Working With DHCP in Oracle® Solaris 11.3

Part No: E54848
November 2016

Working With DHCP in Oracle Solaris 11.3

Part No: E54848

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support 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.

Référence: E54848

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d' applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation 9

1 About DHCP (Overview) 11
About the DHCP Protocol 11
Advantages of Using DHCP 12
How DHCP Works 13
ISC DHCP Server 16
Legacy Sun DHCP Server 16

2 Administering the ISC DHCP Service 17
ISC DHCP Server Tasks 17
▼ How to Grant User Access to DHCP Commands 17
▼ How to Configure an ISC DHCP Server 18
▼ How to Modify the Configuration of the DHCP Service 18

3 Configuring and Administering the DHCP Client 21
About the DHCP Client 21
DHCP Administrative Model 22
DHCP Protocol Details 23
Logical Interfaces 23
Option Negotiation 24
`PARAM_REQUEST_LIST` Keyword Configuration Syntax 24
DHCP Client Startup 25
▼ How to Stop the DHCPv6 Service 25
DHCPv6 Communication 25
How DHCP Client Protocols Manage Network Configuration Information 26
DHCP Client Shutdown 27
Enabling and Disabling a DHCP Client 27
▼ How to Enable a DHCP Client 27
▼ How to Disable a DHCP Client 28

DHCP Client Administration 29
ipadm Command Options for Working With the DHCP Client 29
Setting DHCP Client Configurations 30
DHCP Clients With Multiple Network Interfaces 31
DHCPv4 Client Host Names 32
▼ How to Enable a DHCPv4 Client to Request a Specific Host Name 32
DHCP Client and Name Services 33
DHCP Client Event Scripts 33

4 DHCP Commands and Files (Reference) 37
DHCP Commands 37
Files Used by the DHCP Service 38
SMF Services Used by the DHCP Service 38
DHCP RFCs 39

Index 41

Tables

TABLE 1 Name Service Client Setup Information for DHCP Client 33
TABLE 2 DHCP Client Event Script Keywords 34
TABLE 3 Commands Used in DHCP 37
TABLE 4 Files and Tables Used by DHCP Daemons and Commands 38
TABLE 5 SMF Services Used by DHCP Daemons and Commands 38

Using This Documentation

- **Overview** – Describes how to set up DHCP services on DHCP servers and DHCP clients
- **Audience** – Technicians, system administrators, and authorized service providers
- **Required knowledge** – Experience administering an Oracle Solaris system

Product Documentation Library

Documentation and resources for this product and related products are available at `http://www.oracle.com/pls/topic/lookup?ctx=E53394`.

Feedback

Provide feedback about this documentation at `http://www.oracle.com/goto/docfeedback`.

♦ ♦ ♦ CHAPTER 1

About DHCP (Overview)

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" on page 11
- "Advantages of Using DHCP" on page 12
- "How DHCP Works" on page 13
- "ISC DHCP Server" on page 16
- "Legacy Sun DHCP Server" on page 16

About the DHCP Protocol

The DHCP protocol enables automatic network configuration of systems in a TCP/IP network. DHCP uses a client-server mechanism. DHCP servers store and manage configuration information for DHCP 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 DHCP client and DHCP 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* enable IP addresses to be reclaimed when they are not in use. The reclaimed IP addresses can be reassigned to other DHCP clients. A site that uses DHCP can use a smaller pool of IP addresses than would be needed if all DHCP clients were assigned a permanent IP address.

An implementation of the Internet Systems Consortium (ISC) DHCP server is included in Oracle Solaris. For more information, see "ISC DHCP Server" on page 16.

Advantages of Using DHCP

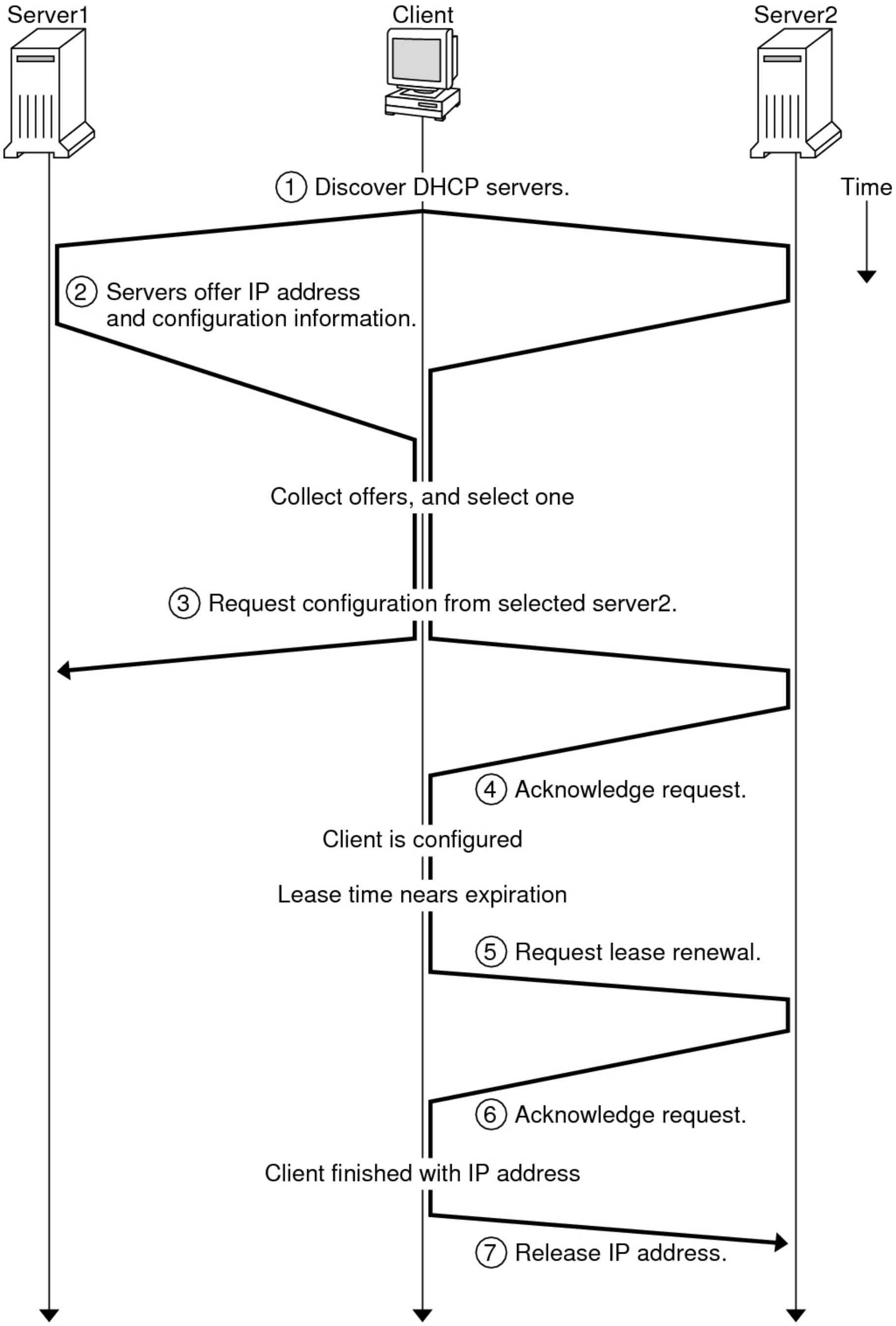
DHCP relieves you of some of the time-consuming tasks involved in setting up a TCP/IP network and in the daily management of that network. DHCP offers the following advantages:

- **IP address management** – In a network without DHCP, you must manually assign IP addresses. You must be careful to assign unique IP addresses to each system and to configure each system individually. If a system moves to a different network, you must make manual modifications for that stem. When DHCP is enabled, the DHCP server manages and assigns IP addresses without administrator intervention. CP clients can move to other networks without the necessity for manual reconfiguration because they obtain newinformation appropriate for the new network from a DCHP server.
- **Centralized network client configuration** – You can create a tailored configuration for certain stems, or for certain types of stems. The configuration information is stored on the DHCP server so you do not need to log in to a stem to change its configuration. You can make changes for multiple stems just by changing the information in the configuration files on the DHCP server.
- **Support for BOOTP clients** – Both BOOTP servers and DHCP servers listen and respond to broadcasts from ystems. 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 boot server.
- **Support for local systems and remote stems** – 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 DHCP requests to DHCP servers that are not on the DHCP client's network 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** – Instead of having to use RARP (Reverse Address Resolution Protocol) and the `bootparams` file, stems can use DHCP to obtain the information that is needed to boot from an boot server on the network. Because RARP booting requires that each subnet have a boot server but DHCP requests can be relayed across subnets, you can deploy fewer boot servers in your network when you use DHCP network booting.
- **Large network support** – DHCP provides the following features that support large networks:
  - The deployment of DHCP servers can be centralized or decentralized.
  - Single DHCP servers can be configured to manage multiple physical networks that are not directly connected to the server with the help of DHCP relay agent.
  - ISC DHCP provides failover between DHCP servers so that when one server fails, the other will cover for it.
  - ISC DHCP load balancing enables more than one DHCP server to provide service at the same time.
  - Multithreading so the DHCP server can process many requests simultaneously.

How DHCP Works

The sequence of events for DHCP service using IPv4 is shown in the following diagram. The numbers in circles correlate to the numbered items in the description following the diagram.

FIGURE 1 Sequence of Events for DHCP Service


Server1
Client
Server2
1 Discover DHCP servers.
Time
2 Servers offer IP address and configuration information.
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
7 Release IP address.

The diagram shows the following steps:

1. The DHCP 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:

   - The network interface on which the request came in. The DHCP server determines whether the DHCP client is on the network to which the interface is connected or is using a BOOTP relay agent connected to that network.
   - Whether 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 DHCP server detects a *relay agent address*, the server knows that the network portion of the address indicates the DHCP client's network address because the relay agent must be connected to the client's network.
   - Whether the DHCP client's network is subnetted. The DHCP 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 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 DHCP 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 DHCP client by broadcasting an *offer message*, which 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 indicates whether it will use the IP address.
3. The DHCP 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 DHCP server that made the best offer. The broadcast indicates to all the responding DHCP servers 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 DHCP server allocates the IP address for the DHCP client and stores the information in the DHCP configuration files. 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 DHCP client monitors the lease time. When a set period of time has elapsed, the client sends a new message to the chosen DHCP 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 DHCP client no longer needs the IP address, the client notifies the DHCP 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 ISC DHCP server is included in Oracle Solaris. is software is not automatically installed.u can add the DHCP server to your system by typing the following command:

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

Some of the important additions for ISC DHCP in the Oracle Solaris release are:

- Several services to support ISC DHCP and the legacy Sun DHCP service. See "SMF Services Used by the DHCP Service" on page 38 for a list of all of the services used by DHCP.
- Three commands: `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.
- The DHCP server configuration files are `/etc/inet/dhcpd4.conf` for DHCPv4 and `/etc/inet/dhcpd6.conf` for DHCPv6.
- A user called `dhcpserv` for the ISC DHCP service.
- A user login or role can use the `solaris.smf.manage.dhcp` and `solaris.smf.value.dhcp` authorizations to provide access to the DHCP commands.

In addition, the ISC DHCP server 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 web page.

Legacy Sun DHCP Server

The legacy Sun DHCP server software is still included in this 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) in the Oracle Solaris 10 documentation set.

♦ ♦ ♦ CHAPTER 2

Administering the ISC DHCP Service

This chapter describes the tasks that you might find useful when you administer the ISC DHCP service.

ISC DHCP Server Tasks

The most important tasks for administering an ISC DHCP server are:

- "How to Grant User Access to DHCP Commands" on page 17
- "How to Configure an ISC DHCP Server" on page 18
- "How to Modify the Configuration of the DHCP Service" on page 18

▼ 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 an appropriate role.**

   Assume a role that can grant the DHCP Management profile to users. If the DHCP Management profile has not been assigned to a user, assume the `root` role.

   Roles contain authorizations and privileged commands. For more information about roles, see "Creating a Role" in *Securing Users and Processes in Oracle Solaris 11.3*. For more information about the DHCP Management profile, see "How to Grant User Access to DHCP Commands" on page 17.

2. **Grant the DHCP Management profile to a user.**

```
# usermod -P+"DHCP Management" username
```

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 "Creating a Role" in *Securing Users and Processes in Oracle Solaris 11.3*.

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

   - **IPv4**: `/etc/inet/dhcpd4.conf`
   - **IPv6**: `/etc/inet/dhcpd6.conf`

   For more information, see the `dhcpd.conf`(7) 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 an appropriate role.**

   Assume a role that can grant the DHCP Management profile to users. If the DHCP Management profile has not been assigned to a user, assume the `root` role.

Roles contain authorizations and privileged commands. For more information about roles, see "Creating a Role" in *Securing Users and Processes in Oracle Solaris 11.3*. For more information about the DHCP Management profile, see "How to Grant User Access to DHCP Commands" on page 17.

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

   - **IPv4**: `/etc/inet/dhcpd4.conf`
   - **IPv6**: `/etc/inet/dhcpd6.conf`

   For more information, see the `dhcpd.conf`(7) man page.

3. **Restart the SMF service.**

   ```
   # svcadm restart 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

♦ ♦ ♦ 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.

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

The DHCPv6 protocol 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 protocol to obtain configuration parameters.

This chapter contains the following information:

- “About the DHCP Client” on page 21
- “Enabling and Disabling a DHCP Client” on page 27
- “DHCP Client Administration” on page 29
- “DHCP Clients With Multiple Network Interfaces” on page 31
- “DHCPv4 Client Host Names” on page 32
- “DHCP Client and Name Services” on page 33
- “DHCP Client Event Scripts” on page 33

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.

The `dhcpagent` daemon is run on the DHCP client. If you install Oracle Solaris by using the LiveCD GUI installer or by specifying DHCP in the text installer, 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 clients that use the DHCP service.

If a system is already running Oracle Solaris but not using DHCP, you can reconfigure the system to use DHCP. You can also reconfigure a DHCP client so that it stops using DHCP and uses static network information that you provide. See "Enabling and Disabling a DHCP Client" on page 27 for more information.

DHCP Administrative Model

DHCPv4 requires explicit client configuration. You must set up the DHCPv4 system for addressing either 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. The signal to use DHCPv6 is carried in Router Advertisement messages from local routers. The `dhcpagent` daemon 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 DHCP 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.

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 (`net0:1`), DUID+IAID is used if no client ID is configured.

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 supplies 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:

net0.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 one IAID to each interface on demand. 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. You can configure specific logical interfaces to run DHCP by specifying a value for `CLIENT_ID` in the `dhcpagent` configuration file. For example:

net0.v6.CLIENT_ID=*DUID*

DHCPv6 works differently because the zeroth logical interface (also known as the “physical” 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 no other assignment method is available, such as a DHCP server. Because the zeroth logical interface cannot be under DHCP control, even though DHCPv6 is run on the zeroth logical 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

DHCPv6 has an Option Request option that 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 can either use the hint to choose among the options to include in the reply or ignore the hint and choose other items to include. On Oracle Solaris, for example, the preferred options might include the 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`.

`PARAM_REQUEST_LIST` Keyword Configuration Syntax

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

The syntax is augmented with a “.v6” marker between the interface name (if any) and the parameter to be configured. The following examples show how to set various configuration options.

To set the global IPv4 option request list:

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

To configure an individual interface to omit the hostname option:

```
net0.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
```

To set an individual interface:

```
net0.v6.PARAM_REQUEST_LIST=21,22,23,24
```

The following example shows a sample `/etc/default/dhcpagent` file for a 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, the in.ndpd daemon starts up DHCPv6 automatically when it is needed.

For DHCPv4, however, you must reconfigure the DHCP client if DHCPv4 was not configured during as part of the installation process. For complete instructions, see “How to Enable a DHCP Client” on page 27.

With either DHCP protocol, 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.

At startup, if persistent DHCP configurations exist in the system, the dhcpagent daemon is started as part of the startup script processes. The dhcpagent daemon then configures the network interfaces as described in “How DHCP Works” on page 13.

▼ How to Stop the DHCPv6 Service

Although the default is to run DHCPv6, 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.

1. **Assume the root role.**

   Roles contain authorizations and privileged commands. For more information about roles, see “Creating a Role” in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Temporarily kill the DHCPv6 service.**

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

3. **Prevent the DHCPv6 service from restarting if the system is rebooted.**

   First, change the /etc/inet/ndpd.conf file to prevent DHCPv6 from starting on reboot. Then stop the service that is currently running.

   ```
   # echo ifdefault StatefulAddrConf false >> /etc/inet/ndpd.conf
   # pkill -HUP -x in.ndpd
   ```

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. On DHCPv6 networks, the `in.ndpd` daemon provides host autoconfiguration.

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

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

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 a DHCP server, see Chapter 1, “About DHCP (Overview)”.

How the DHCPv6 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 searches 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 33 for more information about using the event executable.

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. Because the lease is saved rather than released by default, the DHCP server cannot 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 (DHCPv4) or Confirm (DHCPv6) message to use the same IP address and network configuration information.

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 DHCP client to use the information, `dhcpagent` initiates the DHCP protocol sequence described in "How DHCP Works" on page 13. As a result, the client obtains new network configuration information.

Enabling and Disabling a DHCP Client

To enable or disable a DHCP client, you must reconfigure the system.

Note - In many deployments, crucial parts of the infrastructure are set up with static IP addresses rather than using DHCP. Determining which devices or systems on your network should be configured as DHCP clients (for example routers and systems providing certain srvices)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 an appropriate role.**

Assume a role that can grant the DHCP Management profile to users. If the DHCP Management profile has not been assigned to a user, assume the `root` role.

Roles contain authorizations and privileged commands. For more information about roles, see "Creating a Role" in *Securing Users and Processes in Oracle Solaris 11.3*. For more information about the DHCP Management profile, see "How to Grant User Access to DHCP Commands" on page 17.

2. **Reconfigure the system.**

   - **To interactively reconfigure the system:**

     a. **Issue the following command.**

     ```
     # sysconfig configure -g network,naming_services
     ```

     b. **When the tool starts, select Automatic network configuration on the Network screen.**

   - **To non-interactively reconfigure the system using a system configuration profile, issue the following command.**

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

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

How to Disable a DHCP Client

1. **Assume an appropriate role.**

   Assume a role that can grant the DHCP Management profile to users. If the DHCP Management profile has not been assigned to a user, assume the `root` role.

   Roles contain authorizations and privileged commands. For more information about roles, see "Creating a Role" in *Securing Users and Processes in Oracle Solaris 11.3*. For more information about the DHCP Management profile, see "How to Grant User Access to DHCP Commands" on page 17.

2. **Reconfigure the system.**

   Choose one of the following configuration methods:

   - **To interactively reconfigure the system.**

     a. **Issue the following command.**

```
# sysconfig configure
```

b. **When the tool starts, select either Manual or None as the network configuration on the Network screen.**

- **To non-interactively reconfigure the system using a system configuration profile, issue the following command.**

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

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

DHCP Client Administration

The `dhcpagent` daemon 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 a privileged user on the DHCP client, you can use the `ipadm` command to affect the `dhcpagent` daemon's management of the network interface, if necessary.

`ipadm` Command Options for Working With the DHCP Client

This section summarizes actions that you can accomplish by using `ipadm` command options. These options are documented in the `ipadm`(1M) man page.

- **Create the IP interface** – The `ipadm create-ip` command 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 `ipadm create-addr -T dhcp` *DHCP-addrobj* command initiates the interaction between the `dhcpagent` daemon 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 `ipadm refresh-addr -i` *DHCP-addrobj* command 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 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 systems on the network.

- **Request a lease extension** – The`ipadm refresh-addr` *DHCP-addrobj* command causes `dhcpagent` to issue a request to renew the lease. The DHCP 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 `ipadm delete-addr -r` *DHCP-addrobj* command 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.
- **Release the IP address** – The `ipadm delete-addr -r` *DHCP-addrobj* command 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.
- **Drop the IP address** – The `ipadm delete-addr` *DHCP-addrobj* command 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 DHCP 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 Configurations

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.

Configurations for DHCPv4 and DHCPv6

- The system uses DHCP on one physical network interface.

  If you want to use DHCP on more than one physical network interface, see "DHCP Clients With Multiple Network Interfaces" on page 31.
- The DHCP client is not automatically configured as a name service client if the DHCP client was configured after the Oracle Solaris installation.

See "DHCP Client and Name Services" on page 33 for information about using name services with DHCP clients.

Default DHCPv4 Configuration

- 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 32.
- Default requests for the client are given in `/etc/default/dhcpagent`, and includes DNS Server, DNS domain, and broadcast address.

  You can set up the DHCP client's parameter file 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.

DHCP Clients With Multiple Network Interfaces

The `dhcpagent` daemon 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 `dhcpagent` daemon 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.

Global parameters apply to the system as a whole rather than to a particular network interface, for example, the host name, NIS domain name, and time zone. 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 `dhcpagent` daemon manages leases for logical interfaces and physical interfaces in much the same way. However, it does not manage the default routes that are associated with logical interfaces because the Oracle Solaris kernel associates routes with physical interfaces not logical interfaces. When a physical interface's IP address is established, you should place the necessary default routes 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 `dhcpagent` daemon removes the default routes that are associated with the interface. When a lease expires on a logical interface, the daemon 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.

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 `dhcpagent`aemon does not receive a host name through the DHCP service, the emonchecks 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 DHCP 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 DHCP client to use a specific host name, you can enable the client to request that name. See the following procedure.

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

The following procedure does not work with all DHCP servers because the DHCP server does not have to respect a request for a specific host name and many do not. In some cases, they simply return a different name.

1. **Assume an appropriate role.**

   Assume a role that can grant the DHCP Management profile to users. If the DHCP Management profile has not been assigned to a user, assume the `root` role.

   Roles contain authorizations and privileged commands. For more information about roles, see "Creating a Role" in *Securing Users and Processes in Oracle Solaris 11.3*. For more information about the DHCP Management profile, see "How to Grant User Access to DHCP Commands" on page 17.

2. **If the IP interface does not yet exist, create the IP interface.**

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

3. **If the IP interface already exists with a DHCP address, delete the existing DHCP address.**

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

4. **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 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 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 1 Name Service Client Setup Information for DHCP Client

Name Service	Client Setup Information
`/etc/inet/hosts`	You must set up the `/etc/inet/hosts` file for a DHCP clienthat is to use `/etc/inet/hosts` for its name service. The DHCP client'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 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 receives the DNS domain name through DHCP, then properties of the `dns/client` SMF service are also automatically configured. See *Working With Oracle Solaris 11.3 Directory and Naming Services: DNS and NIS* for more information about DNS.

DHCP Client Event Scripts

You can set up the DHCP client to run an executable program or script, called an *event script*, that can perform any action that is appropriate for the client system. The program or script is automatically executed after certain DHCP lease events occur. You can use the event script 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 event keywords listed in the following table are used by `dhcpagent` to signify DHCP lease events.

TABLE 2 DHCP Client Event Script Keywords

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.
`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.
`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.
`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.
`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. The addresses being removed are marked with the `IFF_DEPRECATED` flag.
`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.

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 new events might be added in the future, 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. For information about how to use the commands, see the related man pages.

The chapter contains the following information:

- "DHCP Commands" on page 37
- "Files Used by the DHCP Service" on page 38
- "SMF Services Used by the DHCP Service" on page 38

DHCP Commands

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

TABLE 3 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 DHCP client on a network with no DHCP servers to DHCP servers on other networks. For more information, see the dhcrelay(8) man page.
/usr/sbin/dhcpagent	The dhcpagent daemon, which implements the client side of the DHCP protocol. For more information, see the dhcpagent(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/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 Files and Tables Used by DHCP Daemons and Commands

File or Table Name	Description
`/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`(7) 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.

`/var/db/isc-dhcp/dhcp4.leases` `/var/db/isc-dhcp/dhcp6.leases`	

SMF Services Used by the DHCP Service

The following table lists the SMF services associated with DHCP.

TABLE 5 SMF Services Used by DHCP Daemons and Commands

SMF Service Name	Description
`svc:/network/dhcp/client`	Contains the `config/debug` and `config/verbose` SMF properties to enable debug logging of the `dhcpagent` daemon.
`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.

DHCP RFCs

For more information about DHCP, see the following RFCs:

- RFC 0951: Bootstrap Protocol
- RFC 1542: Clarifications and Extensions for the Bootstrap protocol
- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 5494: IANA Allocation Guidelines for the Address Resolution Protocol (ARP)
- RFC 6221: Lightweight DHCPv6 Relay Agent
- RFC 6422: Relay-Supplied DHCP Options
- RFC 6644: Rebind Capability in DHCPv6 Reconfigure Messages
- RFC 7083: Modification to Default Values of SOL_MAX_RT and INF_MAX_RT

Index

A

administrative model, 22
advantages to using the DHCP protocol, 12

B

BOOTP protocol
- DHCP servers and, 12
- relation to DHCP, 11

`BOUND` and `BOUND6` DHCP event script keywords, 34

C

client configuration, 22
client IDs
- in DHCPv4 and DHCPv6, 22

commands
- list of, 37

configuring
- DHCP client, 21
- ISC DHCP server, 18
- name services for DHCP client, 33

D

DHCP clients
- administration, 29
- configuration, 30
- configuring name services for, 33
- disabling, 28
- dropping IP address, 30
- enabling, 27
- event scripts, 33
- extending lease, 30
- host name
  - specifying, 32
- logical interfaces, 31
- multiple network interfaces, 31
- network information without lease, 29
- releasing IP address, 30, 30
- running programs with, 33
- shutting down, 27
- starting, 29
- startup, 25

DHCP commands
- granting user access to, 17
- list of, 37
- privileges, 17

DHCP events
- client scripts for, 33

DHCP files
- list of, 38

DHCP protocol
- advantages in Oracle Solaris implementation, 12
- overview, 11
- sequence of events, 13

DHCP RFCs, 39
DHCP server
- configuring, 18

DHCP SMF services
- list of, 38

DHCP tables
- list of, 38

`dhcpagent` daemon
- description, 25, 37

`dhcpagent` file
- server option negotiation, 24

`dhcpd` daemon
- description, 37

`dhcpd4.conf` file
- description, 38

`dhcpd6.conf` file

description, 38
DHCPv4
client IDs, 22
default configuration, 31
management of network interfaces, 26
DHCPv6
administrative model, 22
client IDs, 22
disabling, 25
starting automatically, 25
dhcrelay command
description, 37
disabling
DHCP clients, 28
DHCPv6, 25
DROP and DROP6 DHCP event script keywords, 34
DUID (DHCP Unique Identifier)
definition, 22

E
/etc/default/dhcpagent file
description, 30
/etc/dhcp/eventhook file
description, 34
/etc/dhcp/*interface*.dh* file
description, 38
/etc/inet/dhcpd4.conf file
description, 38
/etc/inet/dhcpd6.conf file
description, 38
enabling
DHCP clients, 27
event scripts
for DHCP clients, 33
eventhook file
description, 34
events
DHCP client scripts for, 33
EXPIRE and EXPIRE6 DHCP event script keywords, 34
EXTEND and EXTEND6 DHCP event script keywords, 34
extending DHCP lease, 30

H
host name
enabling client request of, 32

I
IA (Identity Association)
definition, 23
IAD (Identity Association Identifier)
definition, 22
in.ndpd daemon, 25
INFORM and INFORM6 DHCP event script keywords, 34
IP address management
DHCP and, 12
ipadm command
controlling DHCP client with, 29
DHCP and, 37
ISC DHCP server
configuring, 18
description, 16

L
large network support in DHCP, 12
logical interfaces, 23
configuring to run DHCP, 23
DHCP clients, 31
zeroth, 23
LOSS6 DHCP event script keyword, 34

M
MAC address
in DHCPv4 and DHCPv6, 22
multiple network interfaces
DHCP clients, 31

N
/network/dhcp/client SMF service
used by DHCP, 38
/network/dhcp/relay SMF service
description, 38
/network/dhcp/server SMF service

description, 38
/network/dns/client SMF service
used by DHCP, 38
name services
configuring for DHCP client, 33
negotiation
DHCP server, 24
network booting
DHCP and, 12
network interfaces
managing on DHCPv4 client, 26
multiple, 31

O
omshell command
description, 37
Option Request
in option negotiation, 24

P
PARAM_REQUEST_LIST keyword
in option negotiation, 24
privileges
to access DHCP commands, 17

R
RELEASE and RELEASE6 DHCP event script
keywords, 34
RFCs
related to DHCP, 39
Router Advertisement (RA), 25

S
/system/name-service/switch SMF service
used by DHCP, 38
scripts
DHCP client event scripts, 33
shutting down
DHCP, 27
SMF services
used by DHCP, 38
snoop command
DHCP and, 37
stopping
DHCPv6, 25

T
tables
list of, 38

U
/usr/lib/inet/dhcpd daemon
description, 37
/usr/lib/inet/dhcrelay command
description, 37
/usr/sbin/dhcpagent daemon
description, 37
/usr/sbin/ipadm command
DHCP and, 37
/usr/sbin/omshell command
description, 37
/usr/sbin/snoop command
DHCP and, 37
user access to DHCP commands
assigning, 17