

# Working With DHCP in Oracle® Solaris 11.4



Part No: E61005  
November 2020



Working With DHCP in Oracle Solaris 11.4

**Part No: E61005**

Copyright © 1999, 2020, Oracle and/or its affiliates.

**License Restrictions Warranty/Consequential Damages Disclaimer**

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

**Warranty Disclaimer**

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

**Restricted Rights Notice**

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

**Hazardous Applications Notice**

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

**Trademark Notice**

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

**Third-Party Content, Products, and Services Disclaimer**

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

**Pre-General Availability Draft Label and Publication Date**

Pre-General Availability: 2020-01-15

**Pre-General Availability Draft Documentation Notice**

If this document is in public or private pre-General Availability status:

This documentation is in pre-General Availability status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

**Oracle Confidential Label**

ORACLE CONFIDENTIAL. For authorized use only. Do not distribute to third parties.

**Revenue Recognition Notice**

If this document is in private pre-General Availability status:

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your pre-General Availability trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

**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: E61005**

Copyright © 1999, 2020, Oracle et/ou ses affiliés.

**Restrictions de licence/Avis d'exclusion de responsabilité en cas de dommage indirect et/ou consécutif**

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

**Exonération de garantie**

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.

**Avis sur la limitation des droits**

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 embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

**Avis sur les applications dangereuses**

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 un risque de 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 des applications dangereuses.

**Marques**

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 Inside 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, Epyc, et le logo AMD sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

**Avis d'exclusion de responsabilité concernant les services, produits et contenu tiers**

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.

**Date de publication et mention de la version préliminaire de Disponibilité Générale ("Pre-GA")**

Version préliminaire de Disponibilité Générale ("Pre-GA") : 15.01.2020

**Avis sur la version préliminaire de Disponibilité Générale ("Pre-GA") de la documentation**

Si ce document est fourni dans la Version préliminaire de Disponibilité Générale ("Pre-GA") à caractère public ou privé :

Cette documentation est fournie dans la Version préliminaire de Disponibilité Générale ("Pre-GA") et uniquement à des fins de démonstration et d'usage à titre préliminaire de la version finale. Celle-ci n'est pas toujours spécifique du matériel informatique sur lequel vous utilisez ce logiciel. Oracle Corporation et ses affiliés déclinent expressément toute responsabilité ou garantie expresse quant au contenu de cette documentation. Oracle Corporation et ses affiliés ne sauraient en aucun cas être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'utilisation de cette documentation.

**Mention sur les informations confidentielles Oracle**

INFORMATIONS CONFIDENTIELLES ORACLE. Destinées uniquement à un usage autorisé. Ne pas distribuer à des tiers.

**Avis sur la reconnaissance du revenu**

Si ce document est fourni dans la Version préliminaire de Disponibilité Générale ("Pre-GA") à caractère privé :

Les informations contenues dans ce document sont fournies à titre informatif uniquement et doivent être prises en compte en votre qualité de membre du customer advisory board ou conformément à votre contrat d'essai de Version préliminaire de Disponibilité Générale ("Pre-GA") uniquement. Ce document ne constitue en aucun cas un engagement à fournir des composants, du code ou des fonctionnalités et ne doit pas être retenu comme base d'une quelconque décision d'achat. Le développement, la commercialisation et la mise à disposition des fonctions ou fonctionnalités décrites restent à la seule discrétion d'Oracle.

Ce document contient des informations qui sont la propriété exclusive d'Oracle, qu'il s'agisse de la version électronique ou imprimée. Votre accès à ce contenu confidentiel et son utilisation sont soumis aux termes de vos contrats, Contrat-Cadre Oracle (OMA), Contrat de Licence et de Services Oracle (OLSA), Contrat Réseau Partenaires Oracle (OPN), contrat de distribution Oracle ou de tout autre contrat de licence en vigueur que vous avez signé et que vous vous engagez à respecter. Ce document et son contenu ne peuvent en aucun cas être communiqués, copiés, reproduits ou distribués à une personne extérieure à Oracle sans le consentement écrit d'Oracle. Ce document ne fait pas partie de votre contrat de licence. Par ailleurs, il ne peut être intégré à aucun accord contractuel avec Oracle ou ses filiales ou ses affiliés.

#### **Accessibilité de la documentation**

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité de 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

---

<b>Using This Documentation</b> .....	9
<b>1 About DHCP (Overview)</b> .....	11
About the DHCP Protocol .....	11
Advantages of Using DHCP .....	12
How DHCP Works .....	13
ISC DHCP Server .....	16
<b>2 Administering the ISC DHCP Service</b> .....	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 .....	19
<b>3 Configuring and Administering the DHCP Client</b> .....	21
About the DHCP Client .....	21
DHCP Administrative Model .....	22
DHCP Client Startup .....	22
▼ How to Stop the DHCPv6 Service .....	23
DHCPv6 Communication .....	23
How DHCP Client Protocols Manage Network Configuration Information .....	24
DHCP Client Shutdown .....	25
Enabling and Disabling a DHCP Client .....	25
▼ How to Enable a DHCP Client .....	26
▼ How to Disable a DHCP Client .....	26
DHCP Client Administration .....	27
ipadm Command Options for Working With the DHCP Client .....	27
DHCP Protocol Details .....	29

Logical Interfaces .....	30
Option Negotiation .....	30
param_request_list Property Configuration Syntax .....	31
Setting DHCP Client Configurations .....	31
DHCP Clients With Multiple Network Interfaces .....	32
DHCPv4 Client Host Names .....	32
▼ How to Enable a DHCPv4 Client to Request a Specific Host Name .....	33
DHCP Clients and Name Services .....	34
<b>4 DHCP Commands and Files (Reference) .....</b>	<b>35</b>
DHCP Commands .....	35
Files Used by the DHCP Service .....	36
SMF Services Used by the DHCP Service .....	36
DHCP RFCs .....	37
<b>Index .....</b>	<b>39</b>



## Using This Documentation

---

- **Overview** – Describes how to administer the DHCP service to automatically configure the network for a system while the system boots.
- **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=E37838-01>.

## 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](#)

## 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:

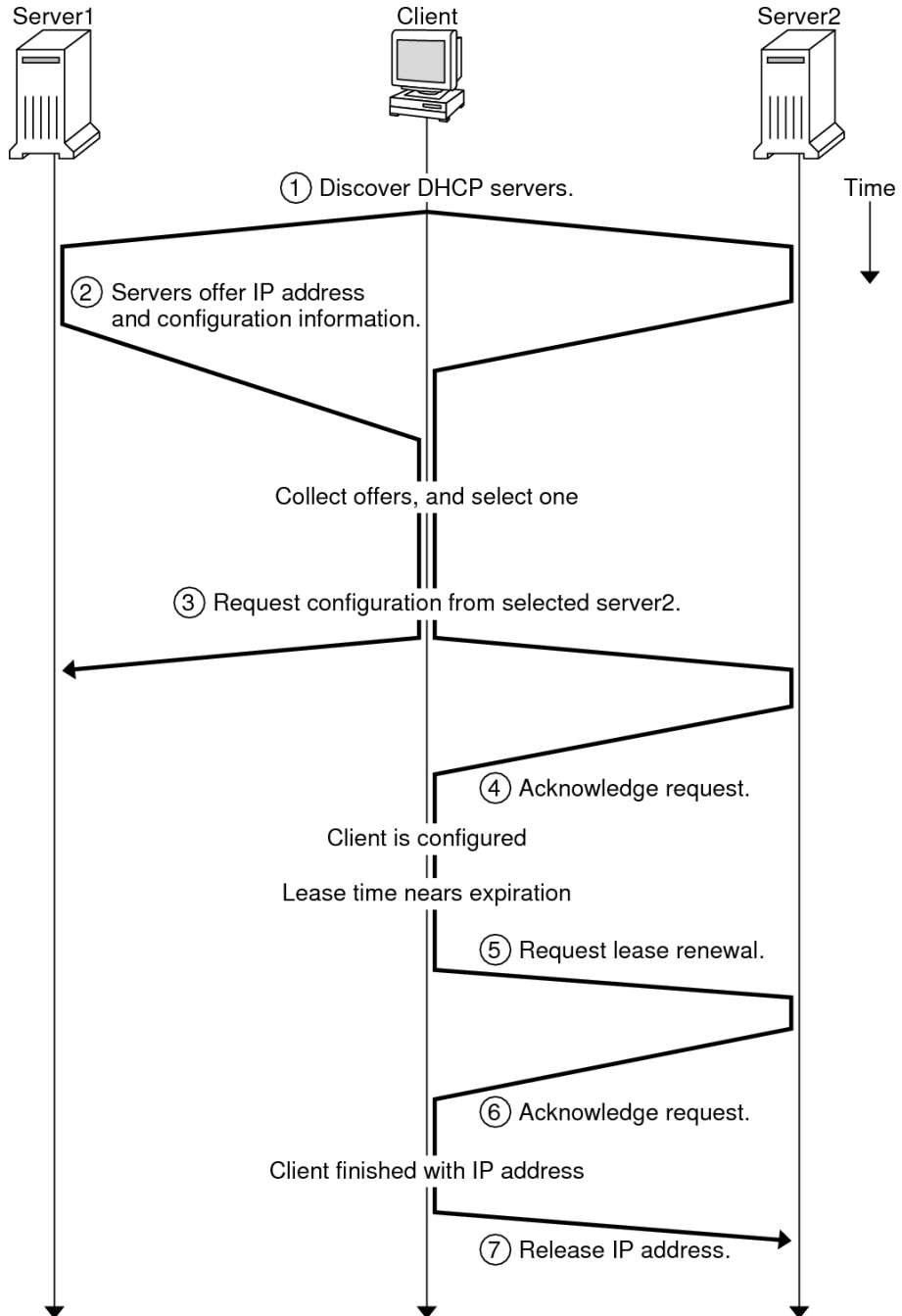
- **IP address management** – In a network without DHCP, you must manually assign IP addresses. You must be careful to assign unique IP addresses to each system and to configure each system individually. If a system moves to a different network, you must make manual modifications for that system. When DHCP is enabled, the DHCP server manages and assigns IP addresses without administrator intervention. DHCP clients can move to other networks without the necessity for manual reconfiguration because they obtain new information appropriate for the new network from a DHCP server.
- **Centralized network client configuration** – You can create a tailored configuration for certain systems, or for certain types of systems. The configuration information is stored on the DHCP server so you do not need to log in to a system to change its configuration. You can make changes for multiple systems 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 systems. 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 systems** – 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, systems 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



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\(5\)](#) man page for information about 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. This software is not automatically installed. You 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. See [“SMF Services Used by the DHCP Service” on page 36](#) for a list of all of the services used by DHCP.
- Three commands: `dhcpcd`, `dhcprelay`, and `omshell`. See [“Files Used by the DHCP Service” on page 36](#) for a list of all of the commands that are associated with DHCP.
- The DHCP server configuration files are `/etc/inet/dhpcpd4.conf` for DHCPv4 and `/etc/inet/dhpcpd6.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.



# ◆◆◆ 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 19](#)

### ▼ 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\(7\)](#), [exec\\_attr\(5\)](#), and [user\\_attr\(5\)](#).

#### 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 11.4\*](#). 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 11.4\*](#).

**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 11.4\*](#). 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/      Provides DHCP and BOOTP requests from IPv4 clients
dhcp/server:ipv4
```

```
svc:/network/      Provides DHCP and BOOTP requests from IPv6 clients
dhcp/server:ipv6
```

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

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



## 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 25](#)
- [“DHCP Client Administration” on page 27](#)
- [“DHCP Clients With Multiple Network Interfaces” on page 32](#)
- [“DHCPv4 Client Host Names” on page 32](#)
- [“DHCP Clients and Name Services” on page 34](#)

### About the DHCP Client

The `dhcagent` daemon is run on the DHCP client. If you install Oracle Solaris 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 25](#) 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(8)` 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 `dhcpgent` 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.

## 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 26](#).

With either DHCP protocol, the `dhcpgent` daemon obtains configuration information that is needed by other processes involved in booting the system. For this reason, the system startup scripts start `dhcpgent` 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 `dhcpgent` daemon is started as part of the startup script processes. The `dhcpgent` 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 11.4\*](#).

### 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 about the interaction between DHCPv4 client and a DHCP server, see [Chapter 1, “About DHCP \(Overview\)”](#).

### How the DHCPv6 Client Manages Network Configuration Information

DHCPv6 communication between a DHCP client and a DHCP 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 DHCP server can supply.

A DHCP 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 be most efficient for the DHCP server to provide the same ones. Regardless of the client's actions (even if it requests no addresses at all), the DHCP server can supply any number of addresses to the DHCP client for a single DHCPv6 transaction.

The typical message dialogue that takes place between the DHCP clients and DHCP servers is as follows:

- A DHCP client sends a Solicit message to locate DHCP servers.
- DHCP servers send an Advertise message to indicate they are available for DHCP service.
- A DHCP client sends a Request message to request configuration parameters, including IP addresses, from DHCP servers with the greatest preference values.  
DHCP server preference values are set by the administrator and extend from 0, at the lowest end, to 255 at the highest.
- The DHCP 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 DHCP server. If the most preferred server does not respond or fails to give a successful



Reply message in answer to the Request message, then the client continues looking for less-preferred DHCP servers (in order) until it has no more Advertise messages. At that point, the client starts over by again sending Solicit messages.

The chosen DHCP 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 `dhcpcd` daemon sends a Release message to the DHCP server that assigned addresses to the DHCP client to indicate that the client will no longer use one or more of the assigned addresses. When the DHCPv4 client shuts down normally, `dhcpcd` writes the current configuration information to a file, if the file exists. The filename for DHCPv4 is `/var/dhcp/interface.dhc`, and `/var/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 DHCP 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, `dhcpcd` 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, `dhcpcd` 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, `dhcpcd` 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 services) 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 11.4\*](#). 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, in the Network screen, select the interface and then choose DHCP.

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

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

See the [sysconfig\(8\)](#) 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 11.4\*](#). 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, in the Network screen, select `No Network` or select the interface and then choose `static` to configure a static IP address.**

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

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

See the [sysconfig\(8\)](#) man page for more information about using a `sc_profile` configuration file.

## DHCP Client Administration

The `dhcpage` daemon does not require administration under normal system operation. The `dhcpage` daemon automatically starts when the system boots, renegotiates leases, and stops when the system shuts down. You should not manually start and stop the `dhcpage` daemon directly. Instead, as a privileged user on the DHCP client, you can use the `ipadm` command to affect the `dhcpage` 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\(8\)](#) 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.  
  
To specify a DHCP tunable parameter when a DHCP address is created, use the `ipadm create-addr -T dhcp -p param=value DHCP-addrobj` command. See the examples in “Option Negotiation” on page 30.
- **Request network configuration information only** – The `ipadm refresh-addr -i static-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. This option does not work with DHCP addresses.
- **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.
- **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.

---

## 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.

## MAC Address and Client ID

**DHCPv4** uses the MAC address and an optional client ID to identify the DHCP 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 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.

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:

```
ipadm set-prop -p client-id=DUID dhcpv6
```

Use the following command to set a particular interface to use a given DUID when creating that DHCP interface and to make the system appear to be multiple independent clients to a DHCPv6 server:

```
ipadm create-addr -T addrconf -p client-id=DUID net0/v6
```

For an interface that already exists, to change the DUID for that interface when it is next enabled after reboot, change the `client-id` property as follows:

```
ipadm set-addrprop -p client-id=DUID net0/v6
```

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 system.

## 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 different value for the client-id when creating that interface. For example:

```
ipadm create-addr -T dhcp -p client-id=DUID net0/v4
```

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 DHCP client to configure.

## Option Negotiation

DHCPv6 has an Option Request option that provides a hint to the DHCP server of what the DHCP client prefers to see. If all possible options were sent from the DHCP 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 DHCP 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 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` property in `ipadm`. For more details,

see the DHCP and Addrconf address properties as well as the DHCPv4 and DHCPv6 protocol properties in the [ipadm\(8\)](#) man page.

## param\_request\_list Property Configuration Syntax

You configure a DHCPv6 client in much like a DHCPv4 client.

To set the global IPv4 option request list:

```
# ipadm set-prop -p param-request-list=1,3,6,12,15,17,28,43 dhcpv4
```

To add to the global IPv4 option request list:

```
# ipadm set-prop -p param-request-list+=50 dhcpv4
```

To configure an individual interface to omit the hostname option:

```
# ipadm create-addr -T dhcp -p param-request-list=1,3,6,15,17,28,43 net0/v4
```

To create a global request list for DHCPv6:

```
# ipadm set-prop -p param-request-list=23,24 dhcpv6
```

To set an individual interface:

```
# ipadm create-addr -T addrconf -p param-request-list=21,22,23,24 net0/v6
```

## Setting DHCP Client Configurations

The following sections cover the configurations for DHCPv4 and DHCPv6. In addition, information about the default IPV4 configuration is included.

### 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 32.
- 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 Clients and Name Services”](#) on page 34 for information about using name services with DHCP clients.

## Default DHCPv4 Configuration

The DHCP client 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](#).

## DHCP Clients With Multiple Network Interfaces

The `dhcpcagent` 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 `dhcpcagent` 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 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 `dhcpcagent` 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 `dhcpcagent` 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 `dhcpage` daemon does not receive a host name through the DHCP service, the daemon 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 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 11.4\*](#). 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 Clients 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\(5\)`](#) 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 summary of each name service and DHCP includes cross-references to documentation that can help you set up clients for each name service:

<code>/etc/inet/hosts</code>	<p>You must set up the <code>/etc/inet/hosts</code> file for a DHCP client that is to use <code>/etc/inet/hosts</code> for its name service.</p> <p>The DHCP client's host name is added to its own <code>/etc/inet/hosts</code> file by the DHCP tools. However, you must manually add the host name to the <code>/etc/inet/hosts</code> files of other systems in the network. If the DHCP server uses <code>/etc/inet/hosts</code> for name resolution, you must also manually add the client's host name on the system.</p>
DNS	<p>If the DHCP client receives the DNS domain name through DHCP, then properties of the <code>dns/client</code> SMF service are also automatically configured. See <a href="#">Working With Oracle Solaris 11.4 Directory and Naming Services: DNS and NIS</a> for more information about DNS.</p>

# ◆◆◆ 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 35
- “[Files Used by the DHCP Service](#)” on page 36
- “[SMF Services Used by the DHCP Service](#)” on page 36

### DHCP Commands

`/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\(8\)](#) 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\(8\)](#) 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\(8\)](#) man page.

## Files Used by the DHCP Service

`/etc/inet/dhcd4.conf` and `/etc/inet/dhcd6.conf`

ISC DHCP only: Contain configuration information for the ISC DHCP server, `dhcpcd`. For more information, see the `dhcpcd.conf(7)` man page.

`/var/dhcp/interface.dhc` and `/var/dhcp/interface.dh6`

Contain 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 `dhcpcagent` daemon caches the current configuration information in `/var/dhcp/interface.dhc` when the interface's IP address lease is dropped. For example, if DHCP is used on the `qe0` interface, the `dhcpcagent` daemon caches the configuration information in `/var/dhcp/qe0.dhc`. The next time DHCP starts on the interface, the DHCP 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` and `/var/db/isc-dhcp/dhcp6.leases`

ISC DHCP only: List leases for DHCPv4 and DHCPv6 servers.

## SMF Services Used by the DHCP Service

`svc:/network/dhcp/client`

Contains the `config/debug` and `config/verbose` SMF properties to enable debug logging of the `dhcpcagent` daemon.

`svc:/network/dhcp/server:ipv4` and `svc:/network/dhcp/server:ipv6`

Contain information for the ISC DHCP service.

`svc:/network/dhcp/relay:ipv4` and `svc:/network/dhcp/relay:ipv6`

Contain 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

## C

- client configuration, 22
- client IDs
  - in DHCPv4 and DHCPv6, 29
- commands
  - list of, 35
- configuring
  - DHCP client, 21
  - ISC DHCP server, 18
  - name services for DHCP clients, 34

## D

- DHCP clients
  - administration, 27
  - configuration, 31
  - configuring name services for, 34
  - disabling, 26
  - dropping IP address, 28
  - enabling, 26
  - extending lease, 28
  - host name

- specifying, 33
- logical interfaces, 32
- multiple network interfaces, 32
- network information without lease, 28
- releasing IP address, 28
- shutting down, 25
- starting, 28
- startup, 22
- DHCP commands
  - granting user access to, 17
  - list of, 35
  - privileges, 17
- DHCP files
  - list of, 36
- DHCP protocol
  - advantages in Oracle Solaris implementation, 12
  - overview, 11
  - sequence of events, 13
- DHCP RFCs, 37
- DHCP server
  - configuring, 18
- DHCP SMF services
  - list of, 36
- DHCP tables
  - list of, 36
- dhcpageant daemon
  - description, 22, 35
- dhcpcd daemon
  - description, 35
- dhcpcd4.conf file
  - description, 36
- dhcpcd6.conf file
  - description, 36
- DHCPv4

- client IDs, 29
- default configuration, 32
- DHCPv6
  - administrative model, 22
  - client IDs, 29
  - disabling, 23
  - management of network interface, 24
  - starting automatically, 22
- dhcrelay command
  - description, 35
- disabling
  - DHCP clients, 26
  - DHCPv6, 23
- DUID (DHCP Unique Identifier)
  - definition, 29

## E

- enabling
  - DHCP clients, 26
- /etc/inet/dhcd4.conf file
  - description, 36
- /etc/inet/dhcd6.conf file
  - description, 36
- extending DHCP lease, 28

## H

- host name
  - enabling client request of, 33

## I

- IA (Identity Association)
  - definition, 30
- IAD (Identity Association Identifier)
  - definition, 29
- in.ndpd daemon, 22
- IP address management
  - DHCP and, 12
- ipadm command
  - controlling DHCP client with, 27
  - DHCP and, 35

- ISC DHCP server
  - configuring, 18
  - description, 16

## L

- large network support in DHCP, 12
- logical interfaces, 29
  - configuring to run DHCP, 30
  - DHCP clients, 32
  - zeroth, 30

## M

- MAC address
  - in DHCPv4 and DHCPv6, 29
- multiple network interfaces
  - DHCP clients, 32

## N

- name services
  - configuring for DHCP clients, 34
- negotiation
  - DHCP server, 30
  - /network/dhcp/client SMF service
    - used by DHCP, 36
  - /network/dhcp/relay SMF service
    - description, 37
  - /network/dhcp/server SMF service
    - description, 37
  - /network/dns/client SMF service
    - used by DHCP, 37
- network booting
  - DHCP and, 12
- network interfaces
  - managing on DHCPv6 client, 24
  - multiple, 32

## O

- omshell command



description, 36  
Option Request  
in option negotiation, 30

## P

param\_request\_list property  
in option negotiation, 30  
privileges  
to access DHCP commands, 17

## R

RFCs  
related to DHCP, 37  
Router Advertisement (RA), 23

## S

shutting down  
DHCP, 25  
SMF services  
used by DHCP, 36  
snoop command  
DHCP and, 36  
stopping  
DHCPv6, 23  
/system/name-service/switch SMF service  
used by DHCP, 37

## T

tables  
list of, 36

## U

user access to DHCP commands  
assigning, 17  
/usr/lib/inet/dhcpd daemon  
description, 35

/usr/lib/inet/dhcrelay command  
description, 35  
/usr/sbin/dhcpagent daemon  
description, 35  
/usr/sbin/ipadm command  
DHCP and, 35  
/usr/sbin/omshell command  
description, 36  
/usr/sbin/snoop command  
DHCP and, 36

## V

/var/dhcp/interface and .dh\* file  
description, 36

