Working With DHCP in Oracle® Solaris 11.1

Part No: E28991–01
October 2012

ORACLE

121010@25097

Contents

Preface

Welcome to the Working With DHCP in Oracle Solaris 11.1. This book is part of a multivolume set that covers a significant part of the Oracle Solaris system administration information. This book assumes that you have already installed Oracle Solaris. You should be ready to configure your network or ready to configure any networking software that is required on your network.

Note – This Oracle Solaris release supports systems that use the SPARC and x86 families of processor architectures. The supported systems appear in the *Oracle Solaris OS: Hardware Compatibility Lists*. This document cites any implementation differences between the platform types.

Who Should Use This Book

This book is intended for anyone responsible for administering systems that run Oracle Solaris, which are configured in a network. To use this book, you should have at least two years of UNIX system administration experience. Attending UNIX system administration training courses might be helpful.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1 Typographic Conventions

Typeface	Description	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for shells that are included in the Oracle Solaris OS. Note that the default system prompt that is displayed in command examples varies, depending on the Oracle Solaris release.

TABLE P–2 Shell Prompts

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	`$`
Bash shell, Korn shell, and Bourne shell for superuser	`#`
C shell	`machine_name%`
C shell for superuser	`machine_name#`

◆ ◆ ◆ CHAPTER 1

About DHCP (Overview)

The ISC DHCP server, `dhcpd`, implements the Dynamic Host Configuration Protocol (DHCP) and the Internet Bootstrap Protocol (BOOTP). DHCP allows hosts on a TCP/IP network to request and be assigned IP addresses, and also to discover information about the network to which they are attached. BOOTP provides similar functionality.

This chapter introduces the Dynamic Host Configuration Protocol (DHCP) and explains the concepts that underlie the protocol. The chapter also describes the advantages of using DHCP in your network.

This chapter contains the following information:

About the DHCP Protocol

The DHCP protocol enables automatic network configuration of hosts in a TCP/IP network. 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 that are 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 the client and server. However, unlike BOOTP messages, DHCP messages can include network configuration data for the client.

A primary benefit of DHCP is its ability to manage IP address assignments through leases. *Leases* allow IP addresses to be reclaimed when they are not in use. The reclaimed IP addresses

can be reassigned to other clients. A site that uses DHCP can use a smaller pool of IP addresses than would be needed if all clients were assigned a permanent IP address.

Advantages of Using DHCP

DHCP relieves you of some of the time-consuming tasks involved in setting up a TCP/IP network and in the daily management of that network. DHCP offers the following advantages:

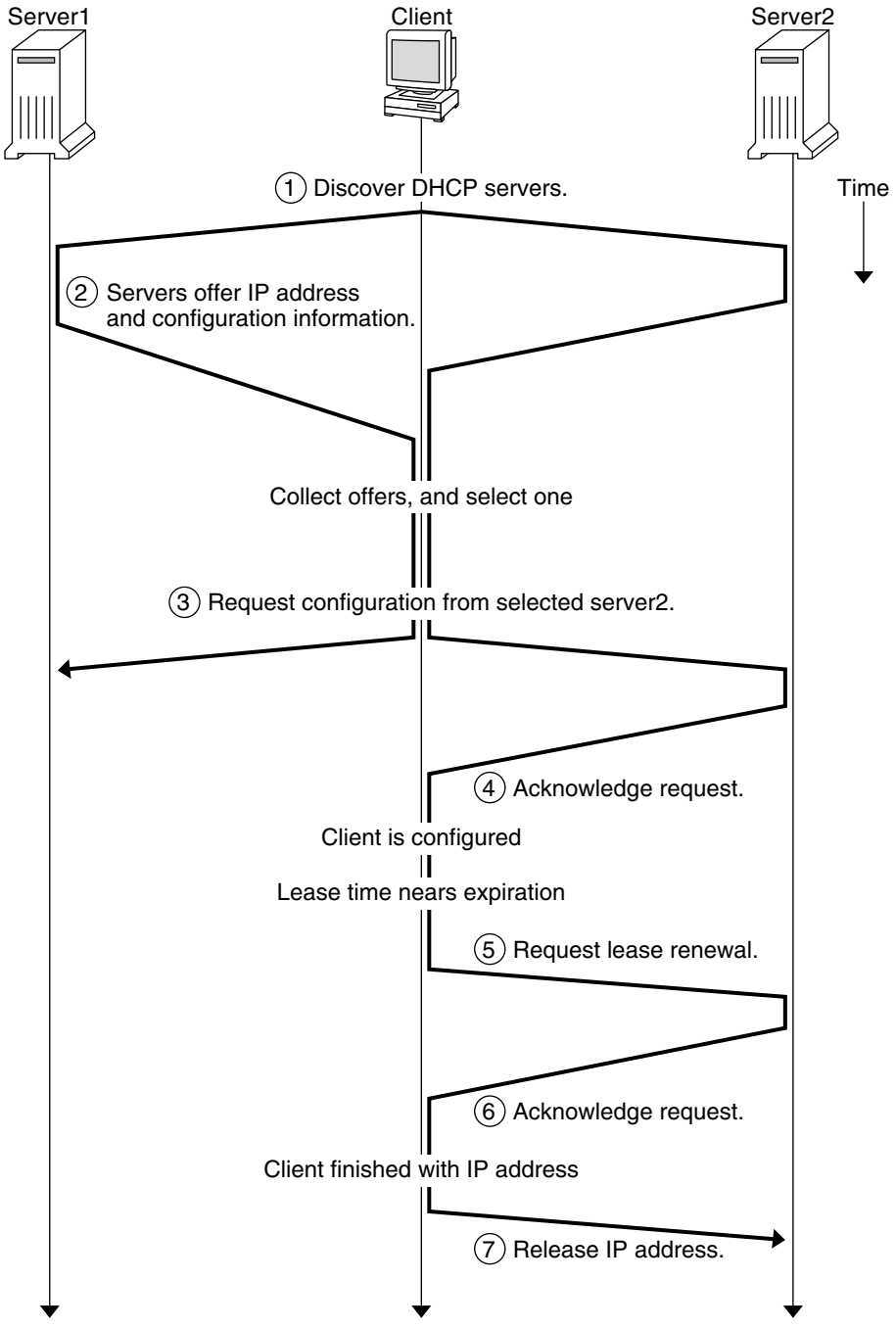
- **IP address management** – A primary advantage of DHCP is easier management of IP addresses. In a network without DHCP, you must manually assign IP addresses. You must be careful to assign unique IP addresses to each client and to configure each client individually. If a client moves to a different network, you 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** – You can create a tailored configuration for certain clients, or for certain types of clients. The configuration information is stored in one place, in the DHCP data store. You do not need to log in to a client to change its configuration. You can make changes for multiple clients just by changing the information in the data store.
- **Support for 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 for local clients and remote clients** – BOOTP provides for the relaying of messages from one network to another network. 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 servers that are not on the client's network. DHCP requests can be relayed in the same manner because, to the router, DHCP requests are indistinguishable from BOOTP requests. The 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 that is needed to boot from a server on the network, instead of using RARP (Reverse Address Resolution Protocol) and the `bootparams` file. The DHCP server can give a client all the information that the client needs to function, including IP address, boot server, and network configuration information. Because DHCP 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 have a boot server.
- **Large network support** – To make DHCP support for large networks better:
  - The deployment of DHCP servers can be centralized or decentralized.

- Single servers can be configured to manage multiple physical networks that are not directly connected to it with the help of DHCP relay agent.
- ISC DHCP provides failover between servers, so that when one server fails, the other will cover for it.
- ISC DHCP load balancing so that more than one server can provide service at the same time.
- The DHCP server uses multithreading to process many client requests simultaneously.

How DHCP Works

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.

FIGURE 1–1 Sequence of Events for DHCP Service



The preceding diagram shows the following steps:

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 DHCP implementation in Oracle Solaris, is derived from the client's Media Access Control (MAC) 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? The server determines either that the client is 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*, the server 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 by 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 it can select an IP address appropriate for the client. See the `netmasks(4)` man page for information on `netmasks`.
2. After the DHCP servers determine the client's network, each server selects an appropriate IP address and verifies that the address is not already in use. The DHCP servers then respond to the client by broadcasting an *offer message*. The offer message 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 the client determines whether to use the IP address.
3. The client selects the best offer, based on the number and type of services offered. The client 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 that the client has chosen a server. The servers that are not chosen can cancel the reservations for the IP addresses that they had offered.
4. The selected server allocates the IP address for the client and stores the information in the DHCP data store. The server also sends an acknowledgement message (ACK) to the client. The *acknowledgement message* contains the network configuration parameters for the client. The client uses the `ping` utility to test the IP address to make sure no other system is using it. The client then continues to join the network.
5. The client monitors the lease time. When a set period of time has elapsed, the client sends a new message to the chosen server to increase the lease time.

6. The DHCP server that receives the request extends the lease time if the lease 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, the client notifies the server that the IP address is released. This notification can happen during an orderly shutdown and can also be done manually.

ISC DHCP Server

An implementation of the Internet Systems Consortium (ISC) DHCP server has been added to Oracle Solaris. Because this software is not automatically installed, you can add this server to your system by typing the following command:

```
# pkg install pkg:/service/network/dhcp/isc-dhcp
```

The following list includes some of the important additions for ISC DHCP in the Oracle Solaris release:

- Several services have been added to support ISC DHCP and the legacy Sun DHCP service. See "SMF Services Used by the DHCP Service" on page 40 for a list of all of the services used by DHCP.
- Three commands have been added: `dhcpd`, `dhcprelay`, and `omshell`. See "Files Used by the DHCP Service" on page 38 for a list of all of the commands that are associated with DHCP.
- For ISC DHCP, the server configuration files are `/etc/inet/dhcpd4.conf` for DHCPv4 and `/etc/inet/dhcpd6.conf` for DHCPv6.
- A user called `dhcpserv` has been added for the ISC DHCP service.
- Access to the commands using a user login or role can be managed by using the `solaris.smf.manage.dhcp` and `solaris.smf.value.dhcp` authorizations.

In addition, the ISC DHCP server shipped with the Oracle Solaris 11.1 release supports DHCP over IPoIB (IP over Infiniband). DHCP over IPoIB, as defined by RFC 4390, improves interoperability.

For more information about ISC DHCP, see the ISC DHCP Documentation web page.

Legacy Sun DHCP Server

The legacy Sun DHCP server software is still included in the Oracle Solaris 11 release, but it has been marked as obsolete and will be removed in a future release. For more information about the legacy DHCP service, see About DHCP (Overview).

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 in this document is a software entity. The DHCP client is a daemon (`dhcpagent`) that runs in Oracle Solaris on a system that is configured to request its network configuration from the DHCP service. The DHCP client is interoperable with both the legacy Sun DHCP server and the ISC DHCP server.

See Chapter 3, "Configuring and Administering the DHCP Client," for detailed information about the DHCP client.

◆ ◆ ◆ CHAPTER 2

Administering the ISC DHCP Service

This chapter describes tasks that you might find useful when you administer the ISC DHCP service. The following tasks are covered:

DHCP Server Tasks

▼ How to Grant User Access to DHCP Commands

By default, only the `root` user can execute `svcadm` and other commands that are required to configure the DHCP service. If you want users who do not have root privileges to use the DHCP commands, you can set up role-based access control (RBAC) to allow access to those commands. The following procedure explains how to assign the DHCP Management profile, which enables the user to execute the DHCP commands.

You might also find the following man pages helpful: `rbac`(5), `exec_attr`(4), and `user_attr`(4).

1 Assume the root role.

Roles contain authorizations and privileged commands. For more information about roles, see "Initially Configuring RBAC (Task Map)" in *Oracle Solaris 11.1 Administration: Security Services*.

2 Add a user or role to the `/etc/user_attr` file.

Edit the `/etc/user_attr` file to add an entry of the following form. Add one entry for each user or role that should manage the DHCP service.

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

For example, for user `ram`, you would add the following entry:

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

How to Configure an ISC DHCP Server

You can use these steps to initially configure an ISC DHCP server.

1. **Assume the root role.**

   Roles contain authorizations and privileged commands. For more information about roles, see "Initially Configuring RBAC (Task Map)" in *Oracle Solaris 11.1 Administration: Security Services*.

2. **Edit the DHCP configuration files for the appropriate services.**

   For IPv4 edit `/etc/inet/dhcpd4.conf` and for IPV6 edit `/etc/inet/dhcpd6.conf`. For more information, see the `dhcpd.conf`(5) man page.

3. **Enable the required service.**

   `# svcadm enable` *service*

   service can be one of the following values:

`svc:/network/dhcp/server:ipv4`	Provides DHCP and BOOTP requests from IPv4 clients
`svc:/network/dhcp/server:ipv6`	Provides DHCP and BOOTP requests from IPv6 clients
`svc:/network/dhcp/relay:ipv4`	Relays DHCP and BOOTP requests from IPv4 clients to a network with a DHCP server
`svc:/network/dhcp/relay:ipv6`	Relays DHCP and BOOTP requests from IPv6 clients to a network with a DHCP server

How to Modify the Configuration of the DHCP Service

1. **Assume the `root` role or a role or user name that has been assigned to the DHCP Management profile.**

   Roles contain authorizations and privileged commands. For more information about roles, see "Initially Configuring RBAC (Task Map)" in *Oracle Solaris 11.1 Administration: Security Services*. For more information about the DHCP Management profile, see "How to Grant User Access to DHCP Commands" on page 15

2. **Edit the DHCP configuration file.**

   For IPv4 edit the `/etc/inet/dhcpd4.conf` and for IPv6 edit `/etc/inet/dhcpd6.conf`. For more information, see the `dhcpd.conf`(5) man page.

3 Refresh the SMF data.

```
# svcadm refresh service
```

◆ ◆ ◆ CHAPTER 3

Configuring and Administering the DHCP Client

This chapter discusses the Dynamic Host Configuration Protocol (DHCP) client that is part of Oracle Solaris. The chapter explains how the client's DHCPv4 and DHCPv6 protocols work, and how you can affect the behavior of the client.

One protocol, DHCPv4, has long been part of Oracle Solaris, and enables DHCP servers to pass configuration parameters such as IPv4 network addresses to IPv4 nodes.

The other protocol, DHCPv6, enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. DHCPv6 is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462), and can be used separately or concurrently with the stateless to obtain configuration parameters.

This chapter contains the following information:

About the DHCP Client

The DHCP client is the `dhcpagent` daemon. If you install Oracle Solaris by using the LiveCD GUI installer, then the DHCPv4 and DHCPv6 protocols are enabled on the installed system. If you install Oracle Solaris by using the text installer, you are prompted to select how the network should be configured on the installed system. If you specify Automatic Network Configuration, then the DHCPv4 and DHCPv6 protocols are enabled on the installed system.

You do not need to do anything else with the Oracle Solaris client to use DHCP. The DHCP server's configuration determines what information is given to DHCP client systems that use the DHCP service.

If a client system is already running Oracle Solaris, but not using DHCP, you can reconfigure the client system to use DHCP. You can also reconfigure a DHCP client system so that it stops using DHCP and uses static network information that you provide. See "Enabling and Disabling a DHCP Client" on page 26 for more information.

The DHCP Administrative Model

DHCPv4 requires explicit client configuration. You must set up the DHCPv4 system for addressing when desired, and this is typically done during initial system installation or dynamically through the use of the `ipadm` command. See the `ipadm(1M)` man page.

DHCPv6 does not require explicit client configuration. Instead, using DHCP is a property of the network, and the signal to use it is carried in Router Advertisement messages from local routers. The DHCP client automatically creates and destroys logical interfaces as needed.

The DHCPv6 mechanism is very similar administratively to the existing IPv6 stateless (automatic) address configuration. For stateless address configuration, you would set a flag on the local router to indicate that, for a given set of prefixes, each client should automatically configure an address on its own by using the advertised prefix plus a local interface token or random number. For DHCPv6, the same prefixes are required, but the addresses are acquired and managed through a DHCPv6 server instead of being assigned "randomly."

MAC Address and Client ID

DHCPv4 uses the MAC address and an optional Client ID to identify the client for purposes of assigning an address. Each time the same client arrives on the network, it gets the same address, if possible.

DHCPv6 uses basically the same scheme, but makes the Client ID mandatory and imposes structure on it. The Client ID in DHCPv6 consists of two parts: a DHCP Unique Identifier (DUID) and an Identity Association Identifier (IAID). The DUID identifies the client **system** (rather than just an interface, as in DHCPv4), and the IAID identifies the interface on that system.

As described in RFC 3315, an identity association is the means used for a server and a client to identify, group, and manage a set of related IPv6 addresses. A client must associate at least one distinct IA with each of its network interfaces, and then uses the assigned IAs to obtain configuration information from a server for that interface. For additional information about IAs, see the next section, "Protocol Details."

DUID+IAID can also be used with DHCPv4. These can be concatenated together unambiguously so that they can serve as the Client ID. For compatibility reasons, this is not done for regular IPv4 interfaces. However, for logical interfaces (`bge0:1`), DUID+IAID is used if no Client ID is configured.

Unlike IPv4 DHCP, DHCPv6 does not provide a "client name" option, so there is no way to name your systems based on DHCPv6 alone. Instead, if you need to know the DNS name that goes with an address provided by DHCPv6, use DNS reverse-resolution (address-to-name query by using the `getaddrinfo(3SOCKET)` function) to find the corresponding name information. One implication of this is that if you are using only DHCPv6 and want a node to have a specific name, you must specify the node name by using the `svccfg` command as follows:

```
# svccfg -s svc:/system/identity:node setprop config/nodename = astring: hostname
```

Differences Between DHCPv4 and DHCPv6

The two major differences between DHCPv4 and DHCPv6 are the following:

- **The administrative model**
  - DHCPv4 – The administrator enables DHCP for each interface. Administration is on a per-logical interface basis.
  - DHCPv6 – Explicit configuration is not necessary. This protocol is enabled on a given physical interface.
- **Protocol details**
  - DHCPv4 – The DHCP server supplies the subnet mask for each address. A hostname option sets the system-wide host name.
  - DHCPv6 – The subnet mask is supplied by Router Advertisements, not the DHCPv6 server. There is no DHCPv6 hostname option.

DHCP Protocol Details

With DHCPv4, the DHCP server supplies the subnet mask to be used with the assigned address. With DHCPv6, the subnet mask (also known as "prefix length") is assigned by the Router Advertisements, and is not controlled by the DHCP server.

DHCPv4 carries a Hostname option that is used to set the system-wide node name. DHCPv6 has no such option.

To configure a Client ID for DHCPv6 you must specify a DUID, rather than allowing the system to choose one automatically. You can do this globally for the daemon, or on a per-interface basis. Use the following format to set the global DUID (note the initial dot):

```
.v6.CLIENT_ID=DUID
```

To set a particular interface to use a given DUID (and make the system appear to be multiple independent clients to a DHCPv6 server):

bge0.v6 CLIENT ID=*DUID*

Each Identity Association (IA) holds one type of address. For example, an identity association for temporary addresses (IA_TA) holds temporary addresses, while an identity association for non-temporary addresses (IA_NA), carries assigned addresses that are permanent. The version of DHCPv6 described in this guide provides only IA_NA associations.

Oracle Solaris assigns exactly one IAID to each interface, on demand, and the IAID is stored in a file in the root file system so that it remains constant for the life of the machine.

Logical Interfaces

In the DHCPv4 client, each logical interface is independent and is an administrative unit. In addition to the zeroth logical interface (which defaults to the interface MAC address as an identifier), the user may configure specific logical interfaces to run DHCP by specifying a CLIENT_ID in the `dhcpagent` configuration file. For example:

bge0.v6 CLIENT ID=*DUID*

DHCPv6 works differently. The zeroth logical interface on an IPv6 interface, unlike IPv4, is always a link-local. A link-local is used to automatically assign an IP address to a device in an IP network when there is no other assignment method available, such as a DHCP server. The zeroth logical interface cannot be under DHCP control, so although DHCPv6 is run on the zeroth logical interface (known, also, as the "physical" interface), it assigns addresses only on non-zero logical interfaces.

In response to a DHCPv6 client request, the DHCPv6 server returns a list of addresses for the client to configure.

Option Negotiation

In DHCPv6 there is an Option Request Option, which provides a hint to the server of what the client prefers to see. If all possible options were sent from the server to the client, so much information could be sent that some of it would have to be dropped on the way to the client. The server might use the hint to choose among the options to include in the reply. Alternatively, the server could ignore the hint and choose other items to include. On Oracle Solaris, for example, the preferred options might include the Oracle Solaris DNS address domain or the NIS address domain, but would probably not include the net BIOS server.

The same type of hint is also provided for DHCPv4, but without the special Option Request Option. Instead DHCPv4 uses the `PARAM_REQUEST_LIST` in `/etc/default/dhcpagent`.

Configuration Syntax

Configure the DHCPv6 client in much the same way as the existing DHCPv4 client, using `/etc/default/dhcpagent`.

The syntax is augmented with a ".v6" marker between the interface name (if any) and the parameter to be configured. For example, the global IPv4 option request list is set like this:

```
PARAM_REQUEST_LIST=1,3,6,12,15,28,43
```

An individual interface can be configured to omit the hostname option like this:

```
bge0.PARAM_REQUEST_LIST=1,3,6,15,28,43
```

To set a global request list for DHCPv6, note the leading dot:

```
.v6.PARAM_REQUEST_LIST=23,24
```

Or, to set an individual interface, follow this example:

```
bge0.v6.PARAM_REQUEST_LIST=21,22,23,24
```

For reference, here is an actual `/etc/default/dhcpagent` file for DHCPv6 configuration:

```
# The default DHCPv6 parameter request list has preference (7), unicast (12),
# DNS addresses (23), DNS search list (24), NIS addresses (27), and
# NIS domain (29).  This may be changed by altering the following parameter-
# value pair.  The numbers correspond to the values defined in RFC 3315 and
# the IANA dhcpv6-parameters registry.
.v6.PARAM_REQUEST_LIST=7,12,23,24,27,29
```

DHCP Client Startup

In most cases, there is nothing you need to do for DHCPv6 client startup. The `in.ndpd` daemon starts up DHCPv6 automatically when it is needed.

For DHCPv4, however, you must request the client startup, if that was not done during Oracle Solaris installation. See "How to Enable a DHCP Client" on page 26.

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.

Although the default is to run DHCPv6, you can choose to not have DHCPv6 run. After DHCPv6 starts running, you can stop it with the `ipadm delete-addr` command. You can also disable DHCPv6 so that it does not start on reboot, by modifying the `/etc/inet/ndpd.conf` file.

The following example show how to immediately shut down DHCPv6:

```
ex# echo ifdefault StatefulAddrConf false >> /etc/inet/ndpd.conf
ex# pkill -HUP -x in.ndpd
ex# ipadm delete-addr -r dhcp-addrobj
```

At startup, if persistent DHCP configurations exist in the system, then the `dhcpagent` is started as part of the startup script processes. The `dhcpagent` then configures the network interfaces as described in "How DHCP Works" on page 9.

DHCPv6 Communication

Unlike DHCPv4, which is invoked by manual configuration, DHCPv6 is invoked by Router Advertisements (RAs). Depending on how the router is configured, the system automatically invokes DHCPv6 on the interface on which the Router Advertisement message was received and uses DHCP to get an address and other parameters, or the system requests only data other than an address (for example, DNS servers) with DHCPv6.

The `in.ndpd` daemon receives the Router Advertisement message. It does this automatically on all interfaces plumbed for IPv6 on the system. When `in.ndpd` sees an RA that specifies that DHCPv6 should run, it invokes it.

To prevent `in.ndpd` from starting up DHCPv6, you can change the `/etc/inet/ndpd.conf` file.

You can also stop DHCPv6 after it starts by using one of the following versions of `ipadm`:

`ipadm delete-addr` *dhcp-addrobj*

or

`ipadm delete-addr -r` *dhcp-addrobj*

How DHCP Client Protocols Manage Network Configuration Information

DHCPv4 and DHCPv6 client protocols manage network configuration information in different ways. The key difference is that with DHCPv4, the negotiation is for the lease of a single address and some options to go with it. With DHCPv6, the negotiation is over a batch of addresses and a batch of options.

For background information on the interaction between DHCPv4 client and server, see Chapter 1, "About DHCP (Overview)."

How the DHCPv4 Client Manages Network Configuration Information

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

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

Each time `dhcpagent` performs an action related to the lease, the daemon looks for an executable file called `/etc/dhcp/eventhook`. If an executable file with this name is found, `dhcpagent` invokes the executable. See "DHCP Client Event Scripts" on page 34 for more information about using the event executable.

How the DHCPv6 Client Manages Network Configuration Information

DHCPv6 communication between client and server begins with the client sending out a Solicit message, to locate servers. In response, all servers available for DHCP service send an Advertise message. The server message contains multiple IA_NA (Identity Association Non-Temporary Address) records plus other options (such as DNS server addresses) that the server can supply.

A client can request particular addresses (and multiples of them) by setting up its own IA_NA/IAADDR records in its Request message. A client typically requests specific addresses if it has old addresses recorded and it would like the server to provide the same ones, if possible. Regardless of what the client does (even if it requests no addresses at all), the server can supply any number of addresses to the client for a single DHCPv6 transaction.

This is a the message dialog that takes place between the clients and servers.

- A client sends a Solicit message to locate servers.
- Servers send an Advertise message to indicate they are available for DHCP service.
- A client sends a Request message to request configuration parameters, including IP addresses, from servers with the greatest preference values. Server preference values are set by the administrator and extend from 0, at the lowest end, to 255 at the highest.
- The server sends a Reply message that contains the address leases and configuration data.

If the preference value in the Advertise message is 255, the DHCPv6 client immediately selects that server. If the most preferred server does not respond, or fails to give a successful Reply to

the Request message, then the client continues looking for less-preferred servers (in order) until there are no more Advertise messages on hand. At that point, the client starts over by again sending Solicit messages.

The chosen server sends a Reply message containing assigned addresses and configuration parameters in response to a Solicit or Request message.

DHCP Client Shutdown

At shutdown, the client sends a Release message to the server that assigned addresses to the client to indicate that the client will no longer use one or more of the assigned addresses. When the DHCPv4 client system shuts down normally, `dhcpagent` writes the current configuration information to a file, if the file exists. The filename for DHCPv4 is `/etc/dhcp/`*interface*`.dhc`, and `/etc/dhcp/`*interface*`.dh6` is for DHCPv6. By default, the lease is saved rather than released, so the DHCP server can not detect that the IP address is not in active use, which enables the client to easily regain the address on next boot. This default action is the same as the `ipadm delete-addr` *dhcp-addrobj* command.

If the lease in that file is still valid when the system reboots, `dhcpagent` sends an abbreviated request to use the same IP address and network configuration information. For DHCPv4, this is the Request message. For DHCPv6, the message is Confirm.

If the DHCP server permits this request, `dhcpagent` 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, `dhcpagent` initiates the DHCP protocol sequence described in "How DHCP Works" on page 9. As a result, the client obtains new network configuration information.

Enabling and Disabling a DHCP Client

To enable the DHCP client on a system that is already running Oracle Solaris and is not using DHCP, you must first unconfigure the system. When the system boots, you must issue some commands to set up the system and enable the DHCP client.

Note – In many deployments it is common practice to have crucial parts of the infrastructure set up with static IP addresses, rather than using DHCP. Determining which devices on your network, for example routers and certain servers, should be client and which should not, is beyond the scope of this guide.

▼ How to Enable a DHCP Client

This procedure is necessary only if DHCPv4 was not enabled during Oracle Solaris installation. It is never necessary for DHCPv6.

1. **Assume the `root` role or a role or user name that has been assigned to the DHCP Management profile.**

   Roles contain authorizations and privileged commands. For more information about roles, see "Initially Configuring RBAC (Task Map)" in *Oracle Solaris 11.1 Administration: Security Services*. For more information about the DHCP Management profile, see "How to Grant User Access to DHCP Commands" on page 15

2. **Reconfigure the system.**

   Choose one of the following configuration methods:

   - **Interactively reconfigure the system.**

     ```
     # sysconfig configure
     ```

     When the System Configuration Interactive Tool starts, select Automatic network configuration on the Network screen.

   - **Non-interactively reconfigure the system.**

     ```
     # sysconfig configure -c sc_profile
     ```

     See the `sysconfig(1M)` man page for more information about using the `sc_profile` configuration file.

How to Disable a DHCP Client

1. **Assume the `root` role or a role or user name that has been assigned to the DHCP Management profile.**

   Roles contain authorizations and privileged commands. For more information about roles, see "Initially Configuring RBAC (Task Map)" in *Oracle Solaris 11.1 Administration: Security Services*. For more information about the DHCP Management profile, see "How to Grant User Access to DHCP Commands" on page 15

2. **Reconfigure the system.**

   Choose one of the following configuration methods:

   - **Interactively reconfigure the system.**

     ```
     # sysconfig configure
     ```

     When the System Configuration Interactive Tool starts, select either Manual or None as the network configuration on the Network screen.

   - **Non-interactively reconfigure the system.**

     ```
     # sysconfig configure -c sc_profile
     ```

See the sysconfig(1M) man page for more information about using the sc_profile configuration file.

DHCP Client Administration

The DHCP client software does not require administration under normal system operation. The dhcpagent daemon automatically starts when the system boots, renegotiates leases, and stops when the system shuts down. You should not manually start and stop the dhcpagent daemon directly. Instead, as superuser on the client system, you can use the ipadm command to affect dhcpagent's management of the network interface, if necessary.

ipadm Command Options Used With the DHCP Client

This section summarizes the command options, which are documented in the ipadm(1M) man page.

The ipadm command enables you to do the following:

- **Create the IP interface** – The command ipadm create-ip creates the IP interface which you then configure with IP addresses. The addresses can either be static or dynamic. Creating the IP interface is a prerequisite command before you can assign the addresses.
- **Start the DHCP client** – The command ipadm create-addr -T dhcp *dhcp-addrobj* initiates the interaction between dhcpagent and the DHCP server to obtain an IP address and a new set of configuration options. This command is 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 ipadm refresh-addr -i *dhcp-addrobj* causes dhcpagent to issue a request for network configuration parameters, with the exception of the IP address. This command is useful when the network interface has a static IP address, but the client system needs updated network options. For example, this command is useful if you do not use DHCP to manage IP addresses, but you do use it to configure hosts on the network.
- **Request a lease extension** – The command ipadm refresh-addr *dhcp-addrobj* causes dhcpagent to issue a request to renew the lease. The client does automatically request to renew leases. However, 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 ipadm delete-addr -r *dhcp-addrobj* causes dhcpagent to relinquish the IP address used by the network interface. Release of the IP address happens automatically when the lease expires. You might want to issue this

command with a laptop, for example, when leaving a network and planning to start the system on a new network. See also the `/etc/default/dhcpagent` configuration file `RELEASE_ON_SIGTERM` property.

- **Drop the IP address** – The command `ipadm delete-addr` *dhcp-addrobj* causes `dhcpagent` to take down the network interface without informing the DHCP server and cache the lease in the file system. This command enables the client to use the same IP address when it reboots.

Note – Currently, the `ipadm` command has no equivalent functionality for the `ifconfig [inet6] interface status` command.

Setting DHCP Client Configuration Parameters

The `/etc/default/dhcpagent` file on the client system contains tunable parameters for the `dhcpagent`. You can use a text editor to change several parameters that affect client operation. The `/etc/default/dhcpagent` file is well documented, so for more information, you should refer to the file as well as to the `dhcpagent(1M)` man page.

By default, the DHCP client is configured as follows:

For DHCPv4

- The client system does not require a particular host name.

  If you want a client to request a specific host name, see "DHCPv4 Client Host Names" on page 31.

- Default requests for the client are given in `/etc/default/dhcpagent`, and includes DNS Server, DNS domain, and broadcast address.

  The DHCP client's parameter file can be set up to request more options in the `PARAM_REQUEST_LIST` keyword in the `/etc/default/dhcpagent` file. The DHCP server can be configured to provide options that were not specifically requested. See the `dhcpd`(8) man page and "Working With DHCP Macros (Task Map)" in *System Administration Guide: IP Services* for information about using DHCP server macros to send information to clients.

For DHCPv4 and DHCPv6

- The client system uses DHCP on one physical network interface.

  If you want to use DHCP on more than one physical network interface, see "DHCP Client Systems With Multiple Network Interfaces" on page 30.

- The client is not automatically configured as a name service client if the DHCP client was configured after the Oracle Solaris installation.

See "DHCP Client Systems and Name Services" on page 32 for information about using name services with DHCP clients.

DHCP Client Systems With Multiple Network Interfaces

The DHCP client can simultaneously manage several different interfaces on one system. The interfaces can be physical interfaces or logical interfaces. Each interface has 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. The client maintains a separate set of network configuration parameters for each interface. Although the parameters are stored separately, some of the parameters are global in nature. The global parameters apply to the system as a whole, rather than to a particular network interface.

The host name, NIS domain name, and time zone are examples of global parameters. Global parameters usually have different values for each interface. However, only one value can be used for each global parameter associated with each system. To be sure that there is only one answer to a query for a global parameter, only the parameters for the primary network interface are used.

The DHCP client manages leases for logical interfaces and physical interfaces identically, except for the following limitation on logical interfaces: the DHCP client does not manage the default routes that are associated with logical interfaces.

The Oracle Solaris kernel associates routes with physical interfaces, not logical interfaces. When a physical interface's IP address is established, the necessary default routes should be placed in the routing table. If DHCP is used subsequently to configure a logical interface associated with that physical interface, the necessary routes should already be in place. The logical interface uses the same routes.

When a lease expires on a physical interface, the DHCP client removes the default routes that are associated with the interface. When a lease expires on a logical interface, the DHCP client does not remove the default routes associated with the logical interface. The associated physical interface and possibly other logical interfaces might need to use the same routes.

If you need to add or remove default routes that are associated with a DHCP-controlled interface, you can use the DHCP client event script mechanism. See "DHCP Client Event Scripts" on page 34.

DHCPv4 Client Host Names

By default, the DHCPv4 client does not supply its own host name, because the client expects the DHCP server to supply the host name. The DHCPv4 server is configured to supply host names to DHCPv4 clients by default. When you use the DHCPv4 client and server together, these defaults work well. However, when you use the DHCPv4 client with some third-party DHCP servers, the client might not receive a host name from the server. If the DHCP client does not receive a host name through DHCP, the client system checks the value that is set in the `config/nodename` property in the `svc:/system/identity:node` service for a name to use as the host name. If the file is empty, the host name is set to `unknown`.

If the DHCP server supplies a name in the DHCP `Hostname` option, the client uses that host name, even if a different value is placed in the value that is set in the `config/nodename` property in the `svc:/system/identity:node` service. If you want the client to use a specific host name, you can enable the client to request that name. See the following procedure.

Note – The following procedure does not work with all DHCP servers. Through this procedure you are requiring the client to send a specific host name to the DHCP server, and to expect the same name in return.

However, the DHCP server does not have to respect this request and many do not. They simply return a different name.

▼ How to Enable a DHCPv4 Client to Request a Specific Host Name

The steps to perform depend on whether an IP interface already exists with a DHCP address.

1. **Assume the `root` role or a role or user name that has been assigned to the DHCP Management profile.**

   Roles contain authorizations and privileged commands. For more information about roles, see "Initially Configuring RBAC (Task Map)" in *Oracle Solaris 11.1 Administration: Security Services*. For more information about the DHCP Management profile, see "How to Grant User Access to DHCP Commands" on page 15

2. **If the IP interface already exists with a DHCP address, do the following:**

   a. **Delete the existing DHCP address.**

      ```
      # ipadm delete-addr -r dhcp-addrobj
      ```

   b. **Register a new DHCP address with a specific host name that you want to use.**

      ```
      # ipadm create-addr -T dhcp -h hostname dhcp-addrobj
      ```

3 **If the IP interface does not yet exist, do the following:**

a. **Create the IP interface.**

```
# ipadm create-ip interface
```

b. **Register a DHCP address with a specific host name that you want to use.**

```
# ipadm create-addr -T dhcp -h hostname dhcp-addrobj
```

DHCP Client Systems and Name Services

Oracle Solaris systems support the following name services: DNS, NIS, and a local file store (`/etc/inet/hosts`). Each name service requires some configuration before it is usable. The `name-service/switch` SMF service must also be appropriately configured. See the `nsswitch.conf(4)` man page for more information.

Before a DHCP client system can use a name service, you must configure the system as a client of the name service. By default, and unless configured otherwise during system installation, only local files are used.

The following table summarizes issues that are related to each name service and DHCP. The table includes cross-references to documentation that can help you set up clients for each name service.

TABLE 3–1 Name Service Client Setup Information for DHCP Client Systems

Name Service	Client Setup Information
NIS	If you are using DHCP to send Oracle Solaris network install information to a client system, you can use a configuration macro that contains the `NISservs` and `NISdmain` options. These options pass the IP addresses of NIS servers and the NIS domain name to the client. The client then automatically becomes an NIS client. If a DHCP client system is already running Oracle Solaris, 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: # **`/usr/sbin/dhcpinfo NISdmain`** # **`/usr/sbin/dhcpinfo NISservs`** **Note –** For DHCPv6, include `-v6` and different protocol keywords in the command as follows: # **`/usr/sbin/dhcpinfo -v6 NISDomain`** # **`/usr/sbin/dhcpinfo -v6 NISServers`** Use the values returned for the NIS domain name and NIS servers when you set up the system as an NIS client. You set up an NIS client for an DHCP client system in the standard way, as documented in Chapter 6, "Setting Up and Configuring NIS (Tasks)," in *Oracle Solaris Administration: Naming and Directory Services*. **Tip –** You can write a script that uses `dhcpinfo` and `ypinit` to automate NIS client configuration on DHCP client systems.
`/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 manually add the host name 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 manually add the client's host name on the system.
DNS	If the DHCP client system receives the DNS domain name through DHCP, then properties of the `dns/client` SMF service are also automatically configured. See *Oracle Solaris Administration: Naming and Directory Services* for more information about DNS.

DHCP Client Event Scripts

You can set up the DHCP client to run an executable program or script that can perform any action that is appropriate for the client system. The program or script, which is called an *event script*, is automatically executed after certain DHCP lease events occur. The event script can be used to run other commands, programs, or scripts in response to specific lease events. You must provide your own event script to use this feature.

The following event keywords are used by `dhcpagent` to signify DHCP lease events:

Event Keyword	Description
`BOUND` and `BOUND6`	The interface is configured for DHCP. The client receives the acknowledgement message (DHCPv4 `ACK`) or (DHCPv6 `Reply`) from the DHCP server, which grants the lease request for an IP address. The event script is invoked immediately after the interface is configured successfully.
`EXTEND` and `EXTEND6`	The client successfully extends a lease. The event script is invoked immediately after the client receives the acknowledgement message from the DHCP server for the renew request.
`EXPIRE` and `EXPIRE6`	The lease expires when the lease time is up. For DHCPv4, the event script is invoked immediately before the leased address is removed from the interface and the interface is marked as down. For DHCPv6, the event script is invoked just before the last remaining leased addresses are removed from the interface.
`DROP` and `DROP6`	The client drops the lease to remove the interface from DHCP control. The event script is invoked immediately before the interface is removed from DHCP control.
`RELEASE` and `RELEASE6`	The client relinquishes the IP address. The event script is invoked immediately before the client releases the address on the interface and sends the DHCPv4 `RELEASE` or DHCPv6 `Release` packet to the DHCP server.
`INFORM` and `INFORM6`	An interface acquires new or updated configuration information from a DHCP server through the DHCPv4 `INFORM` or the DHCPv6 `Information-Request` message. These events occur when the DHCP client obtains only configuration parameters from the server and does not obtain an IP address lease.
`LOSS6`	During lease expiration, when one or more valid leases still remain, the event script is invoked just before expired addresses are removed. Those being removed are marked with the `IFF_DEPRECATED` flag.

With each of these events, `dhcpagent` invokes the following command:

```
/etc/dhcp/eventhook interface event
```

where *interface* is the interface that is using DHCP and *event* is one of the event keywords described previously. For example, when the interface is first configured for DHCP, the `dhcpagent` invokes the event script as follows:

```
/etc/dhcp/eventhook net0 BOUND
```

To use the event script feature, you must do the following:

- Name the executable file `/etc/dhcp/eventhook`.
- Set the owner of the file to be `root`.
- Set permissions to `755` (`rwxr-xr-x`).
- Write the script or program to perform a sequence of actions in response to any of the documented events. Because Sun might add new events, the program must silently ignore any events that are not recognized or do not require action. For example, the program or script might write to a log file when the event is `RELEASE`, and ignore all other events.
- Make the script or program noninteractive. Before the event script is invoked, `stdin`, `stdout`, and `stderr` are connected to `/dev/null`. To see the output or errors, you must redirect to a file.

The event script inherits its program environment from `dhcpagent`, and runs with `root` privileges. The script can use the `dhcpinfo` utility to obtain more information about the interface, if necessary. See the `dhcpinfo(1)` man page for more information.

The `dhcpagent` daemon waits for the event script to exit on all events. If the event script does not exit after 55 seconds, `dhcpagent` sends a `SIGTERM` signal to the script process. If the process still does not exit after three additional seconds, the daemon sends a `SIGKILL` signal to kill the process.

The `dhcpagent(1M)` man page includes one example of an event script.

◆ ◆ ◆ CHAPTER 4

DHCP Commands and Files (Reference)

This chapter explains the relationships between the DHCP commands and the DHCP files. However, the chapter does not explain how to use the commands.

The chapter contains the following information:

DHCP Commands

The following table lists the commands that you can use to manage DHCP on your network.

TABLE 4–1 Commands Used in DHCP

Command	Description
`/usr/lib/inet/dhcpd`	ISC DHCP only: The ISC DHCP server daemon. For more information, see the `dhcpd`(8) man page.
`/usr/lib/inet/dhcrelay`	ISC DHCP only: Enables a means for relaying DHCP and BOOTP requests from a client on a network with no DHCP servers to servers on other networks. For more information, see the `dhcrelay`(8) man page.
`/usr/lib/inet/in.dhcpd`	Legacy Sun DHCP only: The legacy Sun DHCP server daemon. The daemon is started when the system is started. You should not start the server daemon directly. Use DHCP Manager, the `svcadm` command, or `dhcpconfig` to start and stop the daemon. The daemon should be invoked directly only to run the server in debug mode to troubleshoot problems. For more information, see the `in.dhcpd`(1M) man page.
`/usr/sadm/admin/bin/dhcpmgr`	Legacy Sun DHCP only: DHCP Manager, a graphical user interface (GUI) tool used to configure and manage the DHCP service. DHCP Manager is the recommended DHCP management tool. For more information, see the `dhcpmgr`(1M) man page.

TABLE 4–1 Commands Used in DHCP *(Continued)*

Command	Description
`/usr/sbin/dhcpagent`	The DHCP client daemon, which implements the client side of the DHCP protocol. For more information, see the `dhcpagent(1M)` man page.
`/usr/sbin/dhcpconfig`	Legacy Sun DHCP only: Used to configure and unconfigure DHCP servers and BOOTP relay agents. Also used to convert to a different data store format, and to import and export DHCP configuration data. For more information, see the `dhcpconfig(1M)` man page.
`/usr/sbin/dhcpinfo`	Legacy Sun DHCP only: Used by system startup scripts on Oracle Solaris client systems to obtain information (such as the 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. For more information, see the `dhcpinfo(1)` man page.
`/usr/sbin/dhtadm`	Legacy Sun DHCP only: Used to make changes to the options and macros in the `dhcptab` table. This command is most useful in scripts that you create to automate changes to your DHCP information. Use `dhtadm` with the `-P` option, and pipe the output through the `grep` command for a quick way to search for particular option values in the `dhcptab` table. For more information, see the `dhtadm(1M)` man page.
`/usr/sbin/ipadm`	Used at system boot to assign IP addresses to network interfaces, configure network interface parameters, or both. On a DHCP client, `ipadm` starts DHCP to get the parameters (including the IP address) needed to configure a network interface. For more information, see the `ipadm(1M)` man page.
`/usr/sbin/omshell`	ISC DHCP only: Provides a way to query and change the ISC DHCP server's state by using the Object Management API (OMAPI). For more information, see the `omshell`(1) man page.
`/usr/sbin/pntadm`	Legacy Sun DHCP only: Used to make changes to the DHCP network tables that map client IDs to IP addresses and optionally associate configuration information with IP addresses. For more information, see the `pntadm(1M)` man page.
`/usr/sbin/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. For more information, see the `snoop(1M)` man page.

Files Used by the DHCP Service

The following table lists the files that are associated with DHCP.

TABLE 4–2 Files and Tables Used by DHCP Daemons and Commands

File or Table Name	Description
`dhcptab`	Legacy Sun DHCP only: A generic term for the table of DHCP configuration information that is 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 that you use for DHCP information. For more information, see the `dhcptab(4)` man page.
DHCP network table	Legacy Sun DHCP only: Maps IP addresses to client IDs and configuration options. DHCP network tables are named according to the IP address of the network, such as `10.21.32.0`. There is no file that is called `dhcp_network`. The name and location of DHCP network tables is determined by the data store that you use for DHCP information. For more information, see the `dhcp_network(4)` man page.
`/etc/dhcp/eventhook`	Legacy Sun DHCP only: A script or executable that the `dhcpagent` daemon can automatically run. For more information, see the `dhcpagent(1M)` man page.
`/etc/inet/dhcpd4.conf` `/etc/inet/dhcpd6.conf`	ISC DHCP only: Contains configuration information for the ISC DHCP server, `dhcpd`. For more information, see the `dhcpd.conf`(5) man page.
`/etc/inet/dhcpsvc.conf`	Legacy Sun DHCP only: Stores startup options for the DHCP daemon and data store information. This file must not be edited manually. Use the `dhcpconfig` command to change startup options. For more information, see the `dhcpsvc.conf(4)` man page.
`/etc/dhcp/`*interface*`.dhc` `/etc/dhcp/`*interface*`.dh6`	Contains the configuration parameters that are obtained from DHCP for the given network interface. For DHCPv4 the filename ends with `dhc`. For DHCPv6, the filename ends with `dh6`. The client caches the current configuration information in `/etc/dhcp/`*interface*`.dhc` when the interface's IP address lease is dropped. For example, if DHCP is used on the `qe0` interface, the `dhcpagent` caches the configuration information in `/etc/dhcp/qe0.dhc`. 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 process for DHCP lease negotiation.
`/etc/default/dhcpagent`	Sets parameter values for the `dhcpagent` client daemon. See the `/etc/default/dhcpagent` file or the `dhcpagent(1M)` man page for information about the parameters.

TABLE 4–2 Files and Tables Used by DHCP Daemons and Commands *(Continued)*

File or Table Name	Description
`/etc/dhcp/inittab` `/etc/dhcp/inittab6`	Legacy Sun DHCP only: Defines aspects of DHCP option codes, such as the data type, and assigns mnemonic labels. See the `dhcp_inittab(4)` man page for more information about the file syntax. The `/etc/dhcp/inittab6` is used by the DHCPv6 clients. On the client, the information in the `/etc/dhcp/inittab` file is used by the `dhcpinfo` command to provide more meaningful information to human readers of the information. On the DHCP server system, this file is used by the DHCP daemon and management tools to obtain DHCP option information. The `/etc/dhcp/inittab` file replaces the `/etc/dhcp/dhcptags` file that was used in previous releases.

`/var/db/isc-dhcp/dhcp4.leases`
`/var/db/isc-dhcp/dhcp4.leases~`
`/var/db/isc-dhcp/dhcp6.leases`
`/var/db/isc-dhcp/dhcp6.lease~`
	ISC DHCP only: Lists leases for DHCPv4 and DHCPv6 servers. Files with "~" at end of the file name are previous copies.

SMF Services Used by the DHCP Service

The following table lists the SMF services associated with DHCP.

TABLE 4–3 SMF Services Used by DHCP Daemons and Commands

SMF Service Name	Description
`svc:/network/dhcp-server:default`	Contains information for the legacy Sun DHCP service.
`svc:/network/dhcp/server:ipv4` `svc:/network/dhcp/server:ipv6`	Contains information for the ISC DHCP service.
`svc:/network/dhcp/relay:ipv4` `svc:/network/dhcp/relay:ipv6`	Contains information for the service that can relay DHCP or BOOTP requests to a remote ISC DHCP server.
`svc:/network/dns/client`	Contains information used to resolve DNS queries. During DHCP server configuration, this SMF service is consulted for information about the DNS domain and DNS server.
`svc:/system/name-service/switch`	Specifies the location of name service databases and the order in which to search name services for various kinds of information. This service provides accurate configuration information when you configure a DHCP service.

Index