty, click Help in the wizard window to open your web browser and display help for the Add Addresses Wizard.

10. **Review your selections, and click Finish to add the addresses to the network table.**

    The network table is updated with records for each address in the range you specified.

You can add more networks to the DHCP server with the Network Wizard, as explained in "Adding DHCP Networks" on page 89.

Configuring BOOTP Relay Agents

When you configure a BOOTP relay agent, DHCP Manager takes the following actions:

- Prompts you for IP addresses of the DHCP server to which requests should be relayed.
- Edits `/etc/inet/dhcpsvc.conf`, to specify the options needed for BOOTP relay service.

The following figure shows the screen displayed when you choose to configure a BOOTP relay agent.

FIGURE 3–3 Configure BOOTP Relay Dialog Box

▼ How to Configure a BOOTP Relay Agent (DHCP Manager)

1. **Select the system you want to use as a BOOTP relay agent.**

   See "Selecting a Server for DHCP" on page 43.

2. **Become superuser on the server system.**

3. **Type the following command:**

   ```
   #/usr/sadm/admin/bin/dhcpmgr &
   ```

   If the system has not been configured as a DHCP server or BOOTP relay agent, the DHCP Configuration Wizard starts. If the system has already been configured as a DHCP server, you cannot configure it as a BOOTP relay agent unless you unconfigure the server first. See "Unconfiguring DHCP Servers and BOOTP Relay Agents" on page 57.

4. **Select Configure as BOOTP Relay.**

   The Configure BOOTP Relay dialog box opens.

5. **Type the IP address or host name of one or more DHCP servers that are configured to handle BOOTP or DHCP requests received by this BOOTP relay agent, and click Add.**

6. **Click OK to exit the dialog box.**

   Notice that the DHCP Manager offers only the File menu to exit the application and the Service menu to manage the server. Other menu options are disabled because they are useful only on a DHCP server.

Unconfiguring DHCP Servers and BOOTP Relay Agents

When you unconfigure a DHCP server or BOOTP relay agent, DHCP Manager takes the following actions:

- Stops the DHCP daemon (`in.dhpcd`) process
- Removes the `/etc/inet/dhcpsvc.conf` file, which records information about daemon startup and the data store location

The following figure shows the screen that is displayed when you choose to unconfigure a DHCP server.

FIGURE 3–4 Unconfigure Service Dialog Box

DHCP Data on an Unconfigured Server

When you unconfigure a DHCP server you must decide what to do with the `dhcptab` table and the DHCP network tables. If the data is shared among servers, you should not remove the `dhcptab` and DHCP network tables because this would render DHCP unusable across your network. Data can be shared through NIS+ or on exported local file systems. The file `/etc/inet/dhcpsvc.conf` records the data store used and its location.

You can unconfigure a DHCP server but leave the data intact by not selecting any of the options to remove data. If you unconfigure the server and leave the data intact, you disable the DHCP server.

If you want another DHCP server to take ownership of the IP addresses belonging to the server you are unconfiguring, you must move the DHCP data to the other DHCP server before you unconfigure the current server. See "Moving Configuration Data Between DHCP Servers" on page 136 for more information.

If you are certain you want to remove the data, you can select an option to remove the `dhcptab` and network tables. If you had generated client names for the DHCP addresses, you can also elect to remove those entries from the hosts table (whether in DNS, `/etc/inet/hosts`, or NIS+).

Before you unconfigure a BOOTP relay agent, be sure that no clients rely on this agent to forward requests to a DHCP server.

▼ How to Unconfigure a DHCP Server or BOOTP Relay Agent (DHCP Manager)

1. **Become superuser.**
2. **Type the following command:**

   ```
   #/usr/sadm/admin/bin/dhcpmgr &
   ```

3. **From the Service menu, choose Unconfigure.**

   The Unconfigure Service dialog box is displayed. If the server is a BOOTP relay agent, the dialog box enables you to confirm your intention to unconfigure the relay agent. If the server is a DHCP server, you must decide what to do with the

DHCP data and make selections in the dialog box. See Figure 3–4.

4. **(Optional) Select options to remove data.**

   If the server uses shared data (through NIS+ or files shared through NFS), do not select any options to remove the data. If the server does not use shared data, select one or both options to remove the data.

   See “DHCP Data on an Unconfigured Server” on page 58 for more information about removing data.

5. **Click OK to confirm.**

Configuring and Unconfiguring a DHCP Server Using dhcpconfig Commands

This section includes procedures to help you configure and unconfigure a DHCP server or BOOTP relay agent by using dhcpconfig with command-line options.

▼ How to Configure a DHCP Server (dhcpconfig -D)

1. **Select the system you want to use as a DHCP server.**

   Use the guidelines in “Making Decisions for Server Configuration” on page 43.

2. **Make decisions about your data store, lease policy, and router information.**

   Use the guidelines in “Making Decisions for Server Configuration” on page 43.

3. **Become superuser or a user assigned to the DHCP Management profile.**

4. **Type a command of the following format:**

   ```
   #/usr/sbin/dhcpconfig -D -r datastore -p location
   ```

   datastore is one of SUNWfiles, SUNWbinfiles, or SUNWnisplus.

   location is the data-store-dependent location where you want to store the DHCP data. For SUNWfiles and SUNWbinfiles, this must be a UNIX absolute path name. For SUNWnisplus, this must be a fully specified NIS+ directory.

   The dhcpconfig utility uses the server machine’s system and network files to determine values used to configure the DHCP server. See the dhcpconfig man page for information about additional options to the dhcpconfig command that enable you to override the default values.

5. **Add one or more networks to the DHCP service.**

See “How to Add a DHCP Network (dhcpconfig)” on page 90 for the procedure to add a network.

▼ How to Configure a BOOTP Relay Agent (dhcpconfig -R)

1. **Select the system you want to use as a BOOTP relay agent.**

   Use the guidelines in “Making Decisions for Server Configuration” on page 43.

2. **Become superuser or a user assigned to the DHCP Management profile.**

3. **Type the following command:**

   ```
   # /usr/sbin/dhcpconfig -R addresses
   ```

   addresses are the comma-separated IP addresses of DHCP servers to which you want requests to be forwarded.

▼ How to Unconfigure a DHCP Server or BOOTP Relay Agent (dhcpconfig -U)

1. **Become superuser or a user assigned to the DHCP Management profile.**

2. **Type the following on the system that acts as DHCP server or BOOTP relay agent:**

   ```
   # /usr/sbin/dhcpconfig -U
   ```

   If the server does not use shared data (through NIS+ or text files shared through NFS), you can also use the -x option to remove the dhcptab and network tables. If the server uses shared data, do not use the -x option. The -h option can be used to remove host names from the host table. See the dhcpconfig man page for more information about dhcpconfig options.

   See “DHCP Data on an Unconfigured Server” on page 58 for more information about removing data.

Configuring and Unconfiguring a DHCP Server Using Interactive `dhcpconfig`

This section includes procedures to help you configure and unconfigure a DHCP server or BOOTP relay agent by using `dhcpconfig` interactively without command-line options. See “How to Configure a DHCP Server (`dhcpconfig -D`)” on page 59 if you want to use `dhcpconfig` noninteractively.

When you start `dhcpconfig` without command-line options, the DHCP Configuration menu is displayed, as shown in the following figure.

```
***         DHCP Configuration              ***

Would you like to:

        1) Configure DHCP Service

        2) Configure BOOTP Relay Agent

        3) Unconfigure DHCP or Relay Service

        4) Exit

Choice:
```

▼ How to Configure a DHCP Server (Interactive `dhcpconfig`)

1. **Select the system you want to use as a DHCP server.**

   Use the guidelines in “Making Decisions for Server Configuration” on page 43.

2. **Make decisions about your data store, lease policy, and router information.**

   Use the guidelines in “Making Decisions for Server Configuration” on page 43.

3. **Become superuser or a user assigned to the DHCP Management profile.**

4. **Type the following command:**

   ```
   #/usr/sbin/dhcpconfig
   ```

   The text-based DHCP Configuration menu is displayed as shown in Figure 3–5.

5. **Type `1` and press Return to select Configure DHCP Service.**

6. **Answer the prompts as described in the following paragraphs.**

Use the decisions you made after you read Chapter 2. Note that the default value for each prompt is displayed in square brackets. If you want to use a default value, press Return at the prompt.

```
###     DHCP Service Configuration      ###
###     Configure DHCP Database Type and Location      ###

Enter data store (SUNWbinfiles, SUNWfiles or SUNWnisplus) [SUNWnisplus]:
```

Type the name of the data store you have decided to use: **SUNWbinfiles**, **SUNWfiles**, or **SUNWnisplus**.

See the guidelines in "Choosing the Data Store" on page 44 if you need more information about the data store.

```
Enter full path to data location [default-for-data-store]:
```

Type the path to the directory or NIS+ domain that you want to use for the data store. The default location if you selected `SUNWbinfiles` or `SUNWfiles` for the data store is `/var/dhcp`. If you selected NIS+, the default listed is the NIS+ domain that the server is already using, such as `yourcompany.com`.

```
Enter location for hosts data (none, files, dns, or nisplus) [none]:
```

Type the name service that you want DHCP to use to register the host names of DHCP clients. See "Client Host Name Registration" on page 37 for more information. If you select `none`, you must add host names manually to a name service.

```
Enter default DHCP lease policy (in days) [3]:
```

Type the number of days for the lease time. The default is three days. See "Setting a Lease Policy" on page 45 for more information.

```
Do you want to allow clients to renegotiate their leases? ([Y]/N):
```

The default is Y to allow lease negotiation. See "Setting a Lease Policy" on page 45 for more information about lease negotiation. If you type **N**, clients must give up their IP addresses when the lease expires, and then obtain a new lease and IP address.

```
Would you like to specify nondefault daemon options (Y/[N]):
```

You can successfully configure the server without specifying nondefault daemon options if you type **N** at this prompt.

However, if you type **Y** here, the following prompts are displayed.

```
Do you want to enable transaction logging? (Y/[N]):Y
```

Type **Y** if you want to enable transaction logging. See "Changing DHCP Logging Options" on page 78 for information about transaction logging. The following prompt appears only if you enable transaction logging.

```
Which syslog local facility [0-7] do you wish to log to? [0]:
```

See "Changing DHCP Logging Options" on page 78 for information about the local facility for transaction logging.

```
Would you like to specify nondefault server options (Y/[N]):Y
```

You can successfully configure the server without specifying nondefault server options if you type **N** at this prompt.

However, if you type **Y** here, the following prompts are displayed.

```
How long (in seconds) should the DHCP server keep outstanding OFFERs? [10]:
```

Type the number of seconds the server should cache an IP address offer to a client. The default is 10 seconds, which is adequate for most networks. You can increase this time to compensate for slow network performance.

```
How often (in minutes) should the DHCP server rescan
the dhcptab? [Never]:
```

By default, the DHCP server reads the dhcptab only at startup or if signalled by DHCP Manager to read it. DHCP Manager enables you to update the server by reloading the dhcptab after you make a change to the configuration data, so scheduled rescans are not necessary if you use DHCP Manager. Generally, you should use a rescan interval only under the following circumstances:

- The data store is NIS+ and you have more than one DHCP server on your network. Scheduled rescans guarantee that all servers have the latest information.
- You use dhtadm instead of DHCP Manager to make configuration changes. The dhtadm utility does not offer you the option of forcing a rescan of dhcptab after you make a change.

If you decide to use the automatic rescan for dhcptab, type the interval in minutes that the server should wait before it reloads the client configuration information in the dhcptab file.

```
Do you want to enable BOOTP compatibility mode? (Y/[N]):
```

The default is to not enable BOOTP compatibility. See "Supporting BOOTP Clients with DHCP Service" on page 93 if you want to enable BOOTP compatibility.

After you finish entering information about nondefault daemon and server options, the following prompt is displayed:

```
Enable DHCP/BOOTP support of networks you select? ([Y]/N):
```

At this point, you can configure the networks that should use DHCP. Refer to the decisions you made after you read "Making Decisions for IP Address Management" on page 46. If you are not ready to configure IP addresses, type **N** to return to the initial menu. Note that DHCP is not usable until you enable DHCP/BOOTP support of at least one network.

If you are ready to configure IP addresses, type **Y** and continue to Step 4.

▼ How to Configure a BOOTP Relay Agent (Interactive dhcpconfig)

1. **Become superuser on the system you want to configure.**

2. **Type the following command:**

```
# /usr/sbin/dhcpconfig
```

The text-based DHCP Configuration menu is displayed.

3. **Type 2 and press Return to select Configure BOOTP Relay Agent.**

4. **Answer the prompts as follows:**

```
###     BOOTP Relay Agent Configuration ###

Enter destination BOOTP/DHCP servers. Type '.' when finished.
IP address or Hostname:
```

Type one IP address or host name for a BOOTP or DHCP server to which requests should be forwarded and press Return. The prompt appears again to allow you to type more addresses or host names. Type a period and press Return when you are finished.

```
###     Common daemon option setup      ###

Would you like to specify nondefault daemon options (Y/[N]):Y
```

You can successfully configure the server without specifying nondefault daemon options if you type **N** at this prompt.

However, if you type **Y** here, the following prompts are displayed.

```
Do you want to enable transaction logging? (Y/[N]):Y
```

Type **Y** if you want to enable transaction logging. See "Changing DHCP Logging Options" on page 78 for information about transaction logging. The following prompt appears only if you enable transaction logging:

```
Which syslog local facility [0-7] do you wish to log to? [0]:
```

See "Changing DHCP Logging Options" on page 78 for information about the local facility for transaction logging.

The DHCP Configuration menu is redisplayed.

5. **Type 4 to exit dhcpconfig.**

Configuring Networks Using Interactive dhcpconfig

This section describes the procedures for placing a network under DHCP management with the dhcpconfig utility. Each procedure assumes that you have completed the server configuration and you now want to add networks to the DHCP service.

▼ How to Configure the Local Network (Interactive `dhcpconfig`)

1. **Become superuser on the DHCP server system.**
2. **Type the following command:**

   ```
   # /usr/sbin/dhcpconfig
   ```

   The text-based DHCP Configuration menu is displayed.
3. **Type `1` and press Return to select Configure DHCP Service.**
4. **Answer the following prompts as shown to configure the local network.**

   ```
   Enable DHCP/BOOTP support of networks you select? ([Y]/N):Y
   Configure BOOTP/DHCP on local LAN network: 102.31.0.0? ([Y]/N):Y
   ```
5. **Answer the following prompts about client host name generation.**

```
Do you want hostnames generated and inserted in the files hosts table? (Y/[N]):
```

   The server can create host names and associate one with each IP address. See“Client Host Name Generation” on page 47 for more information.

   If you type **`Y`**, answer the next prompt. If you type **`N`**, skip to step Step 6.

   ```
   What rootname do you want to use for generated names? [yourserver-]:
   ```

   The default prefix, or rootname, for generated client names is the name of the DHCP server. You can accept this or change the name to anything you like.

   ```
   Is Rootname name_you_typed- correct? ([Y]/N):Y
   ```

   If you made an error, type **`N`** here to be prompted again for the rootname.

   ```
   What base number do you want to start with? [1]:
   ```

   The base number indicates the first number appended to the rootname used to generate client names. For example, if you accept the default rootname and base number, the client names would be `yourserver-1`, `yourserver-2`, and so on.
6. **Answer the following prompts about the IP addresses in this network that you want to be placed under DHCP management.**

   ```
   Enter starting IP address [102.21.0.0]:
   ```

   The server must generate a range of IP addresses that it is to manage. Type the first address in the range that you want to be placed under DHCP management. See “Number and Ranges of IP Addresses” on page 47 for more information.

   ```
   Enter the number of clients you want to add (x < 65535):
   ```

   The number of clients is the number of IP addresses you want to place under DHCP management. The `dhcpconfig` program uses this information and the base number to add a contiguous block of IP addresses to be managed by DHCP.

   ```
   The dhcp network table: 102.21.0.0 already exists.
   Do you want to add entries to it? ([Y]/N):
   ```

You see this prompt if you are adding a block of addresses in a network for which you have already configured addresses. Type **Y** to modify the network table and add the addresses.

```
Would you like to configure BOOTP/DHCP service on remote networks? ([Y]/N):
```

If you are finished adding networks, type **N**.

If you want to place IP addresses on other networks under DHCP management, type **Y** at this prompt and continue with Step 4.

▼ How to Configure Remote Networks (Interactive `dhcpconfig`)

1. **Become superuser on the DHCP server system.**
2. **Type the following command:**

   ```
   # /usr/sbin/dhcpconfig
   ```

   The text-based DHCP Configuration menu is displayed.
3. **Type `1` and press Return to select Configure DHCP Service.**
4. **Answer the following prompts as shown to configure a remote network.**

```
Enable DHCP/BOOTP support of networks you select? ([Y]/N):Y
Configure BOOTP/DHCP on local LAN network: 102.21.0.0? ([Y]/N):N
Would you like to configure BOOTP/DHCP service on remote networks? ([Y]/N):Y
Enter Network Address of remote network, or <RETURN> if finished:
```

Type the IP address of the network you want to configure for DHCP. Remember that the network address uses 0 for the host portion of the IP address.

```
Do clients access this remote network via LAN or PPP connection? ([L]/P):
```

Indicate whether the network is a local area network (LAN) or a point-to-point protocol network (PPP) by typing **L** or **P**.

```
Do you want hostnames generated and inserted in the files hosts table? (Y/[N]):
```

The server can create host names for each IP address and create entries in the `/etc/inet/hosts` file or NIS+ hosts table. See "Client Host Name Generation" on page 47.

```
Enter Router (From client's perspective), or <RETURN> if finished.
IP address:
```

Type the IP address of the router(s) the clients on this network should use. Note that you cannot specify that clients should use router discovery here.

```
Enter starting IP address [102.21.0.0]
```

Type the first IP address in the range of addresses you want to place under DHCP management. The default value is the network address.

```
Enter the number of clients you want to add (x < 65535):
```

Type the number of IP addresses you want to place under DHCP management. The dhcpconfig utility uses this number and the starting IP address you entered previously to determine a block of IP addresses to place under DHCP control. The number you enter must be less than the value shown in the prompt, which is generated based on the netmask. In this example, the number must be less than 65535.

```
dhcptab macro "102.21.0.0" already exists.
Do you want to merge initialization data with the existing
macro? ([Y]/N):
```

If you have already configured this network, this message is displayed. You should merge the data into the existing macro only if the information you provided applies to all clients on the network you are adding.

```
Disable (ping) verification of 102.21.0.0 address(es)? (Y/[N]):
```

The dhcpconfig utility pings the addresses you want to add to be sure they are not being used, and skips any addresses that are in use. If you type Y at this prompt, dhcpconfig does not ping the addresses.

```
Network: 102.21.0.0 complete.
Enter Network Address of remote network, or <RETURN> if finished:
```

If you want to configure another remote network, enter the network address and answer the prompts for the network. When you have no other remote networks to configure, press Return at this prompt.

Unconfiguring DHCP Servers and BOOTP Relay Agents With Interactive dhcpconfig

When you unconfigure a DHCP server, the server daemon stops and does not start automatically when the system reboots. The server configuration file is deleted as well. Before you unconfigure a DHCP server you must decide what to do with the DHCP data files: dhcptab and the DHCP network tables. If the data is shared among servers, you should not remove the dhcptab and DHCP network tables because this could render DHCP unusable across your network. Data can be shared through NIS+ or on exported local file systems. You can unconfigure a DHCP server and leave the data intact if you do not remove the tables when prompted to do so.

▼ How to Unconfigure DHCP Servers or BOOTP Relay Agents (Interactive dhcpconfig)

1. **Become superuser on the server system.**

2. **Type the following command:**

```
# /usr/sbin/dhcpconfig
```

The text-based DHCP Configuration menu is displayed.

3. **Type 3 and press Return to select Unconfigure DHCP or Relay Service.**

4. **Answer the prompts as follows:**

   ```
   Unconfigure will stop the DHCP service and remove /etc/inet/dhcpsvc.conf.
   Are you SURE you want to disable the DHCP service? ([Y]/N):
   ```

   Type **Y** to unconfigure the server.

   ```
   Are you SURE you want to remove the DHCP tables? (Y/[N]):
   ```

   Type **Y** only if you are certain that the DHCP data is not shared with other DHCP servers. If you type **N**, the server is disabled while the data remains intact.

Configuring and Unconfiguring a Solaris DHCP Client

When you install the Solaris operating environment from CD-ROM, you are prompted to use DHCP to configure network interfaces. If you select yes, the DHCP client software is enabled on your system during Solaris installation. You do not need to do anything else on the Solaris client to use DHCP.

If a client system is already running the Solaris operating environment and not using DHCP, you must unconfigure the system and issue some commands to set up the system to use DHCP when it boots.

If your client is not a Solaris client, consult the client documentation for configuration instructions.

▼ How to Configure a Solaris DHCP Client

This procedure is necessary only if DHCP was not enabled during Solaris installation.

1. **Become superuser on the client system.**

2. **If this system uses preconfiguration instead of interactive configuration, edit the sysidcfg file to add the dhcp subkey to the network_interface keyword.**

   For example, network_interface=le0 {dhcp}. See the sysidcfg(4) man page for more information.

3. **Unconfigure and shut down the system by typing the following command:**

   ```
   # sys-unconfig
   ```

See the sys-unconfig(1M) man page for more information about what configuration information is removed by this command.

4. **Reboot the system after it has completely shut down.**

   You are prompted for system configuration information by sysidtool programs when the system reboots. See the sysidtool(1M) man page for more information.

5. **When prompted to use DHCP to configure network interfaces, specify Yes.**

   If you preconfigured the system by using a sysidcfg file, insert the network_interface keyword, and specify dhcp as a dependent keyword. For example, network_interface=le0 {dhcp}.

▼ How to Unconfigure a Solaris DHCP Client

1. **Become superuser on the client system.**

2. **If you use a sysidcfg file to preconfigure the client, remove the dhcp subkey from the network_interface keyword.**

3. **Unconfigure and shut down the system by typing the following command:**

   ```
   # sys-unconfig
   ```

   See the sys-unconfig(1M) man page for more information about which configuration information is removed by this command.

4. **Reboot the system after it has completely shut down.**

   Because you unconfigured the system, you will be prompted for configuration information by sysidtool programs when the system reboots. See the sysidtool(1M) man page for more information.

5. **When prompted to use DHCP to configure network interfaces, specify No.**

   If you use sysidcfg to specify configuration, you will not be prompted.

CHAPTER **4**

Administering DHCP

This chapter describes tasks you might find useful when you administer the Solaris DHCP service. The chapter includes tasks for the server, BOOTP relay agent, and client. Each task includes a procedure to help you perform the task in DHCP Manager and a procedure for the equivalent task with DHCP command-line utilities. DHCP command-line utilities are more fully documented in man pages.

You should have already completed the initial configuration of your DHCP service and initial network before you use this chapter. Chapter 3 discusses DHCP configuration.

The chapter contains the following information:

- “DHCP Manager” on page 72
- “Setting Up User Access to DHCP Commands” on page 74
- “Starting and Stopping the DHCP Service” on page 75
- “Modifying DHCP Service Options” on page 77
- “Adding, Modifying, and Removing DHCP Networks” on page 87
- “Supporting BOOTP Clients with DHCP Service” on page 93
- “Working With IP Addresses in the DHCP Service” on page 96
- “Working With DHCP Macros” on page 107
- “Working With DHCP Options” on page 115
- “Supporting Solaris Network Booting and Installation with the DHCP Service” on page 122
- “Setting Up DHCP Clients as NIS+ Clients” on page 131
- “Converting to a New Data Store” on page 134
- “Moving Configuration Data Between DHCP Servers” on page 136

DHCP Manager

DHCP Manager is a graphical interface you can use to perform administration tasks on the DHCP service.

The DHCP Manager Window

The DHCP Manager window's appearance differs, depending on whether the server on which it is running was configured as a DHCP server or a BOOTP relay agent.

When the server is configured as a DHCP server, DHCP Manager uses a tab-based window, in which you select a tab for the type of information you want to work with. DHCP Manager features the following tabs:

- **Addresses** – Lists all networks and IP addresses placed under DHCP management. From the Addresses tab, you can add or delete networks and add or delete IP addresses individually or in blocks. You can also modify the properties of individual networks or IP addresses or make the same property modifications for a block of addresses simultaneously. When you start DHCP Manager, it opens on the Addresses tab.
- **Macros** – Lists all macros available in the DHCP configuration database (`dhcptab`) and the options contained within them. From the Macros tab, you can create or delete macros, and modify them by adding options and providing values for the options.
- **Options** – Lists all options that have been defined for this DHCP server. Options listed on this tab are not the standard ones defined in the DHCP protocol. The options are extensions to the standard options, and have a class of Extended, Vendor, or Site. Standard options cannot be changed in any way so they are not listed here.

The following figure shows the DHCP Manager window as it appears when you start it on a DHCP server.

FIGURE 4–1 DHCP Manager on a DHCP Server System

When the server is configured as a BOOTP relay agent, the DHCP Manager window does not show these tabs because the BOOTP relay agent does not need any of this information. You can only modify the BOOTP relay agent's properties and stop/start the DHCP daemon with DHCP Manager. The following figure shows the DHCP Manager window as it appears when you start it on a system configured as a BOOTP relay agent.

FIGURE 4–2 DHCP Manager on a BOOTP Relay Agent System

DHCP Manager Menus

DHCP Manager menus include:

- **File** – Exit DHCP Manager
- **Edit** – Perform management tasks upon networks, addresses, macros, and options
- **View** – Change the look of the tab currently selected
- **Service** – Manage the DHCP daemon and data store.
- **Help** – Open your web browser and display help for DHCP Manager

When DHCP Manager runs on a BOOTP relay agent, the Edit and View menus are disabled.

All DHCP service management activities are accomplished through the Edit and Service menus. You use the commands in the Edit menu to create, delete, and modify networks, addresses, macros, and options, depending on which tab is selected. When the Addresses tab is selected, the Edit menu also lists wizards, which are sets of dialogs that make it easy to create networks and multiple IP addresses. The Service menu lists commands that enable you to manage the DHCP daemon. You can start/stop, enable/disable, modify the server configuration, and unconfigure the server. The Service menu also lists commands that enable you to convert the data store and export and import data on the server.

Starting and Stopping DHCP Manager

You must run DHCP Manager on a DHCP server system as superuser, but you can display it remotely on another UNIX system using the X Window remote display feature.

▼ How to Start DHCP Manager

1. **(Optional) Become superuser on the DHCP server system.**

2. **If you are logged in to the DHCP server system remotely, you can display DHCP Manager on your local system as follows.**

   a. **Type the following on the local system:**

```
# xhost +server-name
```

b. **Type the following on the remote DHCP server system:**

```
# DISPLAY=local-hostname;export DISPLAY
```

3. **Type the following command:**

```
# /usr/sadm/admin/bin/dhcpmgr &
```

The DHCP Manager window opens, displaying the Addresses tab if the server is configured as a DHCP server, or no tabs if the server is configured as a BOOTP relay agent.

▼ How to Stop DHCP Manager

- **Choose Exit from the File menu.**

  The DHCP Manager window closes.

Setting Up User Access to DHCP Commands

To allow users other than root to execute dhcpconfig, dhtadm, and pntadm commands without first becoming superuser, you must set up role-based access control (RBAC) for those commands. RBAC enables you to more precisely define which users can perform which tasks on the system. See rbac(5), exec_attr(4), and user_attr(4) man pages for more information.

The following procedure explains how to assign a user the DHCP Management profile, which enables the user to execute the DHCP commands.

▼ How to Grant Users Access to DHCP Commands

1. **Become superuser on the DHCP server system.**

2. **Edit the file /etc/user_attr to add an entry of the following form for each user you want to be able to manage the DHCP service:**

```
username:::type=normal;profiles=DHCP Management
```

For example, for user ram, add the following entry:

```
ram:::type=normal;profiles=DHCP Management
```

Starting and Stopping the DHCP Service

The starting and stopping of the DHCP service encompasses several degrees of action you can take to affect the operation of the DHCP daemon. You must understand what it means to start/stop, enable/disable, and configure/unconfigure the DHCP service in order to select the correct procedure to obtain the result you want. The terms are explained below.

- **Start, stop, and restart commands** affect the daemon only at the current session. For example, if you stop the DHCP service, the daemon terminates but restarts when you reboot the system. DHCP data tables are not affected when you stop the service.
- **Enable and disable commands** affect the daemon for current and future sessions. If you disable the DHCP service, the currently running daemon terminates and does not start when you reboot the server. You must enable the DHCP daemon for the automatic start at system boot to occur. DHCP data tables are not affected. You can disable and enable the DHCP service only from DHCP Manager.
- **Unconfigure command** shuts down the daemon, prevents the daemon from starting on system reboot, and enables you to remove the DHCP data tables. Unconfiguration is described in Chapter 3.

Note – If a server has multiple network interfaces and you do not want to provide DHCP services on all the networks, see “Specifying Network Interfaces to Monitor for DHCP Service” on page 88.

This section provides the procedures to help you start and stop the DHCP service, and enable and disable it.

▼ How to Start and Stop the DHCP Service (DHCP Manager)

1. **Become superuser on the DHCP server system.**
2. **Start DHCP Manager.**

   See “How to Start DHCP Manager” on page 73 for the procedure.
3. **Select one of the following operations:**

   a. **Choose Start from the Service menu to start the DHCP service.**

   b. **Choose Stop from the Service menu to stop the DHCP service.**

The DHCP daemon stops until it is manually started again, or the system reboots.

c. **Choose Restart from the Service menu to stop the DHCP service and immediately restart it.**

▼ How to Start and Stop the DHCP Service (Command Line)

1. **Become superuser on the server system.**

2. **Choose one of the following operations:**

   a. **To start the DHCP service, type the following command:**

   ```
   # /etc/init.d/dhcp start
   ```

   The DHCP daemon starts, using the configuration parameters set in `/etc/inet/dhcpsvc.conf`.

   b. **To stop the DHCP service, type the following command:**

   ```
   # /etc/init.d/dhcp stop
   ```

   The DHCP daemon stops until it is manually started again, or the system reboots.

▼ How to Enable and Disable the DHCP Service (DHCP Manager)

1. **Start DHCP Manager.**

2. **Choose one of the following operations:**

   a. **Choose Enable from the Service menu to start the DHCP service immediately and configure it for automatic startup when the system boots.**

   b. **Choose Disable from the Service menu to stop the DHCP service immediately and prevent it from starting automatically when the system boots.**

Modifying DHCP Service Options

You can change values for some additional features of the DHCP service, some of which were not offered during the initial configuration with DHCP Manager. If you configured your server with `dhcpconfig`, you may have been prompted to select values for most of these options. You can use the Modify Service Options dialog box in DHCP Manager or specify options on the `in.dhcpd` command to change service options.

The following task map shows the tasks related to service options and the procedures to use:

TABLE 4–1 Modify DHCP Service Options Task Map

Tasks	Description	Where to Find Instructions
Change logging options	Enable or disable verbose logging, enable or disable logging of DHCP transactions, and select a `syslog` facility to use for logging DHCP transactions.	"How to Generate Verbose DHCP Log Messages (DHCP Manager)" on page 80 "How to Generate Verbose DHCP Log Messages (Command Line)" on page 80 "How to Enable and Disable DHCP Transaction Logging (DHCP Manager)" on page 80 "How to Enable and Disable DHCP Transaction Logging for Current Session (Command Line)" on page 81 "How to Log DHCP Transactions to a Separate `syslog` File" on page 81
Change DNS update options	Enable or disable server's adding DNS entries for clients that supply a host name, and determine the maximum time the server should spend attempting to update DNS.	"How to Enable Dynamic DNS Updating for DHCP Clients" on page 83
Enable or disable duplicate IP address detection	Enable or disable the DHCP server's determination that an IP address is not already in use before offering it to a client.	"How to Customize DHCP Server Performance Options (DHCP Manager)" on page 85 "How to Customize DHCP Server Performance Options (Command Line)" on page 86

TABLE 4–1 Modify DHCP Service Options Task Map *(Continued)*

Tasks	Description	Where to Find Instructions
Change options for DHCP server's reading of configuration information	Enable or disable automatic reading of `dhcptab` at specified intervals, or change the interval between reads.	"How to Customize DHCP Server Performance Options (DHCP Manager)" on page 85 "How to Customize DHCP Server Performance Options (Command Line)" on page 86
Change the number of relay agent hops	Increase or decrease the number of networks a request can travel through before being dropped by the DHCP daemon.	"How to Customize DHCP Server Performance Options (DHCP Manager)" on page 85 "How to Customize DHCP Server Performance Options (Command Line)" on page 86
Change the length of time an IP address offer is cached	Increase or decrease the number of seconds that the DHCP service reserves an offered IP address before offering to a new client.	"How to Customize DHCP Server Performance Options (DHCP Manager)" on page 85 "How to Customize DHCP Server Performance Options (Command Line)" on page 86

The following figure shows DHCP Manager's Modify Service Options dialog box.

FIGURE 4–3 Modify Service Options Dialog Box

Changing DHCP Logging Options

The DHCP service can log DHCP service messages and DHCP transactions to `syslog`. See the`syslogd`(1M) and`syslog.conf`(4) man pages for more information about `syslog`.

DHCP service messages logged to `syslog` include:

- Error messages, which notify the administrator of conditions that prevent the DHCP service from fulfilling a request by a client or by the administrator.
- Warnings and notices, which notify the administrator of conditions that are abnormal, but do not prevent the DHCP service from fulfilling a request.

You can increase the amount of information reported by using the verbose option for the DHCP daemon. Verbose message output can be useful in troubleshooting DHCP problems. See "How to Generate Verbose DHCP Log Messages (DHCP Manager)" on page 80.

Another useful troubleshooting technique is transaction logging. Transactions provide information about every interchange between a DHCP server or BOOTP relay and clients. DHCP transactions include:

- ASSIGN – IP address assignment
- ACK – Server acknowledges that client accepts the offered IP address, and sends configuration parameters
- EXTEND – Lease extension
- RELEASE – IP address release
- DECLINE – Client is declining address assignment
- INFORM – Client is requesting network configuration parameters but not an IP address
- NAK – Server does not acknowledge a client's request to use a previously used IP address
- ICMP_ECHO – Server detects potential IP address is already in use by another host.

BOOTP relay transactions include:

- RELAY-CLNT – Message being relayed from the DHCP client to a DHCP server
- RELAY–SRVR – Message being relayed from the DHCP server to the DHCP client

Transaction logging is disabled by default. When enabled, transaction logging uses the `local0` `syslog` facility by default. DHCP transaction messages are generated with a `syslog` severity level of *notice*, so by default, transactions are logged to the file where other notices are logged. However, because they use a local facility, the transaction messages can be logged separately from other notices if you edit the `syslog.conf` file to specify a separate log file.

You can disable or enable transaction logging, and specify a different `syslog` facility, from 0 through 7, as explained in "How to Enable and Disable DHCP Transaction Logging (DHCP Manager)" on page 80. If you edit the server system's `syslog.conf` file, you can also instruct `syslogd` to store the DHCP transaction messages in a separate file, as explained in "How to Log DHCP Transactions to a Separate `syslog` File" on page 81.

▼ How to Generate Verbose DHCP Log Messages (DHCP Manager)

1. **Choose Modify from the Service menu.**

2. **Select Verbose Log Messages.**

3. **Select Restart Server if it is not already selected.**

4. **Click OK.**

   The daemon runs in verbose mode for this session and each subsequent session until you reset this option. Verbose mode can reduce daemon efficiency because of the time taken to display messages.

▼ How to Generate Verbose DHCP Log Messages (Command Line)

1. **Become superuser on the DHCP server system.**

2. **Type the following commands to stop the DHCP daemon and restart it in verbose mode:**

   ```
   # /etc/init.d/dhcp stop
   # /usr/lib/inet/in.dhcpd -v options
   ```

   where *options* are any other options you normally use to start the daemon.

   The daemon runs in verbose mode for this session only.

   Verbose mode can reduce daemon efficiency because of the time taken to display messages.

▼ How to Enable and Disable DHCP Transaction Logging (DHCP Manager)

This procedure enables/disables transaction logging for all subsequent DHCP server sessions.

1. **Choose Modify from the Service menu.**

2. **Select Log Transactions to Syslog Facility.**

   To disable transaction logging, deselect this option.

3. **(Optional) Select a local facility from 0 to 7 to use for logging transactions.**

   By default, DHCP transactions are logged to the location where system notices are logged, which depends on how `syslogd` is configured. If you want the DHCP transactions to be logged to a file separate from other system notices, see "How to

Log DHCP Transactions to a Separate `syslog` File" on page 81.

Message files can quickly become very large when transaction logging is enabled.

4. **Select Restart Server if it is not already selected.**

5. **Click OK.**

   The daemon will log transactions to the selected `syslog` facility for this session and each subsequent session until you disable it in this dialog box.

▼ How to Enable and Disable DHCP Transaction Logging for Current Session (Command Line)

1. **Become superuser on the DHCP server system.**

2. **Type the following commands to enable logging for the current session:**

   ```
   # /etc/init.d/dhcp stop
   # /usr/lib/inet/in.dhcpd -l syslog-local-facility
   ```

   where *syslog-local-facility* is a number from 0 through 7. If you omit this option, 0 is used by default. See "How to Enable and Disable DHCP Transaction Logging (DHCP Manager)" on page 80.

   Note – To disable transaction logging, omit the `-l` option when starting `in.dhcpd`.

   By default, DHCP transactions are logged to the location where system notices are logged, which depends on how `syslogd` is configured. If you want the DHCP transactions to be logged to a file separate from other system notices, see "How to Log DHCP Transactions to a Separate `syslog` File" on page 81.

   Message files can quickly become very large when transaction logging is enabled.

▼ How to Log DHCP Transactions to a Separate `syslog` File

1. **Become superuser on the DHCP server system.**

2. **Edit the `/etc/syslog.conf` file on the server system and add a line of the following format:**

   ```
   localn.notice        path-to-logfile
   ```

   where *n* is the `syslog` facility number you specified for transaction logging, and *path-to-logfile* is the complete path to the file to use for logging transactions.

   For example, you might add the following line:

```
local0.notice /var/log/dhcpsrvc
```

See the syslog.conf(4) man page for more information about the syslog.conf file.

Enabling Dynamic DNS Updates by DHCP Server

If a host name is mapped to the IP address leased to a DHCP client and the DHCP server has been configured to supply host names, the DHCP server will inform the client of the name it has been assigned. Alternatively, the DHCP server may be configured so that DHCP clients may supply their own host names and the DHCP server will attempt DNS updates on their behalf.

DNS provides basic name-to-address and address-to-name services for the Internet. Once a DNS update is made, other systems may refer to the DHCP client system by name.

You can enable the DHCP service to update the DNS service with the host names of DHCP clients that supply their own host names. When a system's name is registered with DNS, the system is visible outside its domain. In order for the DNS update feature to work, the DNS server, DHCP server, and DHCP client must all be set up correctly, and the requested name must not be in use by another system in the domain.

The DHCP server's DNS update feature works if all the following are true:

- DNS server supports RFC 2136.
- DNS software that is BIND-based, whether on the DHCP server system or the DNS server system, must be v8.2.2, patch level 5 or newer.
- DNS server is configured to accept dynamic DNS updates from the DHCP server.
- DHCP server is configured to make dynamic DNS updates.
- DNS support is configured for the DHCP client's network on the DHCP server.
- DHCP client is configured to supply a requested host name in its DHCP request message.
- Requested host name corresponds to a DHCP-owned address or has no corresponding address.

▼ How to Enable Dynamic DNS Updating for DHCP Clients

Note – Be aware that dynamic DNS updates are by nature a *security risk*.

By default, the Solaris DNS daemon (`in.named`) does not allow dynamic updates. Authorization for dynamic DNS updates is granted if the requesting host's IP address is assigned to the `allow-update` keyword in the appropriate zones of the `named.conf` configuration file on the DNS server system. No other security is provided. You must carefully weigh the convenience of this facility for users against the security risk created when you enable dynamic DNS updates.

1. **At the DNS server, edit the `/etc/named.conf` file as root.**
2. **Find the `zone` section for the appropriate domain and add the DHCP server's IP addresses to the `allow-update` keyword.**

   For example, if the DHCP server resides at addresses 10.0.0.1 and 10.0.0.2, a `named.conf` file for the `dhcp.domain.com` zone would be modified as follows:

   ```
   zone "dhcp.domain.com" in {
                type master;
                file "db.dhcp";
                allow-update { 10.0.0.1; 10.0.0.2; };
   };

   zone "10.IN-ADDR.ARPA" in {
                type master;
                file "db.10";
                allow-update { 10.0.0.1; 10.0.0.2; };
   };
   ```

   Note that `allow-update` for both zones must be enabled to allow the DHCP server to update both A and PTR records on the DNS server.
3. **On the DHCP server, start DHCP Manager.**
4. **Choose Modify from the Service menu.**

   The Modify Service Options dialog box opens.
5. **Select Update DNS Host Information Upon Client Request.**
6. **Specify the number of seconds to wait for a response from the DNS server before timing out, then click OK.**

   The default value should be adequate. If you have timeout problems, you can increase the value later.
7. **Click the Macros tab and ensure that the correct DNS domain is specified.**

The `DNSdmain` option must be passed with the correct domain name to any client that expects dynamic DNS update support. By default, `DNSdmain` is specified in the server macro, which is used as the configuration macro bound to each IP address.

8. **Set up the DHCP client to specify its host name when requesting DHCP service.**

   If you use the Solaris DHCP client, see "How to Enable a Solaris Client to Request Specific Host Name" on page 84. If your client is not a Solaris DHCP client, see the documentation for your DHCP client for information about how to do this.

▼ How to Enable a Solaris Client to Request Specific Host Name

1. **On the client system, edit the `/etc/default/dhcpagent` file as root.**

2. **Find the keyword `REQUEST_HOSTNAME` in the `/etc/default/dhcpagent` file and modify it as follows:**

   ```
   REQUEST_HOSTNAME=yes
   ```

   If there is a comment sign (#) in front of the keyword, remove the #. If the keyword is not present, insert it.

3. **Edit the `/etc/hostname.`*interface* file on the client system and add the following line:**

   `inet` *hostname*

   where *hostname* is the name you want the client to use.

4. **As root, type the following commands to have the client perform a full DHCP negotiation upon rebooting:**

   ```
   # pkill dhcpagent
   # rm /etc/dhcp/interface.dhc
   # reboot
   ```

   The DHCP server makes sure that the host name is not in use by another system on the network before the server assigns it to the client. Depending how it is configured, the DHCP server may update name services with the client's host name.

Customizing DHCP Service Performance Options

You can change options that affect the performance of the DHCP service. These options are described in the following table.

TABLE 4–2 Options Affecting DHCP Server Performance

Server Option	Description	Key in `/etc/inet/dhcpsvc.conf`
Number of BOOTP relay agent hops	If a request has traveled through more than a given number of BOOTP relay agents, it is dropped. The default maximum number of relay agent hops is 4, and it is not likely that this number will be surpassed unless your network is set up to pass requests through several BOOTP relay agents before they reach a DHCP server.	`RELAY_HOPS=`*integer*
Verification of IP address availability before making an offer	By default, the server pings an IP address before offering it to a client to verify that it is not already in use. You can disable this feature to decrease the time it takes to make an offer, but this creates the risk of having duplicate IP addresses in use.	`ICMP_VERIFY=TRUE/FALSE`
Automatic reading of `dhcptab` at specified intervals	The server can be set to automatically read the `dhcptab` at the interval in minutes you specify. If your network configuration information does not change frequently, and you do not have multiple DHCP servers, it is not necessary to reload `dhcptab` automatically. Also note that DHCP Manager gives you the option to have the server reload `dhcptab` after you make a change to the data.	`RESCAN_INTERVAL=`*min*
Length of time to reserve an IP address that has been offered	After a server offers an IP address to a client, it caches the offer, during which time the server does not offer the address again. You can change the number of seconds for which the offer is cached. The default is 10 seconds. On slow networks, you made need to increase the offer time.	`OFFER_CACHE_TIMEOUT=`*sec*

The following procedures describe how to change these options.

▼ How to Customize DHCP Server Performance Options (DHCP Manager)

1. **Choose Modify from the Service menu.**

2. **To change the number of BOOTP relay agents a request can pass through, specify a different Maximum Number of Relay Agent Hops.**

3. **To have the DHCP server verify that an IP address is not in use before it offers the address to a client, select Detect Duplicate IP Addresses.**

4. **To have the DHCP server read `dhcptab` at specified intervals, select Reload dhcptab Every *n* Minutes, and type the number of minutes for the interval.**

5. **To change the length of time the server holds an IP address open after it makes an offer, type the number of seconds in the field Cache Offers for *n* Seconds.**

6. **Select Restart Server if it is not already selected.**

7. **Click OK.**

▼ How to Customize DHCP Server Performance Options (Command Line)

If you change options with this procedure, the changed options affect only the current server session. If the DHCP server system reboots, the DHCP server starts with the settings specified during server configuration. If you want settings to apply to all future sessions, you must make changes using DHCP Manager.

1. **Become superuser on the DHCP server system.**

2. **Type the following command:**

```
# /etc/init.d/dhcp stop
# /usr/lib/inet/in.dhcpd options
```

where *options* are any of the following:

`-h` *relay-hops*	Specifies the maximum number of relay agent hops that can occur before the daemon drops the DHCP/BOOTP datagram.
`-n`	Disables automatic duplicate IP address detection. This is not recommended.
`-t` *dhcptab_rescan_interval*	Specifies the interval in minutes that the DHCP server should use to schedule the automatic rereading of the `dhcptab` information.
`-o` *seconds*	Specifies the number of seconds the DHCP server should cache the offers it has extended to discovering DHCP clients. The default setting is 10 seconds.

For example, the following command sets the hop count to 2, disables duplicate IP address detection, sets the rescan interval to 30 minutes, and sets the offer time to 20 seconds.

```
# /usr/lib/inet/in.dhcp -h 2 -n -t 30 -o 20
```

Adding, Modifying, and Removing DHCP Networks

When you configure a DHCP server, you must also configure at least one network in order to use the DHCP service. You can add more networks at any time.

This section describes:

- "Specifying Network Interfaces to Monitor for DHCP Service" on page 88
- "Adding DHCP Networks" on page 89
- "Modifying DHCP Network Configuration" on page 90
- "Removing DHCP Networks" on page 92

The following task map lists tasks you need to perform when working with DHCP networks and the procedures used to carry them out.

TABLE 4–3 Working with DHCP Networks Task Map

Tasks	Description	Where to Find Instructions
Enable or disable DHCP service on server network interfaces	The default behavior is to monitor all network interfaces for DHCP requests, but you can change this.	"How to Specify Network Interfaces for DHCP Monitoring (DHCP Manager)" on page 88
Add a new network to the DHCP service	Place a network under DHCP management, for the purpose of managing IP addresses on the network.	"How to Add a DHCP Network (DHCP Manager)" on page 89
Change parameters of a DHCP-managed network	Modify the information that is passed to clients of a particular network.	"How to Modify Configuration of a DHCP Network (DHCP Manager)" on page 90 "How to Modify Configuration of a DHCP Network (`dhtadm`)" on page 91
Delete a network from the DHCP service	Remove a network so that IP addresses on the network are no longer managed by DHCP.	"How to Remove a DHCP Network (DHCP Manager)" on page 92 "How to Remove a DHCP Network (`pntadm`)" on page 92

Specifying Network Interfaces to Monitor for DHCP Service

By default, both `dhcpconfig` and DHCP Manager’s Configuration Wizard configure the DHCP server to monitor all the server system’s network interfaces. If you add a new network interface to the server system, the DHCP server automatically monitors the new interface when you boot the system. You can then add any networks that will be monitored through the network interface.

However, DHCP Manager also allows you to specify which network interfaces the DHCP service should monitor and which it should ignore. You might want to ignore an interface if you do not want to offer DHCP service on that network.

If you specify that any interface should be ignored, and then install a new interface, the DHCP server ignores the new interface unless you add it to the server’s list of monitored interfaces. You can specify interfaces with DHCP Manager.

This section includes a procedure that enables you to specify which network interfaces DHCP should monitor, and which to ignore. The procedure uses the Interfaces tab of the DHCP Manager’s Modify Service Options dialog box, which is shown in the following figure.

FIGURE 4–4 Interfaces Tab of Modify Service Options Dialog Box

▼ How to Specify Network Interfaces for DHCP Monitoring (DHCP Manager)

1. **Choose Modify from the Service menu.**

   The Modify Service Options dialog box is displayed.

2. **Select the Interfaces tab.**

3. **Select the appropriate network interface and click the arrow buttons to move the interface to the Monitored Interfaces list or the Ignored Interfaces list.**

   For example, to ignore an interface, select it in the Monitored Interfaces list and click the right arrow button to move the interface in the Ignored Interfaces list.

4. **Make sure Restart Server is selected and click OK.**

Adding DHCP Networks

When you use DHCP Manager to configure the server, the first network (usually the local one on the server system's primary interface) is also configured at the same time. If you want to configure additional networks, use the DHCP Network Wizard in DHCP Manager.

If you use `dhcpconfig -D` to configure the server, you must manually configure all networks that will be served by the DHCP service. See "How to Add a DHCP Network (`dhcpconfig`)" on page 90 for more information.

The following figure shows the initial dialog box for the DHCP Network Wizard in DHCP Manager.

FIGURE 4–5 DHCP Manager's Network Wizard

When you configure a new network, DHCP Manager creates the following components:

- Network table in the data store. The new network is shown in the network list on the Addresses tab of DHCP Manager.
- Network macro that contains information needed by clients that reside on this network. The network macro's name matches the IP address of the network. The network macro is added to the `dhcptab` in the data store.

▼ How to Add a DHCP Network (DHCP Manager)

1. **Click the Addresses tab in DHCP Manager.**

   Any networks already configured for DHCP service are listed.

2. **Choose Network Wizard from the Edit menu.**

3. **Select options or type requested information based on the decisions you made during the planning phase.**

   Planning is described in "Planning for Remote Network Configuration" on page 50.

   If you have difficulty with the wizard, click Help in the wizard window to open your web browser and display help for the DHCP Network Wizard.

4. **Click Finish to complete the network configuration when you have finished entering the requested information.**

   The Network Wizard creates a network macro whose name matches the IP address of the network. If you click the Macros tab in the DHCP Manager window and select the network macro, you can confirm that the information you provided in the wizard has been inserted as values for options contained in the macro.

The Network Wizard creates an empty network table, which is listed in the left pane of the window. You must add addresses for the network before the network's IP addresses can be managed under DHCP. See "Adding Addresses to the DHCP Service" on page 100 for more information.

▼ How to Add a DHCP Network (`dhcpconfig`)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type the following command on the DHCP server system:**

   ```
   # /usr/sbin/dhcpconfig -N network_address
   ```

   where *network_address* is the IP address of the network you want to add to the DHCP service. See the `dhcpconfig` man page for suboptions you can use with the `-N` option.

   If you do not use suboptions, `dhcpconfig` uses network files to obtain information it needs about the network.

3. **Add IP addresses for the network so clients on the network can obtain addresses.**

   See "Adding Addresses to the DHCP Service" on page 100.

Modifying DHCP Network Configuration

After you add a network to the DHCP service, you can modify the configuration information you originally supplied by modifying the network macro used to pass information to the clients on the network.

The following figure shows the Macros tab of the DHCP Manager.

FIGURE 4–6 DHCP Manager's Macros Tab

▼ How to Modify Configuration of a DHCP Network (DHCP Manager)

1. **Select the Macros tab.**

   All macros defined for this DHCP server are listed in the left pane.

2. **Select the network macro whose name matches the network whose configuration you want to change.**

   The network macro name is the network IP address.

3. **Choose Properties from the Edit menu.**

   The Macro Properties dialog box displays a table of the options included in the macro.

4. **Select the option you want to modify.**

   The option name and value are displayed in text fields near the top of the dialog box.

5. **Type the new value for the option and click Modify.**

   You can also add options here by clicking Select in the dialog box. See "Modifying DHCP Macros" on page 109 for more general information about modifying macros.

6. **Select Notify DHCP Server of Change and click OK.**

   The change is made to the `dhcptab` and the DHCP server is signaled to reread the `dhcptab` and put the changes into effect.

▼ How to Modify Configuration of a DHCP Network (`dhtadm`)

1. **Determine which macro includes information for all clients of the network.**

   The network macro's name matches the network IP address.

   If you don't know which macro includes this information, you can display the `dhcptab` database to list all macros by using the command `dhtadm -P`.

2. **Type a command of the following format to change the value of the option you want to change:**

   ```
   # dhtadm -M -m macro-name -e 'symbol=value'
   ```

   For example, to change the `188.25.62.0` macro's lease time to 57600 seconds and NIS domain to `sem.west.com`, type the following commands:

   ```
   # dhtadm -M -m 188.25.62.0 -e 'LeaseTim=57600'
   # dhtadm -M -m 188.25.62.0 -e 'NISdmain=sem.west.com'
   ```

3. **Type the following command as root to make the DHCP daemon reread `dhcptab`:**

   ```
   # pkill -HUP in.dhcpd
   ```

Removing DHCP Networks

DHCP Manager enables you to remove multiple networks at once. You have the option to automatically remove the hosts table entries associated with the DHCP-managed IP addresses on those networks as well. The following figure shows DHCP Manager's Delete Networks dialog box.

FIGURE 4–7 Delete Networks Dialog Box

The `pntadm` command requires you to delete each IP address entry from a network before you delete that network. You can delete only one network at a time.

▼ How to Remove a DHCP Network (DHCP Manager)

1. **Select the Addresses tab.**
2. **Choose Delete Networks from the Edit menu.**

   The Delete Networks dialog box opens.
3. **In the Keep Networks list, select the networks you want to delete.**

   Press the Control key while you click with the mouse to select multiple networks, or press the Shift key while you click to select a range of networks.
4. **Click the right arrow button to move the selected networks to the Delete Networks list.**
5. **If you want to remove the host table entries for the DHCP–managed addresses on this network, select Delete Host Table Entries.**

   Note that this does not delete the host registrations at the DNS server for these addresses. It affects only the local name service.
6. **Click OK.**

▼ How to Remove a DHCP Network (`pntadm`)

Note that this procedure deletes the addresses on the network before removing the network. This ensures that the host names are removed from the `hosts` file or database.

1. **On the server system, become superuser or a user assigned to the DHCP Management profile .**

2. **Type a command following this format to remove an IP address and its host name from the name service:**

   ```
   # pntadm -D -y IP-address
   ```

   For example, to remove address 188.25.52.1, type the following command:

   ```
   # pntadm -D -y 188.25.52.1
   ```

   The `-y` option specifies to delete the host name.

3. **Repeat the `pntadm -D -y` command for each address in the network.**

   You might want to create a script to do this if you are deleting many addresses.

4. **After all addresses are deleted, type the following command to delete the network from the DHCP service.**

   ```
   # pntadm -R network-IP-address
   ```

   For example, to remove network 188.25.52.0, type the following command:

   ```
   # pntadm -R 188.25.52.0
   ```

   See the `pntadm` man page for more information about using `pntadm`.

Supporting BOOTP Clients with DHCP Service

To support BOOTP clients on your DHCP server, you must set up your DHCP server to be BOOTP compatible. You can register BOOTP clients in the DHCP server's database or reserve a number of IP addresses for allocation to BOOTP clients, depending how you set up BOOTP compatibility.

You can set up support for BOOTP clients in one of the following ways:

- **Automatic BOOTP support** – Any BOOTP client on a DHCP-managed network, or on a network connected by a BOOTP relay agent to a DHCP-managed network can obtain an IP address from the server. This requires you to reserve a pool of addresses for exclusive use by BOOTP clients. This option may be more useful if the server must support a large number of BOOTP clients.
- **Manual BOOTP support** – Only those BOOTP clients that have been manually registered with the DHCP service will receive a response from the server. This requires you to bind a client's ID to a particular IP address that has been marked for BOOTP clients. This option is useful for a small number of BOOTP clients, or in the event that you want to restrict the BOOTP clients that can use the server.

Note – BOOTP addresses are permanently assigned, whether or not you explicitly assign them a permanent lease.

The following task map lists tasks you need to perform to support BOOTP clients and the procedures used to carry them out.

TABLE 4–4 BOOTP Support Task Map

Tasks	Description	Where to Find Instructions
Set up automatic BOOTP support	Provide IP address for any BOOTP client on a DHCP-managed network, or on a network connected by a relay agent to a DHCP-managed network.	"How to Set Up Support of Any BOOTP Client (DHCP Manager)" on page 94
Set up manual BOOTP support	Provide IP address for only those BOOTP clients that have been manually registered with the DHCP service.	"How to Set Up Support of Registered BOOTP Clients (DHCP Manager)" on page 95

▼ How to Set Up Support of Any BOOTP Client (DHCP Manager)

1. **Select Modify from the Service menu.**

   The Modify Service Options dialog box opens.

2. **In the BOOTP Compatibility section of the dialog box, select Automatic.**

3. **Select Restart Server, if it is not already selected.**

4. **Click OK.**

5. **Select the Addresses tab in DHCP Manager.**

6. **Select addresses that you want to reserve for BOOTP clients.**

   Select a range of addresses by clicking the first address, pressing the Shift key, and clicking the last address.

   Select multiple non-concurrent addresses by pressing the Control key while clicking each address.

7. **Select Properties from the Edit menu.**

   The Modify Multiple Addresses dialog box opens.

8. **In the BOOTP section, select Assign All Addresses Only to BOOTP Clients.**

All other options should be set to Keep Current Settings.

9. **Click OK.**

   Any BOOTP client can now obtain an address from this DHCP server.

▼ How to Set Up Support of Registered BOOTP Clients (DHCP Manager)

1. **Select Modify from the Service menu.**

   The Modify Service Options dialog box opens.

2. **In the BOOTP Compatibility section of the dialog box, select Manual.**

3. **Select Restart Server if it is not already selected.**

4. **Click OK.**

5. **Select the Addresses tab in DHCP Manager.**

6. **Select an address you want to assign to a particular BOOTP client.**

7. **Choose Properties from the Edit menu.**

   The Address Properties dialog box opens.

8. **Select the Lease tab.**

9. **In the Client ID field, type the client's identifier.**

   For a BOOTP client that runs the Solaris operating environment on an Ethernet network, the client ID is a string derived from the client's hexadecimal Ethernet address, preceded by the Address Resolution Protocol (ARP) type for Ethernet (01). For example, a BOOTP client having the Ethernet address 8:0:20:94:12:1e would use the client ID 0108002094121E.

   Tip – As superuser on a Solaris client system, type the following command to obtain the Ethernet address for the interface:

   ```
   ifconfig -a
   ```

   ---

10. **Select Reserved to reserve the IP address for this client.**

11. **Select Assign Only to BOOTP Clients.**

12. **Click OK.**

    In the Addresses tab, BOOTP is displayed in the Status field, and the client ID you entered is listed in the Client ID field.

Working With IP Addresses in the DHCP Service

You can use DHCP Manager or the `pntadm` command to add IP addresses, modify their properties, and remove them from the DHCP service. Before you work with IP addresses, you should refer to Table 4–6 to become familiar with IP address properties. The table provides information for users of DHCP Manager and `pntadm`.

Note – This section does not include procedures for using the `pntadm` command. However Table 4–6 includes examples of using `pntadm` to specify IP address properties while adding and modifying IP addresses. Also refer to the `pntadm` man page for more information about `pntadm`.

The following task map lists tasks you must perform to add, modify, remove IP addresses and the procedures used to carry them out.

TABLE 4–5 IP Addresses in DHCP Task Map

Tasks	Description	Where to Find Instructions
Add single or multiple IP addresses to DHCP service.	Add IP addresses on networks that are already managed by the DHCP service by using DHCP Manager.	"How to Add a Single IP Address (DHCP Manager)" on page 101 "How to Duplicate an Existing IP Address (DHCP Manager)" on page 101 "How to Add Multiple Addresses (DHCP Manager)" on page 102 "How to Add Addresses (`pntadm`)" on page 102
Change properties of an IP address.	Change any of the IP address properties described in Table 4–6.	"How to Modify IP Address Properties (DHCP Manager)" on page 103 "How to Modify IP Address Properties (`pntadm`)" on page 103

TABLE 4–5 IP Addresses in DHCP Task Map *(Continued)*

Tasks	Description	Where to Find Instructions
Remove IP addresses from DHCP service.	Prevent the use of specified IP addresses by DHCP.	"How to Mark Addresses Unusable (DHCP Manager)" on page 104 "How to Mark Addresses Unusable (`pntadm`)" on page 104 "How to Delete IP Addresses from DHCP Service (DHCP Manager)" on page 105 "How to Delete IP Addresses from DHCP Service (`pntadm`)" on page 105
Assign consistent address to a DHCP client.	Set up a client to receive the same IP address each time it requests its configuration.	"How to Assign a Consistent IP Address to a DHCP Client (DHCP Manager)" on page 106 "How to Assign a Consistent IP Address to a DHCP Client (`pntadm`)" on page 107

The following table lists and describes the properties of IP addresses.

TABLE 4–6 IP Address Properties

Property	Description	How to Specify in `pntadm` Command
Network address	Address of the network that contains the IP address you are working with. The network address is displayed in the Networks list on the Addresses tab in DHCP Manager.	The network address must be the last argument on the `pntadm` command line used to create, modify, or delete an IP address. For example, to add an IP address to network 188.21.0.0 **`pntadm -A`** *ip-address options* **`188.21.0.0`**
IP address	Address you are working with, whether you are creating, modifying, or deleting it. The IP address is displayed in the first column of the DHCP Manager's Addresses tab.	The IP address must accompany the `-A`, `-M`, and `-D` options to the `pntadm` command. For example, to modify IP address 188.21.5.12 **`pntadm -M 188.21.5.12`** *options* **`188.21.0.0`**

TABLE 4–6 IP Address Properties *(Continued)*

Property	Description	How to Specify in `pntadm` Command
Client name	Host name mapped to the IP address in the hosts table. This name may be automatically generated by DHCP Manager or interactive `dhcpconfig` when addresses are created. If you create a single address, you can supply the name.	Specify the client name with the `-h` option. For example, to specify client name carrot12 for 188.21.5.12: **`pntadm -M 188.21.5.12 -h carrot12 188.21.0.0`**
Owning server	DHCP server that manages the IP address and is responsible for responding to the DHCP client's request for IP address allocation.	Specify the owning server name with the `-s` option. For example to specify server blue2 to own 188.21.5.12: **`pntadm -M 188.21.5.12 -s blue2 188.21.0.0`**
Configuration macro	Macro the DHCP server uses to obtain network configuration options from the `dhcptab`. Several macros are created automatically when you configure a server and add networks. See "About Macros" on page 30 for more information about macros. When DHCP Manager or interactive `dhcpconfig` create addresses, they create a server macro and assign it as the configuration macro for each address.	Specify the macro name with the `-m` option. For example, to assign the server macro blue2 to address 188.21.5.12 **`pntadm -M 188.21.5.12 -m blue2 188.21.0.0`**
Client ID	Text string that is unique within the DHCP service. If the client ID is listed as 00, the address is not allocated to any client. If you specify a client ID when modifying the properties of an IP address, you manually bind the address to that client for its exclusive use. The client ID is determined by the vendor of the DHCP client. If your client is not a Solaris DHCP client, consult your DHCP client documentation for more information.	Specify the client ID with the `-i` option. For example, to assign client ID 08002094121E to address 188.21.5.12 **`pntadm -M 188.21.5.12 -i 0108002094121E 188.21.0.0`**

TABLE 4–6 IP Address Properties *(Continued)*

Property	Description	How to Specify in `pntadm` Command
	For Solaris DHCP clients, the client ID is derived from the client's hexadecimal hardware address, preceded by the ARP code for the type of network, such as 01 for Ethernet. The ARP codes are assigned by the Internet Assigned Numbers Authority (IANA) in the ARP Parameters section of the Assigned Numbers standard at http://www.iana.com/numbers.html For example, a Solaris client with the hexadecimal Ethernet address 8:0:20:94:12:1e would use the client ID 0108002094121E. The client ID is listed in DHCP Manager and `pntadm` when a client is currently using an address. **Tip:** As superuser on the Solaris client system, type the following command to obtain the Ethernet address for the interface: `ifconfig -a`	
Reserved	The setting that specifies the address is reserved exclusively for the client indicated by the client ID, and the DHCP server cannot reclaim the address. If you choose this option, you manually assign the address to the client.	Specify that the address is reserved, or manual, with the `-f` option. For example, to specify that IP address 188.21.5.12 is reserved for a client: **`pntadm -M 188.21.5.12 -f MANUAL 188.21.0.0`**
Lease type/policy	The setting that determines how DHCP manages the use of the IP address by clients. A lease may be dynamic or permanent. See "Dynamic and Permanent Lease Type" on page 48 for a complete explanation.	Specify that the address would be permanently assigned with the `-f` option. Addresses are dynamically leased by default. For example, to specify that IP address 188.21.5.12 has a permanent lease: **`pntadm -M 188.21.5.12 -f PERMANENT 188.21.0.0`**

TABLE 4–6 IP Address Properties *(Continued)*

Property	Description	How to Specify in `pntadm` Command
Lease expiration time	Date and time when the lease expires, applicable only when a dynamic lease is specified. The date is specified in *mm/dd/yyyy* format.	Specify an absolute lease expiration time with `-e`. For example, to specify an expiration time of January 1, 2002: **`pntadm -M 188.21.5.12 -e 01/01/2002 188.21.0.0`**
BOOTP setting	The setting that marks the address as reserved for BOOTP clients. See “Supporting BOOTP Clients with DHCP Service” on page 93 for more information about supporting BOOTP clients.	Reserve an address for BOOTP clients with `-f`. For example, to reserve IP address 188.21.5.12 for BOOTP clients: **`pntadm -M 188.21.5.12 -f BOOTP 188.21.0.0`**
Unusable setting	The setting that marks the address so it cannot be assigned to any client.	Mark an address unusable with `-f`. For example, to mark IP address 188.21.5.12 unusable: **`pntadm -M 188.21.5.12 -f UNUSABLE 188.21.0.0`**

Adding Addresses to the DHCP Service

Before you add addresses, you must add the network that owns them to the DHCP service. See “Adding DHCP Networks” on page 89 for information about adding networks.

You can add addresses with DHCP Manager or `pntadm`.

On networks that are already managed by the DHCP service, you can add addresses in several ways with DHCP Manager:

- **Add a single IP address** – Place one new IP address under DHCP management.
- **Duplicate an existing IP address** – Copy the properties of an existing IP address managed by DHCP, and supply a new IP address and client name.
- **Add a range of multiple IP addresses** – Use the Address Wizard to place a series of IP addresses under DHCP management.

The following figure shows the Create Address dialog box. The Duplicate Address dialog box is identical to the Create Address dialog box, except that the text fields display the values for an existing address.

FIGURE 4–8 Create Address Dialog Box

The following figure shows the first dialog of the Address Wizard, used to add a range of IP addresses.

FIGURE 4–9 Address Wizard

▼ How to Add a Single IP Address (DHCP Manager)

1. **Select the Addresses tab.**
2. **Select the network where the new IP address is to be added.**
3. **Choose Create from the Edit menu.**

   The Create Address dialog box opens.
4. **Select or type values for the address settings on the Address and Lease tabs.**

   See Table 4–6 for information about the settings.
5. **Click OK.**

▼ How to Duplicate an Existing IP Address (DHCP Manager)

1. **Select the Addresses tab.**
2. **Select the network where the new IP address is located.**
3. **Select the address whose properties you want to duplicate.**
4. **Choose Duplicate from the Edit menu.**
5. **Change the IP address and client name for the address.**

   Most other options should remain the same, but you can change them if necessary.
6. **Click OK.**

▼ How to Add Multiple Addresses (DHCP Manager)

1. **Select the Addresses tab.**

2. **Select the network where the new IP addresses are to be added.**

3. **Choose Address Wizard from the Edit menu.**

   The Address Wizard prompts you to provide values for the IP address properties. See Table 4–6 for more information about the properties. "Making Decisions for IP Address Management" on page 46 includes more extensive information.

4. **Click the right arrow button as you finish entering information in each screen, and click Finish on the last screen.**

   The Addresses tab is updated with the new addresses.

▼ How to Add Addresses (`pntadm`)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type a command of the following format:**

   ```
   # pntadm -A ip-address options network-address
   ```

   Refer to the `pntadm` man page for a list of options you can use with `pntadm -A`. In addition, Table 4–6 shows some sample `pntadm` commands that specify options.

Note – You can write a script to add multiple addresses with `pntadm`. See Example 6–1 for an example.

Modifying IP Addresses in the DHCP Service

After you add IP addresses to the DHCP service, you can modify any of the properties described in Table 4–6 by using DHCP Manager or the `pntadm -M` command. See the `pntadm` man page for more information about `pntadm -M`.

The following figure shows the Address Properties dialog box that you use to modify IP address properties.

FIGURE 4–10 Address Properties Dialog Box

The following figure shows the Modify Multiple Addresses dialog box that you use to modify multiple IP addresses.

FIGURE 4–11 Modify Multiple Addresses Dialog Box

▼ How to Modify IP Address Properties (DHCP Manager)

1. **Select the Addresses tab.**
2. **Select the IP address's network.**
3. **Select one or more IP addresses you want to modify.**

   If you want to modify more than one address, press the Control key while you click with the mouse to select multiple addresses. You can also press the Shift key while you click to select a block of addresses.
4. **Choose Properties from the Edit menu.**

   The Modify Addresses dialog box or the Modify Multiple Address dialog box opens.
5. **Change the appropriate properties.**

   Click the Help button or refer to Table 4–6 for information about the properties.
6. **Click OK.**

▼ How to Modify IP Address Properties (`pntadm`)

1. **Become superuser or a user assigned to the DHCP Management profile .**
2. **Enter a command of the following format:**

   ```
   # pntadm -M ip-address options network-address
   ```

   Many options can be used with the `pntadm` command, which are documented in the `pntadm` man page.

   Table 4–6 shows some sample `pntadm` commands that specify options.

Removing Addresses From DHCP Service

At times you might want the DHCP service to stop managing a particular address or group of addresses. The method you use to remove an address from DHCP depends on whether you want the change to be temporary or permanent.

- To temporarily prevent the use of addresses, you can mark them unusable in the Address Properties dialog box as described in “Marking IP Addresses Unusable by the DHCP Service” on page 104.
- To permanently prevent the use of addresses by DHCP clients, delete the addresses from the DHCP network tables, as described in “Deleting IP Addresses from DHCP Service” on page 105.

Marking IP Addresses Unusable by the DHCP Service

You can use the `pntadm -M` command with the `-f UNUSABLE` option to mark addresses unusable.

In DHCP Manager, you use the Address Properties dialog box, shown in Figure 4–10, to mark individual addresses, and the Modify Multiple Addresses dialog box, show in Figure 4–11, to mark multiple addresses, as described in the following procedure.

▼ How to Mark Addresses Unusable (DHCP Manager)

1. **Select the Addresses tab.**
2. **Select the IP address’s network.**
3. **Select one or more IP addresses you want to mark unusable.**

   If you want to mark more than one address unusable, press the Control key while you click with the mouse to select multiple addresses. You can also press the Shift key while you click to select a block of addresses.
4. **Choose Properties from the Edit menu.**

   The Modify Addresses dialog box or the Modify Multiple Address dialog box opens.
5. **If you are modifying one address, select the Lease tab.**
6. **Select Address is Unusable.**

   If you are editing multiple addresses, select Mark All Addresses Unusable.
7. **Click OK.**

▼ How to Mark Addresses Unusable (`pntadm`)

1. **Become superuser or a user assigned to the DHCP Management profile .**
2. **Enter a command of the following format:**

```
# pntadm -M ip-address -f UNUSABLE network-address
```

For example, to mark address `24.64.3.3` as unusable, type:

```
pntadm -M 24.64.3.3 -f UNUSABLE 24.64.3.0
```

Deleting IP Addresses from DHCP Service

You should delete IP addresses from the DHCP service database if you no longer want the address to be managed by DHCP. You can use the `pntadm -D` command or DHCP Manager's Delete Address dialog box.

The following figure shows the Delete Address dialog box.

FIGURE 4–12 Delete Address Dialog Box

▼ How to Delete IP Addresses from DHCP Service (DHCP Manager)

1. **Select the Addresses tab.**

2. **Select the IP address's network.**

3. **Select one or more IP addresses you want to delete.**

   If you want to delete more than one address, press the Control key while you click with the mouse to select multiple addresses. You can also press the Shift key while you click to select a block of addresses.

4. **Choose Delete from the Edit menu.**

   The Delete Address dialog box lists the address you selected so you can confirm the deletion.

5. **If you want to delete the host names from the hosts table, select Delete From Hosts Table.**

   If the host names were generated by DHCP Manager or `dhcpconfig`, you might want to delete the names from the hosts table.

6. **Click OK.**

▼ How to Delete IP Addresses from DHCP Service (`pntadm`)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type a command of the following format:**

   ```
   # pntadm -D ip-address
   ```

If you include the `-y` option, the host name is deleted from the name service in which it is maintained.

Setting Up DHCP Clients for a Consistent IP Address

The Solaris DHCP service attempts to provide the same IP address to a client that has previously obtained an address through DHCP. However, it is not always possible when a dynamic lease is used.

Routers, NIS/NIS+, DNS servers, and other hosts critical to the network should not use DHCP because they should not rely on the network to obtain their IP addresses. Clients such as print or file servers should have consistent IP addresses as well, but can be set up to receive their network configurations through DHCP.

You can set up a client to receive the same IP address each time it requests its configuration if you reserve, or manually assign, the client's ID to the address you want it to use. You can set up the reserved address to use a dynamic lease to make it easy to track the use of the address, or a permanent lease if you do not need to track address use. However, you might not want to use permanent leases because once a client obtains a permanent lease, it does not contact the server again and cannot obtain updated configuration information unless it releases the IP address and restarts the DHCP lease negotiation. A diskless client is an example of a client that should use a reserved address with a dynamic lease.

You can use the `pntadm -M` command or DHCP Manager's Address Properties dialog box.

The following figure shows the Lease tab of the Address Properties dialog box used to modify the lease.

FIGURE 4–13 Address Properties Lease Tab

▼ How to Assign a Consistent IP Address to a DHCP Client (DHCP Manager)

1. **Determine the client ID for the client you want to have a permanent IP address.**

   See the entry for client ID in Table 4–6 for information about how to determine the client ID.

2. **Select the Addresses tab in DHCP Manager.**

3. **Select the appropriate network.**

4. **Double-click the IP address you want to the client to use.**

   The Address Properties window opens.

5. **Select the Lease tab.**

6. **In the Client ID field, type the client ID you determined from the client's hardware address.**

   See the Client ID entry in Table 4–6 for more information.

7. **Select the Reserved option to prevent the IP address from being reclaimed by the server.**

8. **In the Lease Policy area of the window, select Dynamic or Permanent assignment.**

   Select Dynamic if you want the client to negotiate to renew leases, and thus be able to track when the address is used. Because you selected Reserved, the address cannot be reclaimed even when it uses a dynamic lease. You do not need to enter an expiration date for this lease. The DHCP server calculates the expiration date based on the lease time.

   If you select Permanent, you cannot track the use of the IP address unless you enable transaction logging.

▼ How to Assign a Consistent IP Address to a DHCP Client (pntadm)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type a command of the following format:**

   ```
   # pntadm -M ip-address -i client-id -f MANUAL+BOOTP network-address
   ```

   Refer to the Client ID entry in Table 4–6 for more information about how to determine client identifiers.

Working With DHCP Macros

DHCP macros are containers of DHCP options. The Solaris DHCP service uses macros to gather together options that should be passed to clients. DHCP Manager and dhcpconfig create a number of macros automatically when you configure the server. See "About Macros" on page 30 for background information about macros, and Chapter 3 for information about macros created by default.

You might find that when changes occur on your network, you need to make changes to the configuration information passed to clients. To do this, you need to work with DHCP macros. You can view, create, modify, duplicate, and delete DHCP macros.

When you work with macros, you must know about DHCP standard options, which are described in the `dhcp_inittab` man page.

The following task map lists tasks to help you view, create, modify, and delete DHCP macros.

TABLE 4–7 DHCP Macros Task Map

Tasks	Description	Where to Find Instructions
View DHCP macros.	Display a list of all the macros defined on the DHCP server.	"How to View Macros Defined on a DHCP Server (DHCP Manager)" on page 109 "How to View Macros Defined on a DHCP Server (`dhtadm`)" on page 109
Create DHCP macros.	Create new macros to support DHCP clients.	"How to Create a DHCP Macro (DHCP Manager)" on page 113 "How to Create a DHCP Macro (`dhtadm`)" on page 114
Modify values passed in macros to DHCP clients.	Change macros by modifying existing options, adding options to macros, removing options from macros.	"How to Change Values for Options in a DHCP Macro (DHCP Manager)" on page 110 "How to Change Values for Options in a DHCP Macro (`dhtadm`)" on page 110 "How to Add Options to a DHCP Macro (DHCP Manager)" on page 111 "How to Add Options to a DHCP Macro (`dhtadm`)" on page 112 "How to Delete Options from a DHCP Macro (DHCP Manager)" on page 112 "How to Delete Options from a DHCP Macro (`dhtadm`)" on page 112
Delete DHCP macros.	Remove DHCP macros that are no longer used.	"How to Delete a DHCP Macro (DHCP Manager)" on page 114 "How to Delete a DHCP Macro (`dhtadm`)" on page 115

The following figure shows the Macros tab in the DHCP Manager window.

FIGURE 4–14 DHCP Manager's Macros Tab

▼ How to View Macros Defined on a DHCP Server (DHCP Manager)

1. **Select the Macros tab.**

   The Macros area on the left side of the window displays, in alphabetical order, all macros defined on the server. Macros preceded by a folder icon include references to other macros, while macros preceded by a document icon do not reference other macros.

2. **To open a macro folder, click the open/close widget to the left of the folder icon.**

   The macros included in the selected macro are listed.

3. **To view the contents of a macro, click the macro name and look at the area on the right side of the window.**

   Options and their assigned values are displayed.

▼ How to View Macros Defined on a DHCP Server (`dhtadm`)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type the following command:**

   ```
   # dhtadm -P
   ```

   This command prints to standard output the formatted contents of the `dhcptab`, including all macros and symbols defined on the server.

Modifying DHCP Macros

You might need to modify macros when some aspect of your network changes and one or more clients need to know about the change. For example, you might add a router or a NIS server, create a new subnet, or decide to change the lease policy.

When you modify a macro, you must know the name of the DHCP option that corresponds to the parameter you want to change, add, or delete. The standard DHCP options are listed in the DHCP Manager help and in the `dhcp_inittab` man page.

You can use the dhtadm -M -m command or DHCP Manager to modify macros. See the dhtadm man page for more information about dhtadm.

The following figure shows DHCP Manager's Macro Properties dialog box.

FIGURE 4–15 Macro Properties Dialog Box

▼ How to Change Values for Options in a DHCP Macro (DHCP Manager)

1. **Select the Macros tab.**
2. **Select the macro you want to change.**
3. **Choose Properties from the Edit menu.**

   The Macro Properties dialog box opens.
4. **In the table of Options, select the option you want to change.**

   The option's name and value are displayed in the Option Name and Option Value fields.
5. **In the Option Value field, select the old value and type the new value for the option.**
6. **Click Modify.**

   The new value is displayed in the options table.
7. **Select Notify DHCP Server of Change.**

   This selection tells the DHCP server to reread the dhcptab to put the change into effect immediately after you click OK.
8. **Click OK.**

▼ How to Change Values for Options in a DHCP Macro (dhtadm)

1. **Become superuser or a user assigned to the DHCP Management profile .**
2. **Type a command of the following format:**

   ```
   # dhtadm -M -m macroname -e 'option=value:option=value'
   ```

For example, to change the lease time and the Universal Time Offset in macro bluenote, type the following command:

```
# dhtadm -M -m bluenote -e 'LeaseTim=43200:UTCOffst=28800'
```

▼ How to Add Options to a DHCP Macro (DHCP Manager)

1. **Select the Macros tab.**

2. **Select the macro you want to change.**

3. **Choose Properties from the Edit menu.**

   The Macro Properties dialog box opens.

4. **In the Option Name field, specify the name of an option by using one of the following methods:**

   a. **Click the Select button next to the Option Name field and select the option you want to add to the macro.**

      The Select Option dialog box displays an alphabetized list of names of Standard category options and descriptions. If you want to add an option that is not in the Standard category, use the Category list to select the category you want.

      See "About Macros" on page 30 for more information about macro categories.

   b. **Type `Include` if you want to include a reference to an existing macro in the new macro.**

5. **Type the value for the option in the Option Value field.**

   If you typed **`Include`** as the option name, you must specify the name of an existing macro in the Option Value field.

6. **Click Add.**

   The option is added to the bottom of the list of options displayed for this macro. If you want to change the option's position in the list, select the option and click the arrow keys next to the list to move the option up or down.

7. **Select Notify DHCP Server of Change.**

   This selection tells the DHCP server to reread the dhcptab to put the change into effect immediately after you click OK.

8. **Click OK.**

▼ How to Add Options to a DHCP Macro (dhtadm)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type a command of the following format:**

   ```
   # dhtadm -M -m macroname -e 'option=value'
   ```

   For example, to add the ability to negotiate leases, in macro bluenote, type the following command:

   ```
   # dhtadm -M -m bluenote -e 'LeaseNeg=_NULL_VALUE'
   ```

   Note that if an option does not require a value, you must use _NULL_VALUE as the value for the option.

▼ How to Delete Options from a DHCP Macro (DHCP Manager)

1. **Select the Macros tab.**

2. **Select the macro you want to change.**

3. **Choose Properties from the Edit menu.**

   The Macro Properties dialog box opens.

4. **Select the option you want to remove from the macro.**

5. **Click Delete.**

   The option is removed from the list of options for this macro.

6. **Select Notify DHCP Server of Change.**

   This selection tells the DHCP server to reread the dhcptab to put the change into effect immediately after you click OK.

7. **Click OK.**

▼ How to Delete Options from a DHCP Macro (dhtadm)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type a command of the following format:**

   ```
   # dhtadm -M -m macroname -e 'option='
   ```

   For example, to remove the ability to negotiate leases in macro bluenote, type the following command:

```
# dhtadm -M -m bluenote -e 'LeaseNeg='
```

If an option is specified with no value, it is removed from the macro.

Creating DHCP Macros

You may want to add new macros to your DHCP service to support clients with specific needs. You can use the `dhtadm -A -m` command or DHCP Manager's Create Macro dialog box to add macros. See the `dhtadm` man page for more information about the `dhtadm` command.

The following figure shows DHCP Manager's Create Macro dialog box.

FIGURE 4–16 Create Macro Dialog Box

▼ How to Create a DHCP Macro (DHCP Manager)

1. **Select the Macros tab.**
2. **Choose Create from the Edit menu.**

   The Create Macro dialog box opens.
3. **Type a unique name for the macro.**

   The name can be up to 128 alphanumeric characters. If you use a name that matches a vendor class identifier, network address, or client ID, the macro will be processed automatically for appropriate clients. If you use a different name, the macro can only be processed if it is assigned to a specific IP address or included in another macro that is processed. See "Macro Processing by the DHCP Server" on page 31 for more detailed information.
4. **Click the Select button next to the Option Name field.**

   The Select Option dialog box displays an alphabetized list of names of Standard category options and their descriptions.
5. **If you want to add an option that is not in the Standard category, use the Category list to select the category you want.**

   See "About Options" on page 30 for more information about option categories.
6. **Select the option you want to add to the macro and click OK.**

   The Macro Properties dialog box displays the selected option in the Option Name field.

7. **Type the value for the option in the Option Value field.**

8. **Click Add.**

   The option is added to the bottom of the list of options displayed for this macro. If you want to change the option's position in the list, select the option and click the arrow keys next to the list to move the option up or down.

9. **Repeat Step 6 through Step 8 for each option you want to add to the macro.**

10. **Select Notify DHCP Server of Change when you are finished adding options.**

    This selection tells the DHCP server to reread the dhcptab to put the change into effect immediately after you click OK.

11. **Click OK.**

▼ How to Create a DHCP Macro (dhtadm)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type a command of the following format:**

   ```
   # dhtadm -A -m macroname -d ':option=value:option=value:option=value:'
   ```

   There is no limit to the number of option/value pairs included in the argument to -d. The argument must begin and end with colons, with colons separating each option/value pair.

   For example, to create macro bluenote, type the following command:

   ```
   # dhtadm -A -m bluenote -d \
   ':Router=24.63.6.121:LeaseNeg=_NULL_VALUE:'DNSserv=24.63.28.12:'
   ```

   Note that if an option does not require a value, you must use _NULL_VALUE as the value for the option.

Deleting DHCP Macros

You might want to delete a macro from the DHCP service. For example, if you delete a network from the DHCP service, you can also delete the associated network macro.

You can use the dhtadm -D -m command or DHCP Manager to delete macros.

▼ How to Delete a DHCP Macro (DHCP Manager)

1. **Select the Macros tab.**

2. **Select the macro you want to delete.**

The Delete Macro dialog box prompts you to confirm that you want to delete the specified macro.

3. **Select Notify DHCP Server of Change.**

4. **Click OK.**

▼ How to Delete a DHCP Macro (`dhtadm`)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type a command of the following format:**

   ```
   # dhtadm -D -m macroname
   ```

   For example, to delete macro `bluenote`, type the following command:

   ```
   # dhtadm -D -m bluenote
   ```

Working With DHCP Options

Options are keywords for network configuration parameters that the DHCP server can pass to clients. In the Solaris DHCP service, the only options that you can create, delete, or modify are those that are not specified as standard options in the Solaris DHCP service. For this reason, when you first set up your DHCP service, the Options tab in DHCP Manager is empty until you create options for your site.

If you create options on the DHCP server, you must also add information about the options on the DHCP client. For the Solaris DHCP client, you must edit the `/etc/dhcp/inittab` file to add entries for the new options. See the `dhcp_inittab` man page for more information about this file.

If you have DHCP clients that are not Solaris clients, refer to the documentation for those clients for information about adding new options or symbols. See "About Options" on page 30 for more information about options in Solaris DHCP.

You can use either DHCP Manager or the `dhtadm` command to create, modify, or delete options.

Note – Options are called *symbols* in the DHCP literature. The `dhtadm` command and man page also refer to options as symbols.

The following task map lists tasks you must perform to create, modify, and delete DHCP options and the procedures needed to carry them out.

TABLE 4–8 DHCP Options Task Map

Tasks	Description	Where to Find Instructions
Create DHCP options.	Add new options for information not covered by a standard DHCP option.	"How to Create DHCP Options (DHCP Manager)" on page 118 "How to Create DHCP Options (`dhtadm`)" on page 119 "Modifying the Solaris DHCP Client's Option Information" on page 122
Modify DHCP options.	Change properties of DHCP options you have created.	"How to Modify DHCP Option Properties (DHCP Manager)" on page 120 "How to Modify DHCP Option Properties (`dhtadm`)" on page 120
Delete DHCP options.	Remove DHCP options you have created.	"How to Delete DHCP Options (DHCP Manager)" on page 121 "How to Delete DHCP Options (`dhtadm`)" on page 121

Before you create options, you should be familiar with the option properties listed in the following table.

TABLE 4–9 DHCP Option Properties

Option Properties	Description
Category	The category of an option must be one of the following: Vendor – Options specific to a client's vendor platform, either hardware or software. Site – Options specific to your site. Extend – Newer options that have been added to the DHCP protocol, but not yet implemented as standard options in Solaris DHCP.
Code	The code is a unique number you assign to an option. The same code cannot be used for any other option within its option category. The code must be appropriate for the option category: Vendor – Code values of 1–254 for each vendor class Site – Code values of 128–254 Extend – Code values of 77-127

TABLE 4–9 DHCP Option Properties *(Continued)*

Option Properties	Description
Data type	The data type specifies what kind of data can be assigned as a value for the option. Valid data types are: ASCII – Text string value. BOOLEAN – No value is associated with the Boolean data type. The presence of the option indicates a condition is true, while the absence of the option indicates false. For example, the Hostname option (which is a Standard option and cannot be modified) is a Boolean. If it is included in a macro, it tells the DHCP server that it should consult name services to see if there is a host name associated with the assigned address. IP – One or more IP addresses, in dotted decimal format (*xxx.xxx.xxx.xxx*). OCTET – Uninterpreted hexadecimal ASCII representation of binary data. For example, a client ID uses the octet data type. UNUMBER8, UNUMBER16, UNUMBER32, UNUMBER64, SNUMBER8, SNUMBER16, SNUMBER32, or SNUMBER64 – Numeric value. An initial U or S indicates whether the number is unsigned or signed, and the digits at the end indicates the amount of bits in the number.
Granularity	Specifies how many "instances" of the data type are needed to represent a complete option value. For example, a data type of IP and a granularity of 2 would mean that the option value must contain two IP addresses.
Maximum	The maximum number of values that can be specified for the option. Building on the previous example, a maximum of 2, with a granularity of 2 and a data type of IP Address would mean that the option value could contain a maximum of two pairs of IP addresses.

TABLE 4–9 DHCP Option Properties *(Continued)*

Option Properties	Description
Vendor client classes	This option is available only when the option category is Vendor. It identifies the client class(es) with which the Vendor option is associated. The Class is an ASCII string that represents the client machine type and/or operating system, for example, `SUNW.Ultra5_10`. This type of option makes it possible to define configuration parameters that are passed to all clients of the same class, and *only* clients of that class. You can specify multiple client classes. Only those DHCP clients with a client class value that matches one you specify will receive the options scoped by that class. The client class is determined by the vendor of the DHCP client. For DHCP clients that are not Solaris clients, refer to the vendor documentation for the DHCP client for the client class. For Solaris clients, the Vendor client class can be obtained by typing `uname -i` on the client. To specify the Vendor client class, substitute periods for any commas in the string returned by the `uname` command. For example, if the string `SUNW,Ultra5_10` is returned by the `uname -i` command, you should specify the Vendor client class as `SUNW.Ultra5_10`.

Creating DHCP Options

If you need to pass client information for which there is not already an existing option in the DHCP protocol, you can create an option. See the `dhcp_inittab` man page for a list of all the options that are defined in Solaris DHCP before you create your own.

You can use the `dhtadm -A -s` command or DHCP Manager's Create Option dialog box to create new options.

The following figure shows DHCP Manager's Create Option dialog box.

FIGURE 4–17 Create Option Dialog Box

▼ How to Create DHCP Options (DHCP Manager)

1. **Select the Options tab.**
2. **Choose Create from the Edit menu.**

   The Create Options dialog box opens.

3. **Type a short descriptive name for the new option.**

   The name may contain up to 128 alphanumeric characters including spaces.

4. **Type or select values for each setting in the dialog box.**

   Refer to Table 4–9 for information about each setting.

5. **Select Notify DHCP Server of Change if you are finished creating options.**

6. **Click OK.**

   You can now add the option to macros and assign a value to the option to pass to clients.

▼ How to Create DHCP Options (`dhtadm`)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type a command using the following format:**

   ```
   # dhtadm -A -s option-name-d 'category,code,data-type,granularity,maximum'
   ```

   where

   option-name is an alphanumeric string of 128 characters or less.

   category is `Site`, `Extend`, or `Vendor=`*list-of-classes*, and *list-of-classes* is a space-separated list of vendor client classes to which the option applies. See Table 4–9 for information about how to determine the vendor client class.

   code is a numeric value appropriate to the option category, as explained in Table 4–9.

   data-type is a keyword that indicates the type of data passed with the option, as explained in Table 4–9.

   granularity is a nonnegative number, as explained in Table 4–9.

   maximum is a nonnegative number, as explained in as explained in Table 4–9.

   The following two commands are examples:

   ```
   # dhtadm -A -s NewOpt -d 'Site,130,UNUMBER8,1,1'
   ```

   ```
   # dhtadm -A -s NewServ -d 'Vendor=SUNW.Ultra-1 \
   SUNW.SPARCstation10,200,IP,1,1'
   ```

Modifying DHCP Options

If you have created options for your DHCP service, you can change the properties for an option by using either DHCP Manager or the `dhtadm` command.

You can use the `dhtadm -M -s` command or DHCP Manager's Option Properties dialog box to modify options.

Note that you should modify the Solaris DHCP client's option information to reflect the same modification you make to the DHCP service. See "Modifying the Solaris DHCP Client's Option Information" on page 122.

The following figure shows DHCP Manager's Option Properties dialog box.

FIGURE 4–18 Option Properties Dialog Box

▼ How to Modify DHCP Option Properties (DHCP Manager)

1. **Select the Options tab.**
2. **Select the option whose properties you want to change.**
3. **Choose Properties from the Edit menu.**

   The Option Properties dialog box opens.
4. **Edit the properties as needed.**

   See Table 4–9 for information about the properties.
5. **Select Notify Server of Change when you are finished with options.**
6. **Click OK.**

▼ How to Modify DHCP Option Properties (`dhtadm`)

1. **Become superuser or a user assigned to the DHCP Management profile .**
2. **Type a command using the following format:**

   ```
   # dhtadm -M -s option-name-d 'category,code,data-type,granularity,maximum'
   ```

   where

option-name is the option name whose definition you want to change.

category is `Site`, `Extend`, or `Vendor=`*list-of-classes*, and *list-of-classes* is a space-separated list of vendor client classes to which the option applies. For example, `SUNW.Ultra5_10 SUNW.Ultra-1 SUNWi86pc`.

code is a numeric value appropriate to the option category, as explained in Table 4–9.

data-type is a keyword that indicates the type of data passed with the option, as explained in Table 4–9.

granularity is a nonnegative number, as explained in Table 4–9.

maximum is a nonnegative number, as explained in as explained in Table 4–9.

Note that you must specify all of the DHCP option properties with the `-d` switch, not just the properties you want to change.

The following two commands are examples:

```
# dhtadm -M -s NewOpt -d 'Site,135,UNUMBER8,1,1'
# dhtadm -M -s NewServ -d 'Vendor=SUNW.Ultra-1 \
SUNW.i86pc,200,IP,1,1'
```

Deleting DHCP Options

You cannot delete standard DHCP options, but if you have defined options for your DHCP service, you can delete them by using DHCP Manager or the `dhtadm` command.

How to Delete DHCP Options (DHCP Manager)

1. **Select the Options tab.**
2. **Choose Delete from the Edit menu.**

   The Delete Options dialog box opens.
3. **Confirm the deletion by clicking OK.**

How to Delete DHCP Options (`dhtadm`)

1. **Become superuser or a user assigned to the DHCP Management profile .**
2. **Type a command using the following format:**

```
# dhtadm -D -s option-name
```

Modifying the Solaris DHCP Client's Option Information

If you add a new DHCP option to your DHCP server, you must add a complementary entry to each DHCP client's option information. If you are have a DHCP client that is not a Solaris DHCP client, refer to that client's documentation for information about adding options or symbols.

On a Solaris DHCP client, you must edit the `/etc/dhcp/inittab` file and add an entry for each option that you add to the DHCP server. If you later modify the option on the server, you must also modify the entry in the client's `/etc/dhcp/inittab` file.

Refer to the `dhcp_inittab` man page for detailed information about the syntax of the `/etc/dhcp/inittab` file.

Note – If you added DHCP options to the `dhcptags` file in a previous release of Solaris DHCP, you must add the options to the `/etc/dhcp/inittab` file. See "DHCP Option Information" on page 167 for more information.

Supporting Solaris Network Booting and Installation with the DHCP Service

You can use DHCP to install the Solaris operating environment on certain client systems on your network. Only Sun Enterprise Ultra systems and Intel systems that meet the hardware requirements for running the Solaris operating environment can use this feature.

For information about supporting diskless clients, see "Supporting Remote Boot and Diskless Boot Clients" on page 130.

The following task map shows the high-level tasks that must be performed to enable clients to obtain installation parameters using DHCP.

TABLE 4–10 DHCP Network Installation Task Map

Task	Description	Where to Find Instructions
Set up an install server.	Set up a Solaris server to support clients that want to install the Solaris operating environment from the network.	"Preparing to Install Solaris Software From the Network" in *Solaris 8 Advanced Installation Guide*
Set up client systems for Solaris installation over the network using DHCP.	Use `add_install_client -d` to add DHCP network installation support for a class of client (such as those of a certain machine type) or a particular client ID.	"Preparing to Install Solaris Software From the Network" in *Solaris 8 Advanced Installation Guide* `add_install_client`(1M)
Create DHCP options for installation parameters and macros that include the options.	Use DHCP Manager or `dhtadm` to create new Vendor options and macros which the DHCP server can use to pass installation information to the clients.	"Creating DHCP Options and Macros for Solaris Installation Parameters" on page 123

Creating DHCP Options and Macros for Solaris Installation Parameters

When you add clients with the `add_install_client -d` script on the install server, the script reports DHCP configuration information to standard output. This information can be used when you create the options and macros needed to pass network installation information to clients.

To support clients that require Solaris installation from the network, you must create Vendor category options to pass information that is needed to correctly install the Solaris operating environment. The following table shows the options you must create and the properties needed to create them.

TABLE 4–11 Values for Creating Vendor Category Options for Solaris Clients

Name	Code	Data Type	Granularity	Maximum	Vendor Client Classes *	Description

`SrootOpt`	1	ASCII text	1	0	`SUNW.Ultra-1,`
					`SUNW.Ultra-30,`
					`SUNW.i86pc`
						NFS mount options for the client's root file system

TABLE 4–11 Values for Creating Vendor Category Options for Solaris Clients *(Continued)*

Name	Code	Data Type	Granularity	Maximum	Vendor Client Classes *	Description
`SrootIP4`	2	IP address	1	1	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	IP address of root server
`SrootNM`	3	ASCII text	1	0	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	Host name of root server
`SrootPTH`	4	ASCII text	1	0	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	Path to the client's root directory on the root server
`SswapIP4`	5	IP address	1	0	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	IP address of swap server
`SswapPTH`	6	ASCII text	1	0	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	Path to the client's swap file on the swap server
`SbootFIL`	7	ASCII text	1	0	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	Path to the client's boot file
`Stz`	8	ASCII text	1	0	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	Time zone for client
`SbootRS`	9	NUMBER	2	1	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	NFS read size used by standalone boot program when it loads the kernel
`SinstIP4`	10	IP address	1	1	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	IP address of Jumpstart Install server
`SinstNM`	11	ASCII text	1	0	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	Host name of install server
`SinstPTH`	12	ASCII text	1	0	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	Path to installation image on install server
`SsysidCF`	13	ASCII text	1	0	`SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc`	Path to `sysidcfg` file, in the format *server:/path*

TABLE 4–11 Values for Creating Vendor Category Options for Solaris Clients *(Continued)*

Name	Code	Data Type	Granularity	Maximum	Vendor Client Classes *	Description
SjumpsCF	14	ASCII text	1	0	SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc	Path to JumpStart configuration file in the format *server:/path*
Sterm	15	ASCII text	1	0	SUNW.Ultra-1, SUNW.Ultra-30, SUNW.i86pc	Terminal type

* The vendor client classes determine what classes of client can use the option. Vendor client classes listed here are suggestions only. You should specify client classes that indicate the actual clients in your network that need to install from the network. See Table 4–9 for information about how to determine a client's vendor client class.

When you have created the options, you can create macros that include those options. The following table lists suggested macros you can create to support Solaris installation for clients.

TABLE 4–12 Suggested Macros to Support Network Installation Clients

Macro Name	Contains These Options and Macros
Solaris	SrootIP4, SrootNM, SinstIP4, SinstNM, Sterm
sparc	SrootPTH, SinstPTH
sun4u	Solaris and sparc macros
i86pc	Solaris macro, SrootPTH, SinstPTH, SbootFIL
SUNW.i86pc *	i86pc macro
SUNW.Ultra-1 *	sun4u macro, SbootFIL
SUNW.Ultra-30 *	sun4u macro, SbootFIL macro
xxx.xxx.xxx.xxx (network address macros)	BootSrvA option could be added to existing network address macros. The value of BootSrvA should indicate the tftboot server.

* These macro names match the Vendor client classes of the clients that will install from the network. These names are examples of clients you might have on your network. See Table 4–9 for information about determining a client's vendor client class.

You can create these options and macros by using the dhtadm command or DHCP Manager. If you use dhtadm, it is better to create the options and macros by writing a script that uses the dhtadm command repeatedly.

The following section, “Writing a Script That Uses dhtadm to Create Options and Macros” on page 126, shows a sample script that uses the dhtadm command. If you prefer to use DHCP Manager, see “Using DHCP Manager to Create Install Options and Macros” on page 128.

Writing a Script That Uses dhtadm to Create Options and Macros

You can create a Korn shell script by adapting the example in Example 4–1 to create all the options listed in Table 4–11 and some useful macros. Be sure to change all IP addresses and values contained in quotes to the correct IP addresses, server names, and paths for your network. You should also edit the Vendor= key to indicate the class of clients you have. Use the information reported by add_install_client -d to obtain the data needed to adapt the script.

EXAMPLE 4–1 Sample Script to Support Network Installation

```
# Load the Solaris vendor specific options. We’ll start out supporting
# the Ultra-1, Ultra-30, and i86 platforms. Changing -A to -M would replace
# the current values, rather than add them.
dhtadm -A -s SrootOpt -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,1,ASCII,1,0’
dhtadm -A -s SrootIP4 -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,2,IP,1,1’
dhtadm -A -s SrootNM -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,3,ASCII,1,0’
dhtadm -A -s SrootPTH -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,4,ASCII,1,0’
dhtadm -A -s SswapIP4 -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,5,IP,1,0’
dhtadm -A -s SswapPTH -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,6,ASCII,1,0’
dhtadm -A -s SbootFIL -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,7,ASCII,1,0’
dhtadm -A -s Stz -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,8,ASCII,1,0’
dhtadm -A -s SbootRS -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,9,NUMBER,2,1’
dhtadm -A -s SinstIP4 -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,10,IP,1,1’
dhtadm -A -s SinstNM -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,11,ASCII,1,0’
dhtadm -A -s SinstPTH -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,12,ASCII,1,0’
dhtadm -A -s SsysidCF -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,13,ASCII,1,0’
dhtadm -A -s SjumpsCF -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,14,ASCII,1,0’
dhtadm -A -s Sterm -d ’Vendor=SUNW.Ultra-1 SUNW.Ultra-30 SUNW.i86pc,15,ASCII,1,0’
# Load some useful Macro definitions
# Define all Solaris-generic options under this macro named Solaris.
dhtadm -A -m Solaris -d ’:SrootIP4=188.21.0.2:SrootNM="blue2":SinstIP4=188.21.0.2:\
SinstNM="red5":Sterm="xterm":’
# Define all sparc-platform specific options under this macro named sparc.
dhtadm -A -m sparc -d ’:SrootPTH="/export/sparc/root":SinstPTH="/export/sparc/install":’
# Define all sun4u architecture-specific options under this macro named sun4u. (Includes
# Solaris and sparc macros.)
dhtadm -A -m sun4u -d ’:Include=Solaris:Include=sparc:’
# Solaris on IA32-platform-specific parameters are under this macro named i86pc.
dhtadm -A -m i86pc -d \
’:Include=Solaris:SrootPTH="/export/i86pc/root":SinstPTH="/export/i86pc/install"\
:SbootFIL="/platform/i86pc/kernel/unix":’
# Solaris on IA32 machines are identified by the "SUNW.i86pc" class. All
# clients identifying themselves as members of this class will see these
# parameters in the macro called SUNW.i86pc, which includes the i86pc macro.
dhtadm -A -m SUNW.i86pc -d ’:Include=i86pc:’
# Ultra-1 platforms identify themselves as part of the "SUNW.Ultra-1" class.
# By default, we boot these machines in 32bit mode. All clients identifying
# themselves as members of this class will see these parameters.
dhtadm -A -m SUNW.Ultra-1 -d ’:SbootFIL="/platform/sun4u/kernel/unix":Include=sun4u:’
# Ultra-30 platforms identify themselves as part of the "SUNW.Ultra-30" class.
# By default, we will boot these machines in 64bit mode. All clients
# identifying themselves as members of this class will see these parameters.
dhtadm -A -m SUNW.Ultra-30 -d ’:SbootFIL="/platform/sun4u/kernel/sparcv9/unix":Include=sun4u:’
# Add our boot server IP to each of the network macros for our topology served by our
# DHCP server. Our boot server happens to be the same machine running our DHCP server.
dhtadm -M -m 188.20.64.64 -e BootSrvA=188.21.0.2
dhtadm -M -m 188.20.64.0 -e BootSrvA=188.21.0.2
dhtadm -M -m 188.20.64.128 -e BootSrvA=188.21.0.2
dhtadm -M -m 188.21.0.0 -e BootSrvA=188.21.0.2
dhtadm -M -m 188.22.0.0    -e BootSrvA=188.21.0.2
# Make sure we return host names to our clients.
dhtadm -M -m DHCP-servername -e Hostname=_NULL_VALUE_
# The client with this MAC address is a diskless client. Override the root settings
# which at the network scope setup for Install with our client’s root directory.
dhtadm -A -m 0800201AC25E -d \
```

EXAMPLE 4–14 Sample Script to Support Network Installation *(Continued)*

```
=188.23.128.12":SrootNM="...":SrootPTH="/export/root/188.23.128.12":'
```

As superuser, execute `dhtadm` in batch mode and specify the name of the script to add the options and macros to your `dhcptab`. For example, if your script is named `netinstalloptions`, type the command:

```
dhtadm -B netinstalloptions
```

When you have done this, clients that have vendor client classes that are listed in the `Vendor=` string can use DHCP to obtain the parameters they need for Solaris installation over the network.

Using DHCP Manager to Create Install Options and Macros

You can create the options listed in Table 4–11 and the macros listed in Table 4–12 with DHCP Manager.

See Figure 4–17 and Figure 4–16 for illustrations of the dialog boxes you use to create options and macros.

▼ How to Create Options to Support Solaris Installation (DHCP Manager)

1. **Select the Options tab in DHCP Manager.**
2. **Choose Create from the Edit menu.**

   The Create Option dialog box opens.
3. **Type the option name for the first option and type values appropriate for that option.**

   Use Table 4–11 to look up the option names and values for options you must create. Notice that the vendor client classes are only suggested values. You should create classes to indicate the actual client types that need to obtain Solaris installation parameters from the DHCP service. See Table 4–9 for information about how to determine a client's vendor client class.
4. **Click OK when you have entered all the values.**
5. **In the Options tab, select the option you just created.**
6. **Select Duplicate from the Edit menu.**

   The Duplicate Option dialog box opens.
7. **Type the name of another option and modify other values appropriately.**

The values for code, data type, granularity, and maximum are most likely to need modification. See Table 4–11 for the values.

8. **Repeat Step 5 through Step 7 until you have created all the options.**

   You can now create macros to pass the options to network installation clients, as explained in the following procedure.

Note – You do not need to add these options to a Solaris client's `/etc/dhcp/inittab` file because they are already included in that file.

▼ How to Create Macros to Support Solaris Installation (DHCP Manager)

1. **Select the Macros tab in DHCP Manager.**
2. **Choose Create from the Edit menu.**

   The Create Macro dialog box opens.
3. **Type the name of a macro.**

   See Table 4–12 for macro names you might use.
4. **Click the Select button.**

   The Select Option dialog box opens.
5. **Select Vendor in the Category list.**

   The Vendor options you created are listed.
6. **Select an option you want to add to the macro and click OK.**
7. **Type a value for the option.**

   See Table 4–11 for the option's data type and refer to the information reported by `add_install_client -d`.
8. **Repeat Step 6 through Step 7 for each option you want to include.**

   To include another macro, type **`Include`** as the option name and type the macro name as the option value.
9. **Click OK when the macro is complete.**

Supporting Remote Boot and Diskless Boot Clients

The Solaris DHCP service can support Solaris client systems that mount their operating system files remotely from another machine, called the OS server. Such clients are often called diskless clients. They can be thought of as persistent remote boot clients in that each time they boot, they must obtain the name and IP address of the server that hosts their operating system files, and then boot remotely from those files.

Each diskless client has its own root partition on the OS server, which is shared to the client host name. This means that the DHCP server must always return the same IP address to the client, and that address must remain mapped to the same host name in the name service (such as DNS). To accomplish this, each diskless client must be assigned a consistent IP address.

In addition to the IP address and host name, the DHCP server can supply a diskless client with all the information needed to locate its operating system files on the OS server. However, you must create options and macros that can be used to pass the information in a DHCP message packet.

The following task map lists the tasks required to support diskless clients or any other persistent remote boot clients, and includes links to procedures to help you carry them out.

TABLE 4–13 Task Map for Supporting Diskless Boot Clients with DHCP

Task	Description	Where to Find Instructions
Set up OS services on a Solaris server.	Use the `smosservice` command to create operating system files for clients.	"Managing Diskless Clients" in *Solaris 8 System Administration Supplement* in the Solaris 4/01 Update Collection. Also see the `smosservice` man page.
Set up DHCP Service to support network boot clients	Use DHCP Manager or `dhtadm` to create new Vendor options and macros which the DHCP server can use to pass booting information to the clients. Note that if you already created the options for network install clients, you need only create macros for the Vendor client types of the diskless clients.	"Supporting Solaris Network Booting and Installation with the DHCP Service" on page 122

TABLE 4–13 Task Map for Supporting Diskless Boot Clients with DHCP *(Continued)*

Task	Description	Where to Find Instructions
Assign reserved IP addresses to the diskless clients.	Use DHCP Manager or `pntadm` to mark addresses reserved (or manual) for diskless clients.	"Setting Up DHCP Clients for a Consistent IP Address" on page 106
Set up diskless clients for OS service	Use the `smdiskless` command to add operating system support on the OS server for each client. Specify the IP addresses you reserved for each client.	"Managing Diskless Clients" in *Solaris 8 System Administration Supplement* in the Solaris 4/01 Update Collection. Also see the `smdiskless` man page

Setting Up DHCP Clients as NIS+ Clients

You can use the NIS+ name service on Solaris systems that are DHCP clients, but to do so requires you to partially circumvent one of the security-enhancing features of NIS+ - the creation of DES credentials. When you set up a NIS+ client that is *not* using DHCP, you add unique DES credentials for the new NIS+ client system to the `cred` table on the NIS+ server. There are several ways to accomplish this, such as using the `nisclient` script or the `nisaddcred` command.

For DHCP clients, you *cannot* use these methods because they depend on a static host name to create and store the credentials. If you want to use NIS+ and DHCP, you must create identical credentials to be used for all the host names of DHCP clients. In this way, no matter what IP address (and associated host name) a DHCP client receives, it can use the same DES credentials.

Note – Before you do this, remember that NIS+ was designed with security in mind, and this procedure weakens that security because it allows random DHCP clients to receive NIS+ credentials.

The following procedure shows you how to create identical credentials for all DHCP host names. This procedure is only valid if you know the host names that DHCP clients will use, such as when the host names are generated by the DHCP server.

▼ How to Set Up Solaris DHCP Clients as NIS+ Clients

A DHCP client workstation that is to be a NIS+ client must use credentials copied from another NIS+ client workstation in the NIS+ domain. This procedure only produces credentials for the workstation, which apply only to the superuser logged in to the workstation. Other users logged in to the DHCP client workstation must have their own unique credentials in the NIS+ server, created according to the procedure in the *Solaris Naming Administration Guide.*

1. **Type the following command on the NIS+ server to write the `cred` table entry for the NIS+ client to a temporary file.**

   ```
   # nisgrep nisplus-client-name cred.org_dir > /tmp/file
   ```

2. **View the contents of the temporary file so you can copy the credentials and use them to create credentials for DHCP clients.**

   You must copy the public key and private key, which are long strings of numbers and letters separated by colons.

3. **Type the following commands to add credentials for a DHCP client. Copy the public and private key information from the temporary file.**

   ```
   # nistbladm -a cname=" dhcp-client-name@nisplus-domain" auth_type=DES \
   auth_name="unix.dhcp-client-name@nisplus-domain" \
   public_data=copied-public-data \
   private_data=copied-private-data
   ```

4. **Type the following commands on each DHCP client system to remote copy NIS+ client files to the DHCP client system.**

   ```
   # rcp nisplus-client-name:/var/nis/NIS_COLD_START /var/nis
   # rcp nisplus-client-name:/etc/.rootkey /etc
   # rcp nisplus-client-name:/etc/defaultdomain /etc
   ```

   If you get a “permission denied” message, the systems may not be set up to allow remote copying. You can copy the files as a regular user to an intermediate location and then copy them to the proper location as root on the DHCP client systems.

5. **Type the following command on the DHCP client system to use the correct name service switch file for NIS+:**

   ```
   # cp /etc/nisswitch.nisplus /etc/nisswitch.conf
   ```

6. **Reboot the DHCP client system.**

   The DHCP client system should now be able to use NIS+ services.

Example – Setting up a Solaris DHCP Client as an NIS+ Client

The following example assumes that you have one workstation, `nisei`, which is a NIS+ client in the NIS+ domain `dev.purple.net`, and one DHCP client, `dhow`, that you want to be a NIS+ client.

```
    (first log in as root on the NIS+ server)
# nisgrep nisei cred.org_dir > /tmp/nisei-cred
# cat /tmp/nisei-cred
nisei.dev.purple.net.:DES:unix.nisei@dev.purple.net:46199279911a84045b8e0
c76822179138173a20edbd8eab4:90f2e2bb6ffe7e3547346dda624ec4c7f0fe1d5f37e21cff63830
c05bc1c724b
# nistbladm -a cname="dhow@dev.purple.net." \
auth_type=DES auth_name="unix.dhow@dev.purple.net" \
public_data=46199279911a84045b8e0c76822179138173a20edbd8eab4 \
private_data=90f2e2bb6ffe7e3547346dda624ec4c7f0fe1d5f37e21cff63830\
c05bc1c724b
# rlogin dhow
    (log in as root on dhow)
# rcp nisei:/var/nis/NIS_COLD_START /var/nis
# rcp nisei:/etc/.rootkey /etc
# rcp nisei:/etc/defaultdomain /etc
# cp /etc/nisswitch.nisplus /etc/nisswitch.conf
# reboot
```

The DHCP client system dhow should now be able to use NIS+ services.

Adding Credentials With a Script

If you want to set up a large number of DHCP clients as NIS+ clients, you can write a script to quickly add the entries to the `cred` table. The following sample shows how this might be done.

EXAMPLE 4–2 Sample Script for Adding Credentials for DHCP Clients

```
#! /usr/bin/ksh
#
# Copyright (c) by Sun Microsystems, Inc. All rights reserved.
#
# Sample script for cloning a credential. Hosts file is already populated
# with entries of the form dhcp-[0-9][0-9][0-9]. The entry we're cloning
# is dhcp-001.
#
#
PUBLIC_DATA=6e72878d8dc095a8b5aea951733d6ea91b4ec59e136bd3b3
PRIVATE_DATA=3a86729b685e2b2320cd7e26d4f1519ee070a60620a93e48a8682c5031058df4
HOST="dhcp-"
DOMAIN="mydomain.nisplus.com"

for
i in 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019
```

EXAMPLE 4–2 Sample Script for Adding Credentials for DHCP Clients *(Continued)*

```
do
     print - ${HOST}${i}
     #nistbladm -r [cname="${HOST}${i}.${DOMAIN}."]cred.org_dir
     nistbladm -a cname="${HOST}${i}.${DOMAIN}." \
                       auth_type=DES auth_name="unix.${HOST}${i}@${DOMAIN}" \
                       public_data=${PUBLIC_DATA} private_data=${PRIVATE_DTA} cred.org_Dir
done

exit 0
```

Converting to a New Data Store

Solaris DHCP provides a utility to convert the DHCP configuration data from one data store to another. You may need to convert to a new data store if, for example, your number of DHCP clients increases to the point that you need higher performance or higher capacity from the DHCP service, or if you want to share the DHCP server duties among multiple servers. See "Choosing the Data Store" on page 44 for a comparison of the relative benefits and drawbacks of each type of data store.

Note – If you upgraded to Solaris 8 7/01 on the DHCP server system, the first time you run any Solaris DHCP management tool after Solaris installation, you are prompted to convert your data store. The conversion is required because the format of the data stored in both files and NIS+ has changed. If you do not convert your data store, the DHCP server continues to read the old data store to extend leases for existing clients. You cannot register new DHCP clients or use management tools with the old data store.

The conversion utility is also useful for sites converting from a Sun-provided data store to a third-party data store. The conversion utility looks up entries in the existing data store and adds new entries that contain the same data to the new data store. Data store access is implemented in separate modules for each data store, which enables the conversion utility to convert DHCP data from any data store format to any other data store format, provided each data store has a module. See *Solaris DHCP Service Developer's Guide* for more information about how to write a module to support a third-party data store.

The data store conversion can be accomplished with DHCP Manager through the Data Store Conversion wizard, or with the `dhcpconfig -C` command.

The initial dialog box of the Data Store Conversion wizard is shown in the following figure.

FIGURE 4–19 Data Store Conversion Wizard Dialog Box

Before the conversion begins, you must specify whether to save the old data store's tables (`dhcptab` and network tables) . The conversion utility then stops the DHCP server, converts the data store, and restarts the server when the conversion has completed successfully. If you did not specify to save the old tables, the utility deletes them after it determines the conversion is successful. The process of converting can be time-consuming, so the conversion runs in the background with a meter to inform you of its progress.

How to Convert the DHCP Data Store (DHCP Manager)

1. **Choose Convert Data Store from the Service menu.**

   The Data Store Conversion wizard opens.

2. **Answer the wizard's prompts.**

   If you have trouble providing the requested information, click Help to view detailed information about each dialog box.

How to Convert the DHCP Data Store (`dhcpconfig -C`)

1. **Become superuser or a user assigned to the DHCP Management profile .**

2. **Type a command of the following format:**

   ```
   # /usr/sbin/dhcpconfig -C -r resource -p path
   ```

   where *resource* is the data store (such as `SUNWbinfiles`) and *path* is the path to the data (such as `/var/dhcp`).

   Note that if you want to keep the original data (in the old data store) after the conversion, specify the `-k` option.

Moving Configuration Data Between DHCP Servers

The DHCP Manager and `dhcpconfig` utilities enable you to move some or all the DHCP configuration data from one Solaris DHCP server to another. You can move entire networks and all the addresses, macros, and options associated with it, or select specific IP addresses, macros, and options to move. You can also copy useful macros or options without removing them from the first server when you specify to keep the data on the server.

You might want to move data if you are going to do any of the following tasks:

- Add a server to share DHCP duties
- Replace the DHCP server's system
- Change the path for the data store (while still using the same data store)

Moving DHCP configuration data is a three-part process in which you:

1. Export the data from the first server
2. Import the data to the second server
3. Modify the imported data for the new server environment

In DHCP Manager, you use the Export Data wizard and Import Data wizard to move the data from one server to the other, and modify macros in the Macros tab, as explained in "How to Move Configuration Data Between DHCP Servers (DHCP Manager)" on page 137. The following figures show the initial dialog boxes for the wizards.

FIGURE 4–20 Export Data Wizard Dialog Box

FIGURE 4–21 Import Data Wizard Dialog Box

If you prefer to use commands, export the data by using `dhcpconfig -E`, then import by using `dhcpconfig -I`. Modify the network tables by using `pntadm` and macros by using `dhtadm` as explained in "How to Move Configuration Data Between DHCP Servers (`dhcpconfig`)" on page 138.

▼ How to Move Configuration Data Between DHCP Servers (DHCP Manager)

1. **Become superuser on the server from which you want to move or copy data.**

2. **Choose Export Data on the Service menu.**

3. **Answer the wizard's prompts.**

   If you have difficulty, click Help for detailed information about the prompts.

4. **Move the export file to a file system that is accessible to the DHCP server to which you want to move the data.**

5. **Become superuser on the server to which you want to move the data.**

6. **In DHCP Manager, choose Import Data from the Service menu.**

7. **Answer the wizard's prompts.**

   If you have difficulty, click Help for detailed information about the prompts.

8. **When the data is imported, examine imported data for network–specific information that needs modification.**

   For example, if you moved networks, you must open the Addresses tab and change the owning server of addresses in the imported networks. You might also need to open the Macros tab to specify the correct domain names for NIS, NIS+ or DNS in the macros that specify them.

9. **Open the Addresses tab and select a network that you imported.**

10. **To select all the addresses, click the first address, press and hold the Shift key, and click the last address.**

11. **From the Edit menu, choose Properties.**

    The Modify Multiple Addresses dialog box opens.

12. **At the Managing Server prompt, select the new server's name.**

13. **At the Configuration Macro prompt, select the macro that should be used for all clients on this network.**

14. **Click OK.**

15. **Open the Macros tab.**

16. **Use the Find facility at the bottom of the window to locate the options that are likely to need modified values.**

    `DNSdmain`, `DNSserv`, `NISservs`, `NIS+serv`, and `NISdmain` are examples of options that might need modification on the new server.

17. **When you locate an option that needs to be changed, select the macro name and choose Properties from the Edit menu and change its value.**

▼ How to Move Configuration Data Between DHCP Servers (dhcpconfig)

1. **Become superuser on the server from which you want to move or copy data.**

2. **Type a command of the following format:**

   ```
   # /usr/sbin/dhcpconfig -X filename -a network-addresses -m macros -o options
   ```

   where *filename* is the full path name you want to use to store the compressed exported data. You can use the keyword ALL with the command options to export all the networks, macros, or options. For example:

   ```
   # /usr/sbin/dhcpconfig -X dhcp2465_data -a ALL -m ALL -o ALL
   ```

   Alternatively, you can specify particular network addresses, macros, and configuration options in comma-separated lists. For example:

   ```
   # /usr/sbin/dhcpconfig -X dhcp2465_data -a 24.63.0.0,24.62.0.0 \
   -m 24.63.0.0,24.62.0.0,SUNW.Ultra-5_10 -o Sterm
   ```

   See the dhcpconfig man page for more information about the dhcpconfig command.

3. **Move the file that contains the exported data to a location that is accessible to the server to which you want to move the data.**

4. **Become superuser on the server to which you want to import the data.**

5. **Type a command of the following format:**

   ```
   # /usr/sbin/dhcpconfig -I filename
   ```

   where *filename* is the name of the file that contains the data exported from the first server.

6. **When the import is completed, examine the network tables for data that needs to be modified.**

   If you moved networks, use pntadm -P *network_address* to print out the network tables for the networks you moved. You might need to change the owning server and the configuration macro used for these addresses. For example, to change the owning server (24.60.3.4) and macro (dhcpsrv-2460) for address 24.63.0.2, you would use the following command:

   ```
   pntadm -M 24.63.0.2 -s 24.60.3.4 -m dhcpsrv-2460 24.60.0.0
   ```

   If you have a large number of addresses, you should create a script file that contains commands to modify each address, and then execute the script with the pntadm -B command, which runs pntadm in batch mode. See the pntadm man page.

7. **Examine the `dhcptab` macros for options with values that need modification.**

   Use `dhtadm -P` to print the entire `dhcptab`, and use `grep` or some other tool to search for particular options or values that you might want to change. Then use `dhtadm -M` to modify values. For example, you might need to modify some macros to specify the correct domain names and servers for NIS, NIS+ or DNS. For example, the following command changes the values of `DNSdmain` and `DNSserv` in the macro `mymacro`:

   ```
   dhtadm -M -m mymacro -e 'DNSserv=dnssrv2:DNSdmain=blue.net'
   ```

CHAPTER 5

Troubleshooting DHCP

This chapter provides information to help you solve problems you might encounter when you configure a DHCP server or client, or problems in using DHCP after configuration is complete.

The chapter includes the following information:

- "Troubleshooting DHCP Server Problems" on page 141
- "Troubleshooting DHCP Client Configuration Problems" on page 147

Troubleshooting DHCP Server Problems

The problems you might encounter when you configure the server fall into the following categories:

- NIS+, if you choose to use NIS+ for your data store
- IP address allocation

NIS+ Problems

If you decide to use NIS+ as the DHCP data store, problems you might encounter can be categorized as follows:

- Cannot select NIS+ as a data store
- NIS+ is not adequately configured
- NIS+ access problems due to insufficient permissions and credentials

Cannot Select NIS+ as a Data Store

If you try to use NIS+ as your data store, you might find that DHCP Manager does not offer it as a choice for data store, or `dhcpconfig` returns a message saying NIS+ does not appear to be installed and running. This means that NIS+ has not been configured for this server, although NIS+ might be in use on the network. Before you can select NIS+ as a data store, the server system must be configured as an NIS+ client.

Before you set up the server as an NIS+ client, the domain must have already been configured and its master server must be running. The master server of the domain's tables should be populated, and the hosts table must have an entry for the new client system (the DHCP server system). "Configuring NIS+ Clients" in *Solaris Naming Setup and Configuration Guide* provides detailed information about configuring an NIS+ client.

NIS+ Not Adequately Configured

After you successfully use NIS+ with DHCP, you might encounter errors if changes are made to NIS+ and introduce configuration problems. Use the following table to help you determine the cause of configuration problems.

TABLE 5–1 NIS+ Configuration Problems

Possible Problem	Gather Information	Solution
Root object does not exist in the NIS+ domain.	Enter the following command: `/usr/lib/nis/nisstat` This command displays statistics for the domain. If the root object does not exist, no statistics are returned.	Set up the NIS+ domain using the *Solaris Naming Setup and Configuration Guide*.
NIS+ is not used for `passwd` and `publickey` information.	Enter the following command to view the name service switch configuration file: `cat /etc/nsswitch.conf` Check the `passwd` and `publickey` entries for the "nisplus" keyword.	Refer to the *Solaris Naming Setup and Configuration Guide* for information about configuring the name service switch.
The domain name is empty.	Enter the following command: `domainname` If the command lists an empty string, no domain name has been set for the domain.	Use local files for your data store, or set up an NIS+ domain for your network. Refer to *Solaris Naming Setup and Configuration Guide*.

TABLE 5–1 NIS+ Configuration Problems *(Continued)*

Possible Problem	Gather Information	Solution
The `NIS_COLD_START` file does not exist.	Enter the following command on the server system to determine if the file exists: `cat /var/nis/NIS_COLD_START`	Use local files for your data store, or create an NIS+ client. Refer to *Solaris Naming Setup and Configuration Guide*.

NIS+ Access Problems

NIS+ access problems might cause error messages about incorrect DES credentials, or inadequate permissions to update NIS+ objects or tables. Use the following table to determine the cause of NIS+ errors you receive.

TABLE 5–2 NIS+ Access Problems

Possible Problem	Gather Information	Solution
The DHCP server system does not have create access to the `org_dir` object in the NIS+ domain.	Enter the following command: `nisls -ld org_dir` The access rights are listed in the form `r---rmcdrmcdr---`, where the permissions apply respectively to nobody, owner, group, and world. The owner of the object is listed next.	Use the `nischmod` command to change the permissions for `org_dir`. For example, to add create access to the group, type the following command: `nischmod g+c org_dir`
	Normally the `org_dir` directory object provides full (read, modify, create, and destroy) rights to both the owner and the group, while providing only read access to the world and nobody classes. The DHCP server name must either be listed as the owner of the `org_dir` object, or be listed as a principal in the group, and that group must have create access. List the group with the command: `nisls -ldg org_dir`	See the `nischmod`(1) man page for more information.

TABLE 5–2 NIS+ Access Problems *(Continued)*

Possible Problem	Gather Information	Solution

The DHCP server does not have access rights to create a table under the `org_dir` object.
Usually, this means the server system's principal name is not a member of the owning group for the `org_dir` object, or no owning group exists.
	Enter this command to find the owning group name:
	`niscat -o org_dir`
	Look for a line similar to
	`Group : "admin.myco.com."`
	List the principal names in the group using the command:
	`nisgrpadm -l` *groupname*
	For example:
	`nisgrpadm -l admin.myco.com`
	The server system's name should be listed as an explicit member of the group or included as an implicit member of the group.
		Add the server system's name to the group using the `nisgrpadm` command.
		For example, to add the server name `pacific` to the group `admin.myco.com`, type the following command:
		`nisgrpadm -a admin.myco.com pacific.myco.com`
		See the `nisgrpadm`(1) man page for more information.

The DHCP server does not have valid Data Encryption Standard (DES) credentials in the NIS+ `cred` table.	If this is the problem, an error message states that the user does not have DES credentials in the NIS+ name service.	Use the `nisaddcred` command to add security credentials for the DHCP server system. The following example shows how to add DES credentials for the system `mercury` in the domain `Faxco.COM`: `nisaddcred -p unix.mercury@Faxco.COM \ -P mercury.Faxco.COM. DES Faxco.COM.` The command prompts for the root password (which is required to generate an encrypted secret key). See the `nisaddcred`(1M) man page for more information.

IP Address Allocation Errors

When a client attempts to obtain or verify an IP address, you might see the problems in the following table logged to `syslog` or in server debug output.

TABLE 5–3 IP Address Allocation and Lease Problems

Error Message	Explanation	Solution
`There is no` *n.n.n.n* `dhcp-network table for DHCP client's network.`	A client is requesting a specific IP address or seeking to extend a lease on its current IP address but the DHCP server cannot find the DHCP network table for that address.	The DHCP network table might have been deleted mistakenly. You can recreate the network table by adding the network again using DHCP Manager or `dhcpconfig`.
`ICMP ECHO reply to OFFER candidate:` *n.n.n.n*`, disabling`	The IP address considered for offering to a DHCP client is already in use. This might occur if more than one DHCP server owns the address, or if an address was manually configured for a non-DHCP network client.	Determine the proper ownership of the address and correct either the DHCP server database or the host's network configuration.
`ICMP ECHO reply to OFFER candidate:` *n.n.n.n*`. No corresponding dhcp network record.`	The IP address considered for offering to a DHCP client does not have a record in a network table. This might occur if the IP address record is deleted from the DHCP network table after the address was selected but before the duplicate address check was completed.	Use DHCP Manager or `pntadm` to view the DHCP network table, and if the IP address is missing, create it with DHCP Manager (choose Create from the Edit menu on the Address tab) or `pntadm`.
`DHCP network record for` *n.n.n.n* `is unavailable, ignoring request.`	The record for the requested IP address is not in the DHCP network table, so the server is dropping the request.	Use DHCP Manager or `pntadm` to view the DHCP network table, and if the IP address is missing, create it with DHCP Manager (choose Create from the Edit menu on the Address tab) or `pntadm`.
n.n.n.n `currently marked as unusable.`	The requested IP address cannot be offered because it has been marked in the network table as unusable.	You can use DHCP Manager or `pntadm` to make the address usable.
n.n.n.n `was manually allocated. No dynamic address will be allocated.`	The client's ID has been assigned a manually allocated address, and that address is marked as unusable. The server cannot allocate a different address to this client.	You can use DHCP Manager or `pntadm` to make the address usable, or manually allocate a different address to the client.
`Manual allocation (`*n.n.n.n, client ID* `has` *n* `other records. Should have 0.`	The client that has the specified client ID has been manually assigned more than one IP address. There should be only one. The server selects the last manually assigned address it finds in the network table.	Use DHCP Manager or `pntadm` to modify IP addresses to remove the additional manual allocations.

TABLE 5–3 IP Address Allocation and Lease Problems *(Continued)*

Error Message	Explanation	Solution
`No more IP addresses on` *n.n.n.n* `network.`	All IP addresses currently managed by DHCP on the specified network have been allocated.	Use DHCP Manager or `pntadm` to create new IP addresses for this network.
`Client:` *clientid* `lease on` *n.n.n.n* `expired.`	The lease was not negotiable and timed out.	Client should automatically restart the protocol to obtain a new lease.
`Offer expired for client:` *n.n.n.n*	The server made an IP address offer to the client, but the client took too long to respond and the offer expired.	The client should automatically issue another discover message. If this also times out, increase the cache offer timeout for the DHCP server. In DHCP Manager, choose Modify from the Service menu.
`Client:` *clientid* `REQUEST is missing requested IP option.`	The client's request did not specify the offered IP address, so the DHCP server ignores the request. This might occur if the client is not compliant with the updated DHCP protocol, RFC 2131.	Update client software.
`Client:` *clientid* `is trying to renew` *n.n.n.n*`, an IP address it has not leased.`	The IP address recorded in the DHCP network table for this client does not match the IP address that the client specified in its renewal request. The DHCP server does not renew the lease.	This problem occurs if you delete a client's record while the client is still using the IP address. Use DHCP Manager or `pntadm` to examine the network table, and correct if necessary. The client's ID should be bound to the specified IP address. If it is not, edit the address properties to add the client ID.

TABLE 5–3 IP Address Allocation and Lease Problems *(Continued)*

Error Message	Explanation	Solution

`Client:` *clientid* `is trying to verify unrecorded address:` *n.n.n.n*`, ignored.`	The specified client has not been registered in the DHCP network table with this address, so the request is ignored by this DHCP server.	Another DHCP server on the network might have assigned this client the address.
		However, you might also have deleted the client's record while the client was still using the IP address.
		Use DHCP Manager or `pntadm` to examine the network table on this server and any other DHCP servers on the network and correct if necessary.
		You can also do nothing and allow the lease to expire, after which the client will automatically request a new address lease.
		If you want the client to get a new lease immediately, restart the DHCP protocol on the client by typing the following commands:
		`ifconfig` *interface* `dhcp release`
		`ifconfig` *interface* `dhcp start`

Troubleshooting DHCP Client Configuration Problems

The problems you might encounter with a DHCP client fall into the following categories:

- "Problems Communicating With DHCP Server" on page 147
- "Problems with Inaccurate DHCP Configuration Information" on page 156

Problems Communicating With DHCP Server

This section describes problems you might encounter as you add DHCP clients to the network.

After you enable the client software and reboot the system, the client tries to reach the DHCP server to obtain its network configuration. If the client fails to reach the server, you might see error messages such as:

```
DHCP or BOOTP server not responding
```

Before you can determine the problem you must gather diagnostic information from both the client and the server and analyze the information. To gather information you can:

1. Run the client in debug mode.
2. Run the server in debug mode.
3. Start `snoop` to monitor network traffic.

You can do these things separately or concurrently.

The information you gather can help you determine if the problem is with the client, server, or a relay agent, and then you can find a solution.

▼ How to Run the DHCP Client in Debug Mode

If you have a client that is not a Solaris DHCP client, refer to the client's documentation for information about how to run the client in debug mode.

If you have a Solaris DHCP client, use the following steps.

1. **Become superuser on the client system.**

2. **Type the following commands to kill the DHCP client daemon and restart it in debug mode:**

   ```
   # pkill -x dhcpagent
   # /sbin/dhcpagent -d1 -f &
   # ifconfig interface dhcp start
   ```

   When run in debug mode, the client daemon displays messages to your screen as it performs DHCP requests. See "DHCP Client Debug Output" on page 149 for information about client debug output.

▼ How to Run the DHCP Server in Debug Mode

1. **Become superuser on the server system.**

2. **Type the following commands to kill the DHCP daemon and restart it in debug mode:**

   ```
   # pkill -x in.dhcpd
   # /usr/lib/inet/in.dhcpd -d -v
   ```

   You should also use any `in.dhcpd` command-line options that you normally use when you run the daemon. For example, if you run the daemon as a BOOTP relay agent, include the `-r` option with the `in.dhcpd -d -v` command.

   When run in debug mode, the daemon displays messages to your screen as it processes DHCP/BOOTP requests. See "DHCP Server Debug Output" on page 150 for information about server debug output.

▼ How to Use snoop to Monitor DHCP Network Traffic

1. **Become superuser on the DHCP server system.**

2. **Start snoop to begin tracing network traffic across the server's network interface.**

```
# /usr/sbin/snoop -d interface -o snoop-output-filename udp port 67 or udp port 68
```

   For example:

```
# /usr/sbin/snoop -d le0 -o /tmp/snoop.output udp port 67 or udp port 68
```

   Note that snoop continues to monitor the interface until you stop it explicitly by pressing Control-C after you have the information you need.

3. **Boot the client system, or restart the dhcpagent on the client system.**

   Restarting dhcpagent is described in "How to Run the DHCP Client in Debug Mode" on page 148.

4. **On the server system, use snoop to display the output file with the contents of network packets:**

```
# /usr/sbin/snoop -i snoop-output-filename -x0 -v
```

   For example:

```
# /usr/sbin/snoop -i /tmp/snoop.output -x0 -v
```

The -d switch with the dhcpagent command puts the client in debug mode with level 1 verbosity, and the -f switch causes output to be sent to the console instead of to syslog. Replace *interface* in the ifconfig command line with the name of the network interface of the client (for example, le0).

See "DHCP snoop Output" on page 153 for information about interpreting the output.

DHCP Client Debug Output

The following example shows normal debug output when a DHCP client sends its DHCP request and receives its configuration information from a DHCP server.

EXAMPLE 5–1 Sample Normal DHCP Client Debug Output

```
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x27fc8 (DHCP filter)
/sbin/dhcpagent: debug: init_ifs: initted interface le0
/sbin/dhcpagent: debug: insert_ifs: le0: sdumax 1500, optmax 1260, hwtype 1, hwlen 6
/sbin/dhcpagent: debug: insert_ifs: inserted interface le0
/sbin/dhcpagent: debug: register_acknak: registered acknak id 5
/sbin/dhcpagent: debug: unregister_acknak: unregistered acknak id 5
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x26018 (ARP reply filter)
/sbin/dhcpagent: info: setting IP netmask on le0 to 255.255.192.0
/sbin/dhcpagent: info: setting IP address on le0 to 102.23.3.233
/sbin/dhcpagent: info: setting broadcast address on le0 to 102.23.63.255
```

EXAMPLE 5–1 Sample Normal DHCP Client Debug Output *(Continued)*

```
/sbin/dhcpagent: info: added default router 102.23.0.1 on le0
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x28054 (blackhole filter)
/sbin/dhcpagent: debug: configure_if: bound ifsp->if_sock_ip_fd
/sbin/dhcpagent: info: le0 acquired lease, expires Tue Aug 10 16:18:33 1999
/sbin/dhcpagent: info: le0 begins renewal at Tue Aug 10 15:49:44 1999
/sbin/dhcpagent: info: le0 begins rebinding at Tue Aug 10 16:11:03 1999
```

If the client cannot reach the DHCP server, you might see debug output similar to the following example.

EXAMPLE 5–2 Sample Debug Output for DHCP Client

```
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x27fc8 (DHCP filter)
/sbin/dhcpagent: debug: init_ifs: initted interface le0
/sbin/dhcpagent: debug: select_best: no valid OFFER/BOOTP reply
/sbin/dhcpagent: debug: select_best: no valid OFFER/BOOTP reply
/sbin/dhcpagent: debug: select_best: no valid OFFER/BOOTP reply
```

If you see this message, the request never reached the server, or the server cannot send a response to the client. Run `snoop` on the server as described in “How to Use `snoop` to Monitor DHCP Network Traffic” on page 149 to determine if packets from the client have reached the server.

DHCP Server Debug Output

Normal server debug output shows server configuration information followed by information about each network interface as the daemon starts. After daemon startup, the debug output shows information about requests the daemon processes. Example 5–3 shows debug output for a DHCP server that has just started and then extends the lease for a client that is using an address owned by another DHCP server that is not responding.

EXAMPLE 5–3 Sample Debug Output for DHCP Server

```
Daemon Version: 3.1
Maximum relay hops: 4
Transaction logging to console enabled.
Run mode is: DHCP Server Mode.
Datastore: nisplus
Path: org_dir.dhcp.test..:dhcp.test..:$
DHCP offer TTL: 10
Ethers compatibility enabled.
BOOTP compatibility enabled.
ICMP validation timeout: 1000 milliseconds, Attempts: 2.
Monitor (0005/hme0) started...
Thread Id: 0005 - Monitoring Interface: hme0 *****
MTU: 1500      Type: DLPI
```

EXAMPLE 5–3 Sample Debug Output for DHCP Server *(Continued)*

```
Broadcast: 102.21.255.255
Netmask: 255.255.0.0
Address: 102.21.0.2
Monitor (0006/nf0) started...
Thread Id: 0006 - Monitoring Interface: nf0 *****
MTU: 4352      Type: DLPI
Broadcast: 102.22.255.255
Netmask: 255.255.0.0
Address: 102.22.0.1
Monitor (0007/qe0) started...
Thread Id: 0007 - Monitoring Interface: qe0 *****
MTU: 1500      Type: DLPI
Broadcast: 102.23.63.255
Netmask: 255.255.192.0
Address: 102.23.0.1
Read 33 entries from DHCP macro database on Tue Aug 10 15:10:27 1999
Datagram received on network device: qe0
Client: 0800201DBA3A is requesting verification of address owned by 102.21.0.4
Datagram received on network device: qe0
Client: 0800201DBA3A is requesting verification of address owned by 102.21.0.4
Datagram received on network device: qe0
Client: 0800201DBA3A is requesting verification of address owned by 102.21.0.4
Datagram received on network device: qe0
Client: 0800201DBA3A maps to IP: 102.23.3.233
Unicasting datagram to 102.23.3.233 address.
Adding ARP entry: 102.23.3.233 == 0800201DBA3A
DHCP EXTEND 0934312543 0934316143 102.23.3.233 102.21.0.2
          0800201DBA3A SUNW.SPARCstation-10 0800201DBA3A
```

Example 5–4 shows debug output from a DHCP daemon that starts as a BOOTP relay agent and relays requests from a client to a DHCP server, and relays the servers responses to the client.

EXAMPLE 5–4 Sample Debug Output for BOOTP Relay

```
Relay destination: 102.21.0.4 (blue-servr2)     network: 102.21.0.0
Daemon Version: 3.1
Maximum relay hops: 4
Transaction logging to console enabled.
Run mode is: Relay Agent Mode.
Monitor (0005/hme0) started...
Thread Id: 0005 - Monitoring Interface: hme0 *****
MTU: 1500      Type: DLPI
Broadcast: 102.21.255.255
Netmask: 255.255.0.0
Address: 102.21.0.2
Monitor (0006/nf0) started...
Thread Id: 0006 - Monitoring Interface: nf0 *****
MTU: 4352      Type: DLPI
Broadcast: 102.22.255.255
Netmask: 255.255.0.0
```

EXAMPLE 5–4 Sample Debug Output for BOOTP Relay *(Continued)*

```
Address: 102.22.0.1
Monitor (0007/qe0) started...
Thread Id: 0007 - Monitoring Interface: qe0 *****
MTU: 1500      Type: DLPI
Broadcast: 102.23.63.255
Netmask: 255.255.192.0
Address: 102.23.0.1
Relaying request 0800201DBA3A to 102.21.0.4, server port.
BOOTP RELAY-SRVR 0934297685 0000000000 0.0.0.0 102.21.0.4 0800201DBA3A
N/A 0800201DBA3A
Packet received from relay agent: 102.23.0.1
Relaying reply to client 0800201DBA3A
Unicasting datagram to 102.23.3.233 address.
Adding ARP entry: 102.23.3.233 == 0800201DBA3A
BOOTP RELAY-CLNT 0934297688 0000000000 102.23.0.1 102.23.3.233 0800201DBA3A
N/A 0800201DBA3A
Relaying request 0800201DBA3A to 102.21.0.4, server port.
BOOTP RELAY-SRVR 0934297689 0000000000 0.0.0.0 102.21.0.4 0800201DBA3A
N/A 0800201DBA3A
Packet received from relay agent: 102.23.0.1
Relaying reply to client 0800201DBA3A
Unicasting datagram to 102.23.3.233 address.
Adding ARP entry: 102.23.3.233 == 0800201DBA3A
```

If there is a problem, the debug output might display warnings or error messages. Use Table 5–4 to find error messages and solutions.

TABLE 5–4 DHCP Server Error Messages

Message	Explanation	Solution
`ICMP ECHO reply to OFFER candidate:` *ip_address* `disabling`	Before the DHCP server offers an IP address to a client, it pings the address to verify that the address is not in use. If a client replies, the address is in use.	Make sure the addresses you configured are not already in use.
`No more IP addresses on` *network_address* `network.`	No available IP addresses in the DHCP network table associated with the client's network.	Create more IP addresses using DHCP Manager or `pntadm`. If the DHCP daemon is monitoring multiple subnets, be sure the additional addresses are for the subnet where the client is located.

TABLE 5–4 DHCP Server Error Messages *(Continued)*

Message	Explanation	Solution
`No more IP addresses for` *network_address* `network` when you are running the DHCP daemon in BOOTP compatibility mode (`-b` option).	BOOTP does not use a lease time, so the DHCP server looks for free addresses with the BOOTP flag set to allocate to BOOTP clients.	Use DHCP Manager to allocate BOOTP addresses.
`Request to access nonexistent per network database:` *database_name* `in datastore:` *datastore.*	During configuration of the DHCP server, a DHCP network table for a subnet was not created.	Use DHCP Manager or the `pntadm` to create the DHCP network table and new IP addresses.
`There is no` *table_name* `dhcp-network table for DHCP client's network.`	During configuration of the DHCP server, a DHCP network table for a subnet was not created.	Use DHCP Manager or the `pntadm` to create the DHCP network table and new IP addresses.
`Client using non_RFC1048 BOOTP cookie.`	A device on the network is trying to access an unsupported implementation of BOOTP.	Ignore this message, unless you need to configure this device.

DHCP snoop Output

In the snoop output, you should see that packets are exchanged between the DHCP client system and the DHCP server system. The IP address for each system (and any relay agents or routers in between) is indicated in each packet. If the systems do not exchange packets, the client system might not be able to contact the server system at all, and the problem is at a lower level.

To evaluate snoop output, you should know what the expected behavior is (such as if the request should be going through a BOOTP relay agent). You should also know the MAC addresses and IP address of the systems involved (and those of the network interfaces, if there is more than one) so that you can determine if those values are as expected. The following example shows normal snoop output for a DHCP acknowledgement message sent from the DHCP server on `blue-servr2` to a client whose MAC address is `8:0:20:8e:f3:7e`. In the message, the servers assigns the client the IP address `172.168.252.6` and the host name `white-6`. The message also includes a number of standard network options and several vendor-specific options for the client.

EXAMPLE 5–5 Sample snoop Output for One Packet

```
ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 26 arrived at 14:43:19.14
ETHER:  Packet size = 540 bytes
```

EXAMPLE 5–5 Sample snoop Output for One Packet *(Continued)*

```
ETHER:  Destination = 8:0:20:8e:f3:7e, Sun
ETHER:  Source      = 8:0:20:1e:31:c1, Sun
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:   ----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 526 bytes
IP:   Identification = 64667
IP:   Flags = 0x4 IP:         .1.. .... = do not fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 254 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = 157a
IP:   Source address = 102.21.0.4, blue-servr2
IP:   Destination address = 192.168.252.6, white-6
IP:   No options
IP:   UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 67
UDP:  Destination port = 68 (BOOTPC)
UDP:  Length = 506
UDP:  Checksum = 5D4C
UDP:
DHCP: ----- Dynamic Host Configuration Protocol -----
DHCP:
DHCP: Hardware address type (htype) =  1 (Ethernet (10Mb))
DHCP: Hardware address length (hlen) = 6 octets
DHCP: Relay agent hops = 0
DHCP: Transaction ID = 0x2e210f17
DHCP: Time since boot = 0 seconds
DHCP: Flags = 0x0000
DHCP: Client address (ciaddr) = 0.0.0.0
DHCP: Your client address (yiaddr) = 172.168.252.6
DHCP: Next server address (siaddr) = 102.21.0.2
DHCP: Relay agent address (giaddr) = 0.0.0.0
DHCP: Client hardware address (chaddr) = 08:00:20:11:E0:1B
DHCP:
DHCP: ----- (Options) field options -----
DHCP:
DHCP: Message type = DHCPACK
DHCP: DHCP Server Identifier = 102.21.0.4
DHCP: Subnet Mask = 255.255.255.0
DHCP: Router at = 172.168.252.1
DHCP: Broadcast Address = 172.168.252.255
DHCP: NISPLUS Domainname = dhcp.test
```

EXAMPLE 5–5 Sample `snoop` Output for One Packet *(Continued)*

```
DHCP: IP Address Lease Time = 3600 seconds
DHCP: UTC Time Offset = -14400 seconds
DHCP: RFC868 Time Servers at = 102.21.0.4
DHCP: DNS Domain Name = sem.west.dor.com
DHCP: DNS Servers at = 102.21.0.1
DHCP: Client Hostname = white-6
DHCP: Vendor-specific Options (166 total octets):
DHCP:   (02) 04 octets  0x8194AE1B (unprintable)
DHCP:   (03) 08 octets  "pacific"
DHCP:   (10) 04 octets  0x8194AE1B (unprintable)
DHCP:   (11) 08 octets  "pacific"
DHCP:   (15) 05 octets  "xterm"
DHCP:   (04) 53 octets  "/export/s28/base.s28s_nxt/latest/Solaris_8/Tools/Boot"
DHCP:   (12) 32 octets  "/export/s28/base.s28s_nxt/latest"
DHCP:   (07) 27 octets  "/platform/sun4m/kernel/unix"
DHCP:   (08) 07 octets  "EST5EDT"
  0: 0800 208e f37e 0800 201e 31c1 0800 4500    .. .ó~.. .1...E.
 16: 020e fc9b 4000 fe11 157a ac15 0004 c0a8    ....@....z......
 32: fc06 0043 0044 01fa 5d4c 0201 0600 2e21    ...C.D..]L.....!
 48: 0f17 0000 0000 0000 0000 c0a8 fc06 ac15    ................
 64: 0002 0000 0000 0800 2011 e01b 0000 0000    ........ .......
 80: 0000 0000 0000 0000 0000 0000 0000 0000    ................
 96: 0000 0000 0000 0000 0000 0000 0000 0000    ................
112: 0000 0000 0000 0000 0000 0000 0000 0000    ................
128: 0000 0000 0000 0000 0000 0000 0000 0000    ................
144: 0000 0000 0000 0000 0000 0000 0000 0000    ................
160: 0000 0000 0000 0000 0000 0000 0000 0000    ................
176: 0000 0000 0000 0000 0000 0000 0000 0000    ................
192: 0000 0000 0000 0000 0000 0000 0000 0000    ................
208: 0000 0000 0000 0000 0000 0000 0000 0000    ................
224: 0000 0000 0000 0000 0000 0000 0000 0000    ................
240: 0000 0000 0000 0000 0000 0000 0000 0000    ................
256: 0000 0000 0000 0000 0000 0000 0000 0000    ................
272: 0000 0000 0000 6382 5363 3501 0536 04ac    ......c.Sc5..6..
288: 1500 0401 04ff ffff 0003 04c0 a8fc 011c    ................
304: 04c0 a8fc ff40 0964 6863 702e 7465 7374    .....@.dhcp.test
320: 3304 0000 0e10 0204 ffff c7c0 0404 ac15    3...............
336: 0004 0f10 736e 742e 6561 7374 2e73 756e    ....sem.west.dor
352: 2e63 6f6d 0604 ac15 0001 0c07 7768 6974    .com........whit
368: 652d 362b a602 0481 94ae 1b03 0861 746c    e-6+.........pac
384: 616e 7469 630a 0481 94ae 1b0b 0861 746c    ific.........pac
400: 616e 7469 630f 0578 7465 726d 0435 2f65    ific...xterm.5/e
416: 7870 6f72 742f 7332 382f 6261 7365 2e73    xport/s28/bcvf.s
432: 3238 735f 776f 732f 6c61 7465 7374 2f53    28s_btf/latest/S
448: 6f6c 6172 6973 5f38 2f54 6f6f 6c73 2f42    olaris_x/Tools/B
464: 6f6f 740c 202f 6578 706f 7274 2f73 3238    oot. /export/s28
480: 2f62 6173 652e 7332 3873 5f77 6f73 2f6c    /bcvf.s28s_btf/l
496: 6174 6573 7407 1b2f 706c 6174 666f 726d    atest../platform
512: 2f73 756e 346d 2f6b 6572 6e65 6c2f 756e    /sun4m/kernel/un
528: 6978 0807 4553 5435 4544 54ff              ix..EST5EDT.
```

Problems with Inaccurate DHCP Configuration Information

If a DHCP client receives inaccurate information in its network configuration information, such as the wrong NIS domain name, or incorrect router IP address, you must look at the values of options in the macros that are processed by the DHCP server for this client.

Use the following general guidelines to help you determine the source of the inaccurate information.

- Look at the macros defined on the server as described in "How to View Macros Defined on a DHCP Server (DHCP Manager)" on page 109. Review the information in "Order of Macro Processing" on page 32 and determine which macros are processed automatically for this client.
- Look at the network table to determine what macro (if any) is assigned to the client's IP address as the configuration macro. See "Working With IP Addresses in the DHCP Service" on page 96 for more information.
- Take note of any options that occur in more than one macro and make sure that the value you want for an option is set in the last processed macro.
- Edit the appropriate macro(s) to assure that the correct value is passed to the client. See "Modifying DHCP Macros" on page 109.

Problems with Client-Supplied Host Name

This section describes problems you might experience with DHCP clients that supply their own host names and want the names to be registered with DNS.

Client Does Not Request a Host Name

If your client is not a Solaris DHCP client, consult the client's documentation to determine how to configure the client to request a host name. For Solaris DHCP clients, see "How to Enable a Solaris Client to Request Specific Host Name" on page 84.

DHCP Client Does Not Get Requested Host Name

TABLE 5–5 Problems and Solutions for DHCP Client Host Name Requests

Possible problem	Gather Information	Solution
Client accepted an offer from a DHCP server that does not issue DNS updates.	1. Use snoop or other network packet capture application on the client. Look for the DHCP Server Identifier to get the IP address of the server. 2. Log in to the DHCP server to verify that it is configured to make dynamic updates. Look at the /etc/inet/dhcpsvc.conf file for the entry UPDATE_TIMEOUT. 3. On the DNS server, look at the /etc/named.conf file and determine if the DHCP server's IP address is listed in the allow-update keyword in the zone section of the appropriate domain.	See "Enabling Dynamic DNS Updates by DHCP Server" on page 82 for information about configuring the DHCP server and DNS server. If two DHCP servers are available to the client, the servers should both be configured to provide the DNS updates.
Client is using FQDN option (option code 89) to specify host name. Solaris DHCP does not currently support FQDN option since it not officially in the DHCP protocol.	Use snoop or other network packet capture application on the server, and look for the FQDN option in a packet from client.	Configure the client to specify host name using Hostname option (option code 12). Refer to client documentation for instructions.
DHCP server that offers the client its address does not know the client's DNS domain.	On the DHCP server look for the DNSdmain option with a valid value.	Set the DNSdmain option to the correct DNS domain name in a macro that is processed for this client. DNSdmain is usually contained in the network macro.
Host name requested by client corresponds to an IP address that is not managed by the DHCP server. Solaris DHCP servers do not perform DNS updates for IP addresses they do not manage.	Check syslog for messages from the DHCP server similar to There is no *n.n.n.n* dhcp-network table for DHCP client's network. or DHCP network record for *n.n.n.n* is unavailable, ignoring request.	Configure the client to choose a name for which there is no corresponding IP address, or which corresponds to an address managed by the DHCP server.

TABLE 5–5 Problems and Solutions for DHCP Client Host Name Requests *(Continued)*

Possible problem	Gather Information	Solution
Host name requested by client corresponds to an IP address that is currently in use, leased, or under offer to another client.	Check `syslog` for messages from the DHCP server indicating `ICMP ECHO reply to OFFER candidate:` *n.n.n.n*.	Configure the client to choose a name corresponding to a different IP address. Alternatively, reclaim the address from the client that uses the address.
DNS server is not configured to accept updates from the DHCP server.	Examine the `/etc/named.conf` file on the DNS server and look for the DHCP server's IP address with the `allow-update` keyword in the appropriate zone section for the DHCP server's domain.	See "How to Enable Dynamic DNS Updating for DHCP Clients" on page 83 for information about configuring the DNS server. If the DHCP server has multiple interfaces, you may need to configure the DNS server to accept updates from all of the DHCP server's addresses. Enable debugging on the DNS server to see whether the updates are reaching the DNS server; if they are, examine the debugging output to determine why the updates did not occur.
DNS updates may not have completed in the allotted time. DHCP servers do not return host names to clients if the DNS updates have not completed by the configured time limit. However, attempts to complete the DNS updates continue.	Use the `nslookup` command to determine whether the updates completed successfully. See `nslookup`(1M) man page. For example, if the DNS domain is `hills.oneonta.org`, the DNS server's IP address is 121.76.178.11, and the host name the client wants to register is `cathedral`, you could use the following command to determine if `cathedral` has been registered with DNS: `nslookup cathedral.hills.oneonta.org 121.76.178.11`	If the updates completed successfully, but not in the allotted time, you need to increase the timeout value. See Step 5 in the procedure for enabling DNS updates.

CHAPTER 6

DHCP Reference

This chapter explains the relationships between files and the commands that use the files, but does not explain how to use the commands.

DHCP Commands

The following table lists the commands you might find useful in managing DHCP on your network.

TABLE 6–1 Commands Used in DHCP

Command	Description
`dhtadm`	Used to make changes to the options and macros in the `dhcptab`. This command is most useful in scripts that you create to automate changes you need to make to your DHCP information. Use `dhtadm` with the `-P` option and pipe it through the `grep` command for a quick way to search for particular option values in the `dhcptab`.
`pntadm`	Used to make changes to the DHCP network tables that map client IDs to IP addresses and optionally associate configuration information with IP addresses.
`dhcpconfig`	Used to configure and unconfigure DHCP servers and BOOTP relay agents, convert to a different data store, and import/export DHCP configuration data.
`in.dhcpd`	The DHCP server daemon. System scripts use this command to start and stop DHCP service. You can start `in.dhcpd` with non-default options, such as `-d` for debugging.
`dhcpmgr`	The DHCP Manager, a graphical tool used to configure and manage the DHCP service. DHCP Manager is the recommended Solaris DHCP management tool.

TABLE 6–1 Commands Used in DHCP *(Continued)*

Command	Description
ifconfig	Used at system boot to assign IP addresses to network interfaces, configure network interface parameters, or both. On a Solaris DHCP client, ifconfig starts DHCP to get the parameters (including the IP address) needed to configure a network interface.
dhcpinfo	Used by system startup scripts on Solaris client systems to obtain information (such as host name) from the DHCP client daemon (dhcpagent) . You can also use dhcpinfo in scripts or at the command line to obtain specified parameter values.
snoop	Used to capture and display the contents of packets being passed across the network. snoop is useful for troubleshooting problems with the DHCP service.
dhcpagent	The DHCP client daemon, which implements the client side of the DHCP protocol.

Running DHCP Commands in Scripts

The dhcpconfig, dhtadm, and pntadm commands are optimized for use in scripts. In particular, the pntadm command is useful for creating a large number of IP address entries in a DHCP network table. The following sample script uses pntadm in batch mode to create IP addresses.

EXAMPLE 6–1 addclient.ksh Script with the pntadm Command

```
#! /usr/bin/ksh
#
# This script utilizes the pntadm batch facility to add client entries
# to a DHCP network table. It assumes that the user has the rights to
# run pntadm to add entries to DHCP network tables.

#
# Based on the nsswitch setting, query the netmasks table for a netmask.
# Accepts one argument, a dotted IP address.
#
get_netmask()
{
    MTMP=‘getent netmasks ${1} | awk ’{ print $2 }’‘
    if [ ! -z "${MTMP}" ]
    then
        print - ${MTMP}
    fi
}

#
# Based on the network specification, determine whether or not network is
# subnetted or supernetted.
# Given a dotted IP network number, convert it to the default class
# network.(used to detect subnetting). Requires one argument, the
```

EXAMPLE 6–1 `addclient.ksh` Script with the `pntadm` Command *(Continued)*

```
# network number. (e.g. 10.0.0.0) Echos the default network and default
# mask for success, null if error.
#
get_default_class()
{
    NN01=${1%%.*}
    tmp=${1#*.}
    NN02=${tmp%%.*}
    tmp=${tmp#*.}
    NN03=${tmp%%.*}
    tmp=${tmp#*.}
    NN04=${tmp%%.*}
    RETNET=""
    RETMASK=""

    typeset -i16 ONE=10#${1%%.*}
    typeset -i10 X=$((${ONE}&16#f0))
    if [ ${X} -eq 224 ]
    then
        # Multicast
        typeset -i10 TMP=$((${ONE}&16#f0))
        RETNET="${TMP}.0.0.0"
        RETMASK="240.0.0.0"
    fi
    typeset -i10 X=$((${ONE}&16#80))
    if [ -z "${RETNET}" -a ${X} -eq 0 ]
    then
        # Class A
        RETNET="${NN01}.0.0.0"
        RETMASK="255.0.0.0"
    fi
    typeset -i10 X=$((${ONE}&16#c0))
    if [ -z "${RETNET}" -a ${X} -eq 128 ]
    then
        # Class B
        RETNET="${NN01}.${NN02}.0.0"
        RETMASK="255.255.0.0"
    fi
    typeset -i10 X=$((${ONE}&16#e0))
    if [ -z "${RETNET}" -a ${X} -eq 192 ]
    then
        # Class C
        RETNET="${NN01}.${NN02}.${NN03}.0"
        RETMASK="255.255.255.0"
    fi
    print - ${RETNET} ${RETMASK}
    unset NNO1 NNO2 NNO3 NNO4 RETNET RETMASK X ONE
}

#
# Given a dotted form of an IP address, convert it to its hex equivalent.
#
convert_dotted_to_hex()
```

EXAMPLE 6–1 `addclient.ksh` Script with the `pntadm` Command *(Continued)*

```
{
    typeset -i10 one=${1%%.*}
    typeset -i16 one=${one}
    typeset -Z2 one=${one}
    tmp=${1#*.}

    typeset -i10 two=${tmp%%.*}
    typeset -i16 two=${two}
    typeset -Z2 two=${two}
    tmp=${tmp#*.}

    typeset -i10 three=${tmp%%.*}
    typeset -i16 three=${three}
    typeset -Z2 three=${three}
    tmp=${tmp#*.}

    typeset -i10 four=${tmp%%.*}
    typeset -i16 four=${four}
    typeset -Z2 four=${four}

     hex=‘print - ${one}${two}${three}${four} | sed -e ’s/#/0/g’‘
     print - 16#${hex}
     unset one two three four tmp
}

#
# Generate an IP address given the network address, mask, increment.
#
get_addr()
{
    typeset -i16 net=‘convert_dotted_to_hex ${1}‘
    typeset -i16 mask=‘convert_dotted_to_hex ${2}‘
    typeset -i16 incr=10#${3}

    # Maximum legal value - invert the mask, add to net.
    typeset -i16 mhosts=~${mask}
    typeset -i16 maxnet=${net}+${mhosts}

    # Add the incr value.
    let net=${net}+${incr}

    if [ $((${net} < ${maxnet})) -eq 1 ]
    then
        typeset -i16 a=${net}\&16#ff000000
        typeset -i10 a="${a}>>24"

        typeset -i16 b=${net}\&16#ff0000
        typeset -i10 b="${b}>>16"

        typeset -i16 c=${net}\&16#ff00
        typeset -i10 c="${c}>>8"

        typeset -i10 d=${net}\&16#ff
        print - "${a}.${b}.${c}.${d}"
    fi
    unset net mask incr mhosts maxnet a b c d
}

# Given a network address and client address, return the index.
client_index()
{
    typeset -i NNO1=${1%%.*}
    tmp=${1#*.}
    typeset -i NNO2=${tmp%%.*}
    tmp=${tmp#*.}
    typeset -i NNO3=${tmp%%.*}
    tmp=${tmp#*.}
    typeset -i NNO4=${tmp%%.*}

    typeset -i16 NNF1
    let NNF1=${NNO1}
    typeset -i16 NNF2
    let NNF2=${NNO2}
    typeset -i16 NNF3
    let NNF3=${NNO3}
    typeset -i16 NNF4
    let NNF4=${NNO4}
    typeset +i16 NNF1
    typeset +i16 NNF2
    typeset +i16 NNF3
    typeset +i16 NNF4
    NNF1=${NNF1#16\#}
    NNF2=${NNF2#16\#}
    NNF3=${NNF3#16\#}
    NNF4=${NNF4#16\#}
    if [ ${#NNF1} -eq 1 ]
    then
        NNF1="0${NNF1}"
    fi
    if [ ${#NNF2} -eq 1 ]
    then
        NNF2="0${NNF2}"
    fi
    if [ ${#NNF3} -eq 1 ]
    then
        NNF3="0${NNF3}"
    fi
    if [ ${#NNF4} -eq 1 ]
    then
        NNF4="0${NNF4}"
    fi
    typeset -i16 NN
    let NN=16#${NNF1}${NNF2}${NNF3}${NNF4}
    unset NNF1 NNF2 NNF3 NNF4

    typeset -i NNO1=${2%%.*}
```

EXAMPLE 6–1 `addclient.ksh` Script with the `pntadm` Command *(Continued)*

```
    tmp=${2#*.}
    typeset -i NNO2=${tmp%%.*}
    tmp=${tmp#*.}
    typeset -i NNO3=${tmp%%.*}
    tmp=${tmp#*.}
    typeset -i NNO4=${tmp%%.*}
    typeset -i16 NNF1
    let NNF1=${NNO1}
    typeset -i16 NNF2
    let NNF2=${NNO2}
    typeset -i16 NNF3
    let NNF3=${NNO3}
    typeset -i16 NNF4
    let NNF4=${NNO4}
    typeset +i16 NNF1
    typeset +i16 NNF2
    typeset +i16 NNF3
    typeset +i16 NNF4
    NNF1=${NNF1#16\#}
    NNF2=${NNF2#16\#}
    NNF3=${NNF3#16\#}
    NNF4=${NNF4#16\#}
    if [ ${#NNF1} -eq 1 ]
    then
        NNF1="0${NNF1}"
    fi
    if [ ${#NNF2} -eq 1 ]
    then
        NNF2="0${NNF2}"
    fi
    if [ ${#NNF3} -eq 1 ]
    then
        NNF3="0${NNF3}"
    fi
    if [ ${#NNF4} -eq 1 ]
    then
        NNF4="0${NNF4}"
    fi
    typeset -i16 NC
    let NC=16#${NNF1}${NNF2}${NNF3}${NNF4}
    typeset -i10 ANS
    let ANS=${NC}-${NN}
    print - $ANS
}

#
# Check usage.
#
if [ "$#" != 3 ]
then
    print "This script is used to add client entries to a DHCP network"
    print "table by utilizing the pntadm batch facilty.\n"
    print "usage: $0 network start_ip entries\n"
```

EXAMPLE 6–1 `addclient.ksh` Script with the `pntadm` Command *(Continued)*

```
    print "where: network is the IP address of the network"
        print "       start_ip is the starting IP address \n"
        print "       entries is the number of the entries to add\n"
    print "example: $0 129.148.174.0 129.148.174.1 254\n"
    return
fi

#
# Use input arguments to set script variables.
#
NETWORK=$1
START_IP=$2
typeset -i STRTNUM=‘client_index ${NETWORK} ${START_IP}‘
let ENDNUM=${STRTNUM}+$3
let ENTRYNUM=${STRTNUM}
BATCHFILE=/tmp/batchfile.$$
MACRO=‘uname -n‘

#
# Check if mask in netmasks table. First try
# for network address as given, in case VLSM
# is in use.
#
NETMASK=‘get_netmask ${NETWORK}‘
if [ -z "${NETMASK}" ]
then
    get_default_class ${NETWORK} | read DEFNET DEFMASK
    # use the default.
    if [ "${DEFNET}" != "${NETWORK}" ]
    then
        # likely subnetted/supernetted.
        print - "\n\n###\tWarning\t###\n"
        print - "Network ${NETWORK} is netmasked, but no entry was found in the \n
             ’netmasks’ table; please update the ’netmasks’ table in the \n
              appropriate nameservice before continuing. \n
              (See /etc/nsswitch.conf.) \n" >&2
        return 1
    else
        # use the default.
        NETMASK="${DEFMASK}"
    fi
fi

#
# Create a batch file.
#
print -n "Creating batch file "
while [ ${ENTRYNUM} -lt ${ENDNUM} ]
do
    if [ $((${ENTRYNUM}-${STRTNUM}))%50 -eq 0 ]
    then
        print -n "."
    fi
```

EXAMPLE 6–1 `addclient.ksh` Script with the `pntadm` Command *(Continued)*

```
    CLIENTIP=`get_addr ${NETWORK} ${NETMASK} ${ENTRYNUM}`
    print "pntadm -A ${CLIENTIP} -m ${MACRO} ${NETWORK}" >> ${BATCHFILE}
    let ENTRYNUM=${ENTRYNUM}+1
done
print " done.\n"

#
# Run pntadm in batch mode and redirect output to a temporary file.
# Progress can be monitored by using the output file.
#
print "Batch processing output redirected to ${BATCHFILE}"
print "Batch processing started."

pntadm -B ${BATCHFILE} -v > /tmp/batch.out 2 >&1

print "Batch processing completed."
```

DHCP Files

The following table lists files associated with Solaris DHCP.

TABLE 6–2 Files and Tables Used by DHCP Daemons and Commands

File/Table	Description
`dhcptab`	A generic term for the table of DHCP configuration information recorded as options with assigned values, which are then grouped into macros. The name of the `dhcptab` table and its location is determined by the data store you use for DHCP information.
DHCP network table	Maps IP addresses to client IDs and configuration options. DHCP network tables are named according to the IP address of the network, such as 102.21.32.0. There is no file called `dhcp_network`. The name and location of DHCP network tables is determined by the data store you use for DHCP information.
`dhcpsvc.conf`	Records DHCP daemon startup options and the data store resource and location of the `dhcptab` and network tables. The file is located in the `/etc/inet` directory.
`nsswitch.conf`	Specifies the location of name service databases and the order in which to search them for various kinds of information. The `nsswitch.conf` file is consulted when you configure a DHCP server in order to obtain accurate configuration information. The file is located in the `/etc` directory.

TABLE 6–2 Files and Tables Used by DHCP Daemons and Commands *(Continued)*

File/Table	Description
resolv.conf	Contains information used by the DNS resolver. During DHCP server configuration, this file is consulted for information about the DNS domain and DNS server. The file is located in the /etc directory.
dhcp.*interface*	Indicates that DHCP is to be used on the client's network interface specified in the file name, such as dhcp.qe0. The dhcp.*interface* file might contain commands that are passed as options to the ifconfig *interface* dhcp start *option* command used to start DHCP on the client. The file is located in the /etc directory on Solaris DHCP client systems.
interface.dhc	Contains the configuration parameters obtained from DHCP for the given network interface. The client caches the current configuration information in /etc/dhcp/*interface*.dhc when the interface's IP address lease is dropped. The next time DHCP starts on the interface, the client requests to use the cached configuration if the lease has not expired. If the DHCP server denies the request, the client begins the standard DHCP lease negotiation process.
dhcpagent	Sets parameter values for the dhcpagent client daemon. The path to the file is /etc/default/dhcpagent. See the file itself or the dhcpagent(1M) man page for information about the parameters.
DHCP inittab	Defines aspects of DHCP option codes, such as the data type, and assigns mnemonic labels. See the dhcp_inittab man page for more information about the file syntax. On the client, the information in the /etc/dhcp/inittab file is used by dhcpinfo to provide more meaningful information to human readers of the information. This file replaces the /etc/dhcp/dhcptags file. "DHCP Option Information" on page 167 provides more information about this replacement. On the DHCP server system, this file is used by the DHCP daemon and management tools to obtain DHCP option information.

DHCP Option Information

Historically, DHCP option information has been stored in several places in Solaris DHCP, including the server's dhcptab table, the client's dhcptags file, and internal tables of in.dhcpd, snoop, dhcpinfo, and dhcpmgr. In an effort to consolidate option information, the Solaris 8 DHCP product introduced the /etc/dhcp/inittab file. See the dhcp_inittab man page for detailed information about the file.

The Solaris DHCP client uses the DHCP inittab file as a replacement for the dhcptags file to obtain information about option codes received in its DHCP packet. The in.dhcpd, snoop, and dhcpmgr programs on the DHCP server use the inittab file as well.

Note – Most sites that use Solaris DHCP are *not* affected by this change. Your site is affected only if you plan to upgrade to Solaris 8, you previously created new DHCP options and modified the `/etc/dhcp/dhcptags` file, and you want to retain the changes. When you upgrade, the upgrade log notifies you that your `dhcptags` file had been modified and that you should make changes to the DHCP `inittab` file.

Differences Between `dhcptags` and `inittab`

The `inittab` file contains more information than the `dhcptags` file and it uses a different syntax.

A sample `dhcptags` entry is:

```
33 StaticRt - IPList Static_Routes
```

where `33` is the numeric code that is passed in the DHCP packet, `StaticRt` is the option name, `IPList` indicates the expected data is a list of IP addresses, and `Static_Routes` is a more descriptive name.

The `inittab` file consists of one-line records that describe each option. The format is similar to the format that defines symbols in `dhcptab`. The following table describes the syntax of the `inittab`.

TABLE 6–3 DHCP `inittab` File Syntax

Option	Description
option-name	Name of the option. The option name must be unique within its option category, and not overlap with other option names in the Standard, Site, and Vendor categories. For example, you cannot have two Site options with the same name, and you should not create a Site option with the same name as a Standard option.
category	Identifies the namespace in which the option belongs. Must be one of Standard, Site, Vendor, Field, or Internal.
code	Identifies the option when it is sent over the network. In most cases, the code uniquely identifies the option, without a category. However, in the case of internal categories like Field or Internal, a code might be used for other purposes and thus might not be globally unique. The code should be unique within the option's category, and not overlap with codes in the Standard and Site fields.
type	Describes the data associated with this option. Valid types are IP, Ascii, Octet, Boolean, Unumber8, Unumber16, Unumber32, Unumber64, Snumber8, Snumber16, Snumber32, and Snumber64. For numbers, an initial U or S indicates that the number is unsigned or signed, and the digits at the end indicate the amount of bits in the number. The type is not case sensitive.
granularity	Describes how many units of data make up a whole value for this option.

TABLE 6–3 DHCP inittab File Syntax *(Continued)*

Option	Description
maximum	Describes how many whole values are allowed for this option. 0 indicates an infinite number.
consumers	Describes which programs can use this information. This should be set to sdmi, where: s – snoop d – in.dhcpd m – dhcpmgr i – dhcpinfo

A sample inittab entry is:

```
StaticRt Standard, 33, IP, 2, 0, sdmi
```

This entry describes an option named StaticRt, which is in the Standard category and is option code 33. The expected data is a potentially infinite number of pairs of IP addresses because the type is IP, granularity is 2, and maximum is infinite (0). The consumers of this option are sdmi: snoop, in.dhcpd, dhcpmgr, and dhcpinfo.

Converting dhcptags Entries to inittab Entries

If you previously added entries to your dhcptags file, you must add corresponding entries to the new inittab file. The following example shows how a sample dhcptags entry might be expressed in inittab format.

Suppose you had added the following dhcptags entry for fax machines connected to the network:

```
128 FaxMchn - IP Fax_Machine
```

The code 128 means that it must be in the site category, the option name is FaxMchn, the data type is IP.

The corresponding inittab entry might be:

```
FaxMchn SITE, 128, IP, 1, 1, sdmi
```

The granularity of 1 and maximum of 1 indicate that one IP address is expected for this option.

Index