VitalQIP® DNS/DHCP & IP Management Software

DHCP Configuration Manager | Release 1.0

User's Guide

190-409-122R1.0
Issue 2
July 2009

Licenses

Refer to Appendix C, “Third party software license statements” in the *VitalQIP Release 7.2 Installation Guide* (190-409-043R7.2) for a complete description of all software licenses used to develop this product.

Contents

About this document

Purpose

DHCP Configuration Manager is a web-based GUI that allows quick configuration of a Lucent DHCP server on a VitalQIP appliance. The Web GUI is local to the DHCP server and only used to provision a single server.

Reason for revision

The following table shows the revision history of this document.

Issue	Revision	Location
2	Support for Lucent DHCP 5.6 server policies was added.	Table 2-2, “Server-level policies” (p. 2-15)
2	Failover support for DHCP servers was added.	Table 2-2, “Server-level policies” (p. 2-15)
2	Product name change to DHCP Configuration Manager	Throughout manual.

Intended audience

This manual is intended for DHCP Configuration Manager users who plan to manage and administer a DHCP server in an environment where the VitalQIP product is not fully deployed. The reader is expected to understand basic networking concepts and have a working knowledge of the operating system that DHCP Configuration Manager is running on. Two types of groups interact with DHCP Configuration Manager:

- **DHCP Configuration Manager administrators -** The Information Technology (IT) professionals who install, configure, and administer the DHCP Configuration Manager product.
- **DHCP Configuration Manager users -** The IT professionals who use DHCP Configuration Manager as a service-level monitoring and capacity tool.

How to use this document

This manual is organized as follows:

Chapter 1, "VitalQIP DHCP Configuration Manager overview"

This chapter provides an overview of DHCP Configuration Manager, information on how to access and quit the application, a brief summary of how it works, and ends with a description of the user interface.

Chapter 2, "Server operations"

This chapter describes how to manage the DHCP server status and properties.

Chapter 3, "Subnet operations"

This chapter describes how to manage subnets.

Chapter 4, "Scope operations"

This chapter describes how to manage scopes.

Chapter 5, "DHCP server configuration files"

This chapter describes how to manage configuration and policy files on a DHCP server.

Chapter A, "Configuring DHCP Configuration Manager"

This appendix describes how to customize the behavior of DHCP Configuration Manager and the web server.

Conventions used

The following table lists the typographical conventions used throughout this manual.

Convention	Meaning	Example
Trebuchet bold	Names of items on screens.	Select the **Client** check box.
	Names of buttons you should click on the screen, or names of keys on the keyboard to be pressed.	Click **OK**.
Courier	Output from commands, code listings, and log files	`# Name: Share shared-network _200_200_200_0`
Courier bold	Input that you should enter from your keyboard.	Run the following command: **`c:\setup.exe`**
	Names of commands and routines	The **`qip_getapp1lst`** routine returns the entire list of existing applications.

Convention	Meaning	Example
Courier bold italic	Input variable for which you must substitute another value. The angle brackets also indicate the value is a variable.	**`isql -U sa -P <sa_password>`**
Times bold	Uniform Resource Locators (URLs)	The VitalQIP product site can be found at **http://www.alcatel-lucent.com/wps/portal/products/**.
Times italics	Manual and book titles.	Refer to the *VitalQIP User's Guide*.
	Directories, paths, file names, and e-mail addresses.	A symbolic link must be created from */etc/ named.conf* that points to *named.conf*.
Times bold italic	Emphasis	***Read-only***. The name of the service element.

Related information

The following documents are referenced in this manual:

- *VitalQIP Appliance Packages Configuration Guide* (part number: 190-409-116)

  This guide describes the package configurations for appliances maintained in AMS.
- *VitalQIP Appliance Management Software User's Guide* (part number: 190-409-089)

  This guide describes how to set up appliances and administer them with AMS.

Product Training Support

Alcatel-Lucent University offers cost-effective educational programs that support the VitalQIP product. Our offerings also include courses on the underlying technology for the VitalQIP products (for example, DNS and DHCP). Our classes blend presentation, discussion, and hands-on exercises to reinforce learning. Students acquire in-depth knowledge and gain expertise by practicing with our products in a controlled, instructor-facilitated setting. If you have any questions, please contact us at 1 888 LUCENT8, option 2, option 2.

Technical support

If you need assistance with DHCP Configuration Manager, you can contact the Welcome Center for your region. Contact information is provided in the following table.

Region	Address	Contact information
North, Central, and South America	Alcatel-Lucent 400 Lapp Road Malvern, PA 19355 USA	Phone: 1-866-LUCENT8 (582-3688) Option 1, Option 2 Web: **https://support.lucent.com**
Europe, Middle East, and Africa,	Alcatel-Lucent Voyager Place Shoppenhangers Road Maidenhead Berkshire SL6 2PJ UK	Phone: 00 800 00 LUCENT or +353 1 692 4579 E-mail: *emeacallcenter@alcatel-lucent.com* Web: **https://support.lucent.com**
Central and South America	Alcatel-Lucent Calle 10, No. 145 San Pedro de los Pinos, 01180 Ciudad de Mexico Mexico	Mexico 01 800 123 8705 or (52) 55 5278 7005 Brazil 0800 89 19325 or (55) 193707 7900 Argentina 0800 666 1687 Venezuela 0 800 1004136 Costa Rica 0800-012-2222 or 1800 58 58877 For other local CALA numbers, consult the web site **https://support.lucent.com** or contact your local sales representative.
Asia Pacific	Alcatel-Lucent Australia 280 Botany Road Alexandria NSW 2015 Australia	Phone: 1800-458-236 (toll free from within Australia) (IDD) 800-5823-6888 (toll free from Asia Pacific - China, Hong Kong, Indonesia, South Korea, Malaysia, New Zealand, Philippines, Singapore, Taiwan, and Thailand) (613) 9614-8530 (toll call from any country) E-mail: *apactss@alcatel-lucent.com*

How to order

To order Alcatel-Lucent documents, contact your local sales representative or use the Online Customer Support Site (OLCS) web site (http://support.lucent.com).

How to comment

To comment on this document, go to the Online Comment Form or e-mail your comments to the Comments Hotline (**comments@alcatel-lucent.com**).

1 VitalQIP DHCP Configuration Manager overview

Overview

Purpose

This chapter provides an overview of DHCP Configuration Manager, information on how to access and quit the application, a brief summary of how it works, and ends with a description of the user interface.

Contents

This chapter covers these topics.

Getting started with DHCP Configuration Manager

The VitalQIP DHCP Management solution

Overview

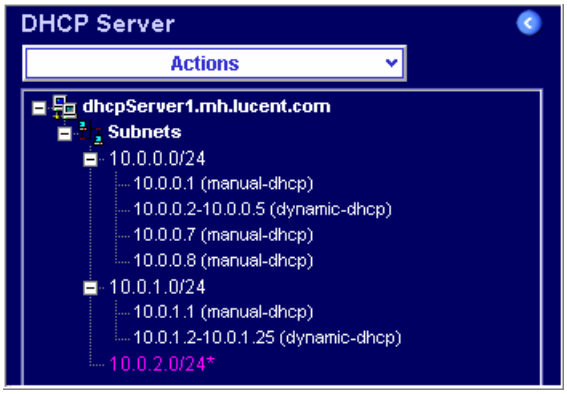
The DHCP Configuration Manager is a web-based UI that allows quick configuration of a Lucent DHCP server on an appliance. The Web UI is local to the DHCP server machine and only used to provision a single server. This feature is not intended to replace VitalQIP but rather to be used in deployments where VitalQIP may not be immediately required. It supports the following functionality.

- Managing subnets and subnet policies in DHCP configuration file (*dhcpd.conf*)
- Managing subnet scopes, scope policies and scope options (*dhcpd.conf*)
- Managing server and subnet level MAC Address pools in DHCP configuration file (*dhcpd.conf*)
- Managing DHCP server policies in DHCP server policy file (*dhcpd.pcy*)
- Start/stop/reload/restart DHCP server
- View/Edit configuration files (*dhcpd.conf*, *dhcpd.pcy*)
- User authentication

The DHCP Configuration Manager is delivered as part of the package delivery mechanism on the VitalQIP Appliance.

DHCP Server configuration hierarchy

The Tree/Hierarchy frame displays the DHCP Server configuration hierarchy with subnets and subnet scopes. Since this is the only tree supported by the DHCP Configuration Manager UI, once it is loaded it remains in the DHCP Server hierarchy frame until a user logs out.



Save Changes function

Unlike the AMS UI, the DHCP Configuration Manager UI does not commit changes to the server as soon as they are submitted. Committing changes modifies the server configuration files and would therefore require the DHCP server to be reloaded. To minimize DHCP server reloads, user changes are maintained in a user's login session until explicitly committed using the **Save Changes** function (in the toolbar) on the **Server Actions** menu. A **Discard Changes** function on the same menu (in the toolbar) allows you to discard any changes you have made.

Uncommitted changes

To identify non-committed changes in the DHCP Server hierarchy, the label of the changed node is shown in a different color and has an asterisk character (*) at the end of the node label, as shown in the above illustration.

Web server

DHCP Configuration Manager uses a web server that runs as the **`qdhcp-httpd`** service. This service can be controlled from the AMS GUI.

To stop/start/kill/restart the service, you need to select the desired appliance in the AMS hierarchy, and select the **Services** tab when the Appliance Properties page is displayed.

Log files

Logs are located in the */opt/qdhcpmgr/log* directory. The following logs are kept:

- *qdhcp_httpd.log* contains logs written by DHCP Configuration Manager Web Server. It logs html pages requested by the client.
- *qdhcp_manager.log* contains the DHCP Configuration Manager application log. The log level of this file is controlled via the **`loglevel`** property in the */opt/qdhcpmgr/conf/qdhcpmgr.properties* file. For more information on this property, refer to "loglevel" (p. A-3).

Log in to DHCP Configuration Manager

Purpose

To log into the DHCP Configuration Manager UI. The DHCP Configuration Manager UI is web-based and launched by entering a URL for DHCP Configuration Manager into the web browser, which opens directly to the DHCP Configuration Manager Login page.

> **Note:** DHCP Configuration Manager can also be run as an SSL application. Refer to "Deploy DHCP Configuration Manager in SSL mode" (p. 1-7).

Before you begin

Ensure the following are true before you begin.

- Be sure that pop-ups are enabled for the DHCP Configuration Manager URL, because the application uses this function to provide messages to the user
- JavaScript is enabled
- Cookies are enabled
- Style sheets enabled
- User accepts certificate when presented by browser.

Procedure

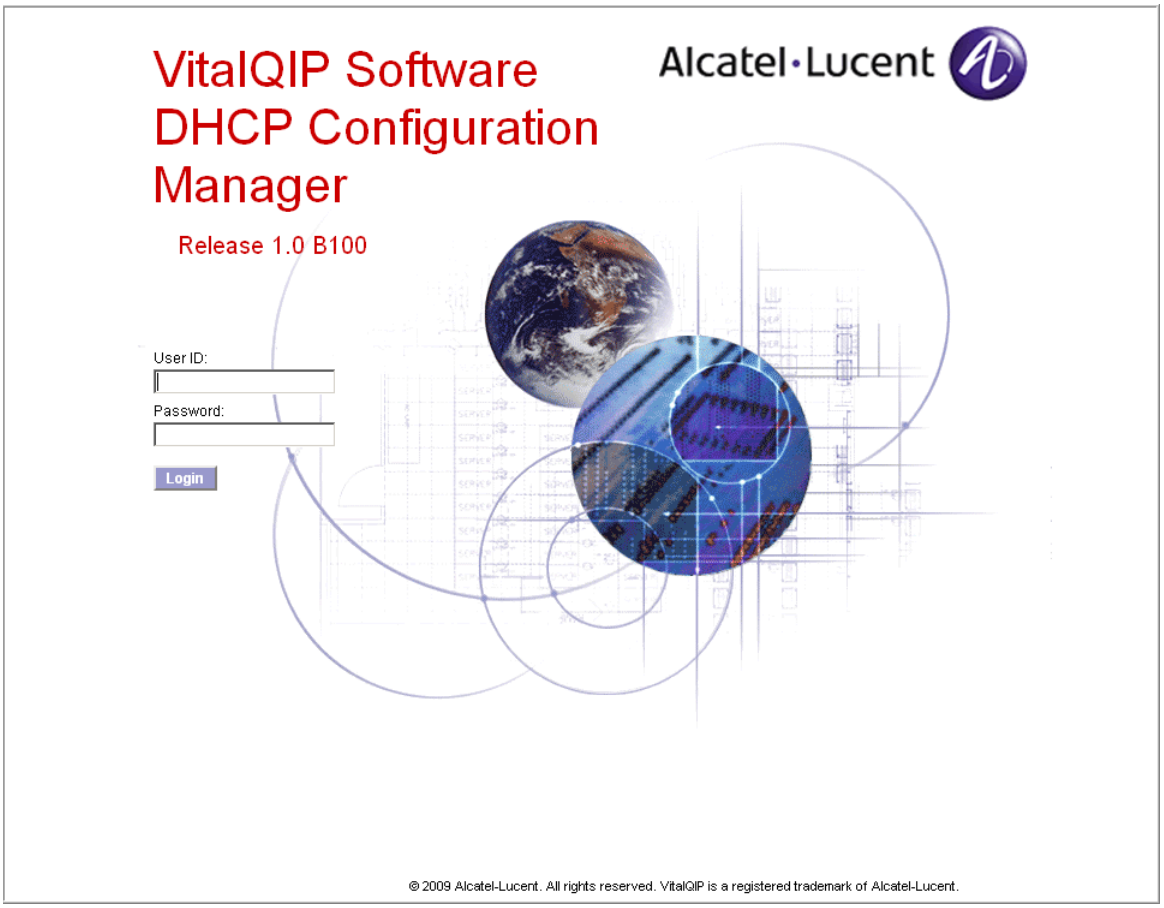
To log into DHCP Configuration Manager, follow these steps:

1. Open a web browser.

2. In the web browser, enter the DHCP Configuration Manager URL in the following format:

   `http://<IP address>:8067/`

Result: The VitalQIP DHCP Configuration Manager Login page opens.



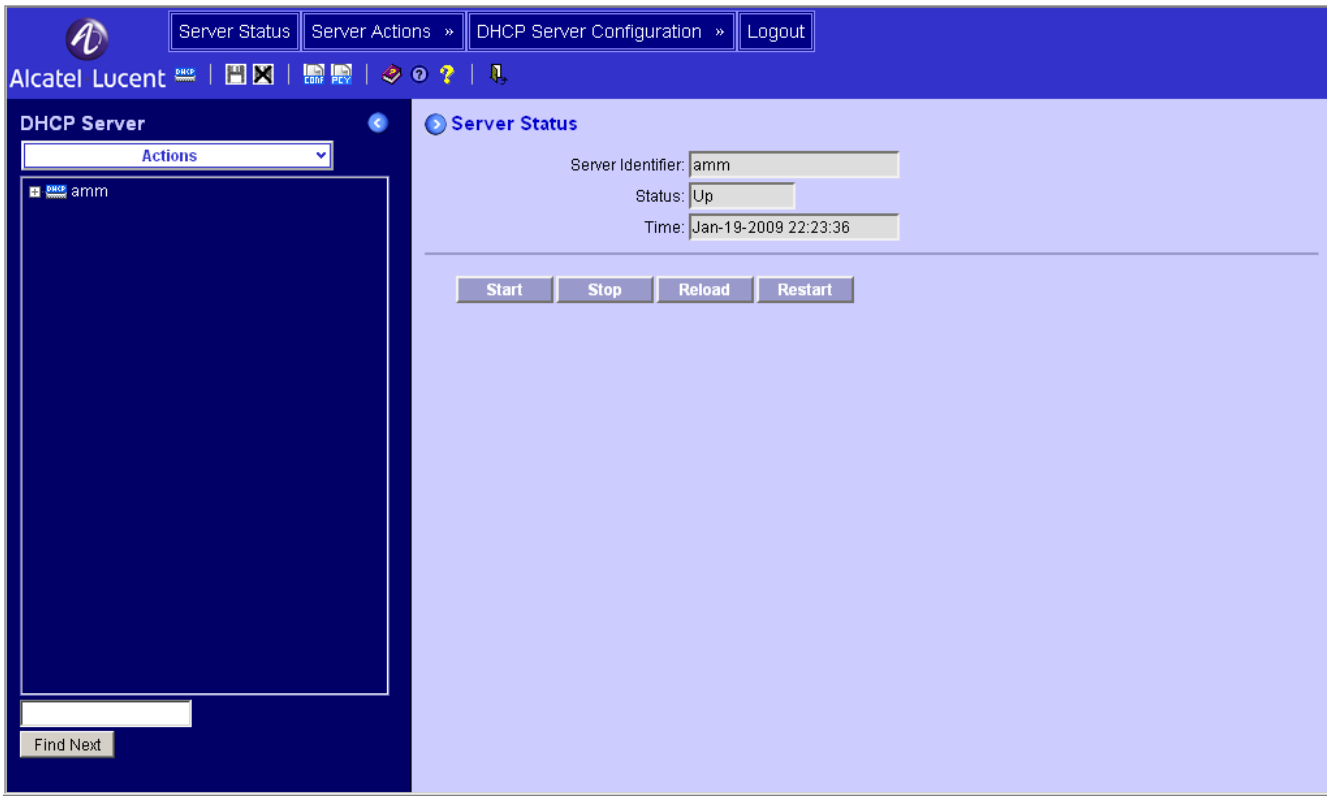
3 Enter your user ID in the **User ID** field and password in the **Password** field.

- To access the full functionality of DHCP Configuration Manager, use the default administrator user ID, which is **`qdmadmin`**. The default password is **`qdmadmin`**.
- To access read-only operations of DHCP Configuration Manager, use the default monitor user ID, which is **`qdmuser`**. The default password is **`qdmuser`**.

Additional user IDs in DHCP Configuration Manager are added with the **`qdmuser`** CLI. For information on adding additional user IDs, refer to "Manage DHCP Configuration Manager users" (p. 1-12).

4 Click **Login**.

Result: The VitalQIP DHCP Configuration Manager main page opens.



For further information on the DHCP Configuration Manager UI, refer to "User interface" (p. 1-16).

END OF STEPS

Deploy DHCP Configuration Manager in SSL mode

Purpose

To deploy DHCP Configuration Manager in SSL mode.

Before you begin

- Create or obtain a trusted certificate file and save it on the AMS machine.
- Changes to the *qdhcp_httpd.conf* and *qdhcpmgr.cer* files must be made in AMS to ensure that they can be reused whenever the DHCP Configuration Manager package is upgraded.

Procedure

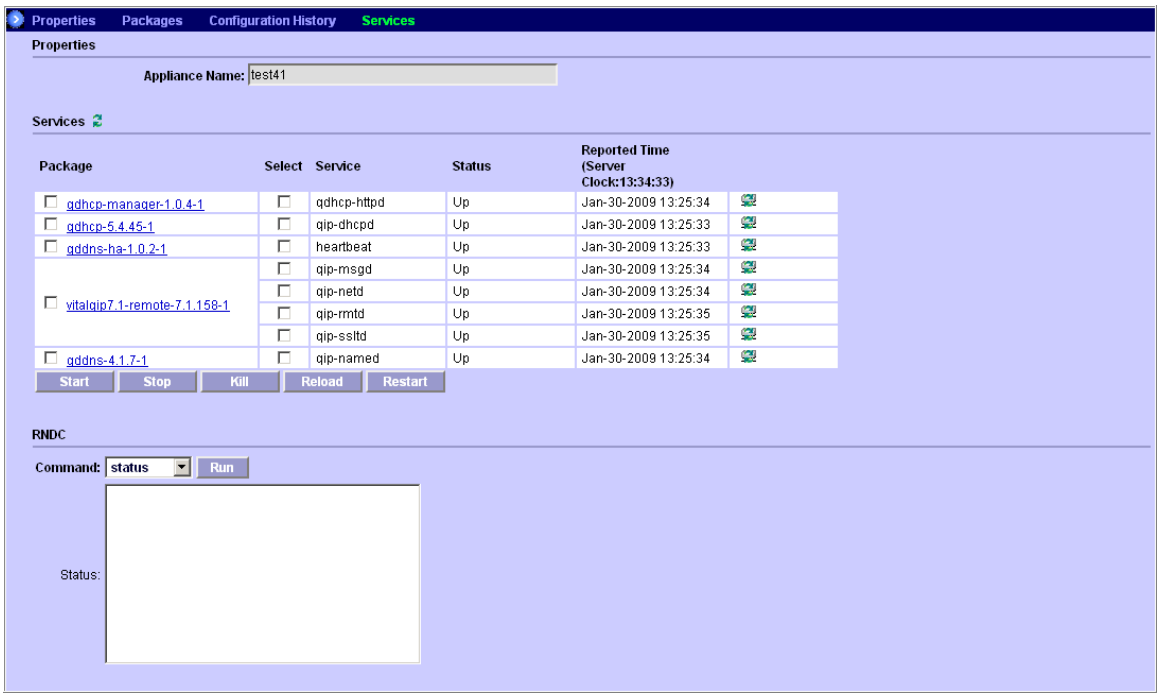
To deploy DHCP Configuration Manager in SSL mode, follow these steps.

1 Log into AMS and locate the appliance where DHCP Configuration Manager is installed.

Result: The Properties page opens.

2 Select the **Services** tab.

Result: The Services page opens.



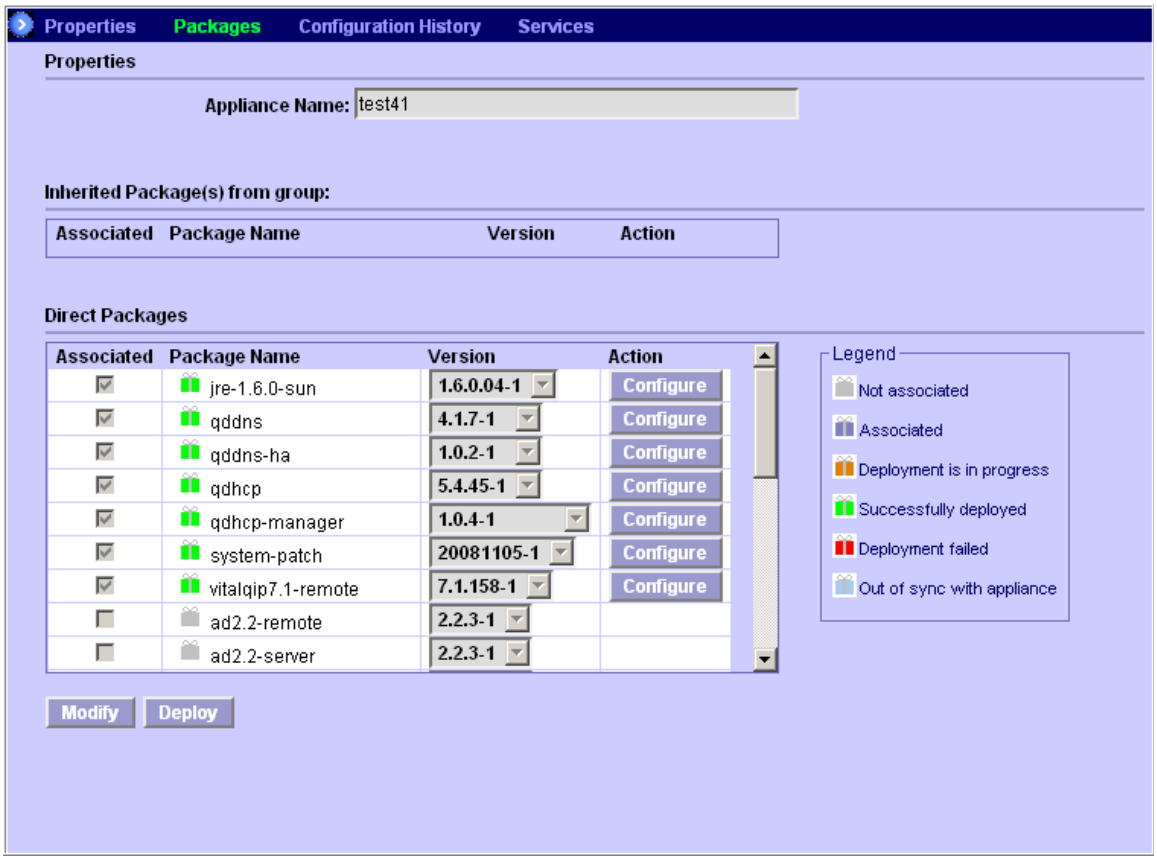
3 Place a check beside the **qdhcp-manager** package.

4 Click **Stop**.

Result: The **qdhcp-httpd** service status changes to **Down**.

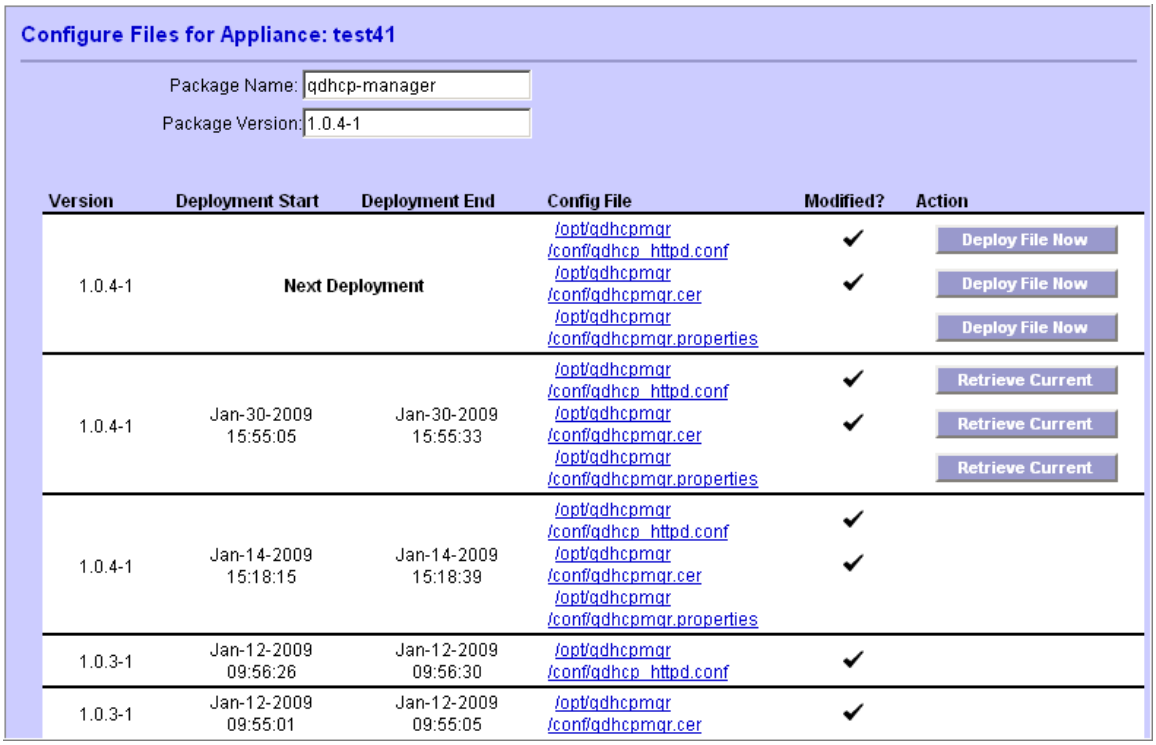
5 In the Appliance Properties page, select the **Packages** tab.

Result: The Packages Properties page opens.



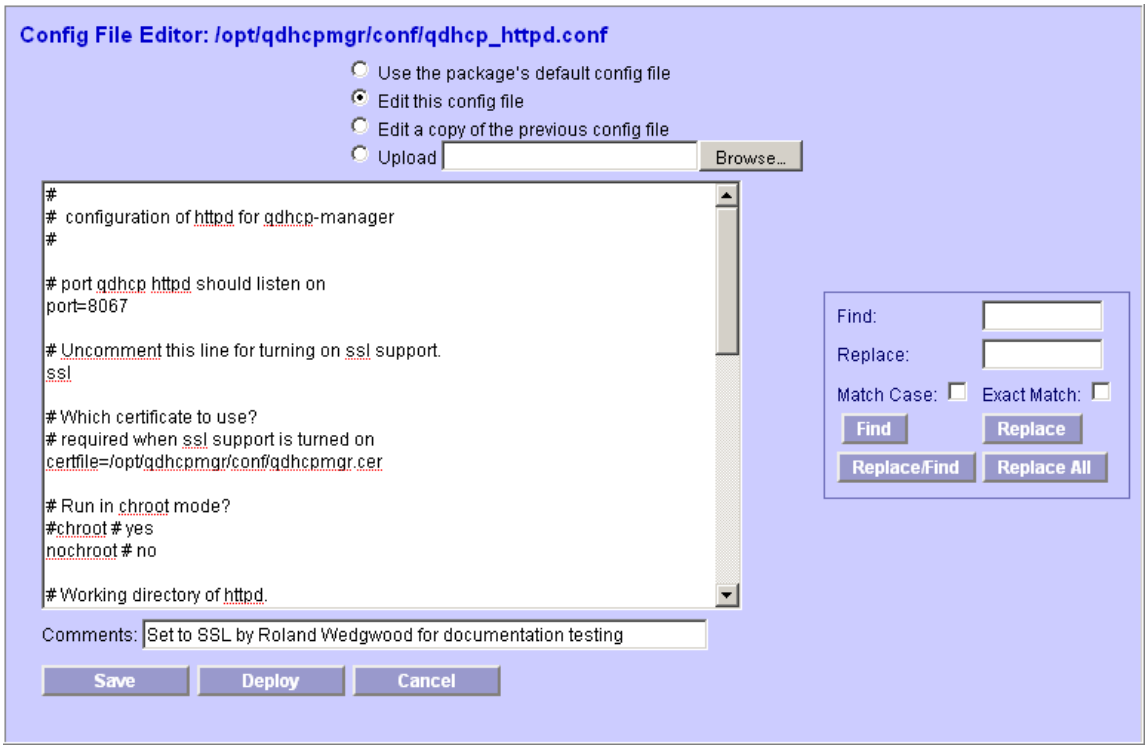
6 Click **Configure** beside the **qdhcp-manager** package.

Result: The Configure Files page for the appliance opens.



7 Click on the link to **/opt/qdhcpmgr/conf/qdhcp_httpd.conf**.

Result: The Config File Editor page opens.



8 Uncomment the **ssl** entry.

9 Uncomment the **certfile** entry and ensure it is set to **/opt/qdhcpmgr/conf/qdhcpmgr.cer**.

10 Click **Save**.

Result: A dialog box opens with the message **Config file changes saved.**

11 Click **OK**.

Result: The Configure Files page for the appliance opens.

12 Click on the link to **/opt/qdhcpmgr/conf/qdhcpmgr.cer**.

Result: The Config File Editor page opens.

13 Select the **Upload** option and click **Browse**.

14 Locate the trusted certificate file you obtained earlier and click **Save**.

15 In the Config Files for appliance page, click **Deploy File Now** beside the link to **/opt/qdhcpmgr/conf/qdhcp_httpd.conf**.

Result: A confirmation dialog box opens with the message **Are you sure you want to deploy this config file to the appliance immediately?**

16 Click **OK**.

Result: After the file has been deployed, an information dialog box opens with the message **Config file deployed**.

17 Click **OK**.

18 Repeat Step 15 to Step 17 on **/opt/qdhcpmgr/conf/qdhcpmgr.cer**.

19 Close the Config Files for appliance page and select the **Services** tab.

Result: The Services Properties page opens.

20 Place a check in the **Select** option beside the **qdhcp-httpd** service and click **Start**.

Result: The **qdhcp-httpd** service status changes to **Up**.

21 DHCP Configuration Manager should now be accessible using “https”.

https://<*appliance ip*>:8067/

END OF STEPS

Manage DHCP Configuration Manager users

Purpose

To add, modify, or delete a DHCP Configuration Manager user.

Before you begin

You must be logged in as "root" user on the VitalQIP appliance to run the **qdmuser** CLI.

qdmuser

The **qdmuser** CLI allows you to add, modify or delete a DHCP Configuration Manager user. It updates user information in the */opt/qdhcpmgr/conf/passwd* file. These users are independent of user accounts on the VitalQIP appliance or the Appliance Management Software (AMS).

Synopsis

qdmuser -a|-m|-d -u *user* [**-p *password***] [**-t read|write**] [**-o *oldpassword***]

Parameters

-a Add user

-m Modify user password or type

-d Delete user

-u User ID

-p Password

-t User privileges (allowed values are "read" or "write")

-o old password (applicable with –m option only)

Usage

To use the **qdmuser** CLI, follow these steps.

1. Log in as root on the appliance where the DHCP Configuration Manager application has been installed.

2. Change directory to */opt/qdhcpmgr/bin*.

3 Run the **qdmuser** CLI, using one of following options.

Add user: **./qdmuser -a -u *user* -p *password* -t write**

Modify user: **./qdmuser -m -u *user* -o *oldpassword* -p *newpassword* -t read**

Delete user: **./qdmuser -d -u user**

Where ***user*** = desired user ID

password = desired password

read = assign read-only privilege to the user

write = assign read and write privilege to the DHCP Configuration Manager User

END OF STEPS

Exit DHCP Configuration Manager

Purpose

Use this procedure to log out of DHCP Configuration Manager.

Before you begin

DHCP Configuration Manager is set up to log out automatically after one hour of inactivity. If you wish to modify that value, refer to "session_inactivity_timeout" (p. A-3).

Procedure

To exit DHCP Configuration Manager, follow these steps.

1. Select the **Logout** menu, or click the Logout icon () in the DHCP Configuration Manager toolbar.

2 Choose one of the following.

If ...	Then ...
If there are unsaved changes to the DHCP server configuration or policy files	1. A confirmation dialog box opens with the message **There are unsaved changes. If you press OK, these changes will be lost. Do you want to continue?** 2. To save those changes, click **Cancel**. 3. Select **Save Changes** from the **Server Actions** menu, or click the Save Changes icon ( ). **Result:** An information dialog box opens with the message **File saved.** 4. Click **OK**. 5. Select the **Logout** menu or click the Logout icon again. 6. A confirmation dialog box opens with the message **Are you sure you want to exit?** 7. Click **OK** to exit. **Result:** The DHCP Configuration Manager login screen opens.
If there are no changes in the current session	1. A confirmation dialog box opens with the message **Are you sure you want to exit?** 2. Click **OK** to exit. **Result:** The DHCP Configuration Manager login screen opens.

END OF STEPS

User interface

Overview

Purpose

This section provides a detailed description of the DHCP Configuration Manager user interface. It describes the different icons used, as well as how the hierarchy page works.

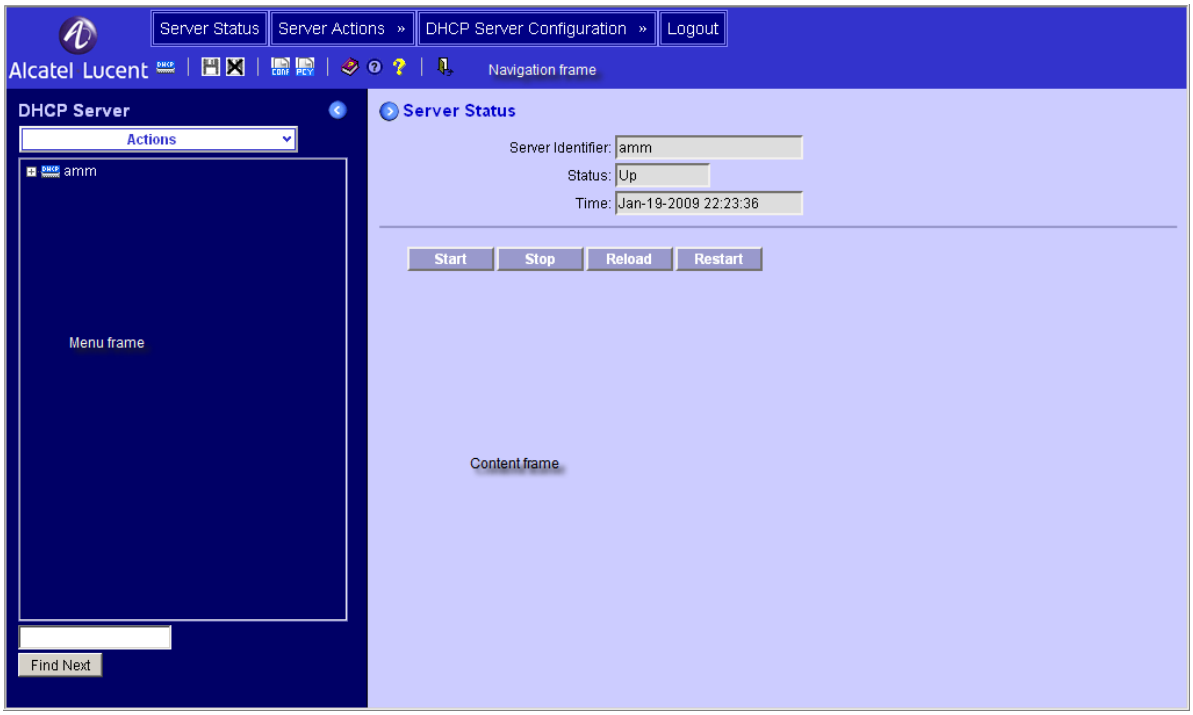
User interface components

This section describes the DHCP Configuration Manager interface components, as well as the buttons and icons that appear in the content frame.

DHCP Configuration Manager page frames

The DHCP Configuration Manager pages are comprised of a navigation frame at the top, a menu frame on the left, and a content frame on the right.

Figure 1-1 DHCP Configuration Manager page frames



Main menu

The main menu is shown at the top of the navigation frame and provides access to all the application's features. The selected menu item is shown in a very deep shade of blue. When you mouse over other menus, they are shown as very dark blue as well.

Sub-menus

Sub-menus appear beneath each expandable main menu item when it is selected. They represent the sub-sections of functionality for that main menu item. The selected sub-menu is shown in a lighter shade of blue. When you mouse over other sub-menus, they are shown as a very dark shade of blue.

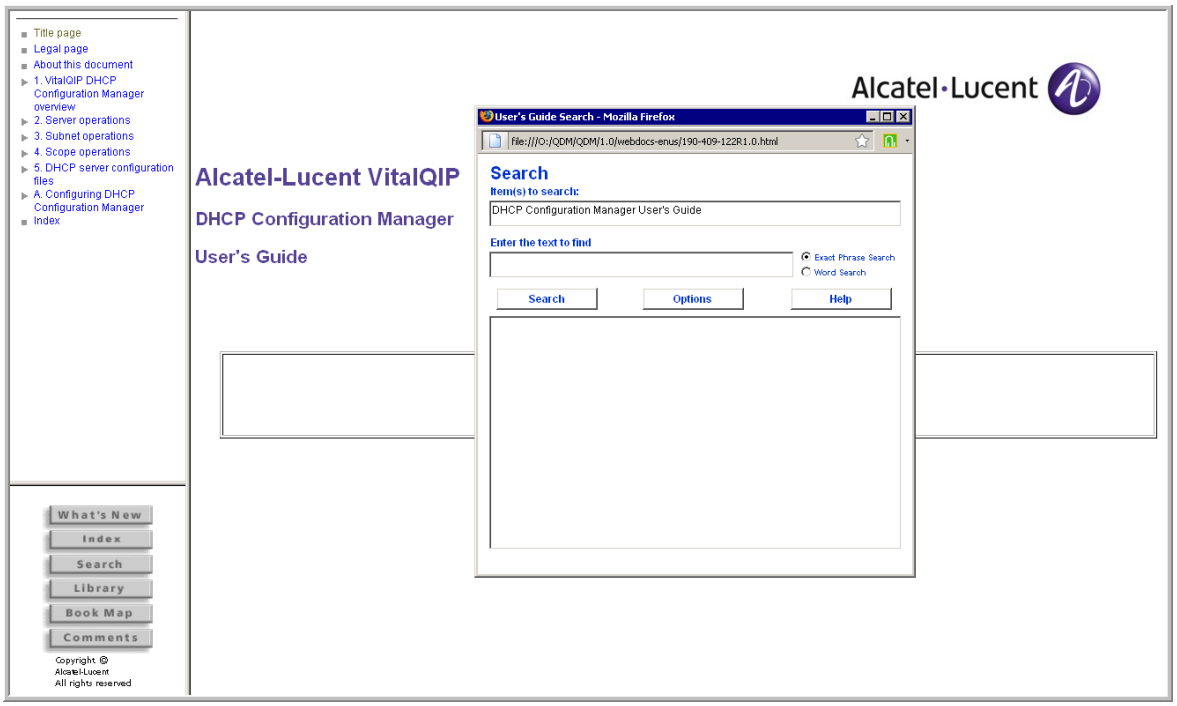
Toolbar

The toolbar appears underneath the main menu bar and contains icons that duplicate the commands on the main menu and sub-menus, so you can invoke the same functions with a single mouse click. When icons that represent commands on the Help menu are invoked, separate browser windows open.

Online Documentation

The Online Documentation icon launches the VitalQIP Products Library. The library contains both HTML and PDF versions of the DHCP Configuration Manager documentation. The Library also contains a useful Search function that allows you to locate matches for exact phrase or word instances across all or a user-specified set of HTML documents in the library.

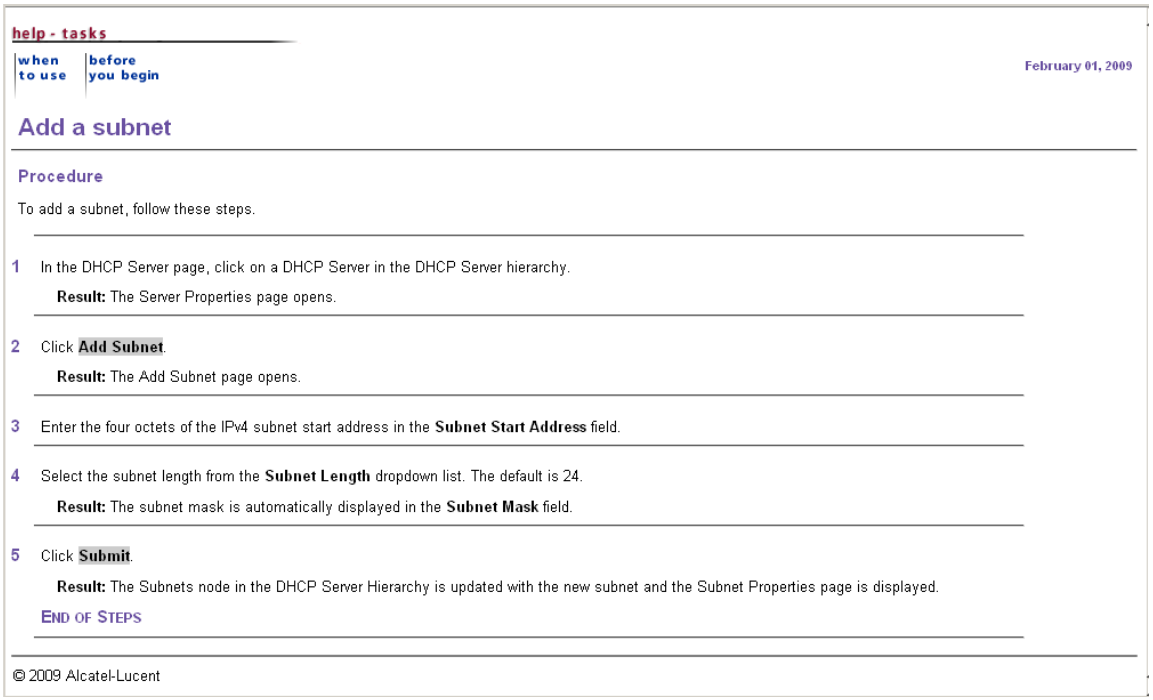
Figure 1-2 Online Documentation screen



Online Help

The Online Help icon launches a list of help screens that are available. A typical help screen is shown below.

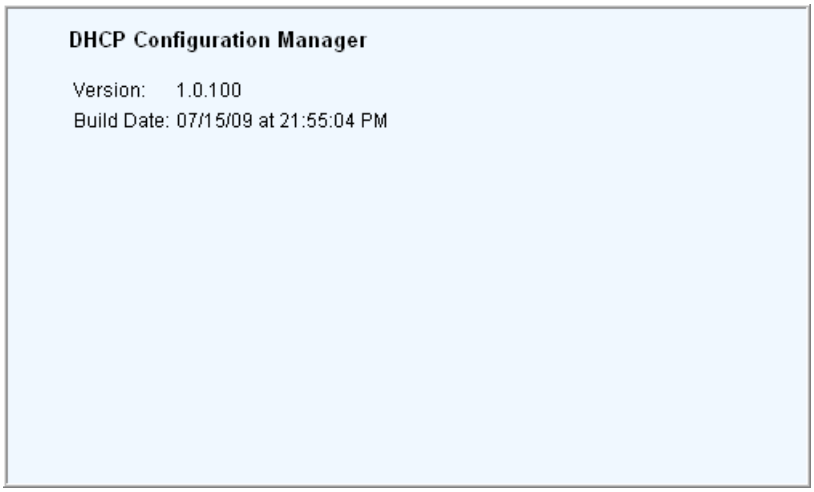
Figure 1-3 Online Help screen



About DHCP Configuration Manager

The About icon launches the DHCP Configuration Manager screen, where you can determine which version of the product you have installed. This information may be useful whenever you need to contact Technical Support.

Figure 1-4 About screen



Content frame icons

The following table describes buttons and icons that commonly occur in the DHCP Configuration Manager content frames.

Table 1-1 Content frame icons

Icon name	Description
Expand / contract buttons	 Select expand/contract buttons to maximize or collapse a frame within the DHCP Configuration Manager UI. To restore the prior configuration, select the icon again. **Note:** You can also drag the edge of a frame to resize it.
Show fields	 Click to show hidden fields in the Content frame.
Hide fields	 Click to hide fields displayed in the Content frame.

Miscellaneous features

Utility dialog boxes

Dialog boxes may be for user input as well as for displaying confirmation and error messages. User input is case-sensitive in dialog boxes.

There are three types of message dialog boxes. These are shown in the illustrations below:

Figure 1-5 Information dialog box

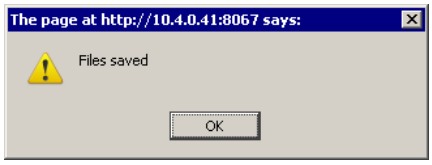


Figure 1-6 Confirmation dialog box

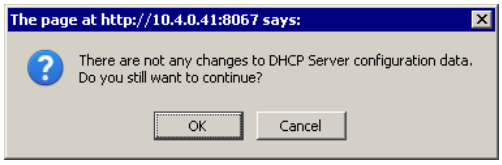
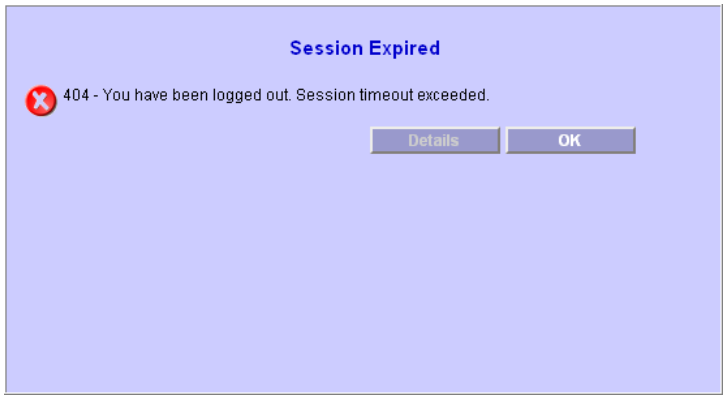


Figure 1-7 Error dialog box



Required fields

Required fields are boldfaced in the DHCP Configuration Manager UI.

Expand/Contract icon description

Expand and Contract icons appear to the left of a hierarchy or tree item. Click on the icons to toggle between displaying and hiding information.

Expand icon 	Displays information associated with a specific value on the page.
Contract icon 	Hides items that have been previously displayed with the Expand icon.

Actions menu

The following functions are available from the **Actions** menu:

	The **Refresh Hierarchy** function retrieves the current data from the DHCP configuration files on the disk if the files have changed and displays it in the hierarchy. If the files have not changed, an information dialog box opens with the message **The dhcp configuration file on disk have not changed since they were last read. Refresh not needed.**
	The **Collapse All** function changes the hierarchy display so only the top-level items are visible in the hierarchy.

Find hierarchy nodes

The **Find Next** function allows you to search for a node in the DHCP Server hierarchy. To locate a specific subnet or scope in the DHCP Server hierarchy, follow these steps.

1. To find a subnet, expand the **Subnets** node. To find a scope, expand the subnet that contains the scope.
2. Enter the IP address you are looking for and click **Find Next**.

   Result: If there is a match, the subnet or scope is highlighted and the Properties page opens.

2 Server operations

Overview

Purpose

This chapter describes how to manage the DHCP server status and properties.

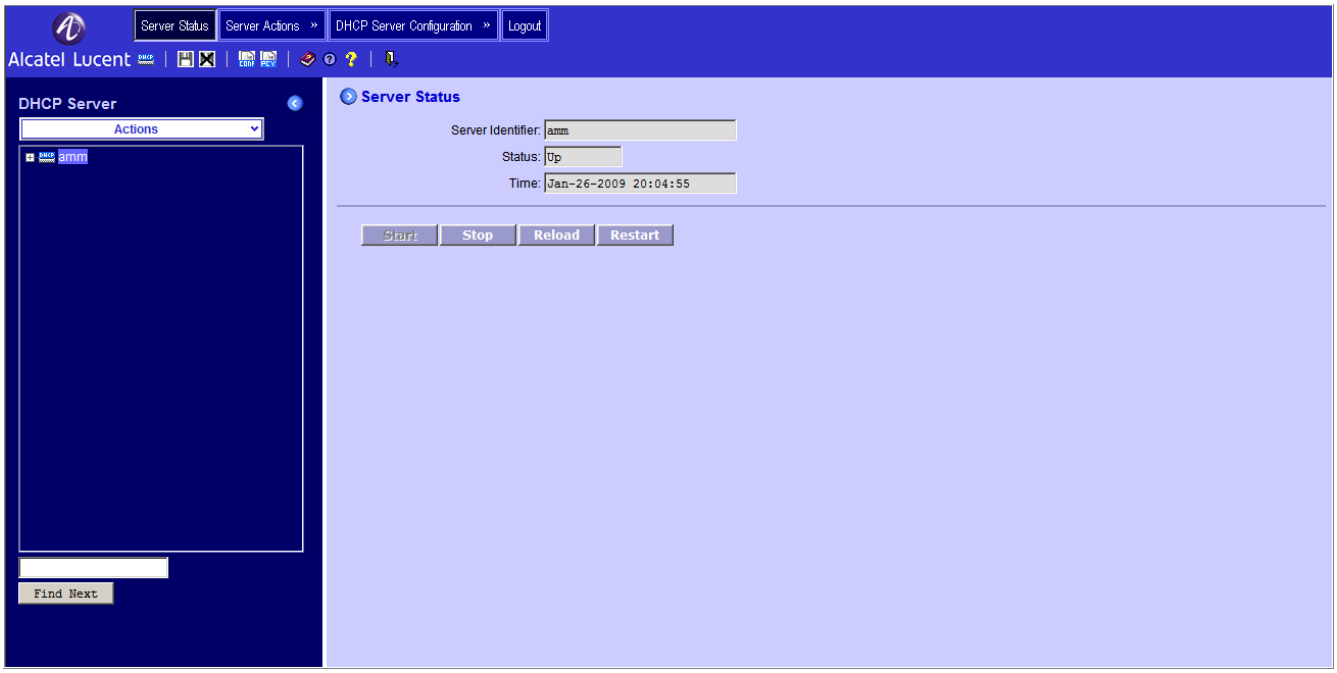
Contents

This chapter covers these topics.

Manage DHCP server

Overview

After a successful login, the DHCP Server hierarchy is populated with the Server node and the Server Status page is displayed.



The following DHCP server functions are available.

- Stop/start/restart/reload server
- View/modify server properties
- Add subnet
- View/modify server policies
- View/modify MAC address pool

Any changes made are not saved in the DHCP configuration file until explicitly saved or discarded. The **Server Actions** menu contains the **Save Changes** and **Discard Changes** sub-menus.

Manage server status

Purpose

To manage the status of a DHCP server.

Before you begin

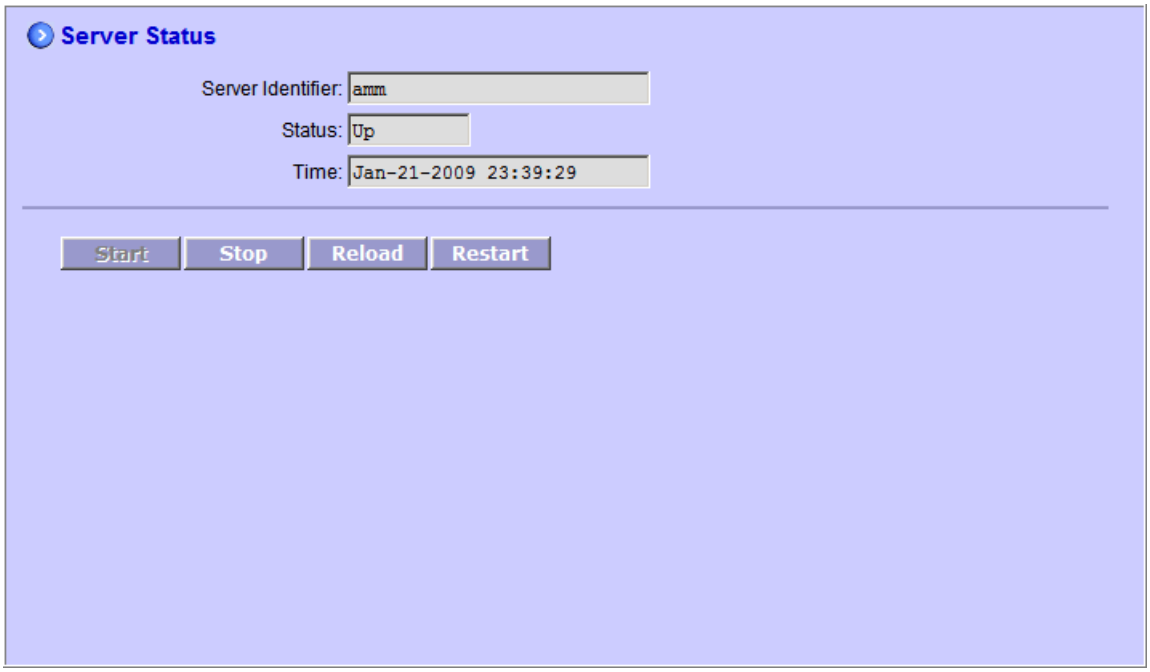
None of the server status functions are available to read-only users.

Procedure

To manage the status of a DHCP server, follow these steps.

1 Click the Server Status menu or the Server Status icon ( ).

Result: The Server Status page opens.



The following table describes the available fields.

Table 2-1 Server Status fields

Field	Description
Server Identifier	Server name or IP address of the DHCP server. The default value is the `server-identifier` field from *dhcpd.conf*. If the file is empty, the hostname of the server is used. For information on changing a server identifier, refer to "Manage server properties" (p. 2-6).
Status	Indicates the status of the server. Values are **Up** and **Down** (**Stopping** and **Starting** are also temporarily displayed after actions are invoked).
Time	Indicates the time that the status was retrieved.

2 Choose one of the following actions..

If you want to…	Then …
Stop the server	1. Click **Stop**. **Result:** The **Status** field changes to **Stopping** and an information dialog box opens. 2. Click **OK**. **Result:** The **Status** field changes to **Down** and the **Time** field is updated.
Reload the server configuration files	1. Click **Reload**. **Result:** The **Status** field changes to **Starting** and an information dialog box opens. 2. Click **OK**. **Result:** The **Status** field changes to **Up** and the **Time** field is updated.
Restart the server while it is still running	1. Click **Restart**. **Result:** The **Status** field changes to **Starting** and an information dialog box opens. 2. Click **OK**. **Result:** The **Status** field changes to **Up** and the **Time** field is updated.
Start the server after a shutdown	1. Click **Start**. **Result:** The **Status** field changes to **Starting** and an information dialog box opens. 2. Click **OK**. **Result:** The **Status** field changes to **Up** and the **Time** field is updated.

END OF STEPS

Manage server properties

Purpose

To manage the properties of a DHCP server.

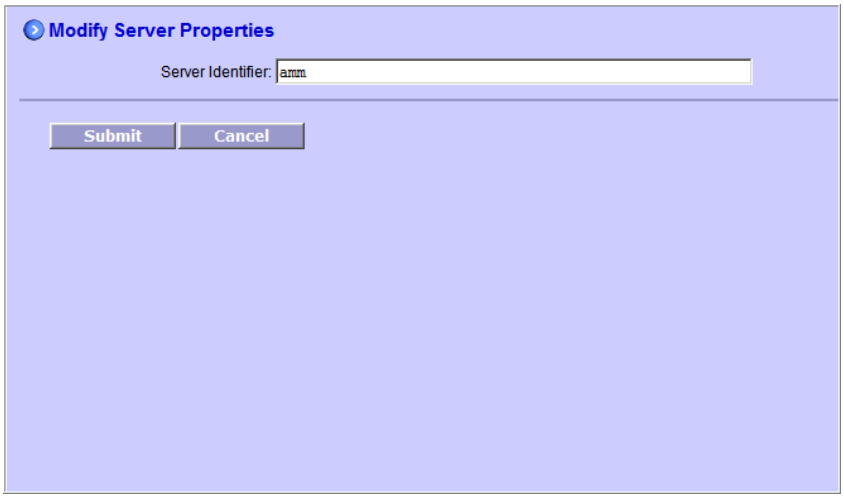
Procedure

To manage the properties of a DHCP server, follow these steps.

1 Click on the DHCP Server in the hierarchy.

Result: The Server Properties page opens.

2 Choose one of the following actions.

If you want to…	Then …
Modify a server identifier	1. Click **Modify**. **Result:** The Modify Server Properties page opens.  2. Enter a different server identifier. It can be a server name or IP address. 3. Click **Submit** to save your changes. **Result:** The Server identifier in the DHCP Server hierarchy is updated. **Note:** This function is not available to read-only users.
Add a subnet	Click **Add Subnet**. For further information, refer to "Add a subnet" (p. 3-3). **Note:** This function is not available to read-only users.
View or modify server MAC address pool	Click **MAC Pools**. For further information, refer to "View/modify a server MAC address pool" (p. 2-8). **Note:** Read-only users can only view server MAC addresses.
View or modify server policies	Click **Server Policies**. For further information on, refer to "View/modify server policies" (p. 2-12). **Note:** Read-only users can only view server policies.

END OF STEPS

View/modify a server MAC address pool

Purpose

To view or modify a MAC address pool at the server level.

Before you begin

- A MAC address pool is used by a DHCP server to define which systems in your network can receive an IP address. This is typically used for security purposes. You can force the DHCP server to give out leases only to MAC addresses that are entered in this pool by setting the **RegisteredClientsOnly** policy for the DHCP server to True. For more information on the **RegisteredClientsOnly** policy, refer to Table 2-2, "Server-level policies" (p. 2-15).
- A read-only user can only view the server MAC address pool.

Procedure

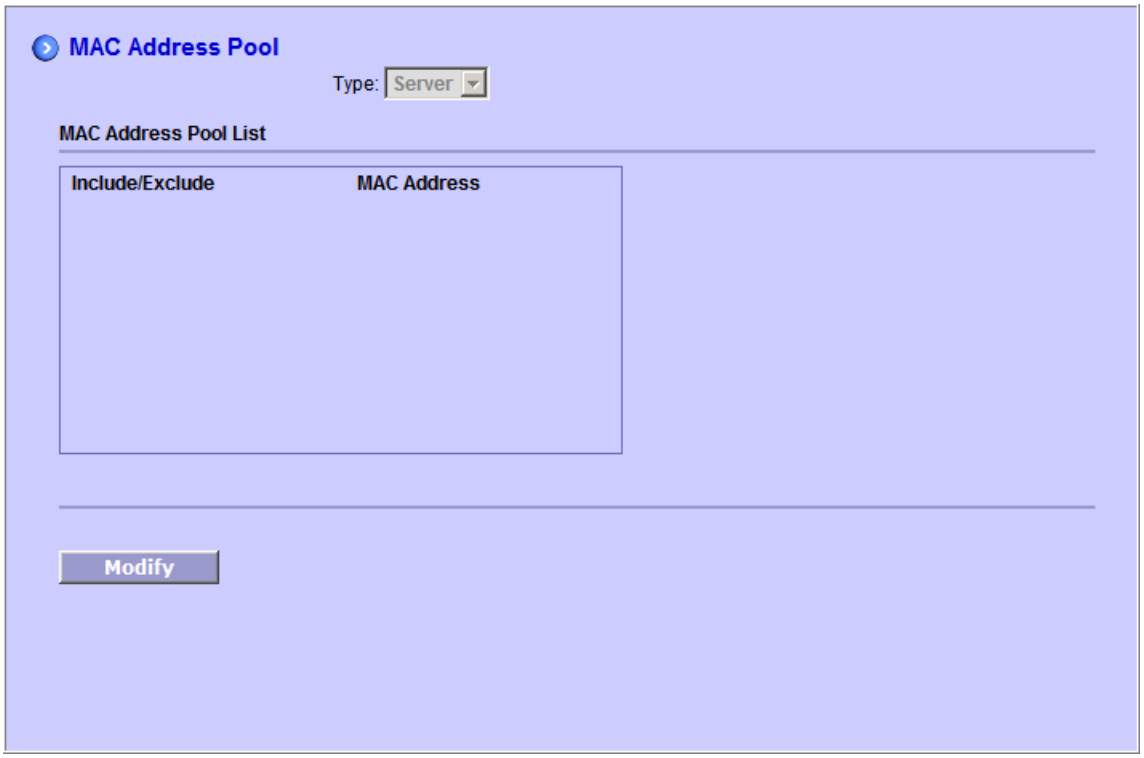
To view or modify a MAC address pool at the server level, follow these steps.

1. Click on the DHCP Server in the hierarchy.

   Result: The Server Properties page opens.

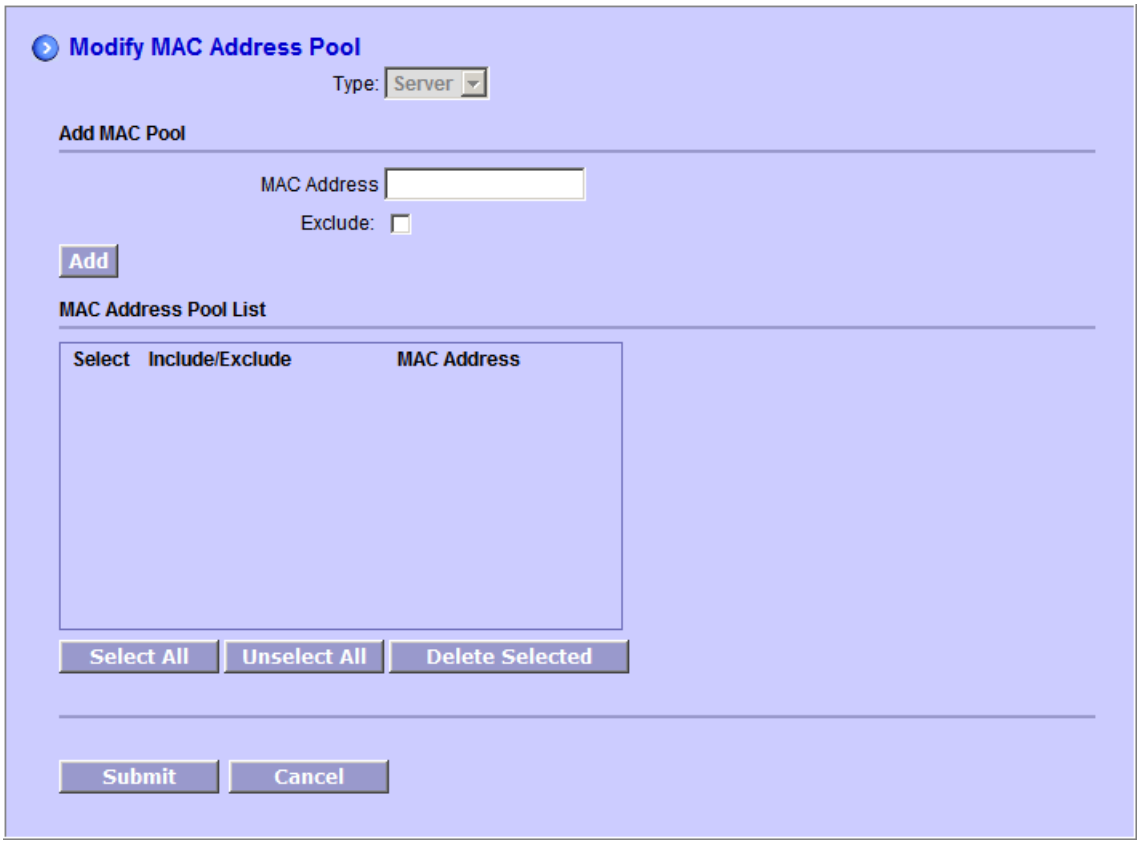
2. Click **MAC Pools**.

Result: The MAC Address Pool page opens.



3 To modify the MAC address pool, at the server level, click **Modify**.

Result: The Modify MAC Address Pool page opens.



4 To add a MAC address to the pool list, enter a valid address in hexadecimal format in the **MAC Address** field. Adhere to the following rules:

- Valid inputs are 0-9 a-f A-F : and the wildcard character *

  Note: Although the standard IEEE format for displaying MAC addresses is six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), the DHCP Configuration Manager UI only accepts colons (the same as VitalQIP).

- Wildcards can be used but only as the last character. At least one hexadecimal digit is required before the wildcard.
- Valid length is 17 (including colons) for server-level MAC Pools. If colons are not used during data entry, the valid length is 12 characters.
- You cannot add duplicate MAC addresses. However, duplicate MAC address ranges as a result of using wildcards are permitted. For example, a MAC address of 1122* and 112* are not considered duplicates. MAC addresses of 1122* and 1122* are considered duplicates, however, and are not permitted (even if one is included and one is excluded).

5 If you want to exclude a MAC address from the pool, select the **Exclude** check box. Otherwise, leave this check box unselected to include this MAC address.

6 Click **Add**.

Result: The address is added to the MAC Address Pool List.

7 If you wish to remove one or more MAC addresses from the MAC Address Pool List, follow these steps.

a. Place a check next to an address to be removed.

To select all MAC addresses, click **Select All**.

To remove all checkmarks, click **Unselect All**.

b. When you are ready to remove selected addresses from the list, click **Delete Selected**.

8 When you have completed modifying the MAC Address Pool List, click **Submit**.

Result: An information dialog box opens with the message **MAC address pool saved**.

9 Click **OK**.

Result: The MAC Address Pool page opens.

END OF STEPS

View/modify server policies

Purpose

To view or modify server policies.

Before you begin

- Policy names starting with **Failover.Primary** are applicable to the primary DHCP server only; those starting with **Failover.Secondary** are applicable to the secondary DHCP server only; and those starting with just **Failover.** are applicable to both primary and secondary DHCP servers.
- When Failover policies are written to *dhcpd.pcy*, the **Failover.**, **Failover.Primary.** and **Failover.Secondary.** prefixes are stripped off. They are for GUI display-purposes only. For example, **Failover.Primary.SecondaryIpAddr=10.4.0.5** is written to *dhcpd.pcy* as `SecondaryIpAddr=10.4.0.5`.
- A read-only user can view server policies.

Procedure

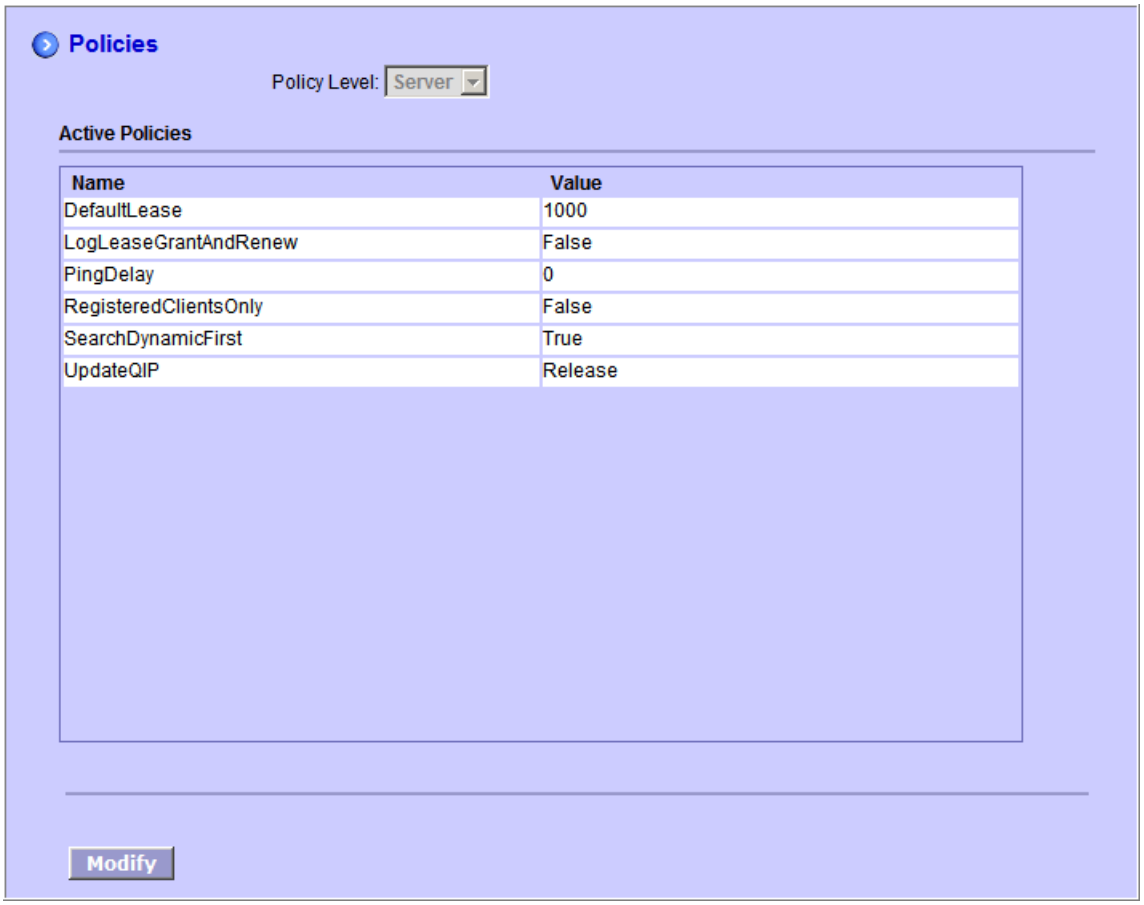
To view or modify server policies, follow these steps.

1 Click on the DHCP Server in the hierarchy.

Result: The Server Properties page opens.

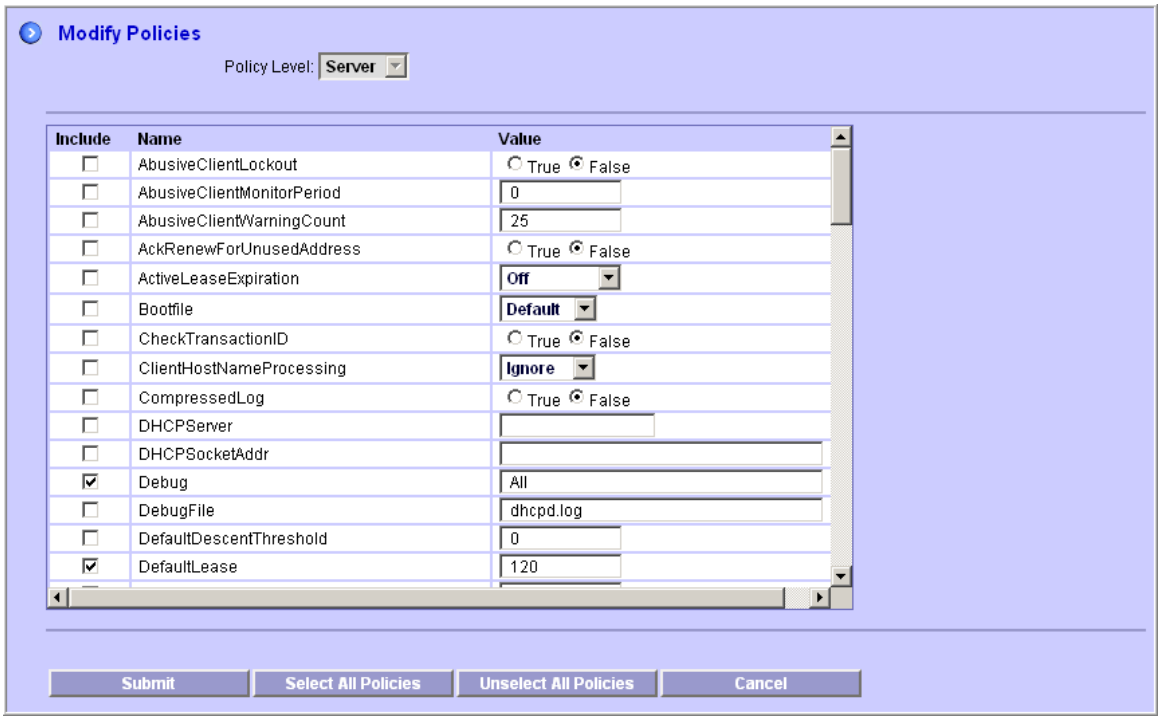
2 Click **Server Policies**.

Result: The Policies page opens. The policies that are currently enabled at the server level are displayed.



3 If you wish to modify an active policy or add a server-level policy, click **Modify**.

Result: The Modify Policies page opens.



4 Modify the server-level policies, as follows.

- Place a check in the checkbox next to a policy you wish to add. Only the checked policies are applied to the server. As you make your changes, refer to the following table for information on each policy.
- To select every policy, click **Select All Policies**.
- Uncheck the checkbox beside a policy you wish to remove.
- To remove checkmarks from all policies, click **Unselect All Policies**.

5 Click **Submit**.

Result: An information dialog box opens with the message **Policies saved**.

6 Click **OK**.

Result: The Policies page opens.

END OF STEPS

Table 2-2 Server-level policies

Policy name	Values	Default value	Usage
AbusiveClientLockout	True False	False	***Lucent DHCP 5.6 server and above only.*** When set to True, the DHCP server adds abusive clients to the global MAC exclusion pool, if a client sends more DHCP packets than the limit specified by the AbusiveClientWarningCount policy within the time specified in the AbusiveClientMonitorPeriod policy. The addition to the MAC exclusion pool is transient and will be removed on the next generation to the DHCP server. By default, the DHCP server does not add abusive clients to the MAC exclusion pool. To create a non-transient entry in the global MAC exclusion pool, the administrator must enter the MAC in the exclusion pool using VitalQIP.
AbusiveClientMonitor Period	Numeric	0	***Lucent DHCP 5.6 server and above only.*** By default, the DHCP server does not attempt to detect abusive clients. The value entered indicates the number of seconds during which the DHCP server determines whether a client is abusive.
AbusiveClientWarning Count	Numeric	25	***Lucent DHCP 5.6 server and above only.*** Indicates the maximum number of DHCP packets the server can receive from a DHCP client within the time period set by the AbusiveClientMonitorPeriod policy, before it issues a warning and adds the client to the MAC exclusion pool.
AckRenewForUnused Address		False	If you set this policy to True, the DHCP server will acknowledge a renew request for an IP address that is not in the server's active lease table, provided that this address is in the server's managed ranges.

Policy name	Values	Default value	Usage
ActiveLeaseExpiration	Off Notify_only Full_delete	Off	Determines how expired leases are handled. The following values are available: • **Off** - causes expired leases to not be actively deleted at expiration. • **Notify_only** - causes only expired lease messages to be sent to the Message Service. • **Full_delete** - causes the lease from DHCP database to be deleted, and the Message Service to be notified of expired leases. **Note:** If expired leases are not deleted upon server restart, you may delete the *dhcpd.exp* file to allow leases to be deleted during the next expiration processing cycle. For example, this situation may occur in the event the **ExpireAllLeasesOnRestart** policy is changed from False to True. **ActiveLeaseExpiration** should only be configured on primary servers. A failover (secondary) server should have this options set to Off.
Bootfile	Default Hwaddr	Default	The following options are available: • **Default** - used if nothing is set for this policy. It indicates that the bootfile is expected to be in the **`options`** block from the template assigned to the scope. • **Hwaddr** - indicates that the server should set the "bootfile" field of the DHCP header to the client's MAC address. This is done only if there is no bootfile defined in the **`options`** block from the template assigned to the scope. The template overrides this setting.

Policy name	Values	Default value	Usage
CheckTransactionID	True False	False	This policy is used to configure the service to ignore multiple discover, request, and Bootp messages that have the same XID. **Note:** This policy should only be turned on in environments where there are multiple routes from the client subnets to the DHCP service, and some of those routes are much slower than other routes. If turned on, Microsoft Windows clients running WINSOCK2 do not obtain a lease when changing subnets, or when negotiating a lease with a new service.
ClientHostName Processing	Ignore Reject Correct	Ignore	This policy determines how the server handles DHCP client requests that have invalid DNS hostnames. The following values are available: • **Ignore** - the server passes all hostnames "as is" to the VitalQIP Message Service for updates to VitalQIP and DNS. • **Reject** - the server does not answer the client's request when its name is invalid for DNS. • **Correct** - the server changes all invalid characters in the client's hostname to dashes (-) before sending to the VitalQIP Message Service for VitalQIP/DNS updates. In the Ignore or Correct modes, the service always replaces embedded or trailing spaces in the hostname with dashes (-).
CompressedLog	True False	False	This policy causes the server logging to put the fields of the incoming/outgoing packets on a single line, depending on the logging level. The options are enumerated on a single line when the policy is set in the full debug mode and spread out to have one option per line when it is not set in the full debug mode.

Policy name	Values	Default value	Usage
DHCPServer	IP address		Defines the "local" subnet for the server in a multi-NIC configuration. Any LOCAL broadcast DHCP client discover, regardless of which NIC it is received on, will result in an address being offered from the subnet containing this address. The server still honors the giaddr criterion for nonlocal broadcast discovers. The DHCPServer policy, when specified, is also used to populate the server ID option (option 54) in outgoing OFFER and ACK messages, as well as the server ID field in the outgoing update messages (to VitalQIP, and so on). When the policy is not specified, these fields are set to the NIC address on which the client request was received. For more information on this policy, refer to Chapter 26 in the *VitalQIP Administrator Reference Manual*.

DHCPSocketAddr	IP address		This policy is used to configure which network interfaces (NICs) the service should listen on. By default, this policy is not set allowing the service to listen on all NICs. In order to specifically tell the Lucent DHCP Service to ignore an interface, each desired interface must be set using this policy, and if specified, the service binds to port 67 on the NIC that has this address. Otherwise, the service binds to all interfaces.
			DHCP Configuration Manager accepts a comma-separated list of IP addresses.
			Each IP address results in one line of `DHCPSocketAddr=`*`Value`*. For example, **`DHCPSocketAddr=10.4.0.1, 10.4.0.2`** on GUI results in the following two lines in *dhcpd.pcy*:
			`DHCPSocketAddr=10.4.0.1`
			`DHCPSocketAddr=10.4.0.2`

Debug			Sets the debug level. For more information, refer to Chapter 4 in the *VitalQIP User's Guide*.
DebugFile		*dhcpd.log*	Sets the debug file name.

Policy name	Values	Default value	Usage
DefaultDescentThreshold	0-100	0	***Used with SNMP Module only***. This policy determines the subnet lease percent unavailable value, which when passed, causes the SNMP trap **`dhcpServerSubnetThresholdDescent`** to be issued. A value of zero disables the monitoring of lease percent unavailable for the server. The policy can be overridden by the **subnet-unavailable-descent-threshold** configuration file policy on a subnet-by-subnet basis. Refer to Table 3-1, "Subnet-level policies" (p. 3-15).
DefaultLease	Numeric	7776000 (90 days)	Lease time offered by the server in the event no Lease Time is defined in the configuration file. The server needs a default lease time in case there is none defined (as a result of a manual or user exit edit).
DefaultUnavailable Threshold	0 - 100	0	***Used with SNMP Module only***. This policy determines the subnet lease percent unavailable, which when exceeded, causes the SNMP trap **`dhcpServerSubnetThresholdExceeded`** to be issued. A value of zero disables the monitoring of lease percent unavailable for the server. The policy can be overridden by the **subnet-unavailable-threshold** configuration file policy on a subnet-by-subnet basis. Refer to Table 3-1, "Subnet-level policies" (p. 3-15).
DropAllDhcpInform Packets	True False	False	If you set this policy to True, the DHCP server precludes the processing of any DHCPINFORM packet, beyond the parsing of the incoming packet. This policy allows administrators to configure the DHCP server to ignore inform packets, when the processing of the same is not required. The default value for the policy is False.
DropZeroMacAddress Packets	True False	True	When set to True, the server checks all incoming packets for a zero MAC address and drops the packet if found. **Note:** DHCPINFORM messages are processed regardless.

Policy name	Values	Default value	Usage
ExpireAllLeasesOnRestart	True False	True	When set to False, only leases that have expired since the service restarted are deleted. When the option is set to True, all expired leases found in the database are deleted.
Failover.Primary.CtlReq RetryMax	Numeric	3	If no CtlRet message is received from the failover server in the time specified by **Failover.Primary.WaitCtlRetSecs**, attempt to contact the failover by resending the CtlReq message this many times. If this maximum is reached without receiving a CtlRet response, the primary assumes that the failover is inoperable, and continues on to operate as a DHCP server. It continues to send all binding changes to the server identified in the **Failover.Primary.SecondaryIpAddr** parameter, even though that server may not be up. The recommended maximum value is 10. **Note:** If both the **Failover.Primary.CtlReqRetryMax** and **Failover.Primary.WaitCtlRetSecs** parameters are specified, while the DHCP server is waiting, no addresses are given out. Large values could cause delays in offering leases following a server startup.
Failover.Primary. SecondaryIpAddr	IP address		IP address that identifies the failover DHCP server.
Failover.Primary.WaitCtl RetSecs	Numeric	5	The number of seconds that the primary server should wait for a response to the CtlReq (request for control) message sent to the failover server at startup. The maximum number of seconds is 3600 (1 hour). If a value of zero is supplied, the default is used. If both the **Failover.Primary.CtlReqRetryMax** and **Failover.Primary.WaitCtlRetSecs** parameters are specified, while the DHCP server is waiting, no addresses are given out.

Policy name	Values	Default value	Usage
Failover.Secondary.Poll Delay	Numeric in seconds	60	The amount of time between each poll/reply sequence, specified in seconds. Upon startup, after synchronization (if specified), the failover sends a poll message to the primary server. It waits for the amount of time specified by the **Failover.Primary.WaitPollRplSecs** parameter for a reply. If a reply is received, the failover server "sleeps" for the amount of time specified by this parameter before sending another poll message to the primary server. The maximum value is 86400 (1 day).
Failover.Secondary.Poll RetryMax	Numeric	3	If no reply to the poll message is received from the primary, the failover retries sending the poll message and waiting for a reply for this number of times before assuming that the primary has crashed and becomes active in handling DHCP client requests. The maximum is 10.
Failover.Secondary. PrimaryIpAddr	IP address		Comma-separated list of IP Addresses identifying all primary DHCP servers for which this server is secondary. Each IP address in the list results in one policy line in the policy file with the following format: `PrimaryIpAddrX=`*`ValueX`* where *`X`* is an incremental number starting with 1 and *`Value`* is the IP address from the list.
Failover.Secondary.Sync Bindings	True False	True	If this policy is True, the failover server requests all current binding information from the primary at startup.
Failover.Secondary.Sync FailCritical	True False	False	If True, the failover server terminates upon failure to synchronize bindings with the primary server. Note that this option only applies if the **Failover.Secondary.SyncBindings** policy is True.

Policy name	Values	Default value	Usage
Failover.Secondary.SyncReqRetryMax	Numeric	3	If no SyncStart message is received from the primary server in the time specified by **Failover.Secondary.WaitSyncStartSecs**, attempt to contact the primary by resending the SyncReq message this many times. If this maximum is reached without receiving a SyncStart response, this failover checks the value of the **Failover.Secondary.SyncFailCritical** policy. If that policy is True, this secondary server terminates. Otherwise, this secondary server initiates polling of the primary server. The maximum value is 10.
Failover.Secondary.WaitPollRplSecs	Numeric (in seconds)	5	The number of seconds that the failover should wait for a poll reply from the primary. Note that if the failover receives a binding update from the primary during this period, the primary is assumed operational, and the binding update message is taken as a response to the poll. The maximum is 3600 (1 hour).
Failover.Secondary.WaitSyncStartSecs	Numeric (in seconds)	5	The number of seconds that the failover server should wait for a response to the SyncReq (request for bindings) message sent to the primary server at start-up. A value of zero causes the server to wait indefinitely. The maximum value is 3600 (1 hour).
Failover.SyncBindRetryMax	Numeric	3	The number of times the server should resend a binding update if an Ack is not received within **Failover.Secondary.WaitSyncBindAckSecs**.
Failover.SyncBindingBufSize	Numeric (in bytes)	1024	Size of the "options" area for synchronizing the binding information between the primary and secondary servers. **Note:** This value ***must*** be the same on ***both*** servers. The minimum value is 64. The maximum value is 4096.
Failover.WaitSyncBindAckSecs	Numeric	5	The number of seconds the server waits for an Ack to a binding update packet when operating on the sending side of synchronizing with the other server.

Policy name	Values	Default value	Usage
Failover.WaitSyncBind UpdateSecs	Numeric	15	The number of seconds that the server should wait for subsequent binding update packets when operating on the receiving side of synchronizing with the other server.
ForceClass	None Both Vendor User	None	Determines if the server verifies a client's request for a lease before issuing a lease. The values are as follows: **None** - allows the server to issue leases from any scope to any incoming client request. **Both** - forces the server to require a match for both user and vendor class against those defined for a particular scope. **Vendor** - causes the server to require a match on vendor class only. **User** - causes the server to require a match on user class only. **Note:** Windows clients always send a vendor class, and optionally send a user class. Therefore, scopes should be defined with vendor class of "MSFT 5.0" and user classes as required. This policy should be set to "Both."
HonorRequestedLease Time	True False	True	If this policy is True, the server honors requested lease times from the client. If set to False, the server offers the configured lease time. **Note:** If this policy is set False and the client is requesting a lease shorter than the configured lease time, the requested lease time is granted.
HonorUnqualifiedBootfile	True False	False	This policy instructs the server to echo the "bootfile" field back to the requesting client on responses, even when this name is unqualified. (The Bootp RFC implies that unqualified names indicate the client is requesting the file configured on the server for the client.)

Policy name	Values	Default value	Usage
InitRebootAddressShuffle	Off On	Off	If this policy is set to Off, an address shuffle is not performed on init/reboot requests. If this policy is set to On, an address shuffle is performed on init/reboot requests. **Note:** This policy can also be specified at the subnet and scope levels (listed in increasing order of precedence) through the *dhcpd.conf* file. The server-level policy is overridden if a different policy value is specified at any of the other levels applicable to a lease.
IssueDropUnknownClient Trap	True False	False	***Used with SNMP Module only***. When set to True, allows the server to generate an SNMP trap whenever a client request is explicitly dropped because its MAC address is either in a MAC exclusion pool, or the MAC address is not in an inclusion pool.
LeaseExpirationSleep Time	Milliseconds	60000	A specified time interval at which lease expiration processing occurs.
LeaveBootpParameters InOptions	True False	False	This policy instructs the service to leave Options 66 and 67 in the "Options" area of the outgoing DHCP reply packets. If this policy is set to False, the service ***moves*** the values assigned for these options to their appropriate locations in the Bootp header – the "sname" and "file" fields respectively. If set to True, the values are ***copied*** and not moved.
ListenOnLoopback	True False	False	This policy causes the server to create a socket and listen on port 67 of the loopback interface 127.0.0.1. This policy is only required when used with the Services Manager add-on product or the Probes package on the appliance, specifically when the DHCP Probe is placed on the same machine with the Lucent DHCP Service.
LogLeaseGrantAndRenew	True False	True	When this policy is set to True, the DHCP server writes an entry to the event/system log for each lease grant and renew. When set to False, logging does not occur.

Policy name	Values	Default value	Usage
MacWarningsToEventLog	True False	False	If this policy is set to False, rejected client requests are sent to the debug log. If this policy is set to True, the rejected client request messages are sent to the event log (Windows 2003/2008) or syslog (UNIX).
MaxDebugFileSize	Numeric	-1	This policy controls the size of the dhcpd.log file, specified in bytes. The default setting of –1 causes the log to grow indefinitely. A value greater than 0 causes the server to replace the log file after the number of bytes designated is written to the log file. If the FeatureBackup setting is used with the Debug policy, the current *dhcpd.log* file is first copied to *dhcpd.bak_1.log* before creating a new *dhcpd.log* file.
MaxOutgoingDhcp MessageSize	Numeric	1024	Allows for the configuration of the maximum size in bytes of a DHCP message sent from the Lucent DHCP server, which may vary from network to network.
MaxPendingSeconds	Numeric	10	The number of seconds that an offered lease remains in a pending state. When the server responds to a client's DHCP Discover request with a DHCP Offer, the address is marked as pending. By default, the server waits ten seconds for a DHCP Request for this address from the client before unmarking the address, and then making it available to offer to another client.
MaxUnavailableTime	Seconds	86400 (1 day)	This policy determines the period of time that an IP address is considered unavailable following a DHCPDECLINE or ping before assign offer response. Beyond this time, the server considers this address as available.
NackDhcpRequestsFor Duplicates	True False	True	When set to True, sends a NAK if a RENEW/REBIND request or SELECTING request is received for an IP already owned by another hardware address. When set to False, the invalid request is merely dropped.

Policy name	Values	Default value	Usage
NakUnknownClients	True False	True	This policy causes the server to NAK clients who request addresses that are not in the service's defined subnets. This policy should be set to False in environments where multiple DHCP services are servicing the same subnets (not failover). When set to True, the service returns a NAK to these client requests, which causes the client to revert to INIT state. The client then obtains a lease from one of the configured scopes for the client's current subnet.
OfferOnlyApiRequested Address	True False	False	This policy forces the DHCP server to offer the address that is specified by the discover API callout in the requested IP address parameter. If the address is not available for any reason (unmanaged, in use, forceClass mismatch, and so on), the discover message will be dropped and an Info level message is written to the DHCP log. This capability allows service provider environments to offer and acknowledge IP addresses specified by Vital Access. The default value for this policy is False.

Policy name	Values	Default value	Usage
Option81Support	Suppress Client Server Ignore	Suppress	The following options are available: • **Suppress** - causes the server to ignore the client FQDN option 81 data in the packet, and update VitalQIP/DNS with the hostname in option 12 of the client's request and the domain name configured for the scope from which the service issued a lease. • **Client** - causes the server to honor the client FQDN option 81, meaning that if instructed by the client, the service updates only the client's PTR record in DNS (via the Message Service or VitalQIP Update Service), using the FQDN contained in option 81. **Note:** If the host name is unqualified, the VitalQIP QIP Update Service (**`qip-qipupdated`**) will attach the default domain for the subnet. If this behavior is not desired, you may remove the default domain from the subnet in VitalQIP. • **Server** - causes the server to perform both the A and PTR record updates, using the FQDN contained in option 81. • **Ignore** - causes the server to exclude option 81 data from OFFER and ACK packets. This feature causes Windows Professional DHCP clients to update their own A and PTR records.
PadBootpReply	True False	True	This policy causes the server to pad Bootp reply and DHCP Offer/ACK messages to 300 bytes.
PingAttempts	Numeric	1	The number of times to perform a ping.
PingBeforeManualBootp	True False	False	Perform a ping before assigning a Manual Bootp address. If an ICMP_REPLY is received from the ping, no Bootp reply is sent to the client, and the address is marked as unavailable.
PingBeforeManualDhcp	True False	True	Perform a ping before assigning a Manual DHCP address. If an ICMP_REPLY is received from the ping, no offer is sent to the client and the address is marked as unavailable.

Policy name	Values	Default value	Usage
PingDelay	Milliseconds	500	This value determines the amount of time the DHCP server waits for a response regarding the availability of an IP address.
PingRetention	Seconds	0	This specifies the amount of time a ping is "good for". If a ping is attempted and no response is returned, then the address is assumed available. If another request comes into the service that would cause it to attempt a ping on a previously pinged address, this ping does not take place if it is within defined seconds of the previous ping.
PingSendDelay	Milliseconds	0	The amount of time between subsequent pings. Applicable only if the PingAttempts is greater than 1.
RegisteredClientsOnly	True False	False	This option is only used when MAC pool addresses are defined at either the global or the subnet level. If this value is set to False, the DHCP Service responds to clients with a MAC address that is unknown to the server. Choose True to have DHCP information provided to only those hosts that have a known MAC address (configured in a MAC pool). Choose False to have DHCP information provided to all clients. If this option is set to True when no MAC pool addresses are defined at either the global or the subnet level, no device will be given a DHCP lease. **Note:** The addresses of manual DHCP and manual Bootp devices are automatically added to the appropriate subnet MAC pool, if it exists. If there is no subnet MAC pool but a global pool exists, they are added there.

Policy name	Values	Default value	Usage
RenewAddressShuffle	Off On	Off	If this policy is set to Off, no address shuffling is performed during lease renewals. If this policy is set to On, address shuffling is performed after the maximum renewals. If this policy is not set, it will not work at lower levels. **Note:** This policy can also be specified at the subnet and scope levels (listed in increasing order of precedence) through the *dhcpd.conf* file. The server level policy is overridden if a different policy value is specified at any of the other levels applicable to a lease.
RenewAddressShuffleMax Count	Numeric	0	This policy defines the maximum number of lease renewals before forcing an address shuffle. **Note:** This policy can also be specified at the subnet and scope levels (listed in increasing order of precedence) through the *dhcpd.conf* file. If renew address shuffling is "On" at more than one level applicable to a particular lease (with different maximum counts), the address shuffle occurs after the lesser of the maximum count is reached.
SearchDynamicFirst	True False	False	If the policy is set to False, then if both the A-DHCP (Automatic DHCP) and D-DHCP (Dynamic DHCP) ranges are specified within a single subnet (or shared subnet), the service uses all A-DHCP addresses first. Otherwise, it must be set to True to issue D-DHCP leases first.
SendRequestedParams Only	True False	False	If set to True, this policy instructs the DHCP Service to send only the options requested by the client. If the client sends a DHCP parameter request list Option (55) in the Discover packet, then the service sends only the Options that are both configured and requested by the client. However, Options subnet-mask (1) and lease-time (51) are always sent to the client, in addition to the IP address. When False, the service sends all configured Options to the client.

Policy name	Values	Default value	Usage
SendServerIdLast	True False	False	When set to True, this policy allows Windows clients to update their A and PTR records: it causes the server to place the server ID (option 54) after most of the other options in the OFFER and ACK packets. When set to False, the server inserts the server ID as the second option, following the message ID.
ShareAutoBootpAndDyn Dhcp	True False	False	If the policy is set to True, Automatic Bootp, Dynamic DHCP and Automatic DHCP clients share address pools. If both D-DHCP/A-DHCP and A-BOOTP ranges are defined in a single subnet, DHCP clients get addresses from the D-DHCP/A-DHCP ranges first and then from the A-BOOTP ranges when the DHCP Addresses are exhausted. Bootp Clients get addresses from the A-BOOTP ranges first, then from the D-DHCP ranges when the A-BOOTP addresses are exhausted.
SharedNetworkThreshold Processing	True False	False	When set to True, the DHCP server performs threshold monitor processing for a shared network as a single entity, rather than on each individual subnet within the shared network. The server continues to perform threshold monitoring on each individual subnet, as the default is set to False. The default server threshold values specified by the **DefaultUnavailableThreshold** and **DefaultDescentThreshold** server policies, are used for threshold monitor processing of all shared networks. When this policy is set to True, subnets that are not part of a shared network will still have individual threshold monitoring. This capability supports the issuing of both the Subnet Threshold Exceeded trap and the Subnet Descent Threshold trap for the shared network, replacing the subnet address in the text of the trap message with the shared network ID. The applicable configured threshold value is also included in the trap message.

Policy name	Values	Default value	Usage
SupportAutoRelease	True False	True	Release any previous leases for a client (based on the MAC address) when the client receives a new lease.
SupportBootpAuto Release	True False	True	Release any previous leases for a client (based on the MAC address) when the client receives a new lease. ***Used for Bootp clients only***.
SupportEncodingLong Options	True False	False	Set to True to allow long options to be split into multiple instances. Currently, there are three options that require long option support: the classless static route option (121), the CableLabs Client Configuration option (122), and the Domain Search option (119). When set to False, options longer than 255 bytes are not split by the server and are ignored.
SupportMultiUserClass		False	You can configure the DHCP server to support user class (option 77) values from DHCP clients that conform to RFC 3004. This RFC allows multiple values in canonical wire format and ASCII encoded format.
SupportRelayAgentDevice Class	True False	False	When set to True, the server supports the assignment of DHCP options specifically by DOCSIS device class. Options are configured using the device class client class in VitalQIP, and will be assigned if the device class suboption of the relay agent option (option 82) matches the device class value specified in the client class. Set to True to enable the device class and make the Device Class Client Class useful.
SupportRelayAgentOption	True False	True	This policy allows the server to support the Relay Agent Option (82). This policy causes the server to echo the contents of option 82, if present, into all outgoing packets.
SupportRelayAgentServer Override		False	This enables the server to process the **Server Override** suboption of the **Relay Agent** option (option 82) according to RFC 5107.

Policy name	Values	Default value	Usage
SupportSubnetSelection	True False	False	When this policy is set to False, the subnet selection option (118) and the option 82 suboption 5 are not processed by the server. Dynamic address allocation proceeds by using the 'giaddr' field in the discover message or the local interface address for determining the DHCP client's subnet. A value of True allows the subnet selection option to be processed by the server. When using this option, a subnet address is specified, and the DHCP server allocates IP addresses from the specified subnet or a subnet on the same network segment as the specified subnet.
ThresholdMonitorSleep Time	Seconds	60	***Used with SNMP Module only***. This policy specifies the time interval at which lease percent unavailable monitoring occurs.
UpdatePreclusion Duration	0-300	60	You can define a time period during which the DHCP server does not send "duplicate" ADD type update messages to the Message Service. Use this policy to reduce the update message queuing problems seen in some customer sites. In particular, where there are redundant relays configured. Any value specified that exceeds a maximum limit value of 300 seconds is overridden with the maximum limit. A policy value of 0 disables this feature.

Policy name	Values	Default value	Usage
UpdateQIP	Autorelease Bootp Decline Delete Expiration Grant Release Renew	all values	If all keywords are set to True, a message is sent to VitalQIP Message Service to update VitalQIP and/or DNS. Otherwise, the policy updates VitalQIP with the values listed. The values are as follows: • **Autorelease** - release is performed by the server when a client changes subnets • **Bootp** - Bootp client gets a lease • **Decline** - refuses a lease • **Delete** - Administrator deletes a lease through the GUI • **Expiration** - lease expiration detected by active lease expiration processing • **Grant** - grants a new lease • **Release** - releases an existing lease • **Renew** - renews an existing lease
ZeroCiAddr	True False	False	This policy only affects the contents of the "ciaddr" field in outgoing packets. If this policy is set to True, the server fills in "ciaddr" with 0.0.0.0 on reply (ACK) packets. **Note:** 0.0.0.0 is always in OFFERs.
UnknownPolicy1			A policy in *dhcpd.pcy* file that DHCP Configuration Manager does not support.
UnknownPolicy2			A policy in *dhcpd.pcy* file that DHCP Configuration Manager does not support.

3 Subnet operations

Overview

Purpose

This chapter describes how to manage subnets.

Contents

This chapter covers these topics.

Manage a subnet

Overview

DHCP Configuration Manager supports the following subnet-level operations:

- Add a subnet
- Delete a subnet
- View subnet properties
- Add a scope
- View/modify subnet-level policies
- View/modify subnet level MAC address pools

Any changes made are not saved in the DHCP configuration file until explicitly saved or discarded. The **Server Actions** menu contains the **Save Changes** and **Discard Changes** sub-menus.

Add a subnet

Purpose

To add a subnet for a DHCP server.

Before you begin

A read-only user cannot add a subnet.

Procedure

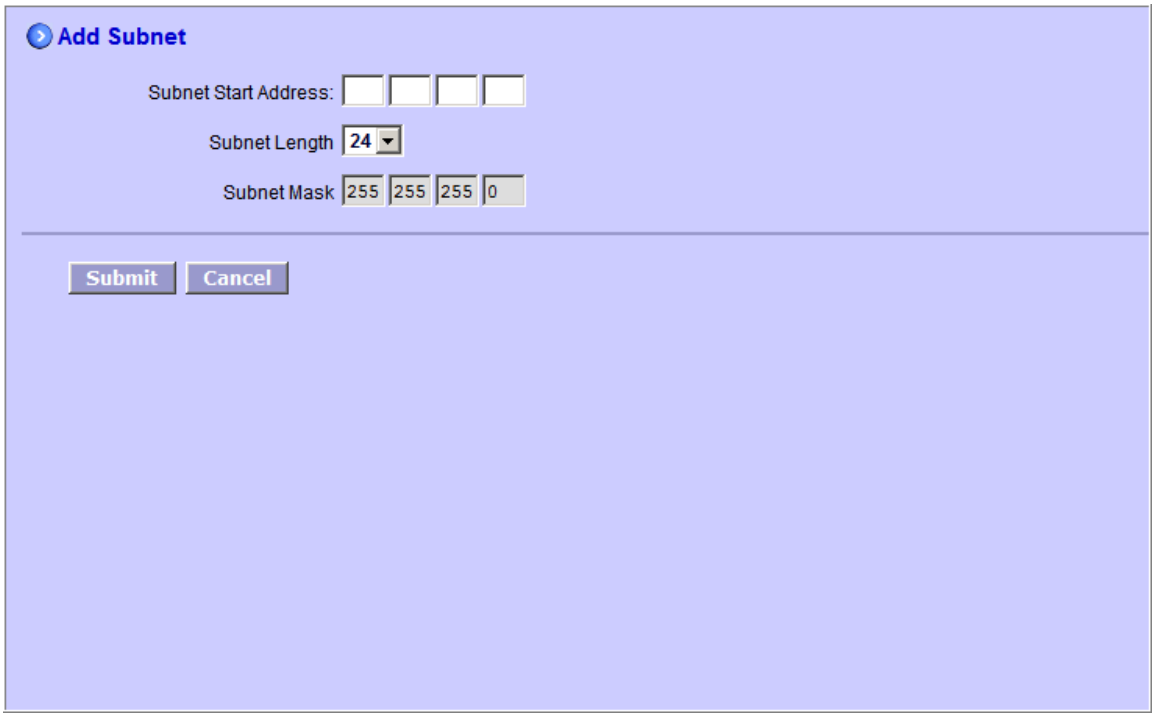
To add a subnet, follow these steps.

1 In the DHCP Server page, click on a DHCP Server in the DHCP Server hierarchy.

Result: The Server Properties page opens.

2 Click **Add Subnet**.

Result: The Add Subnet page opens.



3 Enter the four octets of the IPv4 subnet start address in the **Subnet Start Address** field.

4 Select the subnet length from the **Subnet Length** dropdown list. The default is 24.

Result: The subnet mask is automatically displayed in the **Subnet Mask** field.

5 Click **Submit**.

Result: The Subnets node in the DHCP Server Hierarchy is updated with the new subnet and the Subnet Properties page is displayed.

END OF STEPS

View subnet properties

Purpose

To view the properties of a subnet.

Procedure

To view subnet properties, follow these steps.

1. Click on the Expand icon (⊞) next to the DHCP server in the hierarchy.

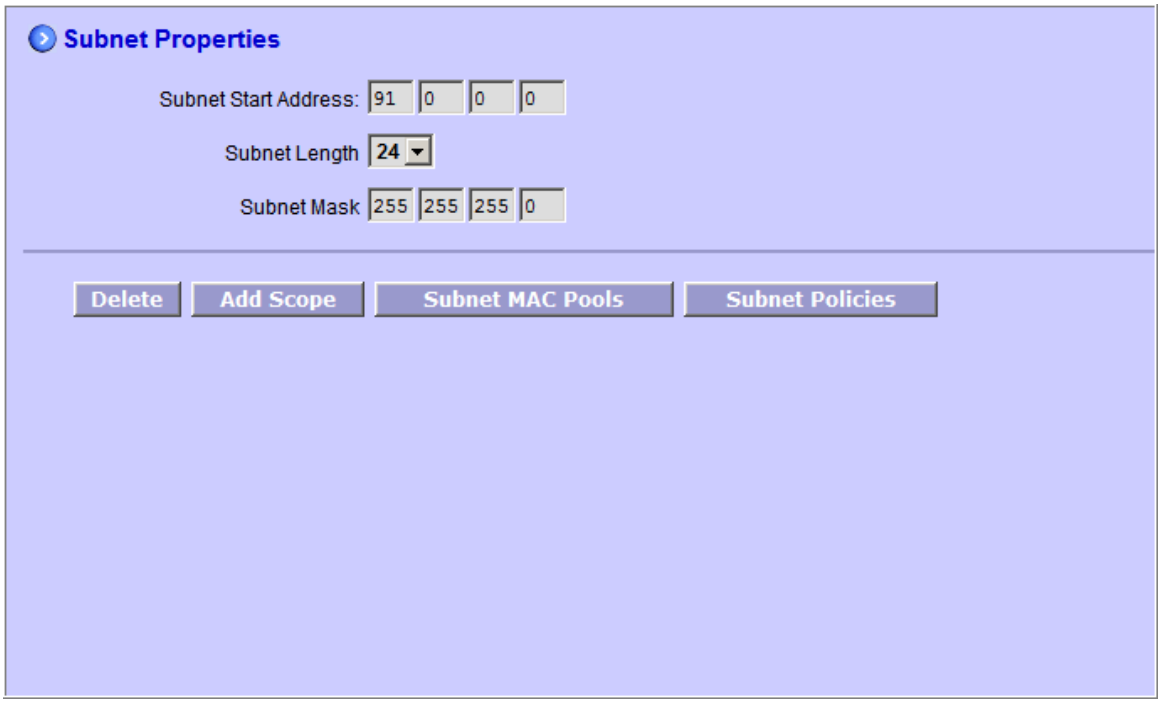
   Result: The Subnets node opens.

2. Click on the Expand icon (⊞) next to the Subnets node.

   Result: The Subnets node displays previously defined subnets.

3. Click on the subnet you want to view.

   Result: The Subnet Properties page is displayed.



4 Choose one of the following actions.

If you want to…	Then …
Delete the subnet	Click **Delete**. For more information, refer to "Delete a subnet" (p. 3-7). **Note:** This function is not available to read-only users.
Add a scope to the subnet	Click **Add Scope**. For more information, refer to "Add a scope" (p. 4-3). **Note:** This function is not available to read-only users.
View the MAC pools defined for the subnet	Click **Subnet MAC Pools**. For more information, refer to "View/modify subnet MAC pool" (p. 3-8).
View subnet-level policies	Click **Subnet Policies**. For more information, refer to "View/modify subnet policies" (p. 3-12). **Note:** Read-only users can only view subnet-level policies.

END OF STEPS

Delete a subnet

Purpose

To delete a subnet.

Before you begin

- When you delete a subnet, you also delete its scopes, MAC pool and subnet-level policies.
- A read-only user cannot delete a subnet.

Procedure

To delete a subnet, follow these steps.

1 Expand the DHCP Server ID and the Subnets node.

2 Click on the subnet you want to delete. Alternatively, enter the subnet address in the Search field and click **Find Next**.

Result: The Subnet Properties page is displayed.

3 Click **Delete**.

Result: A confirmation dialog box opens with the message **Deleting subnet <nnn.nnn.nnn.nnn/n> and its scopes**.

4 Click **OK**.

Result: An information dialog box opens.

5 Click **OK**.

The subnet, its scopes, MAC pool, and policies are removed. The **Subnets** label in the DHCP Server hierarchy changes color to indicate the change.

END OF STEPS

View/modify subnet MAC pool

Purpose

To view or modify a subnet MAC pool.

Before you begin

Read-only users can only view subnet MAC pools.

Procedure

To view or modify a subnet MAC pool, follow these steps.

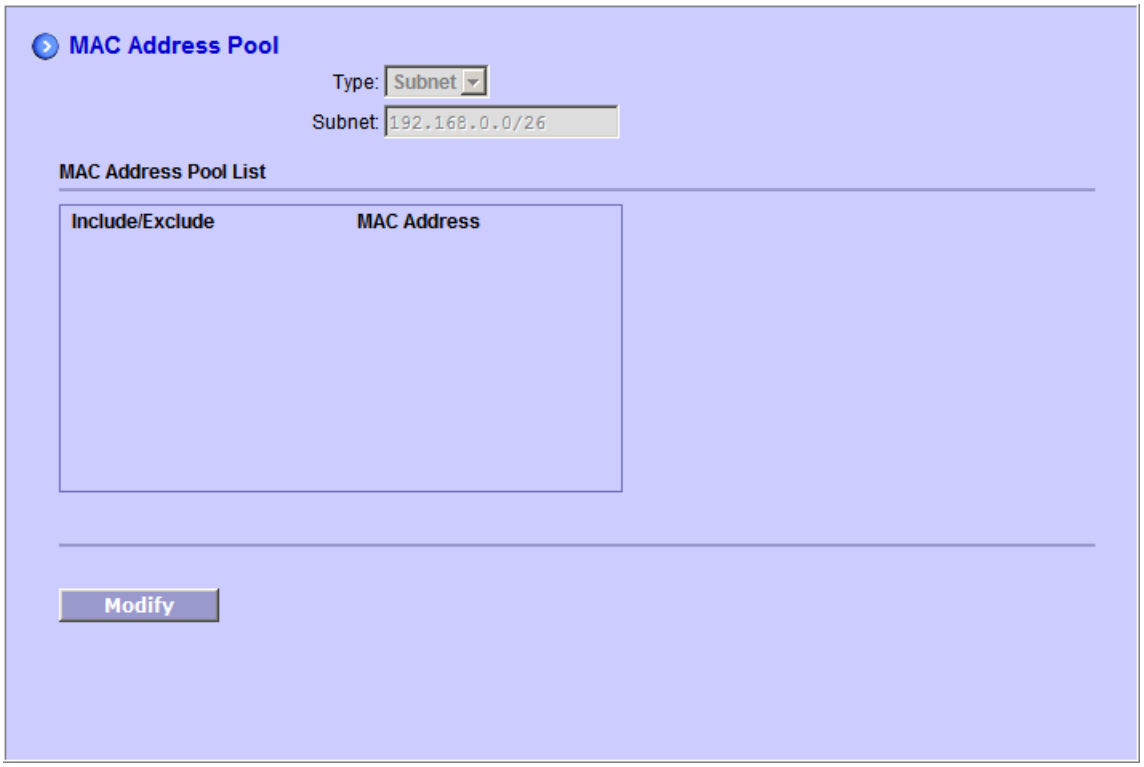
1. Expand the **DHCP Server ID** and the **Subnets** node.

2. Click on the subnet that contains the MAC address pool you want to view or modify.

   Result: The Subnet Properties page is displayed.

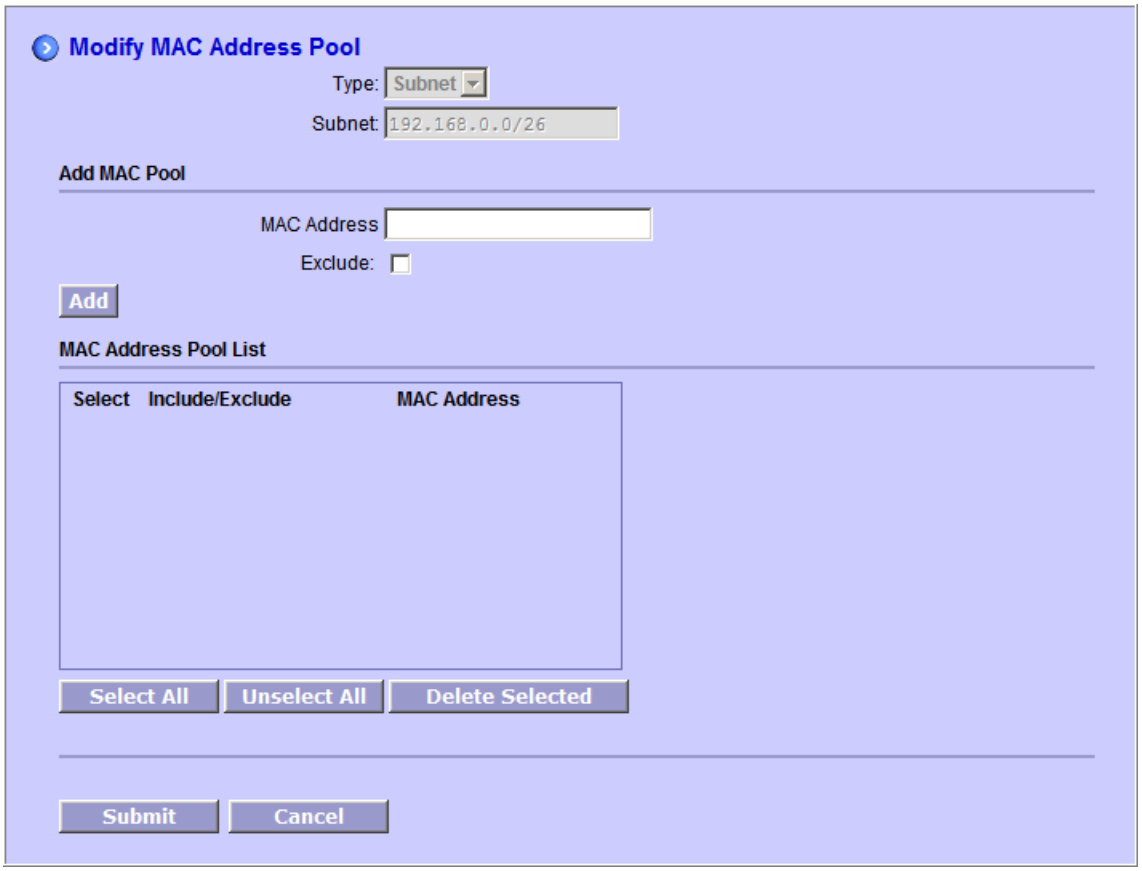
3. Click **Subnet MAC Pools**.

Result: The MAC Address Pool page opens.



4 To modify the MAC address pool, at the subnet level, click **Modify**.

Result: The Modify MAC Address Pool page opens.



5 To add a MAC address to the pool list, enter a valid address in hexadecimal format in the **MAC Address** field. Adhere to the following rules:

- Valid inputs are 0-9 a-f A-F : and the wildcard character *

  Note: Although the standard IEEE format for displaying MAC addresses is six groups of two hexadecimal digits, separated by hyphens (-) or colons (:), the DHCP Configuration Manager UI only accepts colons (the same as VitalQIP).

- Wildcards can be used but only as the last character. At least one hexadecimal digit is required before the wildcard.
- Valid length is 17 or 23 (including colons) for subnet-level MAC Pools. If colons are not used during data entry, the valid length is 12 or 16 characters.

  Note: The larger valid length for subnet MAC address pools is determined by the **allow_sixteen_chars_mac_addr** property in */opt/qdhcpmgr/conf/qdhcpmgr.properties*. If it is set to true, the larger length is considered valid. Refer to "allow_sixteen_chars_mac_addr" (p. A-3).

- You cannot add duplicate MAC addresses. However, duplicate MAC address ranges as a result of using wildcards are permitted. For example, a MAC address of 1122* and 112* are not considered duplicates. MAC addresses of 1122* and 1122* are considered duplicates, however, and are not permitted (even if one is included and one is excluded).

6 If you want to exclude a MAC address from the pool, select the **Exclude** check box. Otherwise, leave this check box unselected to include this MAC address.

7 Click **Add**.

Result: The address is added to the MAC Address Pool List.

8 If you wish to remove one or more MAC addresses from the MAC Address Pool List, follow these steps.

a. Place a check next to an address to be removed.

To select all MAC addresses, click **Select All**.

To remove all checkmarks, click **Unselect All**.

b. When you are ready to remove selected addresses from the list, click **Delete Selected**.

9 When you have completed modifying the MAC Address Pool List, click **Submit**.

Result: An information dialog box opens with the message **MAC address pool saved**.

10 Click **OK**.

Result: The MAC Address Pool page opens.

END OF STEPS

View/modify subnet policies

Purpose

To view or modify subnet-level policies.

Before you begin

A read-only user can only view subnet-level policies.

Procedure

To view or modify subnet-level policies, follow these steps.

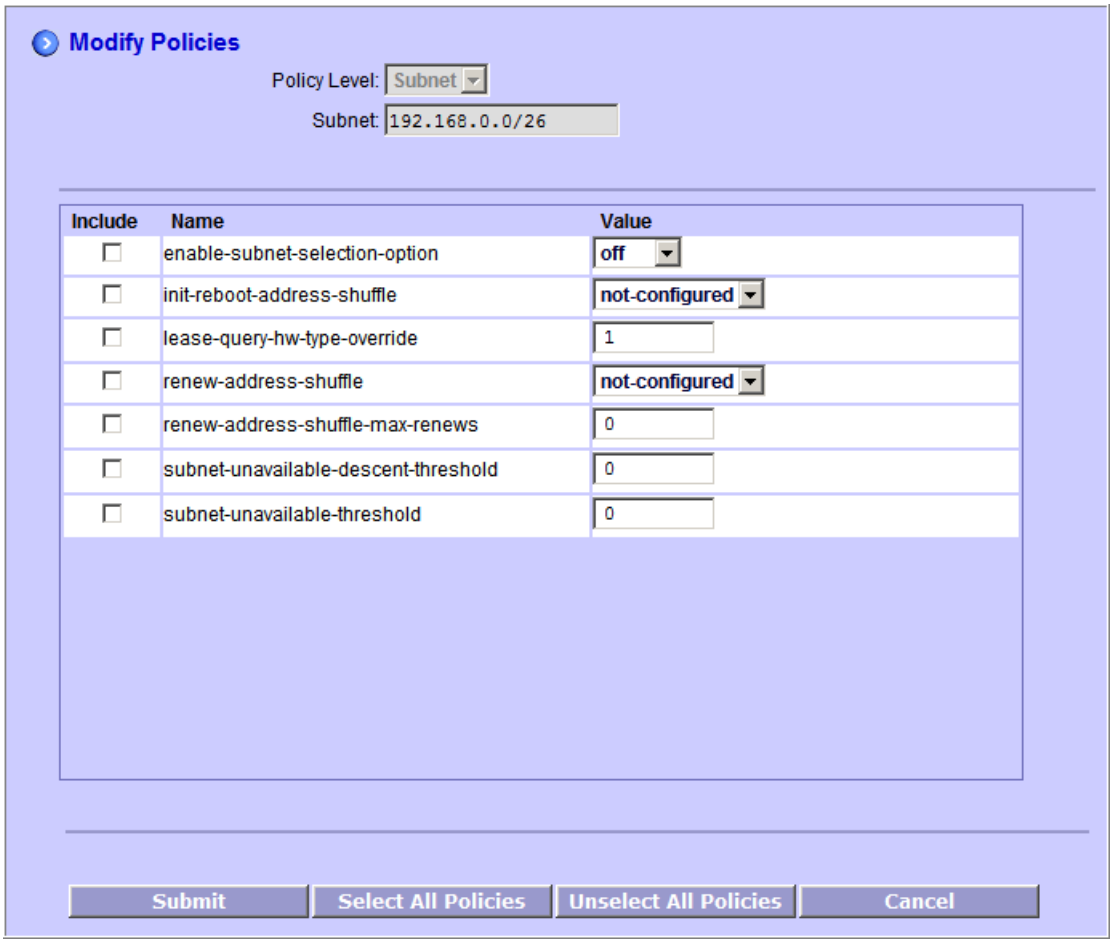
1. Expand the **DHCP Server ID** and the **Subnets** node.
2. Click on the subnet that contains the policies you want to view or modify.

   Result: The Subnet Properties page is displayed.
3. Click **Subnet Policies**.

Result: The Policies page opens. The policies that are currently enabled at the subnet level are displayed.

4 If you wish to modify an active policy or add a subnet-level policy, click **Modify**.

Result: The Modify Policies page opens.



5 Modify the subnet-level policies, as follows.

- Place a check in the checkbox next to a policy you wish to add. Only the checked policies are included in the subnet. As you make your changes, refer to the following table for information on each policy.
- To select every policy, click **Select All Policies**.
- Uncheck the checkbox beside a policy you wish to remove.
- To remove checkmarks from all policies, click **Unselect All Policies**.

Table 3-1 Subnet-level policies

Policy name	Values	Default value	Usage
enable-subnet-selection-option	off, client, lease, both	off	Restricts the use of the subnet selection option at two different levels. 'client' indicates that client requests from that subnet, containing the subnet selection option, will be honored. A policy value of 'lease' indicates that addresses may be requested from this subnet. A policy value of 'both' indicates that the subnet selection option can originate from clients on the subnet and that the subnet can be specified as the target subnet in the subnet selection option. **Note:** This policy is only available at the subnet policy level.
init-reboot-address-shuffle	not-configured, on, off	not-configured	Address shuffling occurs on init/reboot requests when set to On. If this option is set to Off, an address shuffle is not performed on init/reboot requests. This policy can be specified at the subnet and scope levels (listed in increasing order of precedence) using multiple policy templates. A policy value specified at a level with lower precedence will be overridden by a policy value with a higher precedence.
lease-query-hw-type-override	numeric	1	The hardware type (htype) parameter, to be included in the DHCPACK response to the lease query message. Refer to the Internet Assigned Numbers Authority (IANA) list of ARP hardware types in RFC 1700 for a complete list. Since the vast majority of installations are of the Ethernet type, a value of 1 is used by default, if there is no override configured for the subnet. **Note:** This policy is only available at the subnet policy level. It is a Lucent DHCP 5.5 server only policy.
renew-address-shuffle	not-configured, on, off	not-configured	Address shuffling occurs after the maximum renewals when set to On.

Policy name	Values	Default value	Usage
renew-address-shuffle-max-renews	numeric	0	The maximum number of lease renewals before forcing an address shuffle. This policy can be specified at the subnet and scope levels. If renew address shuffling is On at more than one level, applicable to a particular lease, with different maximum counts, the address shuffle occurs after the lesser of the maximum counts has been reached.
subnet-unavailable-descent-threshold	numeric	0	Specifies the percentage when an SNMP **dhcpServerSubnetThresholdDescent** trap is issued when addresses become available on a subnet. For example, if the value of this policy is set to 80, and the number of used addresses on the subnet falls below 80%, the SNMP trap is issued. If this value is set to 0, no **dhcpServerSubnetThresholdDescent** trap is issued for this subnet. If this value is not specified, the server level policy value, **DefaultDescentThreshold** is used. **Note:** This policy is only available at the subnet policy level.
subnet-unavailable-threshold	numeric	0	Specifies the percentage when an SNMP **dhcpServerSubnetThreshold Exceeded** trap is issued when addresses become unavailable on a subnet. For example, if the value of this policy is set to 80, and the number of used addresses on the subnet goes above 80%, the SNMP trap is issued. If this value is set to 0, no **dhcpServerSubnetThreshold Exceeded** trap is issued for this subnet. If this value is not specified, the server level policy value, **DefaultUnavailableThreshold** is used. **Note:** This policy is only available at the subnet policy level.

6 Click **Submit**.

Result: An information dialog box opens with the message **Policies saved**.

7 Click **OK**.

Result: The Policies page opens.

END OF STEPS

4 Scope operations

Overview

Purpose

This chapter describes how to manage scopes.

Contents

This chapter covers these topics.

Manage scopes

Overview

DHCP Configuration Manager supports the following scope-level operations:

- Add a scope
- View scope properties
- Modify a scope
- Delete a scope
- View/modify scope-level policies

Any changes made are not saved in the DHCP configuration file until explicitly saved or discarded. The **Server Actions** menu contains the **Save Changes** and **Discard Changes** sub-menus.

Add a scope

Purpose

To add a scope.

Procedure

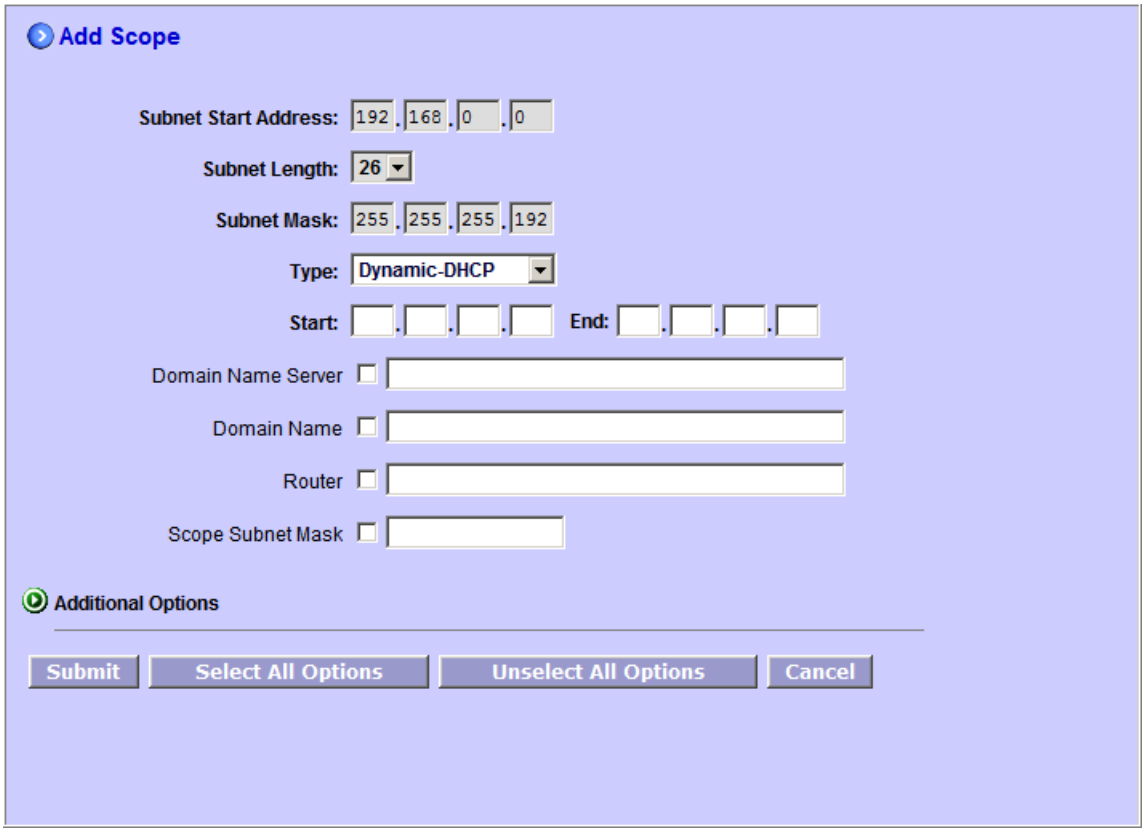
To add a scope, follow these steps.

1 In the DHCP Server hierarchy, expand the Subnets node and click on the subnet to which you want to add a scope.

Result: The Subnet Properties page is displayed.

2 Click **Add Scope**.

Result: The Add Scope page opens.



3 Define the scope type. Enter values in the fields, as described in the following table.

Table 4-1 Scope fields

Field	Description
Type	Dropdown list of the following scope types. • **Automatic-BOOTP** • **Automatic- DHCP** • **Dynamic-DHCP** • **Manual-BOOTP** • **Manual-DHCP** The default scope type is Dynamic-DHCP.
Start	***Dynamic scopes only.*** Start address of scope range in IPv4 address format.
End	***Dynamic scopes only.*** End address of scope range in IPv4 address format.
IP Address	***Manual scopes only.*** IP address of manual scope in IPv4 address format.
MAC Address	***Manual scopes only.*** MAC Address for manual scope.

4 Define the DHCP option parameters for the scope, as follows.

- Place a check in the checkbox next to each parameter that should be included in the scope. Only the checked option parameters are included in the scope. The most frequently used DHCP option parameters (**Domain Name Server**, **Domain Name**, **Router**, and **Scope Subnet Mask**) are listed first.
- The remainder of the Lucent DHCP 5.5 server option parameters are grouped by option categories. Click the Show Fields icon () to reveal parameters associated with a DHCP option.
- To select every parameter, click **Select All Options**. To remove checkmarks from all options, click **Unselect All Options**.

Refer to the following tables for descriptions of each DHCP option parameter.

5 When you have completed entering data for the DHCP option parameters you wish to define, click **Submit**.

Result: An information dialog box opens with the message **Scope saved**.

6 Click **OK**.

Result: The scope appears in the DHCP Server hierarchy and the Scope Properties page for the new scope opens.

END OF STEPS

Table 4-2 Frequently used DHCP options

Parameter	Description
Domain Name Server	A comma-separated list of the DNS name server IP addresses available. Servers should be listed in order of preference.
Domain Name	The domain name you wish to use to resolve hostnames via the Domain Name Service (DNS).
Router	A comma-separated list of router IPv4 addresses. Gateways should be listed in order of preference.
Scope Subnet Mask	A valid subnet mask for the scope.

Table 4-3 Application and Service Parameters

Parameter	Description
Broadcast and Multicast Control Service Address List	Lists server names that host the Broadcast and Multicast services that are specified as IPV4 addresses.
Broadcast and Multicast Control Service Domain List	Lists server names that host the Broadcast and Multicast services that are specified as domain names.
Default Finger Server	The Finger server option specifies a list of Finger servers available to the client. Servers should be listed in order of preference.
Default Internet Relay Chat (IRC) Server	The IRC server option specifies a list of IRC servers available to the client. Servers should be listed in order of preference.
Default World Wide Web (WWW) Server	The WWW server option specifies a list of WWW servers available to the client. Servers should be listed in order of preference.

Parameter	Description
Mobile IP Home Agent	This option specifies an IP address list indicating mobile IP home agents available to the client. Agents should be listed in order of preference.
NetBIOS over TCP/IP Datagram Distribution Server	The NetBIOS datagram distribution server (NBDD) option specifies a list of RFC 1001/1002 NBDD servers listed in order of preference.
NetBIOS over TCP/IP Name Server	The NetBIOS name server (NBNS) or WINS server option specifies a list of RFC 1001/1002 NBNS name servers listed in order of preference.
NetBIOS over TCP/IP Node Type	The NetBIOS node type option allows NetBIOS over TCP/IP clients, which are configurable as described in RFC 1001/1002. Enter the value that identifies the client type, as follows: ValueNode type **1**B-node **2**P-node **4**M-node **8**H-node
NetBIOS over TCP/IP Scope	The NetBIOS scope option specifies the NetBIOS over TCP/IP scope parameter for the client, as specified in RFC 1001/1002.
Network Information Servers	List the IP addresses (in order of preference) identifying the NIS (Network Information Service) servers available to the client.
Network Information Service Domain	Network Information Service (NIS) support is provided on SunOS 4.1x, Solaris 2.x and HP_UX10 only. Name the NIS domain. The domain is formatted as a character string from the NVT ASCII character set.
Network Information Service+ Domain	This option specifies the name of the client's NIS+ domain. The domain is formatted as a character string consisting of characters from the NVT ASCII character set.
Network Information Service+ Servers	This option specifies an IP address list indicating NIS+ servers available to the client. Servers should be listed in order of preference.
Network News Transport Protocol (NNTP) Server	The Network News Transport Protocol (NNTP) server option specifies a list of NNTP servers available to the client. Servers should be listed in order of preference.
Network Time Protocol Servers	List the IP addresses (in order of preference) indicating NTP (RFC 868) servers available to the client.

Parameter	Description
Post Office Protocol (POP3) Server	The POP3 server option specifies a list of POP3 servers available to the client. Servers should be listed in order of preference.
Simple Mail Transport Protocol (SMTP) Server	The SMTP server option specifies a list of SMTP servers available to the client. Servers should be listed in order of preference.
SIP Server Address/Domain List	Lists the SIP servers specified as IPV4 addresses or as domain names.
StreetTalk Directory Assistance (STDA) Server	The StreetTalk Directory Assistance (STDA) server option specifies a list of STDA servers available to the client. Servers should be listed in order of preference.
StreetTalk Server	The StreetTalk server option specifies a list of StreetTalk servers available to the client. Servers should be listed in order of preference.

Parameter	Description
Vendor Specific Information	This option is used by clients and servers to exchange vendor-specific information. The value for this option must be defined in hexadecimal format. The definition of this information is vendor specific. The vendor is indicated in the vendor class identifier option. Servers not equipped to interpret the vendor-specific information sent by a client MUST ignore it (although it may be reported). Clients that do not receive desired vendor-specific information should attempt to operate without it, although they may do so (and announce they are doing so) in a degraded mode. If a vendor potentially encodes more than one item of information in this option, the vendor should encode the option using "Encapsulated vendor-specific options", described as follows: The Encapsulated vendor-specific options field should be encoded as a sequence of code/length/value fields of identical syntax to the DHCP options field with the following exceptions: "Magic cookie" fields cannot be used. Codes other than 0 or 255 MAY be redefined by the vendor within the encapsulated vendor-specific extensions fields, but should conform to the tag-length-value syntax defined in section 2 (BOOTP Extension/DHCP Option Field Format) of RFC 2132. Code 255 (END), if present, signifies the end of the encapsulated vendor extensions, but not the end of the vendor extensions field. If no code 255 is present, the end of the vendor-specific information field is taken from its stated length. **Note:** If you require a sub-option format, refer to the note following this table.
X Window System Display Manager	This option specifies a IP address list of systems that are running the X Window System Display Manager and are available to the client.
X Window System Font Server	This option specifies a list of X Window System Font servers available to the client. Servers should be listed in order of preference.

Note: If you require a sub-option format in the Vendor Specific Information option, enter the data value as follows:

[0x0x0x…]

where '0x' specifies a 2-character hexadecimal representation of a byte. For example, a decimal value of 15 is represented in hexadecimal notation as **0f**, and the letter 'a' is

represented as **61**. Beginning and ending square brackets [ ] are required for the server to interpret the data as hexadecimal.

Let's suppose that a client requires two sub-options to be defined in this option tag (43). The first sub-option number is three, has a length of four, and its value is the IP address 198.200.138.254. The second sub-option number is 21, has a length of 10, and its value is a string of text "suboption2" (length 11 including a null terminator). Enter the following in the GUI:

```
[0304c6c88afe210b7375626f7074696f6e3200]
```

Given what is entered, the following should be generated in the *dhcpd.conf* file (located in the *%QDHCPCONFIG%* directory) for the manual object or dynamic range which contains the Template in which the option 43 tag is defined:

```
option vendor-specific [0304c6c88afe210b7375626f7074696f6e3200]
```

Reads:

`03` First sub-option, option 3

`04` Length of 4 octets

`c6c88afe`IP address 198.200.138.254 in hex

`21` Second sub-option

`0b` Length of 11 octets

`7375626f7074696f6e3200`"suboption2" in hex, null terminated

Table 4-4 DHCP Extensions

Parameter	Description
Bootfile Name	This option is used to identify a bootfile when the file field in the DHCP header has been used for DHCP options.
Client Identifier	This option is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain. DHCP servers should treat identifiers as opaque. The client identifier may consist of type-value pairs. For instance, it may consist of a hardware type and hardware address. In this case, the type field should be one of the Address Resolution Protocol (ARP) hardware types defined in RFC 1700. A hardware type of 0 (zero) should be used when the value field contains an identifier other than a hardware address (for instance, a fully qualified domain name). Each client's client-identifier must be unique among the client-identifiers used on the subnet to which the client is attached. Vendors and system administrators are responsible for choosing client-identifiers that meet this requirement for uniqueness.

Parameter	Description
IP Address Lease Time	This option is used in a client request (DHCPDISCOVER or DHCPREQUEST) to allow the client to request a lease time for the IP address. In a server reply (DHCPOFFER), a DHCP server uses this option to specify the lease time it is willing to offer. Enter default value of **4294967295** for unlimited lease time. For limited lease time, enter any lower value in seconds.
Option Overload	This option is used to indicate that the DHCP sname or file fields are being overloaded by using them to carry DHCP options. A DHCP server inserts this option if the returned parameters exceed the usual space allotted for options. If this option is present, the client interprets the specified additional fields after it concludes interpretation of the standard option fields. Legal values for this option are as follows: 1) The file field is used to hold options; 2) The sname field is used to hold options; 3) Both fields are used to hold options
Rebinding (T2) Time	This option specifies the time interval from address assignment until the client transitions to the rebinding state. You can enter up to 999,999,999 seconds.
Renewal (T1) Time	This option specifies the time interval from address assignment until the client transitions to the renewing state. You can enter up to 999,999,999 seconds.
TFTP Server Name	This option is used to identify a Trivial File Transfer Protocol (TFTP) server when the sname field in the DHCP header has been used for DHCP options.

Table 4-5 IP Layer Parameters per Host

Parameter	Description
Default IP Time-to-Live	Enter the default time-to-live (in seconds) to use on outgoing datagrams as an octet between 1 and 255, inclusive.
IP Forwarding Enable/Disable	Selecting True allows you to configure the IP layer to enable packet forwarding. False disables packet-forwarding.
Maximum Datagram Reassembly Size	Enter the maximum reassembly size of the datagram. Enter a value between 576 and 65,535.
Non-Local Source Routing Enable/Disable	Selecting True allows you to configure the IP layer to allow forwarding of datagrams with non-local source routes. False disables forwarding of the datagrams.

Parameter	Description
Path MTU Aging Timeout	Enter the timeout for aging Path Maximum Transmit Unit (MTU) values discovered by the mechanism defined in RFC 1191. The timeout is in seconds, from 0 to 2,147,483,647.
Path MTU Plateau Table	Identify a table of MTU sizes to use when performing Path MTU Discovery as defined in RFC 1191. The table should be formatted as a list, with a minimum value of 68 and a maximum value of 65,535.
Policy Filter	This option specifies policy filters for non-local source routing. The filters consist of an IP address list and masks, which specify destination/mask pairs with which to filter incoming source routes. The client should discard any source-routed datagram whose next-hop address does not match one of the filters.

Table 4-6 IP Layer Parameters per Interface

Parameter	Description
All Subnets are Local	This selection defines whether all subnets of the IP network to which the user is connected use the same MTU (maximum transmit unit) as the subnet of the network to which the user is directly connected. True indicates all subnets share the same MTU, and false assumes that some of the subnets connected may have smaller MTUs.
Broadcast Address	Enter the broadcast address in use on the client's subnet.
Classless Static Route	Specify one or more static routes, each of which consists of a destination descriptor (the subnet address and subnet mask) and the IP address of the router that should be used to reach that destination.
Interface MTU	Enter the Maximum Transmit Unit (MTU) you want to use on this interface. MTU is the frame size in a TCP/IP network. Enter a value from 68 to 65,535.
Mask Supplier	Selecting True indicates response to the subnet mask request should use Internet Control Message Protocol (ICMP). Selecting False indicates the subnet mask should not respond using ICMP.
Perform Mask Discovery	Selecting True establishes that the client should perform subnet mask discovery. Selecting False indicates no mask discovery should be performed.
Perform Router Discovery	Selecting True allows router discovery to be performed as defined in RFC 1256. Selecting False indicates no router discovery to be performed.

Parameter	Description
Router Solicitation Address	Name the IP address where router solicitation requests should be transmitted.
Static Route	Specify the list of static routes that the client should install in its routing cache. If multiple routes to the same destination are specified, they are listed in descending order of priority. The routes consist of a list of IP address pairs. The first address is the router for the destination. The default route (0.0.0.0) is an illegal destination for a static route.

Table 4-7 Link Layer Parameters per Interface

Parameter	Description
ARP Cache Timeout	Enter the time-out in seconds for ARP cache entries, from 0 to 2,147,483,647.
Ethernet Encapsulation	Use this option to identify the use of Ethernet Version 2 (RFC 894) or IEEE 802.3 (RFC 1042) encapsulation, if the interface is Ethernet. Select True to use RFC 1042 encapsulation Select False to use RFC 894 encapsulation.
Trailer Encapsulation	Select True to identify whether the client should negotiate the use of trailers (RFC 893) when using the Address Resolution Protocol (ARP) protocol. Select False to deter the use of trailers.

Table 4-8 Novell Options

Parameter	Description
NDS Context	This option specifies the initial NDS context the client should use. You can enter up to 255 characters.
NDS Servers	This option specifies one or more NDS servers for the client to contact for access to the NDS database. Servers should be listed in order of preference.
NDS Tree Name	This option specifies the name of the NDS tree the client will be contacting. You can enter up to 255 characters.
Netware/IP Domain Name	This option code is used to convey the NetWare/IP domain name used by the NetWare/IP product. The NetWare/IP Domain in the option is a Network Virtual Terminal (NVT) ASCII text string. You can enter up to 255 characters.

Parameter	Description
Netware/IP Information	The NetWare/IP option code is used to convey all the NetWare/IP related information except for the NetWare/IP domain name. A number of NetWare/IP sub-options can be conveyed. Refer to **RFC 2242** to determine the values required to enter sub-options. A sample converted value for the sub-option NWIP_DOES_NOT_EXIST, for example, is [0100].

Table 4-9 Packet Cable Options

Parameter	Description
CableLabs Client Config (122)	Refer to **RFC 3495** to determine the values required to enter all sub-options combined into one option. A sample converted value for all the sub-options is: [01040a00000102040a0000030305010a000002040c000000320000006400000001050c000000320000006400000001060a08544553544e414d4500070101080164] which corresponds to the following sub-options: TSP's Primary DHCP Server Address=**10.0.0.1** TSP's Secondary DHCP Server Address=**10.0.0.3** TSP's Provisioning Server Address=**10.0.0.2** TSP's AS-REQ/AS-REP Backoff and Retry – Maximum Retry =**1** – Maximum Timeout=**100** – Nominal Timeout=**50** TSP's AP-REQ/AP-REP Backoff and Retry – Maximum Retry =**1** – Maximum Timeout=**100** – Nominal Timeout=**50** TSP's Kerberos Realm Name=**testName** TSP's Ticket Granting Server Utilization=**True** TSP's Provisioning Timer Value=**100**

Table 4-10 RFC 1497 Vendor Extensions

Parameter	Description
Boot File Size	Enter the length of the client's default boot image. The maximum file length is 65,535 bytes.

Parameter	Description
Cookie Server	Enter the IP address of the RFC 865 cookie server available to the client.
Extensions Path	Enter a text string to specify a file, retrievable via Trivial File Transfer Protocol (TFTP), which contains information that can be interpreted in the same way as the 64-octet vendor-extension field within the BOOTP response, with the following exceptions: • the length of the file is unconstrained • all references to Tag 18 (for example, instances of the BOOTP Extensions Path field) within the file are ignored
Host Name	Enter the name of the client. If you define the host name in an option template, it overrides any definition in the Object Profile.
Impress Server	Enter the IP address of the Imagen Impress server available to the client.
Log Server	Enter the IP address of the MIT-LCS UDP log server available to the client.
LPR Server	Enter the IP address of the RFC 1179 line printer server available to the client.
Merit Dump File	Enter the pathname of the file where you wish the core image to be dumped in the occurrence of a crash. The path is formatted as a character string consisting of characters from the Network Virtual Terminal (NVT) ASCII character set.
Name Server	Enter the IP address of the IEN-116 name server available to the client.
Resource Location Server	Enter the IP address of the RFC 887 Resource Location server available to the client.
Root Path	Enter the pathname that contains the client's root directory or partition. The path is formatted as an NVT ASCII character string.
Swap Server	Enter the IP address of the client's swap server.
Time Offset	Specify the offset of the client's subnet (in seconds) from Coordinated Universal Time (also referred to as UTC). A positive offset indicates a location east of the zero meridian and a negative offset indicates a location west of the zero meridian. For example, to enter a time offset for a client subnet located in the Eastern Standard Timezone (5 hours west of the UTC zero meridian), you would enter -18000.
Time Server	Enter the IP address of the RFC 868 time server available to the client.

Table 4-11 RFC 2563 Options

Parameter	Description
Auto Configuration of IPv4 Clients	This option code is used to ask whether, and be notified if, auto-configuration should be disabled on the local subnet. When a server responds with the value “AutoConfigure” (True), the client ***may*** generate a link-local IP address if appropriate. However, if the server responds with “DoNotAutoConfigure” (False), the client ***must not*** generate a link-local IP address, possibly leaving it with no IP address.

Table 4-12 RFC 3397 Option

Parameter	Description
Domain Search Option	Passes the domains in the comma-separated list from the DHCP Server to the DHCP Client to use when resolving hostnames using DNS.

Table 4-13 SLP Protocol Options

Parameter	Description
SLP Directory Agent	This option specifies the location of one or more SLP Directory Agents. For further information, refer to **RFC 2610** to determine how to convert the value. A sample converted value is [010a000001], which corresponds to an address of **`10.0.0.1`** for the Directory Agent Address sub-option, and a setting of True for the Mandatory sub-option.
SLP Service Scope	This option indicates the scopes that a SLP Agent is configured to use. For further information, refer to **RFC 2610** to determine how to convert the value. A sample converted value is [0173636f7065312c73636f706532], which corresponds to **`scope1,scope2`** for the Scope List sub-option, and a setting of True for the Mandatory sub-option.

Table 4-14 TCP Parameters

Parameter	Description
TCP Default TTL	This option defines the default time-to-live (in seconds) to use when sending TCP segments. Enter a value from 1 to 255.
TCP Keepalive Garbage	This option specifies if the TCP keep alive messages should be sent with a garbage octet for compatibility with older implementations. Selecting True enables a garbage octet to be sent. Selecting False does not allow a garbage octet to be sent.

Parameter	Description
TCP Keepalive Interval	Indicate the amount of time, specified in seconds, to wait before sending a keep alive message on a TCP connection. A value of 0 indicates keep alive messages on connections should not be generated unless specifically requested to do so by an application. Enter a value from 0 to 2,147,483,647.

Table 4-15 User Authentication Protocol Options

Parameter	Description
User Authentication Protocol	This option specifies a list of Uniform Resource Locators (URLs), each pointing to a user authentication service that is capable of processing authentication requests encapsulated in the UAP. UAP servers can accept either HTTP 1.1 or SSLv3 connections. If the list includes a URL that does not contain a port component, the normal default port is assumed (that is, port 80 for **`http`** and port 443 for **`https`**). If the list includes a URL that does not contain a path component, the path **`/uap`** is assumed.

View scope properties

Purpose

To view the properties of a scope.

Procedure

To view the properties of a scope, follow these steps.

1. Click on the Expand icon (⊞) next to the DHCP server in the hierarchy.

   Result: The Subnets node opens.

2. Expand the Subnets node.

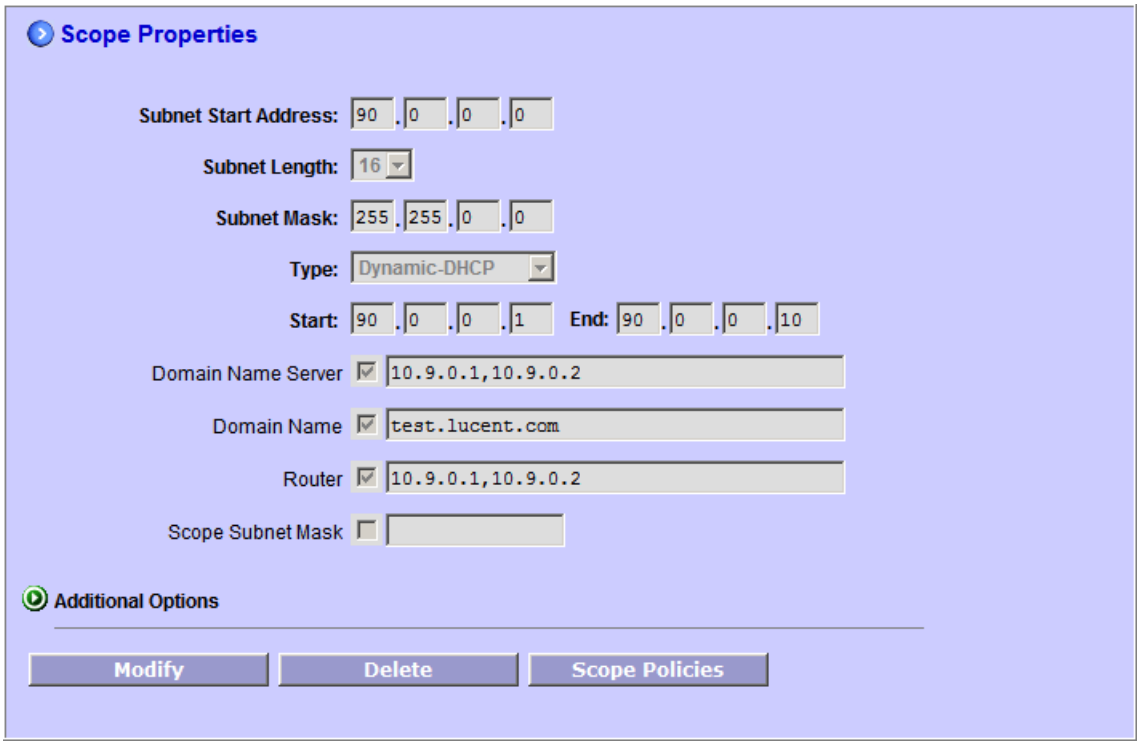
   Result: A list of subnet addresses opens in the hierarchy.

3. Click on the Expand icon (⊞) next to the subnet that contains the scope you wish to view.

   Result: A list of previously defined scope addresses opens in the hierarchy.

4. Click on the scope you wish to view.

Result: The Scope Properties page opens.



Note: Scope-level policies cannot be assigned to manual scopes. The **Scope Policies** button is not displayed if the scope **Type** field is Manual-BOOTP or Manual-DHCP.

5 Choose one of the following actions.

If you want to...	Then ...
Modify the scope properties	Click **Modify**. For more information, refer to "Modify scope properties" (p. 4-19). **Note:** This function is not available to read-only users.
Delete the scope	Click **Delete**. For more information, refer to "Delete a scope" (p. 4-22). **Note:** This function is not available to read-only users.
View or modify scope-level policies	Click **Scope Policies**. For more information, refer to "View/modify scope policies" (p. 4-23). **Note:** Read-only users cannot view scope-level policies.

END OF STEPS

Modify scope properties

Purpose

To modify the properties of a scope.

Before you begin

- You cannot modify a scope address type or its range. If a scope is incorrectly defined, delete it and then add a new scope with the address type and range you prefer.
- Read-only users can only view scope-level properties.

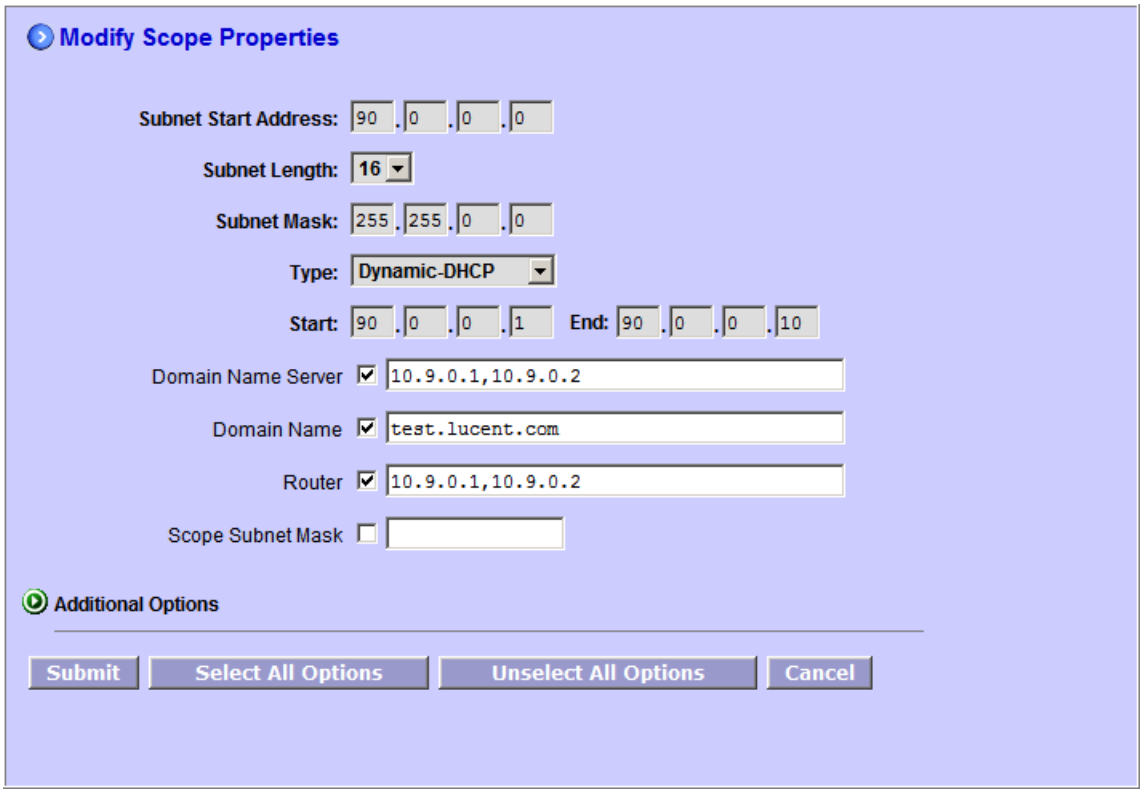
Procedure

To modify a scope's properties, follow these steps.

1. Expand the DHCP Server hierarchy until the scope you want to modify is displayed.
2. Click on the scope.

   Result: The Scope Properties page opens.
3. Click **Modify**.

Result: The Modify Scope Properties page opens.



4 Modify the DHCP option parameters for the scope, as follows.

- To add a parameter, use the Show Fields icon ( ) to reveal parameters associated with the DHCP option that you wish to add and place a check in the checkbox next to it. Only the checked option parameters are included in the scope.
- To select every parameter, click **Select All Options**.
- To remove a parameter, locate the DHCP option containing the parameter and uncheck the checkbox beside it.
- To remove checkmarks from all options, click **Unselect All Options**.

Refer to the tables in "Add a scope" (p. 4-3) for descriptions of each DHCP option parameter.

5 Click **Submit**.

Result: An information dialog box opens with the message **Scope saved**.

6 Click **OK**.

Result: The scope appears in the DHCP Server hierarchy and the Scope Properties page reopens.

END OF STEPS

Delete a scope

Purpose

To delete a scope.

Procedure

To delete a scope, follow these steps.

1 Expand the **DHCP Server ID** and the **Subnets** node.

2 Expand the subnet that contains the scope you want to delete.

Result: The Scope Properties page is displayed.

3 Click **Delete**.

Result: A confirmation dialog box opens with the message **You are about to delete scop**e.

4 Click **OK** to confirm (or **Cancel** to abort).

Result: An information dialog box opens with the message **Scope deleted**.

5 Click **OK**.

Result: The scope is removed from the DHCP Server hierarchy.

END OF STEPS

View/modify scope policies

Purpose

To view or modify scope-level policies.

Before you begin

Read-only users cannot view scope-level policies.

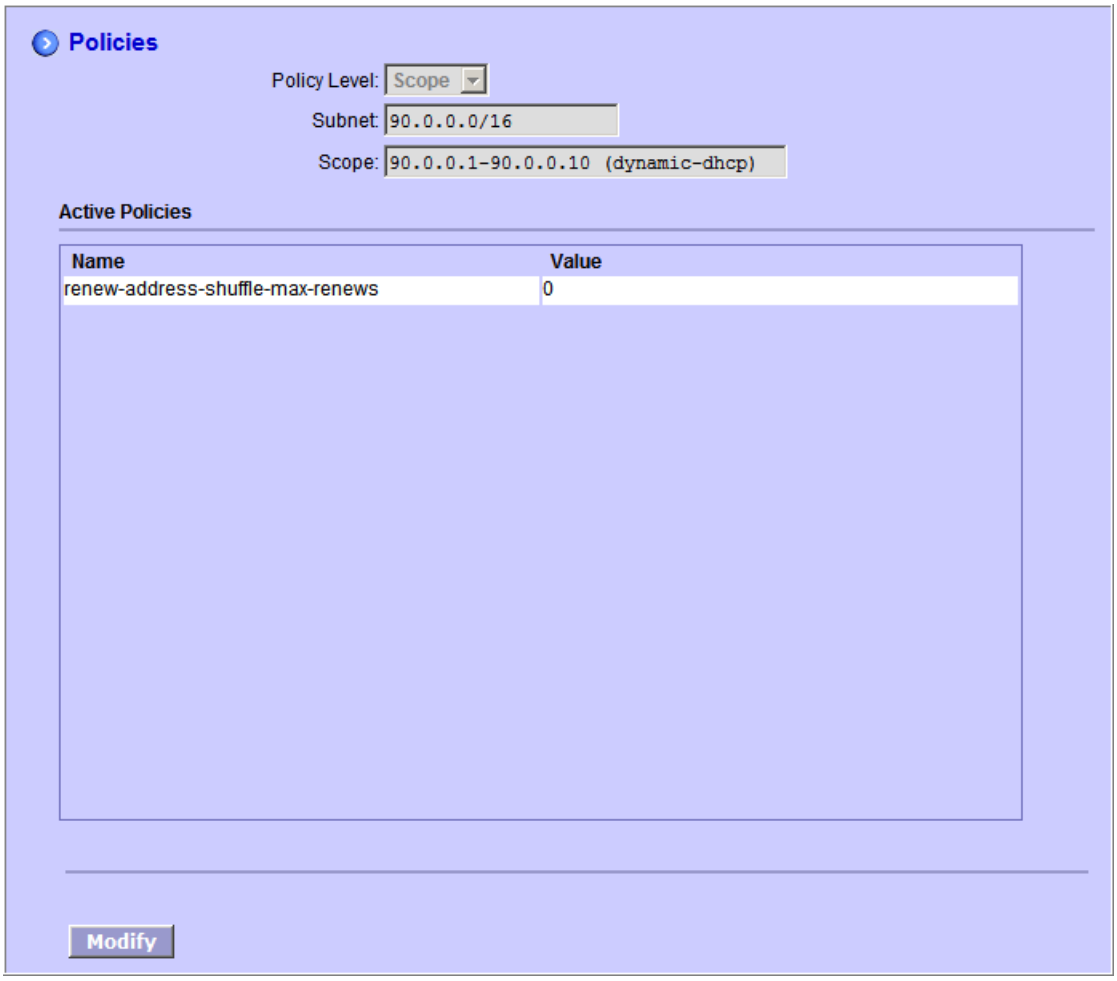
Procedure

To view or modify scope-level policies, follow these steps.

1. Expand the **DHCP Server ID** and the **Subnets** node.
2. Expand the subnet that contains the scope whose policies you want to view or modify.

   Result: The Scope Properties page is displayed.
3. Click **Scope Policies**.

Result: The Policies page opens. The policies that are currently enabled at the scope level are displayed.



4 If you wish to modify an active policy or add another scope-level policy, click **Modify**.

Result: The Modify Policies page opens.

5 Modify the scope-level policies, as follows.

- Place a check in the checkbox next to a policy you wish to add. Only the checked policies are included in the scope. As you make your changes, refer to the following table for information on each policy.
- To select every policy, click **Select All Policies**.
- Uncheck the checkbox beside a policy you wish to remove.
- To remove checkmarks from all policies, click **Unselect All Policies**.

6 Click **Submit**.

Result: An information dialog box opens with the message **Policies saved**.

7 Click **OK**.

Result: The Policies page opens.

END OF STEPS

Table 4-16 Scope-level policies

Policy name	Values	Default value	Usage
excluded-user-classes	string	none	Specifies the DHCP client user class values that will be excluded from receiving a lease on the particular address range or scope to which this policy is assigned. Multiple values can be specified and a trailing wildcard asterisk (*) is supported. **Note:** This policy is only available at the scope policy level.
excluded-vendor-classes	string	none	Specifies the DHCP client vendor class values that will be excluded from receiving a lease on the particular address range or scope to which this policy is assigned. Multiple values can be specified and a trailing wildcard asterisk (*) is supported. **Note:** This policy is only available at the scope policy level.
init-reboot-address-shuffle	not-configured, on, off	not-configured	Address shuffling occurs on init/reboot requests when set to On. If this option is set to Off, an address shuffle is not performed on init/reboot requests. This policy can be specified at the subnet and scope levels (listed in increasing order of precedence) using multiple policy templates. A policy value specified at a level with lower precedence will be overridden by a policy value with a higher precedence.
renew-address-shuffle	not-configured, on, off	not-configured	Address shuffling occurs after the maximum renewals when set to On.

Policy name	Values	Default value	Usage
renew-address-shuffle-max-renews	numeric	0	The maximum number of lease renewals before forcing an address shuffle. This policy can be specified at the subnet and scope levels. If renew address shuffling is On at more than one level, applicable to a particular lease, with different maximum counts, the address shuffle occurs after the lesser of the maximum counts has been reached.

5 DHCP server configuration files

Overview

Purpose

This chapter describes how to manage configuration and policy files on a DHCP server.

Contents

This chapter covers these topics.

Manage DHCP server files

Overview

DHCP Configuration Manager allows viewing and editing of the DHCP Server configuration file (*dhcpd.conf*) and policy file (*dhcpd.pcy*).

Both View and Modify Configuration File pages read files directly from disk. If there are any unsaved changes, users are notified when they try to view the running configuration file. If they then attempt to modify the file, they are offered the choice of saving or discarding those changes. If users choose to save the edits, edits are committed to DHCP files before proceeding with the modify file request. If users choose to discard the changes, pending edits are discarded before proceeding with the modify file request.

The following functions are available for working with DHCP server files.

- View/modify configuration file
- Download configuration file
- View/modify policy file
- Download policy file

View/modify DHCP server configuration file

Purpose

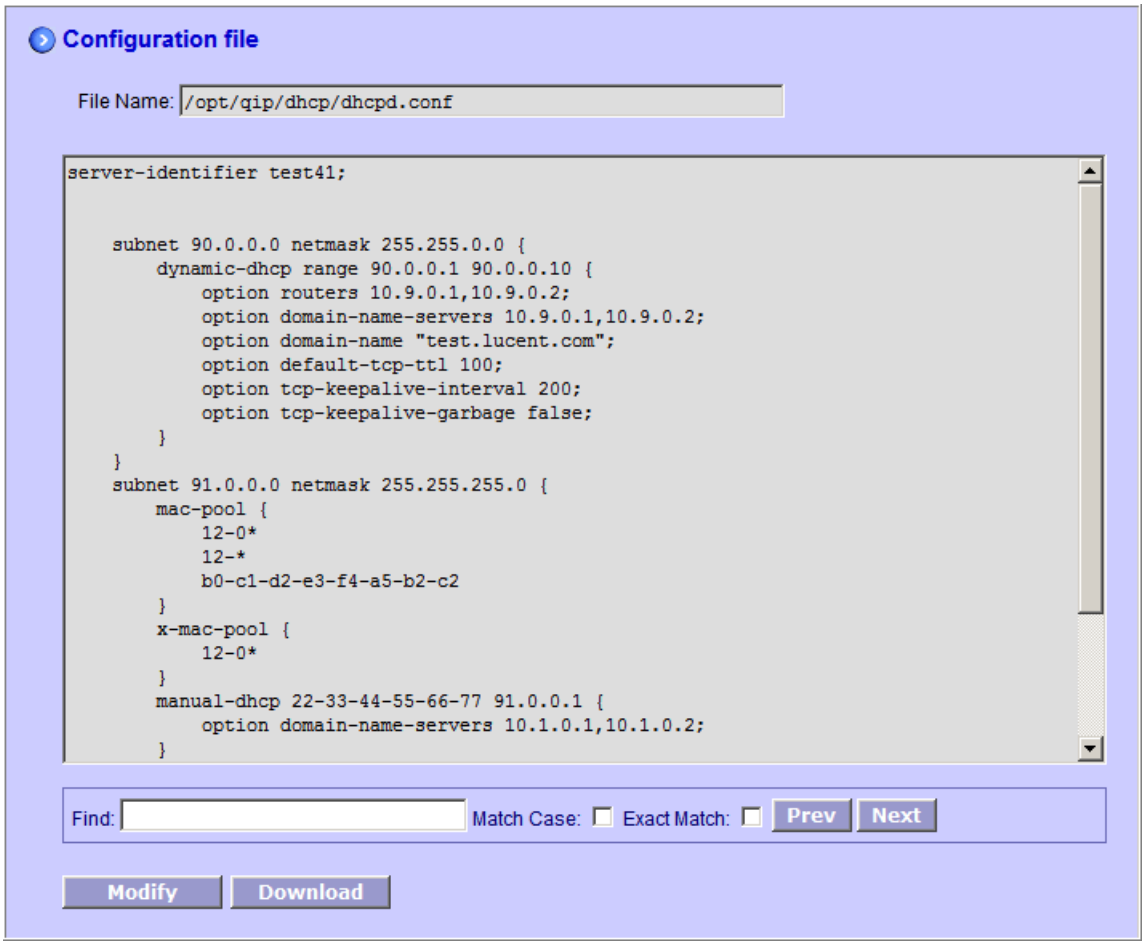
To view or modify the content of the DHCP server configuration file (*dhcpd.conf*).

Procedure

To view or modify the DHCP server configuration file, follow these steps.

1 Select **View Configuration File** from the **DHCP Server Configuration** menu, or click the View *dhcpd.conf* File icon ( ).

Result: The Configuration file page opens.



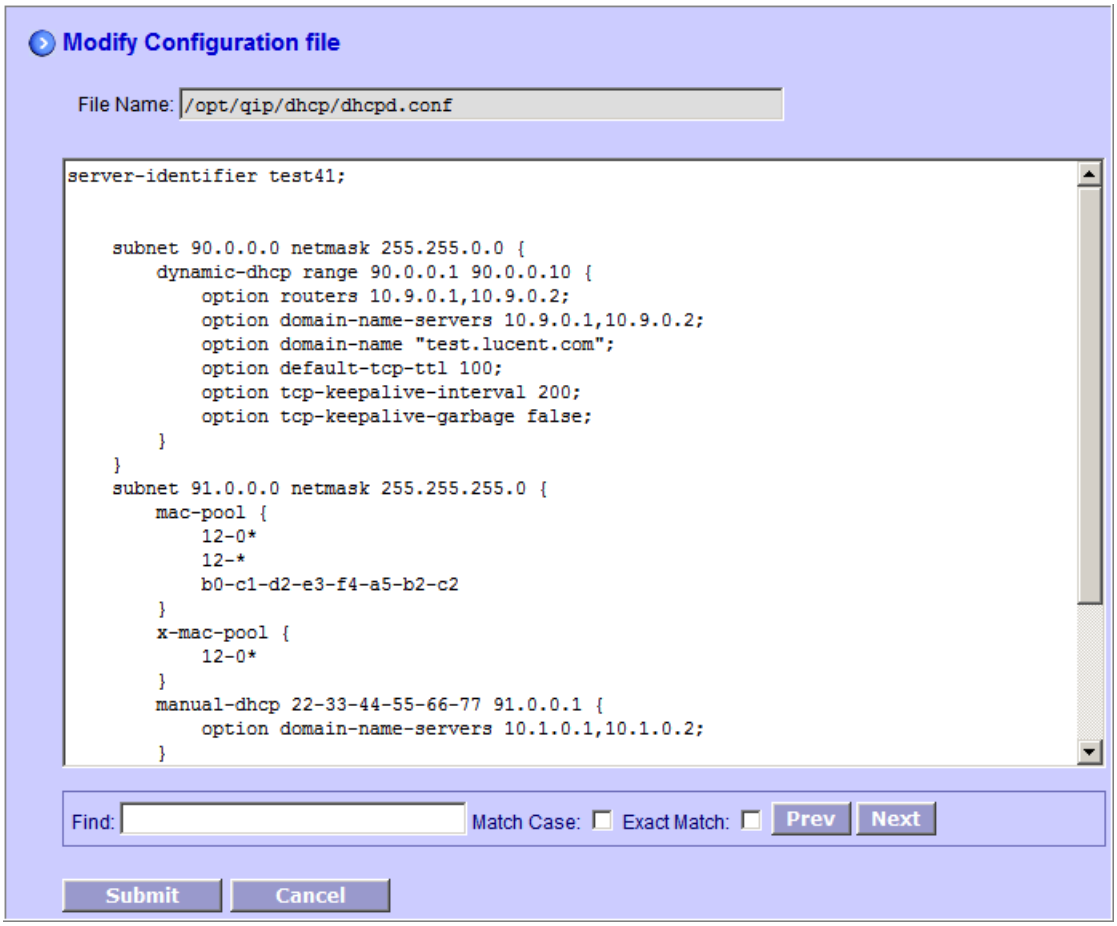
2 To locate an alphanumeric string in the file, enter the string in the **Find** field. To refine the search criteria, check the following checkboxes as needed.

- To find or ignore an item with specific capitalization, select or turn off **Match Case**.
- To match a string exactly, enter the string in the **Find** field and select **Exact Match**.

Click **Next** to find the next instance of the search string or click **Prev** to find the previous instance.

3 To modify the configuration file, click **Modify**.

Result: The Modify Configuration file page opens.



4 Make changes as needed. You can scroll through the file or use the Find feature to locate items you wish to edit.

5 To save your edits, click **Submit**.

Result: An information dialog box opens with the message **File saved**.

6 Click **OK**.

Result: The Configuration file page opens.

END OF STEPS

Download a configuration file

Purpose

To download a DHCP server configuration file.

Procedure

To download a configuration file, follow these steps.

1 Select **View Configuration File** from the **DHCP Server Configuration** menu, or click the View *dhcpd.conf* File icon ().

Result: The Configuration file page opens.

2 Click **Download**.

Result: Your default browser opens a dialog box.

3 Either open the file in a text editor or save it on your computer.

END OF STEPS

View/modify DHCP server policy file

Purpose

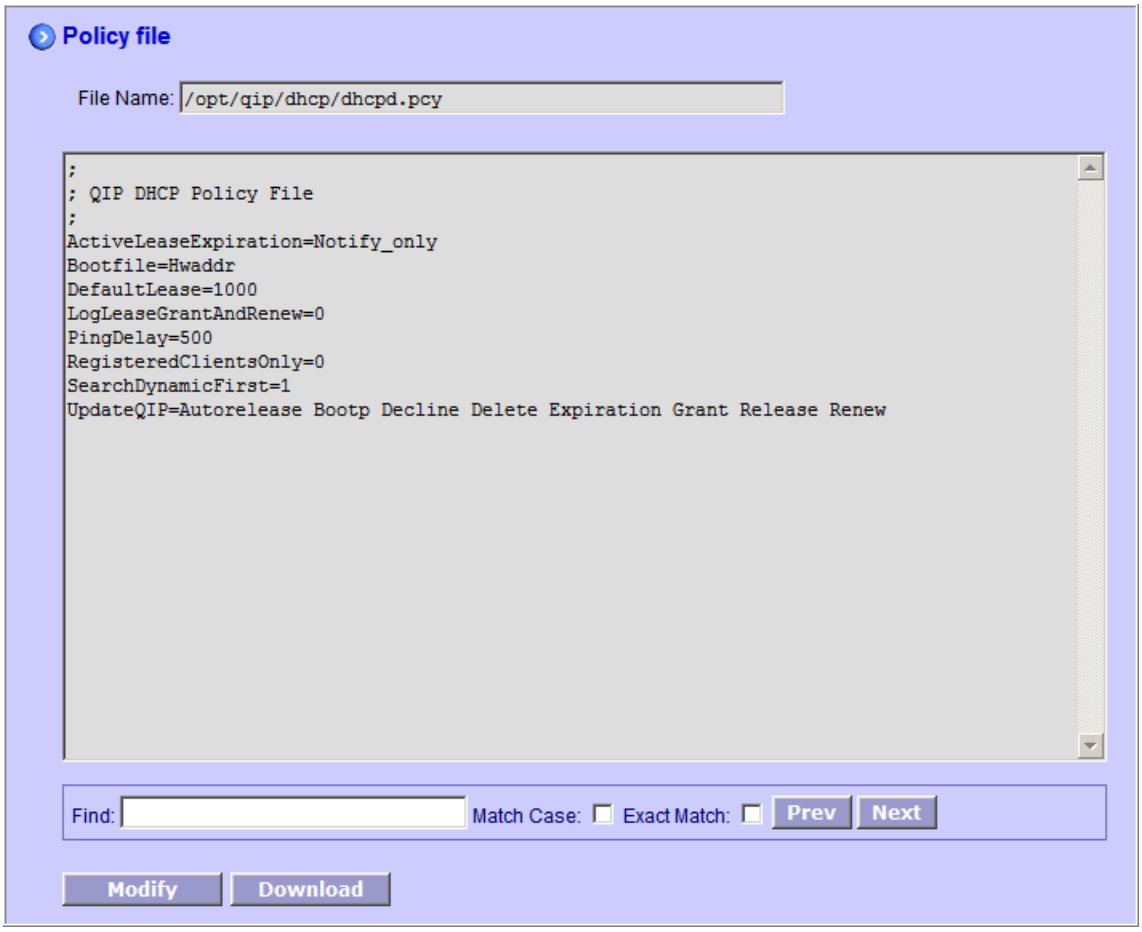
To view or modify a DHCP server policy file (*dhcpd.pcy*).

Procedure

To view or modify a DHCP server policy file, follow these steps.

1 Select **View Policy File** from the **DHCP Server Configuration** menu, or click the View *dhcpd.pcy* File icon ( ).

Result: The Policy file page opens.



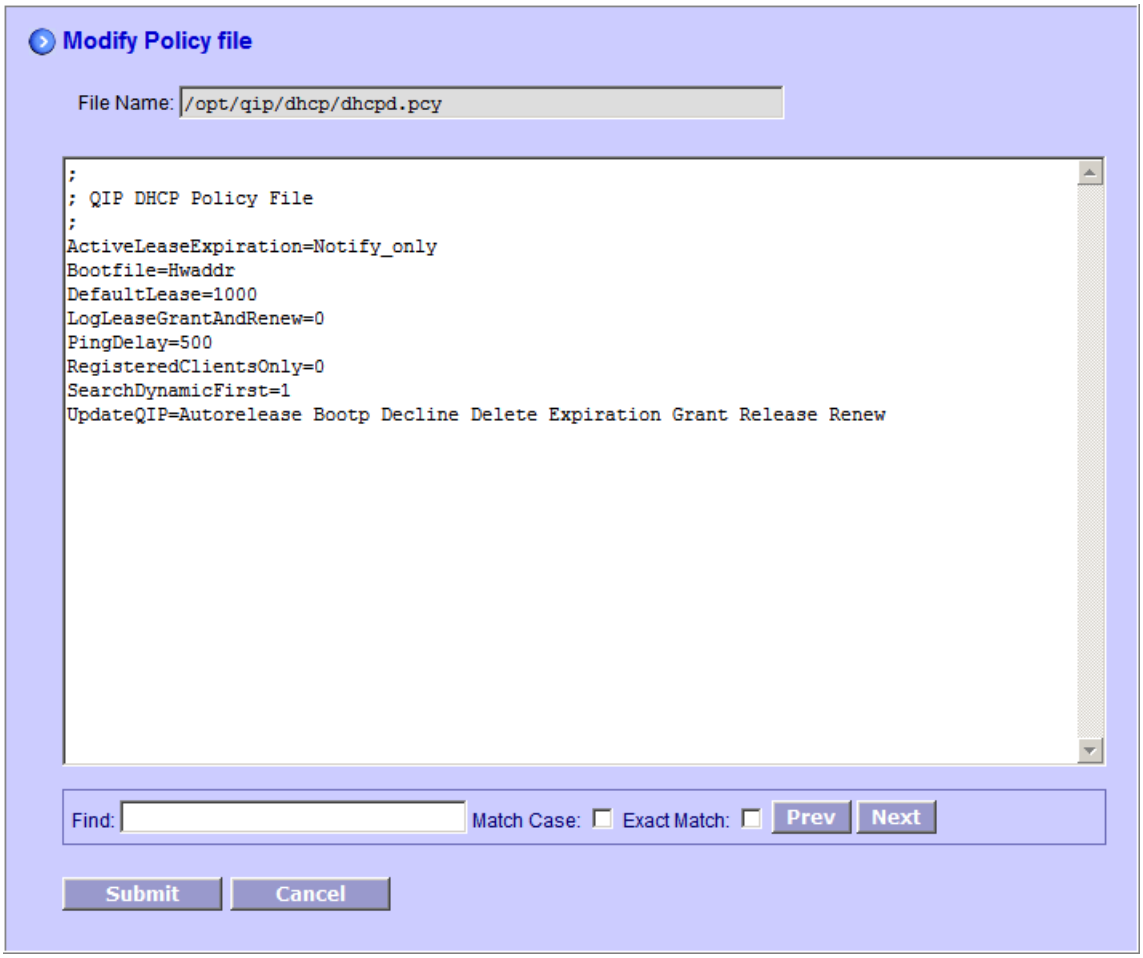
2 To locate an alphanumeric string in the file, enter the string in the **Find** field. To refine the search criteria, check the following checkboxes as needed.

- To find or ignore an item with specific capitalization, select or turn off **Match Case**.
- To match a string exactly, enter the string in the **Find** field and select **Exact Match**.

Click **Next** to find the next instance of the search string or click **Prev** to find the previous instance.

3 To modify the policy file, click **Modify**.

Result: The Modify Policy file page opens.



4 Make changes as needed. You can scroll through the file or use the Find feature to locate items you wish to edit.

5 To save your edits, click **Submit**.

Result: An information dialog box opens with the message **File saved**.

6 Click **OK**.

Result: The Policy file page opens.

END OF STEPS

Download a DHCP server policy file

Purpose

To download a DHCP server policy file (*dhcpd.pcy*).

Procedure

To download a policy file, follow these steps.

1 Select **View Policy File** from the **DHCP Server Configuration** menu, or click the View *dhcpd.pcy* File icon ().

Result: The Policy file page opens.

2 Click **Download**.

Result: Your default browser opens a dialog box.

3 Either open the file in a text editor or save it on your computer.

END OF STEPS

A Configuring DHCP Configuration Manager

Overview

Purpose

This appendix describes how to customize the behavior of DHCP Configuration Manager and the web server.

Contents

This appendix covers these topics.

DHCP Configuration Manager configuration

Overview

Both DHCP Configuration Manager and the DHCP Configuration Manager web server come with property files that control how each product behaves.

If you wish to modify properties of DHCP Configuration Manager or the DHCP Configuration Manager web server, Alcatel-Lucent recommends that these files be modified in the Appliance Management Software (AMS) UI so that you can ensure that any changes you make to these files do not get overwritten the next time the DHCP Configuration Manager package is deployed on an appliance.

The property files are as follows:

- DHCP Configuration Manager:*conf/qdhcpmgr.properties*
- DHCP Configuration Manager web server:*conf/qdhcp_httpd.conf*

Properties that you can customize are described in the following pages.

qdhcpmgr.properties

Overview

The following properties are available for DHCP Configuration Manager. All lines beginning with # character are ignored.

Properties must be specified in the `property=value` format. For example:

```
logfile= /opt/qdhcpmgr/log/qdhcp_manager.log
```

logfile

Description: Absolute path of the file to log DHCP Configuration Manager log messages.

Values: Default: */opt/qdhcpmgr/log/qdhcp_manager.log*

loglevel

Description: Defines log level for DHCP Configuration Manager application.

1=log errors and critical actions such as user login/logout, DHCP server start/stop

5=debug

Default: 1

Values: Allowed: 1 or 5

session_inactivity_timeout

Description: Defines how long a session can be idle before it expires. If session is kept idle longer than session_inactivity_timeout interval, the session is automatically terminated and any pending changes are lost. The value is in seconds. This value cannot be greater than 86400, which is equivalent to 1 day.

Default: 3600 (in seconds)

Values: Allowed: 1 - 86400

allow_sixteen_chars_mac_addr

Description: Controls whether to allow sixteen characters MAC Addresses in subnet level MAC Pool. If set to true, sixteen characters MAC addresses are allowed. Otherwise only twelve characters MAC addresses are allowed in subnet level MAC pool.

Default: true

Values: Allowed: true or false.

qdhcp_httpd.conf

Overview

The following properties are available for the DHCP web server. All lines beginning with # character are ignored.

port

Description: Defines port DHCP Configuration Manager web server listens on.

Default: 8067

Values: Allowed: Any port not used by any other application on appliance.

ssl

Description: Indicates to deploy DHCP Configuration Manager in SSL mode. If this property is present, DHCP Configuration Manager will be deployed in SSL mode; otherwise, it is deployed in non-SSL mode.

Default: Commented out to deploy in non-SSL mode.

Values: Allowed: Property is present or not present

certfile

Description: Indicates from which file to read the certificate when DHCP Configuration Manager is deployed in SSL mode.

Default: Commented out

Values: Allowed: Absolute path of certificate file.

nochroot

Description: Do not run in chroot mode. If present, DHCP Configuration Manager web server runs in chroot mode.

Default: Do not run in chroot mode.

Values: Allowed: Commented out or present.

dir

Description: Defined working directory of DHCP Configuration Manager web server.

Default: */opt/qdhcpmgr/web*

Values: Allowed: Web directory of DHCP Configuration Manager.

logfile

Description: Log file used by DHCP Configuration Manager web server to log web server activities.

Default: */opt/qdhcpmgr/log/qdhcp_httpd.log*

Values: Allowed: Absolute path and filename to be written.

Index