VitalQIP® DNS/DHCP & IP Management Software

VitalQIP® (QIP) | Release 7.2

Web Client User's Guide

190-409-079R7.2
July 2009
Issue 5

Trademarks

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

14 Zones

15 DNS Views

20 DHCP policies and templates

List of tables

About this document

Purpose

Welcome to VitalQIP® – a powerful IP name and address management tool. VitalQIP simplifies the assignment and allocation of IP addresses and services, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS). This product is a comprehensive collection of management tools and user interfaces. Each management tool and user interface provides the ability to plan, manage, and locally administer IP addresses and services across LINUX, Solaris, and Windows platforms. VitalQIP works with directory services and RDBMS configurations.

Reason for Reissue

The following table lists the changes to the VitalQIP Web Client that required the *Web Client User's Guide* to be reissued.

Issue	Feature Name	Description	Feature Impact
5	Access Control	Chapter added on new Access Control feature.	• "Access Control" (p. 23-1)
5	Lucent DHCP 5.6 server	Support added for Lucent DHCP 5.6 server.	• "AbusiveClientLockout" (p. 20-23) • "AbusiveClientMonitorPeriod" (p. 20-23) • "AbusiveClientWarningCount" (p. 20-23) • "Access Control" (p. 20-24) • "SupportClientID" (p. 20-38)

Issue	Feature Name	Description	Feature Impact
5	Audit Reports	Added documentation for new reports: • DC Generation Audit Report • DHCP Server Generation Audit Report • DNS Server Generation Audit Report • Administrator Generation Audit Report	• "Produce a DC Generation Audit report" (p. 29-124) • "Produce a DHCP Server Generation report" (p. 29-127) • "Produce a DNS Server Generation report" (p. 29-131) • "Produce an Administrator Generation Audit report" (p. 29-111)
5	Search objects	• Added documentation on changes made to interface for searching for objects on a subnet. • Added information on property to limit the number of records that can be displayed in reports.	• "Search for an object in a subnet" (p. 10-7) • "Record search limit in qip.properties" (p. 29-6)
5	Contact and Location management	• Chapter added to support management of contacts and locations in the VitalQIP web client. • Updated information on contacts and locations in IPv4 address management • Updated steps for adding contact information when creating an administrator record.	• "Contact and location management" (p. 5-1) • "Modify subnet profile" (p. 9-43) • "Assign location and contact information to an object" (p. 10-45) • "Create an administrator" (p. 6-4)
5	Windows Domain Controller Maintenance	Chapter added to support management of Domain Controllers in the VitalQIP web client.	• "Domain Controller management" (p. 8-2)
5	Clone server	Added documentation on cloning server information.	• "Clone a DNS server" (p. 13-18) • "Clone a DHCP server" (p. 19-9)
5	DHCP server policy	Modified the description for DefaultUnavailableThreshold. Fixes VQIP00021879.	• "DefaultDescentThreshold" (p. 20-27)
5	MAC Pools	Updated descriptions for adding and searching MAC pools on a DHCP server and a subnet.	• "Define global MAC address pools" (p. 19-11) • "Subnet MAC Address Pools" (p. 9-50)
5	IPv4 Object Management	Added information on extra steps needed when creating an object named "null". Fixes VQIP00020537.	• "Add an object" (p. 10-12)

Issue	Feature Name	Description	Feature Impact
5	Zone Resource Records	Note added that auditing is supported for zone resource records.	• "Add/modify zone resource records" (p. 14-18)
5	User and Vendor Class support	Added documentation on add/modify/delete User Class and Vendor Class.	• "DHCP Client Class" (p. 21-1)
5	DNSSEC support	• The DNSSEC enabled server parameter added to support DNSSEC on DNS servers. • The DNSSEC enabled server parameter added to support DNSSEC on zones.	• "DNS BIND-9 parameters" (p. 13-7) • "LUCENT DNS 4.X parameters" (p. 13-11) • "BIND 9.X zone options" (p. 14-28) • "LUCENT DNS 4.X zone options" (p. 14-32)
5	Administrator Security	Clarification on Password Expiration added. Fixes VQIP00022042.	• "Set up administrator security" (p. 6-39)
4	Updates to text	Minor updates were made.	• "Manage a block associated with a subnet" (p. 9-67) • "Define a scope" (p. 10-22) • "Manage a subnet assocated with a block" (p. 28-37)
3	Web Client new look	The Web Client has a new look, which includes GUI color changes and new icons.	Entire document.
3	Administrator maintenance	Administrator management was added.	Chapter 6, "Administrator management"
3	DHCP infrastructure support	DHCP infrastructure support was added. This feature includes: • New DHCP server suppot • New DHCP policies and templates support • Updates to DHCP file generation support	• Chapter 19, "DHCP server" • Chapter 20, "DHCP policies and templates" • Chapter 22, "DHCP configuration file generation"
3	Global Policy maintenance items	Global, naming, and object class policies were added.	Chapter 2, "Policies"
3	IPv4 reclaim functionality	Support for IPv4 address reclaim funcitonality was added.	"Reclaim addresses" (p. 9-89)

Issue	Feature Name	Description	Feature Impact
3	AfriNIC support	AfriNIC support was added.	• "Regional Internet Registries" (p. 26-2) • "AfriNIC reporting" (p. 28-13)
3	New reports	The following reports features were added: • Quick View report feature • IPv4 Objects report • Node Hierarchy report • DHCP Server reports • Resource Record by zone report • Adminstrator Profile Audit report • Administrative Role Audit Report	• "Quick View" (p. 9-18) • "Produce an IPv4 Objects report" (p. 29-51) • "Produce a Node Hierarchy report" (p. 29-76) • "DHCP Server reports" (p. 29-82) • "Produce a Resource Record by zone report" (p. 29-102) • "Produce an Administrator Profile Audit report" (p. 29-114) • "Produce an Administrative Role Audit report" (p. 29-117)
3	DHCP 5.5 Server	DHCP 5.5 server support was added.	"Lucent DHCP 5.4, Lucent DHCP 5.5, and Lucent DHCP 5.6 server types" (p. 19-23)
3	Integration between address allocation and IPv4 address management	Supports added for IPv4 subnets can be associated with blocks.	• "Manage a block associated with a subnet" (p. 9-67) • "Manage a subnet assocated with a block" (p. 28-37)
3	Bulk operations	Bulk operations were added to zone, subnets, and objects. Operations, such as modify and delete, are allowed on more than one item.	• "Subnet management" (p. 9-34) • "Object management" (p. 10-3) • "Search for a zone" (p. 14-4) • "Modify multiple zones" (p. 14-10) • "View scheduled jobs" (p. 30-3)
3	Enhancements to IPv4 search feature.	Enhancements were made to the IPv4 search feature.	• "Perform a global search" (p. 9-7) • "Search for an object in a subnet" (p. 10-7)
2	Editorial changes	Minor editorial changes where made throughout the book.	The entire book.
1	Attribute enhancement	IPv4 infrastructure types and user define field support was added.	• "Add contents to a view" (p. 10) • "Add an attribute or attribute group to an infrastructure type" (p. 17) • "Working with user defined attributes and fields" (p. 23)

Issue	Feature Name	Description	Feature Impact
1	Block allocation enhancement	Space can be allocated from other blocks when adding a block to a child pool.	"Allocate a block to a child pool using its allocation rule" (p. 27-20)
1	DNS server management	DNS server management was added. DNS configuration files can be generated locally.	• Chapter 13, "DNS Server" • "Generate DNS configuration and data files" (p. 17-5)
1	DNS View	DNS Views was added. It allows an organization to present one name server configuration to one community of hosts and a different configuration to another community.	• "Manage domain names in view specific zones" (p. 10-57) • "Search for a node" (p. 11-3) • Chapter 15, "DNS Views"
1	IPv4 Network manangement	IPv4 network management support was added.	"IPv4 network management" (p. 24)
1	IPv4 Subnet organization	IPv4 subnet organization support was added.	"Subnet organization management" (p. 73)
1	Managed files support	Support was added to import files into VitalQIP that can then be copied to remote servers.	Chapter 18, "Managed Files"
1	MyView enhancements	MyView now allows administrators to create and manage personal views.	• "Work with shared and personal views" (p. 19) • Chapter 3, "MyView management"
	New reports	The following reports are new: • IPV4 Object Info • IPV4 Subnet Info • ACL Template Usage • Zone Resource Record • DNS View Audit • IPV4 Network Audit • IPV4 Subnet • Managed Files Audit • Organization Audit • My View Hierarchy	Chapter 29, "Reports"
	Node enhancement	Domain name management was added.	"Manage domain names in an IPv4 or IPv6 address" (p. 11-46)
	Northbound interface updates	The Northbound interface was updated for VitalQIP 7.2.	Chapter 32, "Northbound interface"

Issue	Feature Name	Description	Feature Impact
	Organizations	Organization support was added.	Chapter 4, “Organizations”
	Regional Internet Registry reports	VitalQIP supports new Regional Internet Registry reports.	• “SWIP reporting” (p. 3) • “APNIC reporting” (p. 7)
	Zone management	Zone management was added.	Chapter 14, “Zones”

How to use this information product

This manual is organized as follows:

Chapter 1, “VitalQIP web client user interface”	Provides background about logging in, the default MyView page, Web client navigation, and basic features of the Web client.
Chapter 2, “Policies”	Provides information on naming policies, object classes, and global policies.
Chapter 3, “MyView management”	Provides information on how to set up MyViews.
Chapter 4, “Organizations”	Provides information on using organizations in VitalQIP.
Chapter 5, “Contact and location management”	Describes how to manage contacts and locations.
Chapter 6, “Administrator management”	Provides information on managing administrators, administrator roles, and security.
Chapter 7, “Attributes”	Provides information on creating Attributes.
Chapter 8, “Domain Controller maintenance”	Describes how to manage domain controllers.
Chapter 9, “IPv4 address management”	Provides information about IPv4 nework and subnet management.
Chapter 10, “IPv4 object management”	Provides information about adding and maintaining objects in IPv4 subnets.
Chapter 16, “IPv6 address management”	Provides information about adding and maintaining objects in IPv6 subnets.
Chapter 11, “Node management”	Provides information about adding and maintaining nodes.
Chapter 12, “ACL Template”	Provides information on ACL templates
Chapter 13, “DNS Server”	Provides information on DNS server management in VitalQIP.
Chapter 14, “Zones”	Provides information on zone management in VitalQIP.
Chapter 15, “DNS Views”	Provides information on DNS Views,
Chapter 17, “DNS configuration file generation”	Provides information about DNS file generation.
Chapter 18, “Managed Files”	Provides information about imported file management in VitalQIP.
Chapter 19, “DHCP server”	Provides informaton on managing DHCP servers.
Chapter 20, “DHCP policies and templates”	Provides information managed DHCP policies and templates.
Chapter 21, “DHCP Client Class”	Describes how to manage DHCP Client Classes.

Conventions used

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

Convention	Meaning	Example
boldface	Names of items on screens. Names of commands and routines Names of buttons you should click. Uniform Resource Locators (URLs)	Select the **Client** check box. The **qip_getappllst** routine returns the entire list of existing applications. Click **OK**. The VitalQIP product site can be found at **http://www.alcatel-lucent.com/wps/portal/products**.
Helvetica bold	Names of keys on the keyboard to be pressed.	Press **Enter** to continue.
Letter Gothic	Output from commands, code listings, and log files	`# Name: Share shared-network _200_200_200_0`
Letter Gothic bold	Input that you should enter from your keyboard.	Run the following command: **`c:\setup.exe`**
<angle brackets>	Variables that you must substitute another value for.	*<debugfile>.bak.log*

Convention	Meaning	Example
italics	Manual and book titles. Directories, paths, file names, and e-mail addresses.	Refer to the *VitalQIP User's Guide* for more information. A symbolic link must be created from */etc/named.conf* that points to *named.conf*.
bold italic	Emphasis	***Read-only***. The name of the service element.
click	Click the left button on your mouse once.	To delete the object, click **Delete**.
right-click	Click the right button on your mouse.	Right-click on a service.
double-click	Double-click the left button on your mouse.	Double-click the book icon.

Related information

The following documents are referenced in this manual:

- *VitalQIP Administrator Reference Manual* (part number: 190-409-042R7.2)

  This guide describes planning and configuring your network, information about the VitalQIP interface, advanced DNS and DHCP configurations, and troubleshooting.
- *VitalQIP Installation Guide* (part number: 190-409-043R7.2)

  This guide describes how to install the VitalQIP product.
- *VitalQIP Command Line Interface User's Guide* (part number: 190-409-044R7.2)

  This guide discusses and describes how to use the VitalQIP Command Line Interface.
- *VitalQIP User's Guide* (part number: 190-409-068R7.2)

  This guide describes how to set up and use the VitalQIP user interface.

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 VitalQIP, you can contact the Technical Assistance Center for your region. Contact information is provided in the following table.

Region	Address	Contact information
North America	Alcatel-Lucent 400 Lapp Road. Suite 101 Malvern, PA 19355 USA	Phone: 1-866-LUCENT8 (582-3688) Option 1, Option 2 Web: **https://support.lucent.com**
Europe, Middle East, Africa, and China	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	Phone: Mexico 01 800 123 8705 or (52) 55 5278 7235 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 or contact your local sales representative. Web: **https://support.lucent.com**
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 - 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

Customers can access VitalQIP manuals online at **http://www.lucentdocs.com/cgi-bin/CIC_store.cgi**. Select **VitalQIP** from the Product Line list and click **Go**.

How to comment

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

Part I: Infrastructure

Overview

Purpose

This part of the manual provides information on the web client infrastructure.

Contents

This part includes these chapters.

1 VitalQIP web client user interface

Overview

Purpose

This chapter describes standard web client operations and provides an overview of the user interface.

Contents

This chapter covers these topics.

Web client operations

Overview

Purpose

This section provides information on logging in and out of the web client UI, as well as on other startup operations you can perform before you log in.

Log into VitalQIP web client

Purpose

To log into the VitalQIP web client.

Before you begin

Ensure the following are true before you begin.

- If you use proxies, make sure the address you use for VitalQIP is marked as an exception in your browser's proxy list.
- Be sure that pop-ups are enabled for VitalQIP, as the application uses this function to provide messages to the user.

English is the default language in the VitalQIP web client. If other languages are required, refer to "Character set and language configuration" in Chapter 17 of the *VitalQIP Administrator Reference Manual* for information on how to set up support for another language.

Procedure

To log into the VitalQIP web client, follow these steps.

1 Open a web browser and enter the VitalQIP web client URL. The URL is typically in the following format:

– For a nonsecure Tomcat server:

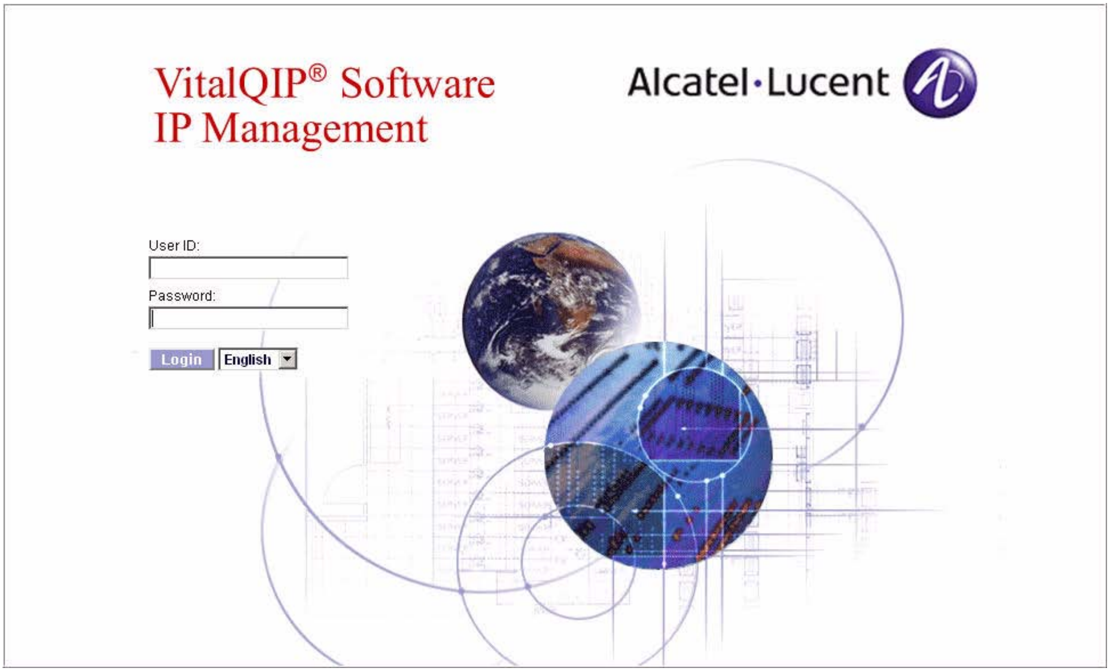
http://*<machine name* or ***IP address>*:*<Tomcat web server port>*/qip**

– For a secure Tomcat server:

http://*<machine name* or ***IP address>*:*<secure Tomcat web server port>*/qip**

Note: If the VitalQIP web client was installed with the nonsecure Tomcat web server port assigned to the default port 80, the URL format is **http://*<machine name*** or ***IP address>*/qip**. The default secure port is 743.

Result: The VitalQIP Login screen opens.



2 Enter the user ID that has been assigned to you in the **User ID** field.

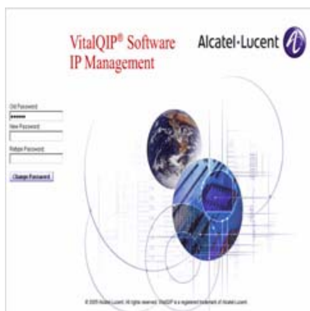
3 Enter the password that has been assigned to you in the **Password** field.

4 ***Optional***. Select a language only if a language other than English has been set up.

5 Click **Login**.

Note: If the **Allow Password Expiration** privilege for your administrator profile is enabled and your password has expired, or the **Require New Admin Password** field is enabled in the Administrator Security screen in the web client and you are logging in for the first time, you will be required to enter a new password. For further information on administrator security settings, refer to "Administrator security" (p. 6-39).

6 Choose one of the following actions.

If ...	**Then..**
The Organization selection screen is displayed	1. Select the organization you wish to use from the **Organization** drop-down list. **VitalQIP Organization** is the default. 2. Click **Continue**. **Result:** The VitalQIP web client UI opens.
The Change password screen is displayed	1. Click **OK** to close the dialog box with the message **Admin *<userID>* requires a new password**. **Result:** The Change Password fields are displayed.  2. Enter your current password in the **Old Password** field. 3. Enter your new password in the **New Password** field. Ensure that it complies with the password creation rules established in the Administrator Security function. 4. Enter your new password again in the **Retype Password** field. 5. Click **Change Password**. **Result:** The **Organization** drop-down list is displayed. To continue logging in, refer to the instructions above.

END OF STEPS

Exit the VitalQIP web client

Purpose

To exit the VitalQIP web client.

Procedure

To exit the VitalQIP web client, follow these steps.

1 Click **Logout** on the VitalQIP toolbar.

Result: A confirmation dialog box opens with the message **Are you sure you want to exit QIP?**

2 Click **OK**.

Result: The VitalQIP Software IP Management splash screen opens with the message **You are logged out. Please Login**.

3 To exit VitalQIP altogether, close the browser session.

END OF STEPS

Start or stop the Tomcat server

Purpose

To start and stop the Tomcat server.

Procedure for UNIX

To start or stop the Tomcat server on UNIX platforms, follow these steps.

1 Be sure your environment variables are set.

2 Change directory to $QIPHOME.

3 Choose one of the following

- To start the Tomcat instance, enter

`./startTomcat.sh`

Result: On startup, Tomcat reads *$QIPHOME/tomcat/conf/server.xml* for configuration information (port numbers, SSL, client connection and other operational parameters).

- To stop the Tomcat instance, enter

`./stopTomcat.sh`

4 Check if the Tomcat server is running by entering the following command:

`ps -ef|grep apache`

A response similar to the following appears:

```
root 24707 1   0 11:22:26 pts/4 10:33
   /opt1/qip70rsweb/jre/bin/java
   -Djava.util.logging.manager=org.apache.juli.Class
```

END OF STEPS

Procedure for Windows

To start or stop the Tomcat server on Windows platforms, follow these steps.

1 Open the Windows Service Controller.

2 Start the service by right-clicking on **VitalQIP Apache Tomcat 5.5 Server** and selecting **Start**.

3 Stop the service by right-clicking on **VitalQIP Apache Tomcat 5.5 Server** and selecting **Stop**.

END OF STEPS

Open multiple browser sessions for the VitalQIP Web UI

Purpose

To allow you to open more than one Firefox browser session to log into the VitalQIP Web UI. This procedure describes how to create a new profile in Firefox. If you use two Firefox browser sessions simultaneously with VitalQIP, each must have a unique profile.

Procedure

To create two Firefox browser profiles, follow these steps.

1. Open a command prompt and enter the following:

   `firefox.exe -p`

2. Create a new profile by following the instructions provided.

3. Set the following variable to use two profiles at the same time:

   `MOZ_NO_REMOTE=1`

4. Go to **Control panel** > **System** > **Advanced** > **Environment Variables** > **System Variables** > **New** and enter the following:

   Variable Name: **`MOZ_NO_REMOTE`**

   Variable Value: **`1`**

5. Click **OK** to close the open dialog boxes.

6. Make two shortcuts for Firefox. Each shortcut will be used to launch Firefox with a different Profile. The target in the shortcut properties will appear as follows:

   Target: "C:\Program Files\Mozilla Firefox\firefox.exe" -p "*profile name*"

   You can now launch two separate Firefox sessions for use with the VitalQIP Web UI.

END OF STEPS

User interface

Overview

Purpose

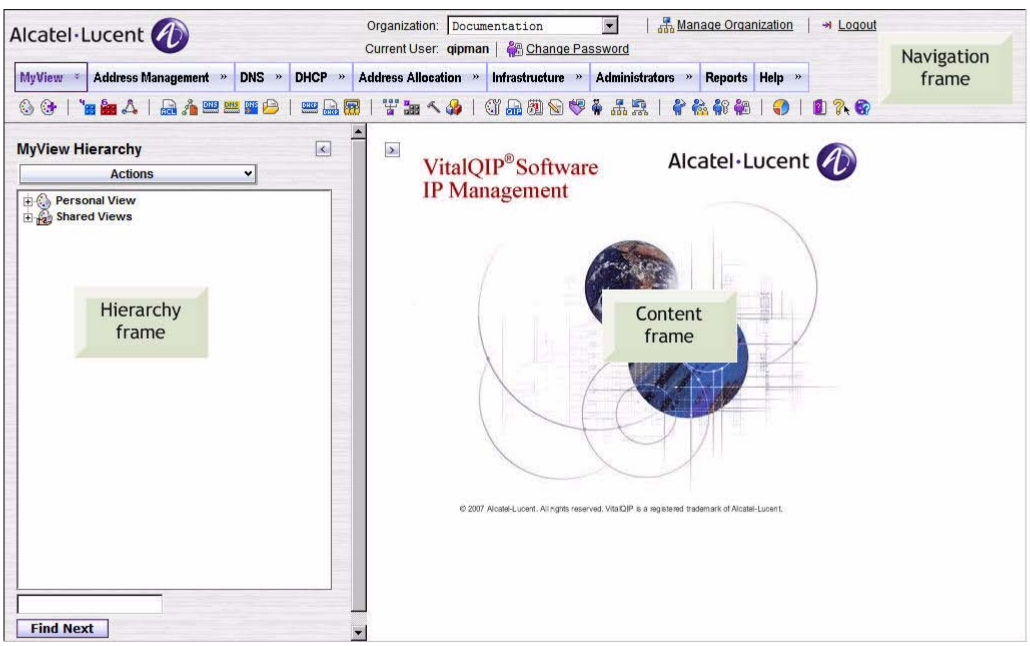
Elements common to most VitalQIP web client pages, such as icons, navigation buttons and command buttons are described in this section. In addition, a description of the entry point to the web client, the MyView hierarchy, .

User interface components

Web client page frames

The VitalQIP web client 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 VitalQIP web client 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 dark blue. When you mouse over other menus, they are shown as dark blue as well.

> **Note:** The **Links** menu only appears in the main menu if a licensed version of a pre-defined add-on has been installed or a customized add-on exists.

Sub-menus

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

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. After most toolbar icons are clicked, the corresponding main menu item is selected and displayed in dark blue. However, when icons that represent commands on the Help menu are invoked, separate browser windows open.

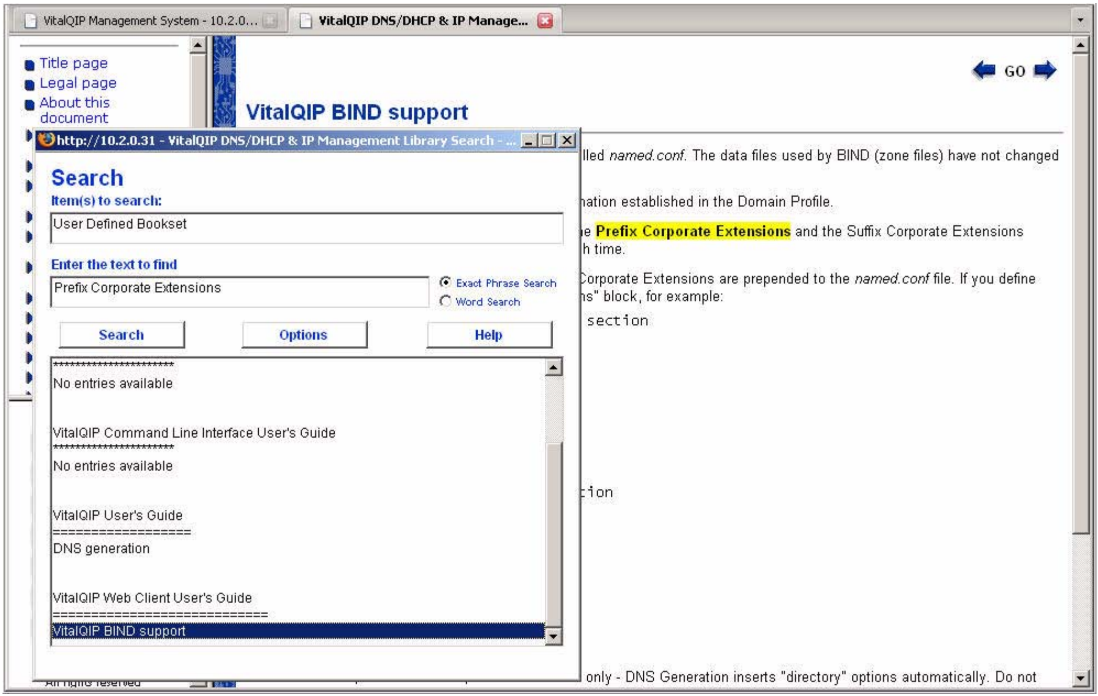
Customized add-ons

VitalQIP supports add-ons that are pre-defined by Alcatel-Lucent, such as AutoDiscovery, as well as customized add-ons that the customer has added and maintained in the data file *Menu_Customized.html.js*. A **Customized Links** sub-menu item can be added under the **Links** menu and a toolbar icon also inserted in the toolbar.

For information on adding access to a web-based application from within the VitalQIP web client, refer to Chapter 17, "Web Client Configuration" in the *VitalQIP Administrator Reference Manual*.

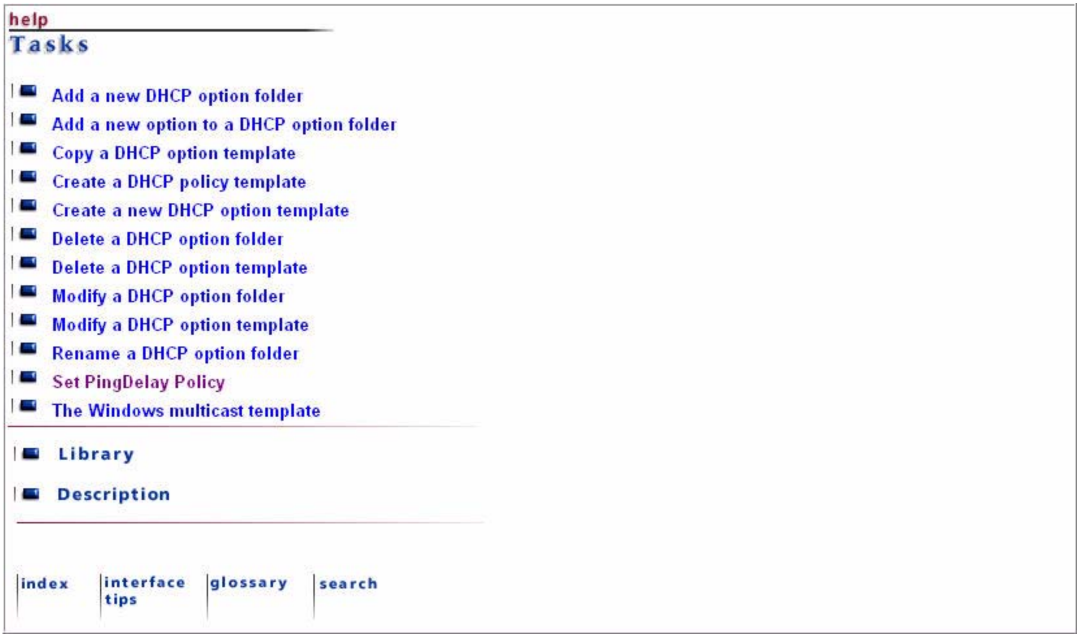
Online Document

The Online document icon launches the VitalQIP Product Library. The library contains both HTML and PDF versions of the VitalQIP 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.



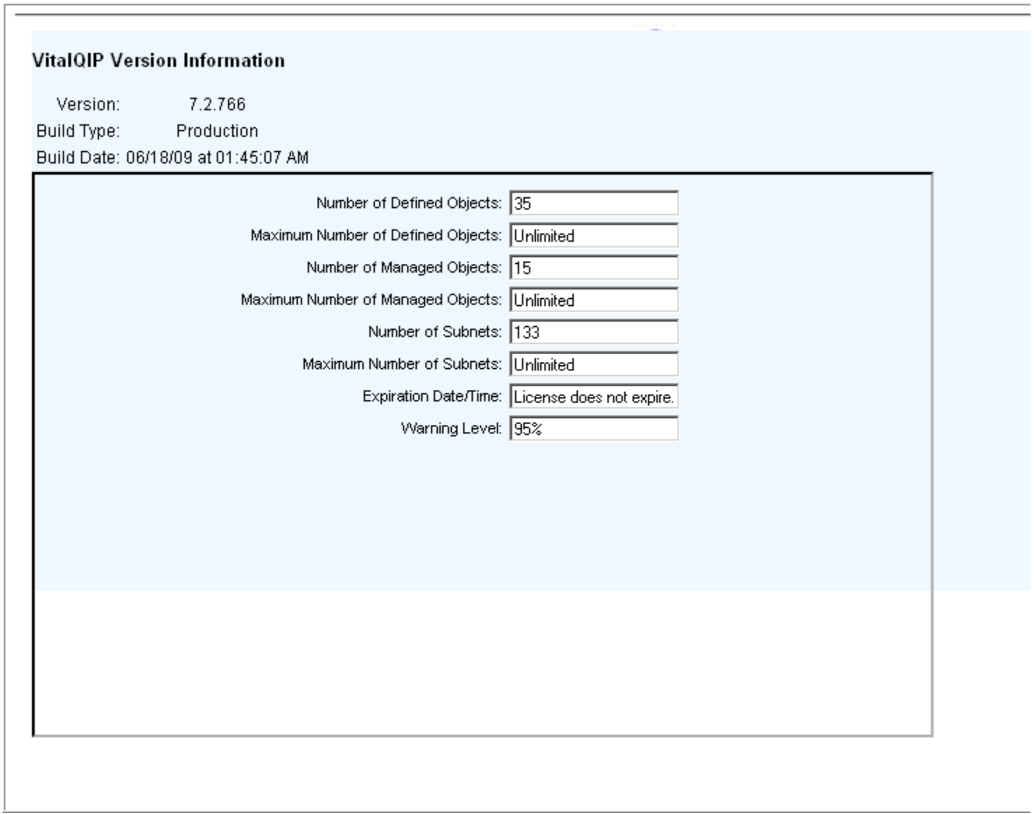
Online Help

The Online Help icon launches a list of help screens that are available for the function that is currently open in the web client UI. For example, if the Block Hierarchy is open, the Online Help icon launches a help screen containing a list of tasks related to using that feature.



About VitalQIP

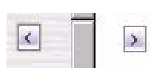
The About VitalQIP icon launches the VitalQIP Version Information screen, where you can determine which version of the product you have installed, as well as information on the maximum number of infrastructure types and subnets allowed by the license key and the actual number currently in use. This information may be useful whenever you need to contact Technical Support.

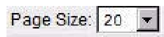


Content frame icons

The following table describes buttons and icons that commonly occur in the VitalQIP web client 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 VitalQIP web client UI. To restore the prior configuration, select the icon again. **Note:** You can also click and drag the edge of a frame to resize it.
List scrolling arrows	 If data is displayed in a list, the  and  arrows allow the user to view the previous or next page of data. The drop-down list allows you to jump directly to a different page of data without viewing the intervening ones.

Icon name	Description
Paged list drop-down	 If data is displayed in a paged list, this drop-down list allows you to specify how many items to display on a page.
Calendar	 Opens a calendar window with the current date highlighted and the current time displayed. 

Hierarchy display

In the hierarchical view at any level, the maximum number of infrastructure objects (Pool, Block, IPv4 address, and IPv6 address) that a folder can hold is defined in the *qip.properties* file by the **`foldersize`** parameter. If no value is specified, 50 is the default value. Folders are displayed only if the total number of objects at the same level reaches or is greater than the **`FolderSize`** parameter.

For example, if there are 70 seed pools defined and the **`FolderSize`** is set to 30, then in the Pool hierarchy, instead of showing all 70 seed pools directly, three pool folders are generated and displayed (The first two folders contain 30 seed pools and the last one contains 10).

Refer to Chapter 17, “Web Client Configuration” in the *VitalQIP Administrator Reference Manual* for detailed information about this parameter.

Expand/Contract icon description

The Expand (plus sign) and Contract (minus sign) icons appear to the left of a hierarchy item. Clicking on the icons allows you to toggle between displaying the information and hiding the information.

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

Hierarchy Display

The following three functions are available from the **Actions** bar for hierarchy listings under most tabs:

	**Refresh Hierarchy** retrieves the current data from the database and displays it in the hierarchy
	Refresh Selection refreshes the selected item with current data from the database and displays it in the hierarchy.
	Collapse All changes the hierarchy display so only the top-level items are visible in the hierarchy.

Search hierarchy tree

Many areas of the VitalQIP Web Client allow you to search the hierarchy from the initial page where it is displayed. This function only searches by the attribute displayed in the hierarchy tree (for example, you can use this to search the pool hierarchy by pool name, but you cannot use this function to search for pools with specific sets of properties).

This function only searches the following:

- Expanded branches of the hierarchy
- Branches of the hierarchy that have been expanded and then collapsed by the user by clicking on the minus sign

This function does not search the following:

- Branches of the hierarchy that have not been expanded
- Branches of the hierarchy that have been expanded, and then collapsed by using the **Refresh Hierarchy** function from the Actions menu
- The VitalQIP database

The search field displays at the bottom of the hierarchy, as shown in the following illustration.

Figure 1-2 Search field

Type the name of the object for which you are searching in the field and click **Find Next.** If an object matches your search, it is highlighted, and its properties appear in the right-hand page of the screen. If you click **Find Next** again, the next match is highlighted until you reach the bottom of the hierarchy.

This search function finds all matches that contain the value you type in the search box, regardless of whether it starts the name of the object or is contained within it.

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 1-3 An information dialog box

Figure 1-4 A confirmation dialog box

Figure 1-5 An error dialog box

Cut, copy and paste

The cut, copy and paste utility associated with the platform that you are using to run the VitalQIP GUI may be used to delete, duplicate, or move data from one text field to another text field. This typically works only for normal text fields for which data also could be accessed from the keyboard of your platform.

For all platforms, the left mouse button can be used to select the data to be manipulated before using **Cut**, **Copy**, or **Paste**.

For PCs, you may use the left mouse button to select the data, then you may use the control sequence shortcuts, **Ctrl-x** to cut, **Ctrl-c** to copy, and **Ctrl-v** to paste or use the right mouse button to access the cut, copy, and paste utility.

Wildcard character in searches

The wildcard character is an asterisk (*). The wildcard can be used in place of zero or more characters when performing a search. It can be the first or only character in a search string.

Required fields

An asterisk (*) preceding a field name indicates that data must be entered or a value must be selected for that field. Required fields also appear in boldfaced type.

Folders in hierarchy views

If the **foldersize** property is set in the *qip.properties* file, folders are displayed in the hierachy view after the node reaches the limit of infrastructure objects defined by this property. For more information, refer to the “Web client configuration” chapter in the *VitalQIP Administrator Reference Manual*.

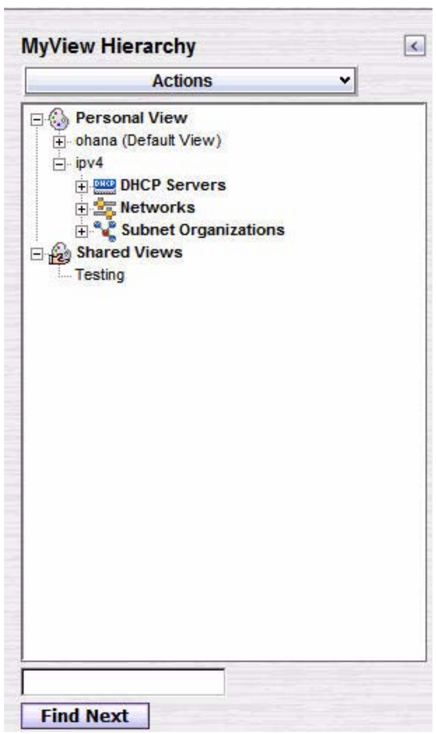
MyView Hierarchy

Overview

The MyView Hierarchy presents a customized hierarchical view of the data that you may access in the VitalQIP database. It contains all the items in your Managed List (as defined in your Administrator Profile), shared views to which you have been assigned by a master or organization administrator (using **MyView Management Hierarchy** on the **Infrastructure** tab) and personal views which you have set up (using **MyView Personalization** on the **MyView** tab). For more information, refer to "MyView administration" (p. 3-2).

Note: Access to the VitalQIP web client may be restricted to the **MyView** tab only, if the **Display MyView Tab Only** privilege is set to true in the Administrator Profile.

Figure 1-6 Sample MyView Hierarchy



Personal View

Personal View enbles you to manage parts of the infrastructure that are assigned to you by a master or organization administrator.

Managed List infrastructure types

The following object types may be part of the MyView Hierarchy since they can be included in an administrator's Managed List, as well as in an Administrative Role:

- Network
- IPv4 Subnet
- Subnet Organization
- OSPF Area
- Server
- Domain
- IPv4 Address Range
- Object Range
- Application

Note: The MyView Hierarchy displays each server type in its own labeled section of the hierarchy, making it more convenient to check specific server properties and file generation times.

Shared Views

Shared Views enable you to manage the following infrastructure elements that cannot be entered in a Managed List.

- Address Pools
- IPv6 seed blocks
- IPv6 address ranges
- IPv6 subnets
- Nodes (IPv4 and IPv6)
- Other Shared Views

Label and order infrastructure

The order in which the infrastructure types are listed, as well as the labels for each type, may be changed. The **Order Infrastructure** and **Label Infrastructure**functions are available on the **Actions** menu. Refer to the following sections for further information:

- Order Infrastructure - "Order infrastructure" (p. 3-26)
- Label Infrastructure - "Label infrastructure" (p. 3-28)

Work with shared and personal views

Purpose

To work with a Shared View that has been assigned to your **Personal View**.

Procedure

To work with a Shared View, follow these steps.

1 Mouse over **MyView Hierarchy** and click the **MyView Hierarchy**.

Result: The MyView Hierarchy opens.

2 If you are working with:

- Personal views, expand **Personal Views**
- Shared views, expand **Shared Views**

Result: A list of views opens.

3 Expand the views until you find the infrastructure item you need to work with. Depending on what infrastructure types are assigned to the Shared View, you may access the functions that are listed in the following table.

Table 1-2 Shared and personal view functions

Infrastructure type	Functions available
Shared Views	• Properties • Report: MyView Audit (page 29-183)

Infrastructure type	Functions available
Address Pools/Seed Pools	• Properties • Add Seed Block (page 27-9) • Modify Pool (page 27-13) • Delete Pool (page 27-13) • Merge Pool (page 27-29) • Add Child Pool (page 27-16) • Allocate a Block (page 27-20) • Explicit Allocation (page 27-23) • Reports: Pool Audit (page 29-170), Pool Block Status (page 29-22), Pool Hierarchy (page 29-26), Pool Statistics (page 29-30), Pool Usage (page 29-34), Pool Free Space (page 29-39
IPv4/IPv6 Blocks	• Block Properties • Modify Block (page 28-19) • Expand Block (page 28-22) • Move Block (page 28-23) • Split Block (page 28-25) • Merge Block (page 28-27) • Renumber Block (page 28-29) • Return to Parent (page 28-31) • Free Block (page 28-33) • Delete Block (page 28-36) • Recover Block (page 28-34) • Reports: Block Audit (page 29-120), Block Hierarchy (page 29-14), Block Utilization (page 29-18)
IPv6 Seed Blocks	• Seed Block Properties • Add Address Range (page 16-7) • Delete Seed Block (page 16-6) • Add Subnets (page 16-11) • Reports: IPv6 Address Audit (page 29-153), IPv6 Subnet Audit (page 29-157), IPv6 Subnets (page 29-73)
IPv6 Address Ranges	• Address Range Properties • Modify Address Range (page 16-9) • Delete Address Range (page 16-10) • Add Subnets (page 16-11) • Reports: IPv6 Address Audit (page 29-153), IPv6 Subnet Audit (page 29-157), IPv6 Subnets (page 29-73)

Infrastructure type	Functions available
IPv6 Subnets	• Subnet Properties • Modify Subnet Profile (page 16-16) • Delete Subnet • Split Subnet (page 16-18) • Join Subnets (page 16-20) • Renumber (page 16-21) • Quick Add (page 16-23) • Manage Addresses (page 16-27) • Reports: IPv6 Address Audit (page 29-153), IPv6 Subnet Audit (page 29-157), Managed Addresses (page 29-69), IPv6 Subnets (page 29-73)
Nodes	• Node Properties • Modify Node (page 11-17) • Delete Node (page 11-19) • Add Interface (page 11-20) • Reports: Node Hierarchy (page 29-76), IPv6 Address Audit (page 29-153)
Interfaces	• Interface Properties • Modify Interface (page 11-22) • Delete Interface (page 11-38) • Add IPv6 Address (page 11-25) • Add IPv4 Address (page 11-29) • Move Interface (page 11-24)
IPv6 Addresses	• IP Address Properties • Modify IP Address (page 11-35) • Delete IP Address (page 11-37) • Add Domain Name (page 11-39) • Move to Subnet (page 11-35) • Move to Interface (page 11-33)
Domain Names	• Domain Name Properties • Modify Domain Name (page 11-42) • Delete Domain Name (page 11-45)

END OF STEPS

2 Policies

Overview

Purpose

This chapter describes the functions on the **Global Policies** and **Object Classes** menus.

Contents

This chapter covers these topics.

Naming Policies

Overview

Purpose

VitalQIP supports multiple methods for naming network objects. These methods provide considerable versatility because they can be used in a selective, global, or ad-hoc fashion. The foundation of the naming policy implementation is the application of a significant/non-significant name to each type of object class.

All generated names are assured uniqueness through the **Instance Length** field. In an environment of multiple administrators simultaneously assigning names to objects, an instance number is automatically incremented to satisfy each request. If an assignment is not used or completed, that instance number is thrown away.

The system-provided naming policies for network objects can be left as is or modified. If you do not wish to have any policies defined, use null (blank) fields.

Establish object naming policies

VitalQIP provides system-generated default object names for each Object Class. They are comprised of a **Prefix** (which can also be preceded by a custom Business Unit ID), an **Instance Length**, and a **Suffix**. The following table shows examples of unique object name policies.

Table 2-1 Sample unique object name policies

Prefix	Instance Length	Suffix	Object Name
pcp	6	ab	pcp000001ab
	6	ad	000001ad
pcp	6		pcp000001

All default object classes have a corresponding Object Naming Policy. Each time you define an object, and assign an **Object Class** (for example, PC, Server, Wiring_HUB, and so on) through the Object Profile in Object Management, it is assigned a corresponding **Object Name**, using the associated Naming Policy.

Customize object names

Purpose

You do not have to use the VitalQIP-generated Object Names for your objects. You can change the default names in the Modify Naming Policy page to any name you choose.

Before you begin

- Although the **Prefix**, **Instance Length**, and **Suffix** fields can be customized for each object class, the **Object Class** field cannot be changed in this window. To add or modify object classes, use the Object Classes function. Refer to "Object classes" (p. 2-10) for more information.
- All naming policies entered are optional except Dynamic_Allocation. Dynamic_Allocation must have a naming policy. Any other Object Class naming policy can be blank. If left blank, the Object Class uses the Dynamic_Allocation policy when the object is added as a reserve or dynamic object. Refer to "Name dynamically allocated objects" (p. 2-6) for further information.

Procedure

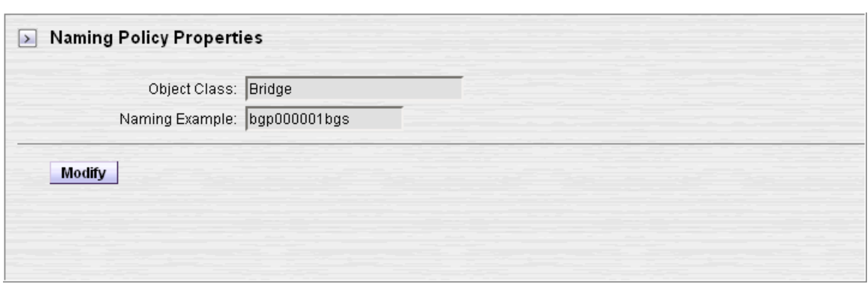
To change object names, follow these steps:

1 Select **Object Classes** from the **Infrastructure** menu.

Result: The Object Class Hierarchy page opens.

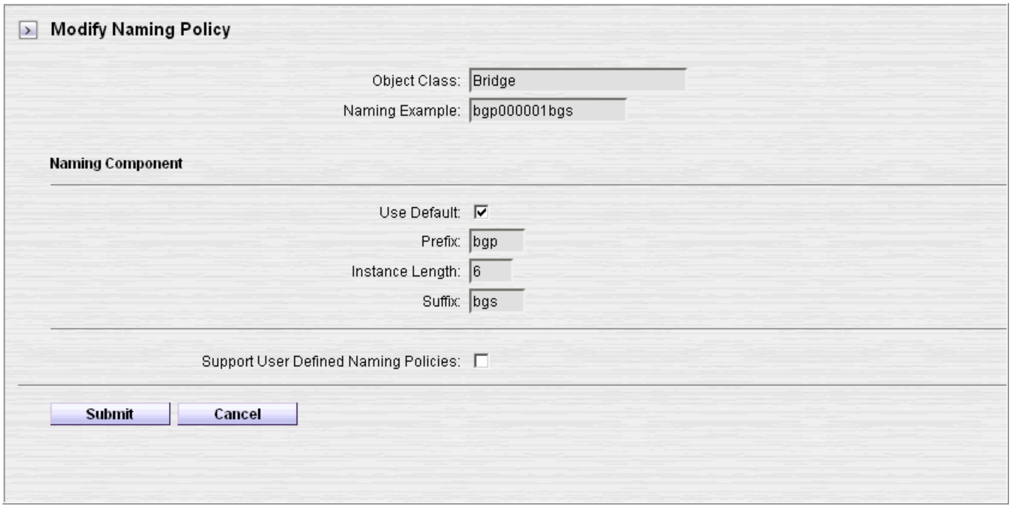
2 Expand **Naming Policies** in the hierarchy and select the **Object Class** you wish to customize.

Result: The Naming Policy Properties page opens.



3 Click **Modify**.

Result: The Modify Naming Policy page opens.



Note: If the default global naming policy is being used, the fields are read only and the **Use Default** checkbox is checked.

4 To override the global default naming policy with one that is used across the current organization, uncheck **Use Default** and fill in the appropriate values as described in the following table. If you click **Use Default** again, the default value for the naming policy appears in the fields, which becomes read-only again.

Table 2-2 Naming Component fields

Field	Description
Prefix	This is a three-character alphanumeric field. It can be left blank.
Instance Length	This is a one-character numeric field. It can be left blank. You can specify a value from 0 to 9 to set the number of digits in the instance number. For example, if you enter 6, numbers from 000001 to 999999 are generated sequentially. Each time an object is assigned to an address, the number is automatically incremented, thereby ensuring that the assigned names are unique.
Suffix	This is a three-character alphanumeric field. It can be left blank.

5 Check the **Support User Defined Naming Policies** box if you want to implement a User Defined Naming Policy. VitalQIP automatically calls a user exit for your unique object naming requirements. Refer to "User-defined object naming policy user exit" (p. 2-7) for detailed information on the fields that are passed with this user exit and how to set it up.

6 Click **Submit** to save your changes.

Result: A Confirmation prompt opens.

7 Click **OK** at the Confirmation prompt.

END OF STEPS

Use a business unit ID to customize object naming policies

Purpose

You can add a Business Unit ID as a prefix to all objects added by a specific administrator.

Procedure

To add a Business Unit ID prefix, follow these steps:

1 Select **Administrator** from the **Administrators** menu.

Result: The Administrator Hierarchy opens.

2 Expand the hierarchy and select an administrator.

Result: The Administrator Properties page opens.

3 Click **Modify**.

Result: The Modify Administrator page opens.

4 Click the **Administrator** tab.

Result: The fields related to the tab are displayed.

5 Enter an ID (of up to 8 characters) in the **Business Unit ID** field. For example, for an Administrator Profile with the login name "jsmith", you might establish a Business Unit ID such as "JS".

6 Click **Submit** to save the change to the profile.

Result: A confirmation dialog box opens.

7 Click **OK** at the Confirmation prompt.

Result: When the administrator "jsmith" creates objects in the Object Profile, the **Object Name** will be prefixed with JS. The following table shows the break down of the **Object Name** when a **Business Unit ID** is used.

Table 2-3 Sample object names with business unit ID

Business Unit ID	Prefix	Instance Length	Suffix	Object Name
JS	pcp	6	ab	JSpcp000001ab
JS		6	ad	JS000001ad
JS	pcp	6		JSpcp000001

END OF STEPS

Name dynamically allocated objects

A special case exists regarding the naming of objects that are dynamically allocated. The object class "Dynamic_Allocation" is assigned to all dynamically and reserved objects that have a blank naming policy (the **Naming Example** appears blank). This ensures a way of consistently naming the dynamic or reserved objects within your network regardless of what type of objects they are.

For example, if you establish a blank naming policy for the object class "PC" in the Naming Policies window, and you then dynamically allocate or reserve addresses in Object Management and assign them a PC object class, VitalQIP automatically gives them the object name of the "Dynamic_Allocation" object class.

A few things to keep in mind

- The **Instance Length** for the "Dynamic_Allocation" object class cannot be less than 4.
- A mixture of naming policies can be employed for different object classes. For example, workstations and PCs may use an **Instance Length**, and the system would automatically generate the object name, whereas servers and gateways may require very significant names, so all fields are left blank and the user inputs the name at the time the IP address is assigned.

Note: Do not assign Dynamic DHCP objects to an object class that does not have a Naming Policy (the **Prefix**, **Suffix** and **Instance Length** fields have all been set to blank) and a "Dynamic_Allocation" Naming Policy containing only an **Instance Length**. Otherwise, the Dynamic Objects are assigned generic hostnames that are numeric values only. When the DHCP configuration files are created, the name pool will contain those numeric values and cause problems for the DHCP server.

User-defined object naming policy user exit

The user-defined naming policy can be used to create unique object names for your system. In order to activate the user-defined naming policy user exit, you must select the **Support User Defined Naming Policies** check box on the Modify Naming Policies window.

Note: The VitalQIP web client uses a different way of configuring user-defined object naming policy. If you want the VitalQIP client and web client to use the same user-defined policies, configure both client to use the same naming convention. Refer to the *VitalQIP Administrator Reference Manual* for more information.

This user exit is called each time an object name is searched. If the exit exists, your custom naming policy is used.

For the user-defined naming policy user exit to be used, the following conditions must be met:

1. Set the **Infrastructure|Global Policies|General|User Exit Name** policy to "True" or check the **Support User Defined Naming Policies** check box in the Modify Naming Policies window.
2. On UNIX systems, a shared library named *qipuserexits.so.5* must exist in the Library Path directory (for example, *$QIPHOME/qipuserexits.so.5*). For Windows systems, a dynamic link library named *qipuserexits* must exist in the *%QIPHOME%\userexits* directory.

3. The **qipuserexits** shared library must contain a C (***not*** C++) function named **qipupnuserexit**, which returns a void and takes a single parameter, a pointer to a NAME_EXIT_STRUCT, as follows:

```
- void qipupnuserexit (NAME_EXIT_STRUCT *name_struct)
```

4. The returned name is checked against certain sets of criteria.
   - If the **Infrastructure|Global Policies|General|Name Validation** policy is set to **DNS_COMPLIANT**, the returned name must be no more than 32 characters long, contain only letters, digits or dashes (-). The first character cannot be a dash.
   - If the **Infrastructure|Global Policies|General|Name Validation** policy is not set to **DNS_COMPLIANT**, the returned name must be no more than 32 characters long, contain only letters, digits and dashes (-), and the first character cannot be a dash (-).
   - The VitalQIP-generated name is used if the name exit is not usable, or the returned name fails validation or is blank (0 length).

Following is the structure that is passed with the user-defined naming policy user exit. It is a standard C structure. A number of brackets after a field name designate the maximum length of the string +1 (all C strings have a terminating 0). The text in bold is the structure. The text following // and shown in italics are notes about the particular line.

```
typedef struct {
  char generated_name[64];  // The default name generated by VitalQIP
  char user_supplied_name[64];  // The user places the generated name here
char class_descr[21];
   char obj_ip_addr[16];
   char domn_name[191];
   char subnet_name[33];
   char subnet_addr[16];
   char subnet_mask[33];
   long subnet_usage;
   char appl_name[31];
   char ftp_svr_name[256];
   unsigned char hardware_type;
   char mac_addr[33];
   char manufacturer[49];
   char model_type[17];
   char asset_no[26];
   char room_id[16];
   char contact_lname[21];
   char contact_fname[21];
   char contact_eaddr[65];
   char contact_phone[21];
   char contact_pager[21];
   char floor[16];
   char street[41];
   char city[21];
```

```
   char state[11];
   char zip[17];
   char country[31];
} NAME_EXIT_STRUCT;
```

A sample user name exit function follows:

```
extern "C" void qipupnuserexit (NAME_EXIT_STRUCT *name_info)
{
sprintf (name_info->user_supplied_name, "%s%d",
name_info->class_descr, name_info->hardware_type);
}
```

Under Windows, the function declaration is:

```
extern "C" __declspec(dllexport) void qipupnuserexit (NAME_EXIT_STRUCT
   *name_info)
```

Compiler and linker options

The following platforms require specific types of compilers and linkers:

- For Windows, create a project and specify DLL as the target type.
- For Solaris, the C function should be compiled using the -KPIC compiler option, and the shared library should be built with the -G option.

Object classes

Overview

Purpose

VitalQIP permits additional object classes that currently do not exist in the static list to be created. Support for multiple object classes for the same device type allows you to enforce similar behavior in VitalQIP for different object classes.

Note: Only a Master administrator can use the Object Classes function.

When you create an object class, you provide a name for the class, assign a device type, and define a default naming policy. The device type is selectable from a set of device types, such as “server”, “host”, and so on. A device type permits the correct fields for a specific object class to appear in the Object Profile when that object class is selected. For example, you may want a “Graphics Workstation” object class to be a specific type of Host. The Graphics Workstation behaves like the Host Object class, only the name is different. You select the Host device type so that the same fields associated with a Host appear when you select Graphics Workstation in the Object Profile.

Note: It is recommended that you include some indication of the device type in the object class name. Users of the web client interface will be better able to identify the fields in which they have to enter appropriate information.

The naming policy created in the Object Classes page becomes the default naming policy for that Object Class. The Object Class is selectable across Organizations, although each Organization can override the naming policy in the Naming Policy screen.

Object class naming rules

Keep the following in mind when working with object classes:

- All object classes can have the names and device types changed except Dynamic_Allocation, External, and Partially_Managed.
- All object classes will have editable naming policies that can be changed.
- All naming policies entered are optional except Dynamic_Allocation. Dynamic_Allocation must have a naming policy. Any other Object Class naming policy can be blank. If left blank, the Object Class uses the Dynamic_Allocation policy when the object is added as a reserved or dynamic object.

Create a new object class

Purpose

To create a new object class.

Procedure

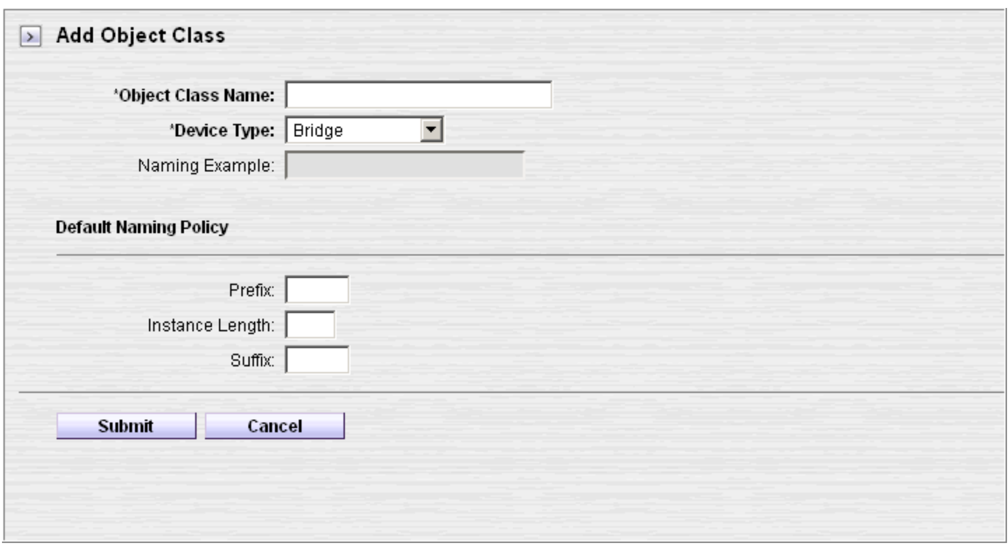
To create an object class, follow these steps:

1 Select **Object Classes** from the **Infrastructure** menu.

Result: The Object Class Hierarchy opens.

2 Select **Add Object Class** from the **Actions** menu.

Result: The Add Object Class page opens.



3 Enter appropriate values, as described in the following table.

Table 2-4 Add Object Class fields

Field	Description
Object Class Name	***Required.*** The name for the object class. Up to 20 characters can be entered. Valid characters are alphanumeric, spaces, underscores and dashes.

Field	Description
Device Type	***Required.*** Select a device type from the Device Type list: • Bridge • Gateway • Host • Printer • Router • Server • Switch • Terminal Server • Wiring HUB
Naming Example	***Read only field.*** The **Naming Example** field is populated with values as you enter them in the **Prefix**, **Instance Length**, and **Suffix** fields.
Prefix	***Optional.*** This is a three-character alphanumeric field. It can be left blank.
Instance Length	***Optional.*** This is a one-character numeric field. It can be left blank. You can specify a value from 0 to 9 to set the number of digits in the instance number. For example, if you enter 6, numbers from 000001 to 999999 are generated sequentially. Each time an object is assigned to an address, the number is automatically incremented, thereby ensuring that the assigned names are unique.
Suffix	***Optional.*** This is a three-character alphanumeric field. It can be left blank.

4 Click **Submit** to save.

END OF STEPS

Modify an object class

Purpose

To modify an object class.

Before you begin

- If Partially_Managed, External, or Dynamic_Allocation is selected, only the Default Naming Policy fields are enabled. The Object Class Name and Device Type are disabled.
- You cannot change a device type if the object class is already assigned to an object.

Procedure

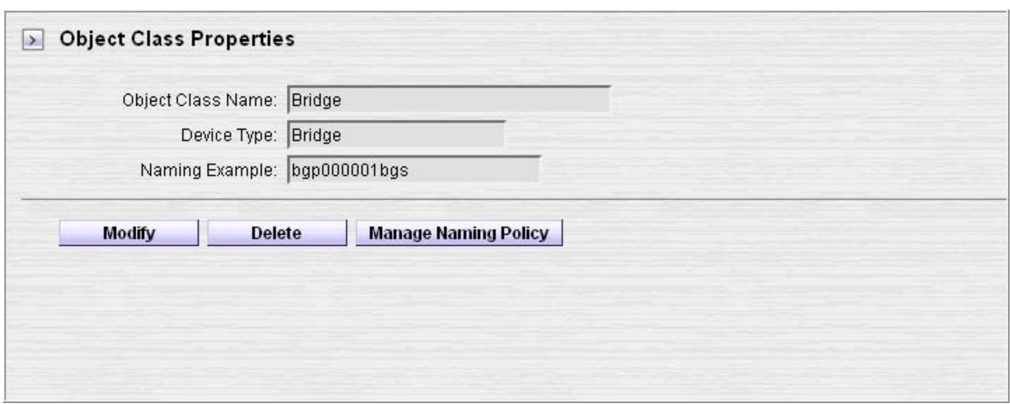
To modify an object class, follow these steps:

1 Select **Object Classes** from the **Infrastructure** menu.

Result: The Object Class Hierarchy opens.

2 Select the object class you wish to modify in the Object Class Hierarchy.

Result: The Object Class Properties page opens.



3 Click **Modify**.

Result: The fields you can modify appear at the bottom of the Modify Object Class page.

4 Make the desired changes. Refer to Table 2-4, "Add Object Class fields" (p. 2-11) for more information on the fields.

5 Click **Submit** to save them.

END OF STEPS

Delete an object class

Purpose

To delete an object class.

Before you begin

- You cannot delete Dynamic_Allocation, External, or Partially_Managed object classes.
- You cannot delete an object class if the object class is already assigned to an object.

Procedure

To delete an object class, follow these steps:

1 Select **Object Classes** from the **Infrastructure** menu.

Result: The Object Class Hierarchy opens.

2 Select the object class you wish to delete in the Object Class Hierarchy.

Result: The Object Class Properties page opens.

3 Click **Delete**.

Result: A confirmation prompt appears in the Object Class Properties page.

4 Click **OK** to delete the object class.

END OF STEPS

Global Policies

Overview

Purpose

Global policies allow you to establish standardized operating behavior for an organization. Policies fall under the Dynamic DNS, General, and Reports categories.

General policies apply to whatever database you have on your enterprise server. Dynamic DNS policies are specific to dynamic DNS and Reports policies are specific to reports. Each policy is explained in a table.

Establish global policies

Purpose

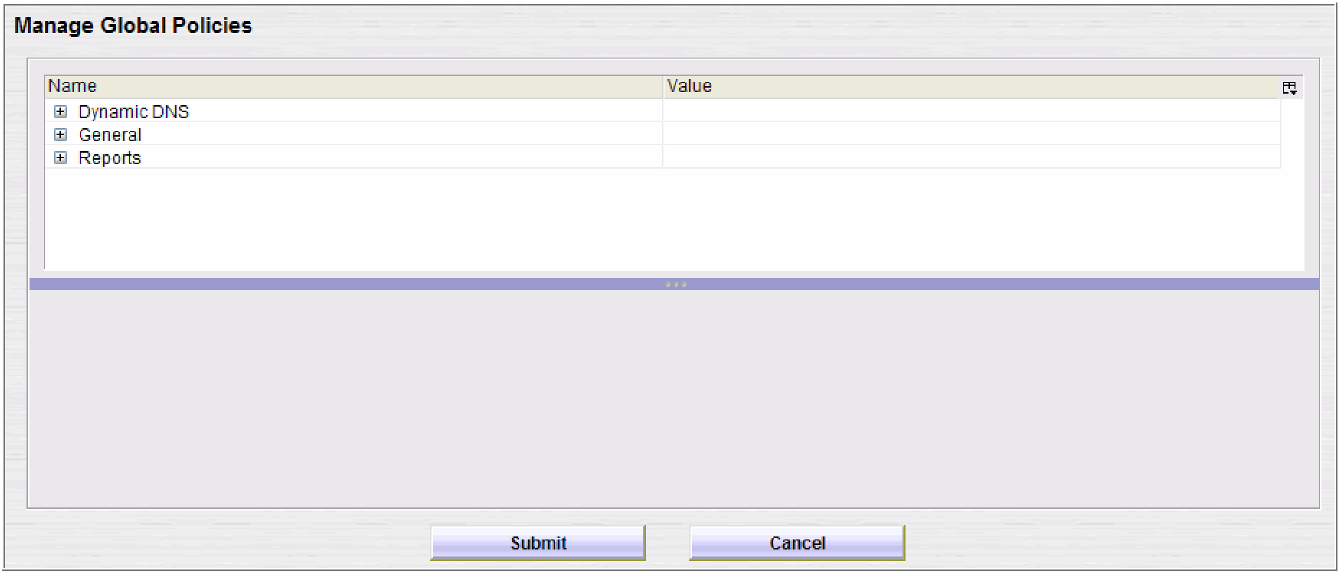
To set up global policies.

Procedure

To set up global policies, follow these steps:

1 Select **Global Policies** from the **Infrastructure** menu.

Result: The Global Policies page opens.



2 Select either **Dynamic DNS**, **General**, or **Reports** you want to modify and expand it to show the available options.

Result: The options and default values associated with that policy appear.

3 As you highlight a policy in the listing, the corresponding **Value** options are displayed based on the policy selected. Review the following tables for explanations of all the global policy options and values.

Note: You can modify multiple policies without leaving the window. Click **Submit** to save the changes and exit the window. Click **Cancel** to exit without saving any changes. If you have made changes before clicking **Cancel**, a dialog box opens asking if you want to save your changes.

Table 2-5 Dynamic DNS policies

Policy name	Values	Default value	Usage
IPv6 Defaults			Opens to display several policies related to publishing IPv6 management.

Policy name	Values	Default value	Usage
Publish AAAA Records	True or False	False	This policy determines if an IPv6 AAAA record for the IPv6 Address is published in a forward zone. Setting this option to True causes the **Publish in Forward Zone** to be checked in the Quick Add and Add Domain Name screens of the **Node Hierarchy** section of the VitalQIP web client. The AAAA record is then published in the forward zone for DNS lookups.
Publish PTR Records	True or False	False	This policy determines if a PTR record for the IPv6 Address is published in a reverse zone. Setting this option to True causes the Publish in Reverse Zone to be checked in the Quick Add and Add Domain Name screens of the **Node Hierarchy** section of the VitalQIP web client. The PTR record is then published in the reverse zone for DNS lookups.
DDNS Retry	The number of times to retry	1	This policy identifies how many times the DDNS updates will be attempted before failing. The value is ignored if the **Static DDNS Update** policy is set to False. **Note:** If this value is set to 0, no DDNS attempts will be made.
DDNS Timeout	Number of seconds	5 seconds	The number of seconds that the resolver library waits for a response to a query/update from a DNS server when performing a dynamic update. The value is ignored if the "Static DDNS Update" policy is set to False.
Dynamic DNS Mask	Selection from list	All values are selected	This policy is used to set the default DDNS values for dynamic (dynamic, A-DHCP, M-DHCP, D-DHCP, A-BOOTP, M-BOOTP) objects. They can be overwritten per object at the object level in the Object Profile, as described in "Dynamic DNS Updates" (p. 10-42).
Secure DNS Updates			Opens to display the following group of policies, specifically designed to set up Secure DNS.

Policy name	Values	Default value	Usage
GSSAPI Immediate Retries	0 to 1000	1	The number of times VitalQIP will retry a GSS TSIG secure dynamic DNS update that fails with a Credential Failure. This option should only be changed on advice from VitalQIP technical support.
GSSAPI Retry Delay	0 to 10000	900 seconds	This option is used when there is a failure sending a GSS TSIG secure dynamic DNS update to a DNS server. It is the number of seconds after the failed update that VitalQIP will wait before sending another GSS TSIG secure dynamic DNS update to the DNS server. This delay should be increased when VitalQIP is spending too much time trying to send GSS TSIG secure dynamic DNS updates to a DNS server that is experiencing transient failures, such as a machine reboot. This delay only applies after the immediate retries specified by the **GSSAPI Immediate Retries** policy.
Kerberos Keytab Path (Unix Only)	*<Filename>*	*/etc/krb5.keytab*	The location of the Kerberos Keytab that contains encrypted principal passwords. Used when VitalQIP performs a Kerberos Initialization before sending GSS TSIG dynamic updates. This option is only used by VitalQIP components running in a Unix environment. The environment variable $QIP_KEYTAB_PATH overrides this option.
PerformKinit (Unix Only)	True or False	False	Indicates whether VitalQIP should perform a Kerberos initialization when sending GSS TSIG dynamic DNS updates. This option is only used by VitalQIP components running in a Unix environment. The environment variable $QIP_DO_KINIT overrides this option.

Policy name	Values	Default value	Usage
Principal Name (Unix Only)			The name of the Kerberos Principal used when VitalQIP performs a Kerberos Initialization before sending GSS TSIG dynamic DNS updates. This option is only used by VitalQIP components running in a Unix environment. The environment variable $QIP_PRINCIPAL_NAME overrides this option.
Static DDNS Update	True or False	True	This policy controls whether RFC 2136 dynamic DNS updates are performed for static objects that are added, modified, or deleted from the GUI. If the option is not found or set to True, then DDNS updates will occur to all DDNS servers assigned to a particular domain (those servers listed in *x.ddns.conf*). **Note:** Dynamic DNS updates come from the VitalQIP Client, not from the Enterprise Server, if the "Use DNS Update Service" policy is set to the default value of False.
Static DNS Mask	Selection from list	All values are selected	This policy is used to set the default DDNS values for static objects. The values selected provide defaults within the GUI as objects are added. They can be overwritten per object at the object level in the Object Profile, as described in "Dynamic DNS Updates" (p. 10-42).
Tombstone Max Life	# DAYS, #HOURS	2 Days, 0 Hours	This policy specifies how long a Tombstoned External object will appear in VitalQIP before it is deleted by the **qip-tombstonepurge** CLI. Tombstoned objects exist in VitalQIP to resolve race conditions that can occur when dynamic DNS create and delete messages arrive at the VitalQIP Update Service in the wrong order. Tombstoned objects do not appear in DNS. Tombstoned resource records are also deleted according to this option, although they do not appear in VitalQIP. The maximum number of days is 31. The maximum number of hours is 23.

Policy name	Values	Default value	Usage
Tombstone Purge Schedule	By Day, By Interval, or None	By Interval, Once per Day	This policy specifies the times of the day that the VitalQIP Message Service should purge tombstoned resource records and objects from the database. If By Interval is selected, the maximum number of days is 31, the maximum number of hours is 23. If By Day is selected, only one purge per hour can be selected. Only six purges per day are permitted. The default is once per day at 1AM.
Update Secondaries	True or False	True	This policy is used to control whether Dynamic DNS Updates are sent to secondary DNS servers. If this policy is set to False, dynamic DNS updates are only sent to primary servers for the zones being updated, and secondary servers are not written to the *ddns.conf* file. When this policy is set to False, secondary servers can get updated DNS data either from zone transfers from a primary server or from a scheduled push from VitalQIP. If this policy is set to True, dynamic DNS updates are sent to both the primary and secondary servers for the zones affected, and both primary and secondary servers are written to the *ddns.conf* file. Set this policy to True to mimic the behavior of VitalQIP 5.X.

Policy name	Values	Default value	Usage
Use DNS Update Service	True or False	False	This policy tells the user interfaces whether to use the VitalQIP DNS Update Service when sending RFC 2136 dynamic DNS updates. When set to False, the user interfaces send RFC 2136 dynamic DNS updates directly to the appropriate DNS servers. Since the update comes from the VitalQIP Client, not from the enterprise server, the client's IP address must appear in the "allow-update" list (entered with the BIND-9.X Use List option in the Domain Profile **Zone Options** tab). When set to True, the user interfaces send the updates in a proprietary format to a VitalQIP Message Service running on the loopback address, or to a VitalQIP Message Service running at the IP address specified by the environment variable **$QIPMESSAGESERVICE**, if set. The VitalQIP Message Service forwards the message to a VitalQIP DNS Update Service if the VitalQIP Message Service is configured with a DNSUpdateObject message route. The VitalQIP DNS Update Service then sends RFC 2136 dynamic DNS update messages to the appropriate DNS servers. **Note:** The environment variable **QIP_USE_DNS_UPDATE_SVC** overrides this policy. If **QIP_USE_DNS_UPDATE_SVC** is set to True, the client sends messages to the DNS Update Service. If set to False, the client sends RFC 2136 updates to the appropriate DNS servers.
Windows 2000 DNS Secure Update Policies			Opens to display the following policies, specifically designed to set up Windows Secure DNS.

Policy name	Values	Default value	Usage
Allow DHCP Clients to Modify Dynamic Object Resource Records	True or False	False	Specifies if control is maintained at the subnet level and if the DNS updates for DHCP clients are to be made. **Note:** To allow Microsoft DHCP clients to send secure updates to a Microsoft DNS server, this policy should be set to True.

Table 2-6 General policies

Policy name	Values	Default value	Usage
ASCII Fully Qualified Name	True or False	True	This policy controls the performance of ASCII validation on a fully qualified hostname in VitalQIP. All the hostnames are checked against the ASCII character set. If this policy is set to **False**, VitalQIP will bypass the hostname ASCII character validation. This is to support the Korean language as well as other international language sets.
Audit Object Access	True or False	False	This policy tracks the objects being accessed in VitalQIP, irrespective of whether the object properties have been modified. This policy controls whether an Audit Manager update message is sent to the Audit Manager when an existing object is displayed in the object profile, irrespective of whether the administrator changed the profile. By default, a message will not be sent to the Audit Manager when modifying an object, if nothing has changed. You need to set this policy to **True** to transmit the message to Audit Manager. If you change the hostname, domain name, IP address or MAC address, a message is sent by the Audit Manager, irrespective of the value that is set for this policy.

Policy name	Values	Default value	Usage
Set Default Servers on Subnet	True or False	True	If this policy is set to True, default servers are assigned. If the policy is set to False, default servers are not assigned, and are left blank.
Allow 16 Character MAC Address	True or False	False	If this policy is set to True, MAC addresses are 16 or 12 characters in length. If False, only MAC addresses 12 characters in length are allowed.
Allow Automatic Reclaim	True or False	False	This policy determines the list of reclaim types that are displayed in VitalQIP when scheduling a reclaim for a subnet. If the policy is set to False, then the only valid reclaim type when scheduling reclaims is Report Only. If the policy is set to True, then the list of valid reclaim types contains Report Only, Reclaim Only, Report and Reclaim.
Allow Dotted Hostnames	True or False	False	When set to True, this policy allows the use of the dot "." in object names. (This indicates that the hostname exists in a subdomain of the object's default domain.) This policy also allows for fully qualified hostnames to be used in searches.

Policy name	Values	Default value	Usage
Allow Duplicate MAC Addresses	True or False	False	MAC addresses are unique identifiers of client hardware network interfaces. This policy governs whether a particular MAC address can have more than one IP address. The default, False, means that a particular MAC address cannot be registered twice. A value of True allows the same MAC address to be registered for another IP address in a new subnet, which might be needed if computer is moved to another location and gets a new address from a DHCP server while its original DHCP lease is still valid. Duplicate MAC addresses are not allowed within the same subnet even if the policy is set to True.
Always Append Router	True or False	True	If this policy is set to True, router objects added to a subnet are automatically added to the default routers list in the Subnet Profile. If this policy is set to False, a router object is not added to the default routers list in the Subnet Profile.
Change Records B-tree Key Size	Numeric	256	This policy represents the size of the b-tree key used in the changed records DNS push. This should only be increased on the advice of VitalQIP technical support or if the error “RR too big for btree key” is generated during a DNS push.
Contact Search	True or False	False	If this policy is set to True, the contact information on the Contact Profile window is not initially loaded with ***all*** data when displayed. **Note:** When large numbers of contacts exist, a False value may affect performance when viewing Contact Profile.

Policy name	**Values**	**Default value**	**Usage**
DNS SOA Serial Number Type	DATE or NODATE	NODATE	This policy defines the format of the serial number in the DNS files. This option applied to serial numbers for BIND 4.9.X servers. If the DATE value is used, the SOA will be ***yyyymmddnn***, where ***nn*** is a sequential number. If the NODATE value is used, the SOA will be a sequential number. For BIND 8.X/BIND 9.X servers including Lucent DNS 3.X and 4.X, an integer is always used (the value NODATE) because the serial number could change many times during a single day, and this prevents the new serial number from being less than the old one.
Delete Lease	True or False	True	This policy determines whether a delete lease should be sent to the server when a dynamic object is deleted. True means that the lease is deleted from the DHCP server whenever a dynamic object is deleted. False means the opposite.
Delete Sites/Subnets from Active Directory	True or False	False	When this policy is set to False, the Domain Controller Generation never tries to delete any information out of Active Directory. Only Sites and Subnets that were added or modified are reflected in Active Directory. When this policy is set to True, the Domain Controller Generation reflects all adds, deletes, and modifies of sites and subnets in Active Directory.
Display All DNS Servers In Subnet Profile	True or False	False	Determines if all DNS servers are displayed in the Subnet Profile or only DNS servers associated with subnets through domains associated with subnets. True enables this policy and False disables this policy.

Policy name	**Values**	**Default value**	**Usage**
FirstIn-LastIn	FIRSTIN or LASTIN	FIRSTIN	This policy takes the place of the external files *last_in.sql* and *first_in.sql*. For more information, refer to the *VitalQIP Administrator Manual*.
Gap Direction	FROM_ START or FROM_END	FROM_ START	This policy is used to determine which Global Allocation Policy (GAP) has precedence in the event that two policies fall on the same address. For example, if you have one GAP defined as 10 from the start and one GAP defined as 245 from the end and they wind up on the same address, this option determines which offset takes precedence.
Generate DNS Records for Dynamic Clients	GENALL or GENUSED	GENALL	The default, GENALL, is to send all entries to DNS during a server push, regardless if they have a MAC address associated with the IP address. This policy applies only to an object defined as dynamic. This policy takes the place of the external files *show_activeonly_dns.sql* and *show_allobject_dns.sql*. If the value is set to GENUSED, only the objects with MAC addresses (for example, dynamic objects assigned a lease) will appear in DNS. Additionally, the lease expiration of the objects is checked so that the objects are only pushed if the lease has not expired. **Note:** If you are creating classless reverse zones (on non-octet boundaries), this option ***must*** be set to GENALL. GENUSED will fail to properly create the CNAME and PTR resource records for the classless reverse zones.

Policy name	Values	Default value	Usage
Generate Simple Unique Names	True or False	True	This policy modifies VitalQIP's behavior when the FirstIn/Lastin policy specifies that a DHCP lease should be renamed. When this policy is True, the lease's address is appended to the current host name, for example `host-270000000001.example.com`. When this policy if False, the lease's host name will be determined by the appropriate naming policy, for example `host udp000001uds.example.com`. Naming policy based names are more expensive to compute, and can slow down the VitalQIP QIP Update Service.
Location Search	True or False	False	If this policy is set to True, the location information on the Location Profile window is not initially loaded with ***all*** data when displayed. **Note:** When large numbers of locations exist, a False value may affect performance when viewing Location Profile.
Match CIDR Netmask On Reverse Zone	True or False	False	Determines if reverse zones have the same netmask as the CIDR network. If this policy is set to False, a CIDR network is created, and the reverse zones that are created “fall” on the network class boundaries. If a network is created and the Support CIDR checkbox in the Network Profile is not checked, the reverse zones are created using class boundaries. If this policy is set to True, a CIDR network is created and the reverse zone that is created will have the same netmask as the CIDR network.

Policy name	**Values**	**Default value**	**Usage**
Name Validation	DNS_COMPLIANT or None	None	If this policy is set to DNS_COMPLIANT, the object names: • Can be up to 63 characters long • Can contain alphanumeric characters and dashes (-) • Cannot have a dash (-) as the first and last character • Cannot consist of only numeric values If this policy is None, object names can be up to 63 characters in length, and may contain alphanumeric characters, underscores (_), dashes (-), plus signs (+) and exclamation points (!). The first character of object must be alphanumeric and the last character of an object must not be a dash (-). This policy affects only the object names entered in the VitalQIP GUI, not names passed by DHCP clients. It is checked when an object is created and an Object Name is assigned through the Object Profile.
Password Masking	ALWAYS_ ON, OFF, or ON	ALWAYS_ ON	This policy defines the default value for Password Masking in the User Profile. Password Masking is whether or not asterisks (*) display in place of a typed password, masking it from view. **ALWAYS_ON**: The password is always masked in the User Profile. **OFF**: The password is always unmasked in the User Profile. **ON**: The Password Mask can be turned on and off by the user in the User Profile.

Policy name	Values	Default value	Usage
Ping Attempts	Numeric (1-10)	1	This policy governs the behavior of VitalQIP when defining the number of pings that are attempted during Reclaim and when using the Ping function in the Object Management window. The selected IP address is pinged for the number of times set by this policy before it is categorized as unreachable/not in use if it does not respond. If it does respond, it is immediately categorized as In Use. Setting a high number of Ping Attempts or a long "Ping Retry Delay" ensures that IP addresses that are in use will not be wrongly identified as Not In Use. The operation will take longer to complete, however. (Ping attempts for Ping-before-Assign of DHCP Servers is defined in the DHCP Server Profile.)
Ping Retry Delay	Numeric (10-2000)	20	This value determines the time, in milliseconds, the system delays before sending another ping. This is only valid when "Ping Attempts" is set to greater than 1.
Ping Timeout	Numeric (10-2000)	500	This value determines the time, in milliseconds (500=1/2 of a second), the system waits for a response from a ping.

Policy name	**Values**	**Default value**	**Usage**
Protect MDHCP/Bootp Objects	True or False	False	If this policy is set to True, a Manual DHCP/Bootp object that already exists in the database, is protected from a dynamic object lease update coming into the database which conflicts with the name of the Manual DHCP/bootp object. The manual object keeps its name, and the dynamic object coming into the database gets a generated unique name. Additionally, updates coming from the DHCP server into the VitalQIP database via the QIP Update Service for Manual DHCP/Bootp objects will not occur in the database. The Manual DHCP/Bootp object name in the database takes precedence and the updates will not occur. If the policy is set to False, the **FIRSTIN/LASTIN** policy determines which object keeps its name.
Remote Server Proxy	IP Address List	0.0.0.0	This policy specifies the proxy servers to be used when VitalQIP connects to the remote server. If left blank, VitalQIP uses the same address as the remote server. The use of a proxy server makes administration of firewalls easier since it limits the number of ports open on the remote server.
Send AC Updates to DHCP	True or False	True	If set to False, prevents dynamic update messages on MAC-User Class mappings from being sent from the DHCP server to the AC Cache Service.

Policy name	**Values**	**Default value**	**Usage**
Subnet Multiple Application Access	True or False	False	This policy determines if an administrator can add objects associated with other applications to subnets. By default, if an administrator has access to a subnet only through a specific application, that administrator cannot add objects to subnets that are associated with any other application. If this policy is set to True, the administrator can add objects associated with other applications.
Support VLSM in NIS Generation	True or False	False	If set to True, this policy allows for VLSM masks and CIDR-style subnets in the NIS files (per RFC 1519). If set to False, only the network and the mask of the first subnet are written to the netmasks file.
User Name Exit	True or False	False	False indicates a user-defined naming policy user exit will not be supported. For more information, refer to "User-defined object naming policy user exit" (p. 2-7).
Validate CNAME Records	See policies below	See polices below	The following sub-policies determine if VitalQIP validates data to prevent CNAME conflicts. Validation checks help prevent CNAME errors on the DNS server. Zones with such errors are not loaded, or are rejected by the DNS server.
Validate CNAMES against Aliases	True or False	True	Validates CNAME records against IPv4 object alias names.
Validate CNAMES against Domains	True or False	True	Validates CNAME records against domain names.
Validate CNAMES against ENUM NAPTRs	True or False	True	Validates CNAME records against ENUM NAPTR records.
Validate CNAMES against IPV4 Objects	True or False	True	Validates CNAME records against IPv4 object hostnames.

Policy name	Values	Default value	Usage
Validate CNAMES against IPV6 Objects	True or False	True	Validates CNAME records against IPv6 object hostnames (node names).
Validate CNAMES against Resource Records	True or False	True	Validates CNAME records against Object, Domain and Reverse Zone Resource Record owner names.
Validate Domain on Move	True or False	False	This option checks to see if the domain that an object belongs to is associated with the target subnet during a move operation. If set to False, a moved object will take on the default domain of the target subnet if its domain is not associated with the target subnet. If set to True, determines whether the domain to which an object belongs in the current subnet is associated with the target subnet. If no association exists, an error message appears indicating that the domain is invalid in the target subnet. You may change the move parameters in the Object Move screen or cancel the move.

Table 2-7 Report policy

Policy name	Values	Default value	Usage
Object Name Length	Numeric	96	This policy defines the maximum length of characters of the Object Names and aliases to print in the subnet reports. Object Names are right truncated.

3 MyView management

Overview

Purpose

This chapter describes how to use MyView Management.

Contents

This chapter covers these topics.

MyView administration

Overview

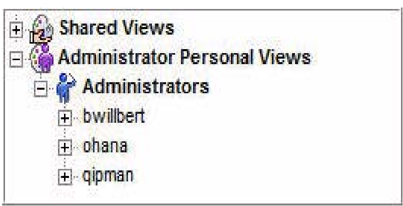
Purpose

With the possibility of millions of address pools, blocks, domains, resource records and infrastructure objects, the amount of data in the VitalQIP database can become quite unwieldy for administrators who need to perform their daily tasks efficiently. MyView Hierarchy Management enables a master or organization administrator to define and set up views of the system that have a narrower scope, views that can then be assigned to one or more normal administrators, and thereby allow them to focus on their daily activities and only the infrastructure items for which they are responsible.

Personal Views

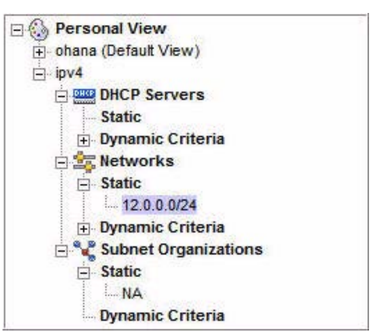
The MyView Management Hierarchy page is split into two areas: **Shared Views** and **Administrator Personal Views**.

Figure 3-1 Sample Personal Views



Each administrator defined in the VitalQIP database has a default Personal View that is created when an administrator logs into VitalQIP for the first time. The Personal View has the same name as an administrator's Login Name, and contains the infrastructure types that have been assigned to his or her Managed List or Administrative Roles, as described in "Add Managed Lists" (p. 6-16) and "Create an administrative role" (p. 6-29).

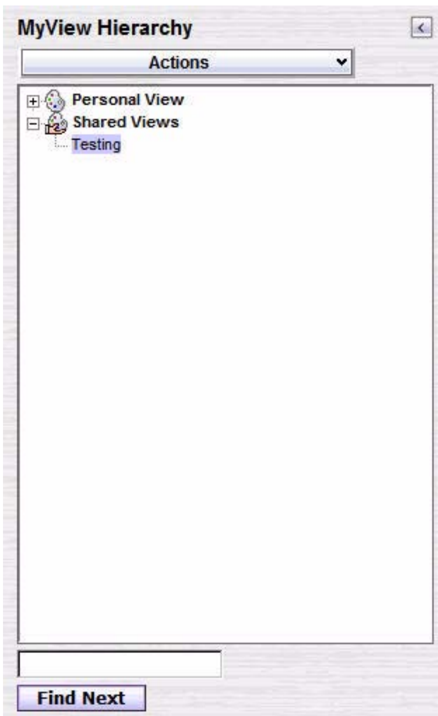
Figure 3-2 Sample Personal View infrastructure types



Shared Views

Because the VitalQIP database can contain many infrastructure types that cannot be added to a Managed List (for example, address pools, IPv6 seed blocks, IPv6 address ranges, IPv6 subnets, and nodes), a master or organization administrator can create "shared views" that contain these additional infrastructure types and assign them to normal administrators. Once assigned to an administrator, the shared view appears in the MyView Hierarchy under **Shared Views** the next time the administrator logs in.

Figure 3-3 Shared Views



When creating a shared view, the administrator specifies the following:

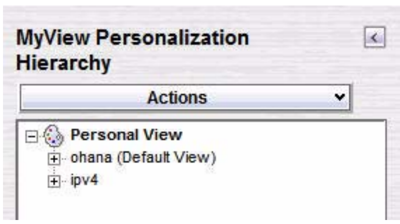
- Types of objects to be included.
- Static objects to be included.
- One or more dynamic criteria (at most eight) to select objects from the database which includes a limited number of static attributes and user defined attributes.
- Other Shared Views to be included.
- Default order in which the shared views and infrastructure types are presented in the MyView Hierarchy. Administrators can later change the default order with the **Order Infrastructure** function on the **Actions** menu.

A user is allowed to traverse down the hierarchy of objects within the shared view, but not traverse up beyond the object included in the shared view (for example, if `Pool_1` is included in the view, the user can access all the pools under `Pool_1`, but not the parent of `Pool_1` or above, nor the siblings of `Pool_1)`.

MyView Personalization Hierarchy

The MyView Personalization Hierarchy offers a grouping mechanism for administrators to see a partial or subset of data that they can access. All administrators can create personal views. The following is a sample MyView Personalization Hieraracy.

Figure 3-4 Sample MyView Personalization Hierarchy



Permissions for the new object types

The master administrator can prevent normal administrators from adding new root level instances to the tree (for example, a seed pool, an IPv6 seed block, or a node) by setting the **Maintain Pools**, **Maintain Seed Pools**, **Access V6 Address Management**, and **Access Node Management** privileges to false in the Administrator Profile.

Only master administrator and organization administrators are allowed to maintain or view Address Templates, Internet Registries, Subnet Profile Templates and Reverse Zone Templates.

Create a shared view

Purpose

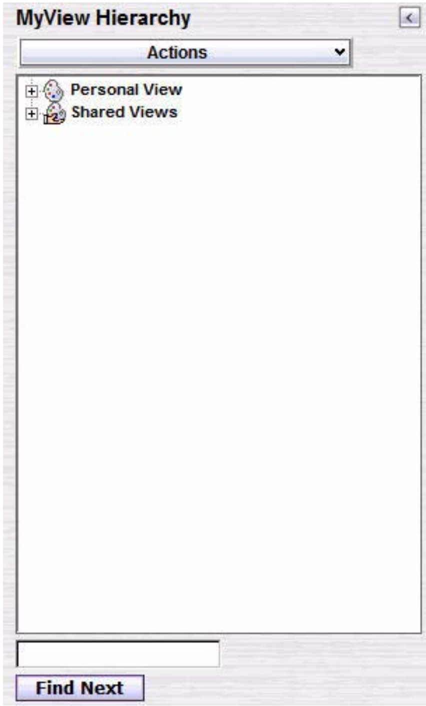
To create a shared view.

Procedure

To create a shared view, follow these steps.

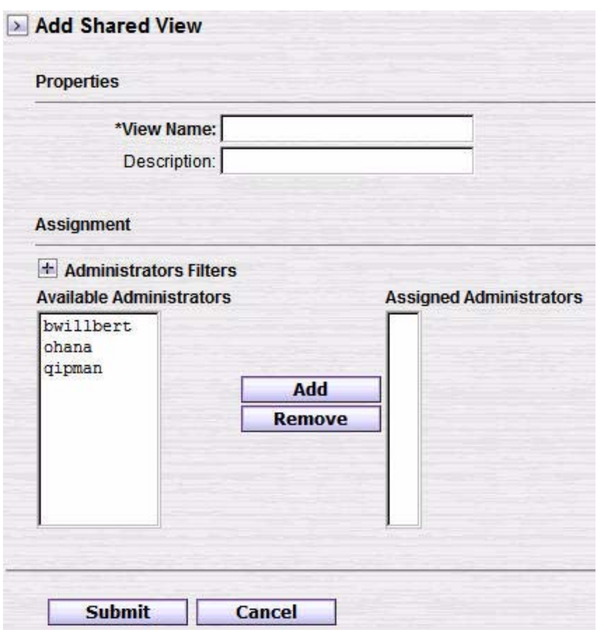
1 Mouse over **Infrastructure** and click **MyView Management**.

Result: The MyView Management Hierarchy opens.



2 Mouse over the **Actions** menu and select **Add a Shared View**.

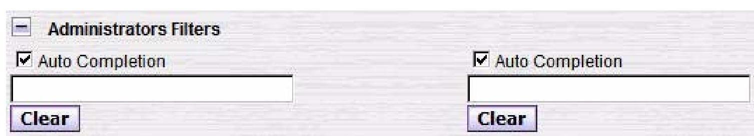
Result: The Properties page opens.



3 ***Required***. Enter a name of up to 64 alphanumeric characters for the shared view in the **Shared View Name** field.

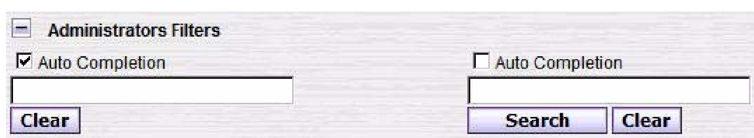
4 Enter a description of up to 255 alphanumeric characters for the shared view in the **Description** field.

5 Choose one of the following actions.

If you want to ...	Then..
Assign administrators	1. Select the administrators you want to assign to the shared view from the **Available Administrators** list. To select multiple administrators, use **Ctrl** or **Shift** as you click on administrator IDs. 2. Click **Add**. **Result:** The selected administrators appear in the **Assigned Administrators** list.
Filter administrators ***automatically*** before assigning them	1. Expand the **Administrators Filters** section. **Result:** The Filter fields appear with the **Auto Completion** check box checked.  2. Enter your search criteria in the Search field above the **Available Administrators** list. **Result:** The Administrator IDs in the **Available Administrators** list are automatically filtered as you type. To cancel a search criterion, click **Clear**. 3. Select the administrators you want to assign to the shared view from the **Available Administrators** list. To select multiple administrators, use **Ctrl** or **Shift** as you click on administrator IDs. 4. Click **Add**. **Result:** The selected administrators appear in the **Assigned Administrators** list.

<table>
<tr><th>If you want to ...</th><th>Then..</th></tr>
<tr><td>Filter administrators manually before assigning them</td><td>1. Expand the Administrators Filters section.
Result: The Filter fields appear with the Auto Completion check box checked.
2. Uncheck the Auto Completion check box above the Available Administrators list.
Result: A Search button appears.


3. Enter your search criteria.
To cancel a search criterion, click Clear.
4. Select the administrators you want to assign to the shared view from the Available Administrators list. To select multiple administrators, use Ctrl or Shift as you click on administrator IDs.
5. Click Add.
Result: The selected administrators appear in the Assigned Administrators list.</td></tr>
<tr><td>Remove administrators from the shared view</td><td>1. Select the administrator you want to remove from the shared view from the Assigned Administrators list.
2. Click Remove.
Result: The selected administrator is removed from the Assigned Administrators list.
3. Repeat the above steps to remove other administrators from the list.</td></tr>
</table>

If you want to ...	**Then..**
Filter administrators ***automatically*** before removing them	1. Expand the **Administrators Filters** section. **Result:** The Filter fields appear with the **Auto Completion** check box checked. 2. Enter your search criteria in the **Search** field above the **Assigned Administrators** list. **Result:** The Administrator IDs in the **Assigned Administrators** list are automatically filtered as you type. To cancel a search criterion, click **Clear**. 3. Select the administrator you want to remove from the shared view from the **Assigned Administrators** list. 4. Click **Remove**. **Result:** The selected administrator is removed from the **Assigned Administrators** list. 5. Repeat the above steps to remove other administrators from the list.
Filter administrators ***manually*** before removing them	1. Expand the **Administrators Filters** section. **Result:** The Filter fields appear with the **Auto Completion** check box checked. 2. Uncheck the **Auto Completion** check box above the **Assigned Administrators** list. **Result:** A **Search** button appears.  3. Enter your search criteria. To cancel a search criterion, click **Clear**. 4. Select the administrators you want to remove from the shared view from the **Assigned Administrators** list. To select multiple administrators, use **Ctrl** or **Shift** as you click on administrator IDs. 5. Click **Add**. **Result:** The selected administrator is removed from the **Assigned Administrators** list. 6. Repeat the above steps to remove other administrators from the list.
Add user defined attributes to a shared view	1. Expand the **Attributes** section, if necessary. 2. Enter attribute values as needed.

6 Click **Submit**.

Result: The shared view is created and a confirmation dialog opens with the message **Shared View successfully created**.

7 Click **OK** to confirm.

Result: The Properties page is refreshed with a summary of the properties and a new set of buttons.

END OF STEPS

Create a personal view

Purpose

To create a personal view.

Before you begin

- Only legacy infrastructure types, subject to the Administrator's Access Control List can be added to a personal view
- A personal view cannot be assigned to other administrators
- A personal view cannot contain another personal view.

Procedure

To create a Personal View, follow these steps:

1 Mouse over **MyView** and click **MyView Personalization**.

Result: The MyView Personalization Hierarchy opens.

2 Mouse over the **Actions** menu and click **Add Personal View**.

Result: The Add Personal View page opens.

3 Enter the appropriate values in the field. Refer to the following table for descriptions of the fields.

Table 3-1 Add Personal View fields

Field	Description
Personal View Name	***Required.*** Name for the Personal View.
Description	***Optional.*** Description for the Personal View.

4 Click **Submit**.

Result: A dialog box opens with the message **Personal View successfully created**.

5 Click **OK**.

END OF STEPS

Add contents to a view

Purpose

Use this procedure to add content to a shared or personal view.

Procedure

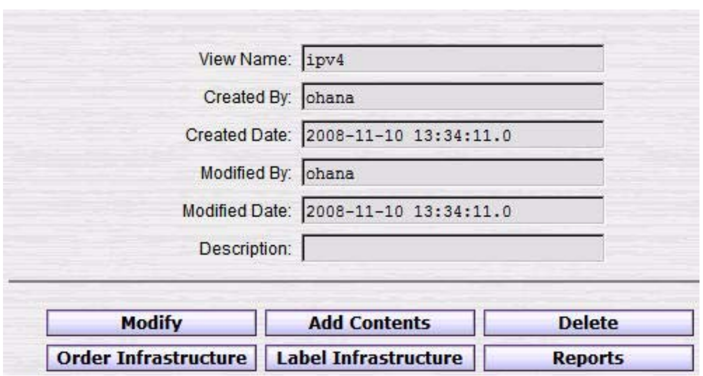
To add content to a shared view, follow these steps.

1 Choose one of the following actions.

If you are...	Then...
Adding content to a shared view	1. Mouse over **Infrastructure** and click **MyView Management**. **Result:** The MyView Management Hierarchy opens. 2. Expand **Shared Views**. **Result:** A list of shared views appear.
Adding content to a personal view	1. Mouse over **MyView** and click **MyView Personalization**. **Result:** The MyView Personalization Hierarchy opens. 2. Expand the hierarchy until you come to the personal view to add content.

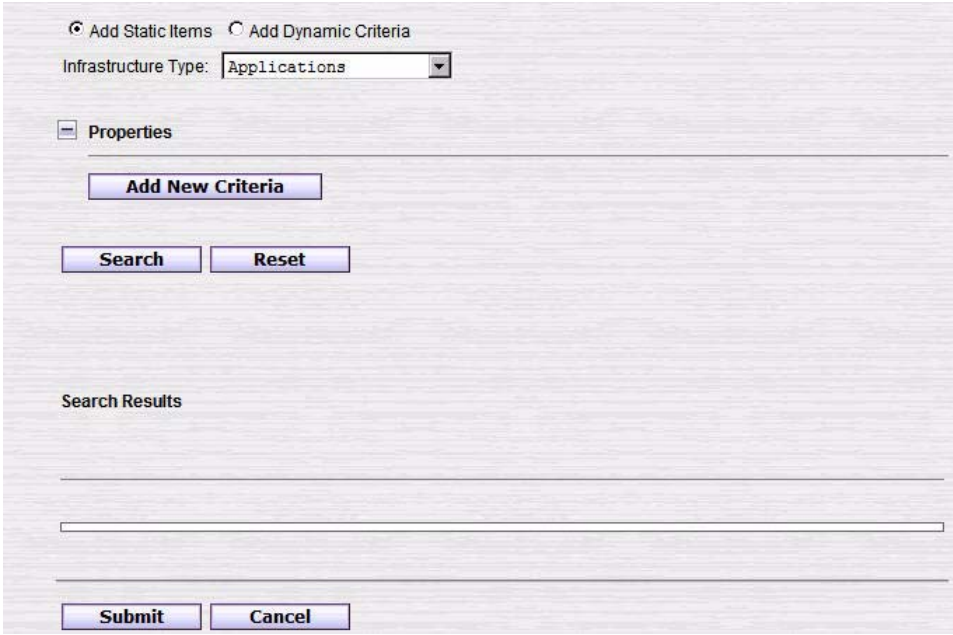
2 Select the view to which you want to add content.

Result: The Personal View Properties or Shared View Properties page opens.



3 Click **Add Contents**.

Result: The Add Contents page opens.



4 Decide whether to add content individually or dynamically.

- To add content item by item, click the **Add Static Items** option.
- To add content dynamically, click the **Add Dynamic Criteria** option.

5 Select an infrastructure type from the **Infrastructure Type** drop-down list. The following table shows the infrastructure types and for what views they are available.

Note: **Address Pools**, I**Pv4 Reverse Zones**, I**Pv6 Address Ranges**, **IPv6 Reverse Zones**, **IPv6 Seed Blocks**, **IPv6 Subnets**, **Nodes**, and **Shared Views** are selectable only for Shared Views and are not displayed when a Personal View is modified.

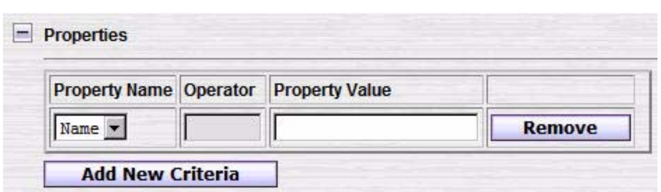
Table 3-2 Available infrastructure types

Infrastructure type	Available in Shared View	Available in Personal View	Notes
Address Pools	X		
Applications	X	X	
BootP Servers	X	X	
DHCP Servers	X	X	

Infrastructure type	Available in Shared View	Available in Personal View	Notes
DNS Servers	X	X	
Forward Zones	X	X	
IPv4 Address Ranges	X	X	
IPv4 Object Ranges	X	X	
IPv4 Reverse Zone	X		
IPv4 Subnets	X	X	
IPv6 Address Ranges	X		
IPv6 Reverse Zones	X		
IPv6 Seed Blocks	X		
IPv6 Subnets	X		
Local Hosts	X	X	
Networks	X	X	
NIS Servers	X	X	
Nodes	X		Choose either the **IPv4 Criteria** or the **IPv6 Criteria** option.
OSPF Areas	X	X	
Shared Views	X		
Subnet Organizations	X	X	

6 To search or preview infrastructure properties, click **Add New Criteria** in the **Properties** section. You may enter up to ten criteria.

Result: Properties criteria fields open.



Property names vary depending on the infrastructure type selected. The following table details the properties available for each infrastructure type.

Table 3-3 Infrastructure type properties

Infrastructure type	Property name	Search values
Address Pools		
	Address Pool Name	String, wildcard
	Parent Pool Name	String, wildcard
	Registry	String, wildcard
	Contact	E-mail address, wildcard
	Address Pool Type	Seed Pool, Child Pool
	IPv4 Allocation Rule	String, wildcard
	IPv6 Allocation Rule	String, wildcard
Applications		
	Name	String, wildcard
Bootp Servers		
	Name	String, wildcard
	IPv4 Address	IPv4 address, wildcard
DHCP Servers		
	Name	String, wildcard
	IPv4 Address	IPv4 address, wildcard
	Server Type	Pick list
DNS Server		
	Name	String, wildcard
	IPv4 Address	IPv4 address, wildcard
	Server Type	Pick list
Forward Zones		
	Name	String, wildcard
IPv4 Address Ranges		
	Network Address	IPV4 address, wildcard
	Network Name	String, wildcard
IPv4 Object Ranges		
	Subnet Address	IPV4 address, wildcard

Infrastructure type	Property name	Search values
	Subnet Name	String, wildcard
IPv4 Reverse Zone		
	Name	String, wildcard
IPv4 Subnets		
	Name	String, wildcard
	Subnet Address	IPV4 address, wildcard
	Network Address	IPV4 address, wildcard
	Network Name	String, wildcard
	Subnet Organization	String, wildcard
	OSPF Area	String, wildcard
	Forward Zone Name	String, wildcard
IPv6 Address Ranges		
	Name	String, wildcard
	Start Address	IPv6 address, wildcard
	Length	Boolean operators: =, >, >=, <, <=
		Pull-down values: 9 to 128
IPv6 Reverse Zone		
	Name	String, wildcard
IPv6 Seed Blocks		
	Length	Boolean operators: =, >, >=, <, <=
		Pull-down values: 9 to 128
	Address Block	IPv6 address, wildcard
IPv6 Subnets		
	Name	String, wildcard
	Start Address	IPv6 address, wildcard
	Length	Boolean operators: =, >, >=, <, <=
		Pull-down values: 9 to 128
Local Hosts		
	Name	String, wildcard

Infrastructure type	Property name	Search values
	IPv4 Address	IPv4 address, wildcard
Networks		
	Name	String, wildcard
	Network Address	IPV4 address, wildcard
NIS Servers		
	Name	String, wildcard
	IPv4 Address	IPv4 address, wildcard
Nodes		
IPv4 attributes		
	IP Object Name	String, wildcard
	IPv4 Object MAC Address	String, wildcard
	IPv4 Address	IPv4 address, wildcard
IPv6 attributes		
	Node Type	A list of Workstation, X-terminal, PC, Printer, Server, Wiring_HUB, Router, Bridge, Terminal Server, Switch, Legacy_System, Gateway, Test_Equipment, Undefined, Others, Partially_Managed, and user-defined object classes.
	Node Name	String, wildcard
	Node Unique ID	String, wildcard
	Node Description	String, wildcard
	Interface Name	String, wildcard
	Interface MAC Address	String, wildcard
	IPv6 Address Name	String, wildcard
	IPv6 Address	IPv6 address, wildcard
	Domain Name	String, wildcard

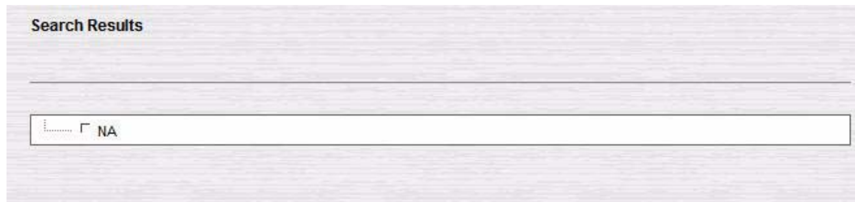
Infrastructure type	Property name	Search values
Shared Views		
	MyView Name	String, wildcard **Note:** If the **Add Dynamic Criteria** option is selected, be careful not to create a circular relationship between shared views (for example where `view1` contains `view2`, and where `view2` contains `view1`): for performance reasons, the UI does not check for such relationships. If the **Add Static Items** option is selected, the UI does check for circular relationships, and returns an error message if you try to create such a relationship. You can also prevent circular relationship checks with the **`CircularMyViewCheck`** policy. Refer to the *Administrator Reference Manual* for more information.
Subnet Organization		
	Name	String, wildcard

7 Enter the desired property criterion for the selected infrastructure type. If you decide not to use the criterion you entered, click **Remove**.

8 If required, click **Add New Criteria** to select another property criterion.

9 If User Defined Attributes or User Defined Fields are assigned to the infrastructure type, the **User Defined Attributes** or **User Defined Fields** section are displayed. Refer to "Working with user defined attributes and fields" (p. 7-23) more information.

10 Choose one of the following actions.

If ...	**Then ...**
Available for UDAs only. **Add Static Items** option is selected	Click **Search**. **Result:** The **Search Results** section opens. If the search results list as folders, you can select specific folders or expand them and select individual objects as you wish. 
Add Dynamic Criteria option is selected	Click **Preview**. **Result:** The **Search Results** section opens. 

11 Choose one of the following actions.

If ...	**Then ...**
Add Static Items option is selected, and you are satisfied with the results of your search criteria	1. ***UDAs only.*** Place check marks in the items that you want to include in the shared view. 2. Click **Submit**. **Result:** A confirmation dialog opens with the message **Infrastructure Objects successfully added**. 3. Click **OK**. **Result:** The hierarchy is updated.

If ...	Then ...
Add Dynamic Criteria option is selected, and you are satisfied with the results of the preview	1. Click **Submit**. **Result:** A confirmation dialog opens with the message **Infrastructure Objects successfully added**. 2. Click **OK**. **Result:** The hierarchy is updated.
Add Static Items option or **Add Dynamic Criteria** option is selected, and you are ***not*** satisfied with the results of your search criteria	1. Click **Reset**. **Result:** All search criteria fields are closed, and the contents of the **Search Results** section are erased. 2. Repeat Step 6 to Step 10.

12 If at any time you wish to leave this function without selecting criteria, click **Cancel**.

Result: The Personal View Properties or Shared View Propertiespage for the selected view opens.

END OF STEPS

Modify a shared view

Purpose

Use this procedure if you want to add/delete administrators who can access a shared view.

Procedure

To modify a shared view, follow these steps.

1 Mouse over **Infrastructure** and click **MyView Management**.

Result: The MyView Management Hierarchy opens.

2 Expand **Shared Views**.

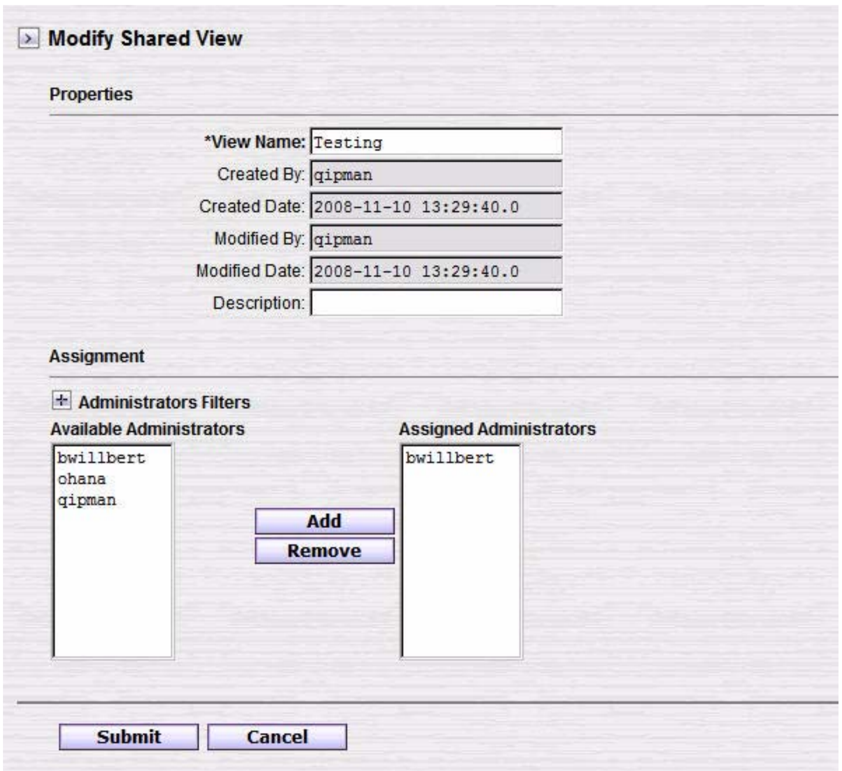
Result: A list of shared views appears.

3 Select the view that you want to modify.

Result: The Properties page opens.

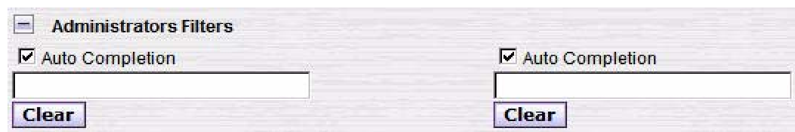
4 Click **Modify**.

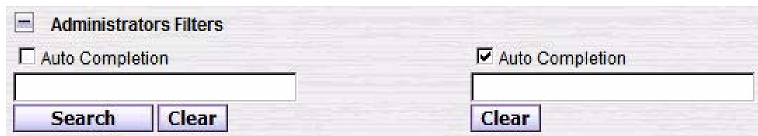
Result: The Properties page expands.



5 Choose one of the following actions.

If you want to...	Then...
Revise the name of the shared view	Enter a new name of up to 64 alphanumeric characters in the **Shared View Name** field.
Revise the Description for the shared view	Enter a new description of up to 255 alphanumeric characters for the shared view in the **Description** field.

If you want to…	**Then…**
Assign administrators	1. Select the administrators you want to assign to the shared view from the **Available Administrators** list. To select multiple administrators, use **Ctrl** or **Shift** as you click on administrator IDs. 2. Click **Add**. **Result:** The selected administrators appear in the **Assigned Administrators** list.
Filter administrator IDs ***automatically*** before assigning them	1. Expand the **Administrators Filters** section. **Result:** The Filter fields appear with the **Auto Completion** check box checked.  2. Enter your search criteria in the Search field above the **Available Administrators** list. **Result:** The Administrator IDs in the **Available Administrators** list are automatically filtered as you type. To cancel a search criterion, click **Clear**. 3. Select the administrators you want to assign to the shared view from the **Available Administrators** list. To select multiple administrators, use **Ctrl** or **Shift** as you click on administrator IDs. 4. Click **Add**. **Result:** The selected administrators appear in the **Assigned Administrators** list.

If you want to...	Then...
Filter administrator IDs ***manually*** before assigning them	1. Expand the **Administrators Filters** section. **Result:** The Filter fields appear with the **Auto Completion** check box checked. 2. Uncheck the **Auto Completion** check box above the **Available Administrators** list. **Result:** A **Search** button appears.  3. Enter your search criteria. To cancel a search criterion, click **Clear**. 4. Select the administrators you want to assign to the shared view from the **Available Administrators** list. To select multiple administrators, use **Ctrl** or **Shift** as you click on administrator IDs. 5. Click **Add**. **Result:** The selected administrators appear in the **Assigned Administrators** list.
Remove administrator IDs from the shared view	1. Select the administrator you want to remove from the shared view from the **Assigned Administrators** list. 2. Click **Remove**. **Result:** The selected administrator is removed from the **Assigned Administrators** list. 3. Repeat the above steps to remove other administrators from the list.

If you want to...	Then...
Filter administrator IDs ***automatically*** before removing them	1. Expand the **Administrators Filters** section. **Result:** The Filter fields appear with the **Auto Completion** check box checked. 2. Enter your search criteria in the Search field above the **Assigned Administrators** list. **Result:** The Administrator IDs in the **Assigned Administrators** list are automatically filtered as you type. To cancel a search criterion, click **Clear**. 3. Select the administrator you want to remove from the shared view from the **Assigned Administrators** list. 4. Click **Remove**. **Result:** The selected administrator is removed from the **Assigned Administrators** list. 5. Repeat the above steps to remove other administrators from the list.
Filter administrator IDs ***manually*** before removing them	1. Expand the **Administrators Filters** section. **Result:** The Filter fields appear with the **Auto Completion** check box checked. 2. Uncheck the **Auto Completion** check box above the **Assigned Administrators** list. **Result:** A **Search** button appears.  3. Enter your search criteria. To cancel a search criterion, click **Clear**. 4. Select the administrators you want to remove from the shared view from the **Assigned Administrators** list. To select multiple administrators, use **Ctrl** or **Shift** as you click on administrator IDs. 5. Click **Add**. **Result:** The selected administrator is removed from the **Assigned Administrators** list. 6. Repeat the above steps to remove other administrators from the list.

If you want to...	Then...
Modify attributes assigned to a shared view	1. Expand the **Attributes** section, if necessary. 2. Enter revised attribute values.

6 Click **Submit**.

Result: The shared view is created and a confirmation dialog opens with the message **Shared View successfully modified**.

7 Click **OK** to confirm.

Result: The Properties page is refreshed with a summary of the properties.

END OF STEPS

Modify a personal view

Purpose

Use this procedure to modifying a personal view.

Procedure

To modify a personal view, follow these steps:

1 Mouse over **MyView** and click **MyView Personalization**.

Result: The MyView Personalization Hierarchy opens.

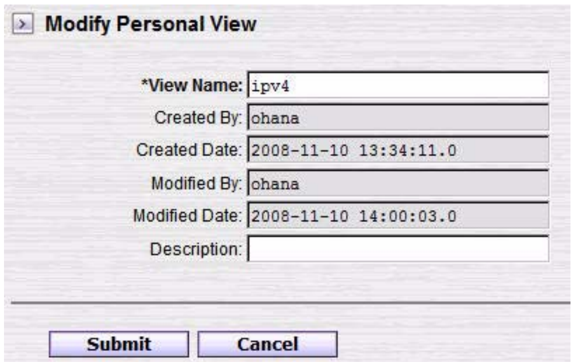
2 Expand the hierarchy until you come to the view you want to change.

3 Select the view.

Result: The Personal View Properties page opens,

4 Click **Modify**.

Result: The Modify Personal View page opens.



5 Make the necessary changes. Refer to "Add Personal View fields" (p. 3-10) for more informtation.

6 Click **Submit**.

Result: A dialog box opens with the message **Personal View successfully modified**.

7 Click **OK**.

END OF STEPS

Delete a view

Purpose

Use this procedure to delete a shared or personal view.

Before you begin

Default personal views cannot be deleted.

Procedure

To delete a view, follow these steps.

1 Choose one of the following actions.

If you are...	Then...
Deleting a shared view	1. Mouse over **Infrastructure** and click **MyView Management**. **Result:** The MyView Management Hierarchy opens. 2. Expand **Shared Views**. **Result:** A list of shared views appears.
Deleting a personal view	1. Mouse over **MyView** and click **MyView Personalization**. **Result:** The MyView Personalization Hierarchy opens.

2 Select the view that you want to delete.

Result: The Properties page opens.

3 Click **Delete**.

Result: A confirmation dialog opens with the message **You are about to delete** *<Shared or Personal>* **View -** *<ViewName>*.

4 Click **OK** to continue.

Result: A confirmation dialog opens with the message *<Shared or Personal>* **View successfully deleted** and the MyView Management Hierarchy is refreshed.

5 Click **OK**.

Result: The VitalQIP IP Management Software splash screen is displayed.

END OF STEPS

Order infrastructure

Purpose

To set up the order in which infrastructure appears in a shared or personal view.

Before you begin

- Once the order is established, this will be the default order in the MyView page. Users can personalize their MyView infrastructure, however.
- When a shared view is added to another shared view, the shared view is listed before infrastructure types by default. This design allows the user to navigate the views in the MyView Management Hierarchy without having to traverse through infrastructure types.

Procedure

To order the infrastructure, follow these steps.

1 Choose one of the following actions.

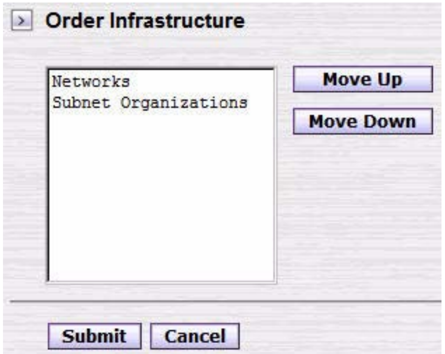
If you are…	Then…
Ordering a shared view	1. Mouse over **Infrastructure** and click **MyView Management**. **Result:** The MyView Management Hierarchy opens. 2. Expand **Shared Views**. **Result:** A list of shared views appears.
Ordering a personal view	1. Mouse over **MyView** and click **MyView Personalization**. **Result:** The MyView Personalization Hierarchy opens. 2. Expand the hierarchy until you come to a personal view.

2 Select a view.

Result: The Properties page opens.

3 Click **Order Infrastructure**.

Result: The Order Infrastructure page opens.



4 Choose one of the following actions.

If you want to ...	Then ...
Move an infrastructure type up the hierarchy order	1. Highlight the infrastructure type you wish to move. 2. Click **Move Up** until the infrastructure type is positioned where you want it. 3. Click **Submit**. **Result:** The hierarchy is updated and the Properties page opens.
Move an infrastructure type down the hierarchy order	1. Highlight the infrastructure type you wish to move. 2. Click **Move Down** until the infrastructure type is positioned where you want it. 3. Click **Submit**. **Result:** The hierarchy is updated and the Properties page opens.

END OF STEPS

Label infrastructure

Purpose

To modify infrastructure labels.

Before you begin

Once the labels are established, these will be the default labels in the MyView page. Users can personalize their MyView infrastructure, however.

Procedure

To change the label on infrastructure items, follow these steps.

1 Choose one of the following actions.

If you are...	Then...
Labeling infrastructure for a shared view	1. Mouse over **Infrastructure** and click **MyView Management**. **Result:** The MyView Management Hierarchy opens. 2. Expand **Shared Views**. **Result:** A list of shared views appears.
Labeling infrastructure for a personal view	1. Mouse over **MyView** and click **MyView Personalization**. **Result:** The MyView Personalization Hierarchy opens. 2. Expand the hierarchy until you come to a personal view.

2 Select the view for which you want to label the infrastructure.

Result: The Properties page opens.

3 Click **Label Infrastructure**.

Result: The Label Infrastructure page opens.

4 Select the label you wish to modify and enter a new label.

5 Repeat as needed for other infrastructure types.

6 Click **Submit**.

Result: The MyView Management Hierarchy is updated and the Properties page opens.

END OF STEPS

Modify selection criteria

Purpose

Use this procedure to modify selection criteria for infrastructure types that were dynamically selected for a shared or personal view.

Procedure

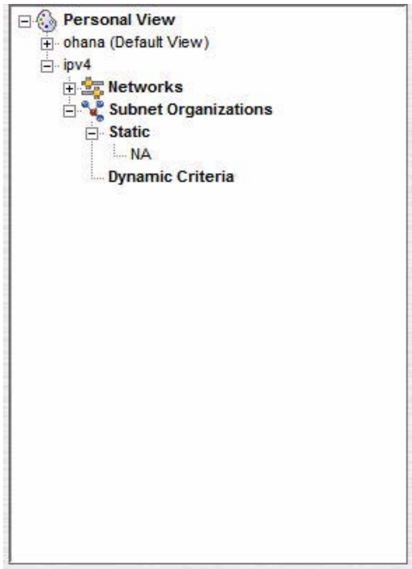
To modify the selection criteria for an infrastructure type that was dynamically selected to a shared view, follow these steps.

1 Choose one of the following actions.

If you are…	Then…
Modifying criteria for a shared view	1. Mouse over **Infrastructure** and click **MyView Management**. **Result:** The MyView Management Hierarchy opens. 2. Expand **Shared Views**. **Result:** A list of shared views appears.
Modifying criteria for a personal view	1. Mouse over **MyView** and click **MyView Personalization**. **Result:** The MyView Personalization Hierarchy opens. 2. Expand **Personal Views**. **Result:** A list of personal views appears.

2 Expand the view that you want to modify.

Result: The list of infrastructure types opens.

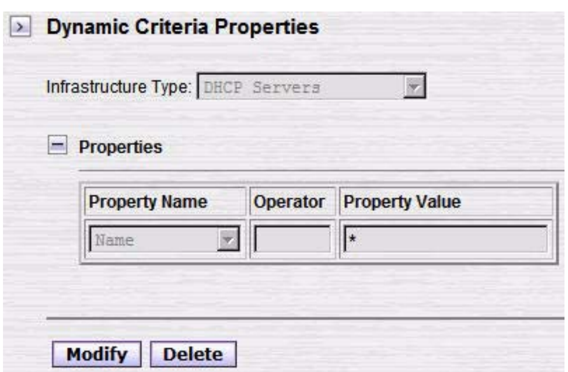


3 Expand the infrastructure type whose dynamic criteria you wish to modify.

Result: The **Static** and **Dynamic Criteria** labels open.

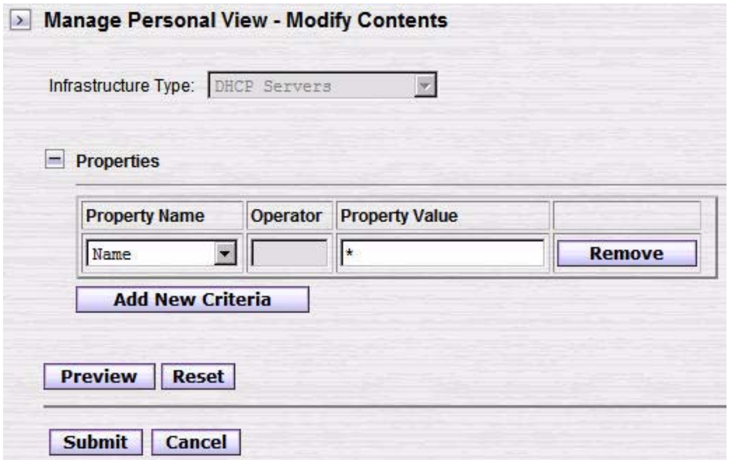
4 Expand **Dynamic Criteria** and select the criteria you wish to modify.

Result: The Properties page for the selected infrastructure type opens.



5 Click **Modify**.

Result: The Manage Shared View - Modify Contents page opens.



6 Add or remove criteria from the **Properties** and **User Defined Attributes** sections as needed. For further information, refer to "Add contents to a view" (p. 3-10).

7 Click **Submit** to save your modified criteria.

Result: A confirmation dialog opens with the message **Dynamic Criteria successfully modified**.

8 Click **OK**.

Result: The Dynamic Criteria Properties page for the selected infrastructure type opens.

END OF STEPS

Delete selection criteria

Purpose

Use this procedure to delete static or dynamic selection criteria for a shared or personal view.

Before you begin

When a normal administrator traverses a shared view for a particular infrastructure type, he or she sees the combination of static entries and dynamic criteria (without duplication) for that infrastructure type.

Procedure

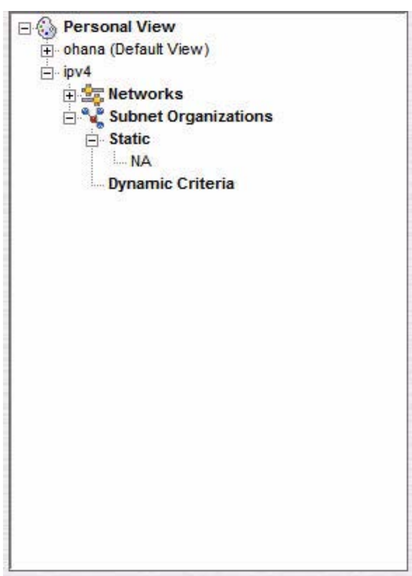
To delete static or dynamic selection criteria for a shared view, follow these steps.

1 Choose one of the following actions.

If you are…	Then…
Deleting selection criteria for a shared view	1. Mouse over **Infrastructure** and click **MyView Management**. **Result:** The MyView Management Hierarchy opens. 2. Expand **Shared Views**. **Result:** A list of shared views appears.
Deleting selection criteria for a personal view	1. Mouse over **MyView** and click **MyView Personalization**. **Result:** The MyView Personalization Hierarchy opens. 2. Expand **Personal Views**. **Result:** A list of personal views appears.

2 Expand the view that you want to modify.

Result: The list of infrastructure types opens.

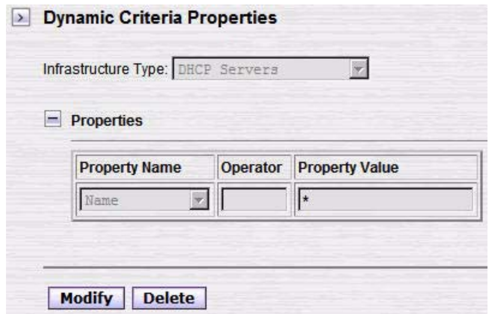


3 Expand the infrastructure type whose criteria you wish to delete.

Result: The **Static** and **Dynamic Criteria** labels open.

4 Choose one of the following actions.

If you want to ...	Then ...
Delete a Static selection	1. Expand the Static label that contains the selection you wish to remove. 2. Select the static selection. **Result:** The Properties page for the static selection opens.  3. Click **Remove**. **Result:** A confirmation dialog box opens with the message **You are about to delete Static Item -** *<infrastructure_item>*. 4. Click **OK**. **Result:** The MyView Management Hierarchy is refreshed and a confirmation dialog box opens with the message **Static Item successfully deleted**. 5. Click **OK**. **Result:** The VitalQIP IP Management Software splash screen is displayed.

If you want to ...	Then ...
Delete a Dynamic Criteria selection	1. Expand the Dynamic Criteria label that contains the item you wish to remove. 2. Select the dynamic criteria selection. **Result:** The Properties page for the selected dynamic criteria opens.  3. Click **Delete**. **Result:** A confirmation dialog box opens with the message **You are about to delete Dynamic Criteria -** *<criteria_items>*. 4. Click **OK**. **Result:** The MyView Management Hierarchy is refreshed and a confirmation dialog box opens with the message **Dynamic Criteria successfully deleted**. 5. Click **OK**. **Result:** The VitalQIP IP Management Software splash screen is displayed.

END OF STEPS

4 Organizations

Overview

Purpose

VitalQIP uses organizations to provide multiple VitalQIP management systems with one physical database. This chapter provides information on using and setting up organizations for your system.

Contents

This chapter covers these topics.

Organization management

Overview

Purpose

You can set up your network into organizations, adding another layer of management of VitalQIP. By separating the network into organizations, you can manage multiple address spaces in a single database. These address spaces can be duplicates of each other, or you can isolate different parts of the same IP address space. Organizations are an optional infrastructure element.

Inheritance rules

Newly created organizations inherit templates and policies from the organization in which an administrator is logged into. A newly created organization does not inherit the infrastructure from the organization in which an administrator is logged into. An organization can inherit the following:

- Naming Policies
- DHCP Option Templates
- Manufacturer Profile
- User defined fields and attributes

Reports

The Organization report can be accessed from the Organization Properties page.

Organizations Hierarchy

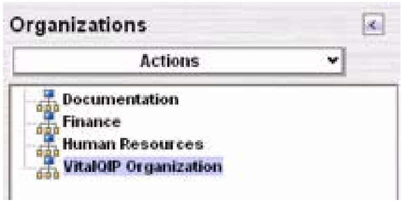
Description

The Organizations page is a list of organizations. The hierarchy always displays the default organization that has “0” in its ID, for instance, VitalQIP Organization.

Sample Organizations Hierarchy

The following figure is an example of the Organizations Hierarchy.

Figure 4-1 Sample Organizations Hierarchy



Add an organization

Purpose

Use this procedure to add a new organization.

Before you begin

- Only master administrators can add organizations.
- When more than one organization is defined in the database, an administrator may be required to select an organization during the login process.

Procedure

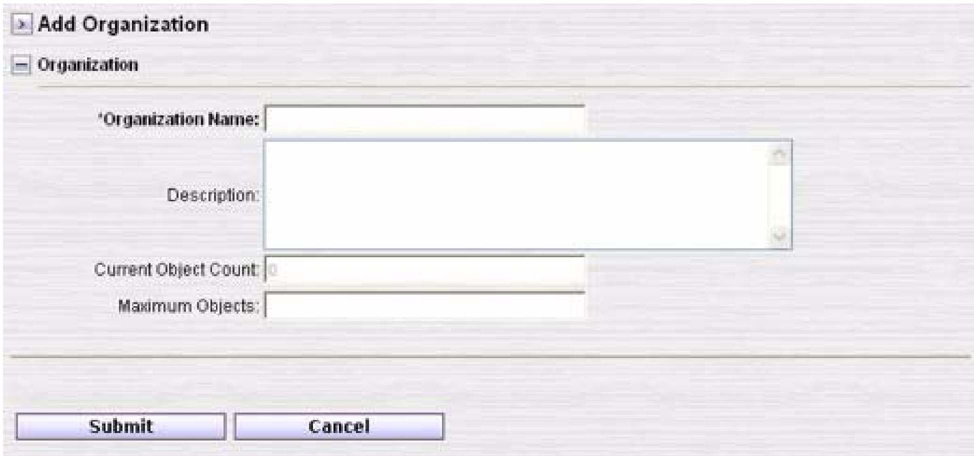
To add an organization, follow these steps:

1 Click **Manage Organization**.

Result: The Organizations Hierarchy page opens.

2 Mouse over the **Actions** menu, and select **Add Organization**.

Result: The Add Organization page opens.



3 Enter values in the **Organization** section. Review the following table for a description of the fields.

Table 4-1 Add organization fields

Field	Description
Organization Name	***Required.*** Enter the name of the organization. The name: • Must be unique from all other organizations • Must contain no more than 255 characters • Must contain any valid ASCII character • Cannot contain a tab, carriage return, or line feed
Description	***Optional.*** Description for the organization. There is 255 character limit.
Current Object Count	***Read only.*** Shows the current number of IPv4 and IPv6 objects in the organization.
Maximum Objects	***Optional.*** A master administrator can define the number of IPv4 and IPv6 objects that can exist for this organization. Zero indicates that there is no limit. An error message is displayed if someone tries to add more objects than the defined limit.

4 If user defined attributes or fields are associated with organizations, an additional section or option, **User Defined Attribute** or **User Define Fields**, is displayed. Refer to "Working with user defined attributes and fields" (p. 7-23) for more information on working with user defined attributes or fields.

5 Click **Submit**.

Result: A dialog box opens with the message **Organization Successfully Added.**

6 Click **OK**.

Result: The Organization Properties page opens for the organization you just created.

END OF STEPS

Modify an organization

Purpose

Use this procedure to modify an organization.

Before you begin

- Only master administrators can modify all the fields, except the **Current Object Count** field.
- An organization administrator can modify the description, user defined fields, and user defined attributes
- A normal administrator cannot modify any fields.

Procedure

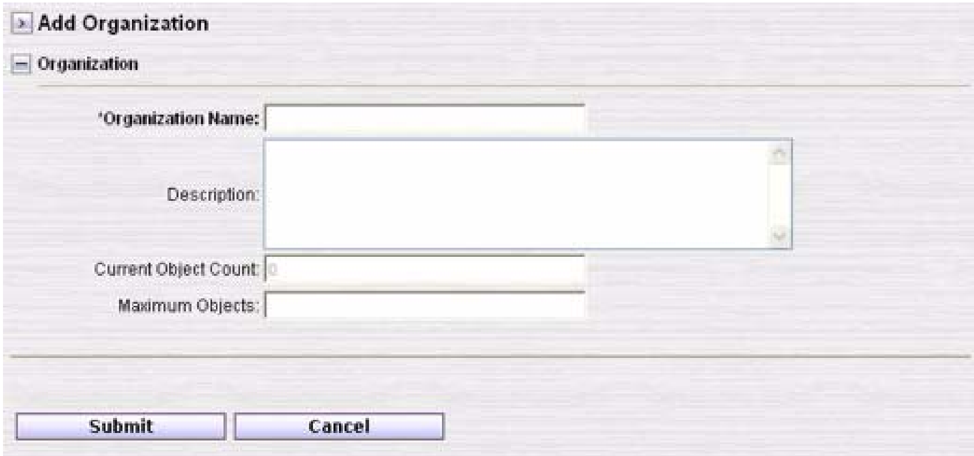
To modify an organization, follow these steps:

1 Click **Manage Organization**.

Result: The Organizations Hierarchy page opens.

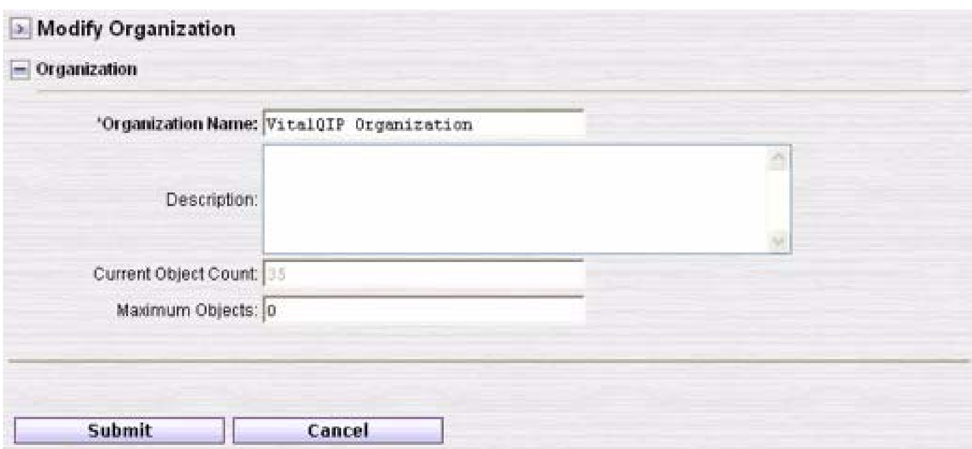
2 Select the organization you wish to modify.

Result: The Organization Properties page opens.



3 Click **Modify**.

Result: The Modify Organization page opens.



4 Modify the fields as needed. Refer to Table 4-1, "Add organization fields" (p. 4-4) for more details.

Note: If associated with an organization, user defined fields and attributes can be modified.

5 Click **Submit** when you have finished making your changes.

Result: A confirmation dialog opens with the message **Organization Successfully Modified.**

6 Click **OK**.

Result: The Organization Properties page opens for the organization you just modified.

END OF STEPS

Delete an organization

Purpose

Use this procedure to delete an organization.

Before you begin

- Only a master administrator can delete an organization.
- Be aware that everything associated with the organization is deleted, including servers, OSPF areas, domains, reverse zones, networks, subnet organizations, subnets, user groups, users, and all IP addresses.
- The organization you are currently logged into cannot be deleted. You must switch to a different organization first.

Procedure

To delete an organization, follow these steps:

1 Click **Manage Organization**.

Result: The Organizations Hierarchy page opens.

2 Select the organization you wish to delete.

Result: The Organization Properties page opens.

3 Click **Delete**.

Result: A dialog box opens with the message **All references to organization** *<organization_name>* **including all networks, domains, subnets and IP Addresses associated with** *<organization_name>* **will be removed. Are you sure you want to delete** *<organization_name>?*

4 Click **OK**.

Result: A confirmation dialog opens with the message **Organization Deleted:** *<organization_name>***.**

5 Click **OK**.

END OF STEPS

Switch organizations

Purpose

To switch between organizations.

Before you begin

- When an organization is switched, the default organization changes to the switched organization. Each time you log in, the switched organization is preselected.
- When an administrator has access to only one organization, the **Switch Organization** button on the Organization Properties page is disabled. The administrator does not need to select an organization during logging in.

Procedure

To switch an organization, follow these steps:

1 Select another organization from the **Organization** drop-down field.

Result: A dialog box opens with the message **Organization has been successfully switched to** *<Organization>*.

2 Click **OK**.

END OF STEPS

5 Contact and location management

Overview

Purpose

This chapter describes how to manage contact and location information.

Contents

This chapter covers these topics.

Contact management

Overview

Purpose

The Manage Contacts page allows you to add, modify, and delete contact information. In addition to First Name and Last Name, you can store Phone, Pager, and Email information.

This information can then be associated with administrator profiles (Add/modify administrator and Clone administrator), subnets (**Location/Contact** in the Subnet Profile), and objects (**General** in the Object Profile).

Figure 5-1 Manage Contacts page

Search Results table

Data in the **Search Results** table can be sorted by column. The Delete and Modify functions are disabled unless an entry in the **Search Results** table is selected.

Toolbar icon

When the **`showIcon.CONTACTS`** property is set to **`true`** in *qip.properties*, the Contacts icon () appears in the Toolbar.

Contact Search global policy

The **`Contact Search`** global policy, described in "Contact Search" (p. 2-24), applies ***only*** to the VitalQIP thick client UI. To see a list of all currently defined contacts in the web client UI, simply click **Search** without any search criteria.

Add a contact

Purpose

Use this procedure to create a contact record of peoples' names, pagers, phone numbers, and email addresses.

Procedure

To create a contact record, follow these steps:

---

1 Mouse over the **Infrastructure** menu and select **Contacts**.

Result: The Manage Contacts page opens.

---

2 Enter contact information in the Search Criteria fields, as described in the following table.

Table 5-1 Contact fields

Field	Description
First Name	***Required.*** Enter up to 20 characters for the contact's first name. The combination of the contact's first and last name must be unique.
Last Name	***Required.*** Enter up to 20 characters for the contact's surname. The combination of the contact's first and last name must be unique.
Phone	Enter up to 20 alphanumeric characters for the contact's phone number.
Pager	Enter up to 20 alphanumeric characters for the contact's pager number.
Email	Enter up to 64 alphanumeric characters for the contact's email address.

3 Click **Add** to create a new contact record.

Result: The contact is added to the **Search Results** table.

4 Add other contacts as required or select another function, such as MyView Hierarchy.

END OF STEPS

Modify contact information

Purpose

Use this procedure to modify contact information.

Procedure

To modify contact information, follow these steps.

1 Mouse over the **Infrastructure** menu and select **Contacts**.

Result: The Manage Contacts page opens.

2 Enter search criteria in the **First Name** and **Last Name** fields so you can so you can retrieve the contacts you want. Use the wildcard character (*) as needed, or leave both fields empty to retrieve all contacts.

3 Click **Search**.

Result: A list of contacts appears in the **Search Results** list.

4 Click on the contact entry you want to modify in the list. Go to other pages and/or modify the page size as needed.

Result: The **Modify** and **Delete** buttons are enabled.

5 Make changes as needed. Click **Clear Fields** to remove all the data in the selected record.

6 Click **Modify**.

Result: The modified information appears in the **Search Results** table.

7 Modify other contacts as required or select another function, such as MyView Hierarchy.

END OF STEPS

Delete a contact

Purpose

Use this procedure to delete one or more contact records.

Before you begin

When you delete a contact record, all information on that contact is removed from the object, subnet, or administrator record with which it was previously associated.

Procedure

To delete one or more contacts, follow these steps.

1 Mouse over the **Infrastructure** menu and select **Contacts**.

Result: The Manage Contacts page opens.

2 Enter search criteria in the **First Name** and **Last Name** fields so you can retrieve the contacts you want. Use the wildcard character (*) as needed, or leave both fields empty to retrieve all contacts.

3 Click **Search**.

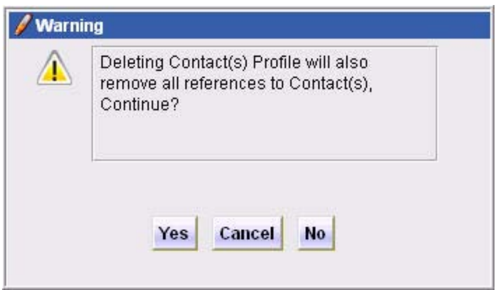
Result: A list of contacts appears in the **Search Results** list.

4 Click on the contact entry you want to delete in the list. Go to other pages and/or modify the page size as needed. To select more than one entry, use the **Shift** and/or **Ctrl** keys in combination with the mouseclicks.

Result: The **Delete** button is enabled (the **Modify** button is enabled only when a single contact record is selected).

5 Click **Delete**.

Result: A warning dialog box opens.



6 Click **Yes** to continue, or click **No** or **Cancel** to abort.

Result: If you click **Yes**, the selected contacts are removed from the database and the **Search Results** list is refreshed. If you select **No** or **Cancel**, the contacts you picked remain selected, ready for your next action.

END OF STEPS

Search for a contact

Purpose

Use this procedure to search for contact records.

Procedure

To search for contacts, follow these steps.

1 Mouse over the **Infrastructure** menu and select **Contacts**.

Result: The Manage Contacts page opens.

2 Enter search criteria in the **First Name** and **Last Name** fields so you can retrieve the contact records you want. Use the wildcard character (*) as needed, or leave both fields empty to retrieve all contacts. The wildcard character can be used in any character position.

To clear all data entry fields, click **Clear Fields**.

3 Click **Search**.

Result: The **Search Results** table is refreshed.

END OF STEPS

Location management

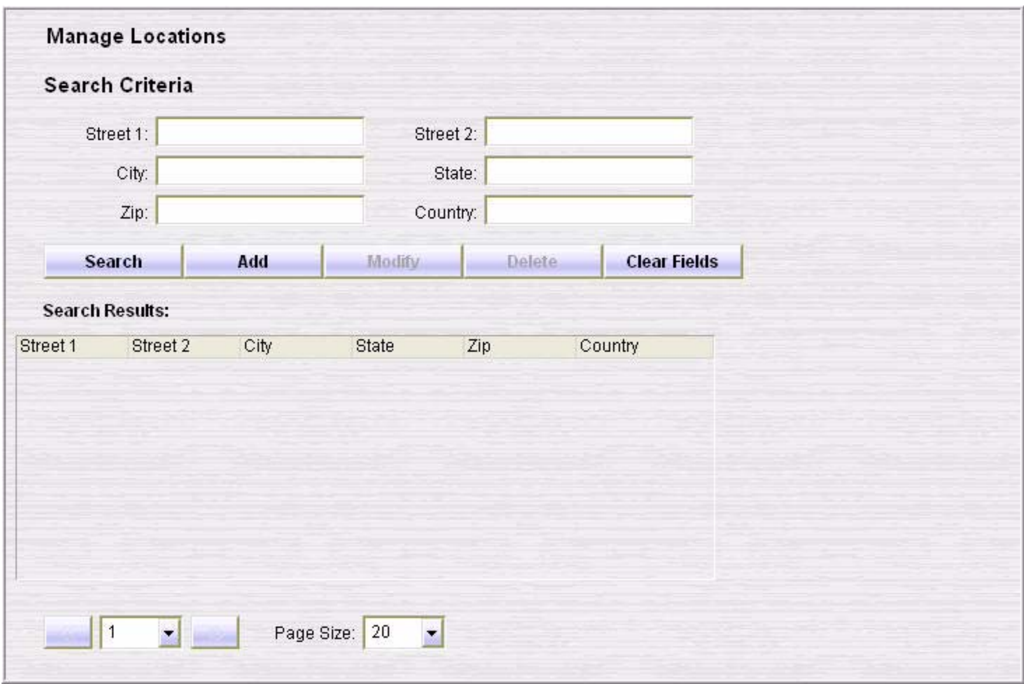
Overview

Purpose

The Manage Locations page allows the user to add, modify, and delete location information. You can store information for Street 1, Street 2, City, State, Zip, and Country. There no required fields for location information, but at least one field must be filled in before a record can be saved.

This information can then be associated with subnets (**Location/Contact** in the Subnet Profile) and objects (**General** in the Object Profile).

Figure 5-2 Manage Locations page



Search Results table

Data in the **Search Results** table can be sorted by column. The Delete and Modify functions are disabled unless an entry in the **Search Results** table is selected.

Toolbar icon

When the **`showIcon.LOCATIONS`** property is set to **`true`** in *qip.properties*, the Locations icon ( ) appears in the Toolbar.

Location Search global policy

The **`Location Search`** global policy, described in "Location Search" (p. 2-27), applies ***only*** to the VitalQIP thick client UI. To see a list of all currently defined locations in the web client UI, simply click **Search** without any search criteria.

Add a location

Purpose

Use this procedure to create an address location record.

Before you begin

At least one field must be filled in before a location record can be created.

Procedure

To create a location record, follow these steps:

1 Mouse over the **Infrastructure** menu and select **Locations**.

Result: The Manage Locations page opens.

2 Enter location information in the search criteria fields, as described in the following table.

Table 5-2 Location fields

Field	Description
Street 1	Enter up to 40 alphanumeric characters for the first line of a street address.
Street 2	Enter up to 40 alphanumeric characters for the second line of a street address.
City	Enter up to 20 alphanumeric characters for the city.
State	Enter up to 10 alphanumeric characters for the state.
Zip	Enter up to 16 alphanumeric characters for the zip code.

Field	Description
Country	Enter up to 30 alphanumeric characters for the country.

3 Click **Add** to create a new location record.

Result: The location is added to the **Search Results** table.

4 Add other location information as required or select another function, such as MyView Hierarchy.

END OF STEPS

Modify location information

Purpose

Use this procedure to modify location information.

Procedure

1 Mouse over the **Infrastructure** menu and select **Locations**.

Result: The Manage Locations page opens.

2 Enter search criteria in any of the **Search Criteria** fields so you can retrieve the locations you want. Use the wildcard character (*) as needed, or leave all fields empty to retrieve all locations.

3 Click **Search**.

Result: A list of locations appears in the **Search Results** list.

4 Click on the location entry you want to modify in the list. Go to other pages and/or modify the page size as needed.

Result: The **Modify** and **Delete** buttons are enabled.

5 Make changes as needed. Click **Clear Fields** to remove all the data in the selected record.

6 Click **Modify.**

Result: The modified location information appears in the **Search Results** table.

7 Modify other location information as required or select another function, such as MyView Hierarchy.

END OF STEPS

Delete a location

Purpose

Use this procedure to delete a location record.

Before you begin

When you delete a location record, all information on that location is removed from the object and/or subnet record with which it was previously associated.

Procedure

To delete one or more locations, follow these steps.

1 Mouse over the **Infrastructure** menu and select **Locations**.

Result: The Manage Locations page opens.

2 Enter search criteria in any of the **Search Criteria** fields so you can retrieve the locations you want. Use the wildcard character (*) as needed, or leave all fields empty to retrieve all locations.

3 Click **Search**.

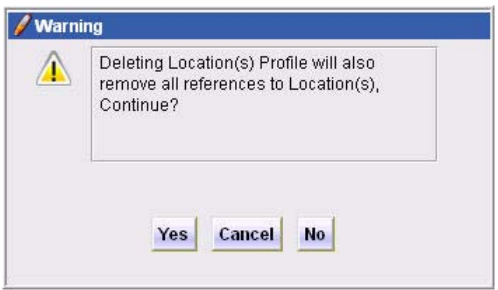
Result: A list of locations appears in the **Search Results** list.

4 Click on the location entry you want to delete in the list. Go to other pages and/or modify the page size as needed. To select more than one entry, use the **Shift** and/or **Ctrl** keys in combination with the mouseclicks.

Result: The **Delete** button is enabled (the **Modify** button is enabled only when a single location record is selected).

5 Click **Delete**.

Result: A warning dialog box opens.



6 Click **Yes** to continue, or click **No** or **Cancel** to abort.

Result: If you click **Yes**, the selected locations are removed from the database and the **Search Results** list is refreshed. If you select **No** or **Cancel**, the locations you picked remain selected, ready for your next action.

END OF STEPS

Search for a location

Purpose

Use this procedure to search for a specific location record.

Procedure

To search for locations, follow these steps.

1 Mouse over the **Infrastructure** menu and select **Locations**.

Result: The Manage Locations page opens.

2 Enter search criteria in any fields so you can retrieve the location records you want. Use the wildcard character (*) as needed, or leave all fields empty to retrieve all locations. The wildcard character can be used in any character position.

To clear all data entry fields, click **Clear Fields**.

3 Click **Search**.

Result: The **Search Results** table is refreshed.

END OF STEPS

6 Administrator management

Overview

Purpose

This chapter describes how to set up and manage VitalQIP administrators. It also contains information on setting up and assigning administrator roles ,as well as administrator login security.

Contents

This chapter covers these topics.

Administrators

Overview

Purpose

Use the Administrator Hierarchy to define the administrative policies, privileges, and roles of those individuals who manage the network or portions of the network, and to define what impact they have on their assigned portions.

Administrator Types

There are three types of administrator in VitalQIP:

- Master — Master administrators have permissions and privileges to create, retrieve and modify any infrastructure type across all organizations.
- Normal — Normal administrators are given access to a limited set of infrastructure types (known as the Managed List) and can be given specific privileges for the infrastructure to which they have access. These privileges can be defined for each organization to which they have access.

Organization — Organization administrators are normal administrators with permission to access all the infrastructure in a given organization. Furthermore, they can have either read-only privileges, or write access to change any infrastructure type in the specified organization.

A node is not created in the Administrator Hierarchy for organization administrators. Instead, they can be searched for by specifying **Organization Administrators** in the **Type** field on the Administrator Search page.

To create an Organization Administrator, first create the Administrator as a normal administrator and then assign organization-level privileges to the specific organization.

VitalQIP also supports Admin Roles in the Managed List. An Admin Role is a grouping mechanism and is used to group a common set of data to various administrators.

Generally, all data is local to a particular organization in VitalQIP. However, an administrator can be set up to manage multiple organizations. The Managed List will contain data from all organizations, however, when administrators are logged in, they will have access only to the data from the organization to which they are currently logged in.

Administrator tab

In the **Administrator** tab, you define the name and initial password, assign organization, different types of administrator and assign privileges to each administrator profile.

Org Privileges tab

In the **Org Privileges** tab, you define network functions that normal administrators can perform.

The privileges you establish in the **Administrator** tab apply to ***all*** the organization privileges for the administrator. The **Org Privileges** tab allows you to “fine-tune” privileges for individual organizations to which an administrator is assigned.

Managed Lists tab

In the **Managed Lists** tab, you specify the network components that normal administrators can modify or view.

If you are setting up similar profiles for several administrators, consider defining an administrative role and assigning it to each administrator. That way, if there are infrastructure changes to the network components assigned to the role, you need only update the administrative role and therefore avoid having to update each administrator profile to reflect the modified infrastructure. For information on setting up administrative roles, refer to “Create an administrative role” (p. 6-29).

Create an administrator

Purpose

Use this procedure to create a new administrator.

Related information

After you create an administrator, you must perform the following procedures:

- “Add organization privileges” (p. 6-8)
- “Add Managed Lists” (p. 6-16)

Before you begin

- Each administrator name must be unique.
- Delegated administrators can create other administrators.
- If you log in as a new administrator, you only see the domains, OSPF areas, subnets, subnet groups, networks, applications, objects, user groups, servers, address ranges, and object ranges assigned to you by the administrator who defined/created your Administrator Profile.
- When a login, password, or organization is changed for a default administrator, the login, password, or organization may also need to be changed in the *<Administrator home directory>/cli.properties, QIPHOME/conf/cli.properties, QIPHOME/qip.pcy*

(the global section) files (if they were specified in any of these files). The login, password, or organization is not updated in these files automatically. Passwords entered in these files must be encrypted with the **`qip-crypt`** command. See the *VitalQIP Command Line Interface User's Guide* for information about **`qip-crypt`**.

- VitalQIP can place restrictions on passwords. See "Administrator security" (p. 6-39) for detailed information. Restrictions can be set for:
  - Disable account
  - Minimum length of password
  - Reuse of password
  - Password expiration
  - Allow the login name and password to be similar
  - Require a new password
- Acceptable values for a password are dependent upon which complexity is set for administrators in the Administrator Security page. The acceptable complexity settings are:
  - Alpha only
  - Numeric only
  - No limitations
  - Alpha and numeric
- Normal administrators cannot modify their own privileges but can modify the privileges of other administrators that they create.
- Normal administrators can create other administrator only if the **Create/Update Administrator** privilege (under **Global Privileges** on the **Administrator** tab) is set to True.

Procedure

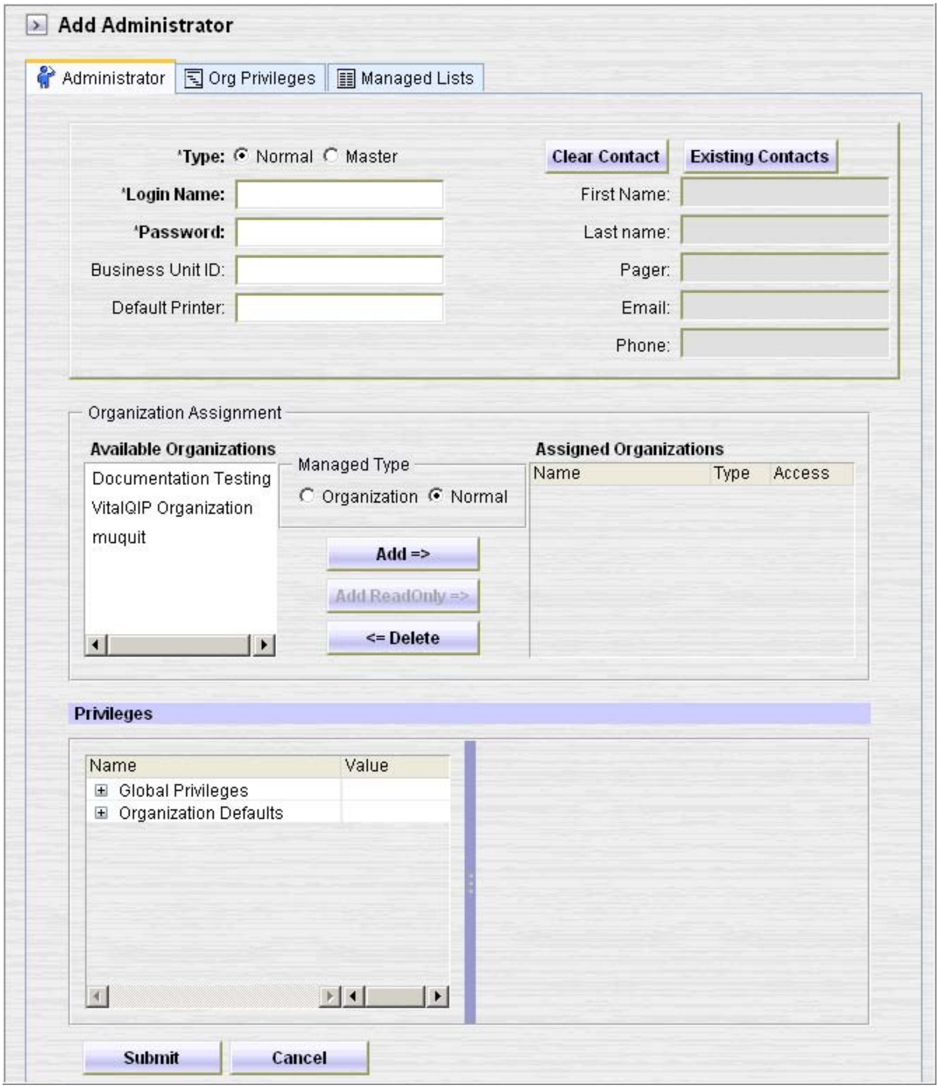
To create an administrator, follow these steps:

1. Select **Administrator** from the **Administrators** menu.

   Result: The Administrator Hierarchy page opens.

2. Mouse over the **Actions** menu and select **Add Administrator**.

Result: The Add Administrator page opens.



3 Select the type of administrator to create in the **Type** field. Once an administrator profile has been added, its **Type** cannot be changed. The types are as follows:

– A **Normal** administrator is the default administrator type and can modify the **Privileges** list in the **Administrator** tab, and add/modify settings in the **Org Privileges** tab or **Managed Lists** tab. A normal administrator can add other normal administrators and assign them privileges, administrative roles and access rights.

– A **Master** administrator has access to all organizations and so has no **Org Privileges** tab. A master administrator also can add, modify, and delete administrative roles. Only master administrators can create, modify, or delete other master administrators.

4 ***Required***. Enter a User ID in the **Admin Name** field. This could be initials or the first letter of the first name and the last name with no spaces, or whatever you want to define.

5 ***Required***. Enter the password the administrator will use in the **Password** field.

6 In the **Business Unit ID** field, enter the alphanumeric prefix (up to 8 characters) that you want to precede the standard object name whenever the administrator you are defining assigns an object to an IP address. The Business Unit ID provides an administrator-specific prefix to the object name.

7 In the **Default Printer** field, enter the name of the default printer to which VitalQIP services, such as reports or email, can be printed.

8 Click **Existing Contact** to open the Search Contacts dialog box. Enter search criteria as needed and select a contact from the **Search Results** list.

9 Click **Select**.

Result: The **First Name**, **Last Name**, **Page**, **Email**, and **Phone** fields display information if it is available.

10 If the **Admin Type** is **Normal**, select the organizations to be managed from the **Available Organizations** list.

11 Click **Add** or **Add ReadOnly** to add the organization to the **Assigned Organizations** list.

Note: If the selected **Managed Type** is **Organization**, you can give an administrator read-only access to that organization by clicking **Add Read Only**.

12 Refer to "Add organization privileges" (p. 6-8) to continue creating an administrator.

END OF STEPS

Add organization privileges

Purpose

Organization privileges define the functions that an administrator can perform. When you add an administrator, you can set up access rights for all organizations for the administrator, or you can fine-tune the access rights for different organizations for the administrator.

The **Administrator** tab allows you to set up privileges for all organizations for an administrator.

The **Org Privileges** tab allows you to set up privileges for individual organizations for an administrator. This tab is only available for normal" administrators. Master administrators do not have the Org Privilege tab associated with them.

Before you begin

- In the **Privileges** list in the **Org Privileges** tab, each Managed Organization has its own privileges that default to the Global Privileges defined on the **Administrator Information** tab. You can change these privileges for any Managed Organization, by setting the **Use Default** privilege to False and customizing the privilege settings as needed.

Note: For those organizations that are assigned with write organization access, you need to set privileges in the **Org Privileges** tab.

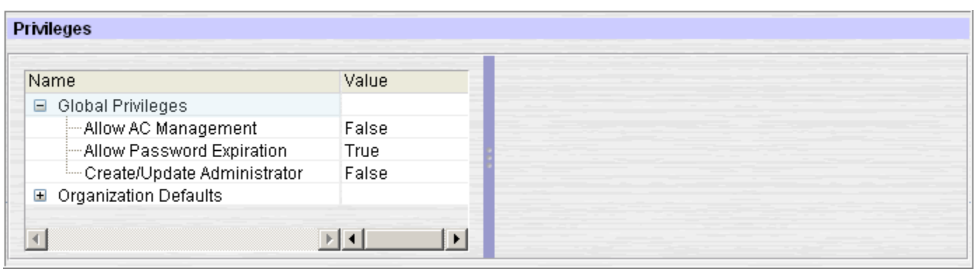
- Normal administrators cannot modify their own privileges but can modify the privileges of other administrators that they create.

Procedure

To assign organization privileges, follow these steps:

1 Choose one of the following action.

If you are...	Then...
Setting organization privileges for all organizations for an administrator	Select the **Administrator** tab and scroll down to the Privileges section.
Setting organization privileges for an individual organization for an administrator or organizations that have a **Managed Type** setting of **Organization** with Write permission.	1. Select the **Org Privileges** tab. 2. Select the organization from the drop-down list to which you are assigning privileges.



2 Select the privileges you wish to assign from the **Privileges** list. Refer to the following table to understand the meaning of each privilege. Select the privilege you wish to set and assign the value in the **Values** field.

Table 6-1 Privilege parameters

Name	Value
Global Privileges	

Name	Value
Allow AC Management	The default value is False. When this privilege is set to True, the administrator can access the Access Control feature in the web client UI.
Allow Password Expiration	The default value is True. When set to True, the administrator password uses the settings in Administrator Security to determine if the password expires, as described in "Set up administrator security" (p. 6-39). If the settings in Administrator Security are set to force the password to expire, the password of the administrator expires. When this privilege is set to False, the administrator password never expires, regardless of what is set in Administrator Security.
Create/Update Administrator	The default value is False and applies to normal administrators only. This privilege allows the administrator to create and/or update other administrators.
Organization Defaults	
Access Address Allocation	The default value is False and applies to normal administrators only. If set to True, this privilege allows the administrator to use address allocation feature of VitalQIP. Other privileges are displayed if True is selected. If this privilege is set to false, no other privileges related to address allocation are displayed.
Maintain Blocks	The default value is True. If set to True, this privilege determines whether an administrator can maintain blocks. This privilege only gives the administrator the ability to modify the User-Defined Field values on a block. Any other block operation is controlled by one of the children of this privilege.
Allocate Blocks	The default value is True. This privilege determines whether an administrator has permission to allocate blocks and enables the **Allocate a Block** button on the Pool Properties screen.

Name	Value
Rule Level	The default is Normal. This privilege determines the rules that an administrator is allowed to process. When a rule is created it is assigned a level (**Normal**, **Advanced**, or **Expert**). This privilege determines which rules the administrator can process. The default is **Normal**. • If set to **Normal**, the administrator can only process **Normal** rules. • If set to **Advanced**, the administrator can process **Normal** and **Advanced** rules. • If set to **Expert**, the administrator can process all rules. This privilege only controls the rules that the administrator can use while allocating a block. It does not control which rules the administrator may be allowed to maintain, which rules the administrator can assign to a pool, or which rules will appear in the reports.
Expand Blocks	The default value is False. The privilege determines if an administrator can expand a block to acquire contiguous space from the parent pool, and enables the **Expand Blocks** button on the Block Properties screen.
Explicitly Create Blocks	The default value is False. This privilege determines whether the administrator has permission to perform explicit block allocations, and enables **Explicit Allocation** button on the Pool Properties screen.
Free Blocks	The default value is False. This privilege determines if an administrator is allowed to free blocks, and enables the **Free** button on the Block Properties screen.
Move Blocks	The default value is False. This privilege determines if an administrator is allowed to move blocks, and enables the **Move Block** button on the Block Properties screen.
Renumber Blocks	The default value is False. This privilege allows an administrator to change the prefix of the address block without changing the IP address component to the right of the prefix. It also enables the **Renumber Block** button in the Block Properties screen
Split\Merge Blocks	The default value is False. This privilege allows an administrator to merge a block with its contiguous block or split a block from its contiguous block. A **Merge Block** and **Split Block** buttons on the Blocks Properties screen.

Name	Value
Maintain Pools	The default value is False. This privilege determines if an administrator is allowed to add, modify, and delete pools.
Maintain Seed Pool	The default value is False. This privilege determines if an administrator is allowed to add, modify, and delete seed pools. It also allows an administrator to add and remove seed blocks from a seed pool.
Rule Override	The default value is False. This privilege determines if an administrator is allowed to override the default rule on a pool when allocating a block against an existing pool.
Write New Infrastructure to Managed List	The default value is True. This privilege determines whether the administrator's Managed List is updated when the administrator performs a block allocation that results in a new VitalQIP subnet. If this is set to True, the new subnet is added to the administrator's Managed List.
Access Node Management	The default value is False and applies to normal administrators only. If this privilege is set to True, the administrator can access the **Node Management** function in the **Address Management** tab of VitalQIP web client. Setting this privilege to False hides the **Address Management | Node Management** tab in the web client from the administrator. A "Master" administrator has full access to this area without restriction. Other privileges are displayed if True is selected. If this privilege is set to False, no other privileges related to **Node Management** are displayed.
Add/Delete Nodes	The default is True. This privilege allows an administrator to add, delete, and manage nodes in the VitalQIP web client.
Manage Nodes	The default is True. This privilege allows an administrator to modify nodes in the VitalQIP web client.
Access V6 Address Management	The default value is False and applies to normal administrators only. If this privilege is set to True, the administrator can access the **IPv6** function in the **Address Management** tab of VitalQIP web client. Setting this function privilege to False hides the **Address Management | IPv6** tab in the VitalQIP web client from the administrator. A master administrator has full access to this functionality without restriction.

Name	**Value**
Highest Level GUI Mode	**Basic Mode** - provides all the Subnet Administrator functions that are needed once the infrastructure has been set up. This mode is the default for any VitalQIP administrator created by the Master VitalQIP administrator. **Standard Mode** - This level provides more options necessary to operate all aspects of VitalQIP. This administrator can also access the Basic Mode functions. **Advanced Mode** - The Advanced Mode displays all functions available with VitalQIP.
Create Infrastructure	***Not available in Basic Mode.*** The default value is False and applies to normal administrators only. This privilege allows the administrator to update any aspect of the VitalQIP infrastructure. If this option is set to True, you can also select the **Dynamic Domain Creation** privilege. If this privilege is set to True, an administrator can add domains from the Object Profile or the Subnet Profile if the domain does not yet exist.
Create Resource Records	***Not available in Basic Mode.*** The default value is False and applies to normal administrators only. This privilege allows the administrator to create and/or update all resource records.
Allow User Selection	The default value is False and applies to normal administrators only. If set to True, this privilege allows the administrator to select users to assign to objects in the Object Profile and the Require User parameter appears. If the “Require User” privilege was set to True by a master administrator, the “Allow User Selection” privilege is automatically set to True and cannot be changed. If the “Require User” privilege was set to False by a master administrator, the administrator can set the “Allow User Selection” to True to allow the option of assigning a user to an object.
Delete Confirmation Warning	The default value is False. This privilege requires the administrator to confirm deletions of objects. This can be tedious if an administrator is deleting a large number of objects at one time. If set to False, only one confirmation screen opens for any number of objects. If set to True, a confirmation screen is displayed for each object.
Display MyView Tab Only	Default is set to False. Setting this to True for normal administrators displays only the **MyView** and **Add-Ons** tabs and hides all other tabs in the VitalQIP web client.

Name	Value
Require Alias	The default value is False. This privilege requires the administrator to enter an Alias for every object name. The Alias is required when a record is added or modified in the Object Profile. “Require” options only apply to static objects.
Require Contact Name	The default value is False. This privilege requires the administrator to select a contact for each object that is managed. Contact Information is checked when a record is added or modified within the Object Profile. “Require” options only apply to static objects.
Require Location	The default value is False. This privilege requires the administrator to provide location information for the object. The Require Location can be satisfied in one of three ways: • Assigning a location to an object. • Entering information into the **Tag** field. • Entering information into the **Room ID** field. Location information is checked when you are adding or modifying a record within the Object Profile. “Require” options only apply to static objects.
Require MAC Address	The default value is False. This privilege requires the administrator to complete the MAC address for all objects assigned. “Require” options only apply to static objects. **Note:** Some object types always require a MAC address (for example, M-DHCP and M-BOOTP). The MAC address is required when adding or modifying a record within the Object Profile.
Require Manufacturer Information	The default value is False. This requires the administrator to select a manufacturer for each object that is managed. Manufacturer information is checked when a record is added or modified within the Object Profile. “Require” options only apply to static objects.
Require User	***Available only when Master is selected***. The default value is False. This privilege, if set to True, requires the administrator to assign at least one user to each object that is managed. User information is checked when a record is added or modified within the Object Profile. “Require” options only apply to static objects.

Name	Value
Restrict CNAME	The default value is False and applies only to normal administrators. When set to True, this privilege prohibits an administrator from entering CNAME and MX records that do not belong to the subnet's assigned domains. If set to False, an administrator can enter CNAME and MX records that do not belong to the administrator's assigned domains without error.
Restrict Subnet	The default value is False, and applies only to normal administrators. When set to True, this privilege prevents an administrator from splitting or deleting subnets where objects are deleted as a result of a split or join. If set to False, an administrator can split or delete subnets.
Unique Name Warning	The default value is True. If this privilege is set to True, a warning message opens whenever the administrator attempts to assign an object name that is not unique. This message can be ignored. DNS allows multiple IP addresses to be associated with a single host name. There are two cases where duplicate names are used: • When the same name is used in different domains, but the fully qualified host name is different. • When multiple addresses in the same domain share the same name (in a load-balancing scenario for example). This is checked when a record is added or modified within the Object Profile or when Alias records are added or modified within the Object Profile.

3 When you have selected the privileges you wish to set for the administrator, proceed to setting up the managed list (for normal administrators). Refer to "Add Managed Lists" (p. 6-16).

END OF STEPS

Add Managed Lists

Purpose

The Managed List allows you to define the network components that a normal administrator can access. This list of components, in conjunction with the organization privileges assigned to the administrator, define the scope of the administrator's capabilities within an organization.

The set of network components (known as the Managed List) and the read/write privilege assigned to them can be defined for each organization.

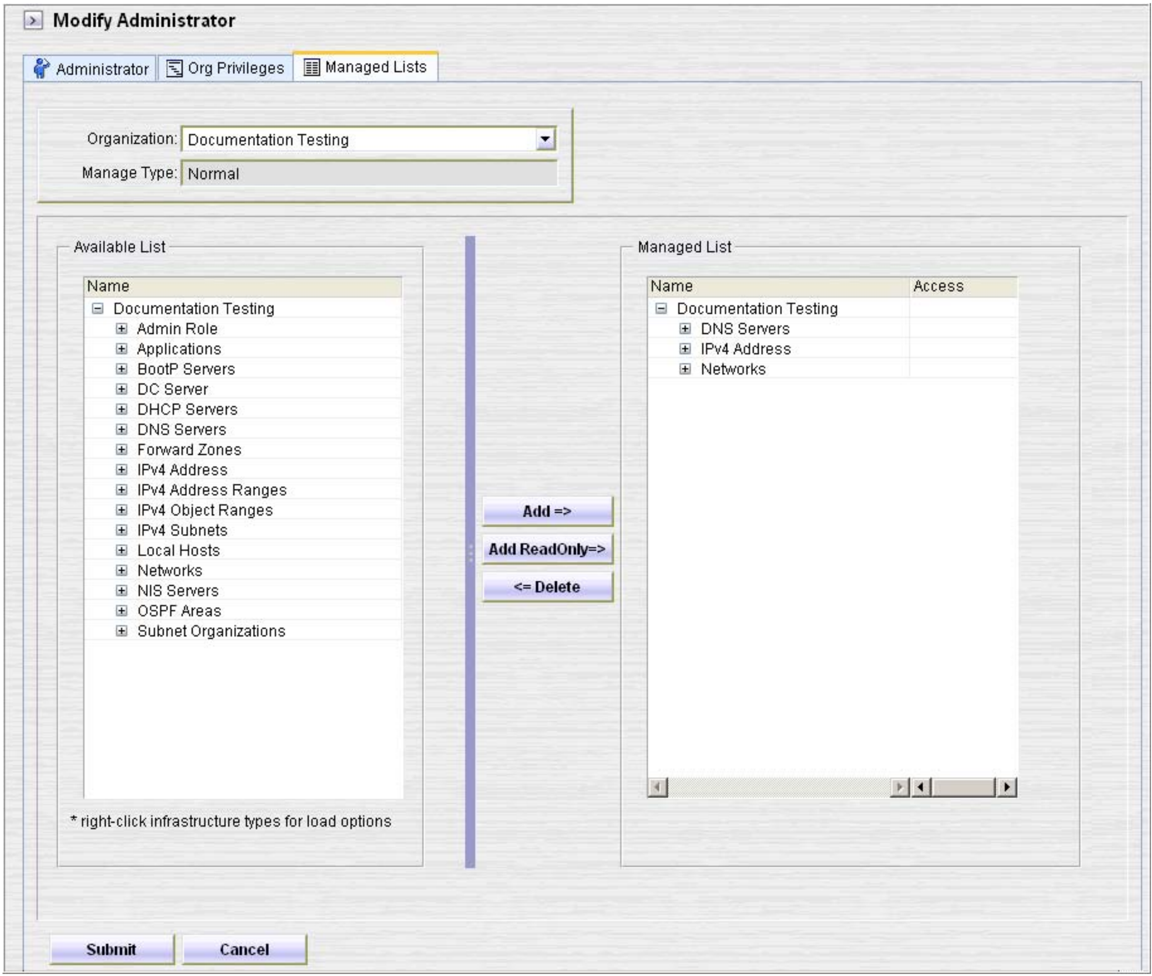
Before you begin

- Multiple ranges can be assigned to a single administrator.
- An administrator with permissions for an object range does not necessarily have permissions for the subnet itself. The administrator can see the associated subnet in the hierarchy, but must have write permissions for a subnet to create an object range in that subnet. If the administrator has permissions to assign an object in that object range or associated subnet, the object can be assigned to a sub-administrator.
- The **Address Range** option in the **Available List** allows you to assign ranges in which the administrator may define and manage ***complete*** subnets. Only subnets that fall entirely within the address range assigned can be accessed by the administrator. Address Ranges are defined in the Network Profile. Object Ranges are defined in the Subnet Profile.
- Normal administrators cannot modify their own privileges but can modify the privileges of other administrators that they create.

Procedure

To create a Managed List, follow these steps.

1 Select the **Managed Lists** tab.



2 Select an organization from the **Organization** drop-down list.

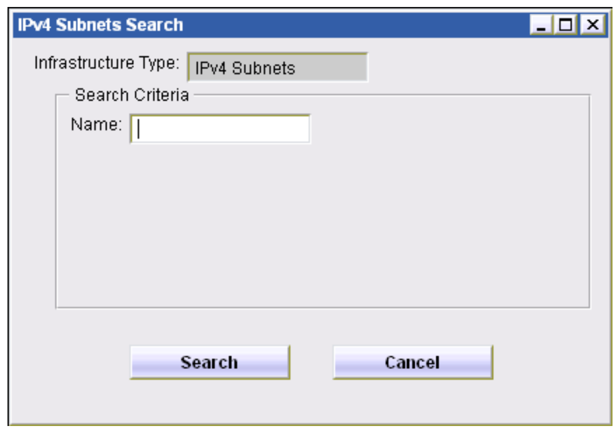
Note: Only organizations with a **Managed Type** of Normal are visible.

3 Select an infrastructure node in the **Available List** that this administrator will be able to view or modify. To select objects, choose one of the following actions.

<table>
<tr><th>If you want to …</th><th>Then …</th></tr>
<tr><td>Search for an infrastructure type (required when you select IPv4 Address)</td><td>

1. Right-click an infrastructure node and select **Search** from the query menu.

Result: A Search window for the selected Infrastructure Type opens.



2. Enter search criteria and click **Search**. You can use the wildcard as needed. For example, if you are searching for IPv4 subnets, entering **`192.*`** returns all subnet addresses that have a matching 192 in the first octet.

Note: If you have a large volume of data, it is preferable to search by subnet name rather than using a wildcard. Using a wildcard can be time consuming, depending on the number of subnets and IPv4 addresses present.

Result: A Search Results node appears in the **Available List**.

3. Expand the Search Results node and select the objects you wish to add to the Managed List. Use the **Shift** key to select a range of objects.

Note: To cancel the results of a search, right-click an infrastructure node and select **Clear** from the query menu.

</td></tr>
<tr><td>Select an infrastructure object</td><td>

1. Expand the infrastructure node.

Result: A list of available objects appears.

2. Select the objects you wish to add to the Managed List. Use the **Shift** key to select a range of objects.

</td></tr>
</table>

4 If you want the administrator to have write access to the components, click **Add**. If you want the administrator to have read-only access, click **Add ReadOnly**.

Read access indicates the administrator can only view these components of the infrastructure. For further information on read/write access rights, refer to Table 6-2, "Administrator read/write access" (p. 6-20).

Note: If you later want to change the status of a component for an administrator, you must remove the component from the **Managed List** and re-add it with the appropriate read/write privileges. To remove a component you added earlier, highlight it in the **Managed List** and click **Delete**.

Note: "Read Only" can apply to some or all items in the **Managed List**. If the same infrastructure component is contained within an assigned Administrative Role and within the Managed List, and one definition is set to "Read Only" and the other is set to "Write", the definition with "Write" capability prevails.

5 Click **Submit** when you have completed your selections.

Result: A dialog opens with the message **Saved Managed List**.

6 Click **OK**.

END OF STEPS

Read/write access in the Managed List

The Access column in the Managed List displays either **Write** or **Read**. Read access is established when you select **Add ReadOnly**. Read access indicates the administrator can only view these segments of the infrastructure.

The following table illustrates what read/write access the administrator has, based on what is assigned to the administrator in this window. "Write access" means the administrator can modify the properties of that item in the infrastructure. Additional comments are shown in the Comments column.

Table 6-2 Administrator read/write access

Managed List type	Read access	Write access	Comments
Domains	Domains Objects Subnets	Domains Objects	
Networks	Networks Objects Subnets	Networks Objects Subnets	
OSPF Areas	Objects OSPF Areas Subnets	Objects OSPF Areas Subnets	
Subnets	Objects Subnets	Objects Subnets	If a subnet that is not in an administrator's Managed List is associated with another Managed List Type (Domain, Subnet Organization, OSPF Area and so on) that ***is*** in an administrator's Managed List, that administrator is allowed read/write access on that subnet. Read/write access to a domain only gives the administrator read access to its subnets.
Objects	Objects	Objects	If an object is not in an administrator's Managed List, but is contained within a Managed List Type (Domain, Subnet, Subnet Organization, OSPF Area, Address Range and so on) that ***is*** in an administrator's Managed List, that administrator is allowed read/write access on that object. In the event that the object is a server, the administrator must have "write" privileges to both the actual object and that server. Otherwise, when the object is being pushed to the server, the administrator will receive a privilege denied message.
Subnet Organizations	Objects Subnets Subnet Organizations	Objects Subnets Subnet Organizations	

Managed List type	Read access	Write access	Comments
Servers	Servers	Servers	Ability to modify servers and create/update configuration files. In the event that the object is a server, the administrator must have "write" privileges to both the actual object and that server. Otherwise, when the object is being pushed to the server, the administrator will get a privilege denied.
Applications	Applications Objects Subnets	Applications Objects	Can create/modify objects in the subnet or object if the subnet has this application defined.
Address Ranges	Networks Subnets Objects	Subnets Objects	You cannot change the properties of the network, but you can add subnets to the network.
Object Ranges	Objects Subnets	Objects	

Clone an administrator

Purpose

You can create a clone of an existing administrator by copying information about that administrator and changing its name.

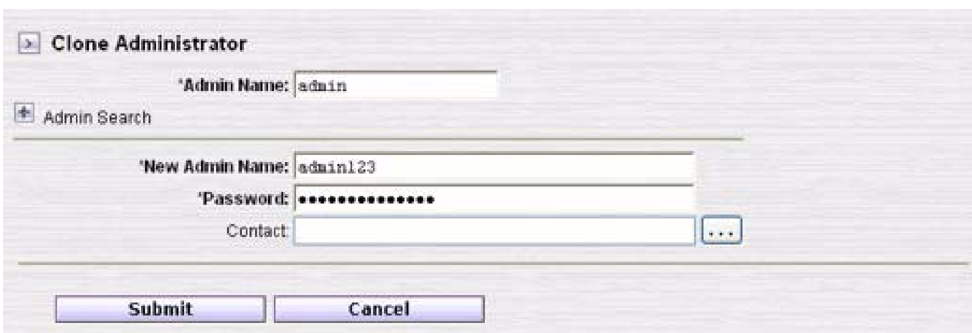
Procedure

To clone an administrator, follow these steps:

1 Choose one of the following:

If you are...	**Then..**
Accessing an administrator from the Administrator Hierarchy	1. Mouse over **Infrastructure** and select **Administrator**. **Result:** The Administrator Hierarchy opens. 2. Select an Administrator from the Administrator Hierarchy. **Result:** The Administrator Properties window opens. 3. Click **Clone**.
Accessing an administrator from the **Actions** menu	1. Mouse over **Infrastructure** and select **Administrator**. **Result:** The Administrator Hierarchy opens. 2. Mouse over **Actions** and select **Clone Administrator**.

Result: The Clone Administrator window opens.



2 In the **Admin Name** field, enter the name of the administrator that you need to clone.

Note: This already contains a value if you started from the Administrator Properties window.

3 ***Required.*** In the **New Admin Name** field, enter the new name of the administrator.

4 ***Required.*** In the **Password** field, enter a password for the cloned administrator.

5 Click ... beside the **Contact** field.

Result: The Contact Search window appears.

a. Enter a search string in the **First Name** field and click **Search**. The search results are displayed.

b. Select the required contact and click **OK**.

6 Click **Submit**.

Result: The administrator is cloned and given the name you specified.

END OF STEPS

Modify an administrator profile

Purpose

Use this procedure to modify an administrator profile.

Before you begin

Normal administrators cannot modify their own privileges but can modify the privileges of other administrators that they create.

Procedure

To modify an administrator profile, follow these steps:

1 Select **Administrator** from the **Administrators** menu.

Result: The Administrator Hierarchy window opens.

2 Select the required administrator in the administrator hierarchy.

Result: The Administrator Properties window opens.

3 Click **Modify**.

For detailed information about the fields in the Administrator Profile, see "Create an administrator" (p. 6-4)

4 Make changes as needed.

5 You will be prompted for saving the changes on each tab. Click **OK**.

Result: A confirmation prompt opens.

6 Click **Submit**.

END OF STEPS

Delete an administrator profile

Purpose

Use this procedure to delete an administrator profile.

Before you begin

- You can delete any "Master" administrator profile, as long as there is at least one "Master" administrator profile remaining in the VitalQIP database.
- Any objects added by an administrator whose profile is later deleted are identified in Object Audit History Reports as "Unknown Administrator".

Procedure

To delete an administrative profile, follow these steps:

1 Select **Administrator** from the **Administrators** menu.

Result: The Administrator Hierarchy window opens.

2 Select the administrator to be deleted from the administrator hierarchy.

Result: The Administrator Properties window opens.

3 Click **Delete**.

Result: A confirmation prompt opens.

4 Click **OK**.

Result: The administrator is deleted.

END OF STEPS

Assign an administrative role

Purpose

If your profile has the **Create/Update Administrator** privilege set to True, you can assign administrative roles to normal administrators. You can assign more than one role to an administrator profile. You also can assign the same role to more than one administrator.

Before you begin

- If you are a master or organization administrator, you can modify or define roles for the administrator profiles. Refer to "Create an administrative role" (p. 6-29) for further information.
- If you are a normal administrator, the list of available roles is limited to the roles currently assigned to the creating administrator.

Procedure

To assign an administrative role to an administrator profiles, follow these steps:

1 Select **Administrator** from the **Administrators** menu.

Result: The Administrator Hierarchy page opens.

2 Select the Administrator Profile from the Administrator Hierarchy to which you wish to assign an administrative role.

Result: The Administrative Properties page opens.

3 Click **Modify**.

Result: The Modify Administrator page opens.

4 Click the **Managed Lists** tab.

5 From the **Organization** drop-down list, select the required organization.

6 In the **Available List**, expand **Admin Role** node and select the administrator role to be assigned and click **Add**.

Result: The administrator roles are added in the **Managed List**.

Note: Use **Ctrl** and **Shift** to select multiple components to add to the **Managed List**.

7 Click **Submit**.

END OF STEPS

Reset a password

Purpose

Use this procedure to reset an administrator password within the web UI. Passwords for both master administrators and normal administrators can be reset. You need to reset passwords for administrators that have been locked.

Before you begin

An Administrator Profile can become locked if an administrator fails to enter the correct password after the number of times specified by the **Account Disable** field in Administrator Security. Another administrator must reset the password in the Administrator Profile to unlock the administrator's account. For information on **Account Disable**, refer to "Account Disable" (p. 6-41).

Procedure

To reset a password, follow these steps.

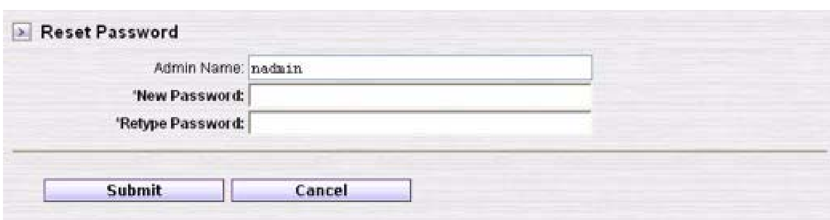
1. Mouse over **Administrators** and click **Administrator**.

2. From the Administrator Hierarchy, select the administrator for which the password has to be reset.

   Result: The Administrator Properties window opens.

3. Click **Reset Password**.

   Result: The Reset Password window opens.



4. Enter a new password in the **New Password** field. Ensure that it complies with the password creation rules established in the Administrator Security function.

5. Enter the password again in the **Retype Password** field.

6. Click **Submit**.

Note: Administrators who now log into VitalQIP are required to change the password again.

END OF STEPS

Administrative roles

Overview

Purpose

An administrative role is a collection of infrastructure components that can be assigned to an administrator as a part of his or her Managed List. By using an administrative role to assign common access to administrators, new infrastructure can be added to the role and as a result all administrators associated with that role have access to the infrastructure. The Administrative Role function therefore reduces the amount of time you need to spend updating every administrator's Managed List to reflect changes in the infrastructure.

You can assign one administrative role to another. If you assign an administrative role to another, the objects defined in the first administrative role are copied to the other. However, objects that are already defined in the first role and present in the second role will be ignored when you copy one administrative role to another.

If two administrative roles (Role 1, Role 2) are added to a third administrative role (Role 3), the permissions defined for objects in the first administrative role (Role 1) override the definitions for the same objects in the second administrative role (Role 2).

Create an administrative role

Purpose

Use this procedure to create an administrative role.

Before you begin

Only "Master" and "Organization" administrators can create administrative roles. Administrative roles are specific to an organization.

Procedure

To create an administrative role, follow these steps:

1. Select **Admin Roles** from the **Administrators** menu.

   Result: The Administrative Role Hierarchy opens.

2 From the **Actions** menu of the Administrative Role Hierarchy, select **Add Administrative Role**.

Result: The Add Administrative Role window is displayed.

3 ***Required***. In the **Name** field, enter a name for the administrator role.

4 In the **Description** field, enter a brief description of the administrator role.

5 Click the **Managed List** tab.

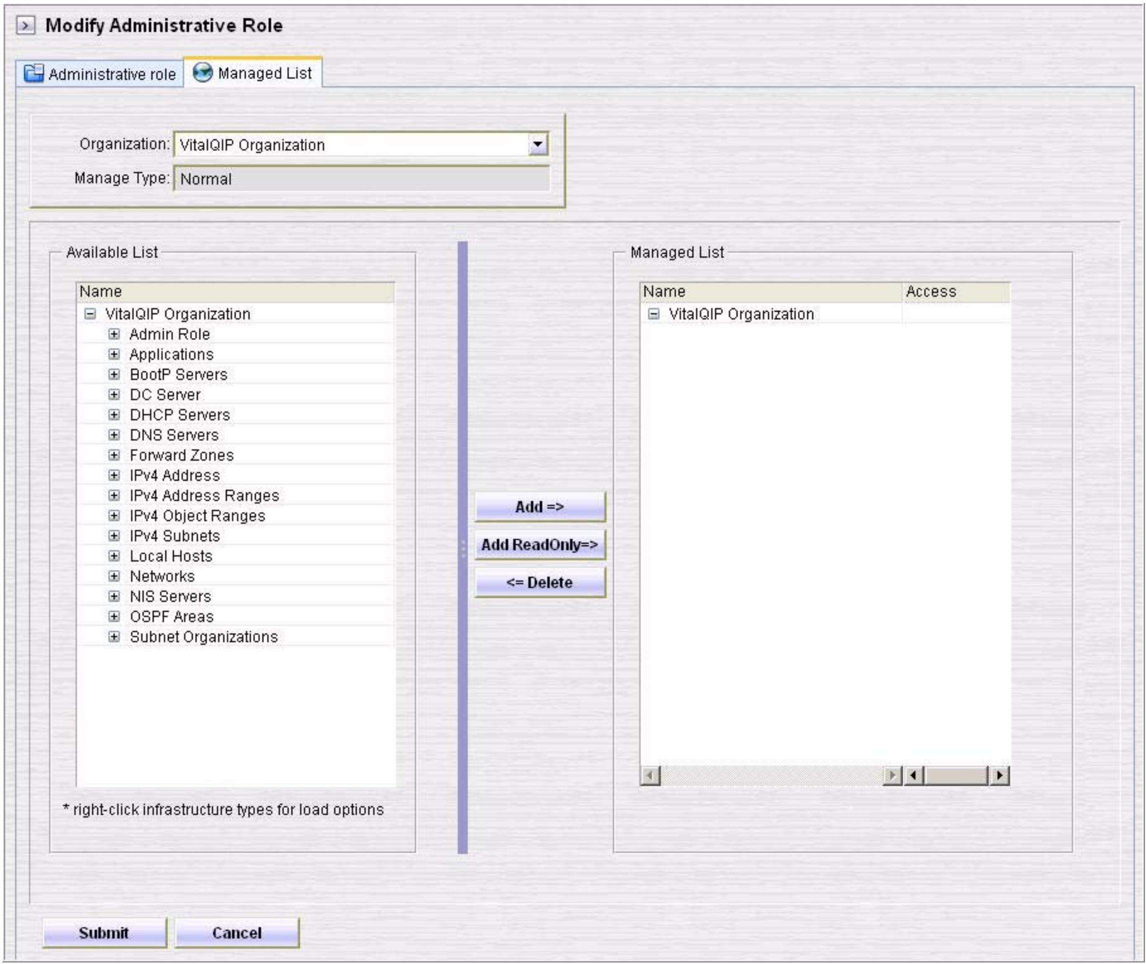
Result: A dialog box opens with the message **Administrative Role has been modified. Save Administrative Role?**

6 Click **Yes** to save the administrative role.

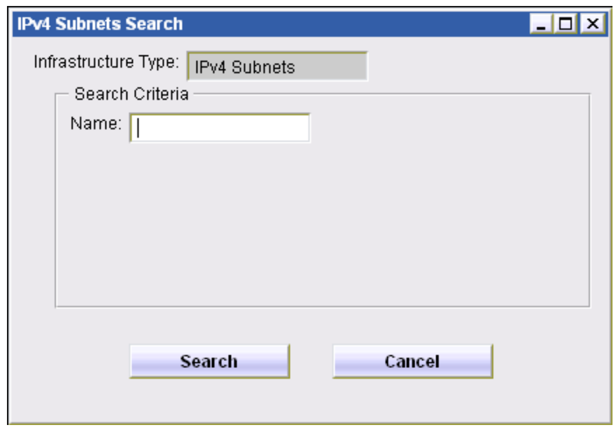
Result: A confirmation dialog opens with the message **Saved Administrative Role**.

7 Click **OK**.

Result: The Modify Administrative Role page opens on the **Managed List** tab.



8 Select an infrastructure node in the **Available List** that this administrator will be able to view or modify. To select objects, choose one of the following actions.

If you want to …	Then …
Search for an infrastructure type (required when you select IPv4 Address)	1. Right-click an infrastructure node and select **Search** from the query menu. **Result:** A Search window for the selected Infrastructure Type opens.  2. Enter search criteria and click **Search**. You can use the wildcard as needed. For example, if you are searching for IPv4 subnets, entering **`192.*`** returns all subnet addresses that have a matching 192 in the first octet. **Note:** If you have a large volume of data, it is preferable to search by subnet name rather than using a wildcard. Using a wildcard can be time consuming, depending on the number of subnets and IPv4 addresses present. **Result:** A Search Results node appears in the **Available List**. 3. Expand the Search Results node and select the objects you wish to add to the Managed List. Use the **Shift** key to select a range of objects. **Note:** To cancel the results of a search, right-click an infrastructure node and select **Clear** from the query menu.
Select an infrastructure object	1. Expand the infrastructure node. **Result:** A list of available objects appears. 2. Select the objects you wish to add to the Managed List. Use the **Shift** key to select a range of objects.

9 If you want the administrator to have write access to the components, click **Add**. If you want the administrator to have read-only access, click **Add ReadOnly**.

Read access indicates the administrator can only view these components of the infrastructure. For further information on read/write access rights, refer to Table 6-2, "Administrator read/write access" (p. 6-20).

If you expand the **Admin Role** node from the **Available List** you can copy the contents of one or more existing administrative roles to the **Managed List**. If there is a duplicate definition, a warning appears. Click **OK**.

> **Note:** "Read Only" can apply to some (or all) components but it cannot be applied to an administrative role if you have selected one to add to the **Managed List**.

To remove a component, highlight it under the **Managed List** and click **Delete**.

10 Add additional components to the **Managed List** until your role definition is complete.

11 Click **Submit** to save the administrative role.

> **Result:** A confirmation dialog opens with the message **Saved Managed List**.

12 Click **OK**.

END OF STEPS

Modify an administrative role

Purpose

Modify the contents of an administrative role when you need to keep administrators up-to-date on changes to the infrastructure. Instead of updating each profile, you can simply update a role. The updated role becomes visible for an administrator on the next login. The infrastructure change you make, however, becomes effective immediately. For example, if an infrastructure component is removed from a role, an administrator assigned that component no longer can access it.

Procedure

1 Select **Admin Role** from the **Administrators** menu.

Result: The Administrative Role Hierarchy window opens.

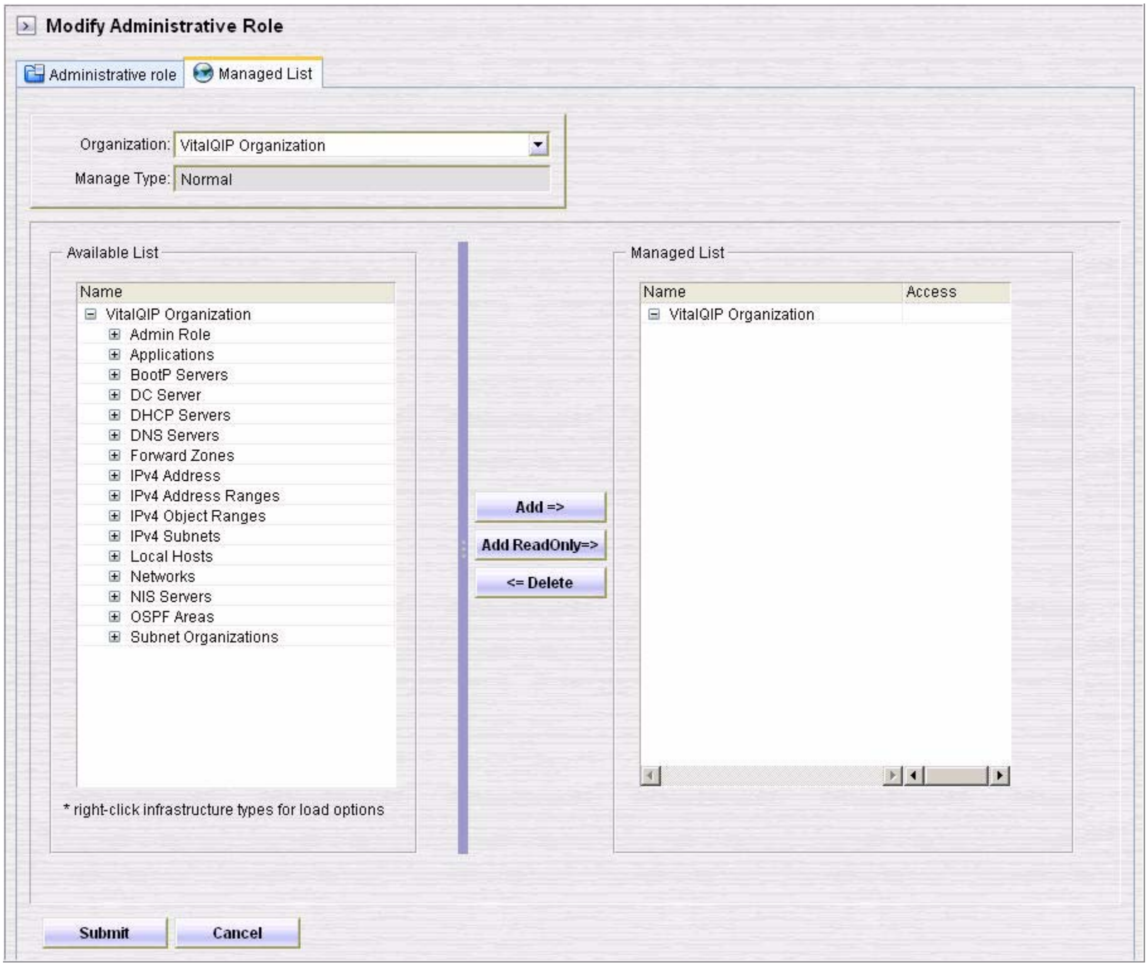
2 Select the role you wish to modify from the **Administrative Roles** list.

Result: The Administrative Role Properties window opens.

3 Click **Modify**.

Result: The Modify Administrative Role window opens. You can modify the admin role name and description in this window.

4 Click the **Managed List** tab. The properties for the administrative role display in the Modify Administrative Role window.



5 Make the changes you need and when completed, click **Submit**.

Result: A confirmation dialog opens with the message **Saved Managed List**.

6 Click **OK**.

Result: Your changes are saved.

END OF STEPS

Delete an administrative role

Purpose

Use this procedure to delete an administrative role.

Procedure

To delete an administrative role, follow these steps:

1 Select **Admin Role** from the **Administrators** menu.

Result: The Administrative Role Hierarchy window opens.

2 Select the role to be deleted from the Administrative Role Hierarchy.

Result: The Administrative Role Properties window opens.

3 Click **Delete**.

Result: A confirmation dialog opens with the message **Are you sure you want to delete the administrative role?**

4 Click **OK**.

Result: The Administrative Role Hierarchy is updated as the administrative role is removed.

END OF STEPS

Check administrative role assignments

Purpose

Use this procedure to check what administrators are assigned to administrative roles.

Procedure

To check which administrators have been assigned to a specific administrative role, follow these steps:

1 Select **Admin Roles** from the **Administrators** menu.

Result: The Administrative Role hierarchy opens.

2 Expand the hierarchy, highlight the role you want to check.

Result: The Administrative Role Properties page opens.

3 Click **View Admins**.

Result: The Administrator Search page opens.

4 Click **Search**.

Result: The Search Results displays a list of administrators assigned to this administrative role. If necessary, use the **Admin Name** field to limit the number of administrators listed for this Administrative Role.

5 Click **OK**.

END OF STEPS

Administrator security

Overview

Purpose

To improve the security of the system, the VitalQIP web client includes additional administrator security options. These options allow:

- Password length and complexity enforcement
- Password not being the same as the Login ID (nor very similar - for example, not the mirror of the Login ID)
- Restricted password reuse
- Ability to disable accounts after a specified number of failed login attempts
- Password aging
- Require password for new administrator

Set up administrator security

Purpose

Use this procedure to establish security settings for all administrators in the VitalQIP database.

Before you begin

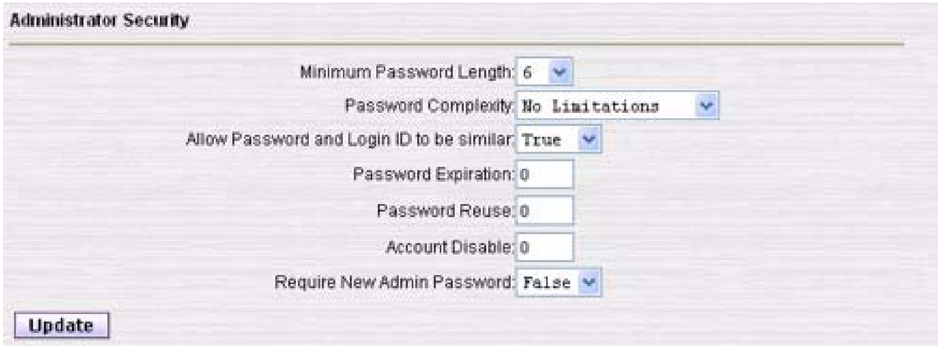
- Administrator Security settings can only be accessed by a master administrator.
- Settings made in the Administrator Security page affect ***every*** administrator with the exception of the **Password Expiration** setting, which can be set up on a case by case basis for each administrator based on the **Allow Password Expiration** privilege in their administrator record. Refer to "Allow Password Expiration" (p. 6-10).

Procedure

To establish security settings, follow these steps.

1 Mouse over **Administrators** and click **Administrator Security**.

Result: The Administrator Security page opens.



2 Refer to the following table as you select the security settings you want to establish for the VitalQIP database.

Table 6-3 Administrator Security options

Field name	Description
Minimum Password Length	***Required.*** The minimum length of an administrator's password. Valid values are from 6 to 25. The default value is 6.
Password Complexity	Select from the list of valid complexity settings. The default value is No Limitations. The settings are: • **Alpha Only** - Password may only contain letters. • **Numeric Only** - Password may only contain numbers. • **No Limitations** - Password may contain any combination of letters, numbers, and special characters. • **Alpha and Numeric** - Password must contain at least one letter and one number. Password may also contain special characters.

Field name	**Description**
Allow Password and Login ID to be similar	Controls whether a password can contain the login ID or the mirror image of the login ID. Values are True or False. True is the default. If this is set to False, the Login ID or the reverse of the Login ID cannot be any part of the password. **Example:** Assuming the Login ID is set to **`abcdef`**, the following list of passwords would not be allowed if this field were set to False: **`abcdef`** **`acbdefasdf`** **`asdfabcdef`** **`fedcba`** **`fedcbaasdf`** **`asdffedcba`**
Password Expiration	Indicates the numbers of days that a password remains valid before an administrator must change it. A setting of 0 (the default) turns off password expiration. The maximum value is 999. **Note:** If the **Allow Password Expiration** privilege in an individual administrator's record is set to False, it overrides a non-zero value entered here. Refer to "Allow Password Expiration" (p. 6-10)
Password Reuse	Indicates the numbers of unique passwords that an administrator must use before being able to reuse old passwords. Zero means that there is no reuse restriction. The default value is 0. The maximum value is 999.
Account Disable	Indicates the number of failed login attempts before a login account is automatically disabled. Zero means that the account will never be disabled. The default value is 0. The maximum value is 999. **Note:** After a login has been locked, that account can be cleared by a master administrator logging in and running Reset Password. Refer to "Reset a password" (p. 6-26)

Field name	**Description**
Require New Admin Password	Determines whether new administrators are required to change their password the first time that they log into VitalQIP. The default is False. **Note:** If an administrator's password is modified in the administrator record (for example, after a record has been locked), this field forces a new password to be entered at login when set to True.

3 Click **Update** to save the new security settings.

Result: A confirmation dialog box with the message **Administrator Security options saved successfully**.

4 Click **OK**.

Result: The confirmation dialog box closes.

5 To close the Administrator Security page, select another function from the VitalQIP web client menu.

END OF STEPS

Change password

Overview

Purpose

The **Password Expiration** field in the Administrator Security function allows a master administrator to establish password aging for all administrators in the VitalQIP database. Additionally, new users may be required to change passwords at their first login attempt if the **Require New Admin Password** field is set to True.

When a password has expired or a new administrator needs to set a new password, VitalQIP presents a change password screen to the user at the next login attempt. For more information, refer to "Log into VitalQIP web client" (p. 1-2).

Change a password

Purpose

Use this procedure to change your password within the web UI. To change your password if your current password has expired, or because the **Require New Admin Password** field is set to True and you are logging in for the first time, follow the procedures outlined in "Log into VitalQIP web client" (p. 1-2).

Before you begin

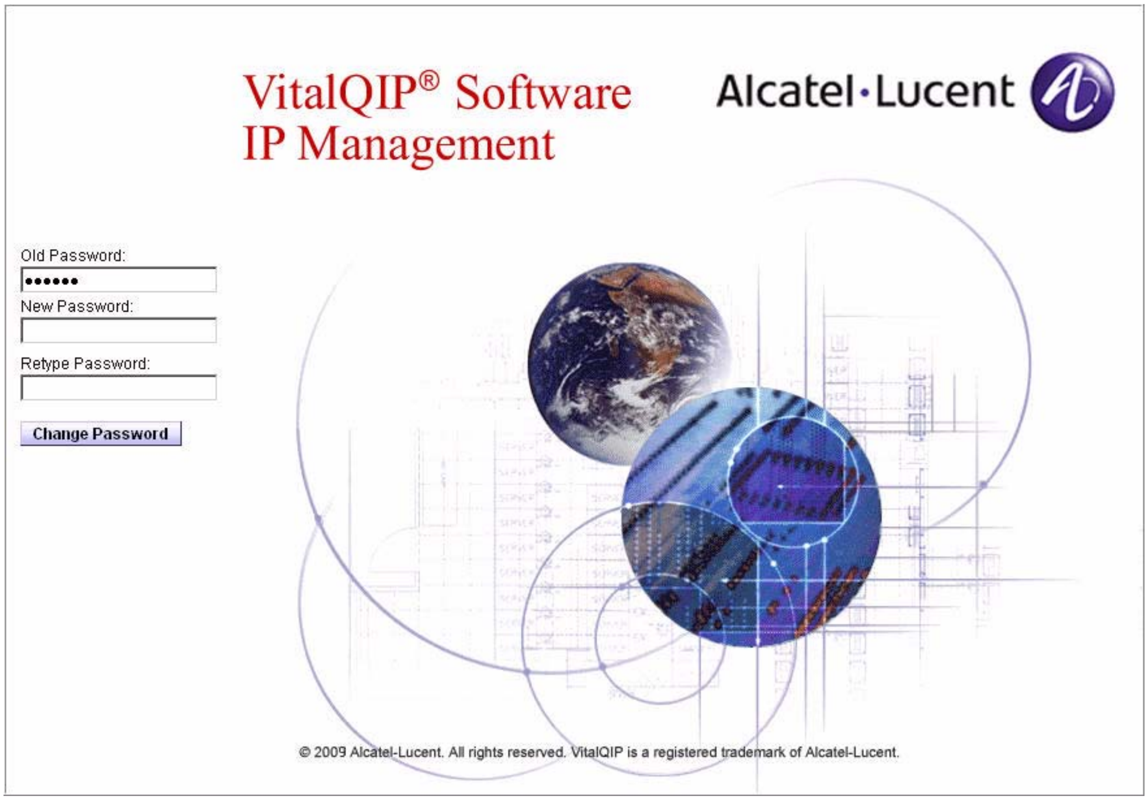
- Master administrators can place restrictions on length, complexity, and similarity to former passwords. These restrictions are configured in Administrator Security. For more information, refer to "Set up administrator security" (p. 6-39).
- When a user ID, password, or organization is changed for a default administrator, the user ID, password, or organization may also need to be changed in the *<Administrator home directory>/cli.properties*, *QIPHOME/conf/cli.properties*, and the global section of *QIPHOME/qip.pcy* (if they were specified in any of these files). The user ID, password, or organization is not updated in these files automatically. Passwords entered in these files must be encrypted by using the **`qip-crypt`** command. Refer to the *VitalQIP Command Line Interface User's Guide* for information about **`qip-crypt`**.

Procedure

To change a password, follow these steps.

1 Click **Change Password**.

Result: The Change Password window opens.



2 Enter your current password in the **Old Password** field and press **Tab**.

3 Enter a new password in the **New Password** field. Ensure that it complies with the password creation rules established in the Administrator Security function.

4 Enter your new password again in the **Retype Password** field.

5 Click **Change Password**.

Result: A confirmation dialog opens with the message **Administrator Password changed successfully**.

6 Click **OK**. To close the Change Password page, select another function from the VitalQIP web client menu.

END OF STEPS

7 Attributes

Overview

Purpose

This chapter describes how to create and use attributes.

Contents

This chapter covers these topics.

Attributes management

Overview

Purpose

Attributes allow you to specify values you want to associate with elements such as pools, blocks, and nodes in the VitalQIP database. You can use these values to tie Address Allocation, Address Management and the DNS and DHCP infrastructure into your corporate processes. For example, you can associate an employee's badge number or cost center with a subnet.

Component of attributes

There are three components to attributes:

- Attributes are the individual pieces of information you want to associate with items in the VitalQIP database. Examples could be Employee Badge Number, Manager's Name, Product Name or Department.
- Attribute groups are a way to organize attribute names. Examples could be Employee Information, Products, or Departments. An attribute does not have to be assigned to an attribute group, or can be assigned to more than one attribute groups.
- Infrastructure types, such as pools, blocks and nodes are defined on the attributes section. You can associate an Attribute with any defined infrastructure type.

You define attributes and groups in the Attributes section of the Web Client. You associate them with various elements of the database when you define those elements. For example, you can define an attribute here and associate it with the infrastructure type **`pool`**, but to associate it with a specific pool, you must edit that pool's properties.

Create an attribute

Purpose

Use this procedure to create an attribute.

Procedure

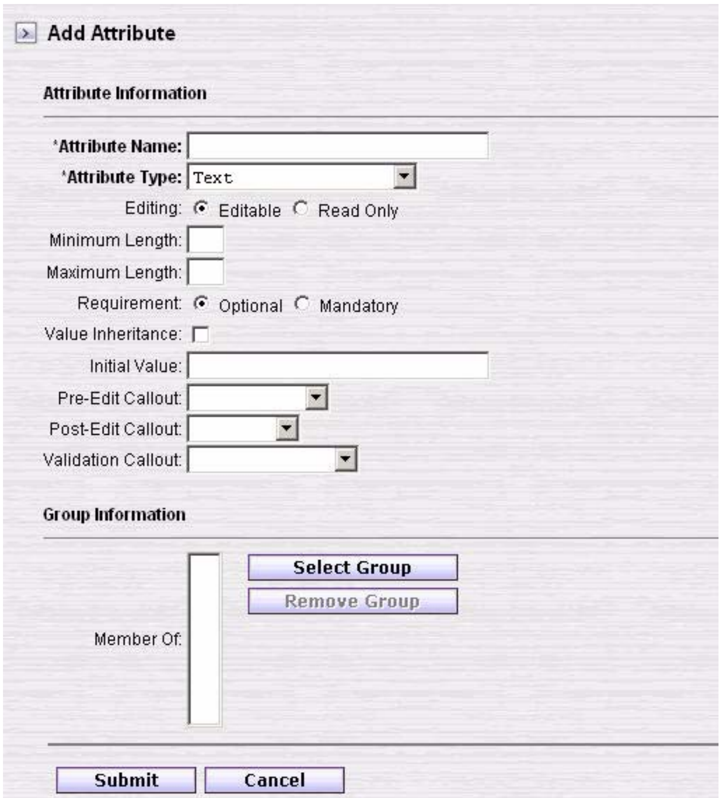
To create an attribute, use the following steps:

1 Mouse over **Infrastructure** and click the **Attribute**.

Result: The Attributes Hierarchy opens.

2 Mouse over **Actions** and select **Add Attribute**.

Result: The Add Attribute page opens.



Note: The fields on this page vary depending on the value you select for the Attribute Type.

3 Review the following table and enter values in the attribute fields.

Table 7-1 Add attribute fields

Field	Description
Attribute Name	***Required***. Defines the name of the attribute. This field is alphanumeric and up to 30-characters long. This field must be unique within an organization. It is case-insensitive (that is, you cannot have an attribute called **userid** and another called **Userid**).

Field	Description
Attribute Type	***Required***. Select an attribute type from the drop-down list. Values are: • **Text** (default) • **Boolean** • **IPv4 Address** • **IPv6 Address** • **Multi-lined Text** • **Numeric** • **Static drop-down List**
Editing	***Required***. Defines whether the Attribute is editable when it is displayed in a properties or properties-like screen associated with an element, such as a pool, block, or node. Select the appropriate radio button: • **Editable** (default) • **Read only**. If this value is selected, the value can be entered either in the Attribute Value field or set by a Pre-Edit callout.
Minimum Length	***Optional***. Defines the minimum length of the value for the Attribute. This field is numeric and has a range of 1 to 999. This field only appears when the Attribute Type is Text.
Maximum Length	***Optional***. Defines the maximum length of the value for the Attribute. This field is numeric and has a range of 1 to 999. This field only appears when the Attribute Type is Text.
Minimum Value	***Optional***. Defines the minimum value of the Attribute. This field is numeric and has a range of -2147483647 to 2147483647. This field only appears when the Attribute Type is Numeric. It must be less than the Maximum Value.
Maximum Value	***Optional***. Defines the maximum value of the Attribute. This field is numeric and has a range -2147483647 to 2147483647. This field only appears when the Attribute Type is Numeric. It must be greater than the Minimum Value.
Requirement	Defines whether the Attribute is required or not. This field only appears when Editing is set to Editable. Select the appropriate radio button: • **Optional** (default) • **Mandatory**

Field	Description
Value Inheritance	If checked, when associating the Attribute with elements of Database (for example, Pool, Block), specifies that the initial value of the Attribute is inherited from its parent item. For example, an Attribute in a block can inherit its initial value from the same Attribute in the block's parent Pool. Default is unchecked.
Initial Value	Defines the initial value for this field. This field only appears when Editing is set to Editable.
Attribute Value	Defines the value for this field. This field only appears when Editing is set to Read-only.
Pre-Edit Callout	***Optional***. Select a callout from the drop-down list. This field contains a string for a callout function which is executed prior to a user editing the Attribute value. **Note:** If a Pre-Edit Callout is selected that will populate an Attribute's initial value and Value Inheritance is activated, then the value associated with the Value Inheritance feature overwrites the value populated by the Pre-Edit Callout.
Post-Edit Callout	***Optional***. Select a callout from the drop-down list. This field contains a string for a callout function that is executed prior to saving the Attribute value in the database. If both Pre-Edit Callout and Post-Edit Callout are selected, the value returned from Post-Edit Callout is saved to the database.
Validation Callout	***Optional***. Select a callout from the drop-down list. This field contains a string for a validation callout function. The validation callout function is executed prior to saving the Attribute value. An error is returned if the function returns false. If there is an error, the user will need to modify the Attribute value to comply with the validation.

Field	Description
Static drop-down List Information	
New Value	If the Attribute Type is set to **Static drop-down List**, then this field and the **Add**, **Remove**, and **Set Default** buttons all display. • To add a value to an Attribute's drop-down list, type the value in this field and click **Add**. The value appears in the right-hand column. **Note:** Values are case-insensitive. If you add multiple values such as `userid` and `Userid`, only one value is saved to the database. • To remove a value from an Attribute's drop-down list, click a value in the right-hand column and then click **Remove**. • To make a value in the list the default value, click a value in the right-hand column and then click **Set Default**. • Also, the **Unset Default** button is displayed when Requirement is set to Optional. For an optional attribute, if the default value is set (that is, the **Default Value** indicator is visible next to the first item), you can unset it by clicking this button.
Group Information	
Member Of	If you want to add this Attribute to one or more existing attribute groups, click **Select Group**. From the list of groups that displays, select the groups to which you want to assign this Attribute, and then click **Submit**. If you want to remove an attribute from one or more groups, click the group name in this field, and then click **Remove Group**.

4 When you are finished, click **Submit** to add the Attribute.

END OF STEPS

Modify an attribute

Purpose

Use this procedure to modify an attribute.

Procedure

To modify an attribute, follow these steps.

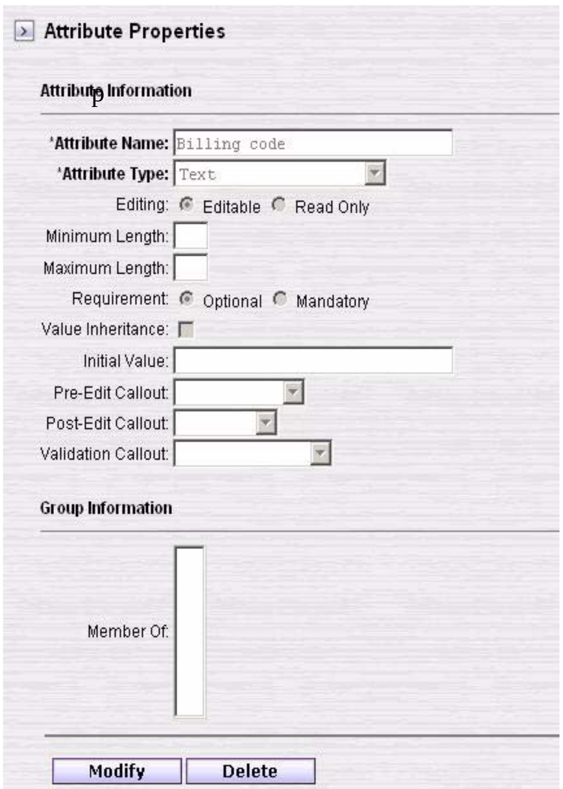
1 Mouse over **Infrastructure** and click **Attribute**.

Result: The Attributes Hierarchy opens.

2 Expand the list of attributes until the one you want to modify is visible.

3 Click the attribute.

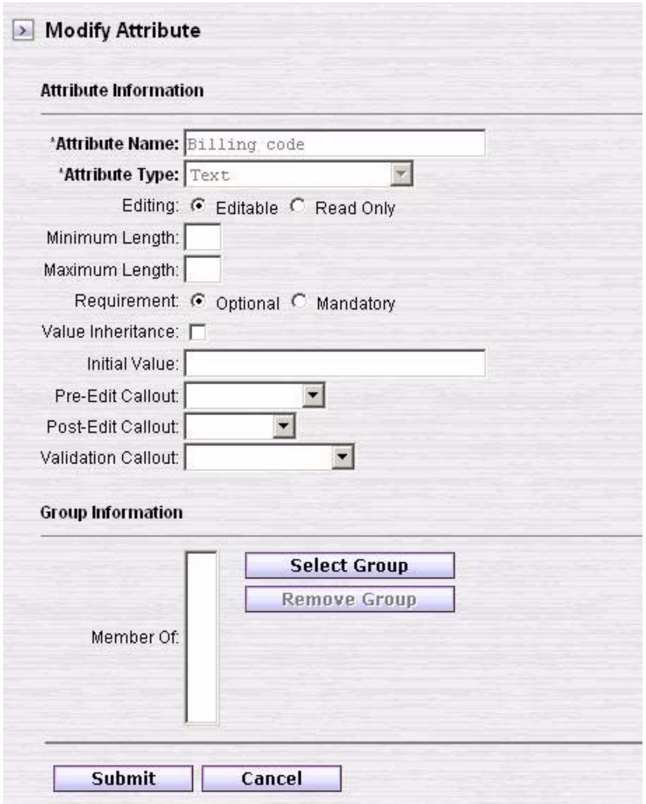
Result: The **Attribute Properties** page opens.



Note: The fields on this page vary depending on how the attribute is defined.

4 Click **Modify**.

Result: The Modify Attribute page appears.



5 Modify fields as necessary for this attribute. Refer to Table 7-1, "Add attribute fields" (p. 7-3) for details on the attribute fields.

Note: You cannot modify the **Attribute Name** or **Attribute Type**. All other fields are modifiable.

6 Click **Submit** when you are finished.

Result: The attribute is modified.

END OF STEPS

Delete an attribute

Purpose

Use this procedure to delete an attribute.

Before you begin

To delete an attribute or a group, the attribute or the group must not be assigned to any infrastructure type.

Procedure

To delete an attribute, follow these steps.

1 Mouse over **Infrastructure** and click **Attribute**.

Result: The Attributes Hierarchy opens.

2 Expand the list of attributes until the one you want to delete is visible.

3 Click the attribute.

Result: The **Attribute Properties** page opens.

4 Click **Delete**.

Result: A dialog box opens with the message **Are you sure you want to delete the selected Attribute?**

5 Click **OK**.

Result: The attribute is deleted.

END OF STEPS

Add an attribute group

Purpose

Use this procedure to create an attribute group.

Procedure

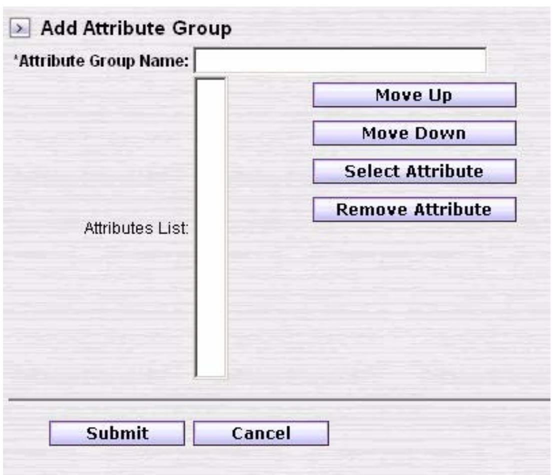
To create an attribute group, use the following steps:

1 Mouse over **Infrastructure** and click **Attribute**.

Result: The Attributes Hierarchy opens.

2 Mouse over **Actions** and select **Add Attribute Group**.

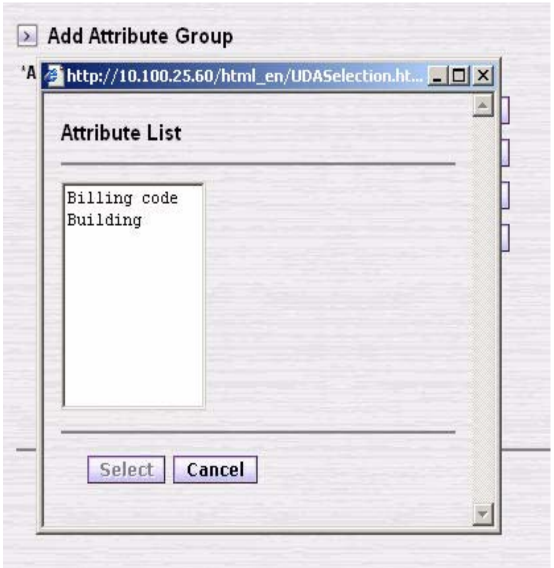
Result: The Add Attribute Group page opens.



3 Type a name in the **Attribute Group Name** field. This field is alphanumeric and can be up to 255 characters long.

4 Click **Select Attribute** to add an attribute to this attribute group. (To add the group without adding any attributes to it, continue to Step 6.)

Result: A list of available attributes opens.



5 Click the attribute you want to add to the attribute group and then click **Select**.

Result: The attribute is added to the group.

6 Click **Submit**.

Result: The attribute group is created.

END OF STEPS

Add an attribute to an attribute group

Purpose

Use this procedure to add an attribute to an attribute group.

Procedure

To add an attribute to an attribute group, follow these steps.

1 Mouse over **Infrastructure** and click **Attribute**.

Result: The Attributes Hierarchy opens.

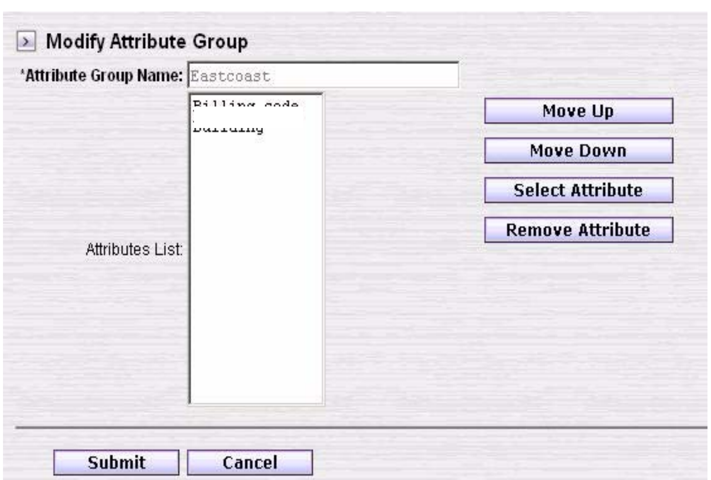
2 Expand the list of attribute groups until you see the attribute group you want to add an attribut.

3 Click the attribute group.

Result: The Attribute Group Properties page.

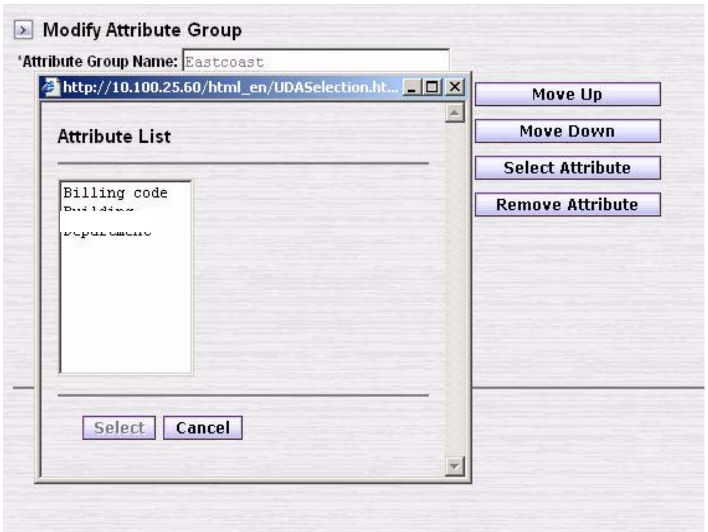
4 Click **Modify**.

Result: The Modify Attribute Group page opens.



5 Click **Select Attribute** to add an attribute to this attribute group.

Result: A list of available attributes opens.



6 Click as many attributes as you want to add to the attribute group and then click **Select**.

7 Click **Submit**.

Result: The attribute is added to the group.

END OF STEPS

Delete an attribute from an attribute group

Purpose

Use this procedure to delete an attribute from an attribute group.

Procedure

To delete an attribute from an attribute group, follow these steps.

1 Mouse over **Infrastructure** and click **Attribute**.

Result: The Attributes Hierarchy opens.

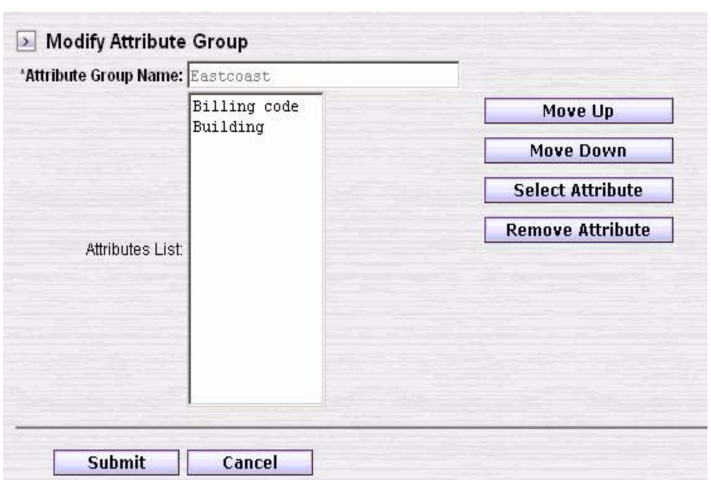
2 Expand the list of attribute groups until the one you from which you want to delete an attribute is visible.

3 Click the attribute group.

Result: The Attribute Group Properties page opens.

4 Click **Modify**.

Result: The Modify Attribute Group page opens.



5 Click the attribute you want to remove from the attribute group and then click **Remove Attribute**.

Result: The attribute is removed from the group.

6 Click **Submit**.

Result: The attribute is deleted from the attribute group.

END OF STEPS

Resequence attributes in an attribute group

Purpose

Use this procedure to change the sequence of attributes in an attribute group.

Procedure

To change the sequence of attributes in an attribute group, use the following steps:

1 Mouse over **Infrastructure** and click **Attribute**.

Result: The Attributes Hierarchy opens.

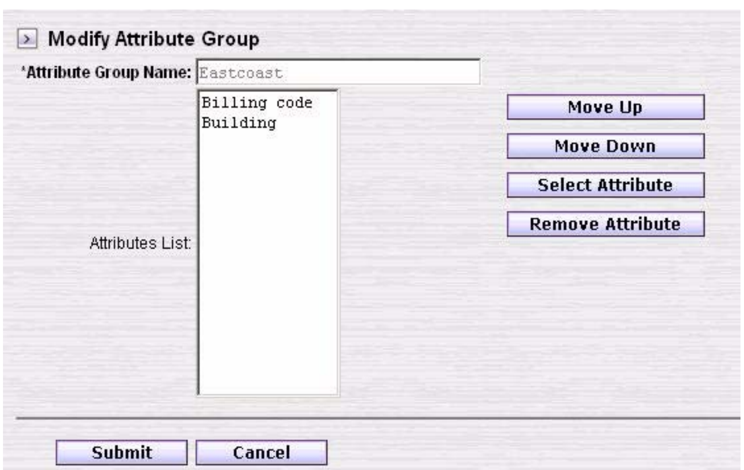
2 Expand the list of attribute groups until the one whose attributes you want to resequence is visible.

3 Click the attribute group.

Result: The Attribute Group Properties page opens.

4 Click **Modify**.

Result: The Modify Attribute Group page opens.



5 Select an attribute in the attribute list whose position you want to change, and click **Move Up** or **Move Down** until you have moved it to its new location in the list.

6 Click **Submit**. The attribute group is modified to reflect the new sequence of attributes.

END OF STEPS

Add an attribute or attribute group to an infrastructure type

Purpose

Use this procedure to add an attribute or attribute group to an infrastructure type. The following infrastructure types are available:

- Address Block
- Address Pool
- Device
- DHCP Server
- DNS Server
- DNS View
- Domain Controller
- Interface
- IPv4 Address
- IPv4 Subnet
- IPv6 Address
- IPv6 Subnet
- Managed File
- MyView
- Network
- Node
- Organization
- Subnet Organization
- Subscriber
- Zone

Before you begin

When you add an organization, it inherits the organizational user defined attributes from the current organization. When you view the Attribute Hierarchy in the organization that inherited the organizational attributes, you only see inherited organizational attributes under the **Infrastructure Type > Organization**. They do not appear under **Attribute** or **Attribute Group** in the Attribute Hierarchy.

Procedure

To add an attribute or attribute group, use the following steps:

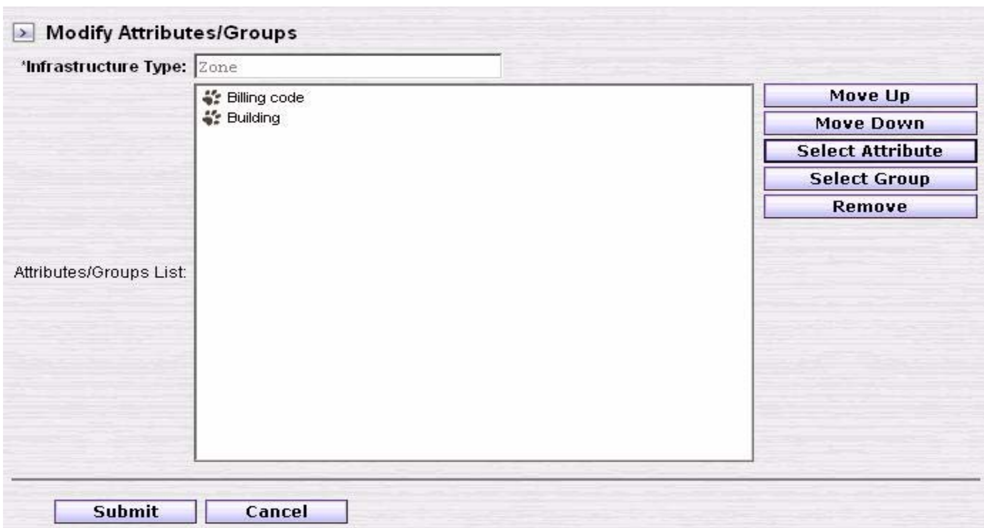
1 Mouse over **Infrastructure** and click **Attribute**.

Result: The Attributes Hierarchy opens.

2 Expand the list of infrastructure types until the one to which you want to add an attribute is visible.

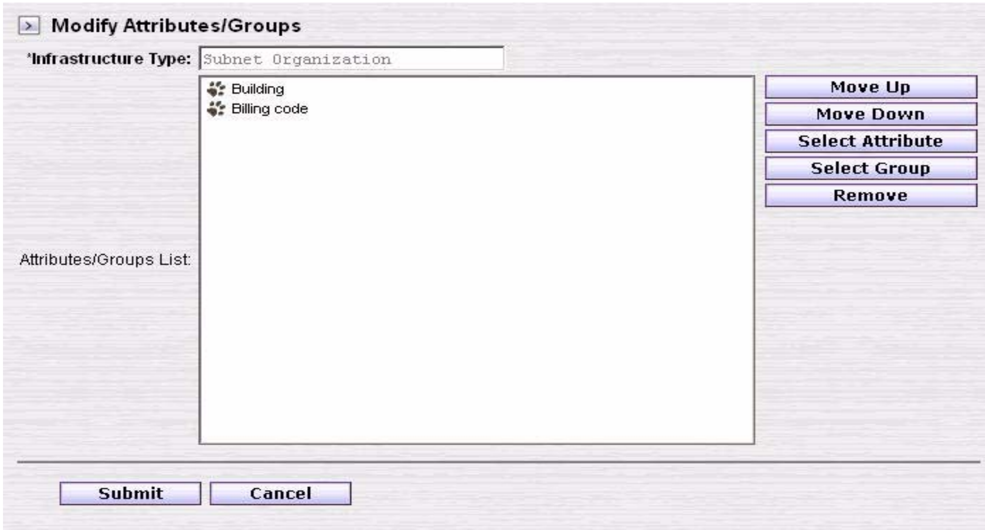
3 Click the infrastructure type (for example a pool or block) to which you want to add an attribute or attribute group.

Result: The Attributes/Group Properties page opens.

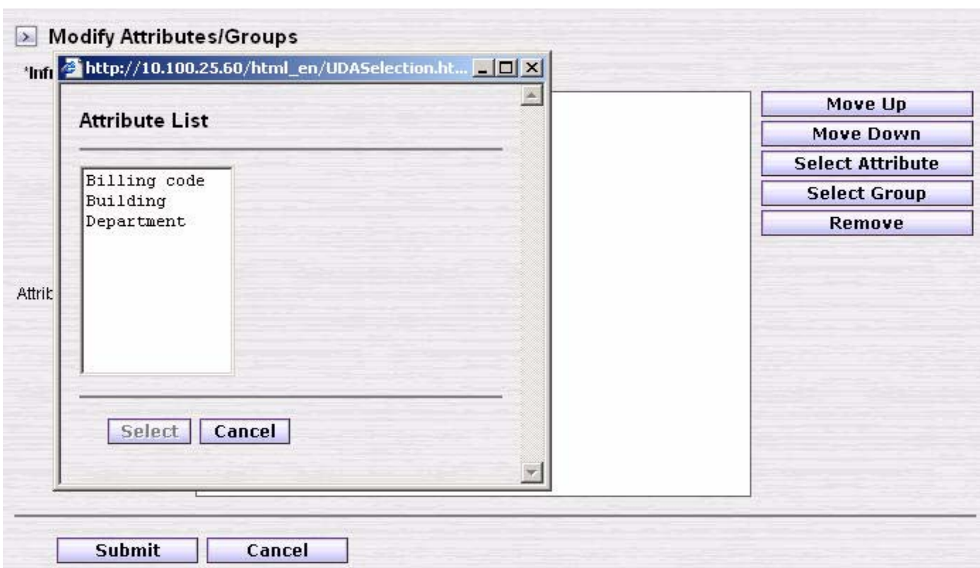


4 Click **Modify**.

Result: The Modify Attributes/Groups page opens.



5 Click **Select Attribute**. A list of available attributes opens.



Note: To add an attribute group, click **Select Group** to see a list of available attribute groups.

6 Click an attribute and then click **Select**. The attribute or attribute group is assigned to the infrastructure type.

7 Click **Submit**.

Result: A dialog box opens with the message **Attributes/Groups list Modified.**

8 Click **OK**.

Result: The updated Attribute Group Properties page is displayed.

END OF STEPS

Delete an attribute or attribute group from an infrastructure type

Purpose

Use this procedure to delete an attribute or attribute group from an infrastructure type, such as a pool or block

Procedure

To delete an attribute or attribute group from an infrastructure type, use the following steps:

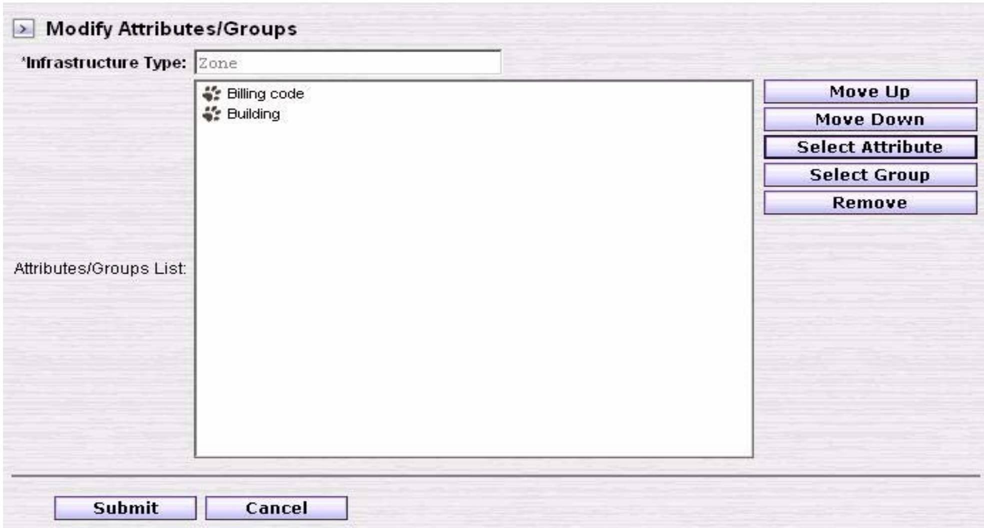
1 Mouse over **Infrastructure** and click **Attribute**.

Result: The Attributes Hierarchy opens.

2 Expand the list of infrastructure types until the one from which you want to delete an attribute is visible.

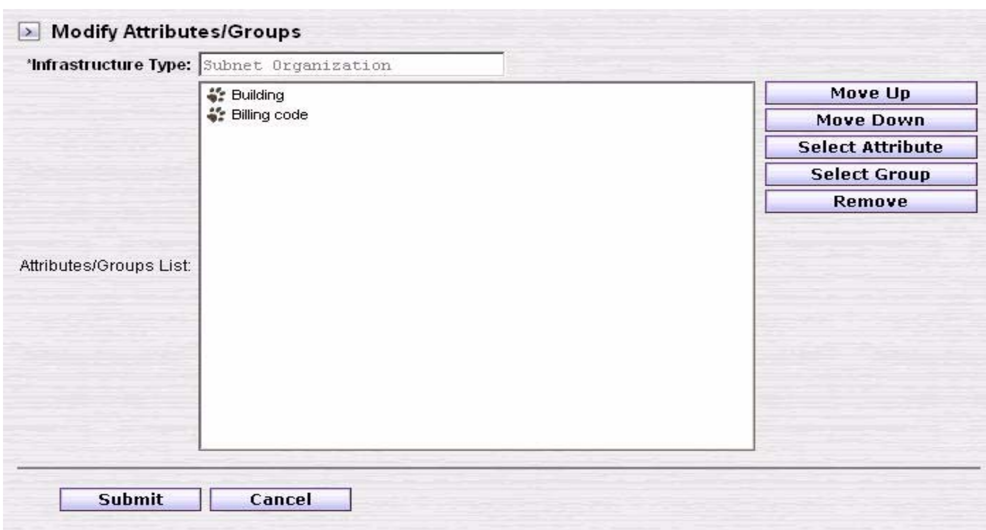
3 Click the infrastructure type (for example a pool or block) from which you want to delete an attribute or attribute group.

Result: The Attributes/Group Properties page opens.



4 Click **Modify**.

Result: The Modify Attributes/Groups page opens.



5 Click the attribute or group you want to delete and then click **Remove**. The attribute or attribute group is removed from the infrastructure type.

Note: This function only removes an attribute or attribute group from an infrastructure type. It does not delete it from the database.

6 Click **Submit**.

Result: A dialog box opens with the message **Attributes/Groups List Modified.**

7 Click **OK**.

Result: The updated Attributes/Groups Properties page is displayed.

END OF STEPS

Working with user defined attributes and fields

Overview

Purpose

User defined attributes and fields appear through the system in their own sections. The sections vary slightly depending on how the user defined attributes and fields are being used. The variances occur when user defined attributes and fields are used in the searches or where input can be entered.

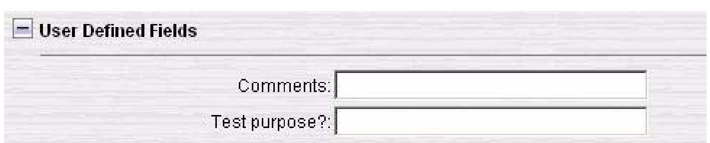
User defined fields and the web client

User defined fields are set up in the VitalQIP client via **User-Defined Fields** from the VitalQIP client. User defined fields are displayed only with IPv4 related infrastructure. Since all organizations have the same UDFs, all administrators can add, modify, and delete UDF values. Refer to the *VitalQIP User's Guide* for more information.

User Defined Fields section

When user defined fields are used to collect information, the **User Defined Fields** section can look as follows.

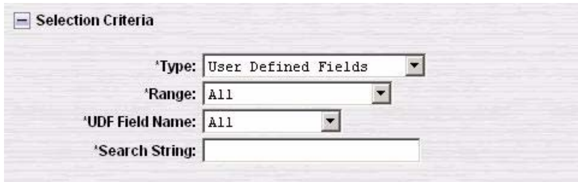
Figure 7-1 User Defined Fields section for information input



When user defined fields are used as search criteria, the **User Defined Fields** section looks as follows.

> **Note:** If both user defined attributes and fields are associated, the User Defined Attributes and User Defined Fields option are shown as opposed to individual sections. Select one of these options to display the appropriate section.

Figure 7-2 User Defined Fields section as search criteria



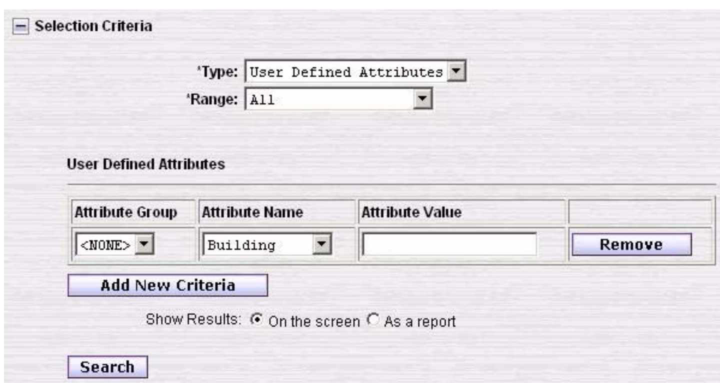
User Defined Attributes section

When user defined attributes are used to collect information, the **User Defined Attributes** section can look as follows.

Figure 7-3 User Defined Attributes section for information input

When user defined attributes are used as search criteria, the **User Defined Attributes** section looks as follows.

Figure 7-4 User Attributes Fields section as search criteria



Enter information in user defined attributes or fields

Purpose

Use this procedure to enter information in user defined attributes or fields.

Procedure

To enter information in user defined attributes or fields, follow these steps:

1 Expand or select:

- **User Defined Attributes**
- **User Defined Fields**

Result: Associated user defined attributes or fields are displayed.

2 In the user defined attributes or fields, enter the appropriate information.

3 Continue to enter other information as needed.

END OF STEPS

Use user defined fields as search criteria

Purpose

Use this procedure to specify user defined fields as search criteria.

Procedure

To specify values as search criteria, follow these steps.

1 Expand or select **User Defined Fields**.

Result: The **User Defined Fields** section opens.

2 Click **Add New Criteria**.

Result: A new user defined field row is displayed.

3 From the **Field Name** field, select the name of any user-defined field, or select **All**.

4 In the **Field Value** field, enter the text or wildcard * for which to search.

5 Click **Remove**, if you wish to remove the UDF.

6 Continue with the search.

END OF STEPS

Use user defined attributes as search criteria

Purpose

Use this procedure to select and specify values for a UDA.

Before you begin

You can add a maximum of five user defined attributes only.

Procedure

To specify values as search criteria, follow these steps.

1 Expand or select **User Defined Attributes**.

Result: The **User Defined Attributes** section opens.

2 Click **Add New Criteria**.

Result: A new user defined attribute row is displayed.

3 Review the following table and fill in the fields you need to complete your search.

Table 7-2 User Defined Attribute fields

Field	Description
Attribute Group	***Required if visible***. If specified, the search is limited to this attribute group. You can specify any attribute groups currently associated with the Pool or one of two pre-defined entries: • **<NONE>** – Select this entry to exclude the Attribute Group from this search criteria row. • **<IGNORE>** – Select this entry if, for this search criteria row, you do not care if a UDA is in a group or not. • **<ANY>** – Select this entry to include all the Attribute Groups in this search criteria row.
Attribute Name	***Required if visible***. If specified, the search is limited to this attribute value. Values in this column are based on the value in the **Attribute Group** column. The available values are: • All Attributes that do not attach to any Attribute Group, plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<NONE>**. • All Attributes plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<IGNORE>**. • All Attributes attached to the specified Attribute Group, plus the pre-defined entry **<ALL>** – if an Attribute Group is selected. • All Attributes attached to at least one Attribute Group, plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<ANY>**.
Attribute Value	Full or partial name (with wildcard) of the attribute. To search for an attribute with a null value, enter two double quotes (“ ”).

4 Click **Remove**, if you wish to remove the user defined attribute.

5 Continue with search.

END OF STEPS

8 Domain Controller maintenance

Overview

Purpose

This chapter describes how to manage Domain Controllers, as well as generate the information on subnets and subnet organizations that Windows stores in its Active Directory.

Contents

This chapter covers these topics.

Domain Controller management

Overview

Because a Windows site and VitalQIP manage much the same information on subnets and subnet organizations, you can set up a server to act as a Windows Domain Controller and add, modify, and even delete sites and subnets in the server's Active Directory (AD) from within VitalQIP. Use the global policy **Delete Sites/Subnets from Active Directory** to control whether a push deletes site and subnet information. Once a Domain Controller is defined, you can associate that server with a subnet organization, using the Windows Site section in the Subnet Organization page (refer to "Add a Windows site" (p. 9-83)). Information on the subnets and subnet organizations can be pushed to Windows 2003 Active Directory (identified by the **Active Directory Domain Name** parameter in the Domain Controller server profile), using **Perform DC Generation** on the Domain Controller Server Properties page. Refer to "Generate Domain Controller configuration files" (p. 8-12).

Note: Remote server does not need to be installed on the Domain Controller to support the functionality described above. When a push is performed, VitalQIP connects directly to the directory server via the LDAP port to perform the generation.

Search for a Domain Controller

Purpose

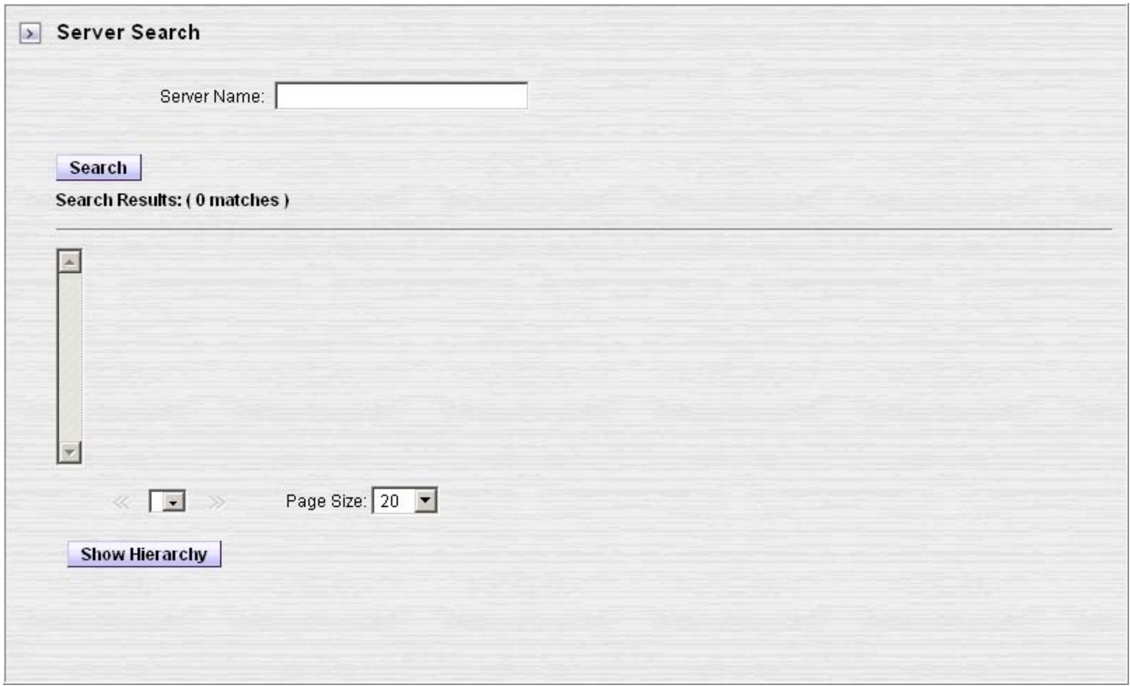
Use this procedure to search for a Domain Controller.

Procedure

To search for a Domain Controller, follow these steps.

1. Select **Domain Controller** from the **Infrastructure** menu.

Result: The Domain Controller Hierarchy opens with Server Search.



2 Enter search criteria in the **Server Name** field and click **Search**.

Result: A list of previously defined domain controllers opens in the **Search Results** list.

3 Select the Domain Controller you want from the list and click **Show Hierarchy**.

Result: The server appears in the Domain Controller Hierarchy.

4 Select the server in the Domain Controller Hierarchy.

Result: The Server Properties page opens.

5 Choose one of the following actions.

If you want to …	Then …
Generate Domain Controller configuration files	Click **Perform DC Generation**. Refer to "Generate Domain Controller configuration files" (p. 8-12).
Manage Windows site associations	Click **Manage Sites**. Refer to "Manage sites" (p. 8-9).
Modify Domain Controller properties	Click **Modify**. Refer to "Modify a Domain Controller" (p. 8-7).
Delete the selected Domain Controller	Click Delete. Refer to "Delete a Domain Controller" (p. 8-16).
Run an audit report	Click Reports. Refer to "Produce a DC Generation Audit report" (p. 29-124).

END OF STEPS

Create a Domain Controller

Purpose

Use this procedure to create a Domain Controller.

Procedure

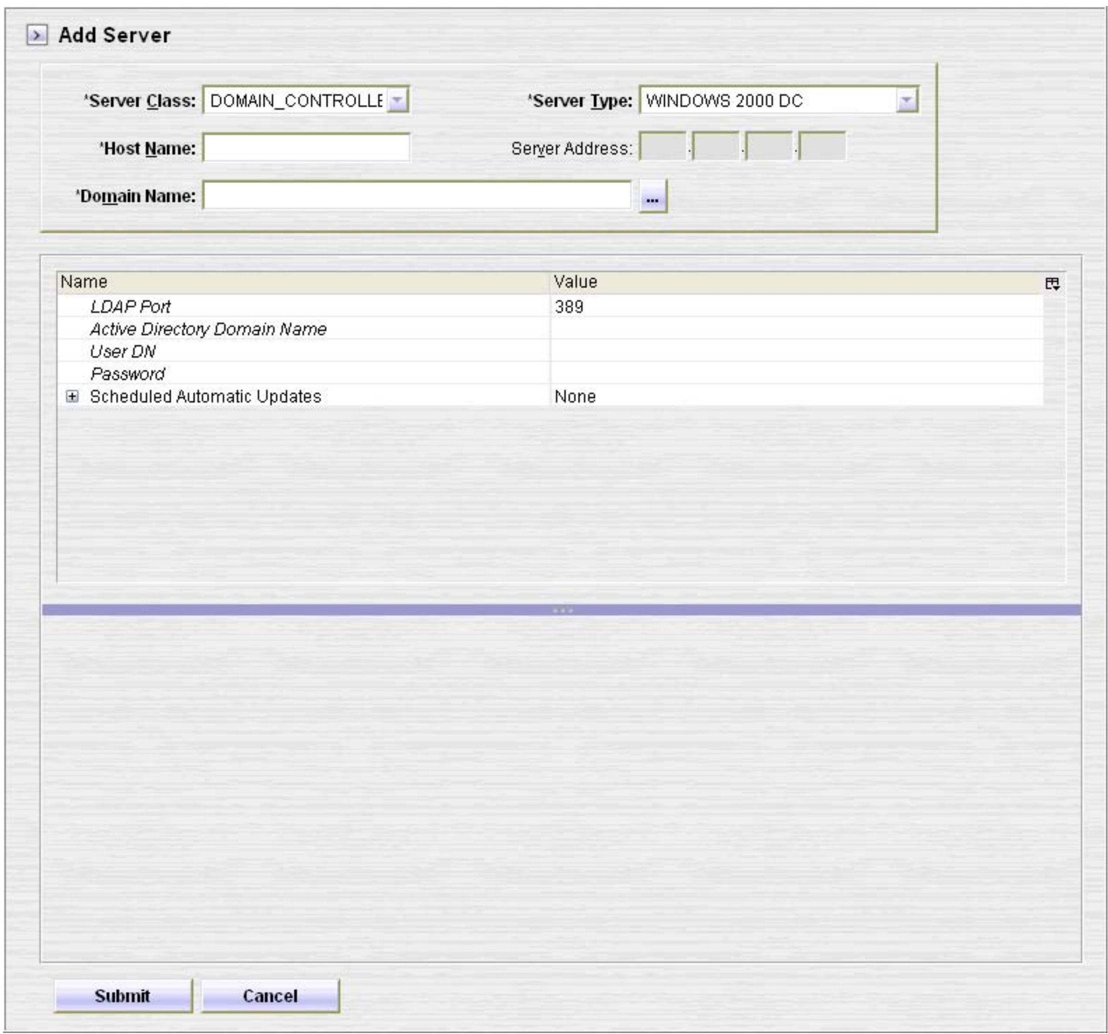
To create a Domain Controller.

1 Select **Domain Controller** from the **Infrastructure** menu.

Result: The Domain Controller Hierarchy opens.

2 Mouse over the **Actions** menu and select **Add Server**.

Result: The Add Server page opens.



3 Refer to the following table as you enter information in the fields. The **Server Class** and **Server Type** fields are pre-defined.

Table 8-1 Domain Controller fields

Field	Description
Host Name	***Required***. Enter a server host name. You can enter a maximum of 63 alphanumeric characters beginning with an alphanumeric. The host name may include the dash (-) character, but cannot contain plus signs (+), exclamation marks (!), or underscores (_). **Note:** Make a note of the host name because when you assign an IP address to the server, you need to assign the host name in the **Object Name** field. Refer to "Enter object information" (p. 10-37).
Domain Name	***Required***. Enter a domain name, or click  to open the Domain Search window and select a domain from the search results.
LDAP Port	***Required***. Identifies the LDAP Port. Default value is 389.
Active Directory Domain Name	***Required***. Identifies the active directory domain name.
User DN	***Required***. The Distinguished Name of the User defined in Active Directory that is used to connect to the directory server. For example, for **`Joe User`** in domain **`your.domain.com`** defined in the default Users folder, the DN would look as follows: **`CN=Joe User,CN=Users,DC=Your, DC=Domain,DC=com`** The user must have adequate permission to add, modify, and delete sites and subnets from Active Directory.
Password	***Required***. The password used to connect to Active Directory Domain Name. By default, the password is secret and encrypted in the database.

Field	Description
Scheduled Automatic Updates	Select **By Day** to push policy and configuration files on a daily basis. Select **By Interval** to push at a certain time interval (the default is 1 hour, which is also the minimum permitted). If this parameter is set to **None**, administrators can manually request VitalQIP to generate the DC data.

4 Click **Submit**.

END OF STEPS

Modify a Domain Controller

Purpose

Use this procedure to modify a Domain Controller.

Procedure

To modify a Domain Controller, follow these steps.

1 Select Domain Controller from the Infrastructure menu.

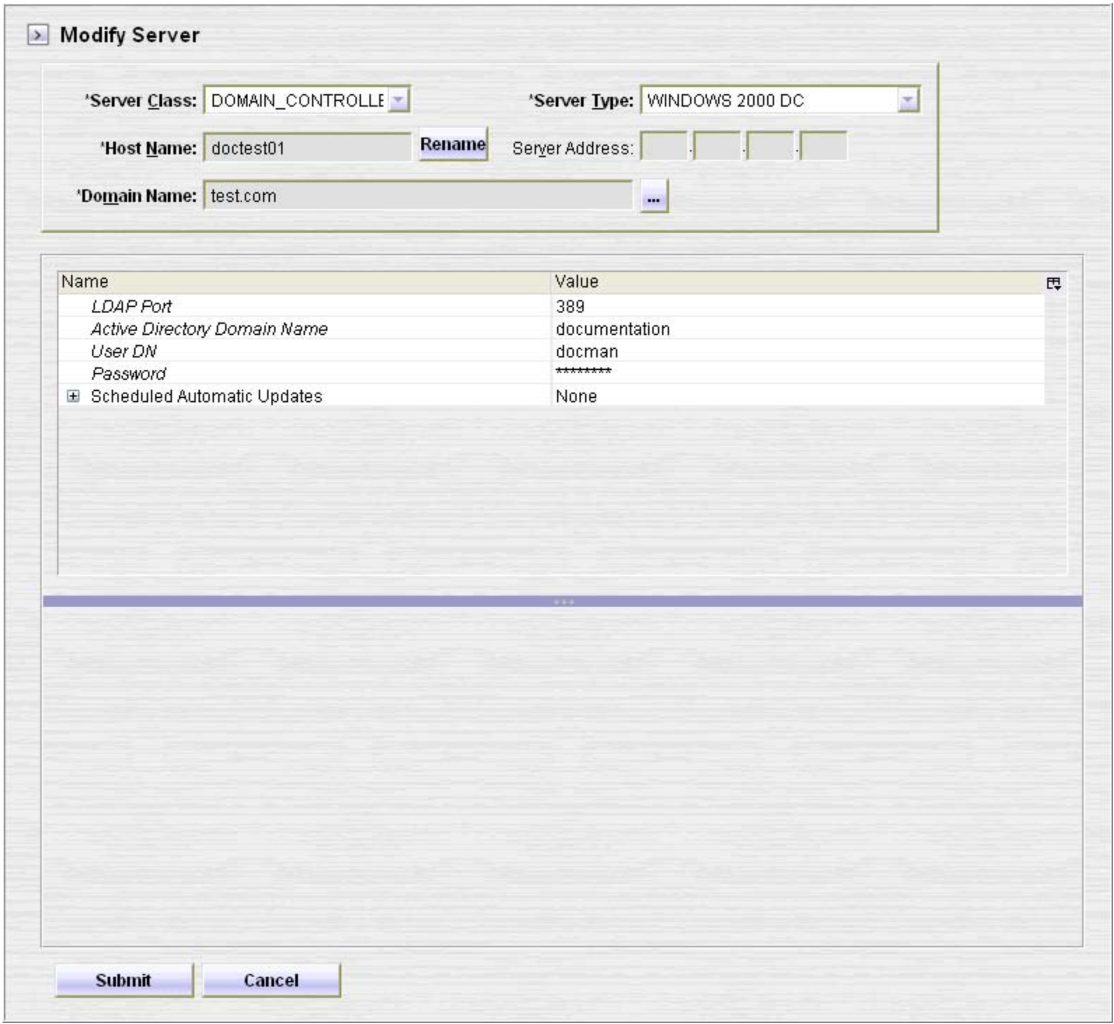
Result: The Domain Controller Hierarchy opens.

2 Locate the server you want to modify in the Domain Controller server hierarchy. Refer to "Search for a Domain Controller" (p. 8-2) for further information.

Result: The Server Properties page opens.

3 Click **Modify**.

Result: The Modify Server page opens.



4 Make changes as needed. To change the host name, click **Rename** and enter a valid name in the **New Host name** field. For information on field values, refer to Table 8-1, “Domain Controller fields” (p. 8-6).

5 Click **Submit**.

Result: A dialog opens with the message **Saved DOMAIN_CONTROLLER Server:** *<host name>*.

6 Click **OK**.

Result: The Server Properties page opens.

END OF STEPS

Manage sites

Purpose

Use this procedure to manage Domain Controller sites.

Before you begin

Similar functionality for managing a Windows site is available in the Windows Site section of the Add Subnet Organization and Modify Subnet Organization pages. Refer to "Add a Windows site" (p. 9-83).

Procedure

To manage Domain Controller sites, follow these steps.

1. Select **Domain Controller** from the **Infrastructure** menu.

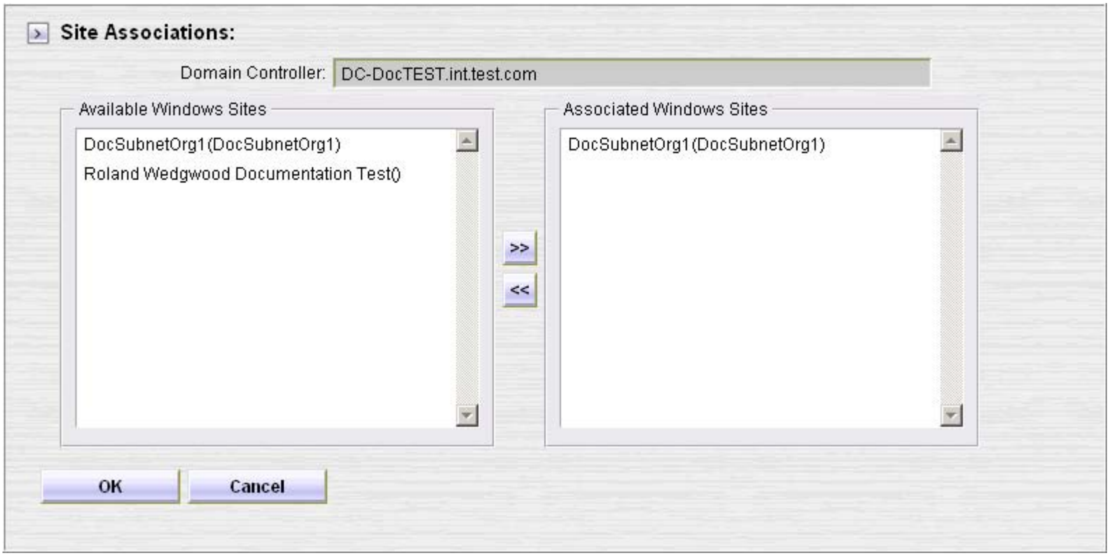
   Result: The Domain Controller Hierarchy opens.

2. Locate the server you want to modify in the Domain Controller server hierarchy. Refer to "Search for a Domain Controller" (p. 8-2) for further information.

   Result: The Server Properties page opens.

3. Click **Manage Sites**.

Result: The Site Associations page opens.



4 Choose one of the following actions if you wish to modify Windows site associations.

- To add a Windows site association, select an entry in the **Available Windows Sites** list and click >>.
- To remove a Windows site association, select an entry in the **Associated Windows Sites** list and click <<.

5 To save modifed Windows site associations, click **OK**.

Result: A dialog opens with the message **Site Associations Saved**.

6 Click **OK**.

Result: The Server Properties page opens.

END OF STEPS

View Windows site associations

Purpose

To view Windows site associations for a Domain Controller.

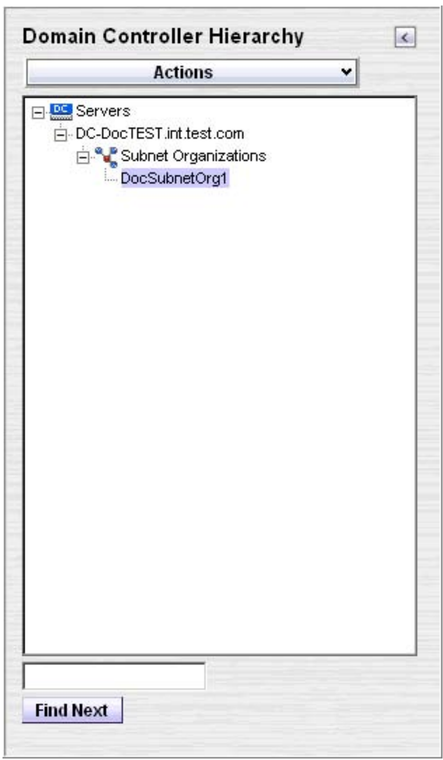
Procedure

To view Windows site associations for a Domain Controller, follow these steps.

1 Select **Domain Controller** from the **Infrastructure** menu.

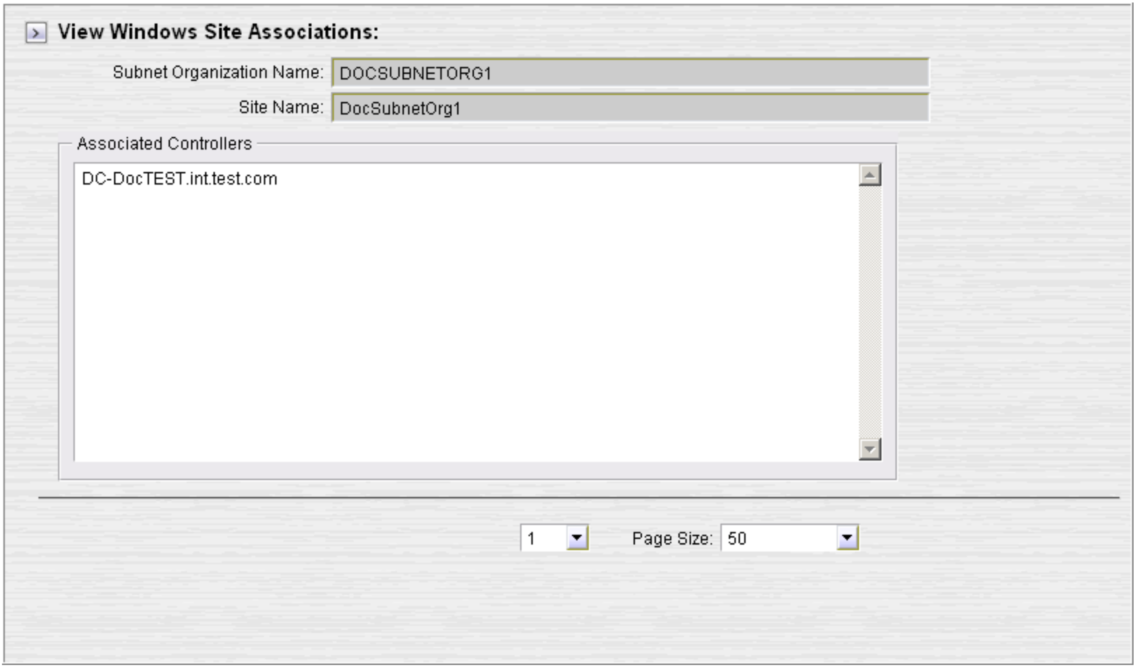
Result: The Domain Controller Hierarchy opens.

2 Expand the hierarchy until the subnet organizations associated with the Domain Controller appear.



3 Select the Domain Controller whose associations you want to view.

Result: The View Windows Site Associations page opens.



END OF STEPS

Generate Domain Controller configuration files

Purpose

Use this procedure to generate configuration files for a Domain Controller.

Procedure

To generate configuration files for a Domain Controller, follow these steps.

1 Select **Domain Controller** from the **Infrastructure** menu.

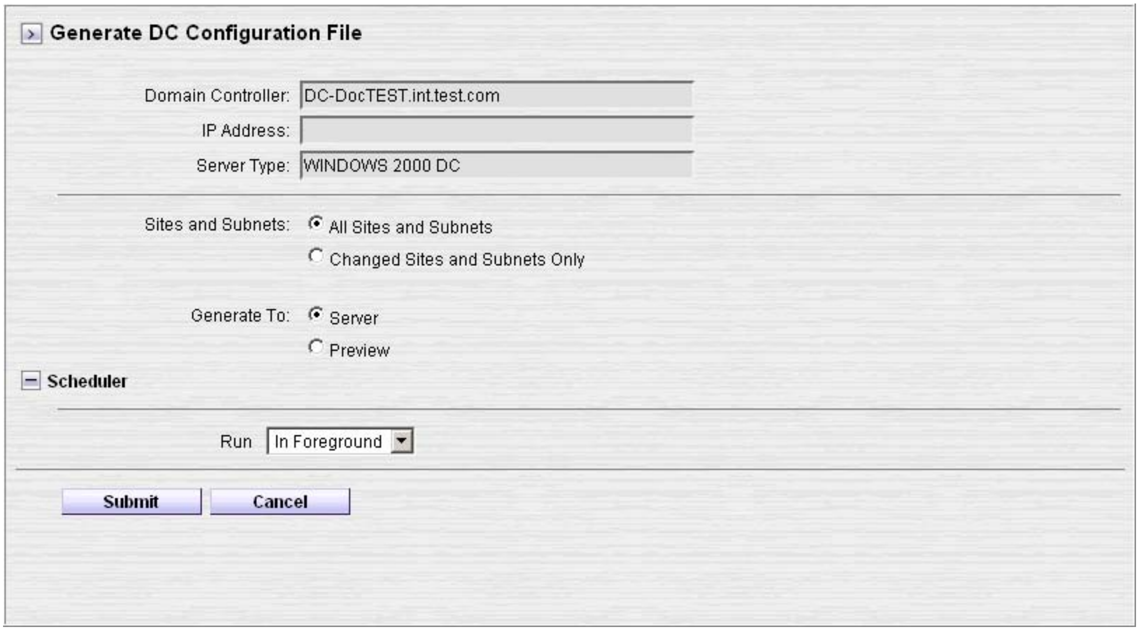
Result: The Domain Controller Hierarchy opens.

2 Locate the Domain Controller for which you want to generate configuration files. Refer to "Search for a Domain Controller" (p. 8-2) for further information.

Result: The Server Properties page opens.

3 Click **Perform DC Generation**.

Result: The Generate DC Configuration File page opens.



4 Choose a **Sites and Subnets** option. Click **Changed Sites and Subnets Only** to push information on sites and subnets that have been modified, or click **All Sites and Subnets** to push to all sites and subnets in a domain.

5 Choose a **Generate To** option. Select **Server** to send the site and subnet records in LDAP Data Interchange Format (LDIF) to the Domain Controller, or **Preview** to generate them on the web server. Files can then be downloaded to the user's PC client.

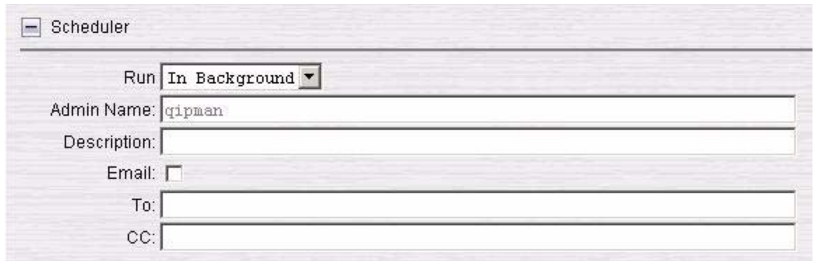
6 Choose when to generate files in the **Scheduler** section. Choose one of the following actions.

If you want to…	Then…
Run the job immediately	Ensure that **In Foreground** is selected in the **Run** drop-down list.

<table>
<tr><th>If you want to…</th><th>Then…</th></tr>
<tr><td>Run the job in background</td><td>

1. Select **In Background** from the **Run** drop-down list.

Result: The Scheduler section expands to display additional fields.



The **Admin** field displays the login ID of the administrator who is scheduling the job,

2. Enter a description of the job in the **Description** field. If you do not enter a description, a description of *<Job Name>:<Run Mode>* is used. You may enter up to 255 characters.
3. If you want an email to be sent when the job completes, place a check in the **Email** check box.

Result: The **To** and **CC** fields are enabled.

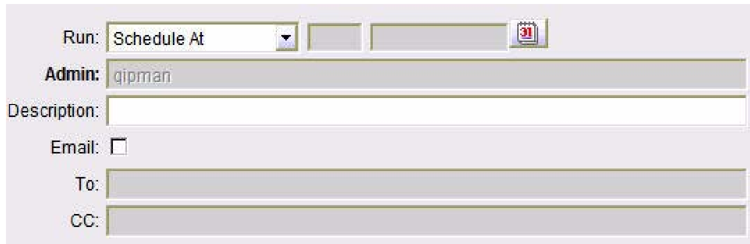
4. Enter an email address of up to 255 characters in the **To** field. If an email address has been entered in the **Contact Profile** for the administrator, it appears by default.
5. If desired, enter a **CC** email address.

</td></tr>
</table>

<table>
<tr><th>If you want to...</th><th>Then...</th></tr>
<tr><td>Schedule the job for a later time</td><td>

1. Select **Scheduled At** from the **Run** drop-down list.

Result: The Scheduler section expands to display additional fields, including a calendar icon.



The **Admin** field displays the login ID of the administrator who is scheduling the job,

2. Click the Calendar icon ( ).

Result: The Calendar widget opens with the current date and time.

3. Choose from the following actions.
   a. To choose a different time, click in the hour and minute fields and enter a new time in 24-hour format.
   b. To choose a different month, choose a later month from the month drop-down list.
   c. To choose a different year, click > to enter a future year or < to return to a prior year.
   d. To choose a different day, click another day in the month.

Result: After a different day is clicked, the calendar widget closes and a new run date and/or time are displayed.

4. Enter a description of the job in the **Description** field. If you do not enter a description, a description of *`<Job Name>:<Run Mode>`* is used. You may enter up to 255 characters.

</td></tr>
</table>

If you want to…	Then…
	5. If you want an email to be sent when the job completes, place a check in the **Email** check box. **Result:** The **To** and **CC** fields are enabled. 6. Enter an email address of up to 255 characters in the **To** field. If an email address has been entered in the **Contact Profile** for the administrator, it appears by default. 7. If desired, enter a **CC** email address.

7 Click **Submit**.

Result: If run in foreground, the configuration files are generated. A dialog opens with the message **DC Generation status successful**.

Result: If run in background or scheduled for a later time/date, a dialog opens with the message **Job scheduled. Job Id is <##>. Continue to the job scheduler page?**

8 Click **OK**.

END OF STEPS

Delete a Domain Controller

Purpose

Use this procedure to delete a Domain Controller.

Procedure

To delete a Domain Controller, follow these steps.

1 Select **Domain Controller** from the **Infrastructure** menu.

Result: The Domain Controller Hierarchy opens.

2 Locate the server you want to delete in the Domain Controller server hierarchy. Refer to "Search for a Domain Controller" (p. 8-2) for further information.

Result: The Server Properties page opens.

3 Click **Delete**.

Result: A dialog opens with the message **Are you sure you want to delete the Domain Controller <host name>?**

4 Click **OK**.

Result: A confirmation dialog opens with the message **Domain Controller deleted successfully**.

5 Click **OK**.

END OF STEPS

Part II: Address management

Overview

Purpose

This part of the manual provides information for managing the IPv4 and IPv6 addresses and objects.

Contents

This part includes these chapters.

9 IPv4 address management

Overview

Purpose

This chapter describes the functions used to manage the network space for IPv4 addresses.

Contents

This chapter covers these topics.

IPv4 address management

Overview

Purpose

IPv4 Address management allows you to manage IPv4 subnets, subnet organizations, and networks. IPv4 address management allows you to add, delete, move or modify objects defined within an IPv4 subnet. It also allows you to define address scopes/ranges.

IPv4 Hierarchy

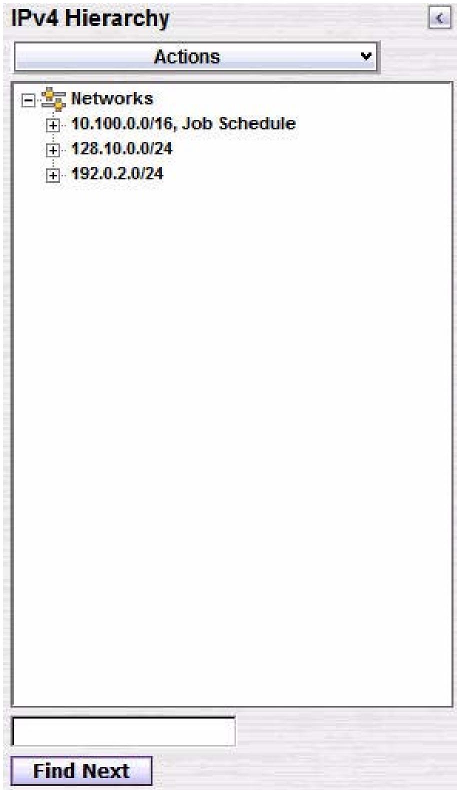
Overview

When you mouse over the Address Management tab and select IPv4, the IPv4 Hierarchy displays. The IPv4 hierarchy allows you to display subnets by their associated networks, domains, or subnet organizations.

Networks

The initial display shows a Networks node. The **Actions** menu allows you to change the display to domains, subnet organizations or subnets. You can expand any of these hierarchies to view all subnets defined for the item you have selected.

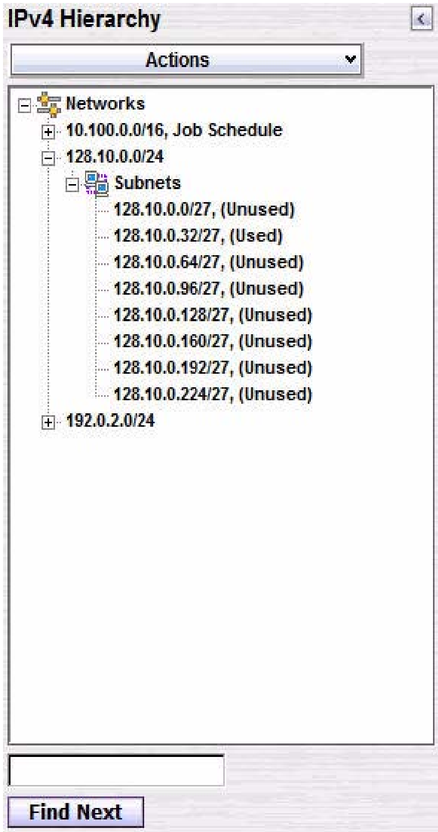
Figure 9-1 IPv4 Hierarchy - Networks node



Subnets

When you expand a network node, a Subnet node displays below it. If you expand that node, all subnets defined for that network display.

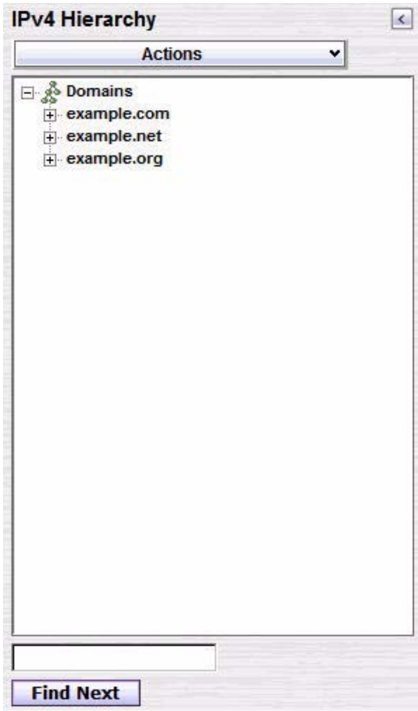
Figure 9-2 IPv4 Hierarchy - Networks and Subnets nodes



Domains

To see networks and subnets that are defined for a specific domain, you can mouse over **Actions** and select **Domains**. You can then expand the Domains node to see all domains defined for the organization.

Figure 9-3 IPv4 Hierarchy - Domains node



When you expand a domain node, all networks defined for that domain display in the tree beneath the domain, with the exception of the instances described below. When you then expand a network, all subnets defined for the network display in the tree below the network.

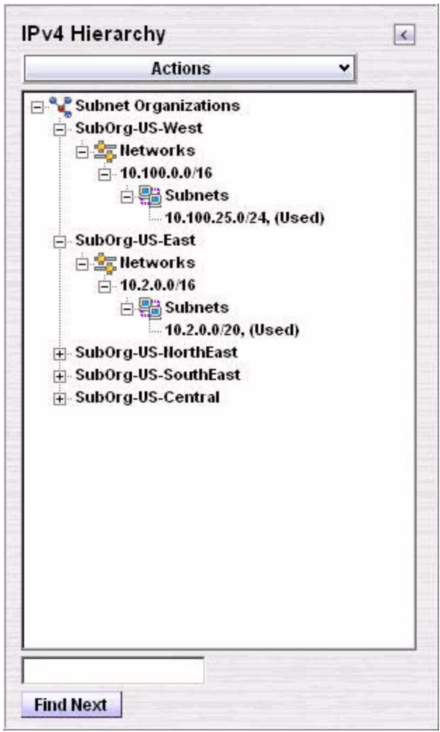
Subnets do not appear in the IPv4 Hierarchy Domain tree under the following circumstances:

- The IPv4 domain tree exists to show which networks have subnets associated with a particular domain. Domains that do not have a subnet association will not appear in the IPv4 Hierarchy Domain tree.
- ENUM zones, despite being stored as domains in the database, are different in that they exist to group phone numbers and have no real network/subnet association. These zones, as well as other domains without subnet associations, can be found under the MyView Hierarchy Domain tree.

Subnet Organizations

You can also see subnet organizations for your organization. Mouse over **Actions** and select **Subnet Organization**. A list of subnet organizations displays. You can expand each subnet organization to see the networks and subnets defined within it.

Figure 9-4 IPv4 Hierarchy - Subnet Organizations node expanded



Perform a global search

Purpose

Use this procedure to search for an IPv4 address management item.

Before you begin

- You can use the wildcard character (*) as part of the search string for all searches.
- When you complete a search with results and then navigate away from the IPv4 Hierarchy page, if you go back to the search results window and click a link, the message **Can't find the search parent screen, this search dialog will be closed now! Please invoke IPv4 search again** will be displayed. Click **OK** to close the message and perform another global search.

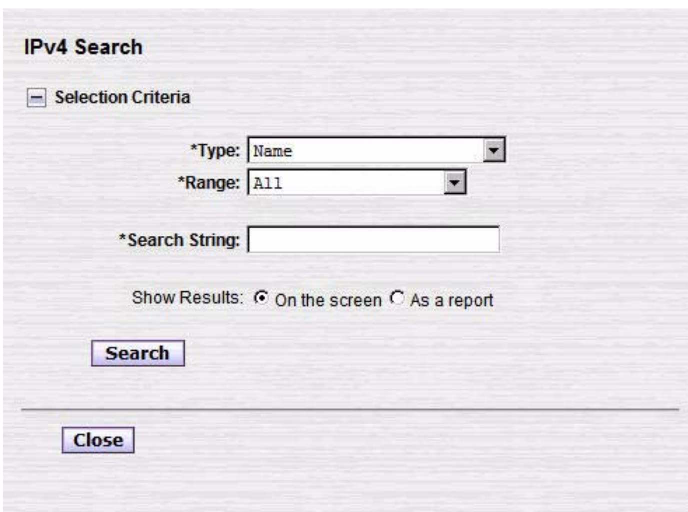
Procedure

To search for an item in the IPv4 hierarchy, follow these steps.

1 Choose one of the following actions to begin.

If you are..	**Then.**
Accessing the search from the IPv4 Hierarchy	1. Mouse over **Address Management** tab and click **IPv4**. **Result:** The IPv4 Hierarchy opens. 2. Mouse over **Actions** and select **Search**.
Accessing the search from the MyView Hierarchy	1. Mouse over **MyView** and click **MyView Hierarchy**. **Result:** The MyView Hierarchy opens. 2. Expand the hierarchy and select an IPv4 item. 3. Mouse over **Actions** and select **Search**.

Result: The IPv4 Search window opens.



2 Choose one of the following actions.

If you are...	Then...
Searching by name	1. From the **Type** field, select **Name**. 2. From the **Range** field, select one of the following: • **All** • **Domain** • **Network** • **Subnet Organization** • **Subnet** • **Object/IPv4 Address** • **Alias Name** • **Router Group** • **View Specific FQDN** 3. In the **Search** field, enter freeform text. You may use the * wildcard character for 0 or more characters.
Searching by address	1. From the **Type** field, select **Address**. 2. From the **Range** field, select one of the following: • **All** • **Network** • **Subnet** • **Object/IPv4 Address** • **View Specific FQDN** 3. In the **Search** field, enter a valid IP address. You can only use a trailing * wildcard character, but each octet must be complete. For example 135.106.* is a valid search address. If you enter an invalid IP address, no matches are returned.
Searching by MAC address	1. From the **Type** field, select **MAC Address**. 2. In the **Search** field, enter a valid MAC Address. The MAC address must be in either 12 or 16 hexadecimal character format. You can use the * wildcard character. For example `adef*` is a valid search address. **Note:** This MAC address length is determined by the **Allow 16 Character MAC Address** global policy. **Note:** You cannot currently enter the `:` character as part of a search.

If you are...	**Then...**
Searching by user defined fields	1. From the **Type** field, select **User Defined Fields**. 2. From the **Range** field, select one of the following: • **All** • **Organization** • **Domain** • **Subnet** • **Object/IPv4 Address** 3. From the **UDF Field Name** field, select **All** or a user defined field. 4. In the **Search** field, enter a value. You can use the * wildcard character.
Searching for user defined attributes	1. From the the **Type** field, select **User Defined Attributes**. 2. From the **Range** field, select: • **All** • **Organization** • **Domain** • **Subnet Organization** • **Subnet** • **Object/IPv4 Address** • **Network** 3. From the **Attribute Group** field, select: • **<NONE>** - the user defined attribute list only displays user defined attributes without associated user defined groups • **<IGNORE>** - the user defined attribute ist displays all user defined attributes regardless of the user defined group association • **<ANY>** - the user defined attribute list displays any user defined attributes that has a user defined group association 4. From the **Attribute Name** field, select the required user-defined attribute. 5. From the **Attribute Value** field, enter text based on the item for which you are searching. 6. To add more search user defined attribute search criteria, click **Add New Search Criteria** and repeat Step 2 to Step 5. You can use the * wildcard character.

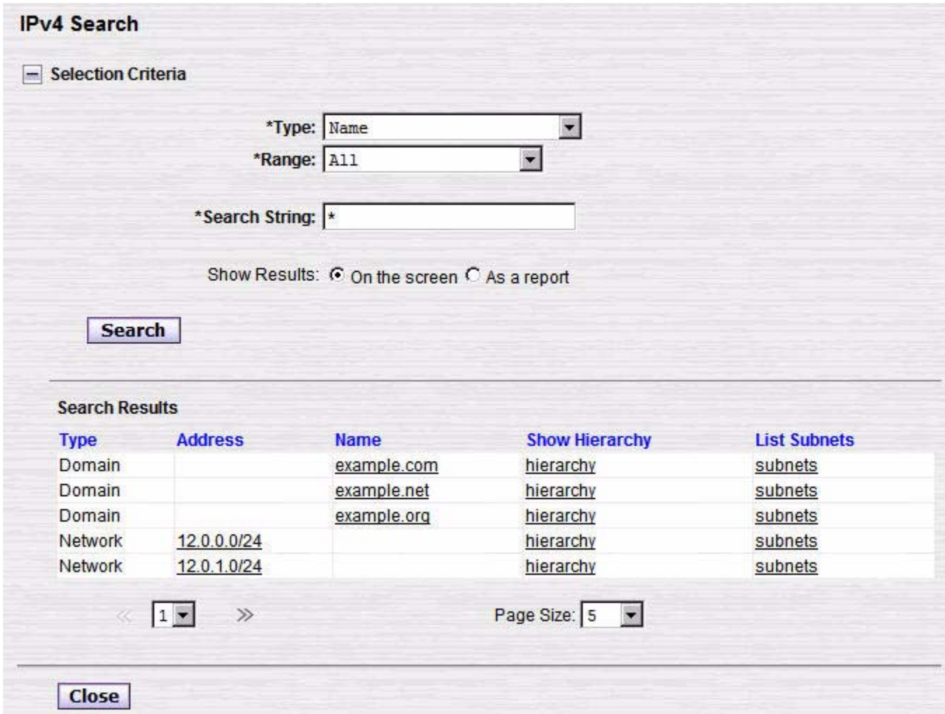
3 Choose one of the **Show Results** options.

If you want to...	**Then ...**
Review search results on the screen	Click **On the screen**.

If you want to...	**Then ...**
Review search results as a report	1. Click **As a report**. **Result:** The **Report Format** and **Run** fields open. 2. Select **html** to produce an HTML report, or select **pdf** to produce a report in PDF format. 3. To run the report immediately, select **In Foreground**. 4. To run the report in background, select **In Background**. **Result:** The Scheduler section expands to display additional fields. The **Admin** field displays the login ID of the administrator who is scheduling the job. a. If desired, enter a description of the job in the **Description** field. A description of <Run Mode>:<Job Name> is used by default. You can enter up to 255 characters. b. If you want an email to be sent when the job completes, check the **Email** check box. The **To** and **CC** fields are enabled. c. Enter an email address of up to 255 characters in the **To** field. If an email address has been entered in the Contact Profile for the administrator, it appears by default. d. If desired, enter a **CC** email address. Multiple emails must be separated by a comma (,) or semi-colon (;). 5. To run the report at a later time, select **Scheduled At**. **Result:** An additional date field opens with the scheduled date default of 10 days from the current date. 6. To modify the scheduled date and/or time, click  and choose a different time and/or date as needed.

4 Click **Search**.

Result: The results appear in the **Search Results** list. You can click on active links to view properties pages for specific items.



5 Click **Close** to exit the IPv4 Search window.

END OF STEPS

Use Quick Add

Purpose

Use this procedure to add an object to the subnet. This function allows you to add any type of object to any free address in the subnet.

Procedure

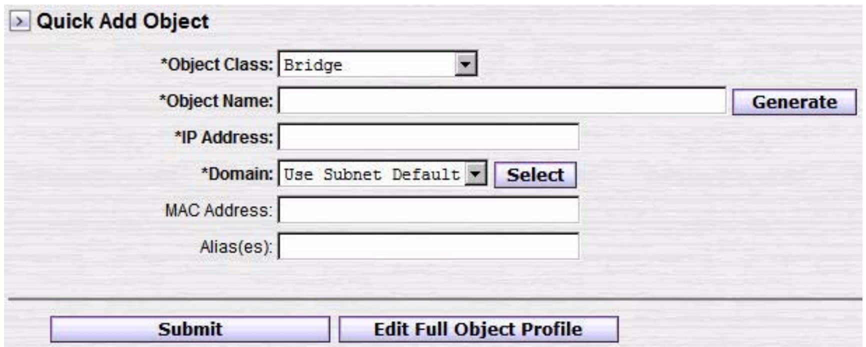
To add an object, follow these steps.

1 Mouse over **Address Management** tab and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over **Actions** and select **Quick Add**.

Result: The Quick Add page opens.



3 Review the following table and fill in the fields as necessary.

Table 9-1 Quick Add fields

Field	Description
Object Class	***Required***. Select a value from the drop-down list. For a definition of the allowable values, refer to Table 24-2, "Object classes" (p. 24-6).
Object Name	***Required***. Enter the name of the object you are adding or click **Generate** to have the system generate a name. This field can contain up to 63 characters. The first and last characters of this field must be alphanumeric.
IP Address	***Required***. Enter the IP address of the object you are adding.
Domain	***Required***. Select the domain of the object you are adding. Click **Select** to populate the drop-down list with all applicable domains, and select a domain from the list or select **Use Subnet Default**. You can also select **<None>**.
MAC Address	***Optional***. Enter the MAC address of the object you are adding.
Alias(es)	***Optional***. Enter the aliases of the object you are adding. **Note:** Multiple aliases must be separated by a space.

4 Choose one of the following actions.

If you want to...	Then...
Add the object without editing it	1. Click **Submit**. **Result:** The object is added and a confirmation dialog opens with the message **Object added:*<objectname>* - *<ipaddress>***. 2. Click **OK** to close the dialog box.
Add the object and edit its profile	1. Click **Edit Full Object Profile**. **Result:** The object is added and a confirmation dialog opens with the message **Object added:*<objectname>* - *<ipaddress>***. 2. Click **OK** to close the dialog box. **Result:** The object profile opens. 3. Edit the object profile, as described in "Object profile" (p. 10-36).

END OF STEPS

Use Quick Delete

Purpose

Use this procedure to delete an object.

Procedure

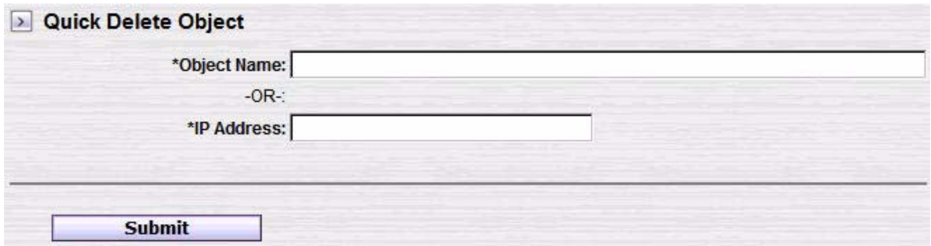
To delete an object, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over **Actions** and select **Quick Delete**.

Result: The Quick Delete page opens.



3 Enter either the Object Name or the IP Address of the object you want to delete.

- If you enter an IP address, it must be an exact match of an existing IP address.
- If you enter an object name:
  - You may enter an exact match.
  - You may enter one or more alphanumeric characters followed by the wildcard character (*). Click **Submit** to return a list of matching object names. You can then place a check in the **Select** checkbox for those objects you wish to delete.

4 Click **Submit**. A dialog box asks you if you are sure you want to delete the object or objects.

5 Click **OK**.

Result: A dialog box opens to confirm that the object was deleted.

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

END OF STEPS

Use Quick Move

Purpose

Use this procedure to move an object.

Procedure

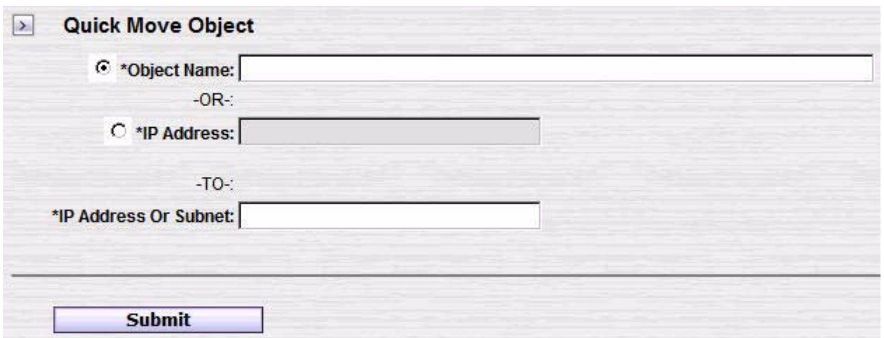
To move an object, follow these steps.

1 Mouse over the **Address Management** tab and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over **Actions** and select **Quick Move**.

Result: The Quick Move page opens.



3 Enter either the **Object Name** or the **IP Address** of the object you want to move.

- If you enter an IP address, it must be an exact match of an existing IP address.
- If you enter an object name:
  - You may enter an exact match.
  - You may enter one or more alphanumeric characters followed by the wildcard character (*). Click **Submit** to return a list of matching object names. You can then place a check in the **Select** checkbox for the object you wish to move.

Note: You can only move one object. If you select more than one, you receive an error message telling you that you can only move one object.

4 Enter either the **IP Address** or **Subnet** to which you are moving the object.

5 Click **Submit**.

Result: A dialog box asks if you are sure you want to move the object.

6 Click **OK**.

Result: The object is moved and the confirmation dialog opens with the message **Moved from:***<ipaddress>* **to:***<ipaddress>*.

7 Click **OK** to close the dialog box.

END OF STEPS

Quick View

Overview

Purpose

Quick View displays pictorial representation of domains, networks, and subnets within an organization. The Quick View option also allows hierarchy navigation. The **Quick View** option is accessible from the Domain Properties, Network Properties and Subnet Properties pages.

When you select this function, a grid view of all the selected subnets and/or objects is displayed. You can access the **Quick View** from any level of the network hierarchy, and the subnets are displayed in the Quick View window. From the subnet level, you can see the objects.

Move the mouse over the grid to display the object's address at the top of the window. The number of objects displayed in the Quick View window is configurable. If there are more than the configured number of objects, you can move to subsequent pages by using the drop-down page number at the bottom of the window.

Use Domain Quick View

Purpose

The Domain Quick View function allows you to see the network status of all domains within the organization.

Procedure

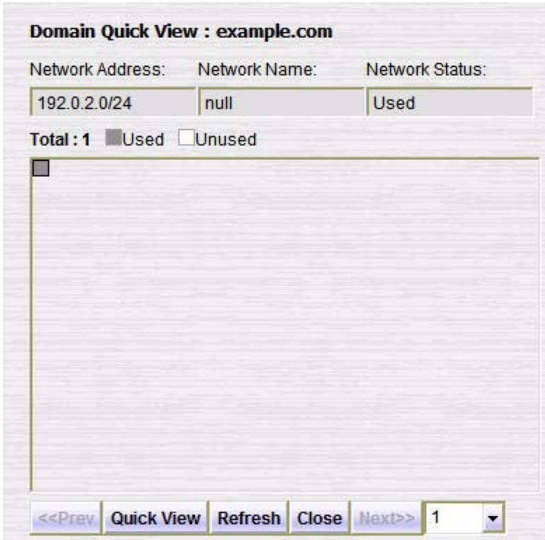
To access the Domain Quick View, follow these steps:

1. Select a Domain in the IPv4 Hierarchy.

   Result: The Domain Properties page opens.

2. Click **Quick View**.

Result: The Domain Quick View opens.



3 Click on a white square to see the network's IP Address, Name (if assigned) and Status displayed in the top of the Quick View Window.

4 Click **Refresh** to update the Quick View window to reflect changes in the status of the displayed network.

5 To see a Quick View of a network, click the box representing that network, and then click **Quick View**.

Result: The Quick View page opens information about the selected network. See "Use Network Quick View" (p. 9-20) for details on the Network QuickView.

6 Click **Close** when you are finished.

END OF STEPS

Use Network Quick View

Purpose

The Network Quick View function allows you to see the status of all subnets within the network.

Procedure

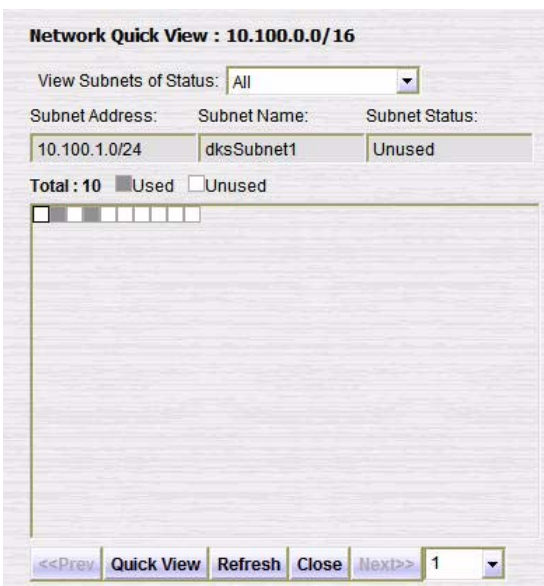
To access the Network Quick View, follow these steps:

1 Select a network in the IPv4 Hierarchy.

Result: The Network Properties page opens.

2 Click **Quick View**.

Result: The Network Quick View opens.



3 Click on a white square to see the object's IP Address, Name (if assigned) and Status displayed in the top of the Quick View Window.

4 Select a status from the **View Subnets of Status** drop-down list if you want to see only subnets of a certain status. Allowable values are:

- All
- Unused
- Used

5 Click **Refresh** to update the Quick View window to reflect changes in the status of the displayed subnets.

6 To see a Quick View of a subnet, click the box representing that subnet, and then click **Quick View**.

Result: The Quick View page displays information about the selected subnet. Refer to "Use Subnet Quick View" (p. 9-21) for details on the Subnet QuickView.

7 Click **Close** when you are finished.

END OF STEPS

Use Subnet Quick View

Purpose

The Subnet Quick View allows you to see the status of all objects within a subnet.

Procedure

To access the Subnet Quick View, follow these steps:

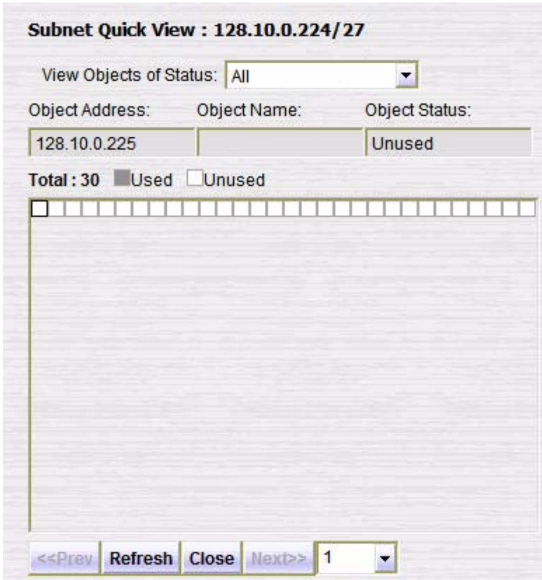
1 Select a subnet in the IPv4 Hierarchy.

Note: You can also select a subnet from the Network Quick View.

Result: The Subnet Properties page opens.

2 Click **Quick View** from either the Subnet Properties page or the Network Quick View.

Result: The Subnet Quick View opens.



3 Click on a white square to see the object's IP Address, Name (if assigned) and Status displayed in the top of the Quick View Window.

4 Select a status from the **View Objects of Status** drop-down list if you want to see only objects of a certain status. Allowable values are:

- All
- Unused
- Used
- Static
- Dynamic
- Reserved
- Manual BootP
- Automatic BootP
- Manual DHCP
- Automatic DHCP
- Dynamic DHCP
- Scheduled Move

5 Click **Refresh** to update the Quick View window to reflect changes in the status of the displayed objects.

6 Click **Close** when you are finished.

Note: If you accessed the Subnet Quick View from the Network Quick View, clicking **Close** returns you to the Network Quick View.

END OF STEPS

IPv4 network management

Overview

Purpose

Network management permits you to create a physical representation of your network in VitalQIP. This representation is used to manage subnets and subquentially address space. Management of your networks includes the ability to:

- Add, modify, and delete networks
- Alert administrators that network address space is almost full
- Assign address ranges to a network
- Manage subnets associated with a network

Reports

The following reports are accessible from the Network properties page:

- IPv4 Subnets Report
- Subnet Usage Report
- IPv4 Object Info Report
- Network Audit Report

Add a network

Purpose

Use this procedure to create a new network.

Before you begin

To create a network, the administrator's type or access permissions must be one of these:

- Master administrator
- Normal administrator with read and write managed type of **Organization** for the organization containing the network
- Normal administrator with a managed type of **Normal** and **Create Infrastructure** privileges under either the **Use Default** privilege hierarchy or **Organization Defaults** privilege hierarchy

Procedure

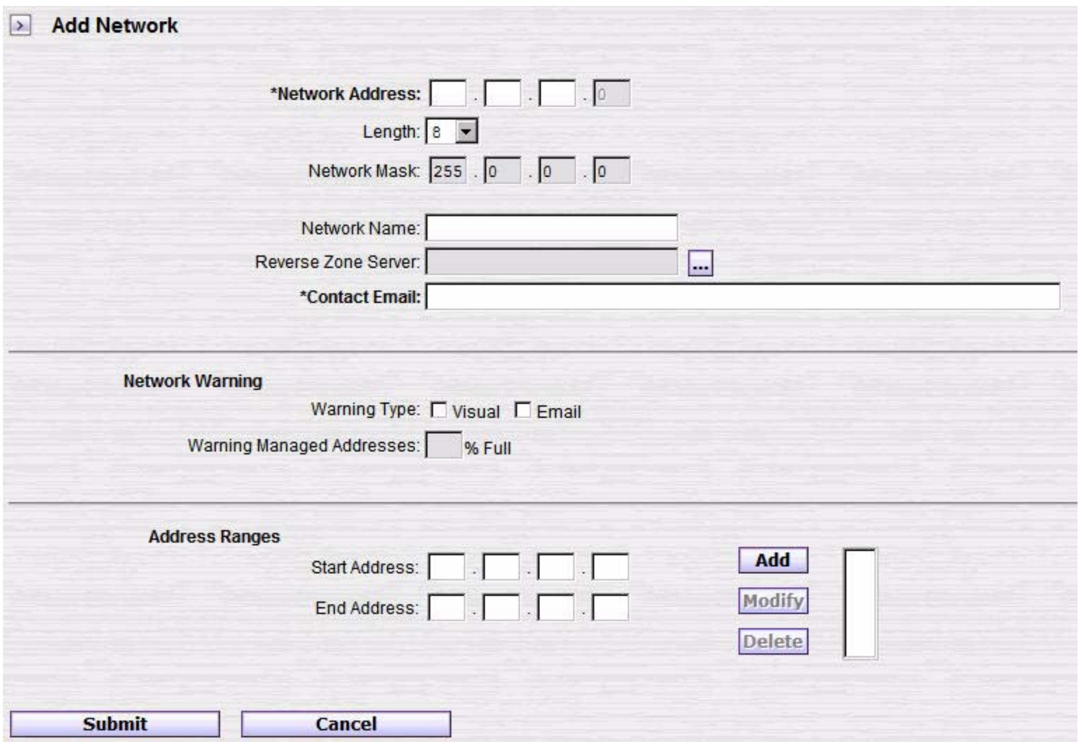
To add a network, follow these steps:

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy page opens.

2 Mouse over the **Actions** menu and select **Add Network**.

Result: The Add Network page opens.



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

Table 9-2 Add network fields

Field	Description
Network Address	***Required***. This field identifies the network you are building. 0, 127 and greater than 239 are not allowed in the first octet since these numbers are reserved. Addresses between 224 and 239 result in a class D network (multi-cast). In case the first octet contains 224 to 239, the length defaults to 8 and cannot be changed. The last three octets cannot be edited.
Length	***Required***. The network address length range 8-24.
Network Mask	***Read only***. Show the mask corresponding to the defined network address length.
Network Name	***Optional***. The name of network to be displayed in VitalQIP.
Contact Email	***Required***. This email address appears in the SOA record for the reverse zone. A sample contact email is *username@company.com*. Any errors posted by DNS are sent to this email address.
Reverse Zone Server	***Optional***. Assigns a reverse zone server to the network. Assigning a DNS server here identifies the Primary Reverse Zone server for this network. When a server is selected, the Contact Email for the selected server is put into the **Contact Email** field. The Network's **Contact Email** field remains editable and can be changed. Refer to "Search for a reverse zone server" (p. 9-27) for details on searching for a reverse zone server.
Network Warning	
Warning Type	***Optional***. Determines the type of warning to give when the network threshold level is exceeded. Check: • **Visual** - Indicates that a visual warning is given for exceeding the network threshold • **Email** - Indicate that an email warning is given for exceeding the network threshold level.
Warning Managed Addresses	***Required if Warning Type is selected and is not editable unless a Warning Type is selected.*** It determines the threshold at which a warning is issued. It is based on the number of addresses in service for this network. If warning type is **Email**, an email is sent to the address in the administrator profile of all administrators assigned to manage the network. Valid values are 1 to 99.

Address Range

4 Address ranges can be defined for the network. Read the following table for more information in address ranges.

To...	Then...
Add an address range	1. In the **Start Address** field, enter the address to start the range. Start address cannot be the same as the network address. 2. In the **End Address** field, enter the address to end the range. 3. Click **Add**. **Result:** The address is displayed in the list.
Modify an address range	1. From the address range list, select an address range. **Result:** The **Start Address** and **End Address** fields are populated with the selected address range. 2. Change the address. 3. Click **Modify**. **Result:** The address range is updated in the list.
Delete an address range	From the address range list, select an address range and click **Delete**. **Result:** The address range is deleted from the list.

User Defined Attributes

5 If user defined attributes are associated with a network, the **User Defined Attributes** section is shown on the page. Refer "Working with user defined attributes and fields" (p. 7-23) for more information.

6 Click **Submit**.

Result: A dialog box opens indicating if the network was successfully added.

END OF STEPS

Search for a reverse zone server

To search for a reverse zone server, follow these steps.

1 Click the ellipsis button (...) that appears next to the **Reverse Zone Server** field.

Result: The Search dialog box opens.

2 In the **Reverse Zone Server** field, enter the first few letters of the reverse zone server and the wildcard character (*) as needed.

3 Click **Search**.

Result: The results appear in the **Existing List** list.

4 In the **Existing List** list, highlight a reverse zone server.

5 Click **OK**.

Result: The Search dialog box closes and the reverse zone server you selected is added to the **Reverse Zone Server** field.

Note: If you wish to clear the **Reverse Zone Server** field, click , make sure nothing is selected in the Search dialog box, and click **OK**. The server is cleared from the **Reverse Zone Server** field.

END OF STEPS

View network properties

Purpose

Use this procedure to view network properties.

Procedure

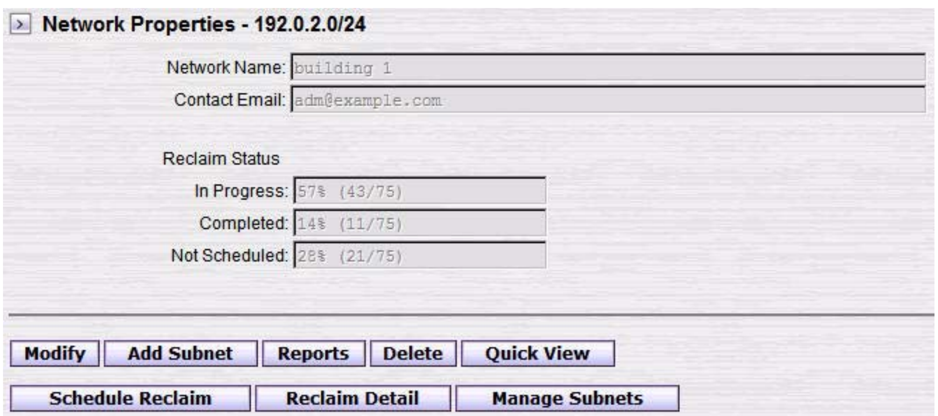
To view network properties, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens in the Network view. Refer to Figure 9-1, "IPv4 Hierarchy - Networks node" (p. 9-4).

2 Select a network.

Result: The Network properties page opens.



From this page, you can perform a number of functions. Refer to the following table for where to go for more information about the function.

If you want to...	Refer to...
Modify network properties	"Modify a network" (p. 9-30)
Add a subnet	"Add a subnet" (p. 9-36)
View reports	Chapter 29, "Reports"
Delete a network	"Delete a network" (p. 9-32)
Quickly view the subnets in the network	"Use Subnet Quick View" (p. 9-21)

If you want to...	Refer to...
Schedule a subnet reclaim	"Schedule an address reclaim" (p. 9-94)
View scheduled subnet reclaims	"Check status of a scheduled reclaim" (p. 9-97)
Manage subnets	"Subnet management" (p. 9-34)

END OF STEPS

Modify a network

Purpose

Use this procedure to modify network.

Before you begin

To modify a network, the administrator's type or access permissions must be one of these:

- Master administrator.
- Normal administrator with read and write managed type of **Organization** for the organization containing the network. If the managed type is read-only, this administrator type can still see the network in the **QIP** hierarchy and bring up the properties pages but cannot make any changes.
- Normal administrator with a managed type of **Normal** and who either possesses an administrator role that contains the network with read and write access, or has the network in its managed list with read and write access.

Procedure

To modify a network, follow these steps:

1 Mouse over **Address Management** and click **IPv4**.

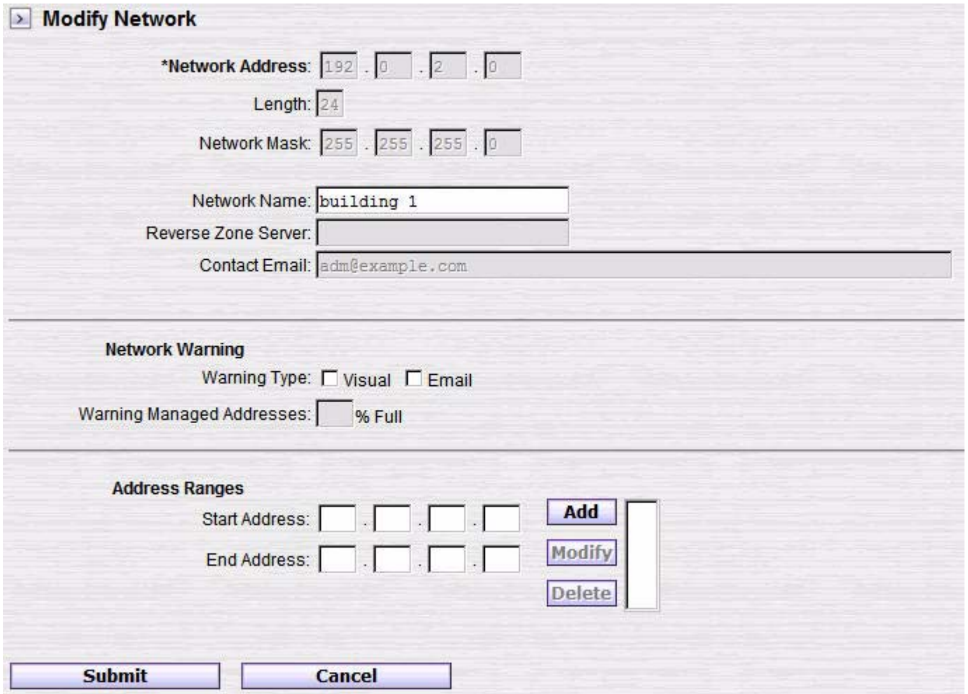
Result: The IPv4 Hierarchy opens in the Network view. Refer to Figure 9-1, "IPv4 Hierarchy - Networks node" (p. 9-4).

2 Select a network.

Result: The Network properties page opens.

3 Click **Modify**.

Result: The Modify Network page opens.



4 Modify the fields as needed. All fields are modifiable except the **Network Address**, **Length**, **Network Mask**, **Reverse Zone Server**, and **Contact Email** fields. Refer to Table 9-2, "Add network fields" (p. 9-26) for more details.

5 Click **Submit** when you finished.

Result: The network is modified.

END OF STEPS

Delete a network

Purpose

Use this procedure to delete a network and all other related structures, such as objects related to the network.

Before you begin

- If a network is deleted, it permanently deletes subnets and related structures.
- To delete a network, the administrator's type or access permissions must be one of these:
  - Master administrator.
  - Normal administrator with read and write managed type of **Organization** for the organization containing the network. If the managed type is read-only, this administrator type can still see the network in the **QIP** hierarchy and bring up the properties pages but cannot make any changes.
  - Normal administrator with a managed type of **Normal** and who either possesses an administrator role that contains the network with read and write access, or has the network in its managed list with read and write access.

Procedure

To delete a network, follow these steps:

---

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens in the Network view. Refer to Figure 9-1, "IPv4 Hierarchy - Networks node" (p. 9-4).

---

2 Select a network.

Result: The Network properties page opens.

---

3 Click **Delete**.

Result: A dialog box opens with the message **Permanently Delete the Network** <*network address*> **and all underlying structures such as subnets etc..**

---

4 Click **OK**.

Result: The network is deleted.

END OF STEPS

Subnet management

Overview

Purpose

This section describes the following aspects of subnet management:

- Add a subnet
- View subnet properties
- Modify subnet properties
- Delete a subnet
- Split a subnet
- Join subnets

Reports

The following reports are accessible from the Subnet properties page:

- IPv4 Object Info Report
- DHCP Utilization Report
- Subnet Subnet Audit Report

The following reports are accessible from the Network properties page:

- IPv4 Object Info Report
- IPv4 Subnet Info Report
- Subnet Usage Report
- DHCP Utilization Report
- Network Audit Report

The IPv4 Subnet Info Report is accessible from the Domain and Subnet Organization properties page:

These reports are described in Chapter 29, “Reports”.

Manage subnets in a network

Purpose

Use this procedure to manage subnets in a network.

Procedure

To manage subnets in a network, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

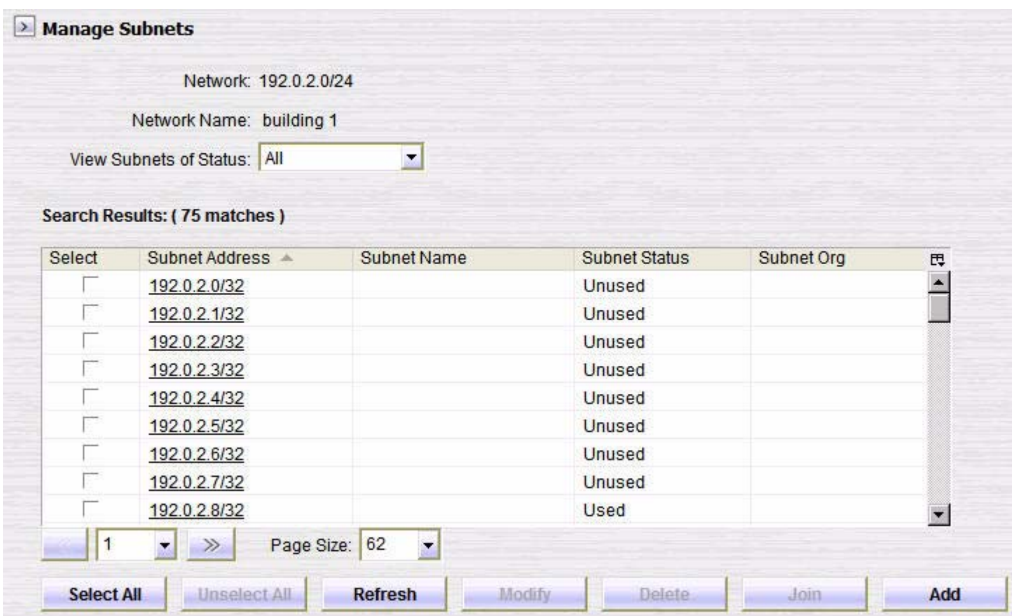
Result: The IPv4 Hierarchy opens in the Network view (refer to Figure 9-1, "IPv4 Hierarchy - Networks node" (p. 9-4)).

2 Expand **Networks** and select the network to which you want to modify subnets.

Result: The Network properties page opens.

3 Click **Manage Subnets**.

Result: The Manage Subnets page opens.



Choose one of the following actions.

If you want to…	Then…
Select one or more subnets	• Select one or more subnets by clicking the checkbox in the **Select** column • Select more than one subnet by clicking holding the **Shift** key and clicking on one or more subnet rows

If you want to...	Then...
Select all subnets in the **Search Results** list	Click **Select All**. **Result:** All subnets are selected.
Unselect subnet in the **Search Results** list	Click **Unselect All**. **Result:** Selected subnets are unselected.
Refresh the Search Results list	Click **Refresh**. **Result:** The **Search Results** list is updated.
Modify one subnet	In the **Subnet Address** column, click on a used subnet. **Result:** The Subnet Profile page opens. Refer to “Modify subnet profile” (p. 9-43) for more information.
Modify more that one subnet	1. Select one or more subnets. 2. Click **Modify**. **Result:** The Modify Subnet Properties page opens. Refer to “Modify multiple subnet properties” (p. 9-57) for more information.
Delete one or more subnets	1. Select one or more subnets. 2. Click **Delete**. **Result:** Refer to “Delete multiple subnets” (p. 9-70) for more information.
Join mutiple subnets	1. Select one or more subnets. 2. Click **Join**. **Result:** The Join Subnet page opens. Refer to “Join multiple subnets” (p. 9-64) for more information.
Add a subnet	Click **Add**. **Result:** The Add Subnet page opens. Refer to “Add a subnet” (p. 9-36) for more information.

END OF STEPS

Add a subnet

Purpose

Use this procedure to create a subnet in the web client. You can also add a subnet with the Network\Reverse Zone function in the VitalQIP UI.

Before you begin

If the subnet is within the scope of a seed block, the subnet cannot be created via IPv4 Address Management. The subnet is being managed by the address allocation process.

Procedure

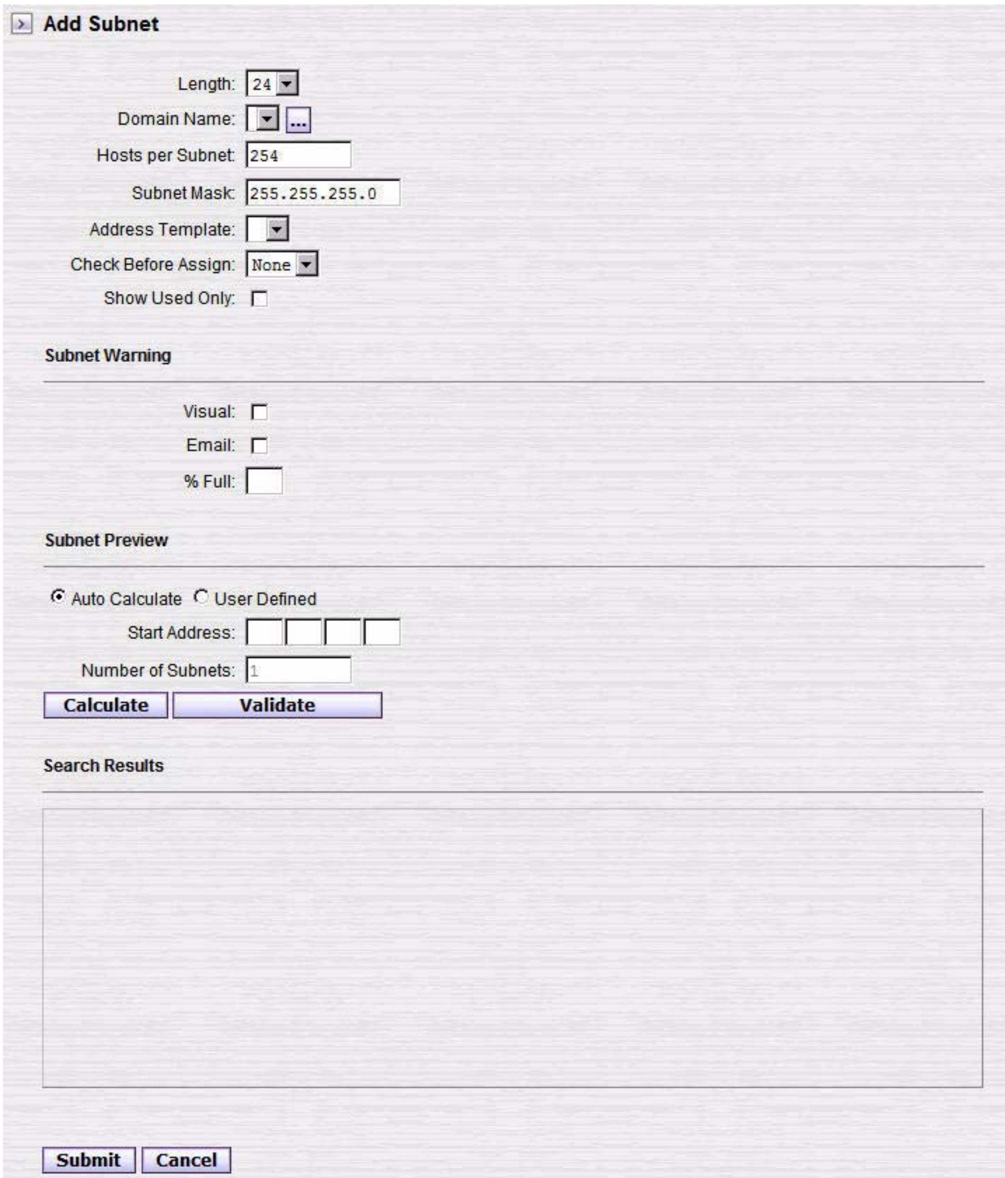
To add a subnet, follow these steps.

1 Choose one of the following.

If you are in...	**Then...**
Network properties page	1. Mouse over **Address Management** and click **IPv4**. **Result:** The IPv4 Hierarchy opens in the Network view (refer to Figure 9-1, "IPv4 Hierarchy - Networks node" (p. 9-4)). 2. Expand **Networks** and select the network to which you want to add a subnet. **Result:** The Network properties page opens.
Managed Subnet page	1. Mouse over **Address Management** and click **IPv4**. **Result:** The IPv4 Hierarchy opens in the Network view (refer to Figure 9-1, "IPv4 Hierarchy - Networks node" (p. 9-4)). 1. Expand **Networks** and select the network to which you want to modify subnets. **Result:** The Network properties page opens. 2. Click **Manage Subnets**. **Result:** The Manage Subnets page opens.

2 Click **Add subnet**.

Result: The Add Subnet page opens.



3 Define the subnet properties, as described in the following table.

Table 9-3 Subnet property fields

Field	Description
Length	Defines the length of the new subnet. Although the default length is the size of the network, you may select a different value from the drop-down list up to a value of 32.

Field	Description
Domain Name	***Optional***. The initial domain name defaults to empty. Use the domain search function to select a domain for the subnet. To search for a domain, follow these steps. 1. Click ... to open the Domain Search window. 2. Enter search criteria in the **Domain Name** field and click **Search**. Leave the field blank to return all domains in the database. You may also use the wildcard (*) as needed. 3. You may associate multiple domains with the subnet. Select a domain from the **Existing List** and click **Add=>** to add the selected domain to the **Selected List**. Repeat as needed. To remove a domain from the **Selected List**, click **<=Delete**. 4. The first subnet in the list is the default domain. To select a different domain as the default, select the domain you want to be the default and click **Set Default**. The domain moves to the top of the **Selected List**. **Note:** Other subnets in this network can have a different default domain.You can also change the default domain by selecting a different domain from the **Domain Name** drop-down list after the Domain Search window is closed. 5. Click **OK**. **Result:** The domain appears in the **Domain Name** field. For further information on searching for a domain, refer to "Search for a domain" (p. 16-29).
Hosts per Subnet	***Read-only***. Displays the number of hosts in the subnet. This is determined by the value selected in the **Length** field.
Subnet Mask	***Read-only***. Displays the subnet mask for the subnet. This is determined by the value selected in the **Length** field.
Address Template	***Optional.*** Select an address template from the drop-down list. Objects are created as specified in the selected template in a manner similar to that used in block allocation. Any domains specified in the address template are also associated with the subnet, in addition to those in the **Selected List**. For more information on address templates, refer to "Address allocation templates" (p. 24-1).
Check Before Assign	The options are **Ping** or **None**. If Ping is selected, VitalQIP will later ping the address when each object is created. If no reply is received to the Ping, the address is free to be assigned. Otherwise, a warning message opens which states that the address is currently in use. It also asks if the user still wishes to allocate it. The message opens only when an object is being added in the VitalQIP client and is not caused by DHCP handing out leases.
Show Used Only	When turned on, this field creates a default in the Object Management window to display all objects that do not have a status of "Unused".

Field	Description
Visual	In the **Subnet Warning** section, select **Visual** to have a warning displayed if the percentage of allocated IP addresses is greater than the percentage defined in the **% Full** field. Allocated addresses include used, reserved, dynamically allocated, planned, or any form of Bootp or DHCP address.
Email	In the **Subnet Warning** section, select **Email** to have an email sent to all administrators assigned to manage the subnet if the percentage of allocated IP addresses is greater than the percentage defined in the **% Full** field. Allocated addresses include used, reserved, dynamically allocated, planned, or any form of Bootp or DHCP address. **Note:** The email address is defined in the administrator record.
% Full	When the number of objects put into service for a subnet reaches the threshold defined in the **% Full** field (from 0% to 99% full), a visual and/or email warning is issued, based on the values of the **Visual** and **Email** check boxes.

4 Choose one of the following actions to preview, validate, or select subnets to be created:

If you want to…	Then…
Calculate subnets automatically	1. Click the **Auto Calculate** option button. 2. Click **Calculate**. **Result:** The **Search Results** list is populated with a foldered list of all possible subnets for the network and length/mask. 3. Select at least one subnet you wish to validate. 4. *Optional*. Click **Validate** to determine if the subnets are in use and if you have the privileges to create them. **Result:** Any subnet that fails validation is deselected in the **Search Results** list. 5. Click **Submit**. **Note:** If the calculation returns more than 65,536 subnets, a warning opens to determine whether you want to continue. Click **Yes** to continue, or click **No** to abort.

If you want to…	Then…
Create your own subnets	1. Click the **User Defined** option button. 2. Enter a starting address in the **Start Address** field. 3. Enter the number of subnets you wish to create in the **Number of Subnets** field. 4. ***Optional.*** Click **Calculate**. In the **Search Results** list, select the subnets you wish to validate. 5. ***Optional***. Click **Validate** to determine if the subnets are in use and if you have the privileges to create them. Any subnet that fails validation is deselected in the **Search Results** list. 6. Click **Submit**. **Note:** You do not need to use Calculate and Validate functions. VitalQIP attempts to create the subnets you requested. If a subnet already exists, the confirmation dialog box shown below would display entries with a subnet creation status of **Failed**.

5 When the subnets have been created, a confirmation dialog opens stating the status of the subnet creation.

6 Click **OK** to confirm.

Result: The subnet is added to the hierarchy. Expand the **Subnets** node to confirm.

END OF STEPS

View subnet properties

Purpose

Use this procedure to access the Subnet Properties page, which is your starting point for managing objects in a subnet, as well as a variety of subnet operations.

Procedure

To view the Subnet Properties page, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

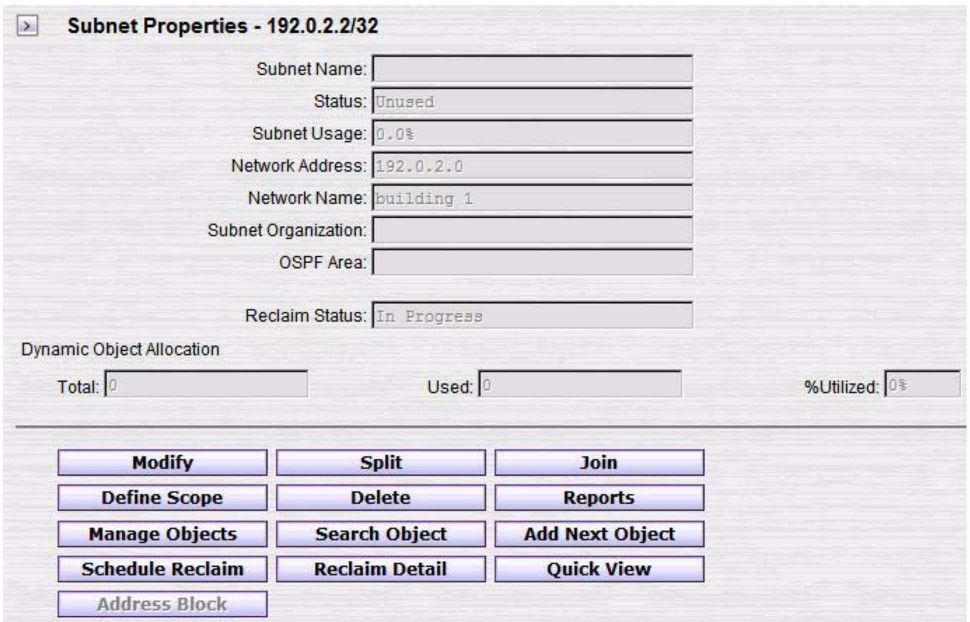
Result: The IPv4 Hierarchy opens.

2 Mouse over **Actions** and select **View Subnets**.

Result: The IPv4 Hierarchy shows the Subnets node.

3 Expand the Subnets node and select the subnet whose properties you want to view.

Result: The Subnet Properties page opens.



From this page, you can perform a number of functions. Refer to the following table for where to go for more information about the function.

If you want to...	Refer to...
Modify a subnet properties	"Modify subnet profile" (p. 9-43)
Split a subnet	"Split a subnet" (p. 9-60)
Join subnets	"Join a subnet with the next available subnet" (p. 9-62)
Define a scope	"Define a scope" (p. 10-22)
Delete a subnet	"Delete a subnet" (p. 9-69)

If you want to...	Refer to...
Create subnet audit, subnet usage, and subnet information reports	Chapter 29, “Reports”
Manage objects	“Manage objects” (p. 10-3)
Search objects	“Search for an object in a subnet” (p. 10-7)
Add next object	“Add an object to the next available address in a subnet” (p. 10-10)
Schedule a subnet reclaim	“Schedule an address reclaim” (p. 9-94)
View scheduled subnet reclaims	“Check status of a scheduled reclaim” (p. 9-97)
Quickly view subnet details	“Use Subnet Quick View” (p. 9-21)
Manage a block associated with a subnet	“Manage a block associated with a subnet” (p. 9-67)

END OF STEPS

Modify subnet profile

Purpose

To modify a subnet profile. The **Subnet Profile** page allows you to fine-tune the settings for a subnet. These settings apply to all objects defined in this subnet. Additionally, defining a DHCP/Bootp and/or a DHCP Subnet Policy Template and attaching such templates to the subnet profile allows all clients on a particular subnet to have the same configuration.

Before you begin

- When an object is added in a subnet, it is assigned to the location and contact selected at the subnet level by default, unless it is overridden within that object’s profile. For further information, refer to “Assign location and contact information to an object” (p. 10-45).
- If you define object ranges in a subnet, the following rules apply.
  - Objects do not have to exist prior to the time the range is being defined.
  - The range must fall entirely within one existing subnet.
  - If the subnet is deleted, the object range is deleted.

- If the subnet size changes due to being split or joined to another subnet, the object range is re-assigned to a subnet that completely contains the range. If no such subnet exists, the object range is deleted.
- Multiple ranges can be defined within one subnet.
- Multiple ranges can be assigned to a single administrator.
- An administrator with permissions on an object range does not necessarily have permissions on the subnet itself. The administrator can see the associated subnet in the hierarchy, but must have write permissions for a subnet to create an object range in that subnet. If the administrator has permissions to assign an object in that object range or associated subnet, the object can be assigned to a sub-administrator.

Procedure

To modify a subnet profile, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over **Actions** and select **View Subnets**.

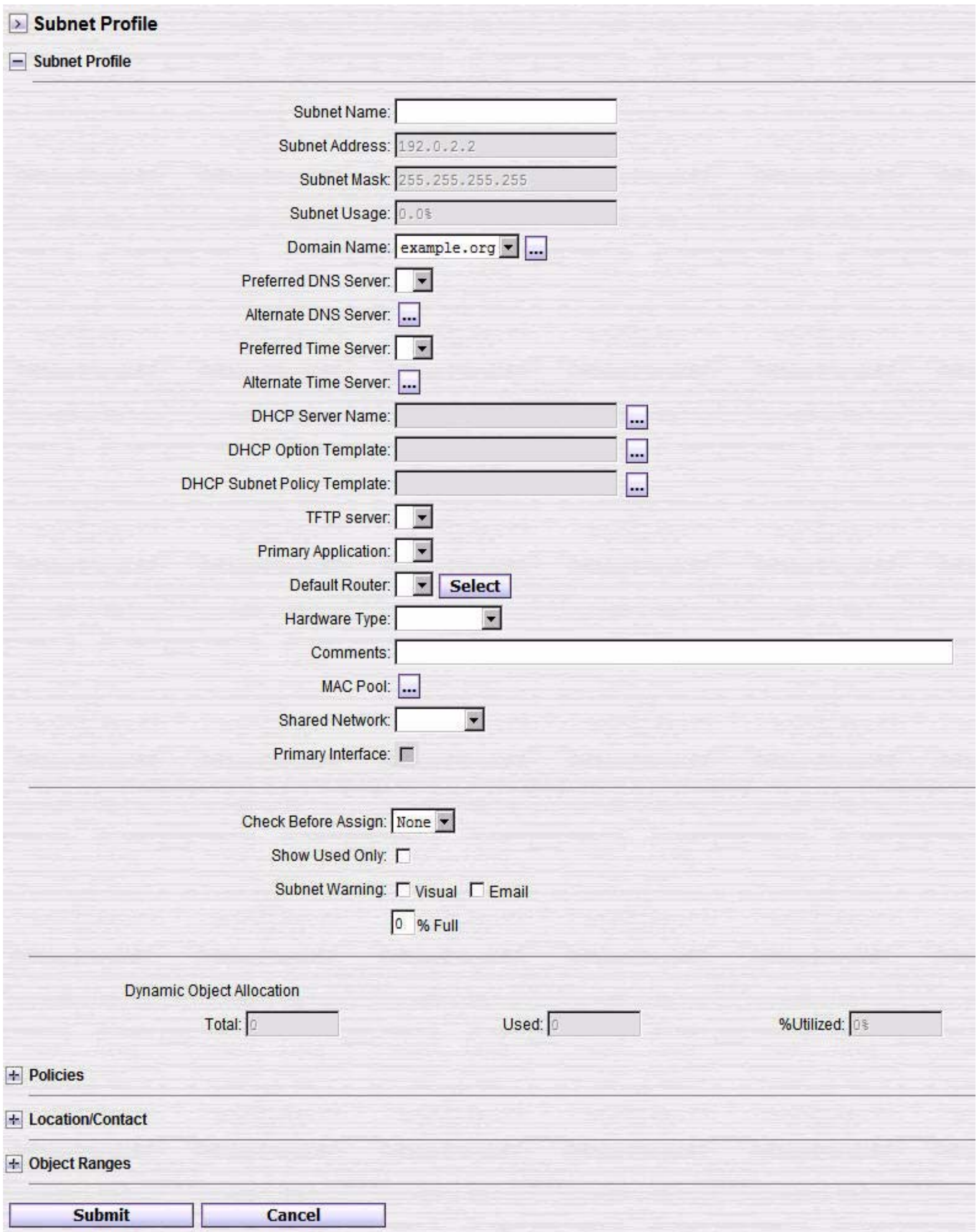
Result: The IPv4 Hierarchy shows the Subnets node.

3 Expand the Subnets node and select the subnet you want to modify.

Result: The Subnet Properties page opens.

4 Click **Modify**.

Result: The Subnet Profile page opens.



5 Enter values in the fields as needed. For more information on a field, refer to the following table.

Table 9-4 Subnet profile fields

Field	Description
Subnet Name	Enter the name (up to 255 characters) for this subnet. This field can be left blank.
Subnet Address	***Read only.*** The subnet address for this subnet displays in this field.
Subnet Mask	***Read only.*** The subnet mask for this subnet displays in this field.
Subnet Usage	***Read only.*** This value indicates the percentage of the IP addresses for this subnet that are currently in use.
Domain Name	Either select one of the subnet's default domains from the drop-down list Alternatively, follow these steps to search for an existing domain. 1. Click ... to open the Domain Search window. 2. Enter search criteria in the **Domain Name** field and click **Search**. Leave the field blank to return all domains in the database. You may also use the wildcard (*) as needed. 3. You may associate multiple domains with the subnet. Select a domain from the **Existing List** and click **Add=>** to add the selected domain to the **Selected List**. Repeat as needed. To remove a domain from the **Selected List**, click **<=Delete**. 4. The first subnet in the list is the default domain. To select a different domain as the default, select the domain you want to be the default and click **Set Default**. The domain moves to the top of the **Selected List**. 5. Click **OK**. **Result:** The domain appears in the **Domain Name** field.
Preferred DNS Server	Assign the preferred DNS server for the objects within the subnet by selecting a DNS server from the drop-down list.
Alternate DNS Server	Assign the alternate DNS server for the objects within the subnet. Click ... to display a list of DNS servers that can be assigned to the subnet. Select a server from the **Selected List** and click **OK**. • To add a server to the list of DNS servers, select a server in the **Available List** and click **Add=>**. • To remove a server from the **Selected List**, select the server and click **<=Delete**.
Preferred Time Server	Assign the preferred Time server of the domain for the subnet. Select a server from the drop-down list.

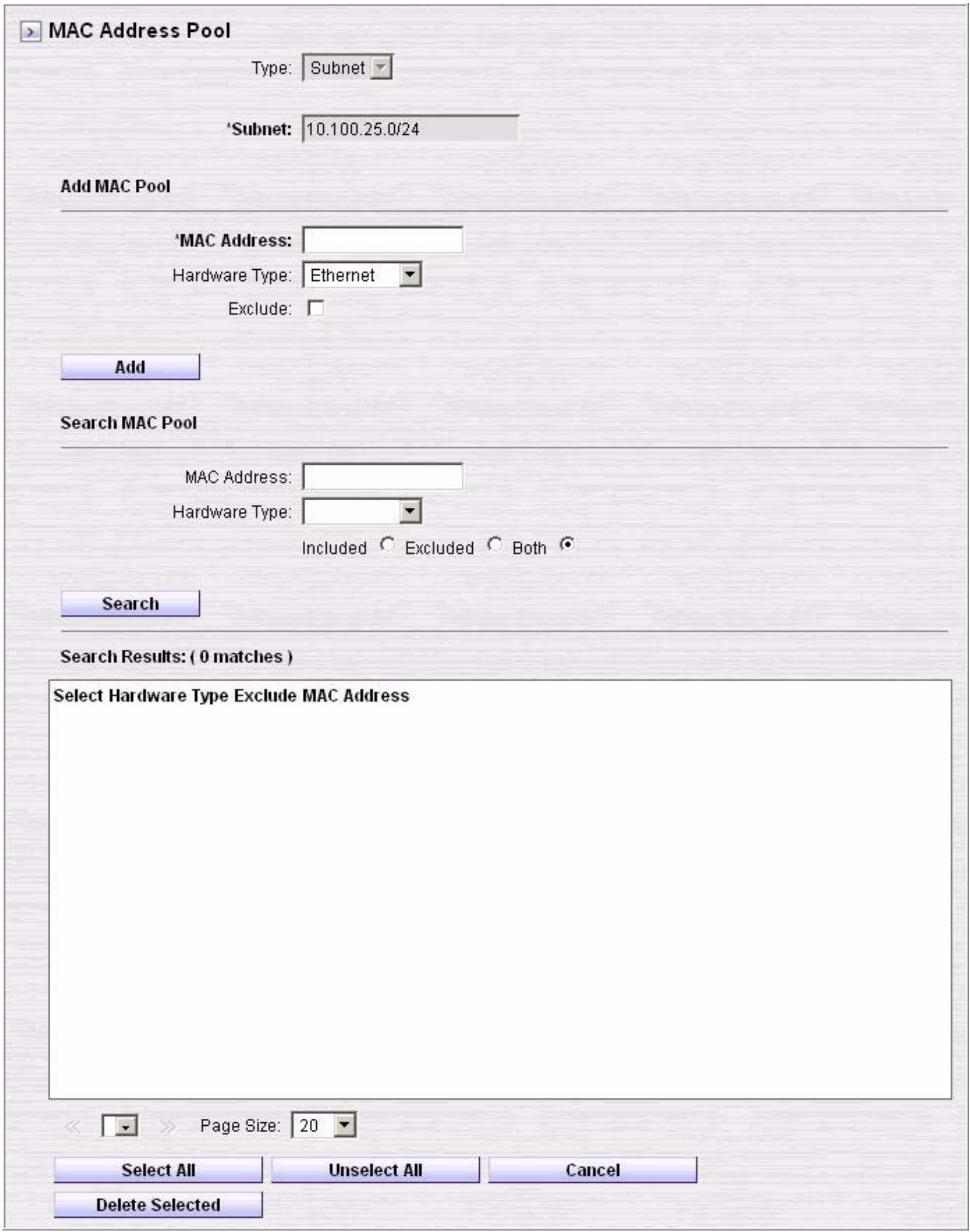
Field	Description
Alternate Time Server	Assign the alternate Time server for the objects within the subnet. Click ... to display a list of servers that can be assigned. Select a server from the **Selected List** and click **OK**. • To add a server to this list, select a server in the **Available List** and click **Add=>**. • To remove a server from the **Selected List**, select the server and click **<=Delete**.
DHCP Server Name	1. Click ... to open the DHCP Server Search window. 2. Enter search criteria in the **DHCP Server Name** field and click **Search**. Leave the field blank to return all DHCP servers in the database. You may also use the wildcard (*) as needed. 3. Select a server from the **Existing List** and click **OK**. **Note:** Select **Same as in SubnetOrg Profile** if the subnet is managed by a subnet organization and you wish to use settings associated with a DHCP server previously assigned to that subnet organization.
DHCP Option Template	The DHCP option template is associated with all objects in the subnet that are tagged with DHCP, unless an object has had a different template assigned to it. Assigning a DHCP option template at the subnet level is optional. If no DHCP option template is assigned to the subnet, either the option template associated with the DHCP server or with an object is used. 1. Click ... to open the DHCP Option Template Search window. 2. Enter search criteria in the **DHCP Option Template** field and click **Search**. Leave the field blank to return all DHCP option templates in the database. You may also use the wildcard (*) as needed. 3. Select a DHCP option template from the **Existing List** and click **OK**. **Note:** Select **Same as in SubnetOrg Profile** if the subnet is managed by a subnet organization and you wish to use settings associated with a DHCP option template previously assigned to that subnet organization.

Field	Description
DHCP Subnet Policy Template	If you want to assign a previously defined subnet policy template to the current subnet, follow these steps. 1. Click ... to open the DHCP Subnet Policy Template Search window. 2. Enter search criteria in the **DHCP Subnet Policy Template** field and click **Search**. Leave the field blank to return all DHCP subnet policy templates in the database. You may also use the wildcard (*) as needed. 3. Select a DHCP subnet policy template from the **Existing List** and click **OK**.
Tftp Server	By default, this is the Bootp server, unless another server has been defined as the Tftp server. Select a server from the drop-down list.
Primary Application	Assigns an application for this subnet. Select the primary application from the drop-down list. **Note:** Applications can be defined in the VitalQIP thick client. Refer to the *VitalQIP User's Guide* for further information.
Default Router	Assign a **Default Router** (or routers) for the subnet in this field. The objects in this subnet inherit all the routers you assign. The routers can be overridden in the Routers section of an Object Profile, or within a DHCP option template. **Note:** The **Always Append Router** policy automatically adds router objects to the default routers list if set to True. By default, this is either the router defined in the Global Allocation Policies for the subnet organization, or the first router that has been defined in the subnet. The default router is important for Bootp and DHCP. To assign a router, follow these steps. 1. Click **Select** to display the **Existing Router List**.  2. Select a router from the list and click >>. **Result:** The router is added to the **Selected Router List**. To remove a router from the **Selected Router List**, click <<. 3. Click **Collapse** to close the Existing Router List.

Field	Description
Hardware Type	Select the hardware type for the objects within the subnet from the drop-down list: **Ethernet**, **Token Ring**, **AX.25**, **Pronet**, **Chaos**, **IEEE802**, or **Arcnet**.
Comments	Add any comments you wish to add about the subnet.
MAC Pool	This function is only used when the **RegisteredClientsOnly** policy is set to True in the *dhcpd.pcy* file. Click ... to manage MAC pools on a subnet. The MAC Address Pool window opens. For information on how to use this window, refer to "Subnet MAC Address Pools" (p. 9-50). **Note:** Duplicate MAC addresses are not allowed in the same subnet, even if the **Allow Duplicate MAC Addresses** global policy is set to True. You receive an error message if you try to add or modify the object and its MAC address is being used by another object in the same subnet.
Shared Network	To use the Secondary Addressing feature of DHCP, you must specify one subnet as primary. To do this, define the subnet as being part of a **Shared Network** by selecting a network from the drop-down list, or by selecting **Add New** and entering a network name in the field that appears. If this is a shared network, the **Primary Interface** check box is enabled. **Note:** You must define at least one dynamic address on the subnet that is defined as the primary interface, and perform a DHCP generation.
Primary Interface	To distinguish this subnet as the primary subnet in the shared network, check the **Primary Interface** check box. When checked, this subnet acts as the primary subnet for all those subnets defined in this physical LAN segment. If you check **Primary Interface** in multiple Subnet Profiles, the last one selected becomes the Primary Interface.
Dynamic Object Allocation	**Total** displays the number of dynamic objects on the subnet. **Used** displays the number of dynamic objects that are in use. **%Utilized** indicates the percentage utilization of dynamic objects defined on the subnet.

Subnet MAC Address Pools

The MAC Address Pool for the subnet opens when you click [...] beside the **MAC Pool** field.



Choose from the following actions.

If you want to …	Then …
Add a MAC address to the subnet pool	1. In the **Add MAC Pool** section, enter a MAC address in the **MAC Address** field. 2. Select the hardware type from the **Hardware Type** field. 3. 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. 4. In the **Search MAC Pool** section, enter the wildcard character (*) in the **MAC Address** field. **Note:** This step avoids an unintended **The search returned no results** message. 5. Click **Add**. **Result:** A confirmation dialog box opens with the message **MAC Pool added successfully**. 6. Click **OK**. **Result:** The MAC address is added to the **Search Results** list for the selected subnet.
Search for an existing MAC address	1. In the **Search MAC Pool** section, enter the MAC address in the **MAC Address** field. Use the wildcard character as needed. 2. Select the hardware type from the **Hardware Type** field. 3. Click **Included**, **Excluded**, or **Both**, depending on whether you need to search for the MAC address that is either included or excluded in the pool, or to search for MAC addresses regardless of their inclusion in the pool. 4. Click **Search**. **Result:** The MAC addresses are listed in the search results.

If you want to …	Then …
Unassign one or more MAC addresses from the selected subnet	1. Search for the MAC addresses, following the steps above. 2. Place checkmarks beside the addresses in the **Search Results** list that you wish to remove. Use **Select All** and **Unselect All** as needed. 3. Click **Delete Selected**. **Result:** A dialog opens with the message **MAC Pools deleted successfully**. 4. Click **OK**. **Result:** The selected MAC addresses are removed.

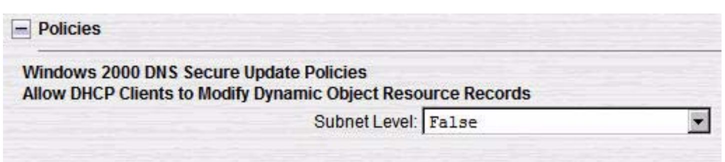
6 Expand other sections to complete the modification of the subnet profile.

Subnet-level policies

The Dynamic DNS section of Global Policies in the VitalQIP UI contains an **Allow DHCP Clients to Modify Dynamic Object Resource Records** policy that defaults to False. This policy should be set to True if Microsoft DHCP clients are to be able to send secure updates to a Windows DNS server. The policy can be enabled at the Global Policies level where the setting would apply to ***all*** subnets, or it can be enabled at the subnet profile level where the policy would apply to a specific subnet only.

To set the **Allow DHCP Clients to Modify Dynamic Object Resource Records** policy at the subnet level, follow these steps.

7 Expand the **Policies** section.



8 Choose one of the following actions.

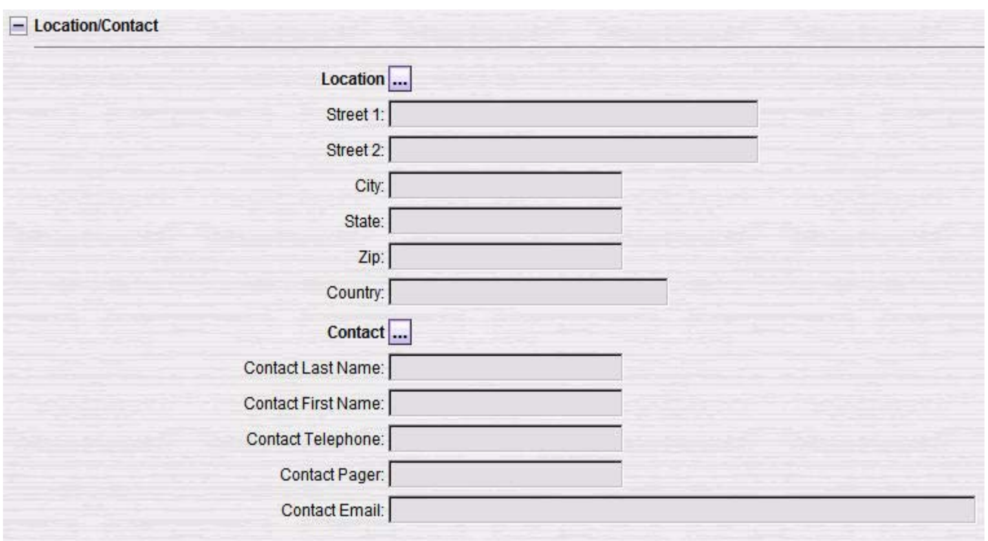
If you want to...	**Then...**
Leave the **Allow DHCP Clients to Modify Dynamic Object Resource Records** policy at the same setting it has in Global Policies.	Select **Same as in Global Policies** in the **Subnet Level** drop-down field.
Override a True setting in Global Policies	Select **False** in the **Subnet Level** drop-down field.
Override a False setting in Global Polices	Select **True** in the **Subnet Level** drop-down field.

Location and contact information

The **Location/Contact** section allows you to specify where the subnet is located and who the contact is.

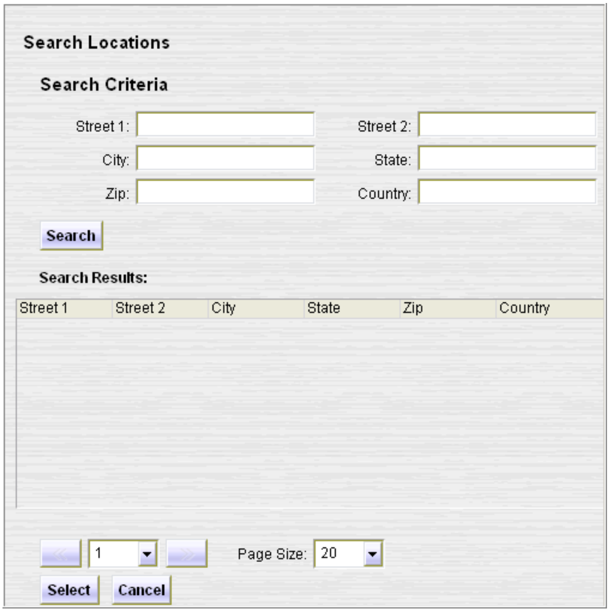
To enter location and/or contact information for the subnet profile, follow these steps.

9 Expand the **Location/Contact** section.



10 Click the icon beside **Location**.

Result: The Search Locations page opens.



---

11 Enter address search criteria as needed and click **Search**. To return all address records in the database, click **Search** without entering any criteria.

Result: The Search Results list displays the results of your search criteria.

---

12 Select the location you wish to assign to the subnet and click **Select**.

Result: The **Location** section of the Subnet Profile is populated.

---

13 Click the  icon beside **Contact**.

Result: The Search Contacts page opens.

14 Enter contact search criteria as needed and click **Search**. To return all contact records in the database, click **Search** without entering any criteria.

Result: The Search Results list displays the results of your search criteria.

15 Select the contact you wish to assign to the subnet and click **Select**.

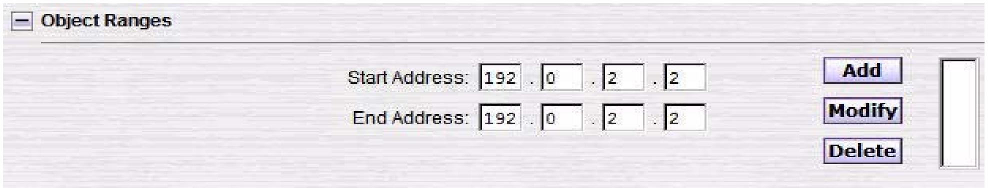
Result: The **Contact** section of the Subnet Profile is populated.

Object ranges

A subnet can be subdivided into object ranges so that administrators can be assigned to administer only a specific set of objects rather than the whole subnet itself. Object ranges can then be assigned to an administrator's Managed List and/or Admin Roles. Refer to "Add Managed Lists" (p. 6-16), and "Create an administrative role" (p. 6-29).

To define a subnet object range, follow these steps.

16 Expand the **Object Ranges** section.



17 Enter valid subnet addresses in the **Start Address** and **End Address** fields. The **Start Address** and **End Address** default to the subnet's first and last address.

18 Click **Add** and the range appears in the **Ranges** list.

19 Repeat Step 17 and Step 18 as necessary.

20 To delete an object range, highlight the appropriate object range in the **Existing Object Ranges** list, and click **Delete**.

21 To modify an object range, highlight the appropriate object range in the **Existing Object Ranges** list, modify the **Start Address** and/or **End Address** fields and click **Modify**.

User defined fields

22 The **User-Defined Fields** section allows you to provide values for fields that have already been established for subnets. User-defined fields are set up through the **User-Defined Fields** function on the **Policies** menu in the VitalQIP UI. Refer to"Enter information in user defined attributes or fields" (p. 7-24) for more information.

23 Choose one of the following actions.

If you want to...	**Then...**
Save your changes to the subnet profile	1. Click **Submit**. **Result:** A confirmation dialog opens with the message **Subnet modified: *<##.##.##.##>***. 2. Click **OK**. **Result:** The Subnet Properties page for the modified subnet opens.
Cancel any changes you made to the subnet profile	Click **Cancel**. **Result:** The Subnet Properties page opens.

END OF STEPS

Modify multiple subnet properties

Purpose

Multiple subnet properties can be modified at one time.

Procedure

To modify multiple subnet properties at once, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Expand the **Networks** node and select the network on which you want to modify multiple subnet properties.

Result: The Network properties page opens.

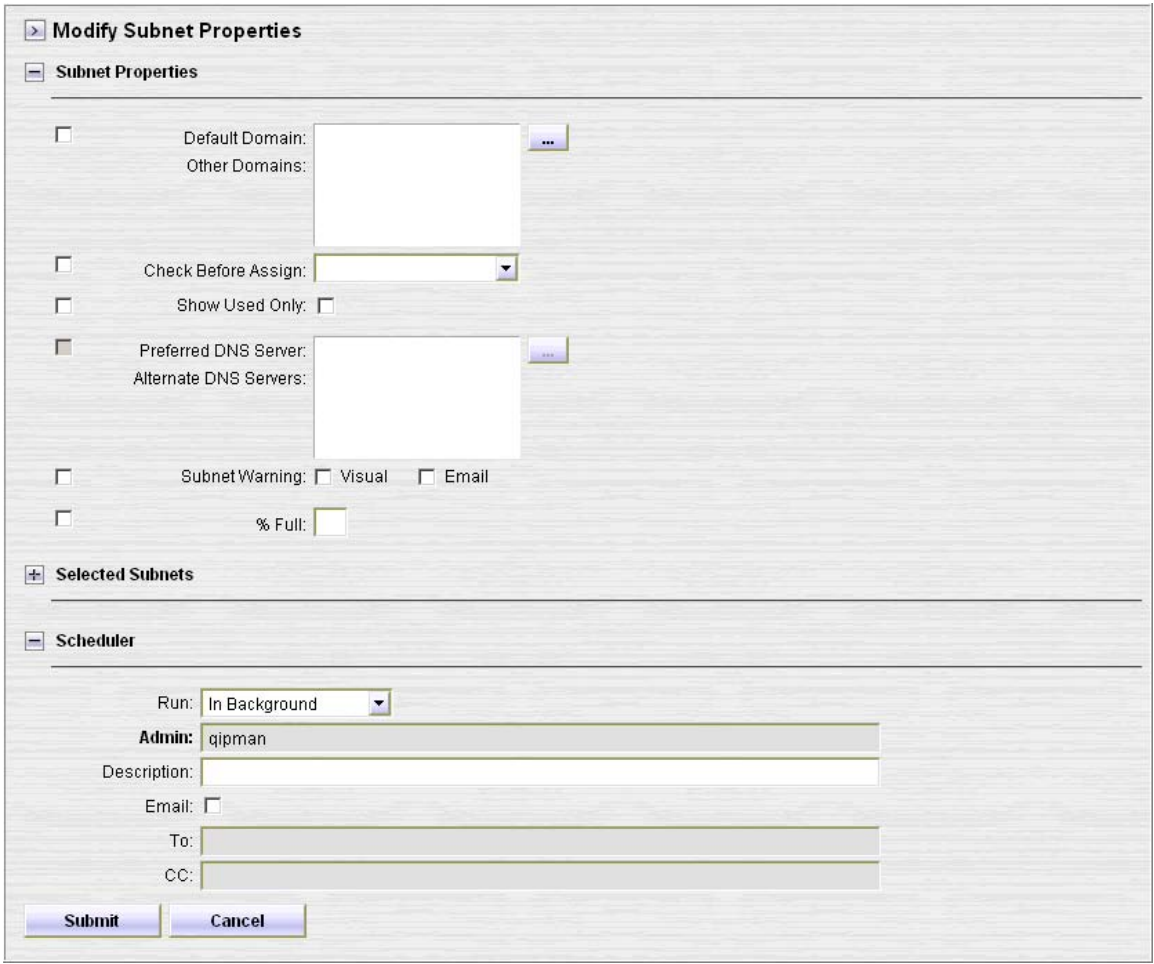
3 Click **Manage Subnets**.

Result: The Manage Subnets page opens.

4 Use the **Shift** and **Ctrl** keys to select the subnets you wish to modify.

5 Click **Modify**.

Result: The Modify Subnet Properties page opens.



6 Choose from the following actions.

If you want to ...	Then...
Modify subnet properties	1. If needed, expand the **Subnet Properties** section. 2. Check the fields you are modifying. 3. Make the appropriate changes to the selected fields, described in Table 9-3, "Subnet property fields" (p. 9-38) and Table 9-4, "Subnet profile fields" (p. 9-46).
View subnets being modified	If needed, expand **Selected Subnets** section.
Modify user defined attributes	Refer to "Use user defined attributes as search criteria" (p. 7-26) for more information.
Modify user defined fields	Refer to "Use user defined fields as search criteria" (p. 7-25) for more information.

If you want to ...	Then...
Set up the Scheduler	Refer to "Scheduler" (p. 9-77) for more information.

7 Click **Submit**.

Result: A confirmation dialog showing the results of the modification to each subnet opens.

8 Click **OK**.

Result: The Manage Subnet page opens.

END OF STEPS

Split a subnet

Purpose

Use this procedure to split a subnet into smaller subnets. You can specify the new subnet length and preview the result.

Before you begin

- If you split one or more subnets, the default router for the group may change.
- An error message is displayed when a user attempts to split a subnet that has a corresponding address block.

Procedure

To split a subnet, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over the **Actions** menu and select **View Subnets**.

Result: The Subnets node opens.

3 Expand the Subnets node.

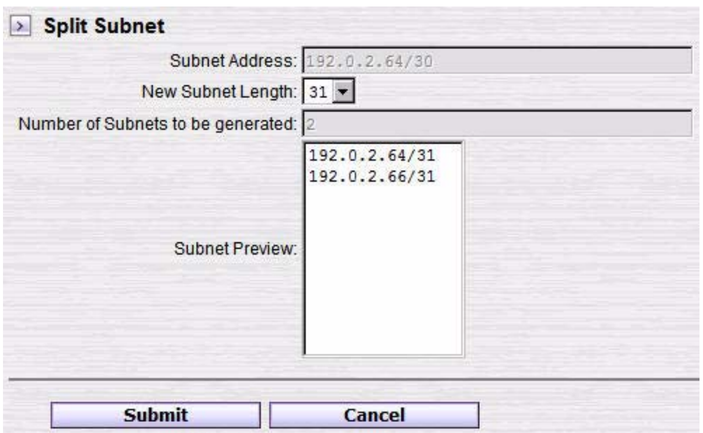
Result: A list of all subnets in the database opens.

4 Select the subnet that you want to split.

Result: The Subnet Properties page opens.

5 Click **Split Subnet**.

Result: The Split Subnet page opens.



6 Select the required length from the **New Subnet Length** drop-down list.

Result: The **Number of Subnets to be generated** field indicates how many subnets will be created, whereas **Subnet Preview** displays a scrollable list of the actual subnets that will result from the split.

7 Click **Submit**.

Result: A warning dialog box opens with the message **When splitting subnets, some properties associated with the subnet may be lost. Continue?**

8 Choose one of the following actions.

If you want to...	Then...
Continue with the subnet split	1. Click **OK**. **Result:** A confirmation dialog opens with the message **Successfully split subnet *<##.##.##.##>* to new length** *<#>*. 2. Click **OK**. **Result:** The list of subnets is updated and the VitalQIP Software IP Management splash screen opens.
Cancel the subnet split	Click **Cancel**. **Result:** The VitalQIP Software IP Management splash screen opens.

END OF STEPS

Join a subnet with the next available subnet

Purpose

Use this procedure to join (or reduce) the number of subnet addresses with the next available subnet on your network and use the space more efficiently.

Before you begin

- If you join subnets, the default router for the resultant subnet may change.
- Subnets cannot be joined if two objects in the “destination” subnets have the same MAC address (because duplicate MAC addresses cannot exist in the same subnet).
- An error message is displayed when a user attempts to split a subnet that has a corresponding address block.
- The target subnet should exist and be the same length (or size) as the source subnet. If no target subnet exists, a dialog box opens with the message **There is no matching subnet to join with** *<sourcesubnet>*.

Procedure

To join subnets, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over the **Actions** menu and select **View Subnets**.

Result: The Subnets view opens.

3 Expand the Subnets node.

Result: A list of all subnets in the database opens.

4 Select the subnet that you want to join.

Result: The Subnet Properties page opens.

5 Click **Join Subnet**.

Result: The Join Subnet page opens with the source and target subnet displayed (only one possible target subnet exists for each source subnet). The resulting subnet has the attributes of the target subnet. Any IP addresses present in the original subnet are moved under the newly created subnet at the same time as the original subnets are deleted.

6 Click **Submit**.

Result: A warning dialog box opens with the message **When joining subnets, some properties associated with the subnets may be lost. Continue?**

7 Choose one of the following actions.

If you want to...	**Then...**
Continue with the subnet join	1. Click **OK**. **Result:** A confirmation dialog opens with the message **Successfully joined subnet *<##.##.##.##>* into subnet *<##.##.##.##/#>***. 2. Click **OK**. **Result:** The list of subnets is updated and the VitalQIP Software IP Management splash screen opens.
Cancel the subnet join	Click **Cancel**. **Result:** The VitalQIP Software IP Management splash screen opens.

END OF STEPS

Join multiple subnets

Purpose

Use this procedure to join mutiple subnets.

Procedure

To join mutiple subnets, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Expand the **Networks** node and select the network on which you want to join multiple subnets.

Result: The Network properties page opens.

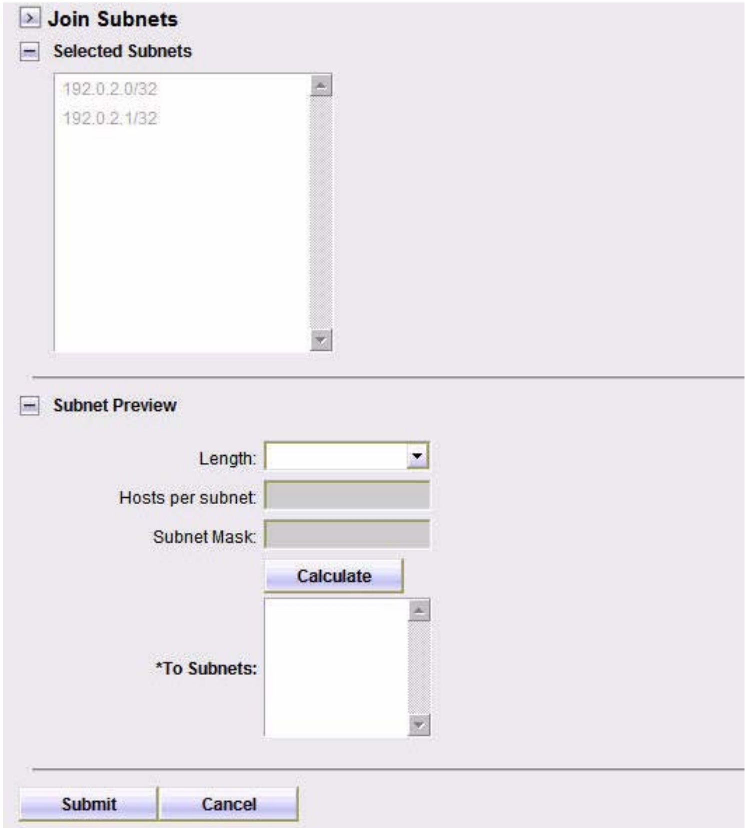
3 Click **Manage Subnets**.

Result: The Manage Subnets page opens.

4 Use the **Shift** and **Ctrl** keys to select the subnets you wish to join.

5 Click **Join**.

Result: The Join Subnets page opens.



6 If desired, you can expand the **Selected Subnets** section to view the subnet to be joined.

7 If not expanded, expand the **Subnet Preview** section.

8 From the **Length** field, select the length of the subnet mask.

Result: The **Host per subnet** and **Subnet Mask** fields are populated. These fields are read-only fields.

9 Click **Calculate**.

Result: A list of available subnets is calculated and displayed in the **To Subnets** field.

10 From the **To subnet** field, select a subnet.

11 Click **Submit**.

Result: A warning dialog box opens with the message **When joining subnets, some properties associated with the subnets may be lost. Continue?**

12 Choose one of the following actions.

If you want to...	Then...
Continue with the subnet join	1. Click **OK**. **Result:** A confirmation dialog opens with the message **Successfully joined subnet *<##.##.##.##>* into subnet *<##.##.##.##/#>***. 2. Click **OK**. **Result:** The list of subnets is updated and the VitalQIP Software IP Management splash screen opens.
Cancel the subnet join	Click **Cancel**. **Result:** The VitalQIP Software IP Management splash screen opens.

END OF STEPS

Manage a block associated with a subnet

Purpose

Use this procedure to manage a block associated with a subnet.

Before you begin

- The **Address Block** button on the Subnet Properties page is only enabled when a block is associated with the subnet.
- The **Address Block** button is not enabled if the **Access Address Allocation** privilege is set to False.
- **Split**, **Expand**, **Merge**, **Free**, **Move**, and **Renumber** operations can be enabled by specific privileges.

Procedure

To manage a block associated with a subnet, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over the **Actions** menu and select **View Subnets**.

Result: The Subnets view opens.

3 Expand the Subnets node.

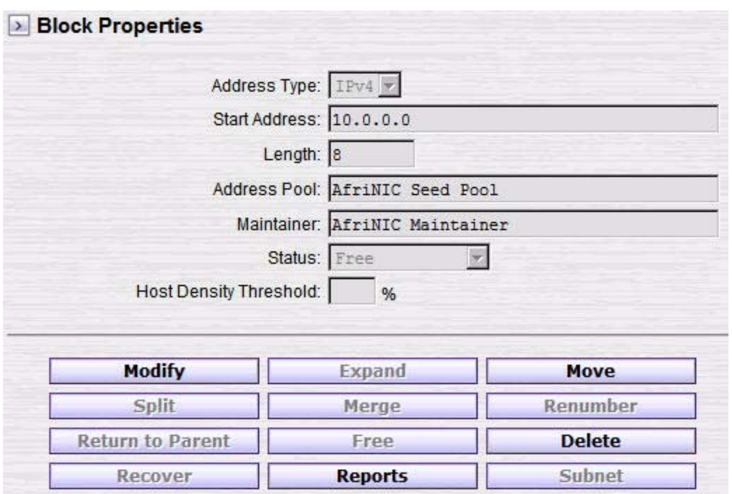
Result: A list of all subnets in the database opens.

4 Select the subnet.

Result: The Subnet Properties page opens.

5 Click **Address Block**.

Result: The Block Properties page opens.



6 A number of block maintenance features can be performed. Refer to the following table for more where to go information about the features.

If you want to...	**Refer to..**
Modify the block	"Modify a block" (p. 28-19)
Expand the block	"Expand a block" (p. 28-22)
Move the block	"Move a block" (p. 28-23)
Split a block	"Split a block" (p. 28-25)
Merge a block	"Merge a block" (p. 28-27)
Renumber block	"Renumber a block" (p. 28-29)
Return the block to the parent	"Return a block to its parent" (p. 28-31)
Free a block	"Free a block" (p. 28-33)
Delete a block	"Delete a block" (p. 28-36)
Recover a block	"Recover a block" (p. 28-34)
View block reports	"Produce a Block Hierarchy report" (p. 29-14) "Produce a Block Utilization report" (p. 29-18)
View the subnet profile associated with the block	"Manage a subnet assocated with a block" (p. 28-37)

END OF STEPS

Delete a subnet

Purpose

Use this procedure to delete a subnet.

Before you begin

- If any objects exist in the subnet you want to delete, they will also be deleted.
- Subnets that were created by the block allocation process cannot be deleted.

Procedure

To delete a subnet, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over the **Actions** menu and select **View Subnets**.

Result: The Subnets node opens.

3 Expand the Subnets node.

Result: A list of all subnets in the database opens.

4 Select the subnet you want to delete.

Result: The Subnet Properties page opens.

5 Click **Delete Subnet**.

Result: A warning dialog opens with the message **Objects associated with selected subnet(s) will be deleted as well. Continue?**

6 Click **OK**.

Result: The subnet is deleted and a confirmation dialog opens with the message **Subnet deleted:** *##.##.##.##*

7 Click **OK**.

Result: The subnet is removed from the IPv4 hierarchy and the VitalQIP Software IP Management splash screen opens.

END OF STEPS

Delete multiple subnets

Purpose

Multiple subnet properties can be deleted at one time.

Before you begin

- If any objects exist in the subnet you want to delete, they will also be deleted.
- Subnets that were created by the block allocation process or have a corresponding address block cannot be deleted.

Procedure

To delete multiple subnet properties at one, foll ow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens in the Network view (refer to Figure 9-1, “IPv4 Hierarchy - Networks node” (p. 9-4)).

2 Expand the **Networks** node and select the network on which you want to delete multiple subnets.

Result: The Network properties page opens.

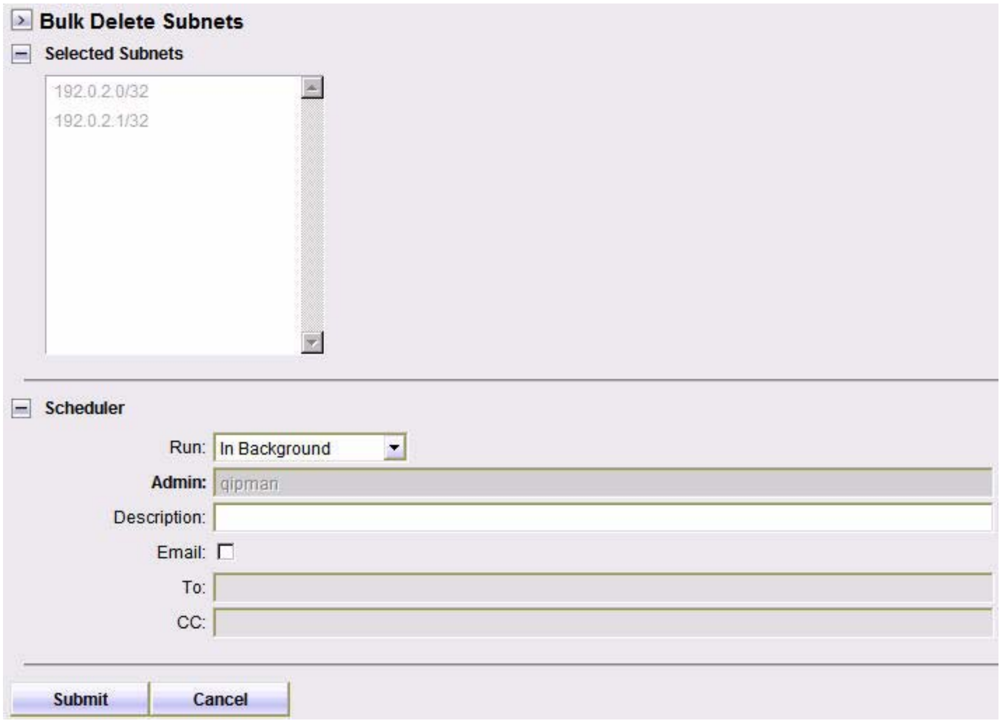
3 Click **Manage Subnets**.

Result: The Manage Subnets page opens.

4 Use the **Shift** and **Ctrl** keys to select the subnets you wish to delete.

5 Click **Delete**.

Result: The Bulk Delete Subnets page opens.



6 Choose the following.

If you want to …	Then…
View objects being deleted	If needed, expand **Selected Objects** section.
Set up the Scheduler	Refer to "Scheduler" (p. 9-77) for more information.

7 Click **Submit**.

Result: A message dialog opens.

8 Click **OK**.

Result: The Manage Subnets page opens.

END OF STEPS

Subnet organization management

Overview

Purpose

Subnet organizations group one or more subnets based on geography or organization. A single subnet cannot belong to more than one subnet organization, nor does it have to belong to any subnet organization at all. However, to handle noncontiguous subnet organizations, the subnets can be expanded (split), and portions of the subnets can be assigned to the subnet organization. Groups of subnets can be given names. A subnet can also be given a name at the time the first object(s) are assigned to it. These names are not significant within DNS.

A subnet organization can have either an address template or GAP associated with it but not both.

Global Allocation Policy

You can use Global Allocation Policy (GAP) to apply rules regarding the assignment of addresses to objects to more than one subnet in a subnet organization. GAP can only be used for static objects.

For example, GAP can cause the router and Wiring HUB to be automatically assigned to the first and second addresses respectively on every subnet in the subnet organization, or to other desired addresses. Global allocation policies can also cause any other object class to be assigned to specific addresses.

Address template assignment

You can use address templates rather than GAP. The address template is a more powerful tool than GAP. It enables you to create dynamic and reserved objects rather than only static objects. You have the option of creating those objects in a selected set of subnets after clicking Submit on the Subnet Organization page. The address template is not used in the creation of objects at any other time outside of the subnet organization add or modify.

Windows 2000 Domain Controller Sites

You can use subnet organizations to define Windows Domain Controller Sites. Refer to “Add a Windows site” (p. 9-83) for more information.

Add a subnet organization

Purpose

Use this procedure to add a subnet organization.

Before you begin

- If an address template is selected for the **Address Template** field, the **Global Allocation Policy** section is disabled and a **Scheduler** section is enabled. Refer to "Use global allocation policy" (p. 9-81) for more information on the **Global Allocation Policy** section.
- When scheduling objects to be created:
  - The job is not scheduled if the subnet organization profile is not successfully saved.
  - There is no roll back file if the scheduled job fails.
  - The subnet organization is not affected if objects fail to be created.
  - Objects are only created in subnets that contain no objects, not even reserved objects.
  - Selected subnets that contain objects are excluded from the object creation process.
  - Objects are created at the addresses that fit in the subnet if the address template is greater than the subnet.
  - No objects are created at the addresses specified in the address template that go beyond the last address of the subnet.
- To create a subnet organization, the administrator's type or access permissions must be one of the following:
  - Master administrator
  - Normal administrator with read and write managed type of **Organization** for the organization containing the subnet organization
  - Normal administrator with a managed type of **Normal** and **Create Infrastructure** privileges under either the **Use Default** privilege hierarchy or **Organization Defaults** privilege hierarchy

Procedure

To add a subnet organization, follow these steps:

1 Mouse over **Address Management** and click **IPv4**.

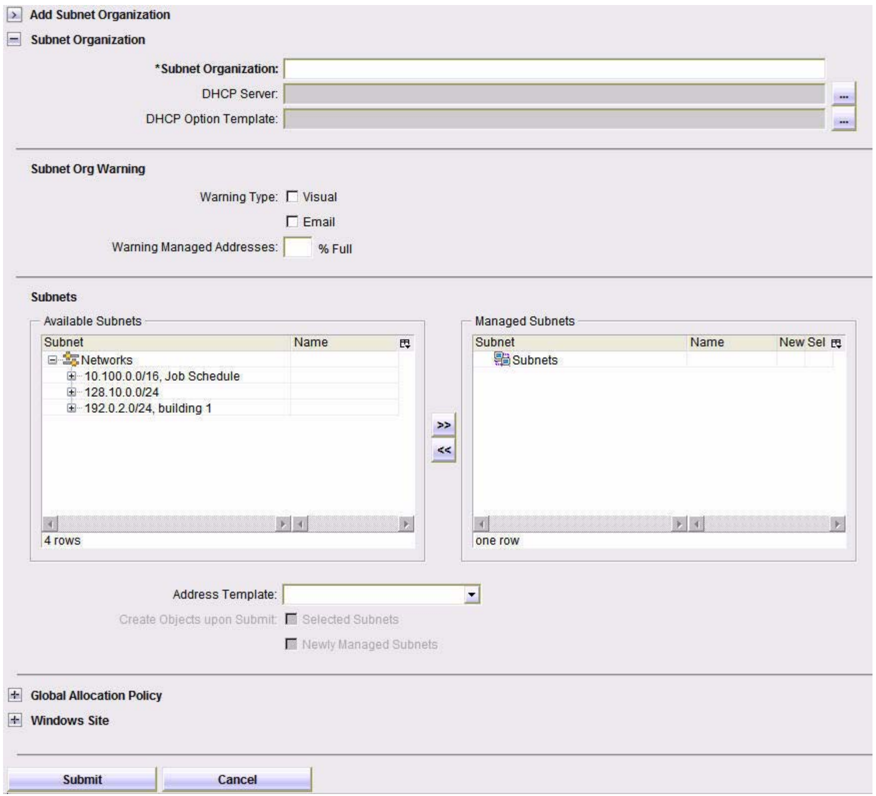
Result: The IPv4 Hierarchy opens.

2 Mouse over the **Actions** menu and select **View Subnet Organizations**.

Result: The IPv4 Hierarchy changes to the subnet organization view.

3 Mouse over the **Actions** menu and select **Add Subnet Organizations**.

Result: The Add Subnet Organization page opens.



4 Review the following table and enter the appropriate information.

Table 9-5 Add Subnet Organization fields

Field	Description
Subnet Organization	***Required.*** The name of the subnet organization. Numbers, letters, special characters, and spaces are allowed. A maximum of 32 characters can entered.

Field	Description
DHCP Server	***Optional***. Determines the DHCP server to associate with the subnet organization. During the push process, all objects in managed subnets that have **Same as in Subnet Profile** selected in the object profile and **Same as in SubnetOrg Profile** selected in the subnet profile use the same DHCP server settings. To search for a DHCP server, follow these steps. 1. Click ... . **Result:** The DHCP Server Search window opens. 2. Enter search criteria for the DHCP server you want in the **DHCP Server Name** field. Use the wildcard character as needed or leave blank to list all DHCP servers. 3. Click **Search**. **Result:** The results are listed in the **Existing List**. 4. Highlight the server you want and click **OK**. **Result:** The DHCP Server Search window closes and the server name you selected appears in the **DHCP Server** field.
DHCP Option Template	***Optional.*** Determines the DHCP Option Template to associate with the subnet organization. During the push process, all objects in the managed subnets that have **Same as in Subnet Profile** selected in the object option template and **Same as in SubnetOrg Profile** selected in the subnet option template use the same DHCP Option Template settings. To search for a DHCP Option Template, follow these steps. 1. Click ... . **Result:** The DHCP Option Template Search window opens. 2. Enter search criteria for the DHCP option template you want in the **DHCP Option Template** field. Use the wildcard character as needed or leave blank to list all DHCP option templates. 3. Click **Search**. **Result:** The results are listed in the **Existing List**. 4. Highlight the DHCP option template you want and click **OK**. The DHCP Option Template Search window closes and the template name you selected appears in the **DHCP Option Template** field.

Field	Description
Warning Type	***Optional***. Determines the type of warning to give when the network threshold level is exceeded. Check: • **Visual** - Indicates that a visual warning is given for exceeding the network threshold • **Email** - Indicates that an email warning is given for exceeding the network threshold level.
Warning Managed Addresses	***Optional***. Determines the threshold at which a warning is issued. It is based on the the number of addresses in service for this network.Valid values are 1 - 99.
Subnet	***Optional.*** A managed list of subnets can be added to or removed from the subnet organization: • To add a subnet or network, select the subnet or network from the **Available Subnets** list and click >> to add it to the **Managed Subnets** list. • To remove a subnet or network, select the subnet or network from the **Managed Subnets** list and click <<.
Address Template	***Optional.*** Assigns an address template to the subnet organization. **Result:** The **Create Object upon option submit** and a **Scheduler** section is displayed if you have an address template assigned to the subnet organization.
Create Objects upon Submit	If an address template is assigned, the following options become enabled: • **Selected Subnets** - Indicates that the selected subnets in the **Managed Subnets** list that contain no objects are created according to the selected address template. • **Newly Managed Subnets** - Indicates that any subnets that are added to the **Managed Subnets** list that contain no objects have objects created according to the selected address template.

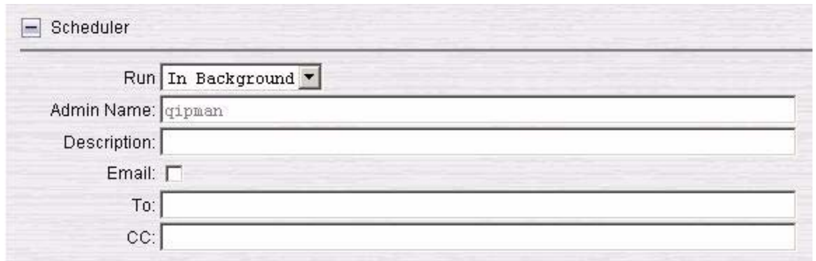
Scheduler

5 If you selected an address template in the **Address Template** field, the **Scheduler** section is displayed offering you the opportunity to schedule the object creation. Choose one of the following actions.

If you want to...	Then...
Run the job immediately	Ensure that **In Foreground** is selected in the **Run** drop-down list.

<table>
<tr><th>If you want to...</th><th>Then...</th></tr>
<tr><td>Run the job in background</td><td>
1. Select In Background from the Run drop-down list.

Result: The Scheduler section expands to display additional fields.



The Admin Name field displays the login ID of the administrator who is scheduling the job.

2. If desired, enter a description of the job in the Description field. You can enter up to 255 characters.
3. If you want an email to be sent when the job completes, place a check in the Email check box.

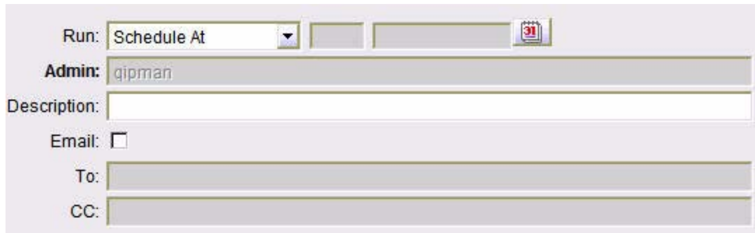
Result: The To and CC fields are enabled.

4. Enter an email address of up to 255 characters in the To field. If an email address has been entered in the Contact Profile for the administrator, it appears by default.
5. If desired, enter a CC email address. Multiple emails must be separated by a comma (,) or semi-colon (;).
</td></tr>
</table>

<table>
<tr><th>If you want to...</th><th>Then...</th></tr>
<tr><td>Schedule the job for a later time</td><td>

1. Select **Scheduled At** from the **Run** drop-down list.

Result: The Scheduler section expands to display additional fields, including a calendar icon.



The **Admin** field displays the login name of the administrator who is scheduling the job.

2. Click the Calendar icon ( ).

Result: The Calendar window opens with the current time and date selected.

3. Choose from the following actions.
   a. To choose a different time, click in the hour and minute fields and enter a new time in 24-hour format.
   b. To choose a different month, click to select a prior month or to select a later month.
   c. To choose a different year, click to select a prior year or to select a future year.
   d. To choose a different day, double-click another day in the month.

Result: After a different day is clicked, the calendar window closes and a new run date and/or time are displayed.

4. Enter a description of the job in the **Description** field. If you do not enter a description, a description of *<Run Mode>:<Job Name>* is used. You may enter up to 255 characters.

</td></tr>
</table>

If you want to...	Then...
	1. If you want an email to be sent when the job completes, place a check in the **Email** check box. **Result:** The **To** and **CC** fields are enabled. 2. Enter an email address of up to 255 characters in the **To** field. If an email address has been entered in the **Contact Profile** for the administrator, it appears by default. 3. If desired, enter a **CC** email address.

Global Allocation Policy

6 The **Global Allocation Policy** section displayed when if **Address Template** field is not set. Refer to "Use global allocation policy" (p. 9-81) for more information.

Windows Site

7 The **Windows Site** section allows you to set up a Windows site for the subnet organization. Refer to "Add a Windows site" (p. 9-83) for more information.

User Defined Attributes

8 The **User Defined Attributes** section is diplayed if user defined attributes are associated with the subnet organization. Refer to "Enter information in user defined attributes or fields" (p. 7-24) for more information.

9 Click **Submit**.

Result: A dialog box open indicating if the subnet organization was successfully added.

END OF STEPS

Use global allocation policy

Purpose

The Global Allocation Policy (GAP) function allows you to assign an object type to an address range on each subnet in the subnet organization.

Take the following example. Suppose you set an offset number of 1 from start to the object class router. When a router is assigned to this address range in a subnet organization, it is given the first address from the beginning of the address range. Assume a subnet organization has the following managed subnets:

170.97.0.128

170.97.1.0

170.97.1.128

It means that the following addresses have been reserved for routers (assuming that the subnets have not yet been used):

170.97.0.129

170.97.1.1

170.97.1.129

Note: The first and last address of each subnet is reserved for network and broadcast.

Before you begin

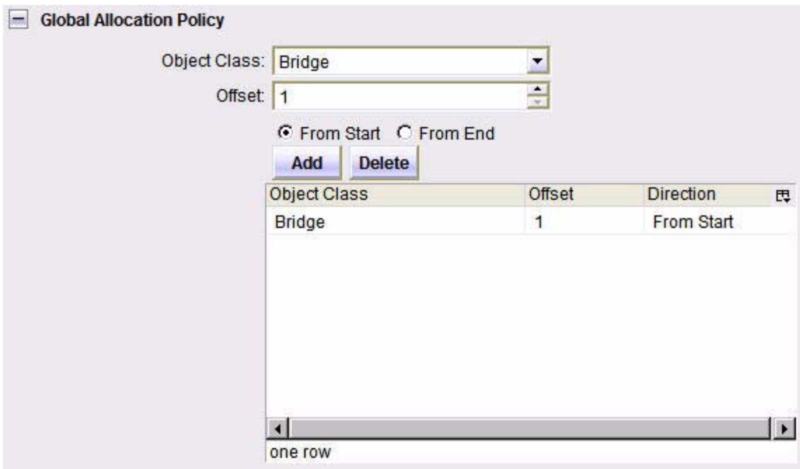
- The **Global Allocation Policy** section is disabled if **Address Template** field is set.
- When GAP objects are defined for a subnet organization and the subnet organization definition is saved, the GAP Objects open in the Object Management window if the subnet is free/empty (Object List) for each subnet, which is part of the subnet organizations Used (GAP). Once any change is made to any address in the subnet (for example, an object is added), all GAP objects become real objects within the Subnet (for example, the object status changes from Used (GAP) to Used).
- A subnet must belong to a subnet organization to use GAP.
- If a subnet in a subnet organization is too small for the GAP, the address index is not used, and and the static GAP object will not be created.
- The global policy, **Gap Direction**, handles conflicts if the values are from the beginning and the end. In other words, if a subnet has two addresses, a GAP specifying one from the start and a GAP specifying one from the end, and they fall on the same address, this Global policy determines the final outcome.

Procedure

To define a Global Allocation Policy for object classes in a subnet organization, follow these steps:

1 In the subnet organization page, expand the **Global Allocation Policy** section.

Result: The **Global Allocation Policy** section opens.



2 In the **Object Class** field, select the object class for GAP objects. The available options are:

- Workstation
- X-terminal
- PC
- Printer
- Server
- Wiring_HUB
- Router
- Bridge
- Terminal_Server
- Switch
- Legacy_System
- Gateway
- Test_Equipment
- Undefined

- Others
- Partially_Managed

3 In the **Offset** field, enter the offset from the start or end of the subnet to set the GAP object. Valid numbers are 1 - 2147483647. No more than 10 digits can be entered.

4 Select where the offset address is:

- **From Start** - Indicates the direction of the offset to be from the start of the subnet. **From End** - Indicates the direction of the offset to be from the end of the subnet.

5 Click **Add**.

Result: A row is added to the Object Class list. The row field is updated to display the number of rows in the **Object Class** list.

6 Repeat Step 2 - Step 5 as needed. If you need to delete an object class from the list, select the object class and click **Delete**.

7 Click **Submit**.

Result: A dialog box opens indicating if your changes were successfully made.

END OF STEPS

Add a Windows site

Purpose

Use this procedure to set up a Windows site.

Before you begin

- To set up VitalQIP so that it can manage a Windows site, a Windows Domain Controller needs to be set up in VitalQIP. Refer to Chapter 8, "Domain Controller maintenance"

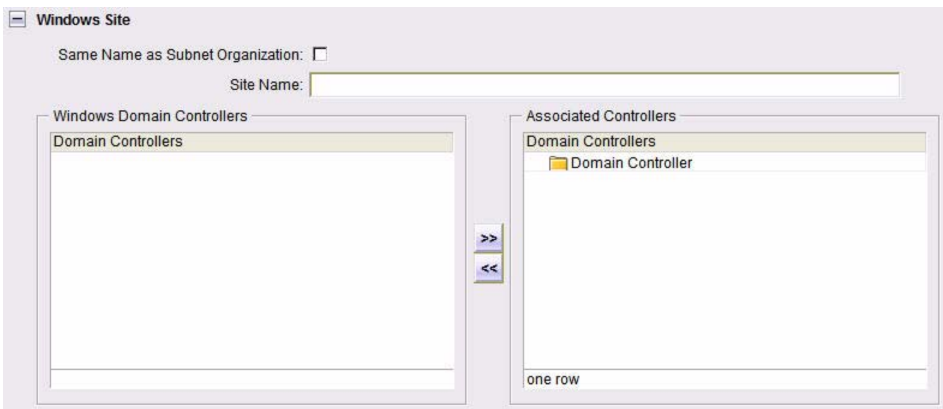
- Define the global policy **Delete Sites/Subnets from Active Directory**. If set to True, it allows you to delete information from Active Directory whenever a subnet and/or subnet organization is deleted from VitalQIP. It is also true of a subnet that is split or joined; not only is it removed from a subnet organization but it is removed from Active Directory. Refer to "Delete Sites/Subnets from Active Directory" (p. 2-25).

Procedure

To set up a Windows Site to be managed by VitalQIP, follow these steps:

1 In the subnet organization page, expand the **Windows Site** section.

Result: The **Windows Site** section opens.



2 Check **Same Name as Subnet Organization** if you want the name of the Windows site to be the same as the subnet organization. Alternatively, you can leave **Same Name as Subnet Organization** unchecked and enter a name in the **Site Name** field.

Note: The site name can only contain alphanumeric characters and hyphen (-). There must be at least one letter of the alphabet; the name cannot be all numerals. Spaces are not allowed. A maximum of 32 characters can be used for the site name.

3 To associate a Domain Controller with the Windows site or remove a Domain Controller:

- To associate a Domain Controller, select a Domain Controller from the **Windows Domain Controller** list and click >> to add it to the **Available Controller** list.
- To remove a Domain Controller, select a Domain Controller from the **Available Controller** list and click <<.

4 Click **Submit**.

Result: A dialog box opens indicating that your changes were successfully made.

END OF STEPS

Modify a subnet organization

Purpose

Use this procedure to modify a subnet organization.

Before you begin

- To modify a subnet organization, the administrator's type or access permissions must be one of these:
  - Master administrator
  - Normal administrator with read and write managed type of **Organization** for the organization containing the subnet organization
  - Normal administrator with a managed type of **Normal** and **Create Infrastructure** privileges under either the **Use Default** privilege hierarchy or **Organization Defaults** privilege hierarchy.

Procedure

To modify a subnet organization, follow these steps:

1 Mouse over the **Address Management** tab and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over the **Actions** menu and select **View Subnet Organizations**.

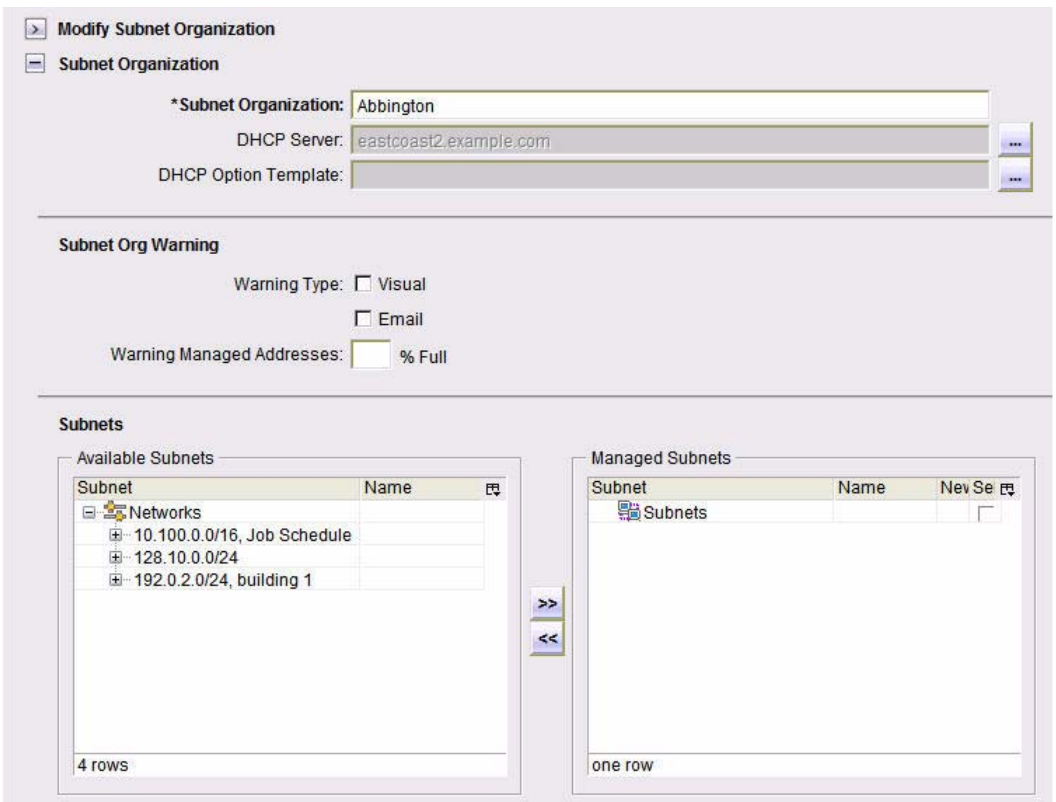
Result: The Subnet Organization node opens.

3 Expand the node and select a subnet organization.

Result: The Subnet Organization Properties page opens.

4 Click **Modify**.

Result: The Modify Subnet Organization page opens.



5 Modify the fields as needed. Refer to Table 9-5, “Add Subnet Organization fields” (p. 9-75) for more details.

Note: When modifying a subnet organization, the **DHCP server** or **DHCP Option Template** fields cannot be changed to blank if at least one of its associated subnets has a DHCP server setting of **Same as in SubnetOrg Profile**.

6 Click **Submit** when you finished.

Result: The subnet organization is modified.

END OF STEPS

Delete a subnet organization

Purpose

Use this procedure to delete a subnet organization.

Before you begin

- To delete a subnet organization, the administrator's type or access permissions must be one of these:
  - Master administrator
  - Normal administrator with read and write managed type of **Organization** for the organization containing the subnet organization
  - Normal administrator with a managed type of **Normal** and **Create Infrastructure** privileges under either the **Use Default** privilege hierarchy or **Organization Defaults** privilege hierarchy.

Procedure

To delete a subnet organization, follow these steps:

1 Mouse over the **Address Management** tab and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over the **Actions** menu and select **View Subnet Organizations**.

Result: The Subnet Organization node opens.

3 Expand the node and select a subnet organization.

Result: The Subnet Organization Properties page opens.

4 Click **Delete**.

Result: A dialog box opens with the message **Permanently Delete the Subnet Organization:** <*subnet organization*>**. Continue?**

5 Click **OK**.

Result: The subnet organization is deleted.

END OF STEPS

Reclaim addresses

IP addresses are a scarce commodity, so there needs to be a mechanism to reclaim unused addresses for re-use. The Reclaim Addresses function is used to select IP addresses that are stale because an object has been moved or a network has been collapsed. These addresses are returned to the pool of available addresses (changing their state to “Unused”).

> **Note:** Only Static, Reserved and Dynamic (None) objects that are unreachable can be reclaimed. M-DHCP, M-Bootp, D-DHCP, A-DHCP, and A-Bootp objects cannot be reclaimed.

The Schedule Reclaim aspect of the **Reclaim** function allows you to develop historical data and reclaim addresses on a subnet at the end of the schedule.

The ability to determine whether an address is in use is much more than simply determining if it is alive or dead. The address may appear dead because a user has switched off a workstation or because the user is on leave. Therefore, historical data needs to be gathered to allow an administrator to make a better judgment. In addition, an address may be in use legally (if it was previously allocated) or illegally. Each time the subnet is pinged, information on each object in the subnet is gathered and placed into files in the VitalQIP database and a report generated in the VitalQIP report directory (*%QIPHOME%\report*). If the addresses in the subnet are not responding to the ping, optionally their database status will change and they will be reclaimed for reuse.

The **Allow Automatic Reclaim** global policy can be set to control the action of the Schedule Reclaim. Refer to Table 2-6, “General policies” (p. 2-22).

The Reclaim window has two buttons that perform distinctive functions. **Check Current Status** accesses network and database information on objects in a subnet by pinging the selected subnets for response. If the ping “fails” (no response is received), the address is available for reclaim. However, **Check Current Status** does not change the address for reclaim, it merely gives the user information regarding that object.

Reclaim Addresses changes that information in the database so that the address can be reused (or reclaimed) in the Subnet Profile. In the Reclaim function, an address can be automatically reclaimed if:

- The Status is “Static”, “Reserved”, or “Dynamic - None”
- The Network Status is “In DNS; Unreachable” or “Not in DNS; Unreachable”

If the object does not respond to the ping and the reclaim type is not report only, the Database Status of the address is marked as “Unused”. To re-use the address, access the address through Object Management.

Reclaim an address

Purpose

Use this procedure to reclaim IP addresses.

Before you begin

Only Static, Reserved and Dynamic (None) objects that are unreachable can be reclaimed. MDHCP, M-Bootp, D-DHCP, A-DHCP, and A-Bootp objects cannot be reclaimed.

Procedure

To reclaim an IP address, follow these steps:

1 Choose one of the following actions.

<table>
<tr><th>If you want to ...</th><th>Then ...</th></tr>
<tr><td>Reclaim an address reclaim at the network level</td><td>

1. Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

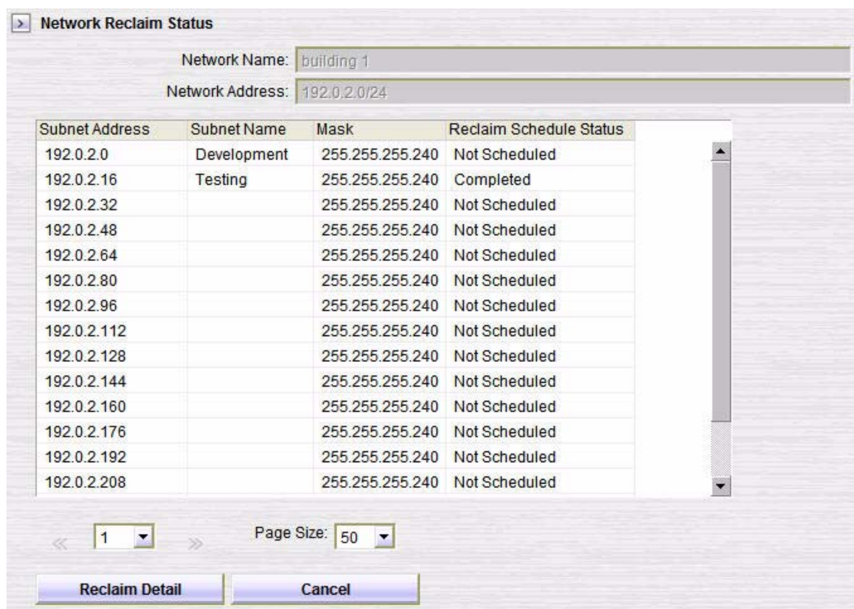
2. From the **Actions** menu, select **View Networks**.

Result: The IPv4 Hierarchy changes to a newtork view.

3. Expand Networks and select the network you want to reclaim.

Result: The Network Properties page opens.

4. Click **Reclaim Detail**. The Network Reclaim Status displays.



Result: The following Reclaim Schedule Statuses for each subnet in the network:

- **Not Scheduled** - subnet is not scheduled for reclaim.
- **In Progress** - subnet reclaim is scheduled and is currently in the process of being reclaimed.
- **Completed** - the reclaim process has finished.

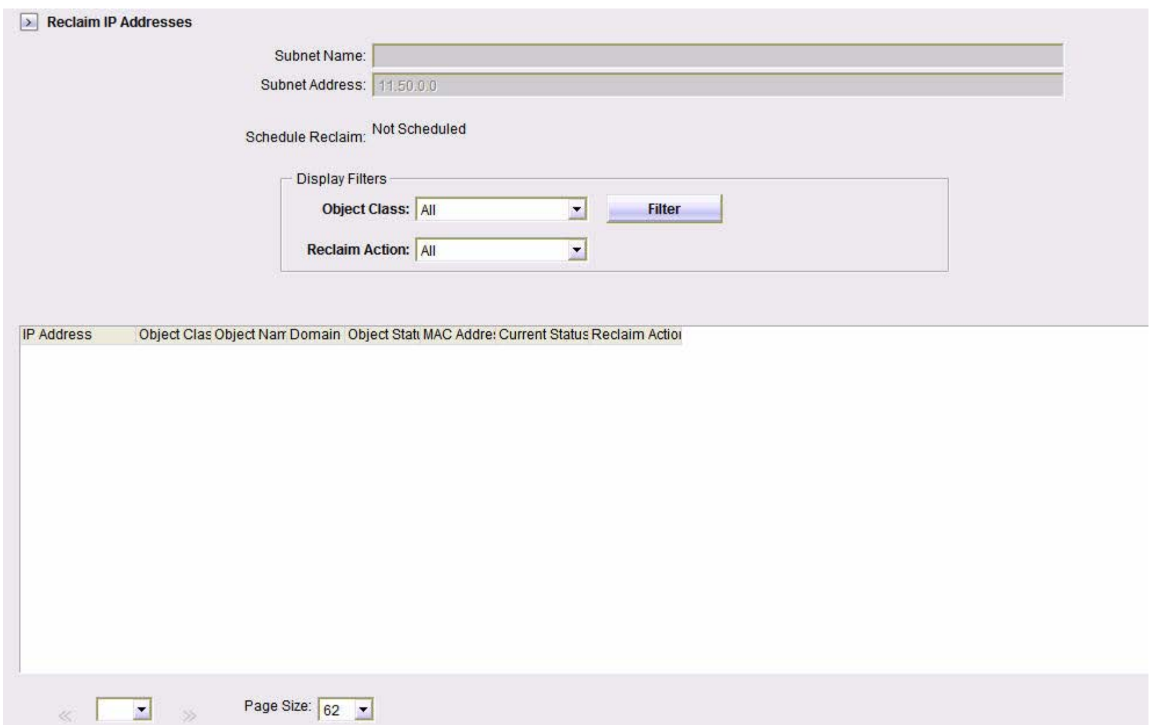
5. Click a subnet you want to reclaim.

</td></tr>
</table>

If you want to ...	Then ...
Reclaim an address at the subnet level	1. Mouse over **Address Management** and click **IPv4**. **Result:** The IPv4 Hierarchy opens. 2. From the **Actions** menu, select **View Subnets**. **Result:** The Subnets node opens. 3. Expand the Subnets node. 4. Select the desired subnet. **Result:** The Subnet Properties page opens.

2 Click **Reclaim Detail**.

Result: The Reclaim IP Addresses page opens.



3 Select the display filters to list the objects you wish to reclaim: select an object class from the **Object Class** drop-down list (or leave it at the default value of All), and choose a status value from the **Reclaim Action** drop-down list:

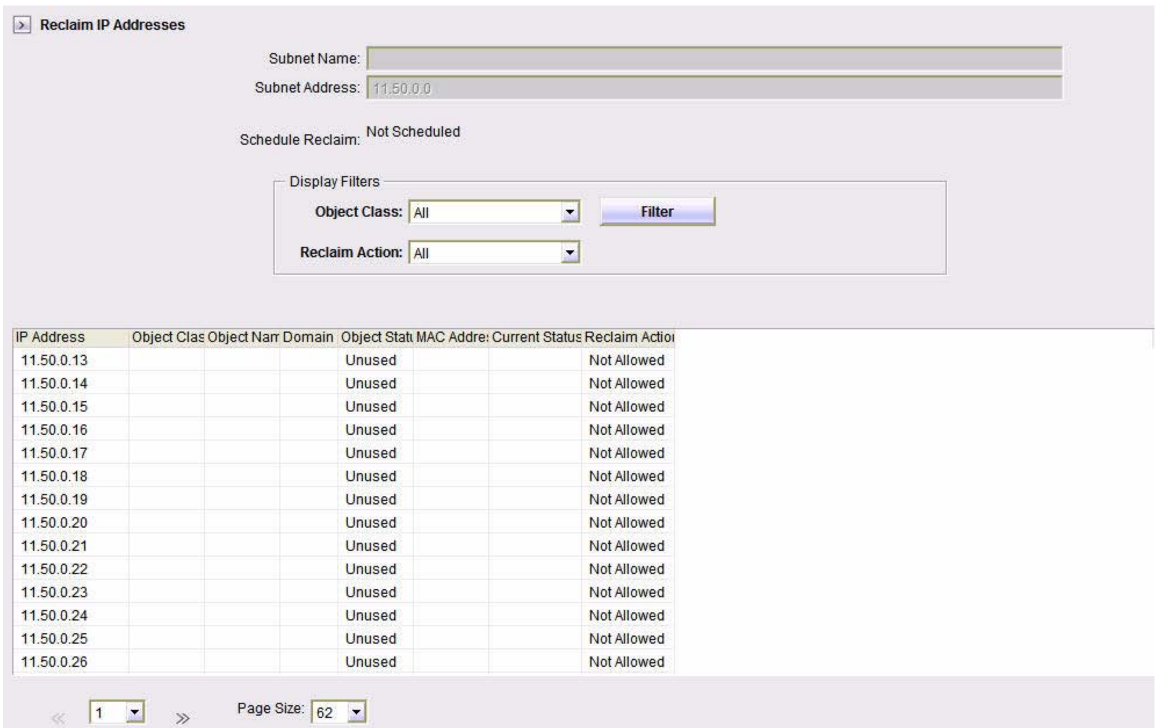
- **All**
- **Allowed**
- **Not Allowed**

- **Not Advised**

  Note: If no reclaim statistics have been collected yet for this subnet, only **All** returns data.

  Not Advised does not return any data if a reclaim on the subnet's reclaim status is "Not Scheduled".

4 Click **Filter** to populate the list of objects.



5 Select the objects you want to reclaim. To make multiple selections, hold the **Ctrl** key while selecting the objects.

6 To reclaim the selected addresses, click **Reclaim Addresses**.

Result: The addresses are reclaimed by deleting the objects.

END OF STEPS

Schedule an address reclaim

Purpose

Use this procedure to schedule reclaim.

Before you begin

- If a subnet split, join or immediate object move occurs on the subnet while a reclaim is scheduled, a warning dialog box appears, indicating that all scheduled reclaims in the selected subnet(s) will be aborted. If users still choose **Yes**, a report is generated with the current statistics and note the reason the scheduled reclaim was canceled, including the name of the administrator who caused the cancellation.
- If you change the **Data Collection (Ping) Schedule** setting from "Schedule By Interval" or "Schedule By Day" to "None," a warning dialog box is displayed. If the subnet schedule reclaim status is "In Progress", a report is sent to the email address (in the **Reclaim Email Address** parameter) with the current statistics and a note identifying the reason the reclaim was aborted, including the name of the administrator who caused the cancellation.

Procedure

To schedule a reclaim, follow these steps:

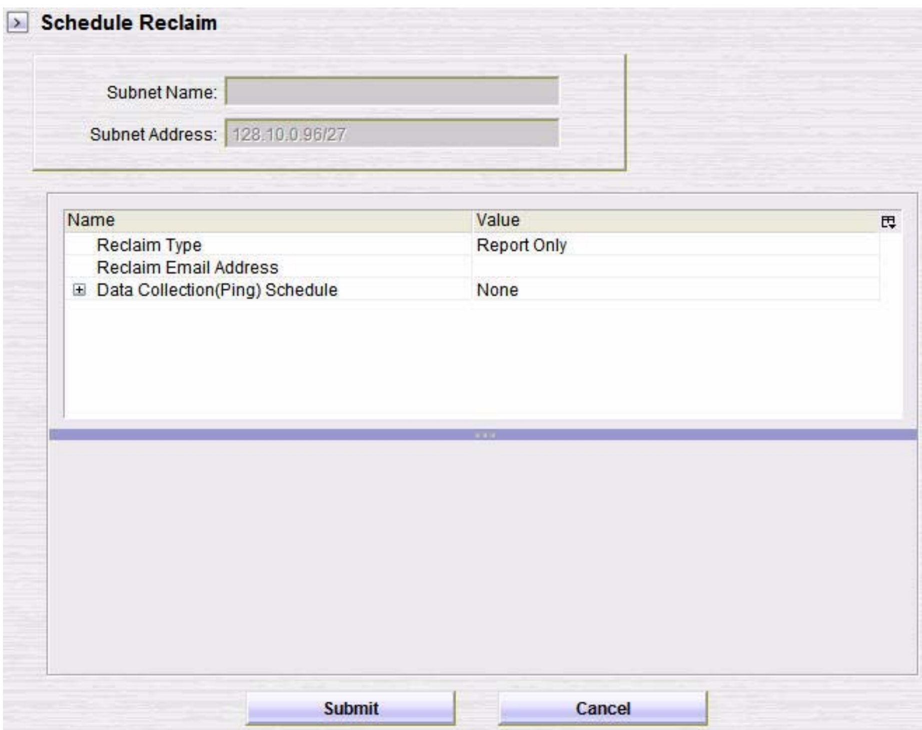
1 Choose one of the following actions.

If you want to…	Then…
Schedule a subnet reclaim through the network level	1. Mouse over **Address Management** and click **IPv4**. **Result:** The IPv4 Hierarchy opens. 2. From the **Actions** menu, select **View Networks**. **Result:** The IPv4 Hierarchy changes to a newtork view. 3. Expand Networks and select the network whose address you want to reclaim. **Result:** The Network Properties page opens.

If you want to...	Then...
Schedule a reclaim through the subnet level	1. Mouse over **Address Management** and click **IPv4**. **Result:** The IPv4 Hierarchy opens. 2. From the **Actions** menu, select **View Subnets**. **Result:** The Subnets node opens. 3. Expand the Subnets node. 4. Select the desired subnet. **Result:** The Subnet Properties page opens.

2 Click **Schedule Reclaim**.

Result: The Schedule Reclaim page opens. The follow example shows the **Network Name** and **Network Address** fields. If the page accessed at a subnet level, the page shows the **Subnet Name** and **Subnet Address** fields.



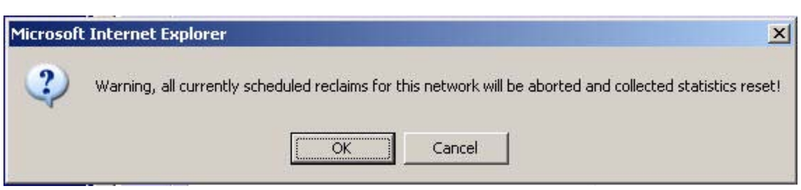
3 Select parameters for scheduling the reclaim, as described in the following table.

Table 9-6 Schedule reclaim parameters

Parameter	Default value	Usage
Reclaim Type	Report Only	Allowable values are: **Report Only**, **Reclaim Only**, and **Report and Reclaim**. **Note:** When **Allow Automatic Reclaim** policy is set to true, the available values are **Report Only**, **Reclaim Only Report**, and **Reclaim**. When **Allow Automatic Reclaim** policy is set to false then the only available value is **Report Only**.
Reclaim E-mail Address		Enter an email address where a report can be sent if a scheduled reclaim is aborted for some reason or to be notified that a scheduled reclaim is complete.
Data Collection (Ping) Schedule	None	Allows you to set up a schedule to ping all objects in a subnet. If you select “By Day”, you can specify a set of times (up to 6) at which the ping will occur in the **Time of Day** field. There must be at least an hour between the times you enter. You may also change the number of days the pinging will occur (up to 365) in the **Total Number of Days** field. If you select “By Interval”, you can specify a time interval over which the pinging will occur by entering a number of days, hours, and minutes in the **Time Interval** field. You may also change the number of times (up to 255) the pinging should occur in the **Total Number of Times** field. If you select “None”, the reclaim is cancelled, and all other data collection values are disabled.

4 Click **Submit** when you have finished setting up the schedule parameters.

Result: If a scheduled reclaim is in progress or completed, the following confirmation prompt opens.



5 Click **OK**.

Result: A prompt confirms that the reclaim schedule has been saved.

END OF STEPS

Check status of a scheduled reclaim

Purpose

Once a scheduled reclaim has started, you may want to check its progress.

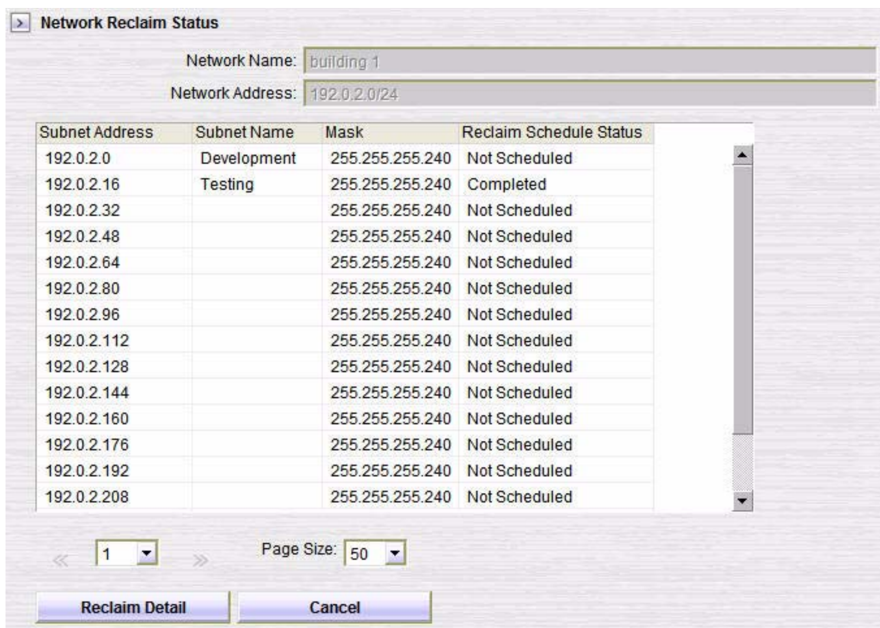
Before you begin

The **Check Status** button is available whether the reclaim has completed, in progress, or not been scheduled

Procedure

To check on a reclaim, follow these steps:

1 To begin, choose one of the following actions.

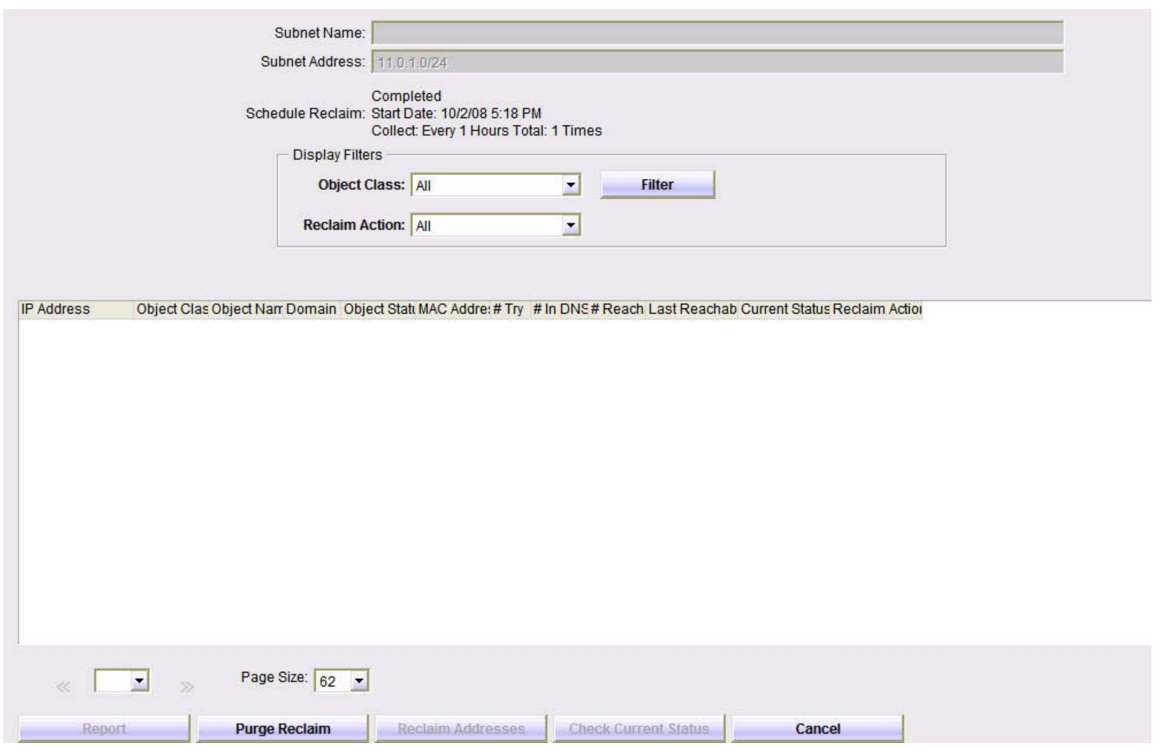
<table>
<tr><th>If you want to …</th><th>Then…</th></tr>
<tr><td>Check the status of subnet reclaim through the network level</td><td>
1. Mouse over **Address Management** and click **IPv4**.
Result: The IPv4 Hierarchy opens.
2. From the **Actions** menu, select **View Networks**.
Result: The Networks node opens.
3. Expand the Networks node and select the network whose address you want to reclaim.
Result: The Network Properties page opens.
4. Click **Reclaim Detail**. The Network Reclaim Status displays.


Result: The following Reclaim Schedule Statuses for each subnet in the network:
• **Not Scheduled** - subnet is currently not scheduled for reclaim.
• **In Progress** - subnet reclaim has been scheduled and is in currently in the process of being reclaimed.
• **Completed** - the reclaim process has finished.
5. Click a subnet you want to schedule for a reclaim.
</td></tr>
</table>

If you want to ...	Then...
Check the status of a scheduled reclaim through the subnet level	1. Mouse over **Address Management** and click **IPv4**. **Result:** The IPv4 Hierarchy opens. 2. From the **Actions** menu, select **View Subnets**. **Result:** The IPv4 Hierarchy changes to a subnet view. 3. Expand hierarchy until you reach the desired subnet. 4. Select the subnet. **Result:** The Subnet Properties page opens.

2 Click **Reclaim Detail**.

Result: The Reclaim IP Addresses window opens. The status of the reclaim is displayed below the subnet's IP address.



3 Select parameters for seeing IP addreses scheduled to be reclaimed.

Table 9-7 Schedule reclaim fields

Field	Description
Object Class	Filters the list by class of objects. Select one of the following: • **All** • **Bridge** • **External** • **Gateway** • **Legacy_System** • **Others** • **Partially_Managed** • **PC** • **Printer** • **Router** • **Server** • **Switch** • **Terminal_Server** • **Test_Equipment** • **Undefined** • **Wiring_HUB** • **Workstation** • **X-terminal**
Reclaim Action	Filter the list by reclaim action. Select one of the following: • **All** • **Allowed** • **Not Allowed** • **Advised**

4 Click **Filter** to populate the list of objects.

5 Select the objects whose reclaim status you want to check. To make multiple selections, hold the **Ctrl** key while selecting the objects.

6 Click **Check Current Status.**

Result: If the subnet's reclaim status is either "Completed" or "In Progress, a dialog opens with the message **Do you want to update the results being collected in the database?**

7 Choose one of the following:

- **Yes** - The database is updated with new results
- **No** - The status is updated in the table

8 The values in the columns are explained in the following table.

Table 9-8 Reclaim status column descriptions

Column	Description
IP Address	The IP address of object.
Object Class	The object class type.
Object Name	The name of the object.
Status	The object status of the address.
# Try	The number of times a ping was attempted against the address during the scheduled reclaim period.
# In DNS	The number of times the object name was found in DNS – this is used for reporting purposes only. If **# In DNS** is greater than 0, but the **Status** is Unused, then the address had an object associated with it at one time, but was deleted sometime during the scheduled reclaim period.
# Reachable	The number of times the ping was responded to. If a machine responded every time the reclaim process performed a ping, the **# Try** and **# Reachable** columns would be equal.
Last Reachable	The last date an address responded to the ping attempt.
Current Status	Collects the network information and indicates whether the address is reachable. The available values are: In DNS; Reachable In DNS; Unreachable Not In DNS; Reachable Not In DNS; Unreachable

Column	Description
Reclaim Action	Shows whether the address is reclaimable. The available values are: • **All** - Displays all subnets regardless of reclaim status. • **Not Allowed** - If the **Status** column is something other than Static, Reserved or Dynamic (none). • **Allowed** - **Status** is reclaimable. The object is Static, Reserved or Dynamic(none) ***and*** the value in the **#Reachable** column is 0. • **Not Advised - Status** is reclaimable. The object is Static, Reserved or Dynamic(none) ***and*** the value in the **#Reachable** is greater than 0.

9 You may also decide, having reviewed the status reports on objects slated to be reclaimed, that enough time has elapsed and that you have enough information to proceed with a manual reclaim. Select the addresses you want to reclaim (the **Reclaim** column should read "Allowed") and click **Reclaim Address**.

Result: A confirmation dialog opens with the message **Selected addresses will be reclaimed as unused addresses. Are you sure?**

10 Click **Yes** to continue.

Result: The addresses are reclaimed. A report is sent to the scheduler's email address with the current statistics and a note identifying the reason the reclaim was aborted, including the name of the administrator who cancelled it. A report is also created under *%QIPHOME%\report* directory for the subnet.

END OF STEPS

Sample reclaim reports

Reports are generated when the **Reclaim Type** parameter is set to "Report Only" and "Report and Reclaim", and at times or intervals specified by the **Data Collection Schedule** parameter in the Schedule Reclaim window. Not only are reports sent to the email address specified in the Schedule Reclaim window, but they are also saved to the *%QIPHOME\Report* directory where they are stored with a date and time stamp in the filename to aid identification. For example, the following reports were generated one day apart at 17:30 each day. The filenames are *SRbcb80020.200202191730* and *SRbcb80020.200202201730*.

```
<<<<< SCHEDULED RECLAIM REPORT >>>>>

Report Date:  02/19/2002 17:30  Start Date:  02/18/2002 23:19
Collection Frequency: Collect: Every Day At (17:30 ) Total: 2 Days
SUBNET: 188.184.0.32
                                    Object      Object   #    #      #
   Reclaim  Last Time
Address              Name                  Class       Status   Try In DNS
   Reachable  Status   Reachable
----------------------------------------------------------------------------
   -------------------------

188.184.0.33 chrom1.chromarty.com      Server      Static  3   0       0
   Not In DNS;Unreachable
188.184.0.34 chrom_backup.chromarty.com Server     Static  3   0       0
   Not In DNS;Unreachable
188.184.0.35 chrom_dhcp.chromarty.com   Server     M-DHCP  1   0       0
   Not In DNS;Unreachable
188.184.0.36 bootp_ross.chromarty.com   Server     M-Bootp 1   0       0
   Not In DNS;Unreachable
188.184.0.37 rtp000003rts.chromarty.com Router     A-Bootp 1   0       0
   Not In DNS;Unreachable
188.184.0.38 whp000024whs.chromarty.com Wiring_HUB  Static  3   0       0
   Not In DNS;Unreachable
188.184.0.39 whp000025whs.chromarty.com Wiring_HUB  Static  3   0       0
   Not In DNS;Unreachable
188.184.0.40 wsp000023wss.chromarty.com Workstation Static  3   0       0
   Not In DNS;Unreachable
188.184.0.41 wsp000024wss.chromarty.com Workstation Static  3   0       0
   Not In DNS;Unreachable
188.184.0.42                                      Unused  1   0       0
   Not In DNS;Unreachable
188.184.0.43                                      Unused  1   0       0
   Not In DNS;Unreachable
188.184.0.44                                      Unused  1   0       0
   Not In DNS;Unreachable
188.184.0.45                                      Unused  1   0       0
   Not In DNS;Unreachable
188.184.0.46                                      Unused  1   0       0
   Not In DNS;Unreachable
```

The report produced after the reclaim, notice how the Static addresses in the first report have been reclaimed in the second report and now have an “Unused” status.

```
<<<<< SCHEDULED RECLAIM REPORT >>>>>

Report Date:  02/20/2002 17:30 Start Date:  02/18/2002 23:19
Collection Frequency: Collect: Every Day At (17:30 ) Total: 2 Days
SUBNET: 188.184.0.32
                                          Object   Object    #    #       #        Reclaim   Last Time
Address             Name                  Class    Status   Try In DNS  Reachable  Status    Reachable
-----------------------------------------------------------------------------------------------------

188.184.0.33                              Unused    Unused   1    0    0      Not In DNS; Unreachable
188.184.0.34                              Unused    Unused   1    0    0      Not In DNS; Unreachable
188.184.0.35  chrom_dhcp.chromarty.com    Server    M-DHCP   1    0    0      Not In DNS; Unreachable
188.184.0.36  bootp_ross.chromarty.com    Server    M-Bootp  1    0    0      Not In DNS; Unreachable
188.184.0.37  rtp000003rts.chromarty.com  Router    A-Bootp  1    0    0      Not In DNS; Unreachable
188.184.0.38                              Unused    Unused   1    0    0      Not In DNS; Unreachable
188.184.0.39                              Unused    Unused   1    0    0      Not In DNS; Unreachable
188.184.0.40                              Unused    Unused   1    0    0      Not In DNS; Unreachable
188.184.0.41                              Unused    Unused   1    0    0      Not In DNS; Unreachable
188.184.0.42                              Unused    Unused   1    0    0      Not In DNS; Unreachable
188.184.0.43                              Unused    Unused   1    0    0      Not In DNS; Unreachable
188.184.0.44                              Unused    Unused   1    0    0      Not In DNS; Unreachable
188.184.0.45                              Unused    Unused   1    0    0      Not In DNS; Unreachable
188.184.0.46                              Unused    Unused   1    0    0      Not In DNS; Unreachable

   <<<<< AUTOMATIC RECLAIM REPORT >>>>>
   <<<<< Please Note: >>>>>
Scheduled Reclaim Process Completed.

Report Date:  02/20/2002 17:30 Start Date:  02/18/2002 23:19
Collection Frequency: Collect: Every Day At (17:30 ) Total: 2 Days
SUBNET: 188.184.0.32
```

Abort a scheduled reclaim

Purpose

Use this procedure to abort reclaims scheduled in the future or in progress.

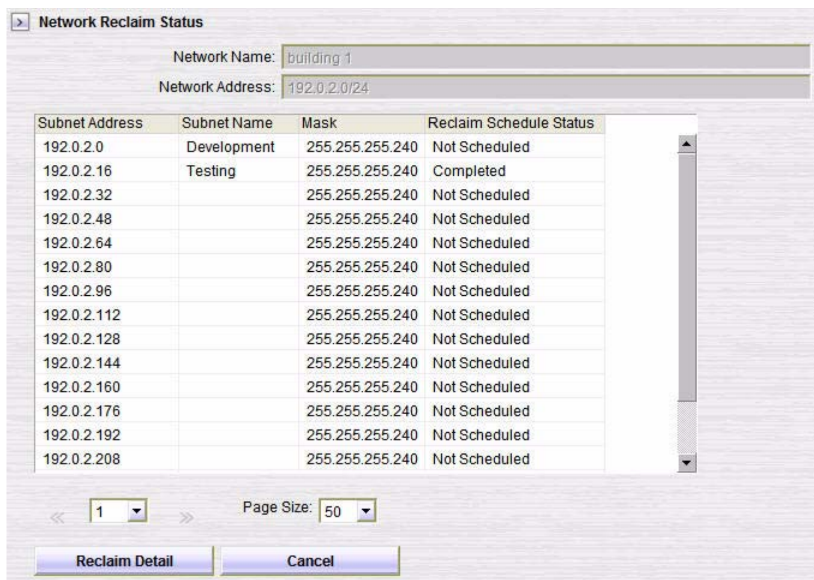
Before you begin

- A scheduled reclaim can be cancelled at any time. If a scheduled reclaim is in the middle of collecting statistic, the reclaim will complete before it is aborted.
- A scheduled reclaim that is scheduled in the future can also be aborted purged by changing the **Data Collection(Ping) Schedule** parameter set to **None**. Refer to Table 9-6, “Schedule reclaim parameters” (p. 9-96) for more information on the parameter.

Procedure

To abort a scheduled reclaim, follow these steps:

1 Chose one of the following actions.

<table>
<tr><th>If you want to …</th><th>Then…</th></tr>
<tr><td>Abort a subnet reclaim through the network level</td><td>
1. Mouse over Address Management and click IPv4.
Result: The IPv4 Hierarchy opens.
2. From the Actions menu, select View Networks.
Result: The IPv4 Hierarchy changes to a newtork view.
3. Expand Networks and select the network whose address you want to reclaim.
Result: The Network Properties page opens.
4. Click Reclaim Detail. The Network Reclaim Status displays.


Result: The following Reclaim Schedule Statuses for each subnet in the network:
• Not Scheduled - subnet is currently not scheduled for reclaim.
• In Progress - subnet reclaim has been scheduled and is in currently in the process of being reclaimed.
• Completed - the reclaim process has finished.
5. Click a subnet you want to schedule for a reclaim.
</td></tr>
</table>

If you want to ...	Then...
Abort a reclaim through the subnet level	1. Mouse over **Address Management** and click **IPv4**. **Result:** The IPv4 Hierarchy opens. 2. From the **Actions** menu, select **View Subnets**. **Result:** The IPv4 Hierarchy changes to a subnet view. 3. Expand hierarchy until you reach the desired subnet. 4. Select the subnet. **Result:** The Subnet Properties page opens.

2 Click **Reclaim Detail**.

Result: The Reclaim IP Addresses window opens. The status of the reclaim is displayed below the subnet's IP address.

3 Filter the IP addresses scheduled to be reclaimed. The following table describes the filter options.

Table 9-9 Schedule reclaim fields

Field	Description
Object Class	Filters the list by class of objects. Select one of the following: • **All** • **Bridge** • **External** • **Gateway** • **Legacy_System** • **Others** • **Partially_Managed** • **PC** • **Printer** • **Router** • **Server** • **Switch** • **Terminal_Server** • **Test_Equipment** • **Undefined** • **Wiring_HUB** • **Workstation** • **X-terminal**
Reclaim Action	Filter the list by reclaim action. Select one of the following: • **All** • **Allowed** • **Not Allowed** • **Advised**

4 Click **Abort Reclaim.**

Result: A dialog box opens with the message **Scheduled Reclaim will be aborted and the subnet will be reset to 'Not Scheduled'?**

5 Click **OK**.

Result: The scheduled reclaim is aborted and the scheduled reclaim status is reset to "Not Scheduled". When the subnet's reclaim status is Completed, the **Abort Reclaim** button is replaced with **Purge Reclaim** button. Clicking on **Purge Reclaim** resets the reclaim statistics and sets the reclaim status to "Not Scheduled".

END OF STEPS

Purge scheduled reclaim information

Purpose

Use this procedure to purge scheduled reclaim information on a specific subnet from the database.

Before you begin

Scheduled reclaim information can only be purged when the status is "Completed".

Procedure

To purge reclaim information from the database, follow these steps:

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 From the **Actions** menu, select **View Subnets**.

Result: The Subnets node opens.

3 Expand the Subnets node.

4 Select the desired subnet.

Result: The Subnet Properties page opens.

5 Click **Reclaim Detail**.

Result: The Reclaim IP Addresses window opens. The status of the reclaim is displayed below the subnet's IP address.

6 Filter the IP addresses scheduled to be reclaimed. The following table describes the filter options.

Table 9-10 Schedule reclaim fields

Field	Description
Object Class	Filters the list by class of objects. Select one of the following: • **All** • **Workstation** • **X-terminal** • **PC** • **Printer** • **Server** • **Wiring_HUB** • **Router** • **Bridge** • **Terminal_Server** • **Switch** • **Legacy_System** • **Gateway** • **Test_Equipment** • **Undefined** • **Others** • **Partially_Managed** • **Workstation**
Reclaim Action	Filter the list by reclaim action. Select one of the following: • **All** • **Allowed** • **Not Allowed** • **Advised**

7 Click **Purge Reclaim**.

Result: A dialog box opens with the message **Scheduled Reclaim will be cleaned out of the database and the subnet will be reset to 'Not Scheduled'. Are you sure?**

8 Click **OK**.

Result: The scheduled reclaim information is purged and the scheduled reclaim status is reset to "Not Scheduled".

END OF STEPS

10 IPv4 object management

Overview

Purpose

This chapter describes the functions used to manage IPv4 objects.

Contents

This chapter covers these topics.

Object management

Overview

Purpose

The object profile is available within the Address Management function. The object profile allows you to add data to an object beyond what is available when you use the Quick Add function.

You access the object profile by selecting a subnet in the hierarchy page (in either IPv4 or IPv6), which displays the Subnet Properties page where you can access objects and their profiles in the subnet. This section describes the functions available to you within the object profile.

Manage objects

Purpose

Use this procedure to view, modify and add objects within the subnet.

Before you begin

VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and you cannot add or modify the profile. You can finetune this feature by enabling or disabling Validate CNAME Records sub-policies in Global Policies. When set to True, these sub-policies allow validation checks to be made against the following whenever you add or modify an object:

- Object aliases
- Object resource records
- Domain resource records
- Reverse zone resource records

Procedure

To access the Manage Objects function, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over **Actions** and select **Network**.

Result: The IPv4 Hierarchy changes to a network view.

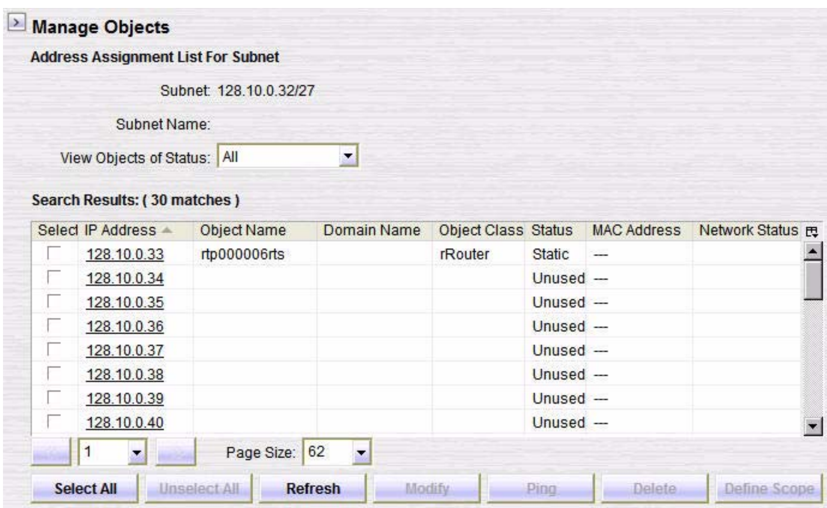
3 Expand the list of networks until you come to the subnet you want.

4 Click the subnet.

Result: The Subnet Properties page opens.

5 Click **Manage Objects**.

Result: The Manage Objects page opens.



The top of this page displays the subnet address and subnet name (if one has been assigned). The remaining fields are described in the following table.

Table 10-1 Address assignment list fields

Field	Description
View Objects of Status	This drop-down list limits the address list to objects with the status you select, as follows. • All • Scheduled Move • Unused • Used • Static • Dynamic • Reserved • Manual Bootp • Automatic Bootp • Manual DHCP • Automatic DHCP • Dynamic DHCP Select a status and click **Refresh** to see the updated list.
Select	This checkbox allows you to select one or more objects in the list to be deleted. After you have selected the objects, you can click **Delete Selected** to delete them.
IP Address	This field contains the IP address of the object. Click on this address to see the object profile for the object.
Object Name	This field contains the name of the object assigned to it when it was created. You can change this name if you modify this object's profile. This field can contain up to 63 characters. The first and last characters of this field must be alphanumeric.
Object Class	This field contains the class of the object assigned when it was created. You can change this class if you modify this object's profile.
Status	This field contains the status of the object assigned to it when it was created. You can change this status if you view this object's profile. The status is "Unused" if no object is created for this IP address yet.
Domain Name	This field contains the domain name of the object assigned to it when it was created. You can change this domain name if you modify this object's profile.

6 You can choose the following actions.

If you want to...	**Refer to...**
Select one or more obectss	You can: • Select one or more objects by clicking the checkbox in the **Select** column • Select more than one object by clicking holding the **Shift** key and clicking on one or more object rows
Select all objects in the **Search Results** list	Click **Select All**. **Result:** All objects are selected.
Unselect all objects in the **Search Results** list	Click **Unselect All**. **Result:** Selected objects are unselected.
Refresh the **Search Results** list	Click **Refresh**. **Result:** The **Search Results** list is updated.
Modify one object	In the **IP Address** column, click on a used object. **Result:** The Modify Object Profile page opens. Refer to "Modify an object" (p. 10-15) for more information.
Modify more than one object	1. Select one or more used IP addresses. **Result:** The **Modify** button is enabled. 2. Click **Modify**. **Result:** The Modify Object Properties page opens. Refer to "Modify multiple object properties" (p. 10-16) for more information.
Delete one or more objects	1. Select one or more used IP addresses. **Result:** The **Delete** button is enabled. 2. Click **Delete**. **Result:** Refer to "Delete an object" (p. 10-20) for more information.
Ping one or more objects	1. Select one or more IP addresses. **Result:** The Ping button is enabled. 2. Click **Ping**. **Result:** The results of the ping are displayed in the **Network Status** column. Refer to "Ping an object" (p. 10-21) for more information.
Add a object	Click on an unused IP address. **Result:** The Add Object Profile page opens. Refer to "Add an object" (p. 10-12) for more information.

If you want to...	Refer to...
Define a scope for an object	1. Select an IP address. 2. Click **Define Scope**. **Result:** The Define Scope/Range page opens. Refer to "Define a scope" (p. 10-22) for more information.

END OF STEPS

Search for an object in a subnet

Purpose

Use this procedure to search for a specific object in a subnet.

Procedure

To search for a specific object, follow these steps.

1. Mouse over **Address Management** and click **IPv4**.

   Result: The IPv4 Hierarchy opens.

2. Mouse over **Actions** and select **View Networks**.

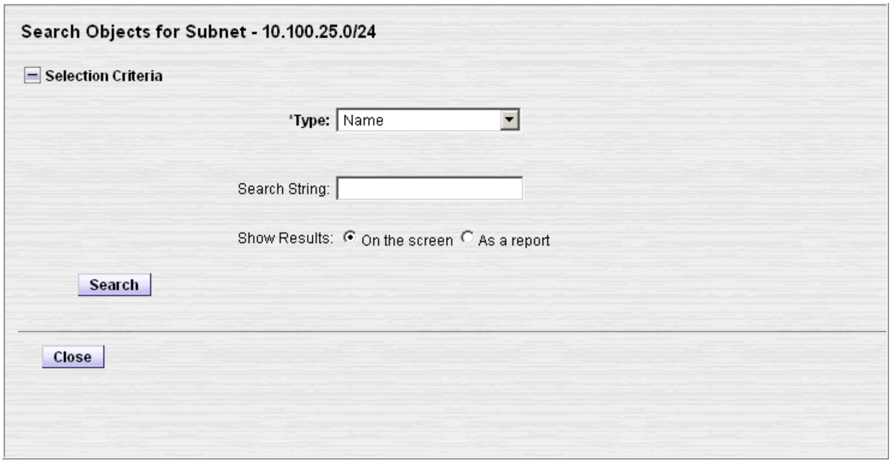
3. Expand the list of networks until you come to the subnet you want.

4. Click the subnet.

   Result: The Subnet Properties page opens.

5. Click **Search Object**.

Result: The Search Objects for Subnet page opens.



6 Choose one of the following actions.

If you want to search by…	Then…
Name	1. In the **Type** field, select **Name**. 2. In the **Search String** field, enter freeform text. You may use the wildcard character (*) for 0 or more characters.
Address	1. In the **Type** field, select **Address**. 2. In the **Search String** field, enter a valid IP address. If you enter an invalid IP address, you receive an error message.
MAC Address	1. In the **Type** field, select **MAC Address**. 2. In the **Search String** field, enter a 12 or 16 hexadecimal character MAC Address. If you use colon separators, the entire MAC address must have colons separating each two hexadecimal characters. If you enter an invalid MAC address, you receive an error message.
User Defined Fields	1. In the **Type** field, select **User Defined Fields**. 2. In the **UDF Field Name** field, select **All** or a specific UDF from the list. 3. In the **Search String** field, enter freeform text. You may use the wildcard character (*) for 0 or more characters.
User Defined Attributes	1. In the **Type** field, select **User Defined Attributes**. 2. Click **Add New Criteria**. 3. In the **Attribute Group** field, select an attribute group. 4. In the **Attribute Name** field, select an attribute. 5. In the **Attribute Value** field, enter a value. 6. Repeat Step 2 to Step 5 as needed. You can enter up to five criteria.

7 Choose one of the **Show Results** options.

If you want to...	Then ...
Review search results on the screen	Click **On the screen**.
Review search results as a report	1. Click **As a report**. **Result:** The **Report Format** and **Run** fields open. 2. Select **html** to produce an HTML report, or select **pdf** to produce a report in PDF format. 3. Choose one of the following **Run** options. a. To run the report immediately, select In **Foreground**. b. To run the report in background, select **In Background**. For information on running a report in background, refer to "Run the job in background" (p. 9-78). c. To run the report at a later time, select **Scheduled At**. For information on running a report at a later time, refer to "Schedule the job for a later time" (p. 9-79).

8 After entering values in the fields on the Search Objects for Subnet page, click **Search**.

Result: A list of IP addresses that match the search criteria opens.

9 Click the IP Address of the object whose object profile you want to view. The Modify Object Profile page opens. For detailed information on modifying the object profile, refer to "Modify an object" (p. 10-15).

END OF STEPS

Add an object to the next available address in a subnet

Purpose

Use this procedure to assign an object, such as a workstation or router, to the next available IP address in a subnet.

Procedure

To use the Add Next Object function, follow these steps.

1 Mouse over **Address Management** and click **IPv4**.

Result: The IPv4 Hierarchy opens.

2 Mouse over **Actions** and select **Network**.

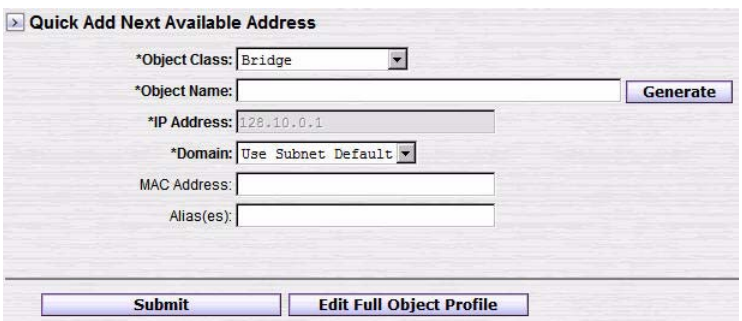
Result: The IPv4 Hierarchy changes to the network view.

3 Expand the list of networks until you come to the subnet you want.

4 Click the subnet.

Result: The Subnet Properties page opens.

5 Click **Add Next Object**. The Quick Add Next Available Address page opens. The IP address is initially filled-in and is not editable.



6 Enter an object name or click **Generate** to fill in the **Object Name** field automatically.

7 Refer to Table 9-1, "Quick Add fields" (p. 9-13) for detailed information on the fields on this page.

8 Choose one of the following actions.

If you want to...	Then...
Add the object without editing it	1. Click **Submit**. **Result:** The object is added and a confirmation dialog opens with the message **Object added:<objectname> - <ipaddress>**. 2. Click **OK** to close the dialog box.
Add the object and edit its profile	1. Click **Edit Full Object Profile**. **Result:** The object is added and a confirmation dialog opens with the message **Object added:<objectname> - <ipaddress>**. 2. Click **OK** to close the dialog box. **Result:** The object profile opens. 3. Edit the object profile, as described in "Object profile" (p. 10-36).

END OF STEPS

Add an object

Purpose

Use this procedure to add an object.

Before you begin

- When you define objects for a subnet, it is best to define the Wiring HUB and its slots/ports first. This enables you to connect objects in this subnet to a specific slot/port number. (If objects are not required to be connected to a specific slot/port, however, there is no need to define the Wiring_HUB first.)
- You cannot modify an object if its MAC address is already defined in another object in the same subnet.
- VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and you cannot add or modify the profile. You can finetune this feature by enabling or disabling Validate CNAME Records sub-policies in Global Policies. When set to True, these sub-policies allow validation checks to be made against the following whenever you add or modify an object:
  - Object aliases

- Object resource records
- Domain resource records
- Reverse zone resource records

- Do not add more objects to a network than your license allows. If you do add more objects than your license allows, you will be locked out of VitalQIP. If you are locked out of VitalQIP and have exceeded the number of IPs covered by your current license, contact your sales representative to obtain a temporary license for a larger number of objects so that you can access the GUI and delete excess objects.
- To check the number of objects covered by your license and how many objects already exist, select **Help | About VitalQIP**.
- Additional steps are required if you wish to use “null” as a static object name. You need to create an A record with the Resource Record function on either the “null” object profile, as described in “Manage object resource records” (p. 10-29), or on the Zone Properties page where it is located, as described in “Add/modify zone resource records” (p. 14-18). Alternatively, use a zone extension to add the A record, as described in “Set zone options” (p. 14-24).

Procedure

To add an object, follow these steps.

1 Expand the list of networks until you come to the subnet you want, or mouse over the **Actions** menu and select **View Subnets**.

2 Select the subnet where you want to add an object.

Result: The Subnet Properties page opens.

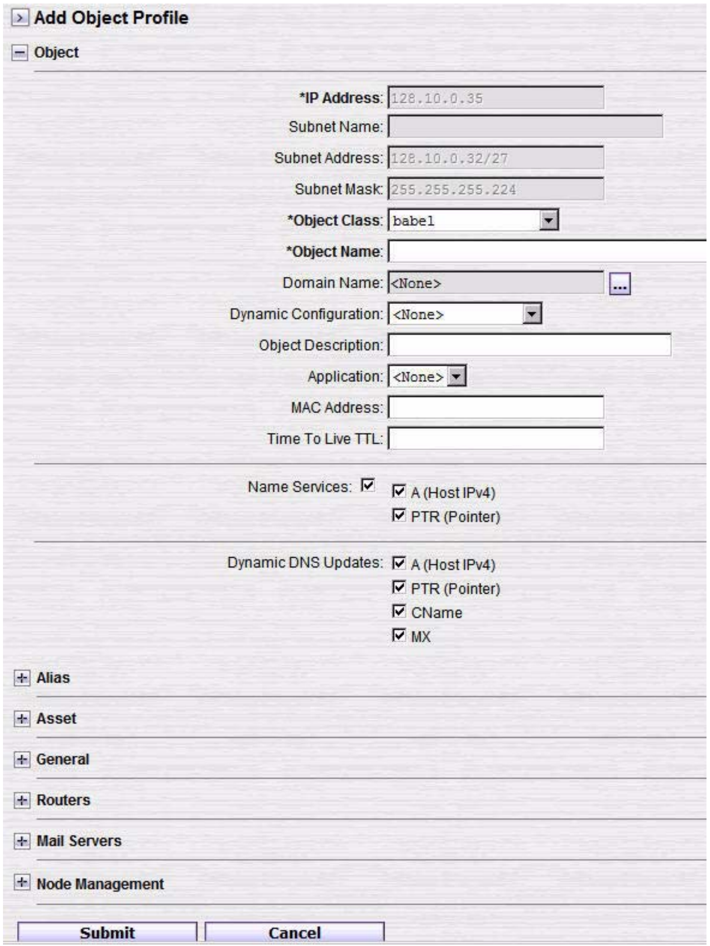
3 Click **Manage Objects**.

Result: The Manage Objects page opens.

4 In the **IP Address** column, double-click the IP address.

Result: The Add Object Profile page opens.

5 Enter the appropriate information in the fields, as described in Table 10-6, "Object fields" (p. 10-38).



6 Click **Submit**.

Result: A dialog message opens.

7 Click **OK**.

END OF STEPS

Modify an object

Purpose

Use this procedure to modify an object.

Before you begin

- You cannot modify an object if its MAC address is already defined in another object in the same subnet.
- Only objects with a status of "Used" can be modified.

Procedure

To modify an object, follow these steps.

1 Expand the list of networks until you come to the subnet you want, or mouse over the **Actions** menu and select **View Subnets**.

2 Select the subnet where the object you want to modify is located.

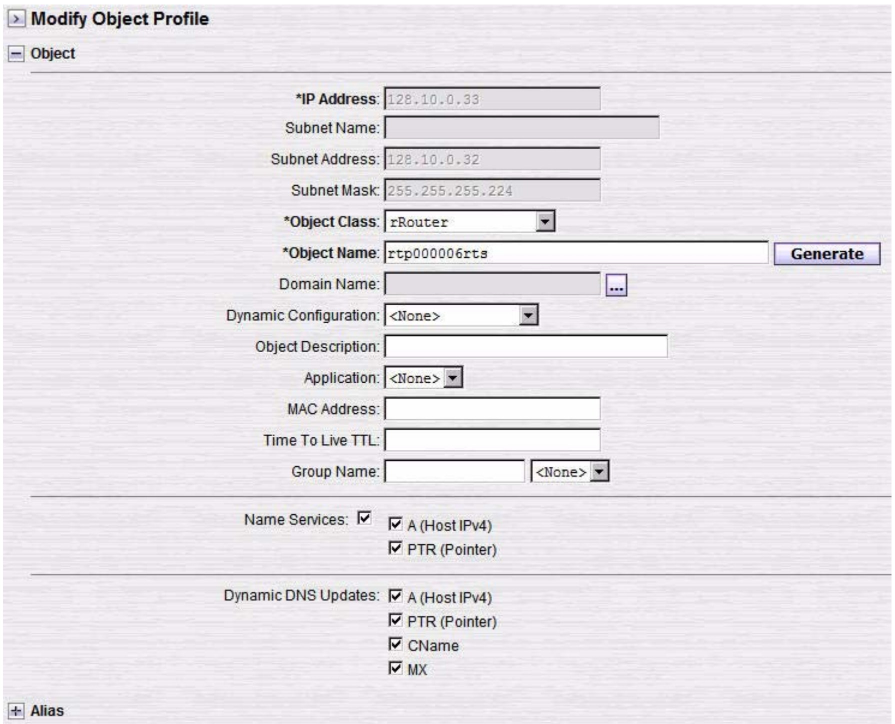
Result: The Subnet Properties page opens.

3 Click **Manage Objects**.

Result: The Manage Objects page opens.

4 In the **IP Address** column, select the IP address you want to modify.

Result: The Modify Object Profile page opens.



5 Modify fields as needed. Refer to “Object profile” (p. 10-36) for more information.

6 Click **Submit**.

Result: A message dialog opens.

7 Click **OK**.

END OF STEPS

Modify multiple object properties

Purpose

Use this procedure to modify multiple object properties at one time.

Before you begin

- When multiple objects are modified at one time, “Modify Objects” appear in the Job Scheduler searches to indicate that multiple changes are scheduled to occur to a group of objects.
- Only objects with a status of “Used” can be modified.
- Bulk modify operation for user defined attribute updates only update those user specified user defiend attributes that are associated with the entity (Subnet, Zone, Object) at the time of job execution, and no warning messages are displayed.

Procedure

To modify multiple object properties at one time, follow these steps.

1 Expand the list of networks until you come to the subnet you want.

2 Click the subnet.

Result: The Subnet Properties page opens.

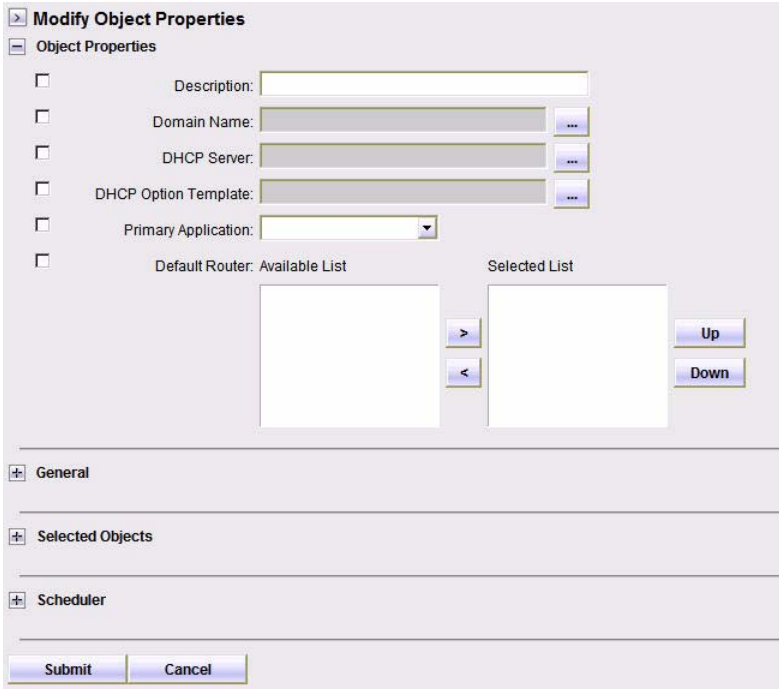
3 Click **Manage Objects**.

Result: The Manage Objects page opens.

4 In the **Select** column, place a check next to one or more objects you want to modify.

5 Click **Modify**.

Result: The Modify Object Properties page opens.



Object Properties section

6 If not expanded, expand the **Object Properties** section.

7 Check the fields you want to modify and enter information as needed, as described in the following table.

Table 10-2 Object Properties fields

Field	Description
Description	Enter a text description of the objects.
Domain Name	Domain name for the objects. Click ... to open the Domain Search window and enter search criteria so you can pick a domain from the **Search Results** list.
DHCP Server	DHCP server name for the objects. Click ... to open the DHCP Server Search window and enter search criteria so you can pick a server from the **Search Results** list.

Field	Description
DHCP Option Template	DHCP option template for the objects. Click ... to open the DHCP Option Template Search window and enter search criteria so you can pick a template from the **Search Results** list.
Primary Application	Primary application assigned to the objects. Applications can be defined in the VitalQIP thick client.
Default Router	Default router for the objects. To add or remove a router, follow these steps. 1. Select a router IP address from the **Available List** and click > to add the selected router to the **Selected List**. Use **Up** and **Down** to order the routers. 2. To remove a router from the **Selected List**, highlight the router and click <.

Other sections

8 Choose one of the following.

If you are...	Then...
Modifying the **General** section	Refer to "Assign location and contact information to an object" (p. 10-45) for more information on the fields.
Viewing object being modified	If needed, expand **Selected Objects** section.
Modifying user defined attributes	Refer to "Use user defined attributes as search criteria" (p. 7-26) for more information.
Modifying user defined fieds	Refer to "Use user defined fields as search criteria" (p. 7-25) for more information.
Modify the **Scheduler** section	Refer to "Scheduler" (p. 9-77) for more information.

9 Click **Submit**.

Result: A message dialog opens.

10 Click **OK**.

END OF STEPS

Delete an object

Purpose

Use this procedure to delete one or more objects.

Before you begin

- Only objects with a status of “Used” can be deleted.

Procedure

To delete one or more objects, follow these steps.

1. Select **IPv4** from the **Address Management** menu.

   Result: The IPv4 Hierarchy opens.

2. Mouse over **Actions** and select **Network**.

   Result: The IPv4 Hierarchy changes to a network view.

3. Expand the list of networks until you come to the subnet you want.

4. Click the subnet.

   Result: The Subnet Properties page opens.

5. Click **Manage Objects**.

   Result: The Manage Objects page opens.

6. In the **Select** column, place a check next to the object or objects you want to delete.

7. Click **Delete**.

   Result: A message dialog opens that asks if you want to delete the object.

8 Click **OK**.

Result: The object is deleted.

END OF STEPS

Ping an object

Purpose

Use this procedure to ping one or more objects.

Procedure

To ping one or more objects, follow these steps.

1 Select **IPv4** from the **Address Management** menu.

Result: The IPv4 Hierarchy opens.

2 Mouse over **Actions** and select **Network**.

Result: The IPv4 Hierarchy changes to a network view.

3 Expand the list of networks until you come to the subnet you want.

4 Click the subnet.

Result: The Subnet Properties page opens.

5 Click **Manage Objects**.

Result: The Manage Objects page opens.

6 In the **Select** column, place a check next to object or objects you want to ping.

7 Click **Ping**.

Result: A progress bar appears that shows the progress of the ping operation. After a few moments, the result of the ping operation is displayed in the **Network Status** column.

END OF STEPS

Define a scope

Purpose

Use this procedure to define a scope.

Before you begin

- Multiple managed ranges may be specified but only one address type (Static, Dynamic, or Reserved) is allowed per scope.
- All IP addresses to be included in the scope must be unused. The scope is not created if any IP address in the range is already used, or overlaps with another range.
- A selected subnet should be associated with at least one domain.
- To define a scope, an administrator needs to have permission for the network and subnet.

Procedure

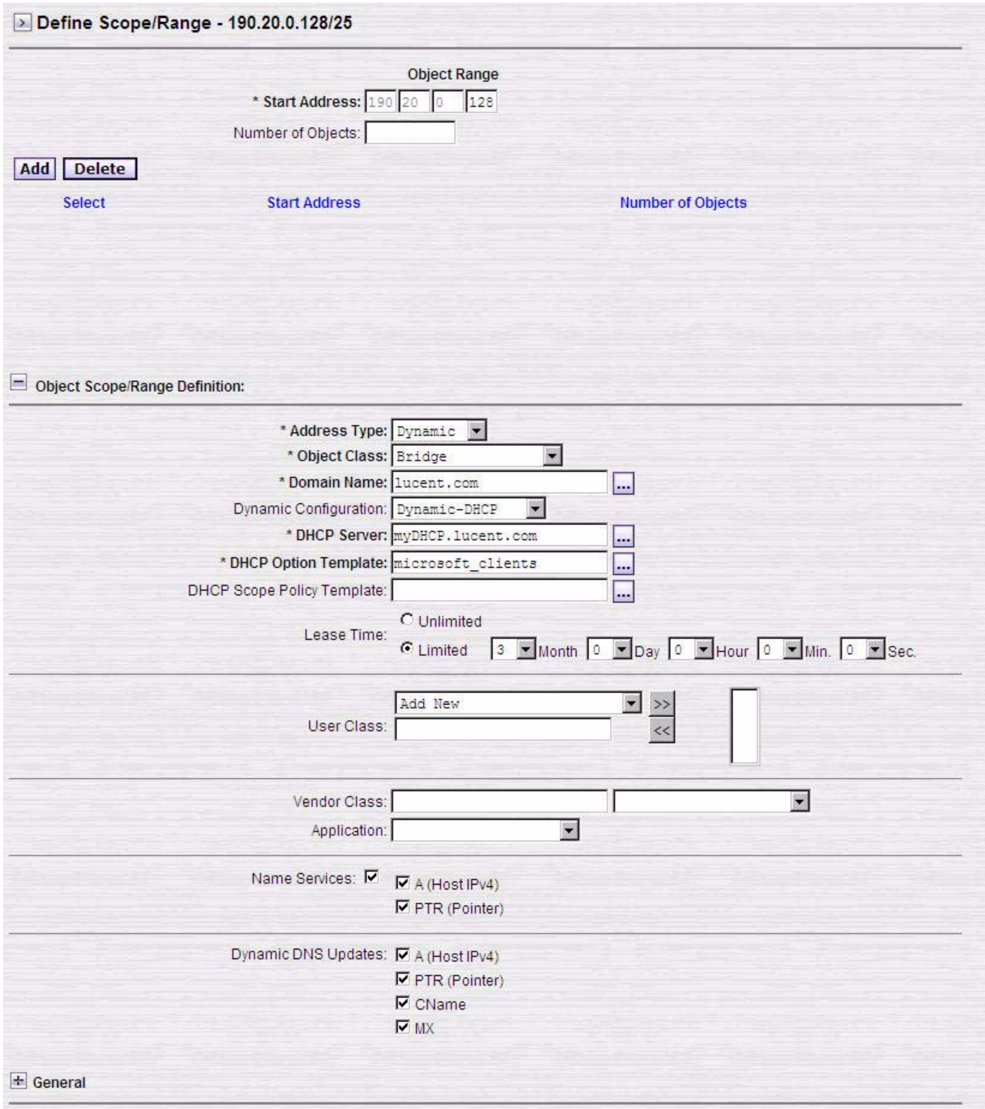
To define a scope, follow these steps.

1 Do one of the following.

From…	**Then…**
Manage Objects page	1. Select **IPv4** from the **Address Management** menu. **Result:** The IPv4 Hierarchy opens. 2. Mouse over **Actions** and select **Network**. **Result:** The IPv4 Hierarchy changes to a network view. 3. Expand the list of networks until you come to the subnet you want. 4. Click the subnet. **Result:** The Subnet Properties page opens. 5. Click **Manage Objects**. **Result:** The Managed Objects page opens. 6. In the **Select** column, check the object.
Subnet Properties page	1. Select **IPv4** from the **Address Management** menu. **Result:** The IPv4 Hierarchy opens in the Network view. 2. Mouse over the **Actions** menu and select **View Subnets**. **Result:** The Subnets view opens. 3. Expand the Subnets view and click the subnet whose properties you want to view. **Result:** The Subnet Properties page opens.

2 Click **Define Scope**.

Result: The Define Scope/Range page opens.



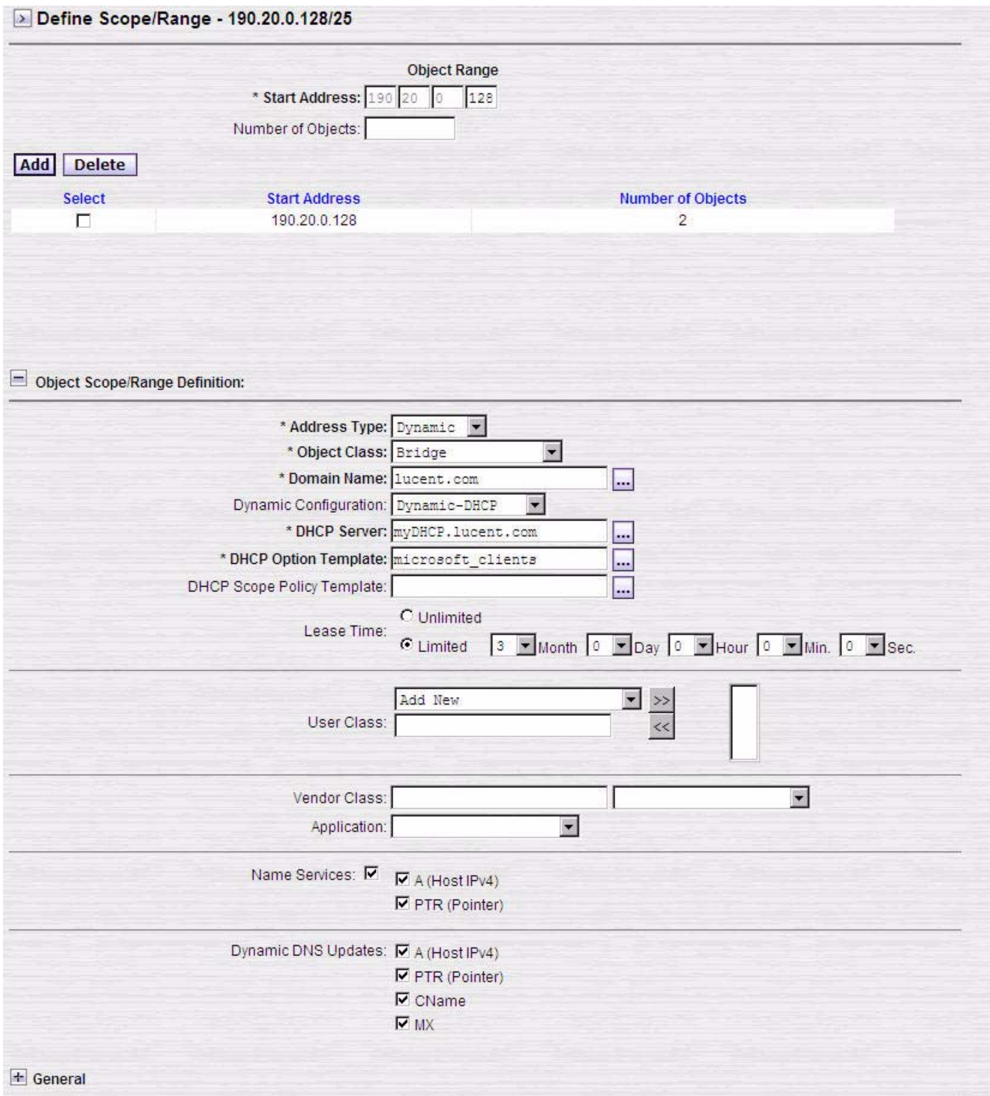
3 ***Required***. In the **Start Address** field, enter an unused start address for the scope. The default value is the subnet address, so this must be changed. VitalQIP checks the following when the scope is created:

- The start address is not the same as the subnet address
- The start address is smaller than the maximum IP address allowed on the subnet
- There is no overlap if multiple ranges are specified
- Addresses in the specified ranges do not already exist in the database.

4 In the **Number of Objects** field, enter the number of objects to be added to the scope. The default is blank.

5 Click **Add**.

Result: The scope appears in the scope list.



6 If required, add more scopes of the same address type and object class and click **Add**.

Result: The scopes are added to the scope list.

If you need to remove scopes from the list, check the **Select** check box beside the scopes you wish to remove and click **Delete**.

Result: The scopes are removed from the scope list.

7 When you have finished adding scopes to the scope list, define the scopes in the **Object Scope/Range Definition** section, as described in the following table.

Table 10-3 Object Scope/Range Definition fields

Field	Description
Address Type	***Required***. Select the type of address to be defined in the scope. The options are: • Static • Dynamic • Reserved The default is Dynamic.
Object Class	***Required.*** Select an object class from the drop-down list. The list includes Workstation, X-Terminal, PC, Printer, Server, Wiring_HUB, Router, Bridge, Terminal_Server, Switch, Legacy_System, Gateway, Test_Equipment, Undefined, Others, and Partially_Managed. The default is Workstation.
Domain Name	***Required***. Enter the domain that is associated with the subnet. To search for domains associated with the subnet, follow these steps, 1. Click [...]. **Result:** The Domain Search dialog box opens. In the **Domain Name** field, enter the first few letters of the domain name and use the wildcard (*) as needed, or leave the field blank to return all domains in the subnet. 2. Click **Search**. **Result:** The results appear in the **Search Results** list. 3. Highlight the domain you want to associate with the scope. 4. Click **Select**. **Result:** The Domain Search dialog box closes and the domain you selected appears in the **Domain Name** field.

Field	**Description**
Dynamic Configuration	Select a configuration method for the object: • **<None>** - Allocates this address without using the Bootp or DHCP protocol. • **Manual-Bootp** - Allocates the address using the Bootp protocol where the MAC address is defined. • **Automatic-Bootp** - Allocates the address using the Bootp protocol where the MAC address is not known. • **Automatic-DHCP** - Allocates the address using the DHCP protocol, from a DHCP template with an infinite lease. • **Dynamic-DHCP** - Defines the address using the DHCP protocol, from a DHCP template for a specific lease time. • **Manual-DHCP** - Allocates this address using the DHCP protocol where the MAC address is defined.
DHCP Server	***Required if Address Type is Dynamic***. Select a DHCP Server to be used for dynamic scopes from the drop-down list. The default is the first DHCP Server in the alphabetized list.
DHCP Option Template	***Required if Address Type is Dynamic***. Select a DHCP option template to be associated with this scope of addresses from the drop-down list. The default is the first DHCP option template in the alphabetized list.
DHCP Scope Policy Template	Select a DHCP scope policy template to be associated with this scope of addresses. The default is blank.
Lease Time	Displays the lease time of dynamic objects. This value is derived from the DHCP Server Profile. The default is typically set to 776000 seconds (or 3 months). Possible values are -1 for an infinite lease, or between 3600 and 2147483647.
User Class	Select a User Class to be associated with this scope of addresses from the drop-down list and click >>. You can add a new User Class, as follows: 1. Select **Add New**. 1. Enter an alphanumeric user class name in the **User Class** field. 2. Click >> to associate the User Class with the addresses. **Note:** You can also create a user class in the DHCP Client Class Hierarchy. Refer to “Add a User Class” (p. 21-17).
Vendor Class	The Vendor Class allows you to define specific categories of vendor options; for example, you could assign a Vendor Class to an object assigned to a contractor that would specify a shorter lease time. Select a Vendor Class from the **Vendor Class** drop-down list or enter a new vendor class of up to 16 alphanumeric characters. **Note:** You can also create a vendor class in the DHCP Client Class Hierarchy. Refer to “Add a Vendor Class” (p. 21-20).

Field	Description
Application	Select the application to be associated with the scope.
Name Services	Defines which Resource Records are written to the DNS server. These options are defaulted via the definition in the Dynamic DNS global policies (Static DNS Mask and Dynamic DNS Mask), but can be overridden by the **Name Services** check boxes that you select here. When a push occurs (Network Services function), the values that are checked are written to the server. You can check either or both of the following values, or you can leave both blank: • **A (Host IPV4)** • **PTR (Pointer)**
Dynamic DNS Updates	Select the type of records you want dynamically updated when this object is created or deleted. These options are set as defaults via the definition in the Dynamic DNS global policies (Static DNS Mask and Dynamic DNS Mask), but can be overridden by the Dynamic DNS Updates check boxes that you select here. You can check any combination of the following values, or you can leave them all blank: • **A (Host IPV4)** • **PTR (Pointer)** • **CNAME** • **MX**

8 Click **Submit**.

Result: A confirmation dialog box opens with the message **Define Scope/Range was Successful!**

Note: If the **Check Before Assign** field (in Subnet Properties) was set to **Ping**, the message reads **Define Scope/Range was Successful! Note: The objects were however not pinged prior to creation.**

9 Click **OK**.

Result: The dialog box closes and the Subnet Properties page opens.

10 Use the Manage Objects function to manage the scope further. Refer to “Manage objects” (p. 10-3) and “Enter object information” (p. 10-37).

END OF STEPS

Manage object resource records

Purpose

This function allows you to create, and modify Resource Records for an object. This option allows Resource Records for an object to be written to the configuration file. VitalQIP validates and formats the information on input.

Before you begin

- The **Resource Records** function is only available if the administrator has the **Create Resource Record** privilege set to True.
- VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and you cannot add or modify the profile. You can finetune this feature by enabling or disabling Validate CNAME Records sub-policies in Global Policies. When set to True, these sub-policies allow validation checks to be made against the following whenever you add or modify an object:
  - Object aliases
  - Object resource records
  - Domain resource records
  - Reverse zone resource records
  - ENUM NAPTR resource records

Procedure

To add or modify a resource record, use the following steps:

1 Select **IPv4** from the **Address Management** menu.

Result: The IPv4 Hierarchy page opens.

2 Mouse over the **Actions** menu and select **View Subnets**.

3 Expand the list of subnets and select the subnet containing the object resource record you want to manage.

Result: The Subnet Properties page opens.

4 Click **Manage Objects**.

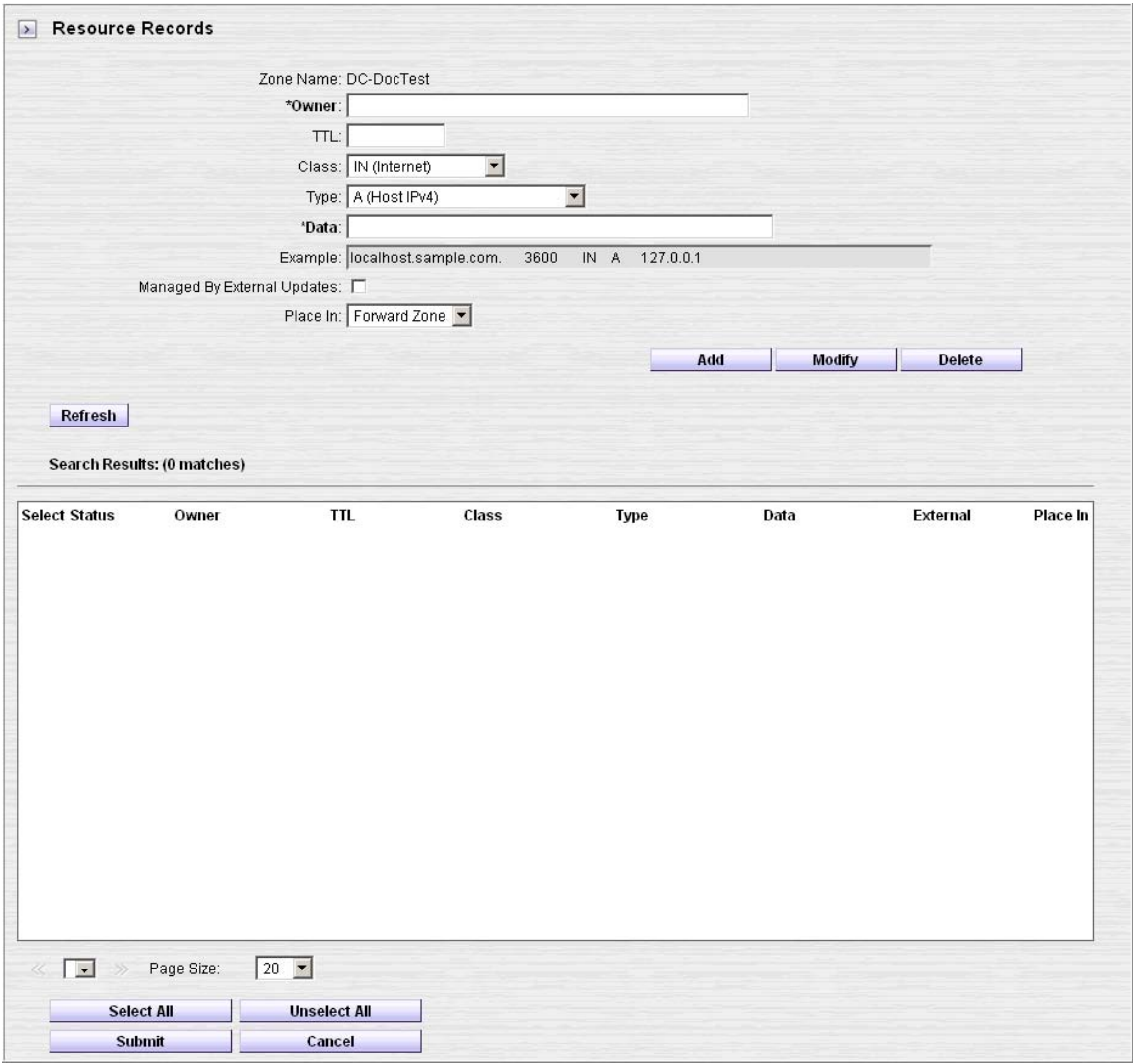
Result: The Manage Objects page opens.

5 Select the object that contains the resource record you want to manage and click **Modify**.

Result: The Modify Object Profile page opens.

6 Click **Resource Records**.

Result: The Resource Records page opens.



- To add a resource record, enter values in the fields, as described in the following table, and click **Add**.
- To modify a resource record, select it from the **Search Results** list and click **Modify**. Its values are displayed in the fields at the top of the page and you can then change them.
- To delete one or more resource records, check the **Select Status** check box beside the resource records you want to delete from the **Search Results** list and click **Delete**. The Status for each selected resource record changes to **Delete**.

Table 10-4 Resource Records tab fields

Field	Description
Owner	Enter whatever name you are using to define the owner for this resource record.
TTL (Time To Live)	The length of time (in seconds) the name server will hold this information. If no TTL is defined, the value is inherited from the zone.
Class	Resource Records are divided into classes. Each class of records pertains to a type of network or software. Select from the drop down listing of default Classes, Default classes are as follows: • IN (Internet) • CS (CSNet Class) • CH (Chaos Class) • HS (Hesiod Class).
Type	Select a Resource Record from the drop-down list, or select **Custom** and enter your own type. The settings for the different resource record types are described in Table 10-5, "Type field values" (p. 10-32). For additional information, refer to *DNS and BIND*, by Cricket Liu and Paul Albitz.
Data	Enter the data associated with the specific resource record type. To assist you, a sample record in the **Example** field displays the required format.
Managed by External Updates	The **Managed by External Updates** checkbox indicates that the selected Resource Record has been added by VitalQIP QIP Update Service. To make changes to a Resource Record that is managed by external updates, uncheck the **Managed by External Updates** checkbox. The **Managed by External Updates** checkbox can only be checked when the Resource Record has been added by the VitalQIP QIP Update Service or **`qip-syncexternal`** command. It is not possible to set this checkbox within the GUI. For further information on VitalQIP support for external objects, refer to "External objects and resource records support", in the *Administrator Reference Manual*.
Place In	Select where you want to place the resource records after they are generated; in the **Forward Zone** or the **Reverse Zone**.

Based on your selection in the **Type** field, enter data as described in the following table.

Table 10-5 Type field values

Type	Data entry values
A (Host IPv4)	**Address** - enter the IP address of the A record.

Type	**Data entry values**
CNAME (Canonical Name)	**Canonical Name** - enter a name that specifies the canonical or primary name for the owner.
HINFO (Host Information)	Enter the following data: **CPU** - enter the central processing unit type. **OS** - enter the operating system type.
MX (Mail Exchanger)	Enter the following data: **Preference** - enter a number, which specifies the preference given to this resource record among others at the same owner (lower values are preferred). **Exchange Name** - enter a fully qualified name, which specifies a host that acts as a mail exchange for the owner.
NAPTR	**Order** - A 16-bit unsigned integer specifying the order in which the NAPTR records must be processed to ensure the correct ordering of rules. **Preference** - A 16-bit unsigned integer that specifies the order in which NAPTR records with equal "order" values should be processed **Flags** - A ***<character-string>*** containing flags to control aspects of the rewriting and interpretation of the fields in the record. Flags are single characters from the set [A-Z 0-9]. **Service** - Specifies the service(s) available down this rewrite path. **Regular Expression** - A string containing a substitution expression that is applied to the original string held by the client to construct the next domain name to lookup. **Replacement** - The next NAME to query for NAPTR, SRV, or address records depending on the value of the flags field.
NS (Name Server)	**Name Server** - enter a fully qualified domain, which specifies a host that is authoritative for the specified class and domain.
PTR (Pointer)	**PTR Name** - enter a fully qualified name which points to some location in the domain name space.
TXT (Text)	**Text Data** - enter descriptive text for the resource record.
WKS (Well-Known Services)	**Address** - enter the 32-bit internet address. **Protocol** - this is usually UDP or TCP, although it can be any entry in the */etc/protocols* file. **Services** - enter a port number below 256. This consists of a service list below port 256 for the */etc/services* files.
AAAA (Host IPv6)	**Ipv6 Address** - enter the MAC address in the octet fields.

Type	Data entry values
AFSDB (Andrew File System Data Base)	**Sub Type** - select the Sub Type. 1 is an AFS cell database server, and 2 is a DCE authenticated name server. **Host Name** - enter the fully qualified name of the host that has a server for the cell named by the owner.
MB (Mailbox Name)	**Mailbox Name** - enter a fully qualified name, which specifies a host that has the specified mailbox.
MG (Mail Group)	**Mail Group** - enter the fully qualified name that specifies a mailbox, which is a member of the mail group specified, by the name.
MINFO (Mailbox Information)	Enter the following data: **Responsible Mailbox** - enter a fully qualified name, which specifies a mailbox that is responsible for the mailing list or mailbox. **Error Mailbox** - enter a fully qualified name, which specifies a mailbox that receives error messages related to the mailing list or mailbox specified by the owner of the MINFO Resource Record.
MR (Mail Rename)	**New Mailbox** - enter a fully qualified name, which specifies a mailbox that is the proper rename of the specified mailbox.
ISDN	Enter the following data: **ISDN Address** - enter the ISDN address, which identifies the ISDN number of owner and Direct Dial In (if any). **Subaddress** - enter a subaddress.
SRV (Server Resource Record)	Enter the following data: **Priority** - enter the priority of the host using any numbers between 0 and 65535. Clients try to contact the host with the lowest priority. **Weight** - enter a weight (any number between 0 and 65535). This field specifies a relative weight for entries with the same priority. **Port** - enter the port number (any number between 0 and 65535) of the service on the host. Target - enter a fully qualified domain name for the host supporting the service.
X25	**PSDN Address** - enter the Public Switched Data Network (PSDN), which identifies the PSDN address.
Custom	When selected, opens a data entry field where you can enter your own resource record.

7 Click **Submit**.

Result: A dialog box opens with the message **Resource records modified successfully**.

8 Click **OK**.

9 Click **Cancel**.

Result: The Modify Object Profile page opens.

10 To return to the Manage Objects page, click **Cancel** again.

END OF STEPS

Object profile

Overview

Purpose

The object profile allows you to add and modify an object's information about the object, alias, hardware information, location, and user-defined fields.

You access the object profile when you add an object from the Subnet Profile page, when you select an existing object from the Manage Objects page, and when you use the Quick Add function. Refer to "Add an object to the next available address in a subnet" (p. 10-10), "Manage objects" (p. 10-3), and "Use Quick Add" (p. 9-12) for details about these functions.

At this point, you can add or modify the fields in the Object Profile. **Cancel** exits the object profile and returns you to your prior starting point.

> **Note:** Do not click **Submit** until you have finished filling in fields in all sections of the Object Profile.

Description

The object profile is divided into the following sections:

- Object (Enter object information)
- Alias (Create an alias for an object)
- Asset (Assign asset information to an object)
- General (Assign location and contact information to an object)
- DHCP (Associate a DHCP server with an object)
- User-Defined Fields (Assign a user-defined field to an object)
- Routers (Associate a router with an object)
- Mail servers (Assign mail forwarding options to an object)
- Policies (Assign policies to an object)
- Node Management (Assign an object to a node)
- DNS View (Manage domain names in view specific zones)

> **Note:** Not all sections of the Object Profile display for all object types. Refer to each section for specific information.

Enter object information

Purpose

Use this procedure to add network information for an object in an object profile.

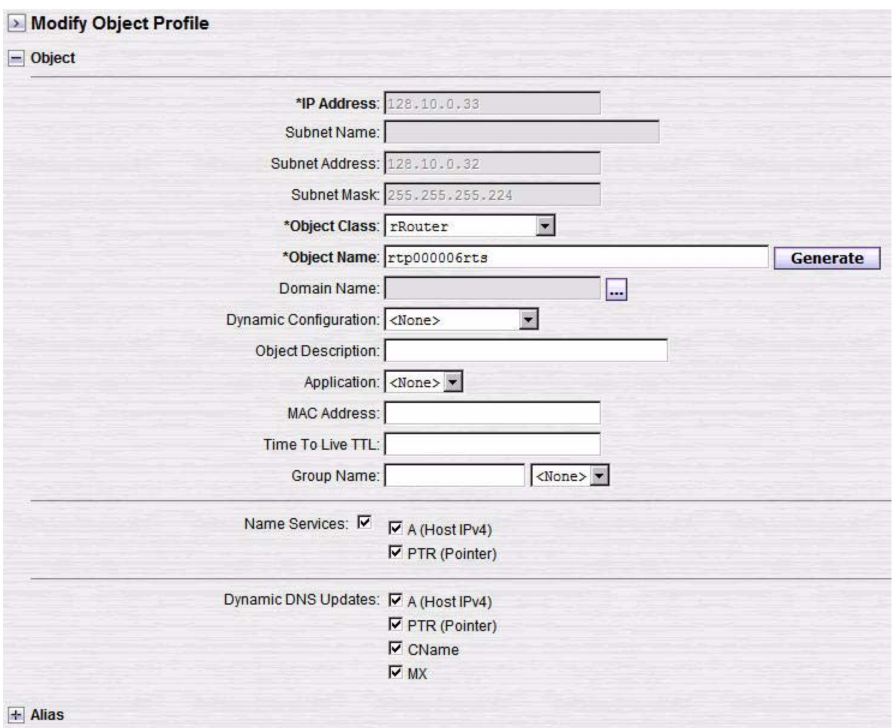
Procedure

To enter network information for an object, follow these steps.

1 Open an object profile, using any of the following methods:

- **Quick Add** > **Edit Full Object Profile**
- **Global Search**
- **Subnet Properties** > **Manage Objects**
- **Subnet Properties** > **Search Object**
- **Subnet Properties** > **Add Next Object** > **Edit Full Object Profile**

Result: The object you selected opens in the Modify Object Profile page.



2 Enter network information in the Object section fields, as described in the following table.

Table 10-6 Object fields

Field	Description
IP Address	***Read only***. This field is filled in automatically.
Subnet Name	***Read only***. Name assigned to the subnet when it was created. This field can be blank (null).
Subnet Address	***Read only***. Address of the subnet.
Subnet Mask	***Read only***. Subnet mask.

Field	Description
Object Class	***Required***. Select a value from the drop-down list. The list of values shown is delivered with VitalQIP, however this list is customizable. Therefore the list may contain additional values, or may not contain some values shown in the following list. Allowable values are as follows: • **Workstation** – defines object as a general-purpose computer used by one person at a time and offers higher performance than normally found in a personal computer. • **X-terminal** – defines object as an intelligent terminal, which operates as an X server directly connected to Ethernet. • **PC** – defines object as a personal computer. • **Printer** – defines object as a device that prints text or graphics on paper. • **Server** – defines object as a computer that provides a service(s) for other computers connected to it via a network. • **Wiring_Hub** – defines object as a hub at a point where a wiring system in a building or a room is connected to a main concentrator. • **Router** – defines object as a device in a network that handles message transfers between computers. • **Bridge** – defines object as a device that forwards traffic between network segments based on data link layer information. • **Terminal_Server** – defines object as a hardware device or server that provides terminals (PCs, printers, and so on) with a common connection point to a local or wide area network. • **Switch** – defines object as a packet or circuit switch. • **Legacy_System** – defines object as a database management system running on mainframes or minicomputers. • **Gateway** – defines object as a device that enables data to flow between different networks. • **Test_Equipment** – defines object as equipment used for testing. • **Undefined** – defines object as an unknown device. • **Others** – defines object as something other than object types listed here. • **External** – defines object as being created by dynamic DNS updates from some product to a DNS server managed by VitalQIP. • **Partially_Managed** – allows an object to be managed by VitalQIP administrators and externally modified by Windows 2000/2003 administrators.

Field	Description
Object Name	***Required***. This field can be automatically filled in by clicking **Generate** if your VitalQIP system uses Object Naming Policies. If this field is not filled in automatically, enter a name for the object (alphanumeric, maximum 32 characters; hyphens and underscores are allowed). The same name cannot be applied to more than one object unless the Unique Name Warning in the Administrator Profile is set to False. An object can never share the same name as a domain, however. **Note:** You cannot change the name of an object that is attached to a server unless you are the Master administrator, or have permissions for the server.
Domain Name	***Optional***. Defaults to the subnet default. To search for a different subnet domain, follow these steps, 1. Click . **Result:** The Domain Search dialog box opens. In the **Domain Name** field, enter the first few letters of the domain name and use the wildcard (*) as needed, or leave the field blank to return all domains in the subnet. 2. Click **Search**. **Result:** The results appear in the **Search Results** list. 3. Highlight the domain you want to associate with the scope. 4. Click **Select**. **Result:** The Domain Search dialog box closes and the domain you selected appears in the **Domain Name** field.

Field	**Description**
Dynamic Configuration	***Optional***. Allowable values are: • **None** Default. Allocates this address without using the Bootp or DHCP protocol. No Bootp or DHCP servers or files are involved. Select **None** to add Static objects. • **M-BOOTP** Manual Bootp. Allocates the address using the Bootp protocol where the MAC address is defined. This option adds the DHCP section to the page. For additional information on assigning Manual Bootp information, refer to "Set up a manual Bootp object" (p. 10-50). • **A-BOOTP** Automatic Bootp. Allocates the address using the Bootp protocol where the MAC address is not known. This option adds the DHCP section to the page. • **M-DHCP** Manual DHCP. Allocates this address using the DHCP protocol where the MAC address is defined. This option adds the DHCP section to the page. • **A-DHCP** Automatic DHCP. Allocates the address using the DHCP protocol, from a DHCP template with an infinite lease. This option adds the DHCP section to the page. • **D-DHCP** Dynamic DHCP. Defines the address using the DHCP protocol, from a DHCP template for a specific lease time. This option adds the DHCP section to the page.
Object Description	***Optional***. Enter a text description of the object.
Application	***Optional***. Defaults to None. Specify the name of the application you want to assign to the IP address or addresses. The application field associates objects with a particular application or use. Objects can then be managed by an administrator based on a defined application. Select an application from the drop-down list of existing applications (which can be defined in the VitalQIP thick client).
Mac Address	***Required*** if Dynamic Configuration is set to **M-BOOTP**. ***Optional*** otherwise. Enter a valid MAC address. This MAC address must be unique for all objects in a specific network.
Time to Live TTL	The amount of time (in seconds) this information lives on the DNS server.

Field	Description
Group Name	If the object is selected to be a "Router", you can select a Group Name this router belongs to, or enter a new router group. Using a router group allows you to group all the interfaces of a router to a single entity. (Each port on a router has a different IP address, but you can map them all to one router group.) Creating a router group creates a record in the DNS files to allow forward and reverse lookups on the router group name and associated IP addresses. **Note:** Router groups can also be used to configure multi-homed objects within VitalQIP, but the objects must be defined as routers.
Name Services	Defines which Resource Records are written to the DNS server. These options are defaulted via the definition in the Dynamic DNS global policies (Static DNS Mask and Dynamic DNS Mask), but can be overridden by the **Name Services** check boxes that you select here. When a push occurs (Network Services function), the values that are checked are written to the server. You can check either or both of the following values, or you can leave both blank: • **A (Host IPV4)** • **PTR (Pointer)**
Dynamic DNS Updates	Select the type of records you want dynamically updated when this object is created or deleted. These options are set as defaults via the definition in the Dynamic DNS global policies (Static DNS Mask and Dynamic DNS Mask), but can be overridden by the Dynamic DNS Updates check boxes that you select here. You can check any combination of the following values, or you can leave them all blank: • **A (Host IPV4)** • **PTR (Pointer)** • **CNAME** • **MX**

3 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

END OF STEPS

Create an alias for an object

Purpose

Use this procedure to specify an alias for an object.

Before you begin

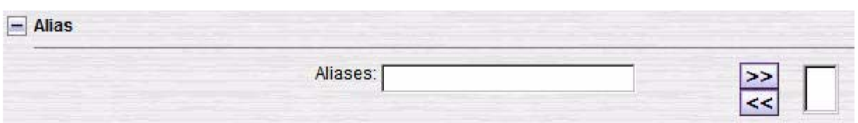
- You cannot create an alias name that has the same name as a domain or an object.
- VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and you cannot add or modify the profile. You can finetune this feature by enabling or disabling Validate CNAME Records sub-policies in Global Policies. When set to True, these sub-policies allow validation checks to be made against the following whenever you add or modify an object:
  - Object aliases
  - Object resource records
  - Domain resource records
  - Reverse zone resource records
  - ENUM NAPTR resource records

Procedure

To create an alias for an object, follow these steps.

1 Expand the **Alias** section.

Result: The **Alias** section opens.



2 Enter an alias (of up to 63 alphanumeric characters) in the **Aliases** field. Hyphens and underscores are allowed.

3 Click the add icon (>>) to add the new alias to the list of current aliases.

4 Repeat step 3 as often as necessary.

Click the remove icon (<<) to delete an alias from the list of current aliases.

5 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

END OF STEPS

Assign asset information to an object

Purpose

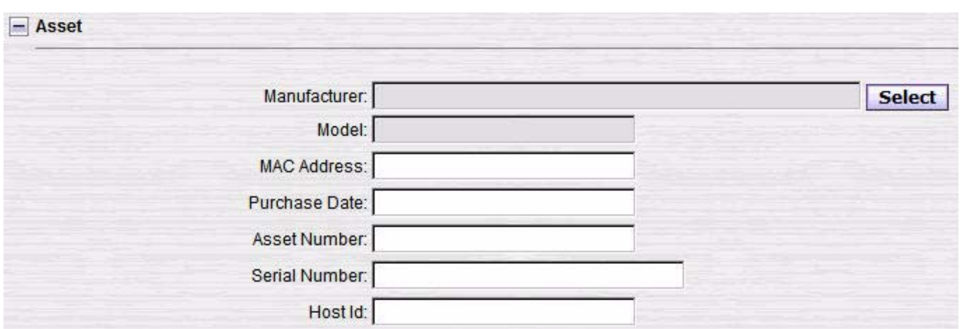
Use this procedure to add asset information for an object. Asset information is generally referred to as additional hardware/object information you want to track.

Procedure

To add asset information for an object, follow these steps.

1 Expand the **Asset** section.

Result: The **Asset** section opens.



.

2 Enter values in the fields, as described in the following table.

Table 10-7 Asset fields

Field	Description
Manufacturer	Click **Select** and the Manufacturer's List window opens. Select a manufacturer from the list. If there are Models associated with the manufacturers, they are listed in this window as well. Select a model from the list.
Model	***Read only***. Defaults from the Model list in the Manufacturer window.
Mac Address	Type the MAC address of the equipment.
Purchase Date	Enter the date this asset was purchased.
Asset Number	If there is a specific Asset Number assigned to this object, enter that number here. This is a 25-character alphanumeric value.
Serial Number	Enter the Asset Serial Number. This is a 30-character alphanumeric value.
Host Id	Enter the Asset Host ID number. This is a 16-character alphanumeric value.

3 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

END OF STEPS

Assign location and contact information to an object

Purpose

Use this procedure to assign location and contact information for an object.

Before you begin

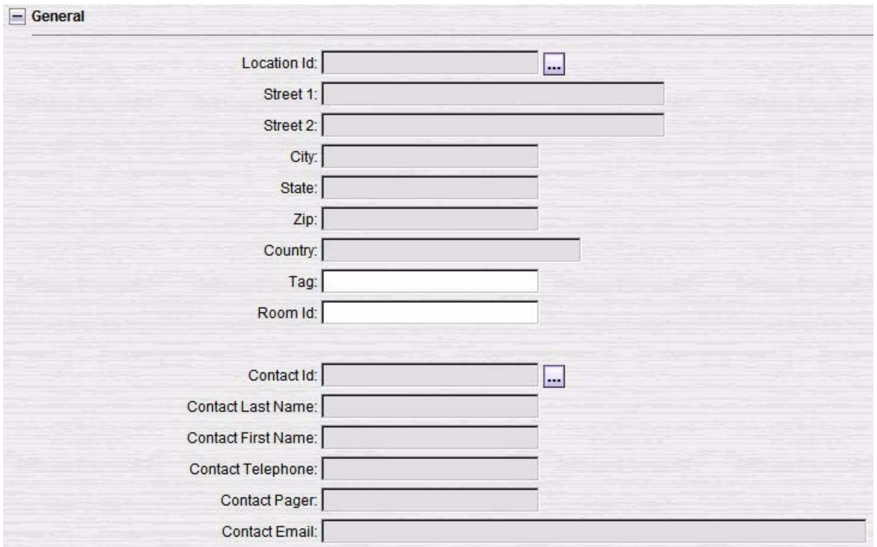
The Location and Contact information defaults to displaying whatever is stored in the Subnet Profile when a new object is added, unless you specify a different location and contact for the object in the General section.

Procedure

To assign location and contact information to an object, follow these steps.

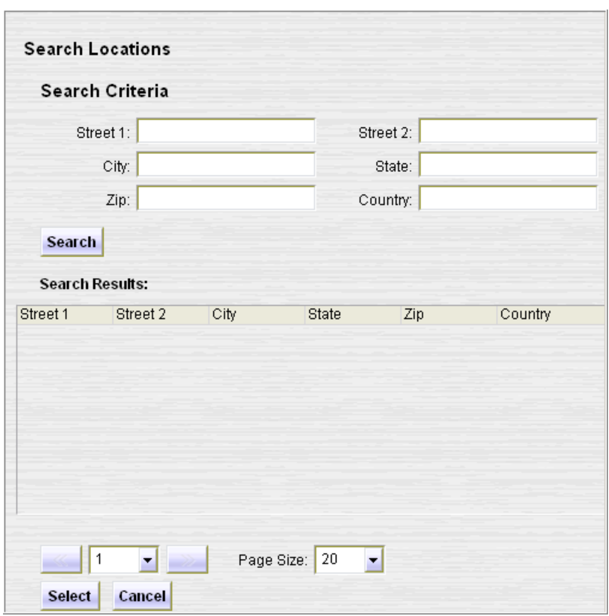
1 Expand the **General** section.

Result: The **General** section opens.



2 Click the  icon beside **Location Id**.

Result: The Search Locations page opens.



3 Enter address search criteria as needed and click **Search**. To return all address records in the database, click **Search** without entering any criteria.

Result: The Search Results list displays the results of your search criteria.

4 Select the location you wish to assign to the object and click **Select**.

Result: The **Location Id** section of the Object Profile is populated.

5 Enter a **Tag** and a **Room ID** if appropriate. You may enter up to 15 alphanumeric characters.

6 Click the  icon beside **Contact Id**.

Result: The Search Contacts page opens.

7 Enter contact search criteria as needed and click **Search**. To return all contact records in the database, click **Search** without entering any criteria.

Result: The Search Results list displays the results of your search criteria.

8 Select the contact you wish to assign to the object and click **Select**.

Result: The **Contact Id** section of the Object Profile is populated.

9 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

END OF STEPS

Associate a DHCP server with an object

Purpose

Use this procedure to assign DHCP settings to an object.

Before you begin

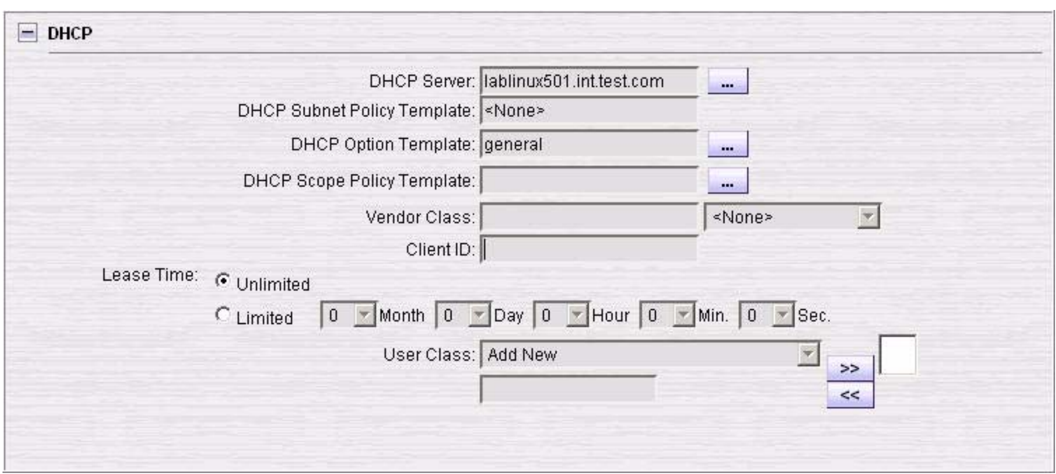
The **DHCP** section is only available if you selected Automatic Bootp, Manual DHCP, Automatic DHCP or Dynamic DHCP from the **Dynamic Configuration** field.

Procedure

To assign DHCP settings to an object, follow these steps.

1 Expand the **DHCP** section.

Result: The **DHCP** section opens.



2 Fill in the fields, as described in the following table.

Table 10-8 DHCP fields

Field	Description
DHCP Server	You must assign a DHCP Server to this object when the **Dynamic Configuration** field is set to **Automatic Bootp**, **Automatic DHCP**, **Dynamic DHCP** or **Manual DHCP**. The field defaults to the **Same as in Subnet Profile**. Select a DHCP server from the drop-down list.
DHCP Subnet Policy Template	Displays the DHCP Subnet Policy Template,
DHCP Option Template	Assigns a DHCP Option Template to the object.
DHCP Scope Policy Template	Assign a DHCP Scope Policy Option Template to this object.
Vendor Class	The Vendor Class allows you to define specific categories of vendor options; for example, you could assign a Vendor Class to an object assigned to a contractor that would specify a shorter lease time. Select a Vendor Class from the **Vendor Class** drop-down list or enter a new vendor class of up to 16 alphanumeric characters. **Note:** You can also create a vendor class in the DHCP Client Class Hierarchy. Refer to "Add a Vendor Class" (p. 21-20).
Client ID	A read-only hex-encoded string that appears when a dynamic object is being viewed, modified, or deleted when the **Dynamic Configuration** field is set to **Automatic DHCP**, **Dynamic DHCP** or **Manual DHCP**.
Lease Time	***Dynamic DHCP only***. If a lease time is defined in the DHCP template, that value overrides this field. You choose one of the following items: • **Unlimited** -The lease time is unlimited. • **Limited** - Limits the lease time. Enter the month, day, hour, minute, and seconds as needed.
User Class	The User Class allows you to define specific categories of users' options; for example, you could assign a User Class for mobile computing that specifies a shorter lease time. Select a User Class from the **User Class** drop-down list or enter a new user class of up to 19 alphanumeric characters. • Click >> to add the new user class to the list of current user classes. • Click << to delete a user class from the list of current user classes. **Note:** You can also create a user class in the DHCP Client Class Hierarchy. Refer to "Add a User Class" (p. 21-17).

3 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

END OF STEPS

Set up a manual Bootp object

Purpose

Use this procedure to set up a manual Bootp object.

Before you begin

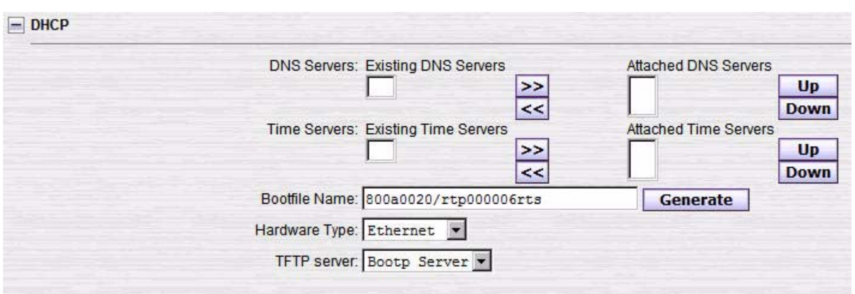
The fields for setting up a Manual Bootp object are only available if you selected "Manual-Bootp" as the value for the **Dynamic Configuration** field in the **Object** section.

Procedure

To set up a manual Bootp object, follow these steps.

1 Expand the **DHCP** section.

Result: The **DHCP** section opens.



2 Select the DNS servers associated with this object. Select a server from the **Existing DNS Servers List** and click >> to add the selected DNS server to the list of **Attached DNS Servers**. Use **Up** and **Down** to order the DNS servers.

To remove a server from the Attached DNS Servers list, highlight the server and click <<.

3 Select the Time servers associated with this object. Select a server from the **Existing Time Servers List** and click >> to add the selected Time server to the list of **Attached Time Servers**. Use **Up** and **Down** to order the Time servers.

To remove a server from the Attached Time Servers list, highlight the server and click <<.

4 The **Bootfile Name** is entered automatically as *<subnet name (hex)>/object name* (or as the model type, if the model type matches the manufacturer, or if there is only one model type for this manufacturer and it contains the tag “before”). Change it as necessary.

5 Select the **Hardware Type** for the object from the drop-down list.

6 By default, the **Tftp Server** is the same as the Bootp server. If you wish to select a different Tftp server, select a different server from the drop-down list.

7 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

END OF STEPS

Assign a user-defined field to an object

Purpose

Use this procedure to assign a user-defined value to an object.

Before you begin

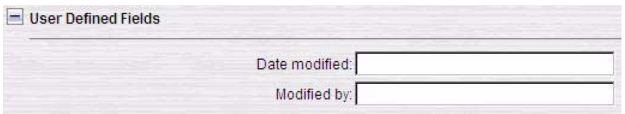
All user-Defined Fields must be established in the **Policies** > **User-Defined Fields** option of the VitalQIP client interface before you can assign them to an object.

Procedure

To assign a user-defined field and value to an object, follow these steps.

1 Expand the **UDF** section.

Result: The **UDF** section opens.



2 Enter a value in the user defined field as needed.

3 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

END OF STEPS

Associate a router with an object

Purpose

Use this procedure to associate a router with an object.

Before you begin

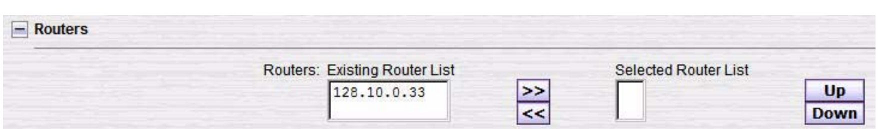
The **Router** section of the object profile only displays if the object is not a router.

Procedure

To associate a router with an object, follow these steps.

1 Expand the **Router** section.

Result: The **Router** section opens.



2 Select a router IP address from the **Existing Router List** and click [>>] to add the selected router to the **Selected Router List**. Use **Up** and **Down** to order the routers.

To remove a router from the **Selected Router List**, highlight the router and click [<<].

3 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

END OF STEPS

Assign mail forwarding options to an object

Purpose

Use this procedure to allow an object to forward mail to another defined mail host. The function creates an MX record.

Before you begin

- This section appears for all Object Classes ***except*** Printer, Terminal_Server, Gateway, Router, Bridge, Switch, and Wiring_HUB.

  Note: To define proper MX resource records within VitalQIP, the mail host or mail server objects must be created before you specify them here. For example, the DNS records could appear as follows:

```
lucent.com
mailhost IN A 10.200.130.20
mailforwarder IN A 10.200.130.21
```

  After mail host or mail server objects have been defined, you can assign one to an object in the **Mail Servers** section of the object profile.

- VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and you cannot add or modify the profile. You can disable this feature by setting the **Validate CNAME Records** policy in the VitalQIP client Global Policies to False. When you add or modify a mail server, validation checks are made against:
  - Object names
  - Domain names
  - Any Object Profile resource records

- Any Domain Profile resource records
- Any Reverse Zone resource records
- ENUM NAPTR resource records
- IPv6 node names
- Mail servers

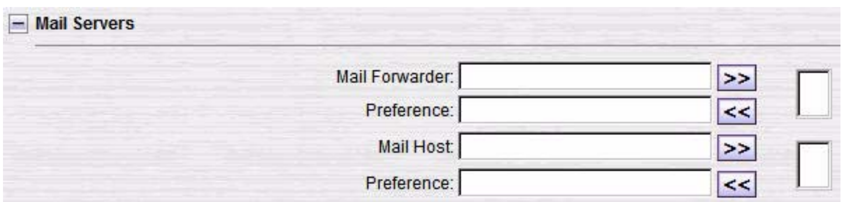
Procedure

To associate a mail server with this object, follow these steps.

---

1 Expand the **Mail Servers** section.

Result: The **Mail Servers** section opens.



---

2 Refer to the following table as you enter a **Mail Forwarder** and **Preference**. Click >> to add the mail forwarder and preference to the list.

To remove a mail forwarder and preference from the list, highlight the mail forwarder you no longer wish to associate with an object and click <<.

Add additional forwarders as necessary.

---

3 Refer to the following table as you enter a **Mail Host** and **Preference**. Click >> to add the mail host and preference to the list.

To remove a mail host and preference from the list, highlight the mail host you no longer wish to associate with an object and click <<.

Add additional mail hosts as necessary.

Table 10-9 Mail server fields

Field	Description
Mail Forwarder	To add a mail forwarder, enter the hostname (if the domain name is the same as the object) or the fully qualified domain name of the Mail Forwarder in this field. Establishing this name will allow mail to be forwarded on to its final destination.
Preference	Type a preference value in this field. This is an unsigned 16 bit number (between 0 and 65535) that adds a parameter to prevent mail routing loops. It determines an order in which a mailer should use them. Mailers will attempt delivery to mail exchangers with the lowest preference values first. For example, you can assign the "best" mail exchanger with a preference value "0".
Mail Host	You can define the object as a Mail Host for one or more domains and/or objects. This defines a host that will process the mail and will deliver it to the individual it is addressed to, or sent through a gateway it to another mail transport.
Preference	Enter a preference value in this field. The lower the preference value, the higher the priority. This is an unsigned 16 bit number (between 0 and 65535) that adds a parameter to prevent mail routing loops. Mailers will attempt delivery to mail exchangers with the lowest preference values first. For example, you can assign the "best" mail exchanger with a preference value of "0".

4 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

END OF STEPS

Assign policies to an object

Purpose

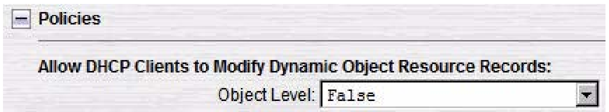
Use this procedure to assign a policy to Automatic Bootp, Dynamic DHCP, Manual DHCP or Automatic DHCP objects.

Procedure

To assign the policy for Windows 2000 DHCP clients to modify dynamic object resources, follow these steps.

1 Expand the **Policies** section.

Result: The **Policies** section opens.



2 Choose one of the following options from the **Object Level** drop-down list. The default is Same as in Subnet Profile.

- **True** – Permits a Windows 2000 DHCP client to take ownership of its dynamic object resource records to update its DNS records.
- **False** – Prohibits a Windows 2000 DHCP client from taking ownership of its resource records. This setting gives VitalQIP control and ownership of these records within DNS.
- **Same As in Subnet Profile** – Uses the policy set on the subnet profile.

3 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

END OF STEPS

Assign an object to a node

Purpose

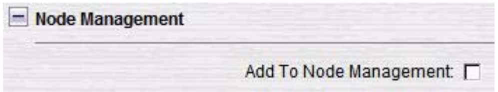
Use this procedure to assign the current object to a node.

Procedure

To assign the current object to a node, follow these steps.

1 Expand the **Node Management** section.

Result: The **Node Management** section opens.



2 Click **Add to Node Management** if you want this object assigned to an IPv6 node.

3 Click **Submit** if you have finished entering all information for the object, or continue to another section of the object profile.

Note: If you check this box, clicking **Submit** opens the Add IP Address page, where you can select a node to which you want to add this object. Refer to "Add an IPv4 Address to an interface" (p. 11-29) for detailed information about this function.

END OF STEPS

Manage domain names in view specific zones

Purpose

Use this procedure to manage fully qualified domain names in view specific zones.

Before you begin

- The **DNS View** section is displayed only when modifying a static object and not when adding a static object.
- Alcatel-Lucent recommends giving servers a view specific fully qualified domain name. In zone files in a DNS View, the view specific domain name will be used for the NS, A, and SOA records instead of the global namespace name available in the server profiles.
- The PTR records for fully qualify domain names are not published in DNS.

Procedure

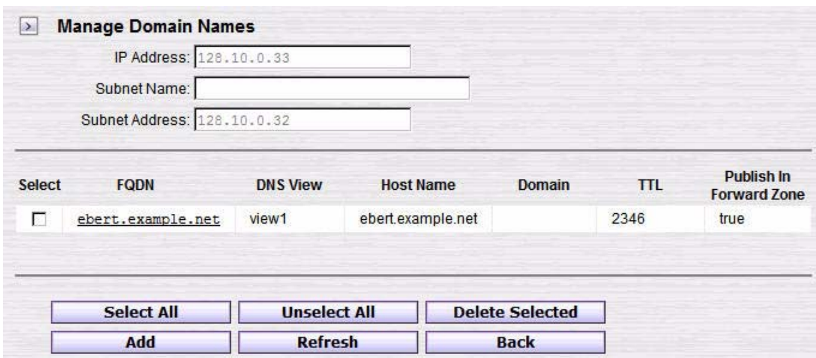
To manage fully qualified domain names for an object in IPv4, follow these steps:

1 Expand the **DNS View** section in the Modify Object Profile page.

Result: The **DNS View** section opens.

2 To manage view specific domains, click **Manage Domain Names**.

Result: The Managed Domain Name page opens.



3 Choose an action.

If you want to...	Then...
Add a fully qualified domain name	1. Click **Add**. **Result:** The Add Domain Name page opens. Only fields in the the **Domain Name** section are enabled. 2. Enter the appropriate information in the Domain Name fields. Refer to Table 11-9, "Add Domain Name fields" (p. 11-41) for field descriptions. **Note:** **Publish in Reverse Zone** is not valid for fully qualified domain names. 3. Click **Submit**. **Result:** The domain name is added to the list.
Modify a fully qualified domain name	1. Click a domain name to modify. **Result:** The Domain Name Properties page opens. 2. Click **Modify**. **Result:** The Modify Domain Name page opens. 3. In the **Domain Name** section, modify the desired fields. Other fields in the page cannot be modified. 4. Click **Submit**. **Result:** A message opens stating if the changes were successful.
Delete a fully qualified domain name	1. Select the domain names from the list. 2. Click **Delete Selected**. **Result:** The domain name are removed from the list.
Select all fully qualified domain names	Click **Select All**. **Result:** All domain names in the list have the checkbox selected.
Unselect all fully qualified domain name	Click **Unselect All**. **Result:** All domain names in the list have the checkbox unselected.
Refresh the list	Click **Refresh**. **Result:** The domain names are updated.
Return to the previous page	Click **Back**. **Result:** You are returned to the previous page.

END OF STEPS

11 Node management

Overview

Purpose

This chapter describes the functions used to manage IPv6 nodes in VitalQIP.

Contents

This chapter covers these topics.

Node management

Overview

Purpose

VitalQIP displays hardware on your network as nodes. A node can be a router, server, laptop computer or any other piece of hardware connected to your network.

A node's physical connection to the network, a Network Interface Card (NIC), is displayed as an interface. Nodes that have more than one NIC card, such as routers, can have an interface for each connection. Interfaces can have MAC addresses defined by the NIC card's manufacturer.

An interface's logical connection to the network is as an IP address. An interface can have multiple IP addresses that share the same physical connection to the network. For example a single NIC card can have an IPv4 address, a link local IPv6 address and a globally routable IPv6 address.

VitalQIP allows administrators to define and track nodes in the Node Management portion of the GUI.

Search for a node

Purpose

Use the **Node Search** function to search for nodes in the node hierarchy.

When you initially select the **Node Search** function, there are no nodes displayed in the node hierarchy. You must search for nodes to be able to access them. You can enter any combination of available search fields.

The search results depend on the information entered. For example, if you enter a value in the IP Address field, the results are a listing of IP addresses. If you enter a value in the Name field, the results are a listing of domain names.

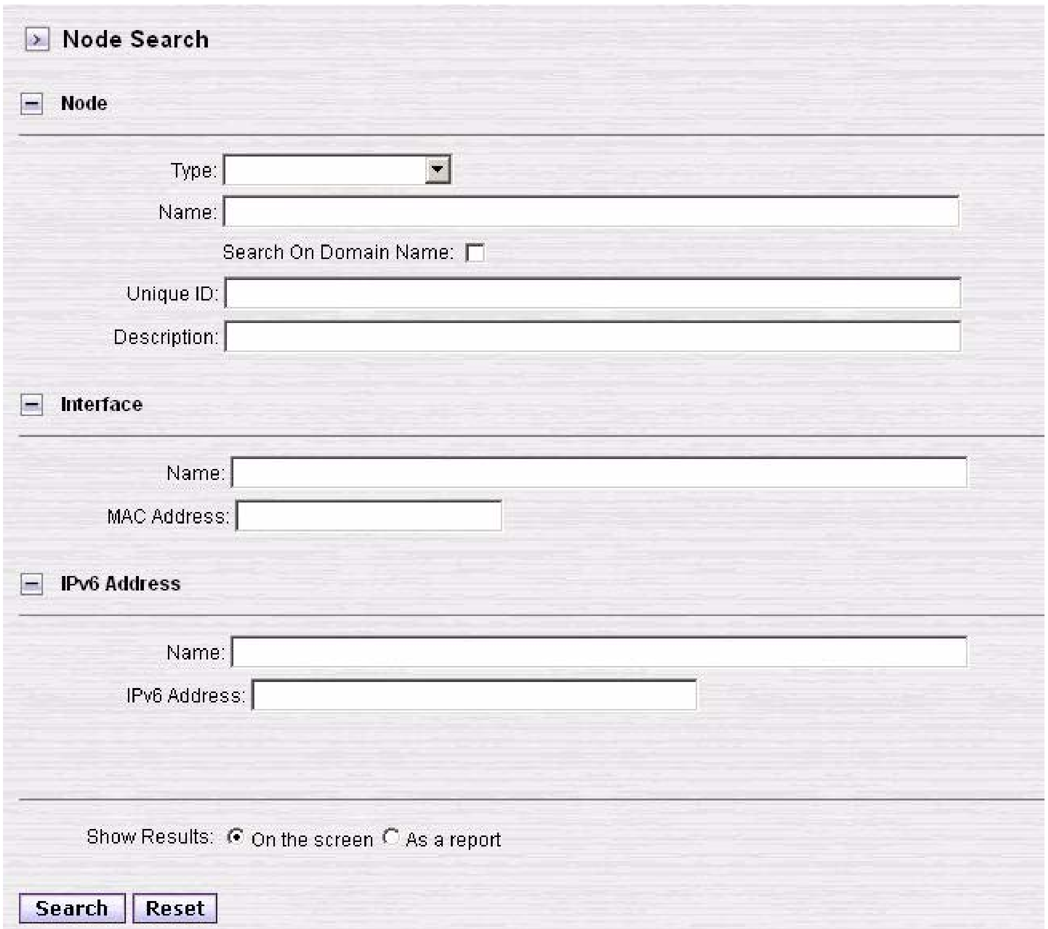
Once the search results are displayed, you can select an item to add to the hierarchy. For example, when you select an IP Address in the search results and click **Add to Hierarchy**, the node corresponding to this IP address is added to the hierarchy, and the node is expanded in the hierarchy to the IP address selected. If the node is already in the hierarchy, the hierarchy is simply expanded. The search attributes are grouped in collapsible pages by Node, Interface, and IP Address.

Procedure

To search for a node, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.



2 Enter the value or values you want to use to search for a node. You can enter values in all or some sections of the Node Search page. You can also leave all fields blank, however this returns all nodes defined in the system.

Note: You can use the asterisk (*) as a wildcard in any text field on this screen. You can use the asterisk at the beginning, middle or end of a string.

Review the following table for a description of the fields.

Table 11-1 Node search fields

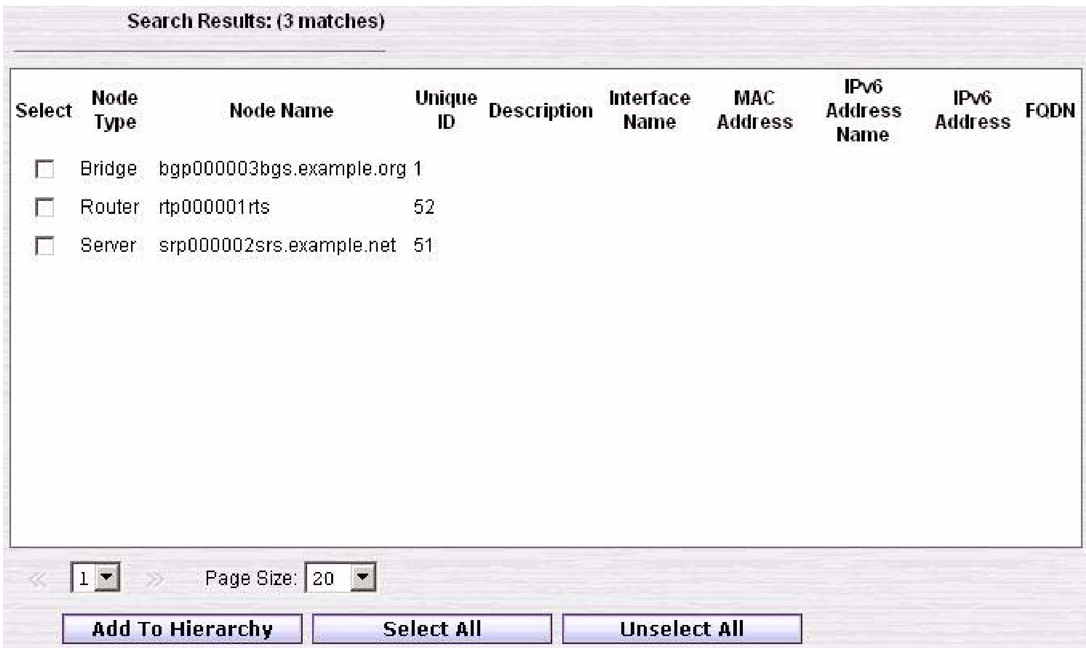
Field	Description
Node	
Type	The type of node for which you are searching. Select a value from the drop-down list. The list of values shown is delivered with VitalQIP, however this list is customizable. Therefore the list may contain additional values, or may not contain some values shown in the following list. • Workstation • X-terminal • PC • Printer • Server • Wiring_Hub • Router • Bridge • Terminal_Server • Switch • Legacy_System • Gateway • Test_Equipment • Undefined • Others • Partially_Managed
Name	Name of the node for which you are searching.
Search On Domain Name	If selected, the search is performed on the domain name. If cleared, the search is performed on the node name.
DNS Views	***Appears only when Search On Domain Name is selected.*** Searches for domains across DNS views. Select one of the following: • *`<null>`* - Searches in any DNS View or the global namespace. • **None** - Does not search in DNS Views. The search occurs only in the global namespace. • **Any** - Searches in all DNS Views and not the global namespace. • *`<DNS View>`* - Searches only within a specific DNS View. All DNS Views in the organization are listed for selection.
Unique ID	Unique ID assigned to the node.
Description	Text description assigned to the node.

Field	Description
Interface	
Name	Name of the interface assigned to the node.
MAC Address	MAC address of the interface card assigned to the node.
IP Address	
Name	Name of the IP address assigned to the node.
IP Address	IPv6 address assigned to the node.
Node Attributes **Note:** This section only appears when user defined attributes are associated with the **Node** infrastructure type.	
Attribute Group	Select an attribute group from the drop-down list. The allowable values consist of **<NONE>** and any attribute groups defined at your site.
Attribute Name	Select an attribute name from the drop-down list. The allowable values consist of **<ALL>** and any attributes defined at your site. The list is limited to those items specified in the Attribute Group field.
Attribute Value	Enter a value associated with the attribute you are using in your search.
Add New Criteria	This button adds a row for an attribute search criteria fields.
Remove Criteria	Removes the criteria.
Interface Attributes **Note:** This section only appears when user defined attributes are associated withthe **Interface** infrastructure type.	
Attribute Group	Select an attribute group from the drop-down list. The allowable values consist of **<NONE>** and any attribute groups defined at your site.
Attribute Name	Select an attribute name from the drop-down list. The allowable values consist of **<ALL>** and any attributes defined at your site. The list is limited to those items specified in the Attribute Group field.
Attribute Value	Enter a value associated with the attribute you are using in your search.
Add New Criteria	This button adds a row for an attribute search criteria fields.
Remove Criteria	Removes the criteria.
IP Address Attributes **Note:** This section only appears when user defined attributes are associated with the **IPv4 Address** and **IPv6 Address** infrastructure types.	
Attribute Group	Select an attribute group from the drop-down list. The allowable values consist of **<NONE>** and any attribute groups defined at your site.

Field	Description
Attribute Name	Select an attribute name from the drop-down list. The allowable values consist of **<ALL>** and any attributes defined at your site. The list is limited to those items specified in the **Attribute Group** field.
Attribute Value	Enter a value associated with the attribute you are using in your search.
Add New Criteria	This button adds a row for an attribute search criteria fields.
Remove Criteria	Removes the criteria.

3 Click **Search**.

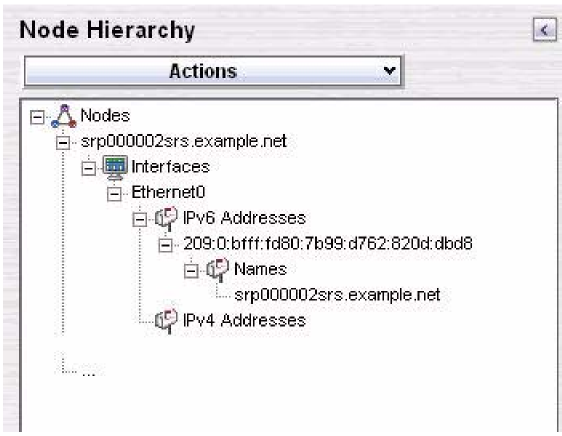
Result: A list of matching nodes is displayed in the **Search Results** list.



4 Click the checkbox in the **Select** column beside each node whose hierarchy you want to view. You can click the **Select All** button to select all nodes displayed on this page of results. You can click the **Deselect All** button to clear all the checkboxes displayed on this page of results.

5 Click **Add to Hierarchy**.

Result: The node's hierarchy is displayed on the left side of the screen.



END OF STEPS

Search for an IPv4 object

Purpose

Use the IPv4 Object Search function to find IPv4 objects in the node hierarchy.

Before you begin

Only IPv4 addresses that are currently associated to an interface in Node Management are returned.

Procedure

To search for an IPv4 object, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Mouse over the **Actions** menu and select **IPv4 Object Search**.

Result: The IPv4 Object Search page opens.

3 Enter the value or values you want to use to search for an object. You can enter values in all or some sections of the IPv4 Object Search page. You can also leave all fields blank, however this returns all nodes associated with an IPv4 address that are defined in the system.

Note: You can use the asterisk (*) as a wildcard in any text field on this screen. You can use the asterisk at the beginning, middle or end of a string.

Review the following table for a description of the fields.

Table 11-2 IPv4 object search fields

Field	Description
Name	Name of the object for which you are searching.
IP Address	IP address assigned to the object.
MAC Address	MAC address of the interface card assigned to the node.
User-Defined Field	This value consists of two fields. The first is a drop-down list that allows you to select from all user-defined fields, or to specify one. The second field allows you to enter a value assigned to the user-defined field you have selected. **Note:** This field only displays if a user-defined field is assigned to nodes.

4 If user defined attributes or fields are associated with IPv4 object, the **User Defined Fields** or **User Defined Attributes** section is displayed. Refer to "Working with user defined attributes and fields" (p. 7-23) for more information.

5 Click **Search**.

Result: A list of matching nodes is displayed at the bottom of the IPv4 Object Search page.

6 Click the check boxes in the **Select** column for the nodes whose hierarchies you want to view. Click **Select All** to select all objects displayed on this page of results. Click **Unselect All** to unselect all objects displayed on this page of results.

7 Click **Add to Hierarchy**.

Result: The selected node's hierarchy is added to the Node Hierarchy.

END OF STEPS

Add a node

Purpose

Use this procedure to add a node. When you add a node using this procedure, VitalQIP takes you through the process of adding a node, adding an interface to the node, and then adding an address to the interface. You have the option of adding all components, or initially can add just the node, and add its subcomponents later.

Before you begin

VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and you cannot add or modify the profile. You can disable this feature by setting the **Validate CNAME Records** policy in the VitalQIP client Global Policies to False. When you add or modify an IPv6 node, validation checks are made against:

- Object aliases
- Object resource records

- Domain resource records
- Reverse zone resource records

Procedure

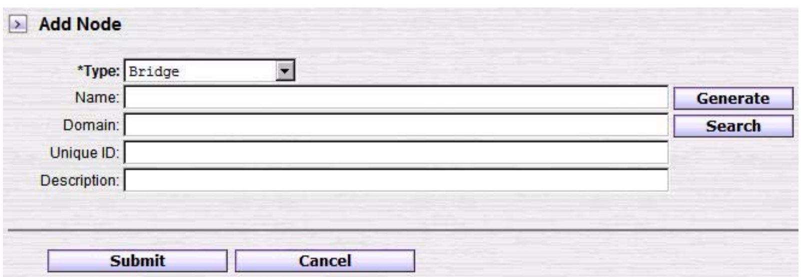
To add a node, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Mouse over the **Actions** menu and select **Add Node**.

Result: The Add Node page opens.



3 Enter the values you want to use to add a node. Review the following table for a description of the fields.

Table 11-3 Add node fields

Field	Description
Type	***Required***. Type of node for which you are adding. Allowable values are site-specific. The following values are supplied at the time VitalQIP is installed. Your list may be different if it has been customized at your site: • Workstation • X-terminal • PC • Printer • Server • Wiring_Hub • Router • Bridge • Terminal_Server • Switch • Legacy_System • Gateway • Test_Equipment • Undefined • Others • Partially_Managed
Name	Enter the name of the node. Click **Generate** to have the database provide one for you. You must enter a value in this field or in the **Domain** field or both.
Domain	Enter the domain to which this node is assigned. Click **Search** to search for a domain. You must enter a value in this field or the **Name** field, or both.
Unique ID	***Optional***.Unique ID assigned to the node. If you leave this field blank, the system assigns a value.This must be unique within the organization.
Description	***Optional***. Text description assigned to the node.

4 Click **Submit**.

Result: A dialog box opens with the message **Node Created.**

5 Click **OK**.

Result: The Node Properties page opens.

END OF STEPS

Quickly add a node and all subcomponents

Purpose

Use this procedure to add a node, interface and IP address all on one screen. When you add a node using this procedure, you must add all components at once. If you want to add a node without adding an interface and IP address, refer to "Add a node" (p. 11-10).

Procedure

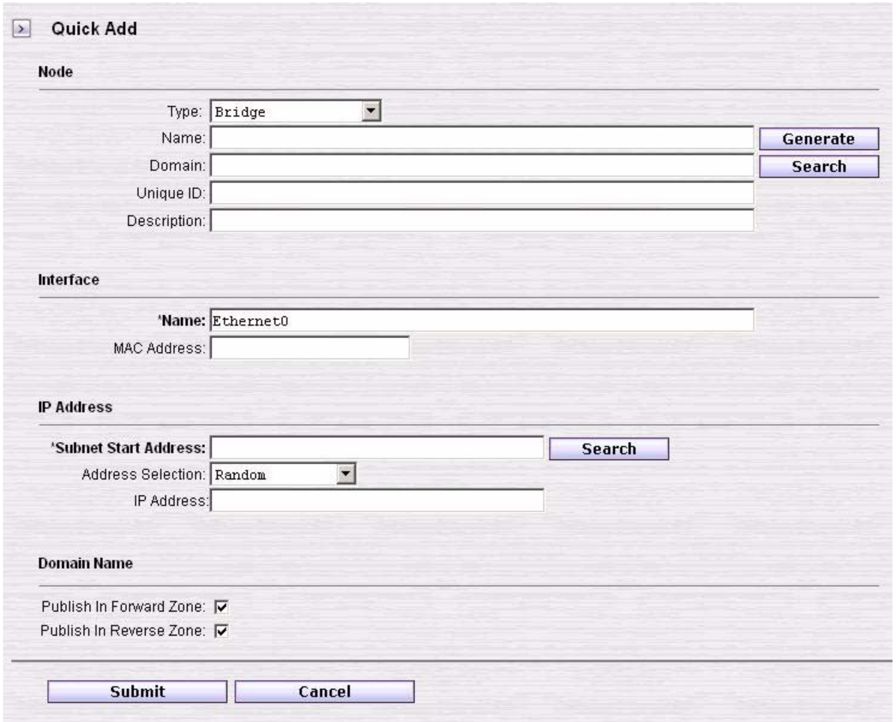
To quickly add a node, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Mouse over the **Actions** menu and select **Quick Add**.

Result: The Quick Add page opens.



3 Enter the values you want to add a node. Review the following table for a description of the fields.

Table 11-4 Quick add node fields

Field	Description
Node	
Type	***Required***. Type of node you are adding. Allowable values are site-specific. The following values are supplied at the time VitalQIP is installed. Your list may be different if it has been customized at your site: • Workstation • X-terminal • PC • Printer • Server • Wiring_Hub • Router • Bridge • Terminal_Server • Switch • Legacy_System • Gateway • Test_Equipment • Undefined • Others • Partially_Managed
Name	Name of the node you want to use.You must enter a value in this field, the **Domain** field, or both. Click **Generate** to automatically generate a node name.
Domain	Domain to which this node is assigned. Click **Search** to search for a domain. You must enter a value in this field or the **Name** field, or both.
Unique ID	Unique ID assigned to the node.If you leave this field blank, the system assigns a value. This value must be unique within the organization.
Description	Text description assigned to the node.
Interface	
Name	***Required***. Name of the interface assigned to the node.
MAC Address	MAC address of the interface card assigned to the node.

Field	Description
IP Address	
Subnet Start Address	***Required***. Enter the subnet address that contains the IP address you want to assign to this interface. Click **Search** to open the subnet selection window to select a subnet. If you select a subnet from the Subnet Selection window, this field is populated from that value.
Address Selection	***Required***. Determines how the address assigned to this interface is determined. Select a value from the drop-down list. Allowable values are as follows: • **Next Available** • **Last Available** • **Random** • **Specific** If you select **Specific**, you can enter a specific IP address in the IP address field.
IP Address	***Optional***. The IPv6 address you want to add to the interface. You can only enter an IP address if you chose **Specific** in the Address Selection field.
Domain Attributes	
Publish in Forward Zone	This checkbox determines if an IPv6 AAAA record for the IPv6 Address is published in a forward zone. The AAAA record is then published in the forward zone for DNS lookups.
Publish in Reverse Zone	This checkbox determines if a PTR record for the IPv6 Address is published in a reverse zone. The PTR record is then published in the reverse zone for DNS lookups.

4 Enter appropriate values for any Attributes.

5 Click **Submit**.

Result: A dialog box opens with the message **Node added successfully!**

6 Click **OK**.

Result: The Node Properties page opens.

END OF STEPS

Modify a node

Purpose

Use this procedure to modify a node's properties.

Before you begin

You can modify a node after you have first searched for it and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To modify a node, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

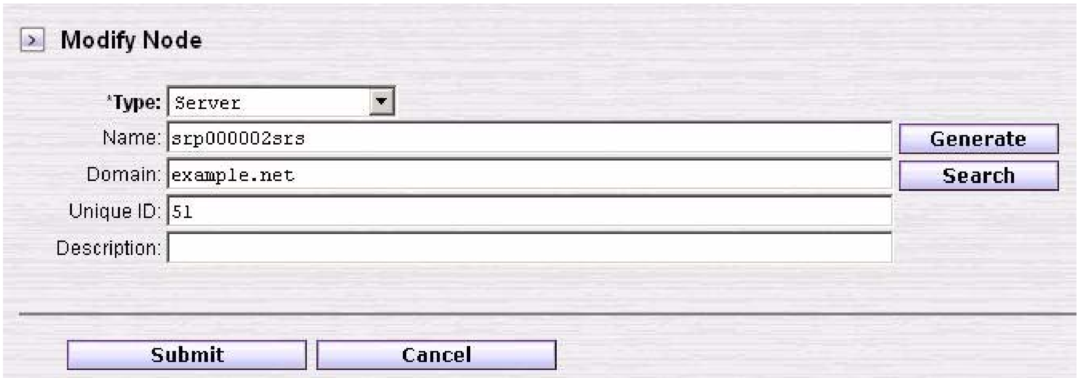
2 Enter search criteria to locate the node you want to modify, as described in "Search for a node" (p. 11-3).

3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

Result: The Node Properties page opens.

4 Click **Modify**.

Result: The Modify Node page opens.



5 Modify node information on the Node Modify page. Review the following table for a description of the fields.

Table 11-5 Modify node fields

Field	Description
Type	Type of node. Allowable values are site-specific. The following values are supplied at the time VitalQIP is installed. Your list may be different if it has been customized at your site: • Workstation • X-terminal • PC • Printer • Server • Wiring_Hub • Router • Bridge • Terminal_Server • Switch • Legacy_System • Gateway • Test_Equipment • Undefined • Others • Partially_Managed
Name	Name of the node.

Field	Description
Domain	Domain where the node resides.
Unique ID	***Optional.*** Unique ID assigned to the node.If you leave this field blank, the system assigns a value. This value must be unique within the organization.
Description	Text description assigned to the node.

6 If the node has Attributes associated with it, you can modify those as well.

7 When you are finished making changes, click **Submit**.

Result: A dialog box opens with the message **Node Modified.**

8 Click **OK**.

Result: The Node Properties page opens with the modified values as applicable.

END OF STEPS

Delete a node

Purpose

Use this procedure to delete a node.

Before you begin

You can delete a node after you have first searched for it and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To delete a node, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Enter search criteria to locate the node you want to delete, as described in "Search for a node" (p. 11-3).

3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

Result: The Node Properties page opens.

4 Click **Delete**.

Result: A dialog box opens with the message **This action will delete the Node, ALL the interfaces on the Node and ALL the IP Addresses on these interfaces and their associated DNS records. Are you sure you want to proceed?**

5 Click **OK**.

Result: A dialog box opens with the message **Node Deleted.**

6 Click **OK**.

Result: The node is deleted and removed from the Node Hierarchy:

END OF STEPS

Add an interface to a node

Purpose

Use this procedure to add an interface to a node.

Before you begin

You can add an interface to a node after you have first searched for it and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To add an interface to a node, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

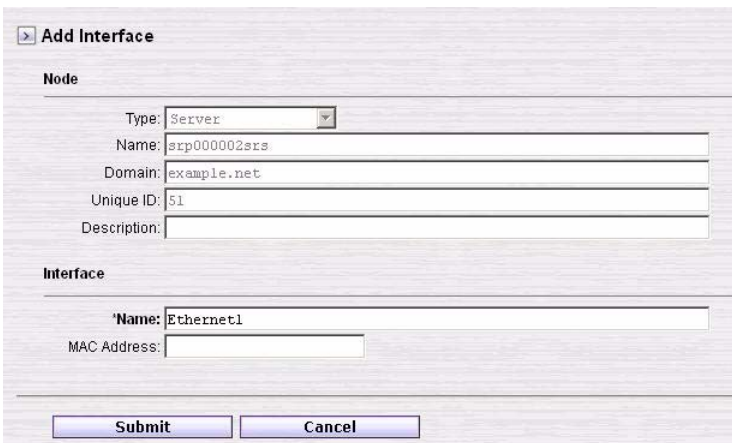
2 Enter search criteria to locate the node to which you want to add an interface, as described in "Search for a node" (p. 11-3).

3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

Result: The Node Properties page opens.

4 Click **Add Interface**.

Result: The Add Interface page opens.



5 Modify interface information, as decribed in the following table.

Note: Node fields are read only on this page. Review Table 11-5, "Modify node fields" (p. 11-18) for a description of the node fields.

Table 11-6 Interface fields

Field	Description
Name	***Required***. Name of the interface assigned to the node. VitalQIP generates a default name, which you can change. This name must be unique within this node.
MAC Address	***Optional***. MAC address of the interface card assigned to the node.

6 Click **Submit**.

A dialog box opens with the message **Interface Created.**

7 Click **OK**.

Result: The Node is displayed on the Node Hierarchy with the new interface and the Interface Properties page is displayed.

E N D O F S T E P S

Modify an interface

Purpose

Use this procedure to modify an interface.

Before you begin

You can modify an interface after you have first searched for the node that contains the interface and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To modify an interface, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Enter search criteria to locate the node that contains the interface you want to modify, as described in "Search for a node" (p. 11-3).

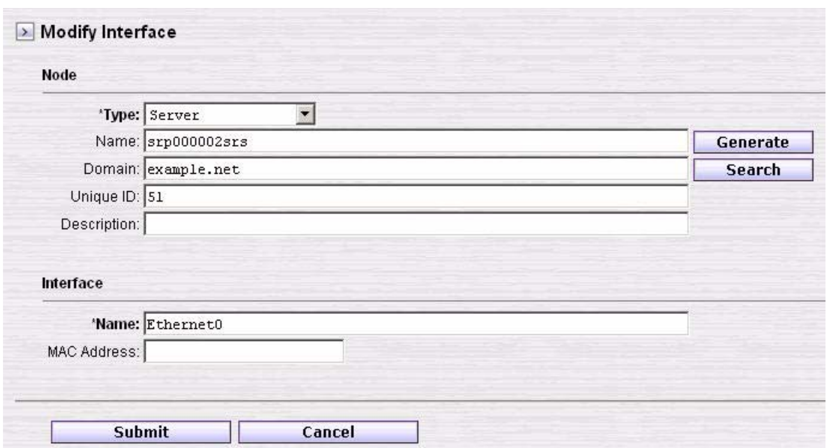
3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

4 Expand the node and select the interface you want to modify.

Result: The Interface Properties page opens.

5 Click **Modify**.

Result: The Modify Interface page opens.



6 Review Table 11-6, "Interface fields" (p. 11-22) for information about these fields.

7 Click **Submit** when you are finished modifying fields.

Result: A dialog box opens with the message **Interface Modified.**

8 Click **OK**.

Result: The Interface Properties page displays the modified information.

END OF STEPS

Move an interface to another node

Purpose

Use this procedure to move an interface to another node.

Before you begin

You can move an interface to another node after you have first searched for the node that currently contains the interface and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To move an interface to a different node, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Enter search criteria to locate the node that contains the interface you want to move, as described in "Search for a node" (p. 11-3).

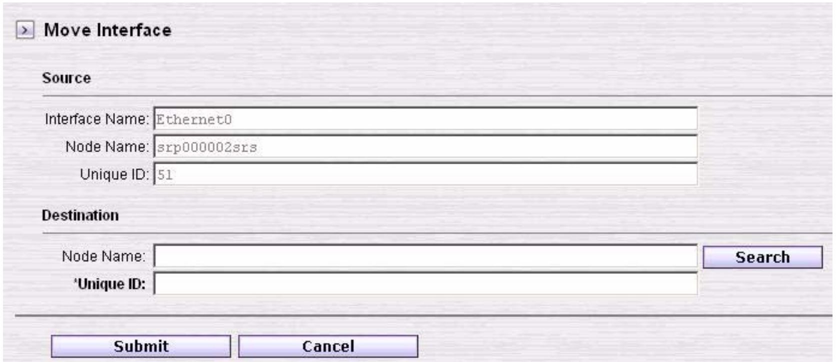
3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

4 Expand the node and select the interface you want to move.

Result: The Interface Properties page opens.

5 Click **Move**.

Result: The Move Interface page opens.



6 Enter a value in the **Node Name** field by using the **Search** button to select a node name from a list of available nodes. This field is optional.

Note: Selecting a node from the list of available nodes automatically populates the **Unique ID** field.

7 Enter a node's unique ID in the **Unique ID** field. This field is required. If you have selected a Node Name in the previous step, this field contains the unique ID for that node.

8 Click **Submit**.

A dialog box opens with the message **Interface Moved Successfully!**

9 Click **OK**.

Result: The hierarchy is updated to reflect the move, and the newly moved interface properties are displayed.

END OF STEPS

Add an IPv6 address to an interface

Purpose

Use this procedure to add an IPv6 address to an interface.

Before you begin

You can add an IPv6 address to an interface after you have first searched for the node that currently contains the interface and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To add an IP address to an interface, follow these steps.

1. Mouse over **Address Management** and select **Node**.

   Result: The Node Hierarchy opens with the Node Search page.

2. Enter search criteria to locate the node containing the interface to which you want to add an IPv6 address, as described in "Search for a node" (p. 11-3).

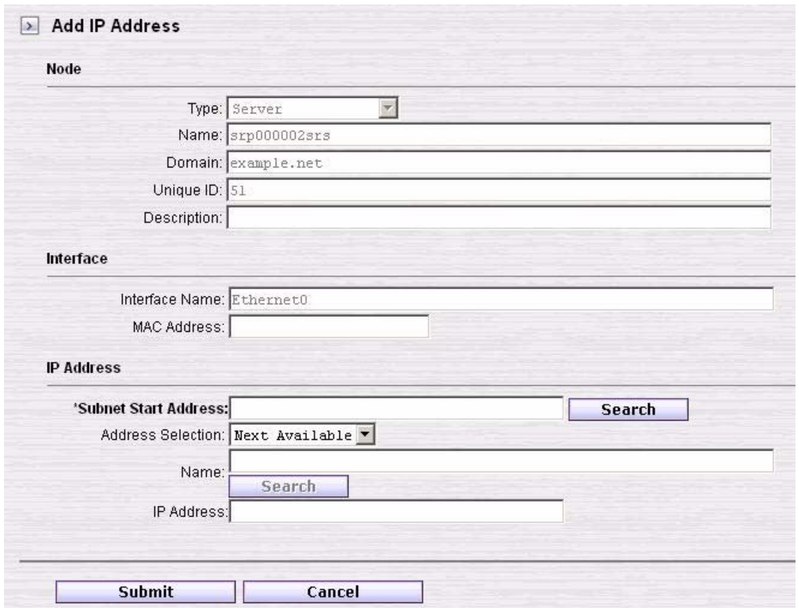
3. Click **Add To Hierarchy** and select the node in the Node Hierarchy.

4. Expand the node and select the interface.

   Result: The Interface Properties page opens.

5. Click **Add IPv6 Address**.

Result: The Add IP Address page opens.



6 Add IP address information on the Add IP Address page.

Note: Node fields and Interface fields are read only on this page. Review Table 11-5, "Modify node fields" (p. 11-18) for a description of the node fields. Review Table 11-6, "Interface fields" (p. 11-22) for a description of interface fields.

7 Review the following table for a description of the IP Address fields.

Table 11-7 IP Address fields

Field	Description
Subnet Start Address	***Required***. Enter the subnet address that contains the IP address you want to assign to this interface. You can use **Search** to open the subnet selection window to select a subnet. If you select a subnet from the Subnet Selection window, this field is populated from that value. If you select **Specific** from the Address Selection field, you can enter a specific IP address in the IP address field. If you select **Existing** from the Address Selection field, the Subnet Start Address, Name and IP Address fields are unavailable, and you must select an existing IP Address using the **Search** button next to the Name field.

Field	Description
Address Selection	***Required***. Determines how the address assigned to this interface is determined. Select a value from the drop-down list. Allowable values are as follows: • **Next Available** • **Last Available** • **Random** • **Existing** • **Specific** If you select **Specific**, you can enter a specific IP address in the IP address field. If you select **Existing**, the Subnet Start Address, Name and IP Address fields are unavailable, and you must select an existing IP Address using the Search button next to the Name field. Adding an existing address to a interface means that the IP address will exist on more than one interface. Examples of this configuration include TCP load balancers and multicast groups.
Name	***Optional***. Name associated with an IP address. The Search buttons is unavailable unless you select **Existing** in the Address Selection field. The name of an IP address is particularly useful for identifying multicast groups.
IP Address	***Optional***. The IP address you want to add to the interface. You can only enter an IP address if you chose **Specific** in the Address Selection field.

8 Click **Submit**.

Result: A dialog box opens with the message **Address Created.**

9 Click **OK**.

Result: The interface is displayed on the Node Hierarchy with the new IP address and the IP address properties are displayed in the right-hand page.

END OF STEPS

Add an IPv4 Address to an interface

Purpose

Use this procedure to add an IPv4 address to an interface.

Before you begin

You can add an IPv4 address to an interface after you have first searched for the node that currently contains the interface and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To add an IP address to an interface, follow these steps.

1. Mouse over **Address Management** and select **Node**.

   Result: The Node Hierarchy opens with the Node Search page.

2. Enter search criteria to locate the node containing the interface to which you want to add an IPv6 address, as described in "Search for a node" (p. 11-3).

3. Click **Add To Hierarchy** and select the node in the Node Hierarchy.

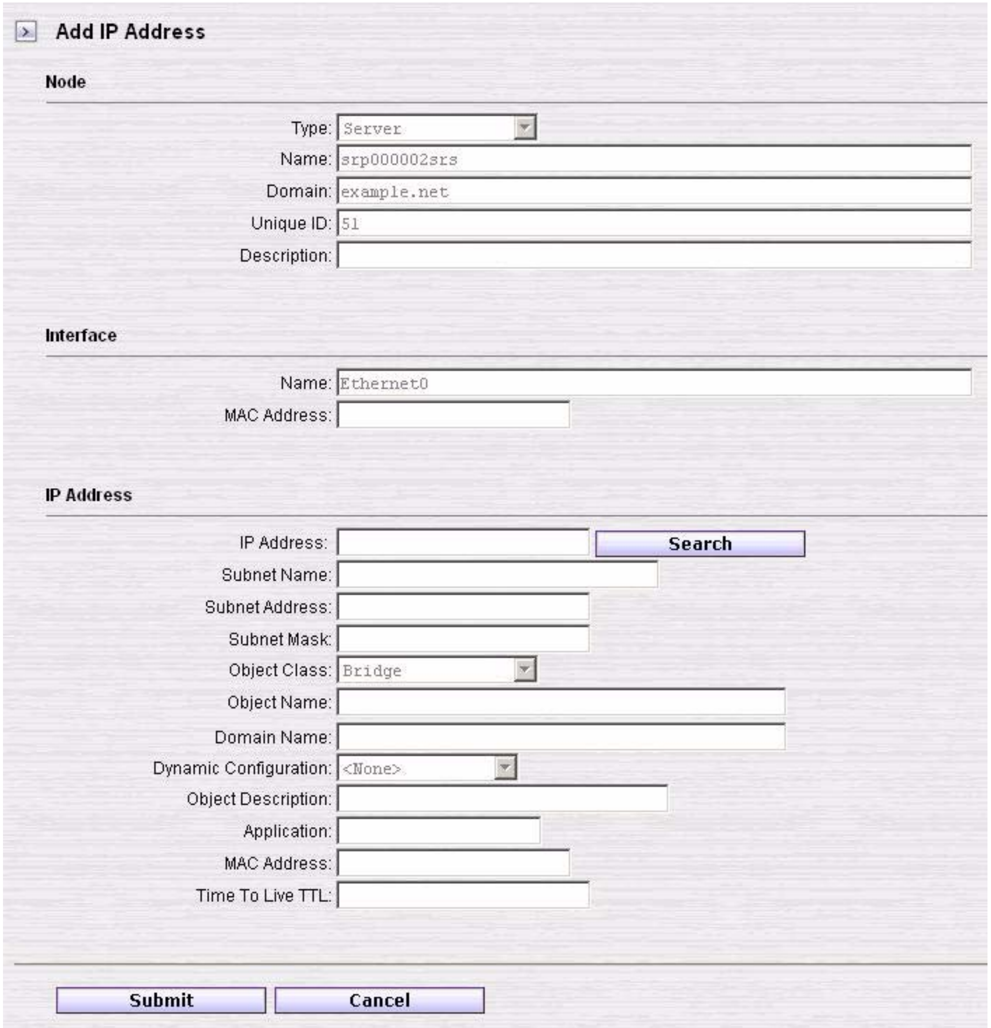
4. Select a node from the Node Hierarchy.

5. Expand the node and select the interface.

   Result: The Interface Properties page opens.

6. Click **Add IPv4 Address**.

Result: The Add IP Address page opens.



Note: Node fields and Interface fields are read-only on this page. Review Table 11-5, "Modify node fields" (p. 11-18) for a description of the node fields. Review Table 11-6, "Interface fields" (p. 11-22) for a description of interface fields.

7 Enter an IP address in the **IP Address** field or click **Search** to find an IPv4 IP address with the same object class as the current node. Only addresses that are not associated with an interface are returned.

Note: The remaining IP Address fields on this screen are read-only, and take on the value associated with the IP address you enter.

8 Click **Submit** to add the IPv4 address to the interface.

END OF STEPS

Modify an IP address associated with an interface

Purpose

Use this procedure to modify IP address fields associated with an interface.

Before you begin

- You cannot change the IP address of an interface. You must delete it and add a new one.
- You can modify IP address fields associated with an interface after you have first searched for the node that contains the interface and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To modify an IP address associated with an interface, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

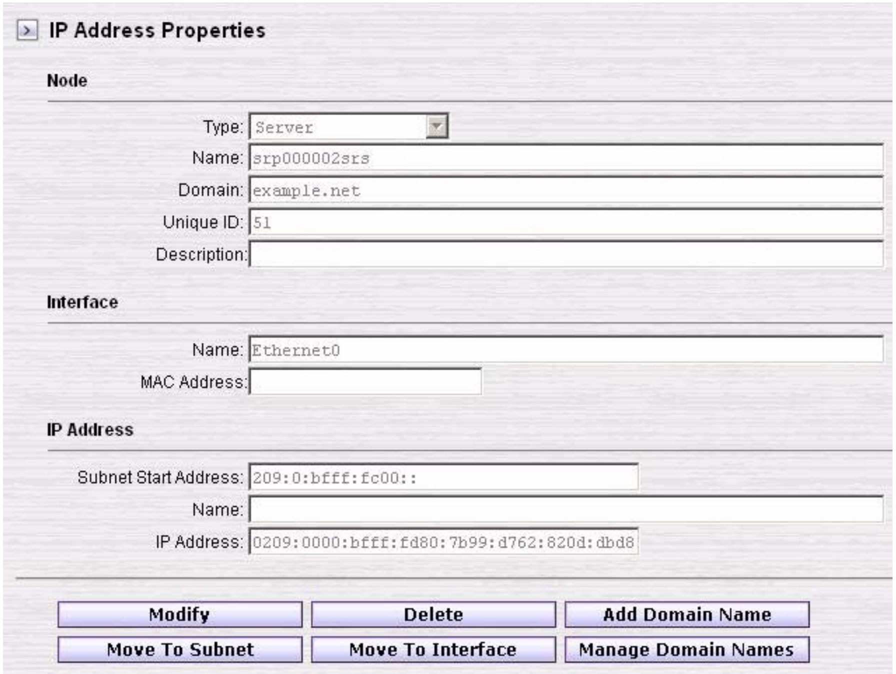
2 Enter search criteria to locate the node containing the interface with the IP address fields that require changes, as described in "Search for a node" (p. 11-3).

3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

4 Expand the node and select the interface containing the IP address information you want to modify.

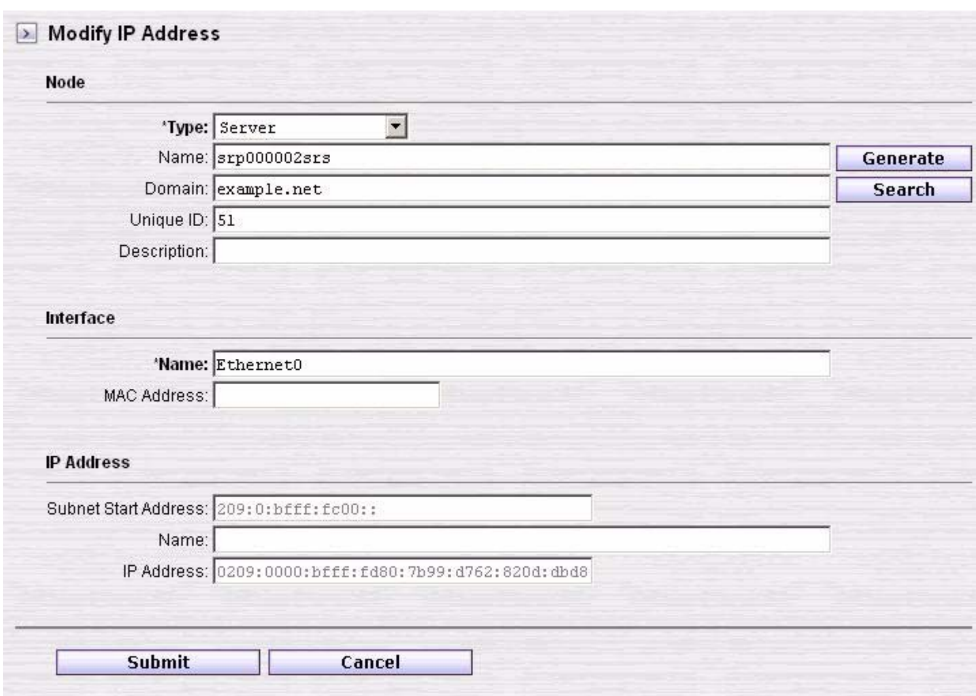
5 Expand the interface and select the IP address.

Result: The IP Address Properties page opens.



6 Click **Modify**.

Result: The Modify IP Address page opens.



7 Modify the address as needed.

- For IPv6 addresses, refer to Table 11-7, "IP Address fields" (p. 11-27) for a detailed explanation of the fields on this screen.
- For IPv4 addresses, you can modify Node and Interface information. Refer to Table 9-1, "Quick Add fields" (p. 9-13) for a detailed explanation of fields on this screen.

8 Click **Submit**.

Result: A dialog box opens with the message **IP Address Modified.**

9 Click **OK**.

Result: The IP address has been modified and the IP address' properties are displayed in the right-hand page.

END OF STEPS

Move an IP address to a different interface

Purpose

Use this procedure to reassign an IP address from one interface to another.

Before you begin

You can move an IP address to a different interface after you have first searched for the node that currently contains the interface and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To move an IP address to a different interface, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Enter search criteria to locate the node containing the interface with the IP address you want to move, as described in "Search for a node" (p. 11-3).

3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

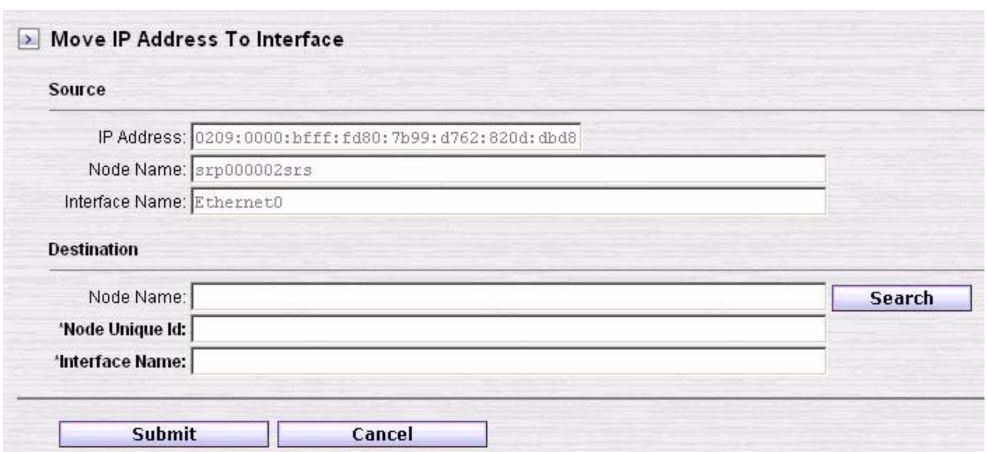
4 Expand the **Interfaces** node.

5 Expand the **IPv4 Addresses** or **IPv6 Addresses** node and select the IP address you want to move.

Result: The IP Address Properties page opens.

6 Click **Move to Interface**.

Result: The Move IP Address To Interface page opens.



7 Enter values in the **Destination** fields based on the descriptions in the following table:

Table 11-8 Move IP Address To Interface fields

Field	Description
Node Name	***Optional***. Name of the node containing the interface to which you want to move this IP address. **Note:** You can only use **Search** to enter a node name in this field. If you do, the following two required fields are automatically filled in.
Node Unique ID	***Required***. Unique ID assigned to the node. Automatically filled in if you use **Search** to find the node name.
Interface Name	***Required***. Name of the interface to which you are reassigning this IP address. Automatically filled in if you use **Search** button to find the node name.

8 When you have entered values in the fields, click **Submit**.

Result: A dialog box opens with the message **IP Address moved successfully!**

9 Click **OK**.

Result: The Node Hierarchy is updated to reflect the move and the IP Address Properties page opens.

END OF STEPS

Move an IP address to a different subnet

Purpose

Use this procedure to reassign an IPv6 address on an interface from one subnet to another.

Before you begin

You can move an IPv6 address to a different subnet after you have first searched for the node that currently contains the address and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To move an IPv6 address to a different subnet, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Enter search criteria to locate the node containing the interface with the IP address you want to move, as described in "Search for a node" (p. 11-3).

3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

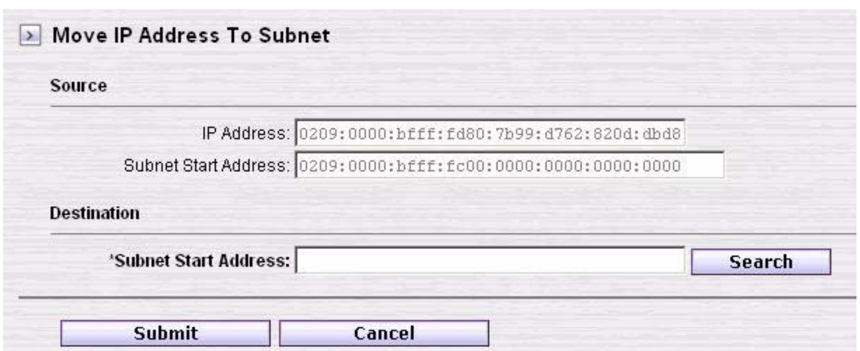
4 Expand the **Interfaces** node.

5 Expand the **IPv6 Addresses** node and select the IP address.

Result: The IP Address Properties page opens:

6 Click **Move to Subnet**.

Result: The Move IP Address To Subnet page opens.



7 Value the destination **Subnet Start Address** field.

Note: You can use the **Search** button to select a subnet for this field.

8 Click **Submit**.

Result: A dialog box opens with the message **IP Address moved successfully!**

9 Click **OK**.

Result: The Node Hierarchy is updated to indicate the IP address has been moved and the IP Address Properties page opens.

END OF STEPS

Delete an IP address from an interface

Purpose

Use this procedure to delete an IP address from an interface.

Before you begin

- You can delete an IP address from an interface after you have first searched for the node that currently contains the interface and used **Add To Hierarchy** to display it in the Node Hierarchy.
- You cannot change an IP address associated with an interface. You must delete it and add a new one.

Procedure

To delete an IP address associated with an interface, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Enter search criteria to locate the node containing the interface with the IP address you want to delete, as described in "Search for a node" (p. 11-3).

3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

4 Expand the node until the interface with the IP address you want to delete is visible.

5 Click the IP address.

Result: The IP Address Properties page opens:

6 Click **Delete**.

Result: A dialog box opens with the message **Are you sure you want to delete the selected IP Address?**

7 Click **OK**.

Result: A dialog box opens with the message **IP Address deleted.**

8 Click **OK**.

END OF STEPS

Delete an interface

Purpose

Use this procedure to delete an interface.

Before you begin

You can delete an interface after you have first searched for the node that currently contains it and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To delete an interface, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Enter search criteria to locate the node containing the interface you want to delete, as described in "Search for a node" (p. 11-3).

3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

4 Expand the node and select the interface you want to delete.

Result: The Interface Properties page opens.

5 Click **Delete**.

Result: A dialog box opens with the message **Are you sure you want to delete the selected Interface?**

6 Click **OK**.

Result: A dialog box opens with the message **Interface deleted.**

7 Click **OK**.

Result: The Node Hierarchy is updated.

END OF STEPS

Add a domain name to an IPv4 or IPv6 address

Purpose

Use this procedure to add a domain name to an interface's IPV4 or IPv6 address.

Before you begin

You can add a domain name to an IPv4 or IPv6 address after you have first searched for the node that contains the address and used **Add To Hierarchy** to display the node in the Node Hierarchy.

Procedure

To add a domain name to an interface's IPv6 address, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens with the Node Search page.

2 Enter search criteria to locate the node containing the interface with the address to which you want to add a domain name, as described in "Search for a node" (p. 11-3).

3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

4 Expand the node until the interface to which you want to add a domain name is visible.

5 Expand the **Interfaces** node.

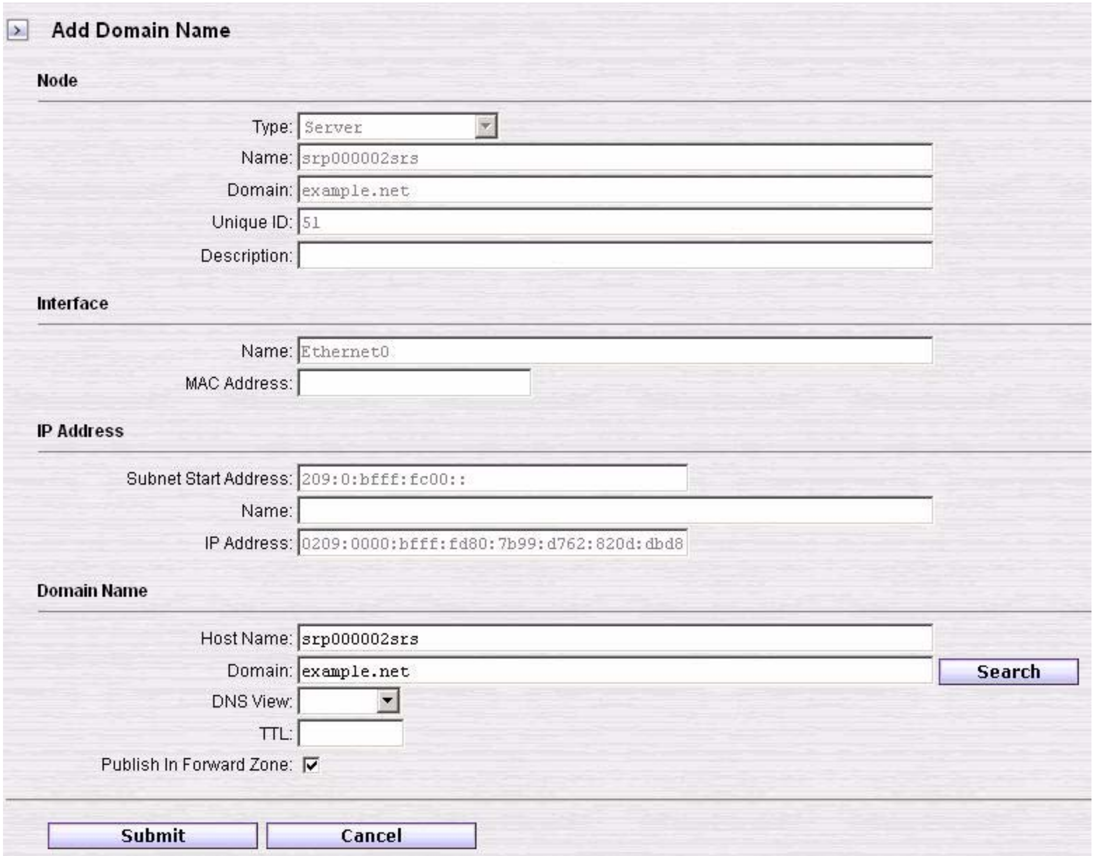
6 Expand the **IPv4 Addresses** or **IPv6 Addresses** node

7 Select the IP address to which you want to add a domain.

Result: The IP Address Properties page opens.

8 Click **Add Domain Name**.

Result: The Add Domain Name page opens.



Note: The Node, Interface and IP Address fields on this page are read-only.

9 Enter the appropriate values in the fields. Refer to the following table for a description of the fields.

Table 11-9 Add Domain Name fields

Field	Description
Host Name	***Required***. Enter a host name. You must enter a value in this field, the **Domain** field or both fields.
Domain	***Required.*** A domain name in the **Domain** field. You must enter a value in this field, the **Host Name** field, or both. Click **Search** to find a list of available domains. **Note:** If this name is in a DNS View, selecting the DNS. Only view-specific zones in the selected view are returned.

Field	Description
TTL	***Optional.*** A Time To Live value. A blank value indicates that it uses the default TTL.
DNS View	***Optional.*** Assigns the name to a specific DNS View. Assigning the Domain Name to a DNS View is not enough to guarantee the name is published in DNS. Once a DNS View is assigned, this name only appears in a view specific zone and not in a shared zone. The DNS View can only be set when adding the Domain Name; it cannot be changed by a modify operation.
Publish in Forward Zone	*Optional.* Publishes a forward zone record for this domain name in DNS.
Publish in Reverse Zone	***Optional.*** Publishes a reverse zone record for this domain name in DNS.

10 Click **Submit**.

Result: A dialog box opens with the message **Domain Name created.**

11 Click **OK**.

Result: The domain is added to the IP address in the Node Hierarchy and the Domain Name Properties page opens.

END OF STEPS

Modify a domain name on an IPv4 or IPv6 address

Purpose

Use this procedure to modify a domain name associated with an interface's IPv4 or IPv6 address.

Before you begin

You can modify a domain name on an IPv4 or IPv6 address after you have first searched for the node and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To modify a domain name on an interface's IPv4 address or IPv6 address, follow these steps.

1. Mouse over **Address Management** and select **Node**.

    Result: The Node Hierarchy opens with the Node Search page.

2. Enter search criteria to locate the node containing the interface with the address that needs a domain name change, as described in "Search for a node" (p. 11-3).

3. Click **Add To Hierarchy** and select the node in the Node Hierarchy.

4. Expand the node until the interface with the address that needs a domain name change is visible.

5. Expand the **Interfaces** node.

6. Expand the **IPv4 Addresses** or **IPv6 Addresses** node.

7. Select the IP address that needs a domain name change.

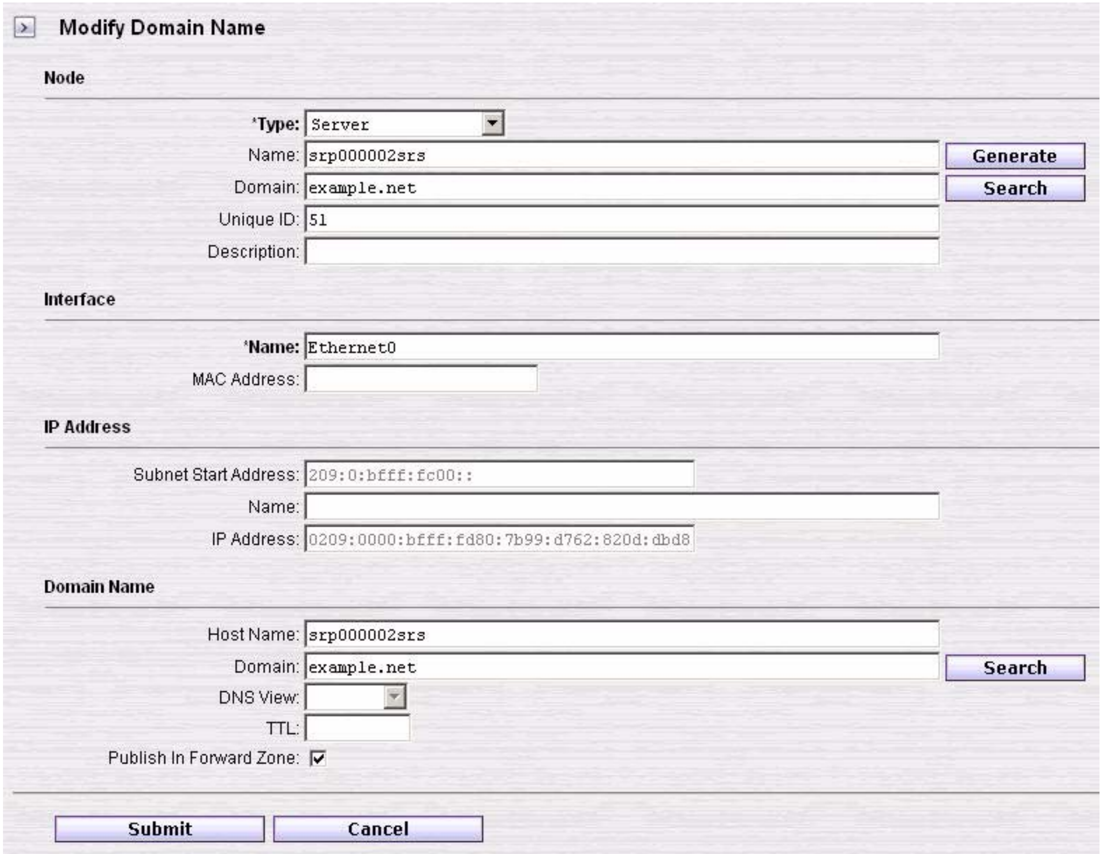
    Result: The **Names** node opens in the hierarchy.

8. Select the domain name.

    Result: The Domain Name Properties page opens.

9. Click **Modify**.

Result: The Modify Domain Name page opens.



10 Modify fields as required. Refer to Table 11-9, "Add Domain Name fields" (p. 11-41) for a detailed explanation of the fields on this screen.

11 Click **Submit**.

Result: A dialog box opens with the message **Domain Name modified.**

12 Click **OK**.

Result: The Node Hierarchy is updated and the Domain Name Properties page opens.

END OF STEPS

Delete a domain name from an IPv4 or IPv6 address

Purpose

Use this procedure to delete a domain name from an interface's IPv4 or IPv6 address.

Before you begin

Before you can delete a domain name from an address, you must first search for the node that contains the address, and display it in the Node Hierarchy.

Procedure

To delete a domain name from an interface's IP address, follow these steps.

1. Mouse over **Address Management** and select **Node**.

   Result: The Node Hierarchy opens with the Node Search page.

2. Enter search criteria to locate the node containing the interface with the address that needs a domain name to be deleted, as described in "Search for a node" (p. 11-3).

3. Click **Add To Hierarchy** and select the node in the Node Hierarchy.

4. Expand the node until the interface with the address that needs a domain name to be deleted is visible.

5. Expand the **Interfaces** node.

6. Expand the **IPv4 Addresses** or **IPv6 Addresses** node.

7. Select the IP address that needs a domain name to be deleted.

   Result: The **Names** node opens in the hierarchy.

8. Select the domain name.

Result: The Domain Name Properties page opens.

9 Click **Delete**.

Result: A dialog box opens with the message **Are you sure you want to delete the selected Domain Name?**

10 Click **OK**.

Result: A dialog box opens with the message **Domain Name deleted** and the domain name is removed from the Node Hierarchy.

11 Click **OK**.

END OF STEPS

Manage domain names in an IPv4 or IPv6 address

Purpose

Use this procedure to manage fully qualified domain names in IPv4 or IPv6 addresses.

Before you begin

You can manage a domain name in an IPv4 or IPv6 address after you have first searched for the node that contains the address and used **Add To Hierarchy** to display it in the Node Hierarchy.

Procedure

To manage domains in an IPv4 or IPv6 address, follow these steps.

1 Mouse over **Address Management** and select **Node**.

Result: The Node Hierarchy opens.

2 Enter search criteria to locate the node containing the interface with the address that needs a domain name to be managed, as described in “Search for a node” (p. 11-3).

3 Click **Add To Hierarchy** and select the node in the Node Hierarchy.

4 Expand the node until the interface with the address that needs a domain name to be managed is visible.

5 Expand the **Interfaces** node.

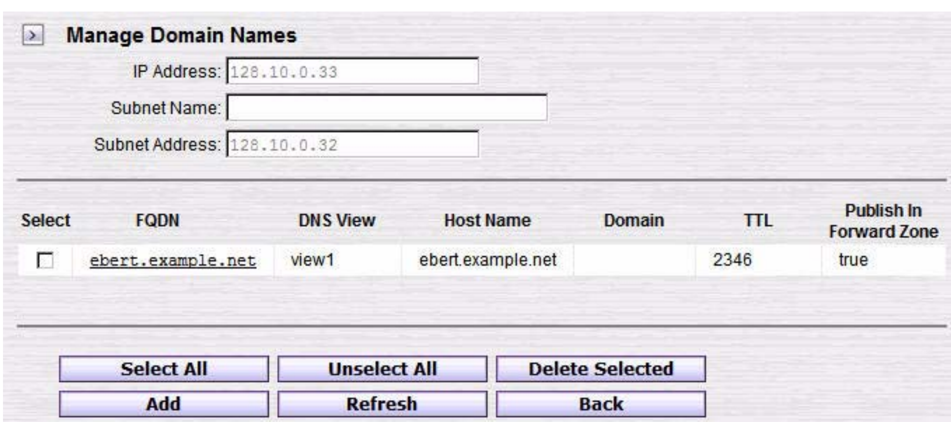
6 Expand the **IPv4 Addresses** or **IPv6 Addresses** node.

7 Select the IP address that needs a domain name to be managed.

Result: The IP Address Properties page opens.

8 Click **Manage Domain Names**.

Result: The Managed Domain Name page opens. The following is an example of an IPv4 Managed Domain Name page. The IPv6 Managed Domain Name page has **Subnet Start Address**, **IP Address Name**, and **IP Address** fields; these fields are read-only fields.



9 Choose an action.

If you want to...	Then...
Add a fully qualified domain name	1. Click **Add**. **Result:** The Add Domain Name page opens. Only fields in the the **Domain Name** section are enabled. 2. Enter the appropriate information in the Domain Name fields. Refer to Table 11-9, “Add Domain Name fields” (p. 11-41) for field descriptions. **Note: Publish in Reverse Zone** is not valid for fully qualified domain names. 3. Click **Submit**. **Result:** The domain name is added to the list.
Modify a fully qualified domain name	1. Click a domain name to modify. **Result:** The Domain Name Properties page opens. 2. Click **Modify**. **Result:** The Modify Domain Name page opens. 3. In the **Domain Name** section, modify the desired fields. Other fields in the page cannot be modified. 4. Click **Submit**. **Result:** A message opens stating if the changes were successful.
Delete a fully qualified domain name	1. Select the domain names from the list. 2. Click **Delete Selected**. **Result:** The domain name are removed from the list.
Select all fully qualified domain names	Click **Select All**. **Result:** All domain names in the list have the checkbox selected.
Unselect all fully qualified domain names	Click **Unselect All**. **Result:** All domain names in the list have the checkbox unselected.
Refresh the list	Click **Refresh**. **Result:** The domain names are updated.
Return to the previous page	Click **Back**. **Result:** You are returned to the previous page.

END OF STEPS

Part III: DNS administration

Overview

Purpose

The purpose is to provide information on DNS administration in VitalQIP.

Contents

This part includes these chapters.

12 ACL Template

Purpose

This chapter describes ACL Template management.

Contents

This chapter covers these topics.

ACL template administration

Overview

Purpose

VitalQIP provides a template mechanism to create and maintain Access Control Lists (ACLs). ACLs are written to the *named.conf* file.

Permissions

All administrators who have write access to at least one part of the infrastructure can add, modify, or delete ACLs. ACL templates are only available in the organization in which they are created.

Reports

The ACL Template Usage report can be accessed from the ACL Template Properties page.

ACL template hierarchy

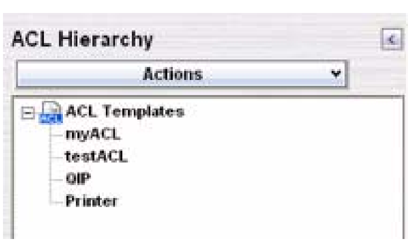
Description

The ACL Template page is a hierarchical a list of ACL templates.

Sample ACL Template Hierarchy

The following figure is an example of an ACL Template Hierarchy.

Figure 12-1 Sample ACL Hierarchy



Add an ACL template

Purpose

Use this procedure to create an ACL template.

Procedure

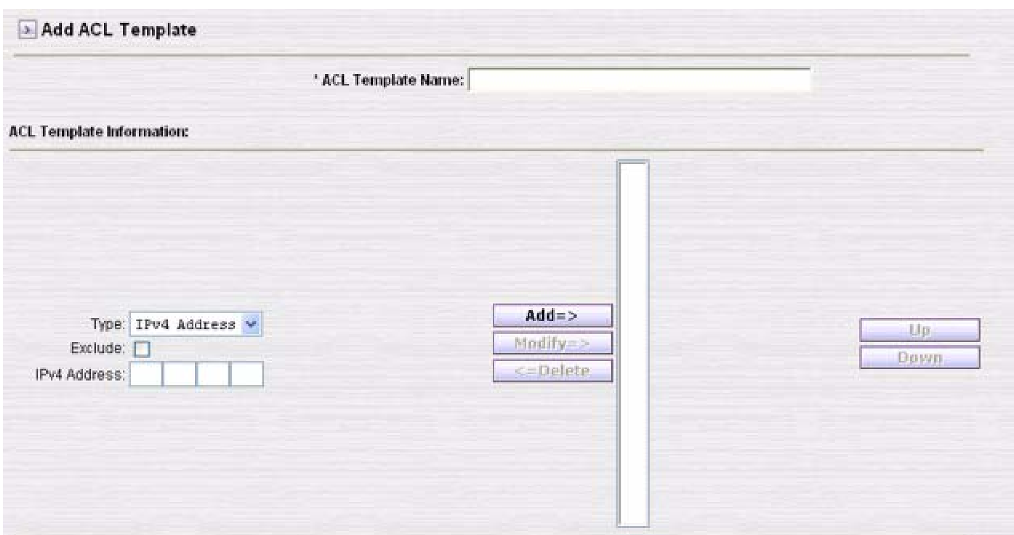
To add an ACL template, follow these steps:

1 Mouse over **DNS** and click **ACL Template**.

Result: The ACL Template Hierarchy opens.

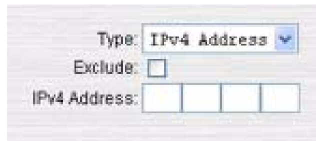
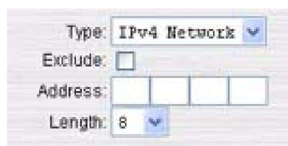
2 Mouse over the **Actions** menu and select **Add ACL Template**.

Result: The Add ACL Template page opens.



3 In the **ACL Template Name** field, enter the name for the ACL template.

4 Choose one of the following actions.

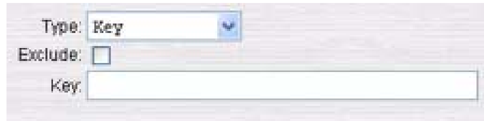
If you want to ...	**Then ...**
Add an IPv4 address ACL element	1. In **Type** field, select **IPv4 Address**. **Result:** IPv4 related fields are displayed.  2. Check **Exclude** if you wish to prevent access when matching this element. 3. In the **IPv4 Address** field, enter a IPv4 address. 4. Click **Add**. **Result:** The IPv4 address is added to the list.
Add an IPv4 network ACL element	1. In **Type** field, select **IPv4 Network**. **Result:** IPv4 network related fields are displayed.  2. Check **Exclude** if you wish to prevent access when matching this element. 3. In the **Address** field, enter a network address. 4. In the **Length** field, select the length of the network address. 5. Click **Add**. **Result:** The IPv4 network is added to the list.

If you want to ...	Then ...
Add an IPv6 address ACL element	1. In **Type** field, select **IPv6 Address**. **Result:** IPv6 address related fields are displayed.  2. Check **Exclude** if you wish to prevent access when matching this element. 3. In the **IPv6 Address** field, enter a IPv6 address. 4. Click **Add**. **Result:** The IPv6 address is added to the list.
Add a IPv6 network ACL element	1. In **Type** field, select **IPv6 Network**. **Result:** IPv6 network related fields are displayed.  2. Check **Exclude** if you wish to prevent access when matching this element. 3. In the **IPv6 Network** field, enter a network address. 4. In the **Length** field, select the length of the network address. 5. Click **Add**. **Result:** The IPv6 network is added to the list.

<table>
<tr><th>If you want to …</th><th>Then …</th></tr>
<tr><td>Add a nested ACL template element</td><td>
1. In **Type** field, select **ACL Template**.
Result: ACL Template related fields are displayed.


2. Check **Exclude** if you wish to prevent access when matching this element.
3. In the **ACL Template** field, enter an ACL template. Alternatively, you can search for an ACL template:
a. Click  to search.
Result: The ACL Search dialog box opens.


b. Enter a few letters of the ACL template name or wildcard.
c. Click **Search**.
d. Select the ACL template from the **Search Results** list.
e. Click **Select**.
Result: The ACL template is added to the **ACL Template** field.
4. Click **Add**.
Result: The ACL template is added to the list.
</td></tr>
</table>

If you want to …	Then …
Add a key ACL element	1. In **Type** field, select **Key**. **Result:** Key related field is displayed.  2. Check **Exclude** if you wish to prevent access when matching this element. 3. In the **Key** field, enter a key. 4. Click **Add**. **Result:** The key is added to the list.
Add other types of ACL elements	1. In **Type** field, select **Other**. **Result:** Other related fields are displayed.  2. Check **Exclude** if you wish to prevent access when matching this element. 3. In the **Other** field, select one of the following: - **localhost** - **localnets** - **text** 4. If you selected **Text**, enter the text in the **Text** field. 5. Click **Add**. **Result:** The element is added to the list.
Modify an ACL element	1. Select an ACL element from the list. **Result:** The fields are populated with the defined element information. 2. Make the appropriate changes. 3. Click **Modify**. **Result:** The element is updated in the list.
Delete an ACL element	1. Select an ACL element from the list. 2. Click **Delete**. **Result:** The element is deleted from the list.

If you want to ...	**Then ...**
Move an ACL element up and down in the list	1. Select an ACL element from the list. 2. Click: – **Up** to move the element one row up in the list – **Down** to moved the element one row down in the list.

5 Click **Submit**.

Result: A dialog box opens that states the ACL template was successfully added.

END OF STEPS

Modify or copy an ACL template

Purpose

Use this procedure to modify an ACL template. Alternatively, you can copy an ACL template to create new one.

Procedure

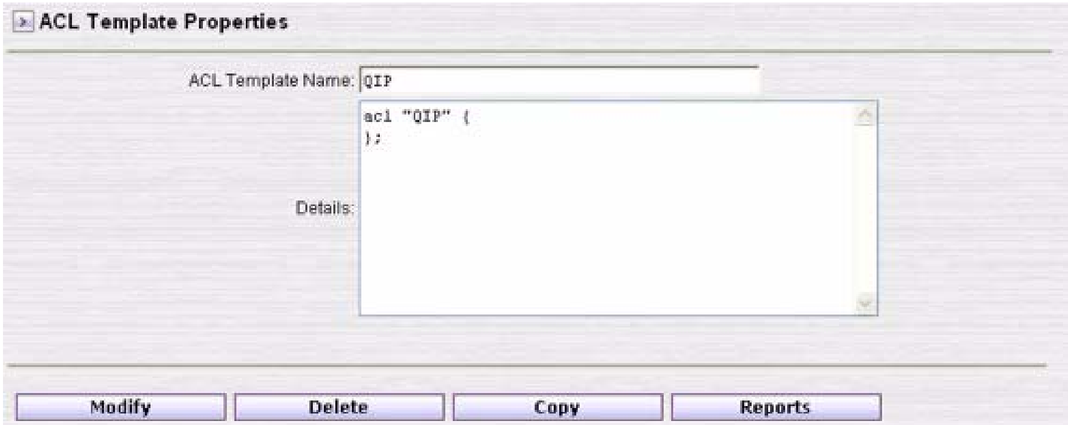
To modify or copy an ACL template, follow these steps:

1 Mouse over **DNS** and click **ACL Template**.

Result: The ACL Template Hierarchy opens.

2 Select an ACL template.

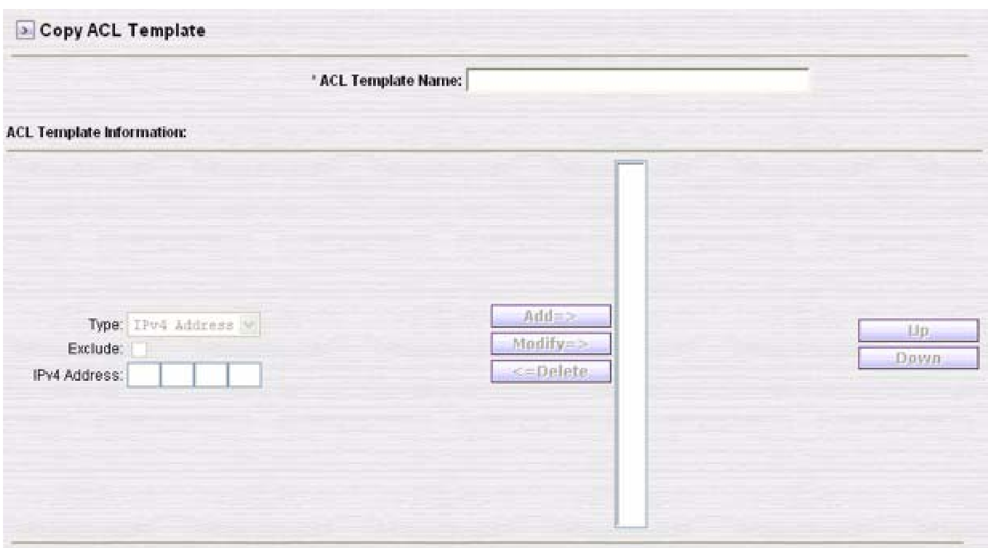
Result: The ACL Template Properties page opens.



3 If you want to:

- Modify an existing ACL template, click **Modify**.
- Copy the current ACL template, click **Copy**.

Result: The Modify ACL Template or Copy ACL Template page opens.



4 Make changes as needed. Refer to "Add an ACL template" (p. 12-3) for information on change ACL template information.

5 Click **Submit**.

Result: A dialog box opens that states if the ACL template was updated successfully.

END OF STEPS

Delete an ACL template

Purpose

Use this procedure to delete an ACL Template.

Before you begin

When you delete an ACL Template, references to the ACL Template are removed from DNS Views, zones, and servers.

Procedure

To delete an ACL Template, follow these steps:

1 Mouse over **DNS** and click **ACL Template**.

Result: The ACL Template Hierarchy opens.

2 Select an ACL Template.

Result: The ACL Template Properties page opens.

3 Click **Delete**.

Result: A dialog box asks you to confirm that you want to delete the ACL template. If the ACL is referenced in another ACL template, view, zone or reverse zone, an additional dialog box tells you that the ACL template you are deleting is being used, and asks you to confirm that you want to delete it.

If the ACL template is being referenced elsewhere, you can click **OK** to delete it, or click **Details** to go to the ACL Template Usage report.

4 Click **OK**.

Result: The ACL Template is deleted.

END OF STEPS

13 DNS Server

Overview

Purpose

The DNS Server function allows you to add and modify DNS Servers.

Contents

This chapter covers these topics.

DNS Server Hierarchy

Overview

Purpose

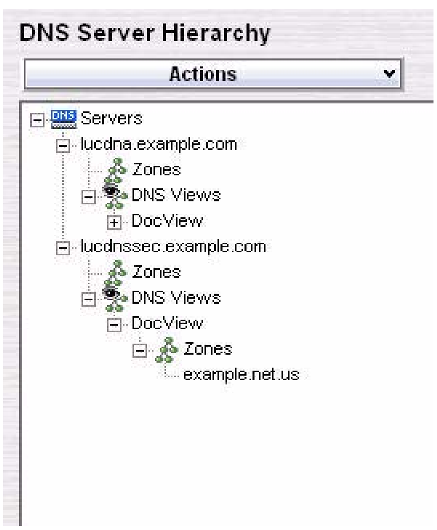
The DNS Server Hierarchy displays the managed zones in the hierarchy. If views are associated with the server, they are shown under the server in the hierarchy and the zones are displayed under the corresponding view name.

When you mouse over **DNS**, then select **DNS Server**, the DNS Server Hierarchy opens.

Under each server within the hierarchy are the zones associated with the server and a Views folder containing the views. Under each view is a list of zones associated with that view. If the number of zones extends beyond the foldering limit, the hierarchy groups zones in folders the same way the zone hierarchy is displayed.

The following is an example of a DNS Server Hierarchy:

Figure 13-1 DNS Server Hierarchy



DNS servers

To set up your DNS servers, you establish the name server configuration files with various options.

Notice that when you set up the Domain Profile and the optional Reverse Zone profile, you also establish various “Start of Authority” (SOA) options, as well as server and zone options by default.

If an organization's internal DNS server receives a query for a domain name for which it is not authoritative, by basic DNS operation, the name server will contact a root server to try to provide name resolution for the query.

Root name servers know where authoritative name servers are for all the top-level domains. The root domain is capable of directing a query for any domain in its *db.root* file, which is populated with all top-level domains. In addition, those top-level name servers can provide the list of name servers that are authoritative for the second-level domain in which the domain name resides. Each name server queried gives the querier information about how to get "closer" to the answer it is seeking, or provides the answer itself.

DNS configuration and data files

Your VitalQIP system may be set to generate the DNS configuration and data files automatically for a server at specified time(s) of day or a specified time interval (available through the "Scheduled Automatic Updates" parameter). If your VitalQIP system is not set up for automatic generation of DNS data, you can manually request VitalQIP to compile the data for a server and generate the DNS files.

Whenever the VitalQIP enterprise server performs an update to the DNS files, regardless of whether it is on a local or remote machine, or whether it is an Automatic Update or forced via **DNS**, VitalQIP uses temporary space in the *%QIPHOME%\tmp* directory of the target system. You need to ensure that you have enough *%QIPHOME%\tmp* (*$QIPHOME/tmp* on Unix machines) space to contain a copy of the DNS files. Once VitalQIP builds the files in the *%QIPHOME%\tmp* directory, they are moved to the location specified for that DNS server and the temporary files are deleted.

Remote DNS servers

If you want VitalQIP to manage primary and/or secondary DNS servers on your network that are physically separate from the VitalQIP server, the VitalQIP Remote Server software must be installed on them. The scope of each remote server is defined within VitalQIP. The VitalQIP Remote Service should be installed on any server running DNS or DHCP services. For further information on the VitalQIP Remote Service, refer to the *Administrator Reference Manual.*

> **Note:** A non-managed DNS server can be a secondary for a zone that is on a VitalQIP-managed Primary DNS server. In this case, the secondary DNS server does not necessarily need Remote Service, nor does it need to be defined in VitalQIP in either "Infrastructure/Server" or "Infrastructure/Non-Managed DNS Server". The

secondary server needs to have an NS record in the zone, unless it is being configured as a "stealth" name server. Refer to "Stealth Server zone options" (p. 14-35) for more information.

Add/modify DNS server

Purpose

Use this procedure when you want to add or modify a primary or secondary DNS server.

Procedure

Use the following steps to add or modify a DNS server:

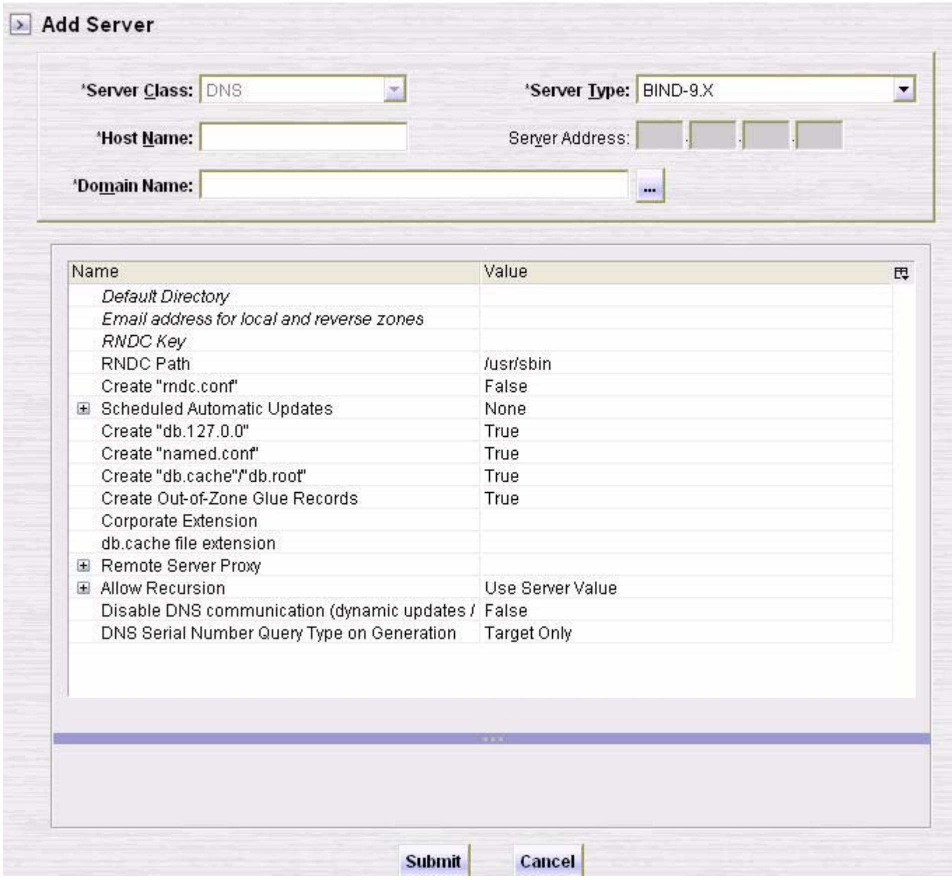
1 Mouse over **DNS** and select **DNS Server**.

Result: The DNS Hierarchy page opens.

2 To add a server, mouse over the **Actions** menu and select **Add Server**.

To modify a server, locate the server in the DNS Hierarchy and select it. When the Server Properties page opens, click **Modify**.

Result: The Server Information page opens.



- The screen contains default values if you are adding a server.
- The screen contains values for the server you selected if you are modifying a server.

3 Select a server type from the **Server Type** drop-down list in the following table.

Note: There are server types shown in the Server Type drop-down list that are no longer supported. VitalQIP allows you to import these server types but you cannot manage the servers in VitalQIP. You can change the server type when you modify the server. The following server types are no longer supported:

- BIND 4.9.x
- BIND-8.X
- LUCENT DNS 3.X
- MICROSOFT-NT4.0

The following table shows a list of server types available for DNS servers:

Table 13-1 DNS server types

Server type	Parameter tables
BIND-9.X	Table 13-2, "DNS BIND-9 parameters" (p. 13-7)
LUCENT DNS 4.X	Table 13-3, "LUCENT DNS 4.X parameters" (p. 13-11)
WINDOWS 2000 DNS	Table 13-4, "Windows 2000 DNS parameters" (p. 13-15)

4 In the **Host Name** field, enter either a new or existing server host name. You can enter a maximum of 63 alphanumeric characters beginning with an alphanumeric. The host name can include the dash (-) character, but cannot contain plus signs (+), exclamation marks (!), or underscores (_).

5 Enter a domain in the **Domain Name** field, or click ... to open the Domain Search window and select a domain from the search results.

6 Once the Server Type is selected (Step 3 above), a set of parameters appears in the **Parameters/Values** list. Fill in the values for all associated parameters and click **OK**. The confirmation prompt opens with the message **Server saved**.

7 Click **OK** and the Server Profile window closes as the profile is saved.

END OF STEPS

BIND-9 DNS server type

BIND 9 server parameters are identical to the BIND 8.x server type except for the addition of a new parameter called "RNDC Key". This key value is placed in *named.conf* so that **`rndc`** can communicate with the DNS server. See the *Administrator Reference Manual* for information on BIND 9 or refer to information on BIND 9 at the Internet Software Consortium website at **www.isc.org**.

The following table describes the parameters for DNS BIND 9 server type. Items in **bold** in the Options column of the table are defaults.

Table 13-2 DNS BIND-9 parameters

Parameters	Value type	Options	Usage
Default Directory	Text		***Required.*** Location of the DNS data files specified with a fully-qualified path name. On Windows-based systems this must be set to the BIND-9 installation *\etc* subdirectory (for example, *c:\BIND9\install\etc*). Refer to the registry entry **`HKEY_LOCAL_MACHINE\SOFTWARE\ISC\BIND`** if necessary.
Email address for local and reverse zones	Text		***Required***. This is the mail address that appears in the SOA record of a zone file.
RNDC Key	Text	True or **False**	Enter the value of the key to be placed in the *named.conf* file, which allows the **`rndc`** tool to restart the DNS server.
RNDC Path	Text		Enter the pathname for the **`rndc`** executable.
Create "rndc.conf"	Boolean	**True** or False	When set to True, creates an *rndc.conf* file using the value for the RNDC Key parameter. This is required when reloading zone information for the local DNS server. When pushed on a Microsoft platform, the file is pushed to the *\etc* directory with the *name.conf* file. When pushed on UNIX and Linux platforms, *rndc.conf* is root read-only by default, although this setting is controlled by the RootReadOnlyNamedConf parameter in the *qip.pcy* file (refer to the *Administrator Reference Manual*). This parameter defaults to False on existing Bind 9 servers that have been upgraded from previous VitalQIP releases.

Parameters	**Value type**	**Options**	**Usage**
DNSSEC enabled server	Boolean	True or **False**	When the parameter is set to True and the user exit is configured (described in the "Configure DNSSEC Support" section of the *Administrator Reference Manual*), a DNS push using the DNS Generation function to the DNSSEC-enabled server signs the zones of the DNSSEC-enabled server using configured keys. All parent zones are updated with DS records of child zones and signed, hence establishing a chain of trust.
Scheduled Automatic Updates	Time Interval or Time of Day	By Day, By Interval, **None**	Selecting By Day or By Interval causes VitalQIP to compile the DNS resource records automatically at the specified time(s) of day or time interval (minimum of one hour). These records are saved in multiple files in the directory defined in the Default Directory parameter. Zone files are generated for primary servers only. **Note:** A limit of six parameters is allowed. For automatic updates of DNS to take effect, an IP address must have been assigned to each domain's primary server through the **Manage objects** function. If this parameter is set to None, administrators can manually request VitalQIP to generate the DNS data for a single domain or all domains. The file is sent to the specified Default Directory (refer above for details).
Create "db.127.0.0"	Boolean	**True** or False	If you select True for this parameter, the *db.127.0.0* file is generated when a **DNS** > **DNS Generation** is performed. If the file exists, it is overwritten.
Create "named.conf"	Boolean	**True** or False	If you select True for this parameter, the *named.conf* file is generated when a **DNS** > **DNS Generation** is performed. If the file exists, it is overwritten.

Parameters	Value type	Options	Usage
Create “db.cache”/”db.root”	Boolean	**True** or False	If you select True for this parameter, the *db.cache* and *db.root* files are generated when a **DNS** > **DNS Generation** is performed. If the server is ***not*** an internal root server, the *db.cache* file is created; if the server is an internal root server, the *db.root* file is created. If the files exist, they are overwritten.
Create Out-of-Zone Glue Records	Boolean	**True** or False	If set to True, glue records are only created if the name server is ***not*** in the current zone (or sub-zone).
Corporate Extension	Multi-Line Text		Directives, such as options logging and control statement or additional zones, to be used or managed by this server. Options should be included in an **`options {…}`** block. These additional options are covered in *DNS and BIND*, and the *Administrator Reference Manual*.
db.cache file extension	Multi-Line Text	User defined	This parameter allows you to enter additional entries, which appear at the beginning of the *db.cache* file. Use standard *db.cache* file format.
Remote Server Proxy	IP Address List	0.0.0.0	When a firewall prevents a client from pushing to a remote server, enter IP address(es) to a remote proxy server that has access to the remote server through the firewall. Use the **Description** field to describe how the remote server is used. You can enter up to 255 characters. You can use this field, for example, to keep track of which proxies are configured to accept secure connections.

Parameters	**Value type**	**Options**	**Usage**
Allow Recursion	Text	Yes, No, Use List, **Use Server Value, ACL Templates, Other**	This parameters determines if recursion is allowed for the remote proxy server. These values can be used: • **Yes** - allows recursion for the server. • **No** - disables recursion for the server. • **Use Server Value** - allows the DNS server to use its own default. • **Use List** - allows the administrator to specify a list of IP addresses from which the server will allow recursive queries. This option has two sub-parameters: • **ACL Templates** - allows the administrator to pick from the set of allowed addresses from the list of pre-defined ACL templates. • **Other** - allows the user to type addresses that are not specified by an ACL Template.
Disable DNS communication (dynamic updates / SOA queries) from QIP	Boolean	True or **False**	When set to True, the VitalQIP client does not attempt to send dynamic updates to the DNS server or query for serial numbers on DNS generation. Also, the **`qip-genddsnconfs`** command does not include this server in the *ddns.conf* file that it generates for the DNS Update Service.
DNS Serial Number Query Type on Generation	Text	None, All Primaries, **Target Only**	This parameter determines which servers are queried to determine the serial number of a zone. These values can be used: • **None** - does not do SOA queries during the push. Useful if there are no secondary servers defined. • **All Primaries** - queries all primary servers for the SOA serial number. Required if there are secondary servers that point to more than one primary server. • **Target Only** - queries only the DNS server that is being pushed to. Useful for organizations whose secondary servers point to only one primary server.

LUCENT DNS 4.X server type

The following table describes the parameters for the LUCENT DNS 4.X server type. Items in **bold** in the Options column of the table are defaults.

Note: Selecting this version of BIND DNS establishes *named.conf* as your DNS configuration file.

Table 13-3 LUCENT DNS 4.X parameters

Parameters	Value type	Options	Usage
Default Directory	Text		***Required.*** Location of the DNS data files specified with a fully-qualified path name. On Windows-based systems, this includes the drive letter (for example, *c:\qip\named*).
Email address for local and reverse zones	Text		***Required***. This is the mail address that appears in the SOA record of a zone file.
RNDC Key	Text		Enter the value of the key to be placed in the *named.conf* file, which allows the **`rndc`** tool to restart the DNS server.
RNDC Path	Text		Enter the pathname for the **`rndc`** executable.
Create "rndc.conf"	Boolean	**True** or False	When set to True, creates an *rndc.conf* file using the value for the RNDC Key parameter. This is required when reloading zone information for the local DNS server. When pushed on a Microsoft platform, the file is pushed to the *\etc* directory with the *name.conf* file. When pushed on UNIX and Linux platforms, *rndc.conf* is root read-only by default, although this setting is controlled by the **`RootReadOnlyNamedConf`** parameter in the *qip.pcy* file (refer to the *Administrator Reference Manual*). This parameter defaults to False on existing Lucent DNS 4.X servers that have been upgraded from previous VitalQIP releases.
DNSSEC enabled server	Boolean	True or **False**	When the parameter is set to True and the user exit is configured (described in the "Configure DNSSEC Support" section of the *Administrator Reference Manual*), a DNS push using the DNS Generation function to the DNSSEC-enabled server signs the zones of the DNSSEC-enabled server using configured keys. All parent zones are updated with DS records of child zones and signed, hence establishing a chain of trust.

Parameters	**Value type**	**Options**	**Usage**
Secure DNS Updates	Boolean	True or **False**	If set to True, three sub-parameters must also be set to True or False: • **Use Domain as Realm** If set to True, VitalQIP uses the server's DNS domain name for the domain of the server's Kerberos principal name. If set to False, you can specify a different realm name with the **Override Realm** parameter. • **Use GSS Interop Flags Default** This parameter should be left at True since it is designed to permit support of legacy software. Do not change it without first contacting VitalQIP Technical Support. • **Use GSS Max Contexts Default** The maximum number of security contexts that the server can have active at a time. The default is 5,000. Set to False only if a server has a very high volume of active contexts, and enter a new value with the **GSS Max Contents** parameter.
RR Set Ordering	No, Use Server Value, Yes	No, **Use Server Value**, Yes	The order in which the DNS Server returns resource records in response to a client lookup. You can select one of the following: • **Yes** - indicates the ordering is of a random cyclic type. • **No** - indicates the ordering is a fixed order (the order in which the resource records are written in the zone). • **Use Server Value** - uses the server default value.
Allow-Secondary-Update	No, Use Server Value, Yes	No, **Use Server Value**, Yes	Indicates whether the secondary server can accept dynamic updates.

Parameters	**Value type**	**Options**	**Usage**
Scheduled Automatic Updates	Time Interval or Timeof Day	By Day, By Interval, **None**	Selecting By Day or By Interval causes VitalQIP to compile the DNS resource records automatically at the specified times of day or time interval (minimum of one hour). These records are saved in multiple files in the directory defined in the Default Directory parameter. Zone files are generated for primary servers only. **Note:** A limit of six parameters is allowed. For automatic updates of DNS to take effect, an IP address must have been assigned to each domain's primary server through the **Manage objects** function. If this parameter is set to None, administrators can manually request VitalQIP to generate the DNS data for a single domain or all domains. The file is sent to the specified Default Directory.
Create "db.127.0.0"	Boolean	**True** or False	If you select True for this parameter, the *db.127.0.0* file is generated when a **DNS** > **DNS Generation** is performed. If the file exists, it is overwritten.
Create "named.conf"	Boolean	**True** or False	If you select True for this parameter, the *named.conf* file is generated when a **DNS** > **DNS Generation** is performed. If the file exists it is overwritten.
Create "db.cache"/ "db.root"	Boolean	**True** or False	If you select True for this parameter, the *db.cache* and *db.root* files are generated when a **DNS** > **DNS Generation** is performed. If the server is ***not*** an internal root server, the *db.cache* file is created; if the server is an internal root server, the *db.root* file is created. If the files exist, they are overwritten.
Create Out-of-Zone Glue Records	Boolean	**True** or False	If set to True, glue records are only created if the name server is ***not*** in the current zone (or sub-zone).
Corporate Extension	Multi-Line Text		Directives, such as options logging and control statement or additional zones, to be used or managed by this server. Options should be included in an **`options {…}`** block. These additional options are covered *DNS and BIND*, and the *Administrator Reference Manual*.
db.cache file extension	Multi-Line Text	User defined	This parameter allows you to enter additional entries, which appear at the beginning of the *db.cache* file. Use standard *db.cache* file format.

Parameters	Value type	Options	Usage
Remote Server Proxy	IP Address List	0.0.0.0	When a firewall prevents a client from pushing to a remote server, enter IP addresses to a remote proxy server that has access to the remote server through the firewall. Use the **Description** field to describe how the remote server is used. You can enter up to 255 characters. You can use this field, for example, to keep track of which proxies are configured to accept secure connections.
Allow Recursion	Text	Yes, No, Use List, **Use Server Value**	This parameters determines if recursion is allowed for the remote proxy server. These values can be used: • **Yes** - allows recursion for the server. • **No** - disables recursion for the server. • **Use Server Value** - allows the DNS server to use its own default. • **Use List** - allows the administrator to specify a list of IP addresses from which the server will allow recursive queries. This option has two sub-parameters: • **ACL Templates** - allows the administrator to pick from the set of allowed addresses from the list of pre-defined ACL templates. ACL templates are defined in the VitalQIP thick client. • **Other** - allows the user to type addresses that are not specified by an ACL Template.
Disable DNS communication (dynamic updates / SOA queries) from QIP	Boolean	True or **False**	When set to True, the VitalQIP client does not attempt to send dynamic updates to the DNS server or query for serial numbers on DNS generation. Also, the **`qip-genddsnconfs`** command does not include this server in the *ddns.conf* file that it generates for the DNS Update Service.
DNS Serial Number Query Type on Generation	Text	None, All Primaries, **Target Only**	This parameter determines which servers are queried to determine the serial number of a zone. These values can be used: • **None** - does not do SOA queries during the push. Useful if there are no secondary servers defined. • **All Primaries** - queries all primary servers for the SOA serial number. Required if there are secondary servers that point to more than one primary server. • **Target Only** - queries only the DNS server that is being pushed to. Useful for organizations whose secondary servers point to only one primary server.

Windows 2000 DNS server type

The following table describes the parameters for the Microsoft Windows 2003 DNS server type. Items in **bold** in the Options column of the table are defaults. Also, refer to the *Administrator Reference Manual* on the configuration of Microsoft Windows 2003 DNS servers.

Table 13-4 Windows 2000 DNS parameters

Parameters	Value type	Options	Usage
Default Directory	Text		The default directory for the Windows server is *Read-Only*, and displays on the screen as *%systemroot%\system32\dns*.
Email address for local and reverse zones	Text	User defined	***Required***. This is the mail address that appears in the SOA record of a zone file.
Boot Method	Text	**File** or Directory	If you are booting from file, all zones are file-based. If you are booting from a directory, all zones are directory-based. When booting from Active Directory, any parameters not specified in the Active Directory are taken from the Registry. When booting from disk, any parameters not specified in the boot file are taken from the Registry. If you select Directory, you can expand this parameter to set up secure zones for Windows 2003 DNS. The parameters are as follows:
Secure DNS Updates	Boolean	True or **False**	If **Boot Method** is set to Directory, secure DNS updates for Windows 2003 DNS can be enabled. When the parameter is set to True, the following parameters are shown.
Proxy Kerberos Principal Name	Alpha-numeric		This is the user login name of the proxy user.
Proxy Kerberos Principal Password	Alpha-numeric		This is the password of the proxy user.
Strong Kerberos Principal Name	Alpha-numeric		This is the user login name of the strong user.
Strong Kerberos Principal Password	Alpha-numeric		This is the password of the strong user.

Parameters	**Value type**	**Options**	**Usage**
Use server DNS domain as Active Directory domain	Boolean	**True** or False	Determines if the server uses the DNS domain as the Active Directory domain. If this parameter is set to False, the following parameter is shown.
Active Directory Domain	Text		The domain used by Active Directory.
Scheduled Automatic Updates	Time Interval or Timeof Day	By Day, By Interval, **None**	Selecting By Day or By Interval causes VitalQIP to compile the DNS resource records automatically at the specified times of day or time interval (minimum of one hour). These records are saved in multiple files in the directory defined in the Default Directory parameter. For automatic updates of DNS to take effect, an IP address must have been assigned to each domain's primary server through the **Manage objects** function. If this parameter is set to None, administrators can manually request VitalQIP to generate the DNS data for a single domain or all domains. The file is sent to the specified Default Directory.
Create "db.127.0.0"	Boolean	True or **False**	Windows DNS servers do not allow the removal or modification of the 127.in-addr.arpa zone. This option must be set to False.
Create "boot"	Boolean	**True** or False	This parameter is specific to the selection of Microsoft Server as the Server Vendor/Version. If you select True for this parameter, the boot file is generated when a **DNS** > **DNS Generation** is performed. If the file exists, it is overwritten.
Create "db.cache"/"db.root"	Boolean	**True** or False	If you select True for this parameter, the *db.cache* and *db.root* files are generated when a **DNS** > **DNS Generation** is performed. If the server is ***not*** an internal root server, the *db.cache* file is created; if the server is an internal root server, the *db.root* file is created. If the files exist, they are overwritten.
Create Out-of-Zone Glue Records	Boolean	**True** or False	If set to True, glue records are only created if the name server is ***not*** in the current zone (or sub-zone).
Disable Recursion	Boolean	**True** or False	This option determines whether or not the server does recursive lookups.

Parameters	Value type	Options	Usage
Round Robin	Boolean	True or **False**	This option determines whether the server round robins multiple A records.
Scavenging Interval	Numeric in hours	0	This period specifies how often a DNS server is enabled for scavenging to remove stale records. The default of zero indicates that scavenging is not set.
Prefix Corporate Extension	Multi-Line Text		Directives are required to be in **dnscmd** format and are executed at push time. Refer to your Microsoft documentation for more information.
Suffix Corporate Extension	Multi-Line Text		Directives are required to be in **dnscmd** format and are executed at push time. Refer to your Microsoft documentation for more information.
db.cache file extension	Multi-Line Text	User defined	This parameter allows you to enter additional entries, which appear at the beginning of the *db.cache* file. Use standard *db.cache* file format.
Remote Server Proxy	IP Address List	0.0.0.0	When a firewall prevents a client from pushing to a remote server, enter IP addresses to a remote proxy server that has access to the remote server through the firewall. Use the **Description** field to describe how the remote server is used. You can enter up to 255 characters. You can use this field, for example, to keep track of which proxies are configured to accept secure connections.
Disable DNS communication (dynamic updates / SOA queries) from QIP	Boolean	True or **False**	When set to True, the VitalQIP client does not attempt to send dynamic updates to the DNS server or query for serial numbers on DNS generation. Also, the **qip-genddsnconfs** command does not include this server in the *ddns.conf* file that it generates for the DNS Update Service.

Parameters	**Value type**	**Options**	**Usage**
DNS Serial Number Query Type on Generation	Text	None, All Primaries, **Target Only**	This parameter determines which servers are queried to determine the serial number of a zone. These values can be used: • **None** - does not do SOA queries during the push. Useful if there are no secondary servers defined. • **All Primaries** - queries all primary servers for the SOA serial number. Required if there are secondary servers that point to more than one primary server. • **Target Only** - queries only the DNS server that is being pushed to. Useful for organizations whose secondary servers point to only one primary server.
Server Startup Timeout (seconds)	Seconds	300 seconds	Determines the number of seconds to wait before the server fails a DNS push.

Clone a DNS server

Purpose

To clone a DNS server.

Before you begin

- A server can be cloned by master and organization administrators, as well as by normal administrators with write privileges for the server being cloned and a Create Infrastructure privilege setting of True.
- All DNS server options, including the relationship of the server with managed files and user-defined attributes (UDAs), are cloned.
- If you opt to clone zone associations, all associations relating to each zone (views, view zone options, push schedule, extensions, and zone options) are cloned. Forward zones, reverse zones, V4 zones, V6 zones are copied when **Clone Zone Associations** is selected. If a non-managed server has a relationship with any of the zones for the server that is being cloned, that relationship is copied to the new server as well.
- Both primary and secondary DNS servers can be cloned.
- User-defined fields (UDFs) cannot be cloned since they are associated with the IP address of the server, not the server itself.

- Non-managed servers cannot be cloned.
- When a server that is associated with a reverse zone template is cloned, the new server is not associated with that reverse zone template.

Procedure

To clone a DNS server, follow these steps.

1 Select **DNS Server** from the **DNS** menu.

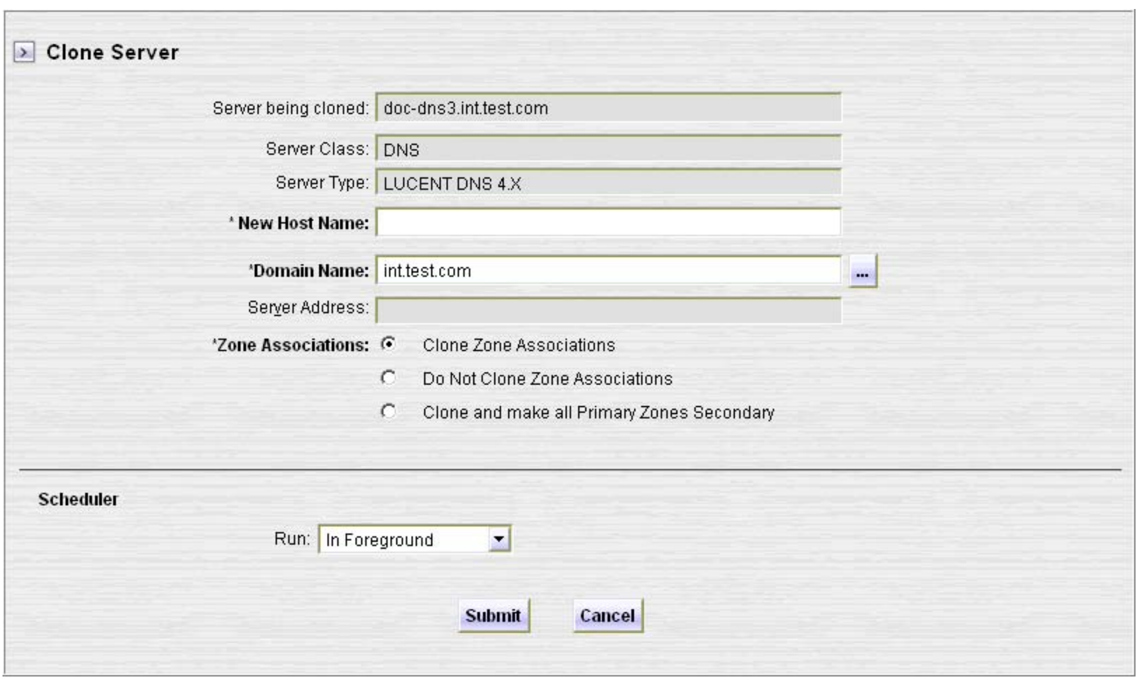
Result: The DNS Server Hierarchy opens.

2 Expand the DNS Servers list and select the server that you wish to clone.

Result: The Server Properties page opens.

3 Click **Clone**.

Result: The Clone Server page opens.



4 Enter a new server host name in the **New Host Name** field. You can enter a maximum of 63 characters, beginning with an alphanumeric. The host name can include the dash (-) character, but cannot contain plus signs (+), exclamation marks (!), or underscores (_).

5 Click to open the Domain Search window and select a domain from the search results.

6 Choose one of the following **Zone Associations** options.

- **Clone Zone Associations**

  Zones/zone options associated with the existing DNS server are cloned to the new DNS server. Both forward and reverse zones, as well as V4 and V6 zones are cloned. DNS Views information is copied, as well as the relationship of the server with managed files. The primary/secondary relationship between the server being cloned and the zone is maintained. If a non-managed server has a relationship with any of the zones for the server that is being cloned, that relationship is copied to the new server as well.

- **Do Not Clone Zone Associations**

  Zone associations are not cloned.

- **Clone and make all Primary Zones Secondary**

  Accomplishes the same result as the Clone Zone Associations option except that the server that results from the clone operation will be secondary for all the zones.

7 Choose one of the **Run** options in the **Scheduler** section. For information on Scheduler options, refer to "Scheduler" (p. 9-77).

8 Click **Submit**.

Result: If run in foreground, the server is cloned, the hierarchy is updated, and the properties of the new server are displayed. A dialog opens with the message **Server <server name> cloned successfully**.

Result: If run in background or scheduled for a later time/date, a dialog opens with the message **Cloning of server <server name> scheduled. Schedule Id=<##>. Continue to the job scheduler page? Click OK to proceed to the job scheduler or Cancel**.

END OF STEPS

Delete a DNS server

Purpose

Use this procedure to delete a DNS server.

Procedure

To delete a DNS server, follow these steps:

1 Select the DNS server you want to delete in the DNS Server Hierarchy.

Result: The Server Properties page opens.

2 Click **Delete**.

Result: A dialog box asks you to confirm that you want to delete the server.

3 Click **OK**.

Result: The server is deleted.

END OF STEPS

Non-managed DNS server

Overview

Purpose

The Non-Managed DNS Server function is designed to allow DNS servers that are defined by VitalQIP to act as secondary DNS servers for primary DNS servers that are not defined within the VitalQIP infrastructure.

For example, a domain, example.com, is managed by VitalQIP. Its DNS server is called DNS1, which is defined in a subnet that is under VitalQIP control. If another part of the organization has its own domain, say admin.example.com and they choose not to use VitalQIP to manage that domain, a server in the example.com domain can act as a secondary server for the admin.example.com domain.

Add/modify a non-managed DNS server

Purpose

Use this procedure to define or modify a non-managed DNS server.

Procedure

Use the following steps to create or modify a non-managed DNS server.

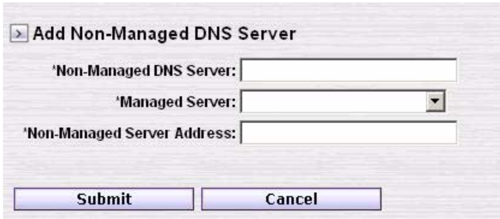
1. Mouse over **DNS** and select **Non-Managed DNS server**.

   Result: The Non-Managed DNS Server hierarchy opens.

2. To add a non-managed DNS server, mouse over **Actions** and select **Add Non-Managed DNS Server.**

   To modify an existing non-managed DNS server, find the server in the Non-Managed DNS Server hierarchy and select it. When the Server Properties page opens, select **Modify**.

Result: The Add or Modify Non-Managed Server page opens.



- The screen contains no values if you are adding a server.
- The screen contains values for the server you selected if you are modifying a server.

3 Enter or change values in the following fields

Table 13-5 Add Non-Managed Server fields

Field	Description
Non-Managed DNS Server	Enter the fully qualified name of the non-managed server. (64 characters maximum)
Managed Server	Select the VitalQIP defined server you wish to have as secondary to zones on this Non-Managed Server. This server must already be established.
Non-Managed Server Address	Enter the IP address of the non-managed server. This address must not be the same as that of any DNS server that is managed by VitalQIP.

4 Click **Submit**.

Result: The non-managed server is added or modified.

END OF STEPS

Add a zone to a non-managed server

Purpose

Use this procedure to add a zone to a non-managed server.

Procedure

Use the following steps to add a zone to a non-managed server:

1 Mouse over **DNS** and select **Non-Managed Servers**.

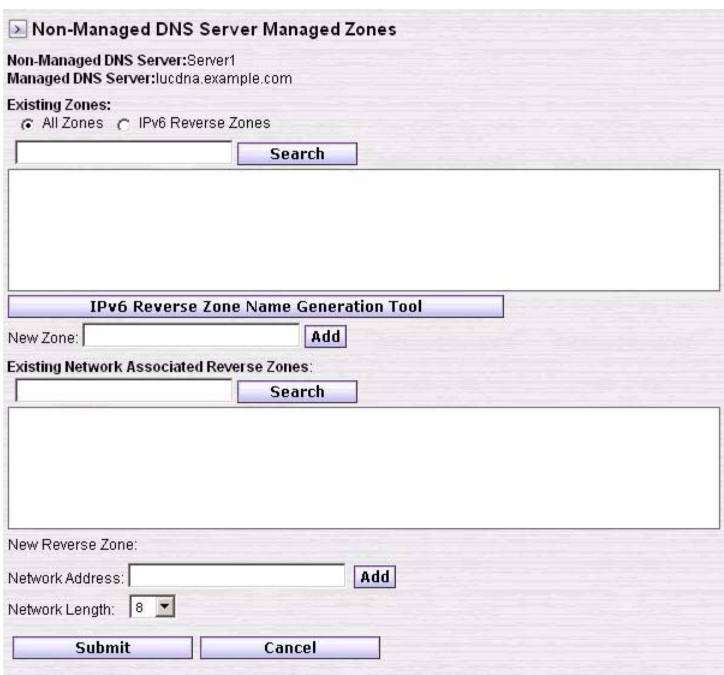
Result: The Non-Managed DNS Server Hierarchy page opens.

2 Find the server to which you want to add a zone and select it.

Result: The Non-Managed DNS Server page opens.

3 Click **Add Zones**.

Result: The Non-Managed DNS Server Managed Zones page opens.



4 Enter a zone name in the fields provided, or search for a zone using the values on this screen. Note the following:

- You must type in a prefix and select search to retrieve all the existing zones.
- Specifying a wildcard (* All Zones) has serious performance implications.

- Selecting **All Zones** lists all forward zones and IPv6 reverse zones, but selecting V6 Reverse Zones only lists IPv6 reverse zones,while selecting **Existing Network Associated V4 Reverse Zone** lists all IPv4 managed and non-managed reverse zones.
- Only CIDR notation is supported.

5 Click **Submit** when you have entered your search parameters.

Result: A list of available zones opens.

6 Select one or more zones to add to the server by clicking the checkbox next to the server name.

7 Click **Submit**.

Result: The zones are added to the server and appear as managed zones under the non-managed server in the Non-Managed DNS Server Hierarchy.

END OF STEPS

Add zone options to a non-managed server

Purpose

Use this procedure to establish zone options for a new domain or reverse zone on a non-managed DNS server.

Before you begin

- When you assign an existing zone to a non-managed DNS server, the zone options cannot be modified.
- When you assign a new zone to a non-managed DNS server, you can specify options for that zone. If that same zone is later assigned to another non-managed DNS server, the same zone options apply.

Procedure

To establish zone options on a non-managed server, use the following steps:

1 Mouse over **DNS** and select **Non-Managed Servers**.

Result: The Non-Managed DNS Server Hierarchy page opens.

2 Find a zone on the non-managed server to which you want to add zone options in the DNS Server Hierarchy and select it.

Result: The Non-Managed DNS Server Zone Properties page opens.

3 Click **Zone Options**.

Result: The Non-Managed Server Managed Zones page opens.

4 See "Set zone options" (p. 14-24) for specific information on setting zone options.

END OF STEPS

Delete a non-managed DNS server

Purpose

Use this procedure to delete a non-managed DNS server

Procedure

To delete a non-managed DNS server, follow these steps:

1 Select the non-managed DNS server you want to delete in the Non-Managed DNS Server Hierarchy.

Result: The Server Properties page opens.

2 Click **Delete**.

Result: A dialog box asks you to confirm that you want to delete the server.

3 Click **OK**.

Result: The server is deleted.

END OF STEPS

14 Zones

Overview

Purpose

This chapter describes the management of zones. This function allows you to add, modify, and delete forward, IPv4 reverse, and IPv6 reverse zones.

Contents

This chapter covers these topics.

About zones

Overview

Purpose

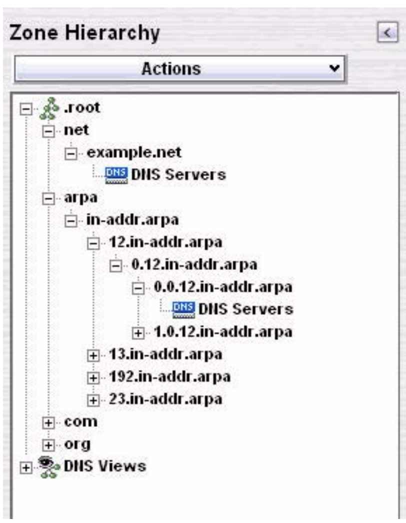
Zones can be defined through the **Zone** function on the **DNS** menu. VitalQIP organizes zones into a logical hierarchy under this function,

Zone hierarchy

Description

Zones appear in the Zone Hierarchy. The Zone Hierarchy appears as follows:

Figure 14-1 Zone Hierarchy



When the user selects a branch in the hierarchy that is a managed zone, the zone properties screen described in the following section is displayed. If the user selects a node that is simply an unmanaged zone label, then the splash screen is displayed.

> **Note:** Administrators can see all zones in the tree, however the action buttons will be grayed out and the SOA information will not be displayed when they select a zone for which they do not have admin privileges. Also, views are only visible in the hierarchy for master administrators.

The Zone Hierarchy allows you to switch the display between short names and fully-qualified names by selecting **Turn On/Off Fully-Qualified Names** from the **Actions** menu.

Define internal root zone for internal root server

In previous releases of VitalQIP, if you wanted to have a DNS server manage an internal namespace that was not connected to the Internet, you needed to set a root server flag in the server profile. In VitalQIP, the root zone is now a separate zone in the zone hierarchy. All zone options and SOA values are defined in the zone profile for that zone. To create the root zone, you simply need to create a root zone called "." (without the quotes). The root zone is not created by default since it is not commonly needed. If you create an internal root zone, the following conditions apply:

- When you add the root zone, a confirmation dialog box appears explaining that you are about to create a root DNS zone. You must click **Yes** to continue.
- Once a root zone is created, you cannot change the name.
- Renaming an existing zone to "." when it is not a root zone is not permitted.
- The root zone cannot be assigned to subnets or objects.
- The root zone only appears in the hierarchy and in the **Existing zone List** in the zone Option: Add window.
- The root zone cannot be created from the subnet profile.
- The push logic retrieves the SOA, options, and extensions for the root zone from the zone profile for the root zone.

Search for a zone

Purpose

This procedure allows you to search for a zone and display its properties.

Procedure

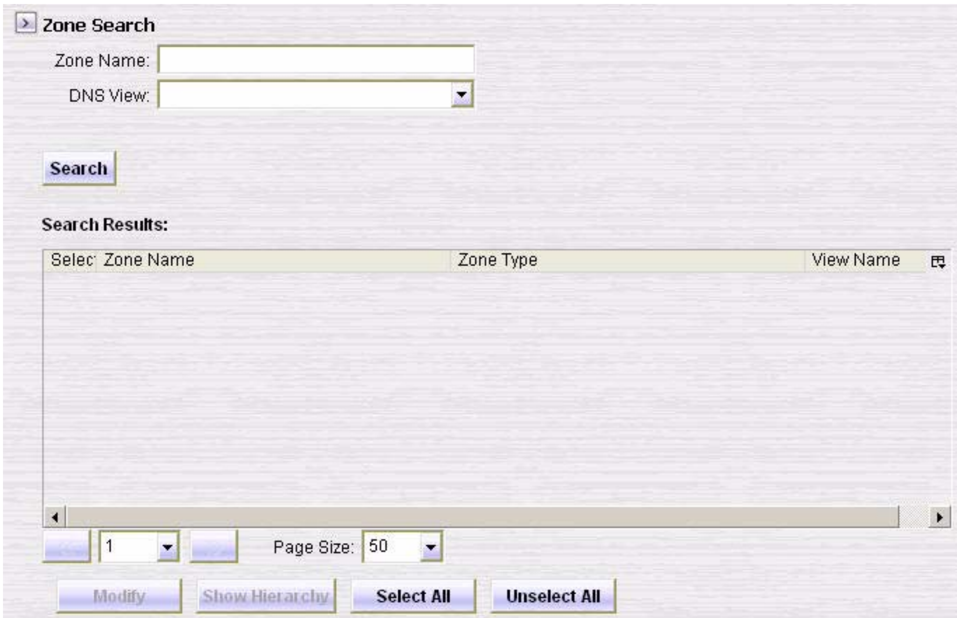
To search for a zone, follow these steps:

1 Mouse over **DNS** and select **Zone**.

Result: The Zone Hierarchy opens.

2 To search for a zone, mouse over the **Actions** menu and select **Zone Search**.

Result: The Zone Search page opens.



3 Enter the full or partial name of the zone for which you are searching in the **Zone Name** field.

Note: You can use the asterisk as a wildcard.

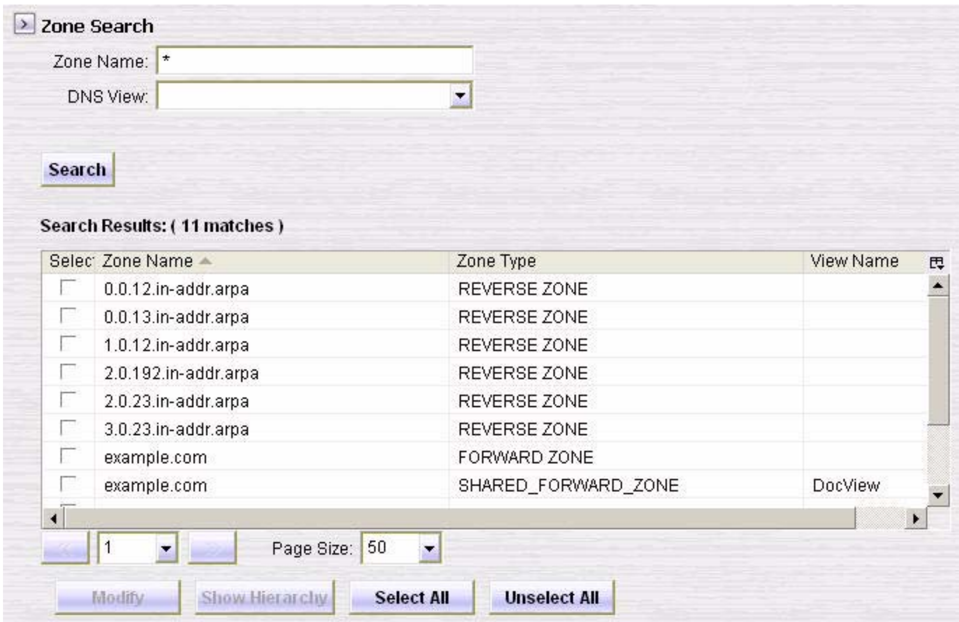
4 To specify a DNS View as a search option, select one of the following from the DNS View drop-down list.

Table 14-1 Search options

Value	Search Result
Blank (default)	Searches for all matching zones regardless of whether they are contained within a DNS View.
`None`	Searches for all matching zones that are not contained within a DNS View.
`Any`	Searches for all matching zones that are contained within any DNS View.
<viewname>	Searches for all matching zones that are only contained within the selected DNS View.

5 Click **Search**.

Result: All matching zones are displayed in the **Search Results** field.



6 Choose one of the following.

If you want to...	Then...
Select one or more zones	You can: • Select one or more zones by clicking the checkbox in the **Select** column • Select more than one zone by clicking holding the **Shift** key and clicking on one or more zone rows
Select multiple zones	Click **Select All**.
Unselect zones	Click **Unselect All**.
View zone properties	1. Select the zone for which you want to display properties. 2. Select **Show Hierarchy**. **Result:** The zone properties are displayed on the right side of the screen, and the zone is shown in the zone hierarchy on the left side of the screen.
Modify multiple zones	Refer to "Modify multiple zones" (p. 14-10) for more information.

END OF STEPS

Add/modify a zone

Purpose

Use this procedure to add a zone to which you want to assign subnets, servers, or objects.

Before you begin

You must have a zone defined before you can create a DNS server.

Procedure

To add or modify a zone, follow these steps:

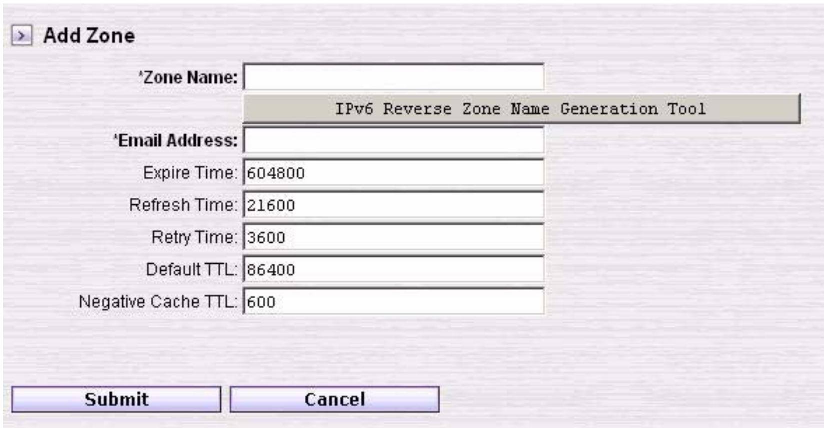
1 Mouse over **DNS** and select **Zone**.

Result: The Zone Hierarchy page opens in the left pane of the window.

2 To add a zone, mouse over the **Actions** menu and select **Add Zone**.

To modify a zone, locate the zone in the Zone Hierarchy and select it. When the Zone Properties page opens, click **Modify**.

Result: The Add Zone or Modify Zone page opens.



- The screen contains default values if you are adding a zone.
- The screen contains values for the zone you selected if you are modifying a zone.

3 Refer to the following table as you enter values in the fields on this page:

Table 14-2 Zone fields

Field	Description
Zone Name	***Required.*** Enter the name you are assigning to the zone. If you are adding an IPv6 reverse zone use the **IPv6 Reverse Zone Name Generation Tool** button to add a name. This button allows IPv6 reverse zones to be created. See "IPv6 Reverse Zone Tool" (p. 14-9) for additional information.
Email Address	***Required.*** Enter the email address of the person responsible for maintaining the zone.
Expire Time	***Required***. When the Expire Time is reached, the slave server will stop handing out information about the data because the data is too old to be useful. The default value for this expire time is 604,800 seconds (one week).

Field	Description
Refresh Time	***Required***. The refresh time dictates how often the secondary server should verify its data against the primary server. The default is 21,600 seconds (six hours).
Retry Time	***Required***. The retry time dictates the interval for attempting to refresh in the event that the primary server is unavailable. The default value is 3,600 seconds (one hour).
Default TTL	***Required***. The default TTL defines the time interval for other servers to cache all resource records in the database file if the TTL is not defined at the object level. The TTL (Time To Live) is supplied with query responses. The default value is 86,400 seconds (one day). With implementation of BIND 8.2.2-based code (Lucent DNS 3.0), RFC 2308 indicates the minimum time is applicable to negative responses and the $TTL directive is the minimum time for cache information.
Negative Cache TTL	***Required***. The Negative Cache TTL defines the amount of time to cache negative responses (that is, entries that do not exist). This field applies only to BIND 9-based servers (BIND 9.X and Lucent 4.X). A typical value is 600 seconds.

4 Click **Submit**.

Result: The zone is created or modified.

END OF STEPS

IPv6 Reverse Zone Tool

You can create reverse zone options for IPv6 by doing the following:

1 Click **IPv6 Reverse Zone Name Generation Tool**.

Result: The IPV6 Reverse Zone Generation screen opens.

.

2 In the **IPv6 Address/Length** field, enter the IPv6 address and the prefix-length in IPv6 address/prefix-length format. For example, **`fec0:0:0:1::/64`**. Note that no more than 43 characters are allowed, only hexadecimal values, **`:`**, and **`/`** for the prefix-length are allowed, and the prefix-length must be divisible by four.

3 The address must be validated and converted to a reverse zone address. To do so, click **Generate**.

Result: The address is validated. If the address is valid, a value is displayed in the **Zone Name** field, such as `1.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa`.

4 To add the reverse zone name to the **Zone Name** field of the Zone Profile screen, click **OK**.

END OF STEPS

Modify multiple zones

Purpose

Use this procedure to modify multiple zones.

Before you begin

- Only multiple forward zones or reverse zones can be modified at a time. You cannot modify both multiple forward and reverse zones at the same time.
- Modifying multiple zones is only supported for forward and reverse zones.

Procedure

To modify multiple zones, follow these steps.

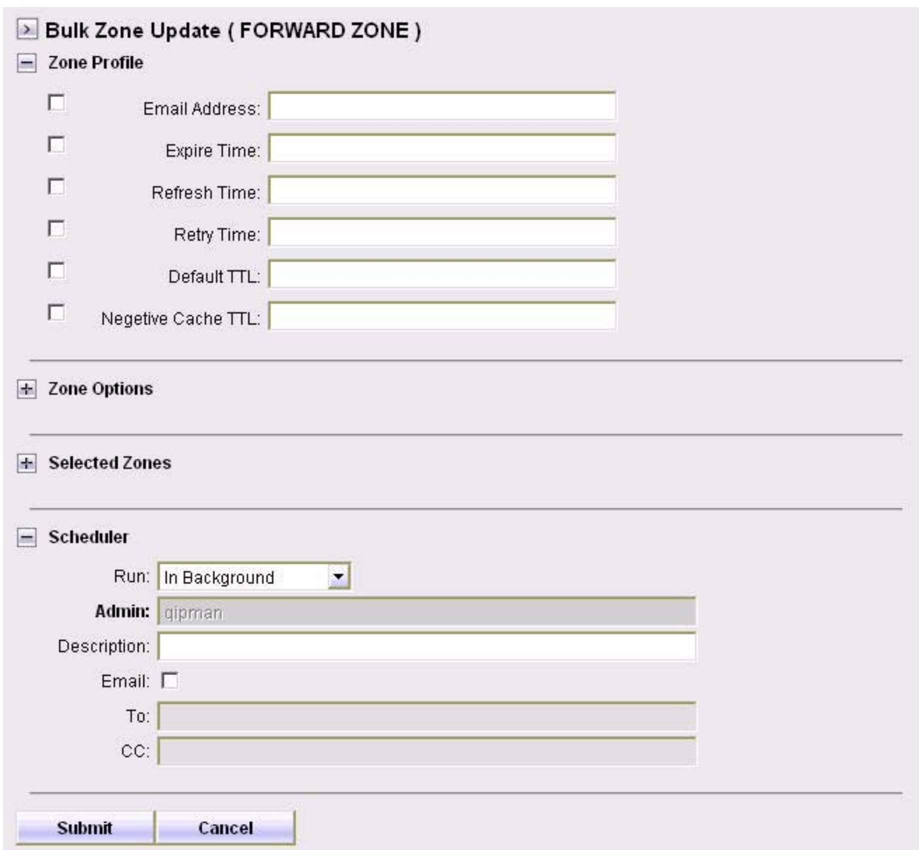
1 Search for the zone you want to modify. Refer to "Search for a zone" (p. 14-4) for more information.

Result: The Search Results are displayed.

2 Select the zones you wish to modify. Use the **Shift** and **Ctrl** keys to select multiple zones.

3 Click **Modify**.

Result: The Bulk Zone Update page opens.



4 Choose the following.

If you are...	Then...
Modifying a value	1. If necessary, expand the **Zone Profile** section. 2. Place checkmarks beside the fields you wish to modify. 3. Make the appropriate changes to the selected fields. Refer to Table 14-2, "Zone fields" (p. 14-8) for description of the fields.
Modifying options for a DNS zone	1. Expand the **Zone Options** section. 2. Expand the zone option you wish to modify. 3. Place a checkmark in the **Select** column beside any field you wish to modify. 4. Make the appropriate changes to the selected fields. Refer to the following for more information on zone option values: • "Extensions zone options" (p. 14-25) • "BIND 8.X zone options" (p. 14-26) • "BIND 9.X zone options" (p. 14-28) • "LUCENT DNS 3.X zone options" (p. 14-30) • "LUCENT DNS 4.X zone options" (p. 14-32) • "Windows 2000 DNS Zone Options" (p. 14-34)
Viewing zones being modified	Expand **Selected Zones** section.
Modify user defined attributes	Refer to "Use user defined attributes as search criteria" (p. 7-26) for more information.
Modify user defined fieds	Refer to "Use user defined fields as search criteria" (p. 7-25) for more information.
Scheduler	Refer to "Scheduler" (p. 9-77) for more information.

5 Click **Submit**.

Result: A confirmation dialog opens.

6 Click **OK**.

Result: The confirmation dialog closes.

END OF STEPS

Delete a zone

Purpose

Use this procedure to delete a zone.

Procedure

To delete a zone, follow these steps:

1 Select the zone you want to delete in the Zone Hierarchy.

Result: The Zone Properties page opens

2 Click **Delete**.

Result: A dialog box asks you to confirm that you want to delete the zone.

3 Click **OK**.

Result: The zone is deleted.

END OF STEPS

Add primary server to a zone

Purpose

Use this procedure to add one or more primary servers to a zone.

Before you begin

- For VitalQIP, it is a good idea to have at least one primary server defined for all zones, although VitalQIP does allow you to have a zone defined without adding a primary server.
- If you choose to define multiple primary servers for a zone, you can associate the same secondary to multiple primaries; VitalQIP correctly creates all files.
- The **Send Secure Updates** parameter only appears if the server is secure.

Procedure

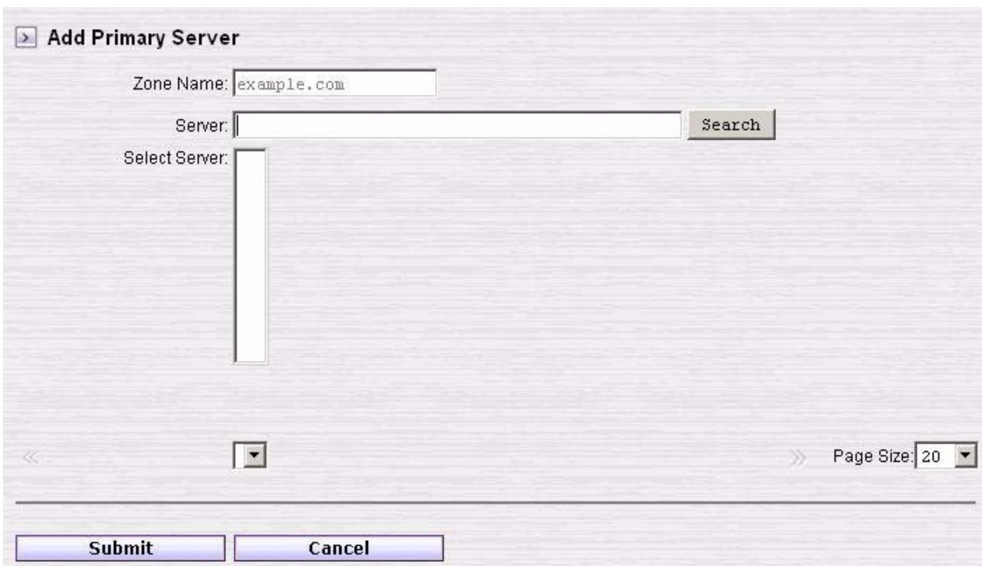
To add a primary server to a zone, follow these steps:

1 Select the zone to which you want to add a primary server in the Zone Hierarchy.

Result: The Zone Properties page opens.

2 Select **Add Primary Server**.

Result: The Add Primary Server page opens.



3 Enter either a complete or partial server name in the **Server** field. You can use asterisks as a wild card. Click **Search**.

Result: The Select Server list is populated with a list of available servers.

4 Select one or more servers to add as a primary server and click **Submit**.

Result: A dialog opens with the message **All Servers Added!**

5 Click **OK**.

END OF STEPS

Add secondary server to a zone

Purpose

Use this procedure to add one or more secondary servers to a zone.

Before you begin

- If you have defined multiple primary servers for a zone, you can associate the same secondary to multiple primaries; VitalQIP correctly creates all files.
- The **Send Secure Updates** parameter only appears if the server is secure.

Procedure

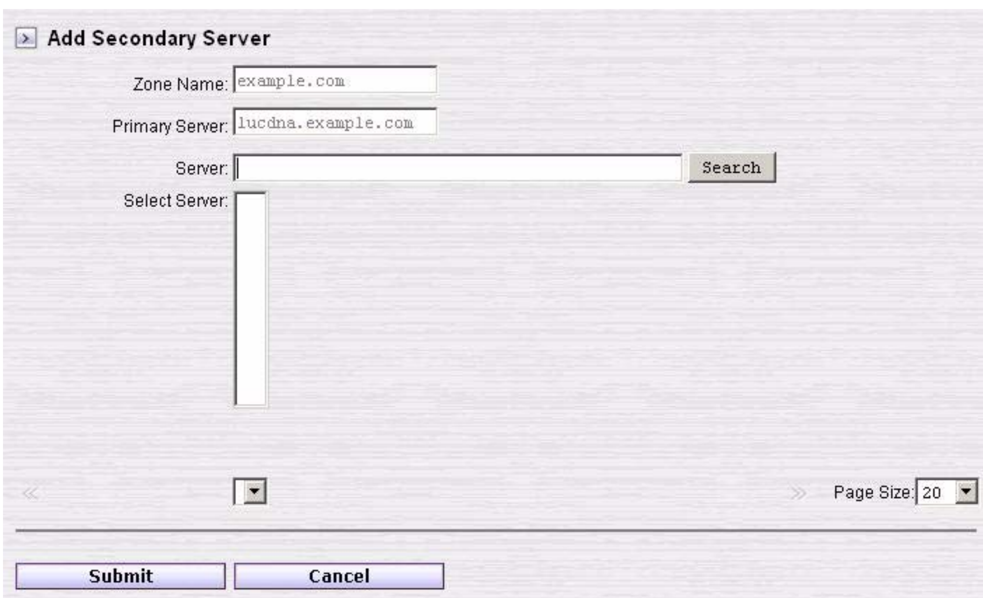
To add a secondary server to a zone, follow these steps:

1 Expand the zone hierarchy and click the primary server to which you want to add a secondary server.

Result: The Primary DNS Server page opens.

2 Select **Add Secondary Server**.

Result: The Add Secondary Server page opens.



3 Enter either a complete or partial server name in the Server field. You can use asterisks as a wild card. Click **Search**.

Result: The Select Server list is populated with a list of available servers.

4 Select one or more servers to add as a secondary zone and click **Submit**.

Result: A dialog confirms that all servers have been added.

END OF STEPS

Search for a resource record

Purpose

This procedure allows you to search for a resource record and display its properties.

Procedure

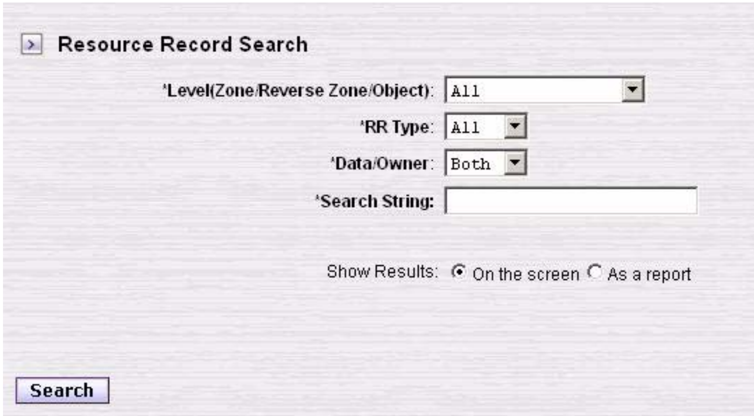
To search for a resource record, follow these steps:

1 Mouse over **DNS** and select **Zone**.

Result: The Zone Hierarchy page opens.

2 To search for a resource record, mouse over the **Actions** menu and select **Resource Record Search**.

Result: The Resource Record Search page opens.



3 Refer to the following table as you select values.

Table 14-3 Resource Record Search fields

Field	Description
Level	Specifies the level of the resource record. The options are: • All (Default) • Object • IPv4 Reverse Zone • IPv6 Reverse Zone • Zone
RR Type	Select the resource record type. For a description of the resource record types, refer to Table 14-5, “Type field values” (p. 14-21).
Data/Owner	Select one of the following options: • **Both** - Both the data and owner are selected. This option is selected by default. • **Data** - The data associated with the specific resource record type is selected. • **Owner** - The name used to define the owner for this resource record is selected.
Search String	Enter freeform text. You can use the wildcard character (*) for 0 or more characters.

Field	Description

Show Results	Select one of the following options:
	• **On the screen** - Select this option if you wish to view the search results on the screen.
	• **As a report** - Select this option if you wish to view the search results in a report. The following sub-options are displayed only if you choose to display the search results as a report.
	  • **Report Format** - The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.
	  • **Run** - Select when to run the report. Refer to "Schedule a report" (p. 29-6) for more information.

4 Click **Search**.

Result: The results appear in the **Search Results** list.

Add/modify zone resource records

Purpose

This function allows you to create, and modify resource records for a zone. This option allows resource records for the zone to be written to the configuration file. VitalQIP validates and formats the information on input.

Before you begin

- The **Resource Records** button is only available if the administrator has the Create Resource Records privilege set to True.
- VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and you cannot add or modify the profile. You can fine-tune this feature by enabling or disabling Validate CNAME Records sub-policies in Global Policies. When set to True, these sub-policies allow validation checks to be made against the following whenever you add or modify an object:
  – Object aliases
  – Object resource records
  – Domain resource records
  – Reverse zone resource records
  – ENUM NAPTR resource records

– IPv6 node names

- In addition to object resource records, all zone resource records, including those that are externally managed, are now audited. Audit records for zones are added to the **rrs_aud** and **zone_rrs_aud** tables in the VitalQIP database.

Procedure

To add or modify a resource record, use the following steps:

1 Mouse over **DNS** and select **Zone**.

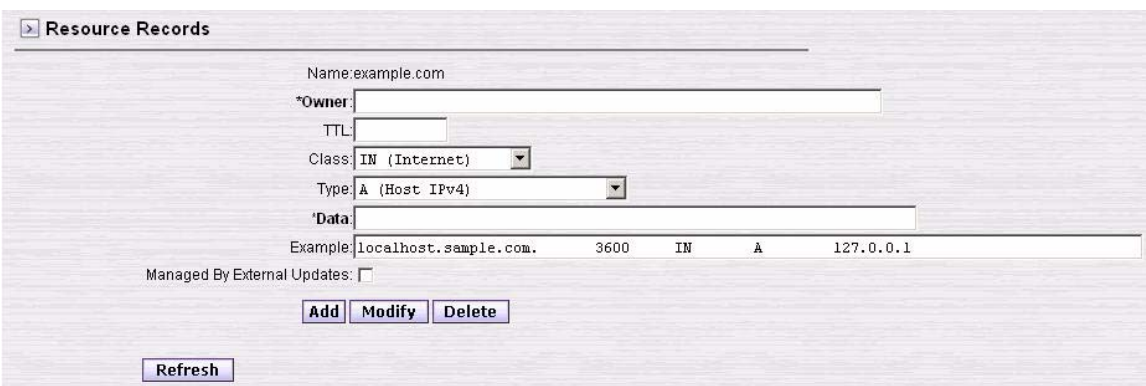
Result: The Zone Hierarchy page opens.

2 Find the zone to which you want to add a new resource record or modify an existing one and select it.

Result: The Zone Properties page opens.

3 Click **Resource Records**.

Result: The Resource Records page opens:



- To add a resource record, enter values in the fields, as described in the following table.
- To modify a resource record, select it from the list at the bottom of the page and click **Modify**. Its values are displayed in the fields at the top of the page and you can then change them. Refer to the following table.

Table 14-4 Resource Records fields

Field	Description
Owner	***Required***. Enter whatever name you are using to define the owner for this resource record.
TTL (Time To Live)	The length of time (in seconds) the name server will hold this information. If no TTL is defined, the value is inherited from the zone.
Class	Resource Records are divided into classes. Each class of records pertains to a type of network or software. Select from the drop down listing of default Classes, Default classes are as follows: • IN (Internet) • CS (CSNet Class) • CH (Chaos Class) • HS (Hesiod Class).
Type	Select a Resource Record from the drop-down list, or select **Custom** and enter your own type. The settings for the different types are described in Table 14-5, “Type field values” (p. 14-21). For additional information on these resource record types, refer to *DNS and BIND*, by Cricket Liu and Paul Albitz.
Data	***Required***. Enter the data associated with the specific resource record type. Refer to the **Example** field for the format required for each resource record type.
Managed by External Updates	The **Managed by External Updates** checkbox indicates that the selected Resource Record has been added by VitalQIP QIP Update Service. To make changes to a Resource Record that is managed by external updates, uncheck the **Managed by External Updates** checkbox. The **Managed by External Updates** checkbox can only be checked when the Resource Record has been added by the VitalQIP QIP Update Service or **`qip-syncexternal`** command. It is not possible to set this checkbox within the GUI. For further information on VitalQIP support for external objects, refer to the *Administrator Reference Manual*.

Based on your selection in the **Type** field, enter data as described in the following table. A sample record displays in the **Example** field based on the type you selected.

Table 14-5 Type field values

Type	Data entry values
A (Host IPv4)	**Address** - enter the IP address of the A record.
CNAME (Canonical Name)	**Canonical Name** - enter a name that specifies the canonical or primary name for the owner.
HINFO (Host Information)	Enter the following data: **CPU** - enter the central processing unit type. **OS** - enter the operating system type.
MX (Mail Exchanger)	Enter the following data: **Preference** - enter a number, which specifies the preference given to this resource record among others at the same owner (lower values are preferred). **Exchange Name** - enter a fully qualified name, which specifies a host that acts as a mail exchange for the owner.
NAPTR	**Order** - A 16-bit unsigned integer specifying the order in which the NAPTR records must be processed to ensure the correct ordering of rules. **Preference** - A 16-bit unsigned integer that specifies the order in which NAPTR records with equal “order” values should be processed. **Flags** - A ***<character-string>*** containing flags to control aspects of the rewriting and interpretation of the fields in the record. Flags are single characters from the set [A-Z 0-9]. **Service** - Specifies the services available down this rewrite path. **Regular Expression** - A string containing a substitution expression that is applied to the original string held by the client to construct the next domain name to lookup. **Replacement** - The next NAME to query for NAPTR, SRV, or address records depending on the value of the flags field.
NS (Name Server)	**Name Server** - enter a fully qualified domain, which specifies a host that is authoritative for the specified class and domain.
PTR (Pointer)	**PTR Name** - enter a fully qualified name which points to some location in the domain name space.
TXT (Text)	**Text Data** - enter descriptive text for the resource record.

Type	Data entry values
WKS (Well-Known Services)	**Address** - enter the 32-bit internet address. **Protocol** - this is usually UDP or TCP, although it can be any entry in the */etc/protocols* file. **Services** - enter a port number below 256. This consists of a service list below port 256 for the */etc/services* files.
AAAA (Host IPv6)	**Ipv6 Address** - enter the MAC address in the octet fields.
AFSDB (Andrew File System Data Base)	**Sub Type** - select the Sub Type. 1 is an AFS cell database server, and 2 is a DCE authenticated name server. **Host Name** - enter the fully qualified name of the host that has a server for the cell named by the owner.
MB (Mailbox Name)	**Mailbox Name** - enter a fully qualified name, which specifies a host that has the specified mailbox.
MG (Mail Group)	**Mail Group** - enter the fully qualified name that specifies a mailbox, which is a member of the mail group specified, by the name.
MINFO (Mailbox Information)	Enter the following data: **Responsible Mailbox** - enter a fully qualified name, which specifies a mailbox that is responsible for the mailing list or mailbox. **Error Mailbox** - enter a fully qualified name, which specifies a mailbox that receives error messages related to the mailing list or mailbox specified by the owner of the MINFO Resource Record.
MR (Mail Rename)	**New Mailbox** - enter a fully qualified name, which specifies a mailbox that is the proper rename of the specified mailbox.
ISDN	Enter the following data: **ISDN Address** - enter the ISDN address, which identifies the ISDN number of owner and Direct Dial In (if any). **Subaddress** - enter a subaddress.
SRV (Server Resource Record)	Enter the following data: **Priority** - enter the priority of the host using any numbers between 0 and 65535. Clients try to contact the host with the lowest priority. **Weight** - enter a weight (any number between 0 and 65535). This field specifies a relative weight for entries with the same priority. **Port** - enter the port number (any number between 0 and 65535) of the service on the host. Target - enter a fully qualified domain name for the host supporting the service.
X25	**PSDN Address** - enter the Public Switched Data Network (PSDN), which identifies the PSDN address.

Type	Data entry values
Custom	When selected, opens a data entry field where you can enter your own resource record.

END OF STEPS

Delete a resource record

Purpose

Use this procedure to delete a resource record from a zone.

Procedure

To delete a resource record, use the following steps:

1 Mouse over **DNS** and select **Zone**.

Result: The Zone Hierarchy page opens.

2 Find the zone from which you want to delete a resource record and select it.

Result: The Zone Profile opens.

3 Click **Resource Records**.

Result: The Resource Record page opens.

4 Check the **Select** checkbox beside any resource records you want to delete from the **Search Results** list and click **Delete**.

Result: The **Status** for the selected resource records changes to **Delete**.

5 Click **Submit**.

Result: A dialog opens with the message **Resource records modified successfully.**

6 Click **OK**.

Result: The **Search Results** list is updated as the selected resource records are removed.

END OF STEPS

Set zone options

Purpose

Use this procedure to set your zone options.

Procedure

To set zone options on a zone, follow these steps:

1 Mouse over **DNS** and click **Zone**.

Result: The Zone Hierarchy page opens.

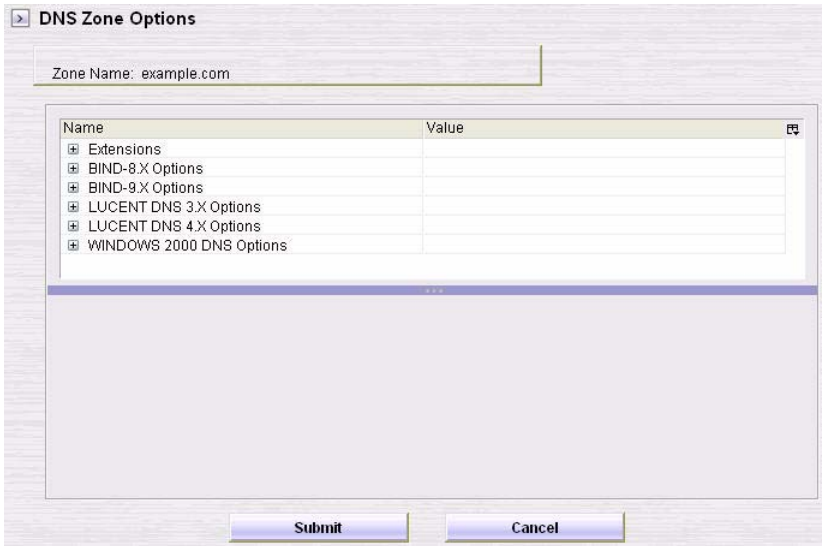
2 Expand the hierarchy until you come to the zone to set the zone options.

3 Select the zone.

Result: The Zone Properties page opens.

4 Click **Zone Options**.

Result: The DNS Zone Options page opens.



5 To set up your zone options (listed in the following table), expand a zone option, select a zone option, and enter/select the value.

Table 14-6 Zone options

Zone Options	Values
Extensions	See "Extensions zone options" (p. 14-25).
BIND-8.X Options	See "BIND 8.X zone options" (p. 14-26).
BIND-9.X Options	See "BIND 9.X zone options" (p. 14-28).
Lucent DNS 3.X Options	See "LUCENT DNS 3.X zone options" (p. 14-30).
Lucent DNS 4.X Options	See "LUCENT DNS 4.X zone options" (p. 14-32).
Windows 2000 DNS Options	See "Windows 2000 DNS Zone Options" (p. 14-34).

Extensions zone options

The Extensions zone options described in the following table allow you to enter extensions not offered through the VitalQIP GUI to a domain's database files for entities not managed by VitalQIP. These extensions, **Prefix of zone db file** and **Postfix of zone db** file, appear before and/or after the zone.

Table 14-7 Extension options

Option	Description
Prefix of zone db file	Text appears before the domain in the zone file and is added to the Domain Zone file exactly as you enter it. You must use proper DNS syntax and must not exceed 255 characters per line. For example: $TTL 86400

Postfix of zone db file	Text appears after the domain in the zone file and is added to the Domain Zone file exactly as you enter it. You must use proper DNS syntax and must not exceed 255 characters per line. For example:
	`mailhost2   IN A       198.200.138.234`
	`mailhost1   IN MX      mailhost2.quadritek.com.`
	`oneillt     IN A       198.200.138.236`
	`myalias     IN CNAME   oneillt.quadritek.com.`
	Refer to *DNS and BIND,* by Cricket Liu and Paul Albitz for details on other domain information you can input for domains.

BIND 8.X zone options

BIND-8.X required zone options described in the following table are applied to the *named.conf* file. The **Setting** area displays values based on the selected zone option parameter. Default values in the Option value column appear in boldface.

Note: If Use Server Value is selected, the option will not be written to the configuration file and the DNS server uses its default value. **BIND 8.X zone options**

BIND 8.X zone option	Value type	Option value	Usage
allow-query	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive specifies which hosts are allowed to ask questions of a server. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value -** This value will ***not*** be pushed to the server.

BIND 8.X zone option	Value type	Option value	Usage
allow-transfer	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive determines whether zone transfers are allowed for this zone. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server.
allow-update	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive specifies which hosts are allowed to submit dynamic DNS updates to the server. The **Use List** option presents three sub-options: • **ACL Template** - allows you to select an ACL template.. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** -This value will ***not*** be pushed to the server. A valid setting in the options block overrides the server's default behavior.
check-names	Selection	**Warn**, Fail, Ignore, Use Server Value	Select one of the following values: • **Warn** - Invalid names are logged, but processing continues normally. • **Fail** - Invalid names are logged and the offending data is rejected. • **Ignore** - No checking is performed. The most common reason for setting to “Ignore” is to allow underscores in the host names. • **Use Server Value** - This value will ***not*** be pushed to the server.
notify	Selection	Yes, **No**, Use Server Value	If this option is set to “yes”, DNS NOTIFY messages are sent when a zone server is authoritative for changes. The **also notify** sub-option is displayed so you can add IP addresses. **Use Server Value** - This value will ***not*** be pushed to the server.

BIND 8.X zone option	Value type	Option value	Usage
zone block of named.conf	Alphanumeric	None	Any text typed in the free text field appears in the zone block of the *named.conf* file. To add text, click **Modify**, type the appropriate text, and then click **Apply**. **Note:** As this text is associated with the zone and not a particular server, ensure all servers authoritative for the zone support the text for this field.

BIND 9.X zone options

BIND-9.X required zone options described in the following table are applied to the *named.conf* file. The **Setting** area displays values based on the selected zone option parameter. Default values in the Option value column appear in boldface. For more information on zone option directives, refer to the *Administrator Reference Manual*.

Note: If the parameter value is set to Use Server Values, and the DNS options are not written to the config value, the server uses its default value.

Table 14-8 BIND 9.X zone options

BIND 9.X zone option	Value type	Option value	Usage
DNSSEC enabled zone	Boolean	True, **False**	When this option is set to True, a zone is signed with configured keys when a DNS push is run with DNS Generation.
allow-notify	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive specifies which hosts are allowed to notify slaves (secondary servers) of a zone change, in addition to the zone masters. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server.

BIND 9.X zone option	Value type	Option value	Usage
allow-query	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive specifies which hosts are allowed to ask questions of a server. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server.
allow-transfer	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive determines whether zone transfers are allowed for this zone. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server.
allow-update	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive specifies which hosts are allowed to submit dynamic DNS updates to the server. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server. A valid setting in the options block overrides the server's default behavior.
notify	Selection	Yes, **No**, Explicit, Use Server Value	If this option is set to “yes”, DNS NOTIFY messages are sent when a zone the server is authoritative for changes. The **also notify** sub-option is displayed so you can add IP addresses. If this option is set to **Explicit**, notifies are only sent to servers explicitly listed in the **also-notify** sub-option. **Use Server Value** - This value will ***not*** be pushed to the server.

BIND 9.X zone option	Value type	Option value	Usage
zone block of named.conf	Alphanumeric	None	Any text typed in the free text field appears in the zone block of the *named.conf* file. To add text, click **Modify**, type the appropriate text, and then click **Apply**. **Note:** As this text is associated with the zone and not a particular server, ensure all servers authoritative for the zone support the text for this field.

LUCENT DNS 3.X zone options

The following table describes LUCENT DNS 3.X zone options. Default values in the Option value column appear in boldface.

Table 14-9 LUCENT DNS 3.X zone options

Lucent DNS 3.X zone option	Value type	Option value	Usage
Import External Updates	Selection	True, **False**	Determines if external DNS updates are imported into VitalQIP.
allow-query	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive specifies which hosts are allowed to ask questions of a server. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server.

Lucent DNS 3.X zone option	Value type	Option value	Usage
allow-transfer	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive determines whether zone transfers are allowed for this zone. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server.
allow-update	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive specifies which hosts are allowed to submit dynamic DNS updates to the server. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server. A valid setting in the options block overrides the server's default behavior.
check-names	Selection	**Warn**, Fail, Ignore, Use Server Value	The following values are valid: • **Warn** - Invalid names are logged, but processing continues normally. • **Fail** - Invalid names are logged and the offending data is rejected. • **Ignore** - No checking is performed. The most common reason for setting to “Ignore” is to allow underscores in the host names. • **Use Server Value** - This value will ***not*** be pushed to the server.
notify	Selection	Yes, **No**, Use Server Value	If this option is set to “yes”, DNS NOTIFY messages are sent when a zone the server is authoritative for changes. The **also notify** sub-option is displayed so you can add IP addresses. **Use Server Value** - This value will ***not*** be pushed to the server.

Lucent DNS 3.X zone option	Value type	Option value	Usage
zone block of named.conf	Alphanumeric	None	Any text typed in the free text field appears in the zone block of the *named.conf* file. To add text, click **Modify**, type the appropriate text, and then click **Apply**. **Note:** As this text is associated with the zone and not a particular server, ensure all servers authoritative for the zone support the text for this field.

LUCENT DNS 4.X zone options

The following table describes the LUCENT DNS 4.X zone options. Default values in the Option value column appear in boldface.

Table 14-10 LUCENT DNS 4.X zone options

LUCENT DNS 4.X zone option	Value type	Option value	Usage
DNSSEC enabled zone	Boolean	True, **False**	When this option is set to True, a zone is signed with configured keys when a DNS push is run with DNS Generation.
Import External Updates	Selection	True, **False**	Determines if external DNS updates are imported into VitalQIP.
allow-notify	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive specifies which hosts are allowed to notify slaves (secondary servers) of a zone, in addition to the zone masters. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server.

LUCENT DNS 4.X zone option	Value type	Option value	Usage
allow-query	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive specifies which hosts are allowed to ask questions of a resolver. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server.
allow-transfer	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive determines whether zone transfers are allowed for this zone. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server.
allow-update	Selection	**Any**, None, localhost, localnets, Use List, Use Server Value	This directive specifies which hosts are allowed to submit dynamic DNS updates to the server. The **Use List** option value presents three sub-options: • **ACL Template** - allows you to select an ACL template. • **Other** - allows you to enter free form text. You may use commas to delimit addresses. • **Use Server Value** - This value will ***not*** be pushed to the server. A valid setting in the options block overrides the server's default behavior.

LUCENT DNS 4.X zone option	Value type	Option value	Usage
notify	Selection	Yes, **No**, Explicit, Use Server Value	If this option is set to “yes”, DNS NOTIFY messages are sent when a zone the server is authoritative for changes. The notify sub-option is displayed so you can add IP addresses.The **also notify** sub-option is displayed so you can add IP addresses. If this option is set to **Explicit**, notifies are only sent to servers explicitly listed in the **also-notify** sub-option. **Use Server Value** - This value will ***not*** be pushed to the server.
zone block of named.conf	Alphanumeric	None	Any text typed in the free text field appears in the zone block of the *named.conf* file. To add text, click **Modify**, type the appropriate text, and then click **Apply**. **Note:** As this text is associated with the zone and not a particular server, ensure all servers authoritative for the zone support the text for this field.

Windows 2000 DNS Zone Options

The following table describes the Windows 2000 zone options. Default values in the Option value column appear in boldface.

Note: Windows 2000 zone options can also be used with a Windows 2003 DNS server.

Table 14-11 Windows 2000 DNS zone options

Windows 2000 DNS zone option	Value type	Option value	Usage
aging	Selection	True, **False**, Use Server Value	This option determines whether aging and scavenging are enabled for this zone.
allow-transfer	Selection	**Any**, None, Name Servers Only, Use List, Use Server Value	This option determines whether zone transfers are allowed for this zone.

Windows 2000 DNS zone option	Value type	Option value	Usage
allow-update	Selection	Yes, **No**, Use Server Value	This option determines whether clients may automatically update the zone. For the **Use Server Value**, a valid setting in the options block overrides the server's default behavior. **Note:** Dynamic update will not function if this is set to **No**. If you want dynamic DNS to work properly, you must set this option to a value other than **No**.
no-refresh-interval	Numeric	Time in hours	This is the no refresh value for scavenging. A value of 0 means do not push to the server.
notify	Selection	Yes, **No**, Use List, Use Server Value	This option determines whether a notify packet is sent when the zone is updated.
refresh-interval	Numeric	Time in hours	This is the refresh interval for scavenging. A value of 0 means do not push to the server.
zone options	Text		This is free form text where information can be entered in the dnscmd format (a utility supplied by Microsoft). For more information on the **`dnscmd`** utility, refer to your Windows documentation.

Stealth Server zone options

The following table describes the Stealth server options. Default values in the Option value column appear in boldface.

Note: The Stealth Server options only appear when a DNS server is assigned to a zone.

Table 14-12 Stealth Server options

Stealth Server option	Value type	Option value	Usage
Stealth Server	Selection	True, **False**	Determines if a DNS server's NS records are no longer placed in the zone files on other servers.
Override Server Name in SOA	Selection	True, **False**	Determinies if the host name of the server appears in the SOA record instead of the stealth server's name.

15 DNS Views

Overview

Purpose

This chapter describes the use and management of DNS Views.

Contents

This chapter covers these topics.

About DNS Views

Overview

Purpose

VitalQIP supports configuration of DNS Views for Lucent DNS 4.x and Bind-9.x DNS servers. DNS Views, based on source or destination criteria, are used to provide:

- Different permissions or restrictions to DNS clients
- Different answers to DNS clients

VitalQIP configures zones for DNS Views through one of these methods:

- Sharing existing global zone data into a DNS View. Any subsequent changes made to the data in the global zone, except the SOA MNAME and NS records, comprise the zone data in the DNS View.
- Defining a zone with contents specific to a DNS View. All new data specified through Object FQDNs and View-specific Node Domain Names in addition to new SOA, and NS records comprise the zone data in the DNS View.

Both methods allow DNS to provide different access or restrictions. Only view specific zones can provide clients with answers that are different from the global namespace.

Zones in the global namespace

Any zone configured in VitalQIP that is not associated with a DNS View is considered to exist in the global namespace. These zones are referred to as global zones.

DNS servers do not allow more than 1 instance of a zone, per DNS View, although multiple zones of the same name can exist in multiple DNS Views. If aDNS server has at least one DNS View, VitalQIP's DNS generation creates a default view called `_vitalqip_global_namespace` at the end of that DNS server's *named.conf* file. The `_vitalqip_global_namespace` view contains the global namespace zones and reverse zones assigned to that DNS server. DNS servers use the first matching view to answer a client's request. DNS servers use the `_vitalqip_global_namespace` view to process requests that do not match any views appearing earlier in the *named.conf* file.

VitalQIP can be configured to only send dynamic updates to zones in the global namespace. Only zones in the global namespace hosted by Lucent DNS can participate in External Dynamic Update propagation. Refer the *VitalQIP Administrator Reference Manual* for more information on external dynamic update propagation.

NS record processing

NS records are automatically added to a parent zone based on the presence of child zones stored in VitalQIP. These records allow a DNS client to navigate the namespace hierarchy by indicating which DNS servers to query for which zones.

When processing NS records for DNS views, NS records are generated based on the zones that appear in the view. NS records are not generated for zones in other views or the global namespace.

Name collisions

All DNS name, domain name, IPv6 node name, IPv4 object name, object alias, and CNAME resource record name collision checking is governed by the Validate CNAME Records global policy setting in VitalQIP.

DNS names added to an object or node are only checked for collisions against CNAMEs. CNAME is shared into a DNS View when an IPv4 object has an alias and that object is in a zone that is shared into the DNS view. Name collisions for CNAMEs are checked in the global namespace; any collision check for a shared zone has already occurred. Refer to “Create an alias for an object” (p. 10-43) for information about aliases. CNAMEs cannot be added to view specific zones, so no collision checking is necessary.

Permissions

Only master and organization administrators are able to create, modify, and delete DNS Views and zones in DNS Views.

Reports

The DNS View report can be viewed from the DNS View Properties page.

Shared zones

Description

VitalQIP allows global zone data to be shared into a view. This type of zone always contains the same data as the zone in the global namespace.

Shared Zones Properties page

When a zone is shared, the Zone Properties page has “(Shared)” displayed in the page title. The following is an example Shared Zone Properties page.

Figure 15-1 Sample Shared Zone Properties page

From the Zone Properties page, you can:

- Add a primary server
- Configure zone options
- Delete the zone

Note: Shared zone properties cannot be modified.

Usage scenario for global zones

The following shows an usage scenario for sharing global zones.

Table 15-1 Global zones and DNS View usage example

Scenario	A company *example.com* wishes to provide recursive DNS services for internal clients, but non-recursive services for external clients.
Problem	It needs to done on a single DNS server.
Solution	The company defines a single DNS View called External with a match-clients list that does not match addresses in the corporate intranet. In this DNS View VitalQIP administrators set allow-recursion to 127.0.0.1 and share all globally defined zones and reverse zones into the External view. VitalQIP generates the _vitalqip_global_namespace view to contain all global namespace zones and reverse zones on the server. The server is configured with **`allow-recursion = { any; };`** in this view. This configuration allows a single server to provide recursion for internal users while restricting recursion for external users.

Resulting named.conf file	The following is the resulting *named.conf* file: **Note:** The two example.com zone files referred to below contain the same resource records.

```
acl external {!<internal networks>};
view "external" {
match-clients { external;};
// options defined here apply to all zones in this view
      allow-recursion = { 127.0.0.1; };

  zone "example.com" {
    type master;
    file "external/example.com";
// this file contains delegation and glue records
// appropriate to the external namespace.
  }.;
};
view "_vitalqip_global_namespace" {
  // Global namespace view generated by VitalQIP
match-clients { any;};
  match-destinations { any;}; allow-recursion { any; };

zone "example.com"; {
    type master;
    file "example.com"
    // this file contains delegation and glue records
// appropriate to VitalQIP's global namespace.
  };
};
```

View specific zones

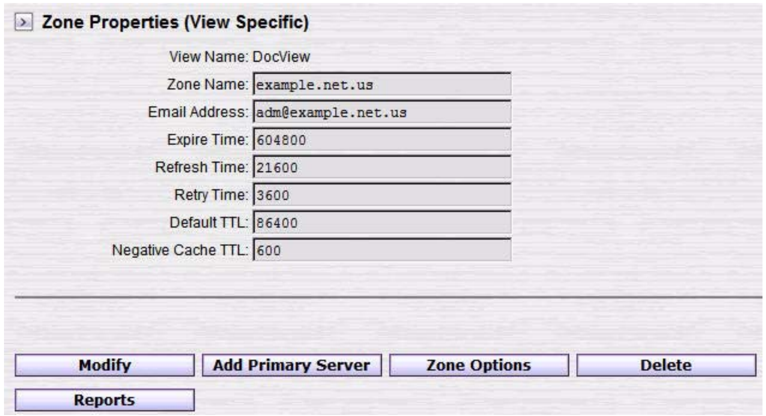
Description

Zones can be defined with data specifical to a DNS View. These zones are referred to as view specific zones. View specific zones can provide clients with different DNS responses than they would receive in the global namespace. A view specific zone can contain a different set of resource records than a globally managed zone of same name.

View specific Zone Properties page

View specific zones have different configuration parameters than shared zones. When a zone is view specific, the Zone Properties page has “(View Specific)” displayed in the page title. The following is an example View Specific Zone Properties page.

Figure 15-2 Sample View Specific Zone Properties page



From the view specific Zone Properties page, you can:

- Modify the view specific zone properties
- Add a primary server
- Configure zone options
- Delete the zone

Usage scenario for view specific zones

The following shows a usage scenario for view global zones.

Table 15-2 View specific zones and DNS View usage scenario

Scenario	The company *example.com* uses a block of private address space inside its corporate intranet. All internal servers and workstations have addresses allocated out of 10.0.0.0/8. *Example.com* also uses a block of globally routable address space for routers and servers that access the Internet.
Problem	The company has a single DNS server on a host with a globally routable IP address. This server hosts a single zone *example.com* for internal use. Hosts in this zone have addresses from both private and public address space. The company cannot publish this zone on the Internet as it contains unroutable addresses on the company's intranet. The company wants to use the same DNS server to host *example.com* for external use.

<table>
<tr><td>Solution</td><td>The company defines a DNS View called External with a match-clients list that does not match the addresses within the corporate intranet. Within the External view, VitalQIP administrators create the zone example.com that contains only resource records pointing to hosts with publicly routable IP addresses. The zone does not contain resource records of hosts with unroutable addresses. Both the view specific example.com and the global example.com are added to the same name server.

This configuration allows a single DNS server to provide internal clients with resource records that point to addresses in the private address space while external users only see with resource records that point to addresses in publicly routable address space.</td></tr>
<tr><td>Resulting named.conf file</td><td>The following is the resulting named.conf file:

Note: The two example.com zone files below contain different resource records:

<pre>
acl external {!<internal networks>};
view "external" {
  match-clients { external;};
  zone "example.com" {
    type master;
    file "external/example.com";
    // this file has resource records from the
// external/Internet namespace.
  }.;
};
view "_vitalqip_global_namespace" {
// Global namespace view generated by VitalQIP
  match-clients { any;};
  match-destinations { any;};
  zone "example.com" {
     type master;
     file "example.com";
     // this file has resource records from
// VitalQIP's global/intranet namespace
  };
};
</pre></td></tr>
</table>

Primary and secondary servers in DNS Views

Background

DNS Servers assigned to view specific and shared zones appear under the zone in a sub-folder labeled **DNS Servers** in the Zone hierarchy. Secondary servers are listed under the appropriate primary servers in the hierarchy.

Server properties and DNS views

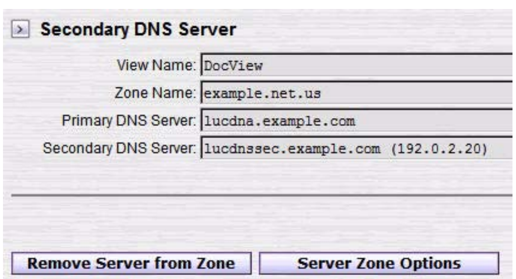
The Primary and Secondary DNS Server pages are read only.

The following figure shows how the Primary DNS Server page looks when it is accessed by clicking the DNS server in the Zone Hierarchy.

Figure 15-3 Sample Primary DNS Server

The following figure shows how the Secondary DNS Server page looks when it is accessed by clicking the secondary server in the Zone Hierarchy.

Figure 15-4 Sample Secondary DNS Server



Option management in DNS Views

Background

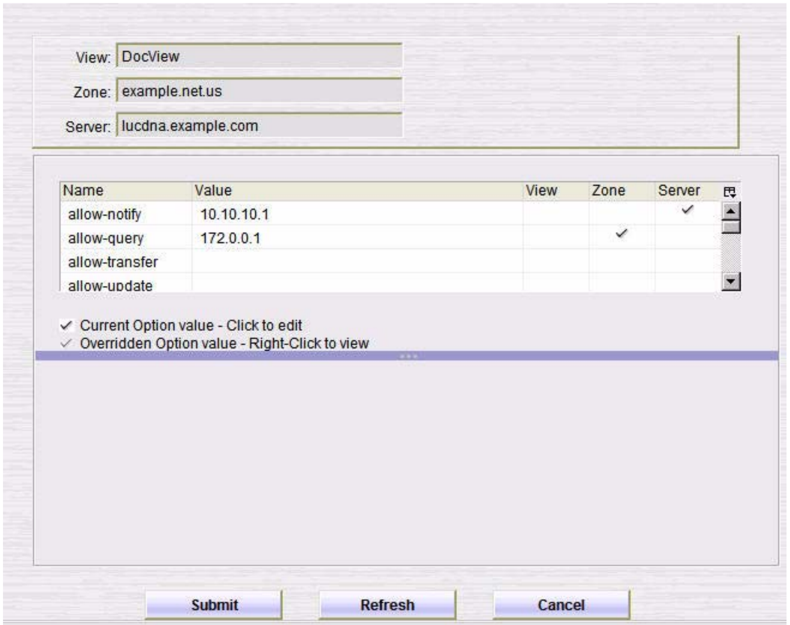
DNS options can be managed at these levels:

- View level from the DNS View Properties page
- Zone level from the View Specific or Shared Zone Properties pages
- Server level from the Primary and Secondary DNS Server pages

View specific zone options

The following figure is an example of a zone option management page for a DNS server.

Figure 15-5 Sample of view specific server Zone Options page



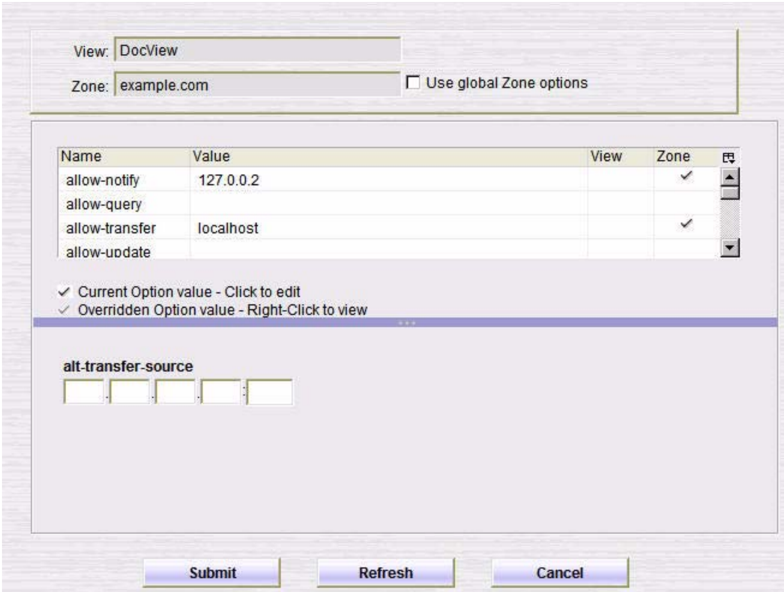
The headers and visible columns on the option management page vary according to the invoking page. Checkmarks appear in the columns for options that are assigned at the view, zone, or server levels.

Shared zone options

Shared zones can have two different table representations at zone level that depend if **Use global Zone options** is checked. **Use global Zone options** determines if the shared zone is inheriting a read-only copy of the global zone options or if zone options can be set at the zone and server levels for this zone.

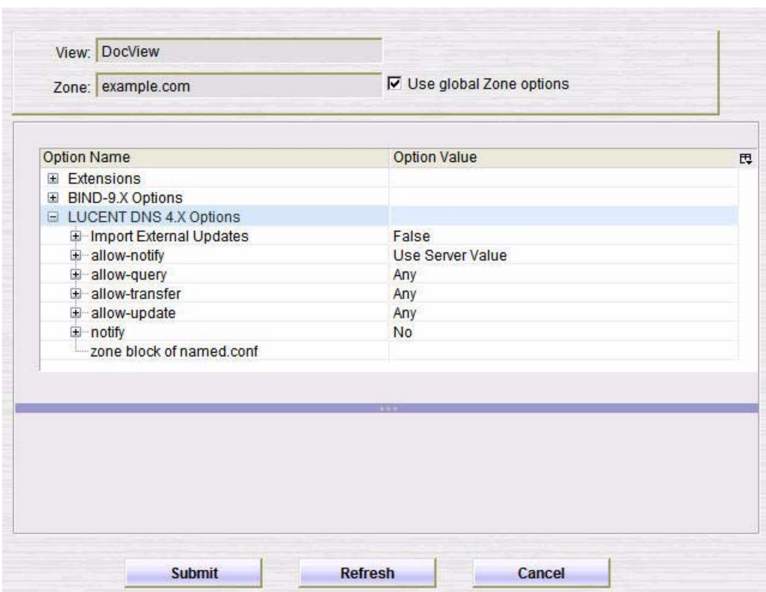
When **Use global Zone options** is not checked, options applicable to the zone are displayed. The Zone Option page looks as follows.

Figure 15-6 Zone Options page with editable options



When **Use global Zone options** is checked, the global zone options are displayed. The Zone Page looks as follows. These options are not editable.

Figure 15-7 Zone options page with global zone options



Supported zone options

A number of different zone options are available for DNS Views, shared zones, and view specific zones. Zone options are available at different levels. The following table shows the supported Zone options and the levels at which the options are supported. For descriptions of zone options, refer to the most current edition of *DNS and BIND* by Paul Albitz and Cricket Liu.

Table 15-3 Supported options

Option Name	Values	Notes	View level	Zone level	Server level
acache-cleaning-interval	minutes	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	---	---
acache-enable	yes, no	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	---	---
additional-from-auth	yes, no		X	---	---
additional-from-cache	yes, no		X	---	---
allow-notify	address match list		X	X	X
allow-query	address match list		X	X	X
allow-query-cache	address match list	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	---	---
allow-recursion	address match list		X	---	---
allow-transfer	address match list		X	X	X
allow-update	address match list		X	X	X
allow-update-forwarding	address match list		X	X	X
also-notify	IPv4 or IPv6 address port list		X	X	X

Option Name	Values	Notes	View level	Zone level	Server level
alt-transfer-source	IPv4 address port list		X	X	X
alt-transfer-source-v6	IPv6 address port list		X	X	X
auth-nxdomain	yes, no		X	---	---
check-mx	fail, warn, ignore	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	X	X
check-mx-cname	fail, warn, ignore	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	X	X
check-integrity	yes, no	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	X	X
check-names	fail, warn, ignore		---	X	X
check-sibling	yes, no	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	X	X
check-wildcard	yes, no	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	X	X
check-srv-cname	fail, warn, ignore	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	X	X
cleaning-interval	minutes		X	---	---
clients-per-query	numeric	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	---	---
delegation-only	yes, no		---	X	X
dnssec-accept-expired	yes, no	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	---	---

Option Name	Values	Notes	View level	Zone level	Server level
dnssec-enable	yes, no		X	---	---
dnssec-validation	yes, no	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	---	---
edns-udp-size	number of bytes		X	---	---
empty-zones-enable	yes, no	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	---	---
forward	only, first		X	X	X
forwarders	IPv4 or IPv6 address port list		X	X	X
ixfr-from-differences	yes, no		X	X	X
lame-ttl	seconds		X	---	---
masterfile-format	text, raw	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	X	X
max-acache-size	size specification	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher The syntax of the data is an 11 character string where the first character must be a number (0-9). You can optionally add a unit of b, k, m, or g (for bytes, kilobytes, megabytes, and gigabytes) at the end. These characters are not case sensitive. If no unit is defined, the value is in bytes. Examples are 12345, 12345b, 200k, 40m, and 1g.	X	---	---

Option Name	Values	Notes	View level	Zone level	Server level
max-cache-size	size specification	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher The syntax of the data is an 11 character string where the first character must be a number (0-9). You can optionally add a unit of b, k, m, or g (for bytes, kilobytes, megabytes, and gigabytes) at the end. These characters are not case sensitive. If no unit is defined, the value is in bytes. Examples are 12345, 12345b, 200k, 40m, and 1g.	X	---	---
max-cache-ttl	seconds		X	---	---
max-clients-per-query	numeric	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	---	---
max-journal-size	size specification	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher The syntax of the data is an 11 character string where the first character must be a number (0-9). You can optionally add a unit of b, k, m, or g (for bytes, kilobytes, megabytes, and gigabytes) at the end. These characters are not case sensitive. If no unit is defined, the value is in bytes. Examples are 12345, 12345b, 200k, 40m, and 1g.	X	X	X
max-ncache-ttl	seconds		X	---	---
max-refresh-time	seconds		X	X	X
max-retry-time	seconds		X	X	X

Option Name	Values	Notes	View level	Zone level	Server level
max-transfer-idle-in	minutes		X	X	X
max-transfer-idle-out	minutes		X	X	X
max-transfer-time-in	minutes		X	X	X
max-transfer-time-out	minutes		X	X	X
max-udp-size	size specification	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	---	---
min-refresh-time	seconds		X	X	X
min-retry-time	seconds		X	X	X
minimal-responses	yes, no		X	---	---
multi-master	yes, no		X	X	X
notify	yes, no, explicit, master-only		X	X	X
notify-delay	seconds	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	X	X
notify-source	IPv4 address port		X	X	X
notify-source-v6	IPv6 address port		X	X	X
other-view-options	multilined text		X	---	---
other-zone-options	multilined text		---	X	X
preferred-glue	A, AAAA, NONE		X	---	---
provide-ixfr	yes, no		X	---	---
recursion	yes, no		X	---	---
request-ixfr	yes, no		X	---	---
root-delegation-only	exclude domain list		X	---	---
sig-validity-interval	days		X	X	X

Option Name	**Values**	**Notes**	**View level**	**Zone level**	**Server level**
transfer-format	one-answer, many-answers		X	---	---
transfer-source	IPv4 address port		X	X	X
transfer-source-v6	IPv6 address port		X	X	X
update-check-ksk	yes, no	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	X	X
use-alt-transfer-source	yes, no		X	X	X
zero-no-soa-ttl	yes, no	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	X	X
zero-no-soa-ttl-cache	yes, no	Supported for: • BIND 9.4 and higher • Lucent DNS 4.1 and higher	X	---	---
zone-statistics	yes, no		X	X	X

DNS Views administration

Zone hierarchy and DNS Views

Description

The Zone hierarchy page is split into two areas:

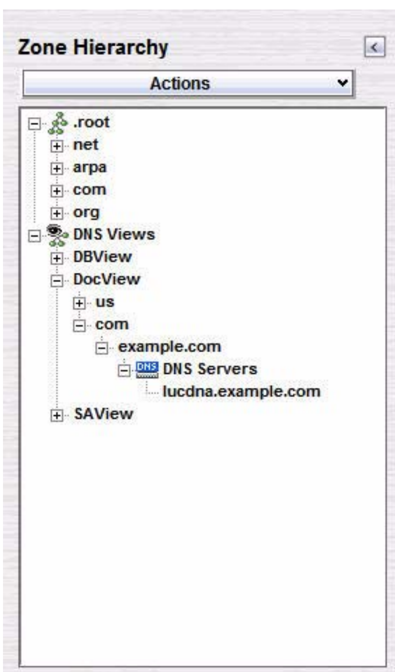
- Global zones (.root)
- DNS Views

Any zones that reside in the global namespace appear under **.root** in the Zone hierarchy and are referred to as global zones. When DNS Views are created, the views appear under **DNS Views** in the Zone hierarchy.

Sample Zone Hierarchy and DNS Views

The following figure shows an example with global zones and DNS Views defined.

Figure 15-8 Zone hierarchy with global zones and DNS Views



Search for a DNS View

Purpose

Use this procedure to search for a DNS View.

Procedure

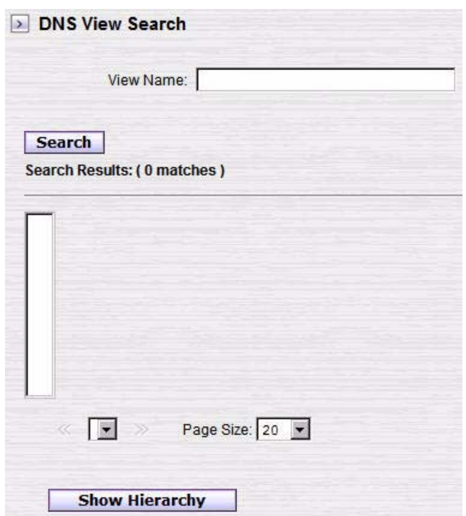
To search for a DNS View, follow these steps:

1. Mouse over **DNS** and click **Zone**.

   Result: The Zone Hierarchy page opens.

2. Mouse over the **Action** menu and select **DNS View Search**.

   Result: The DNS View Search page opens.



3. In the **View Name** field, enter the first few letters of the DNS view and the wildcard character (*) as needed. If you leave this field blank, a list of all views is returned.

4. If user defined attributes or fields are associated with DNS Views, you can use user defined attributes or fields as search criteria. For more information, refer to "Use user defined fields as search criteria" (p. 7-25) or "Use user defined attributes as search criteria" (p. 7-26)

5 Click **Search**.

Result: The results appear in the Search Results list.

6 In the Search Results list, highlight a view.

7 Click **Show Hierarchy**.

Result: The DNS View is added to the Zone Hierarchy and highlighted. The DNS View Properties page opens.

END OF STEPS

Add a DNS View

Purpose

Use this procedure to add a DNS View.

Procedure

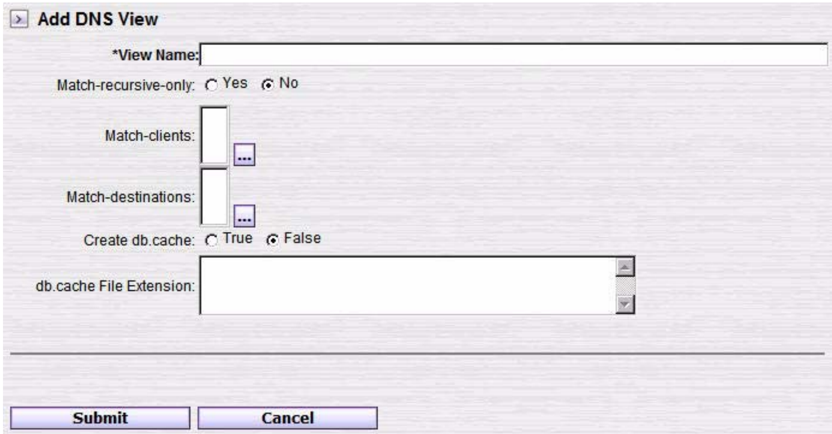
To add a DNS View, follow these steps:

1 Mouse over **DNS** and click **Zone**.

Result: The Zone Hierarchy page opens.

2 Mouse over the **Actions** menu and select **Add DNS View**.

Result: The Add DNS View page opens.



3 Enter the values. Review the following table for a description of the fields.

Table 15-4 Add DNS View fields

Field	Description
View Name	The name of the DNS view. Valid characters are 0-9, a-z, A-Z, - (dash), _ (underscore), and . (dot).
Match-recursive-only	Determines whether a client request matches a view based on whether it is requesting recursion. Select one of the following: • **Yes** • **No** (default setting)
Match-clients	A list of ACL elements that will cause a query to match the DNS View based on the requesting client criteria. Use the Set Match-clients dialog box to add criteria. Refer to "Assign ACL elements to a DNS View" (p. 15-22) for instructions.
Match-destination	A list of ACL elements that will cause a query to match the DNS View based on the receiving destination criteria. Use the Set Match-destinations dialog box to add criteria. Refer to "Assign ACL elements to a DNS View" (p. 15-22) for instructions.
Create db cache	Generate a *db.cache* file and appropriate *named.conf* entry specific to this DNS View. The default file always contains a TTL directive. Select one of the following: • **True** • **False** (default setting)

Field	Description
db.cache File Extension	Determines the contents of a *db.cache* file for the DNS view. The value is printed in the view's *db.cache* file. If no value is specified, and **Create db.cache** is set to true, a *db.cahe* file is created with only a TTL statement.

4 Click **Submit**.

Result: A dialog box open that indicates if the DNS View was successfully added.

END OF STEPS

Assign ACL elements to a DNS View

Purpose

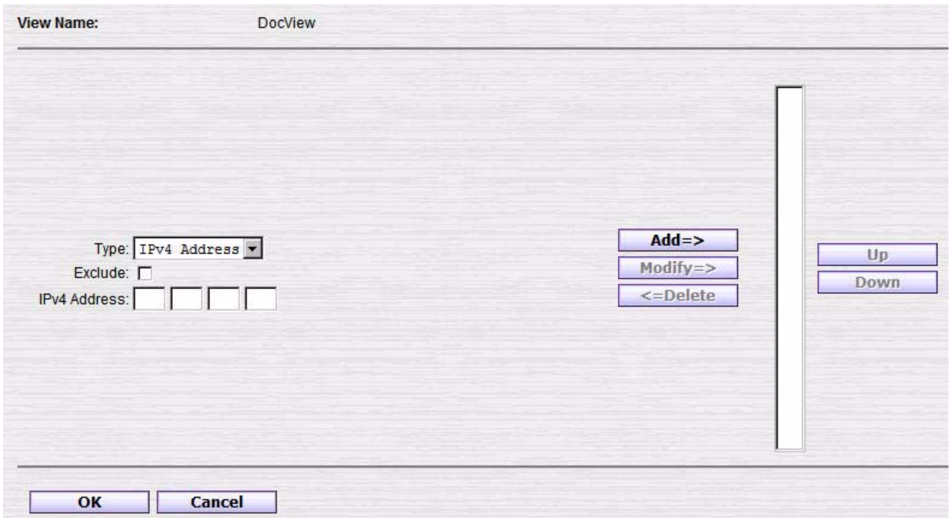
Use these instructions to assign ACL elements to a DNS View.

Procedure

To assign ACL elements to a DNS View, follow these steps:

1 Click **...** next to the **Match-clients** or **Match-destinations** field.

Result: Depending on the field you are adding to the ACL elements, The Set Match-clients or Set Match-destinations dialog box opens. The dialog boxes are identical to each other.



2 Choose one of the following actions.

If you are…	**Then…**
Adding a IPv4 address element	1. In **Type** field, select **IPv4 Address**. 2. Check **Exclude** to prevent access when matching this element. 3. In the **IPv4 Address** field, enter an IPv4 address. 4. Click **Add**. **Result:** The IPv4 address is added to the list.
Adding a IPv4 network element	1. In **Type** field, select **IPv4 Network**. 2. Check **Exclude** to prevent access when matching this element. 3. In the **Address** field, enter an IPv4 network address. 4. In the **Length** field, select the network length (mask). 5. Click **Add**. The IPv4 network is added to the list.
Adding a IPv6 address element	1. In **Type** field, select **IPv6 Address**. 2. Check **Exclude** to prevent access when matching this element. 3. In the **IPv6 Address** field, enter an IPv6 address. 4. Click **Add**. The IPv6 address is added to the list.

<table>
<tr><th>If you are…</th><th>Then…</th></tr>
<tr><td>Adding a IPv6 network element</td><td>1. In Type field, select IPv6 Network.
2. Check Exclude to prevent access when matching this element.
3. In the IPv6 Network field, enter a network address.
4. In the Length field, select an IPv6 network length (prefix).
5. Click Add.

Result: The IPv6 network is added to the list.</td></tr>
<tr><td>Adding an ACL template element</td><td>1. In Type field, select ACL Template.
2. Check Exclude to prevent access when matching this element.
3. In the ACL Template field, enter an ACL template or click ... to search and select an ACL Template.
4. Click Add.

Result: The ACL template is added to the list.</td></tr>
<tr><td>Adding a key ACL element</td><td>1. In Type field, select Key.
2. Check Exclude to prevent access when matching this element.
3. In the Key field, enter a key name.
4. Click Add.

Result: The key is added to the list.</td></tr>
<tr><td>Adding other types of elements</td><td>1. In Type field, select Other.
2. Check Exclude to prevent access when matching this element.
3. In the Other field, select one of the following:
- any
- none
- localhost
- localnets
- Text
4. If you selected Text, enter the desired text in the Text field.
5. Click Add.

Result: The element is added to the list.</td></tr>
<tr><td>Modifying an element</td><td>1. Select an element from the list.

Result: The Proper Type is selected and the fields are populated with the selected element information.

2. Make the appropriate changes.
3. Click Modify.

Result: The element is updated in the list.</td></tr>
<tr><td>Deleting an element</td><td>1. Select an element from the list.
2. Click Delete.

Result: The element is deleted from the list.</td></tr>
</table>

If you are…	**Then…**
Moving an element up and down in the list	1. Select an ACL element from the list. 2. Click: – **Up** to move the element one row up in the list – **Down** to move the element one row down in the list. **Result:** The element is moved one row up or down in the list. **Note:** You must click **Submit** on the Modify DNS View page for your changes to be saved.

3 Click **OK**.

Result: The **Match-clients** or **Match-destinations** field is updated.

END OF STEPS

Modify a DNS View

Purpose

Use this procedure to modify a DNS View.

Procedure

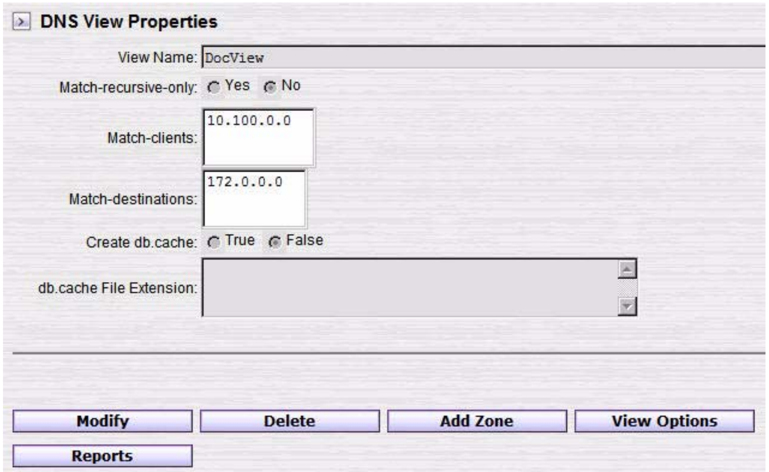
To modify a DNS View, follow these steps:

1 Mouse over **DNS** and click **Zone**.

Result: The Zone Hierarchy page opens.

2 Expand the hierarchy and select a DNS View.

Result: The DNS View Properties page opens.



3 Click **Modify**.

Result: The Modify DNS View page.

4 Make the necessary changes. Refer to Table 15-4, "Add DNS View fields" (p. 15-21) for information on the fields.

5 Click **Submit**.

Result: A dialog box open that states whether the changes were made.

6 Click **OK**.

END OF STEPS

Delete a DNS View

Purpose

Use this procedure to delete a DNS View.

Procedure

To delete a DNS View, follow these steps:

1 Mouse over **DNS** and click **Zone**.

Result: The Zone Hierarchy page opens.

2 Expand the hierarchy and select a DNS View.

Result: The DNS View Properties page opens.

3 Click **Delete**.

Result: A dialog box opens with the message **Are you sure you want to delete the select DNS View?**

4 Click **OK**.

END OF STEPS

Order DNS Views

Purpose

Use this procedure to specify the order in which DNS Views appear in the *named.conf* file. This operation does not impact the Zone hierarchy.

Before you begin

New DNS Views are added at the bottom of the order. The DNS View Order determines the order in which the views are defined in the DNS server's *named.conf* configuration file. The order is important as the first DNS View criteria that matches a client request is the DNS View the server uses.

Procedure

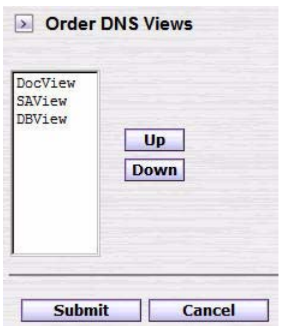
To order the DNS View, follow these steps.

1 Mouse over **DNS** and click **Zone**.

Result: The Zone Hierarchy opens.

2 Mouse over **Actions** and select **Order DNS Views**.

Result: The Order DNS Views page opens.



3 Choose one of the following actions.

If you want to…	Then…
Move a DNS View up higher in the list	1. Select the DNS View. 2. Click **Up** until the view is positioned where you want it.
Move a DNS View lower in the list	1. Select the DNS View. 2. Click **Down** until the view is positioned where you want it.

4 Click **Submit**.

Result: A dialog box opens that states if DNS View orders are saved.

5 Click **OK**.

END OF STEPS

Assign a zone to a DNS View

Purpose

Use this procedure to add a zone to a DNS View.

Before you begin

Review "About DNS Views" (p. 15-3) to determine the best method of adding a shared or view specific zone.

Procedure

To assign a zone to a DNS View, follow these steps:

1 Mouse over **DNS** and click **Zone**.

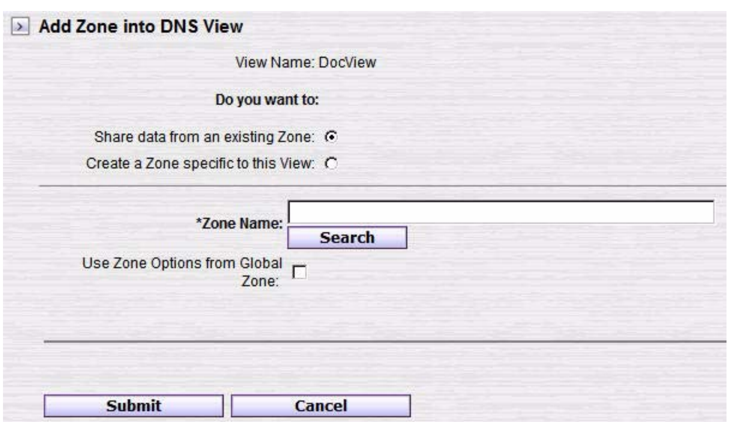
Result: The Zone Hierarchy page opens.

2 Expand **DNS Views** and select the DNS View in which you wish to add the zone.

Result: The DNS View Properties page opens.

3 Click **Add Zone**.

Result: The Add Zone into DNS View page opens.



4 Select either **Share data from an existing zone** or **Create a Zone specific to this View**.

Result: The page displays fields related to this selection. The fields that are displayed depend upon if the type of zone, a shared or view specific zone, you are adding.

5 Enter information as appropriate. Refer to the following table for information on the fields.

Table 15-5 Add Zone into DNS View fields

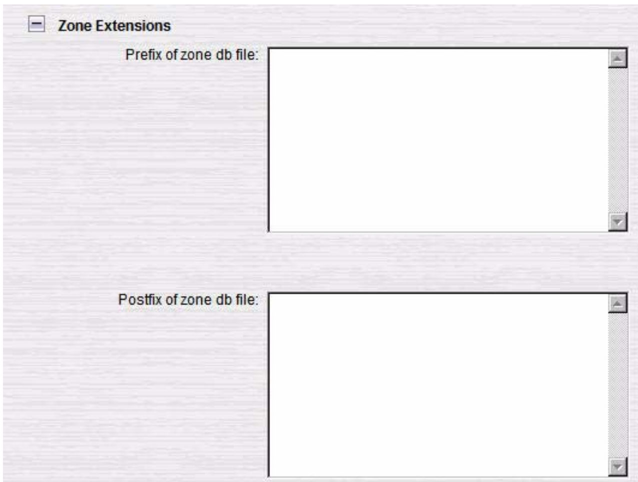
Field	Description
Share data from an existing Zone	Information from an existing zone is assigned to the DNS View. The following fields are displayed:
Zone Name	Enter the name of an existing global zone. Alternatively, click **Search** to find an existing global zone.
Uses Zone Options from Global Zone	Uses the zone options from a global zone.
Create a Zone specific to this View	Creates a zone specific to this DNS View. The following fields are displayed and are all ***required***:
Zone Name	Enter the name of the zone.
Email Address	The email address that appears in the SOA record for the zone. You must have a value for this field.
Expire Time	When the Expire Time is reached, a slave server will cease to be authoritative for the zone because the data is too old to be useful. The default value is 604,800 seconds (one week).
Refresh Time	The refresh time dictates how often a secondary server verifies its data. The default is 21,600 seconds (six hours).
Retry Time	The retry time dictates the interval of subsequent refresh attempts in the event that a previous attempt has failed. The default value is 3,600 seconds (one hour).
Default TTL	The default Time to Live value is used for the $TTL statement at the beginning of the zone file and defines the Time to Live value for any resource records that do not have an explicit TTL in the zone file. The TTL (Time To Live) is supplied with query responses. The default value is 86,400 seconds (one day).
Negative Cache TTL	The Negative Cache TTL is the Time to Live for negative responses (NXDOMAIN responses). The default value is 600 seconds (ten minutes).

Zone extensions

Zone extensions can be added to view specific zones.

6 Expand **Zone Extensions** section.

Result: The **Zone Extensions** section opens.



7 Enter the appropriate information in the fields. Refer to the following table for a description of the fields.

Note: Refer to *`DNS and BIND`*, by Cricket Liu and Paul Albitz for details on proper zone data syntax.

Table 15-6 Zone Extensions fields

Field	Description
Prefix of zone db file	Text appears before the SOA record in the zone file exactly as you enter it. For example: `$TTL 86400`

Postfix of zone db file	Text appears at the end of the zone file exactly as you enter it. You must use proper DNS
	syntax. For example:
	`mailhost2IN A198.200.138.234`
	`mailhost1IN MXmailhost2.example.com.`
	`oneilltIN A198.200.138.236`
	`myaliasIN smtp.example.com.`

8 Click **Submit**.

Result: A dialog box open that indicates if the zone is successfully added to the DNS View.

END OF STEPS

Modify a zone

Purpose

Use this procedure to modify a zone at the DNS View level.

Before you begin

Shared zones cannot be modified. Shared zones inherit global namespace data.

Procedure

To modify a view specific zone, follow these steps:

1 Mouse over **DNS** and click **Zone**.

Result: The Zone Hierarchy opens.

2 Expand **DNS Views**, the appropriate DNS View name, any necessary folders, and select a zone.

Result: The Zone Properties page opens.

3 Click **Modify**.

Result: The Modify Zone (View Specific) page opens.

4 Make the necessary changes.

5 Click **Submit**.

Result: A dialog box opens that states whether the changes were successfully saved.

6 Click **OK**.

END OF STEPS

Delete a zone from a DNS View

Purpose

Use this procedure to remove a zone from a DNS View.

Before you begin

- Deleting a shared zone from a DNS View does not affect the global zone or other shared zones.
- Deleting a view specific zone deletes the view specific zone from the view, but not the view specific fully qualified domain names and domain names associated with objects and nodes.

Procedure

To delete a zone, follow these steps:

1 Mouse over **DNS** and click **Zone**.

Result: The Zone Hierarchy opens.

2 Expand **DNS Views** until you come to the zone to delete.

Result: The Zone Properties page opens.

3 Click **Delete**.

Result: A dialog box opens with the message **Are you sure you want to delete the select Zone?**

4 Click **OK**.

END OF STEPS

Assign/remove a primary server to/from a zone

Purpose

Use this procedure to assign a primary server to a zone in a DNS View.

Assign a primary to zone

To assign a primary server, follow these steps:

1 Mouse over **DNS** and click **Zone**.

Result: The Zone Hierarchy page opens.

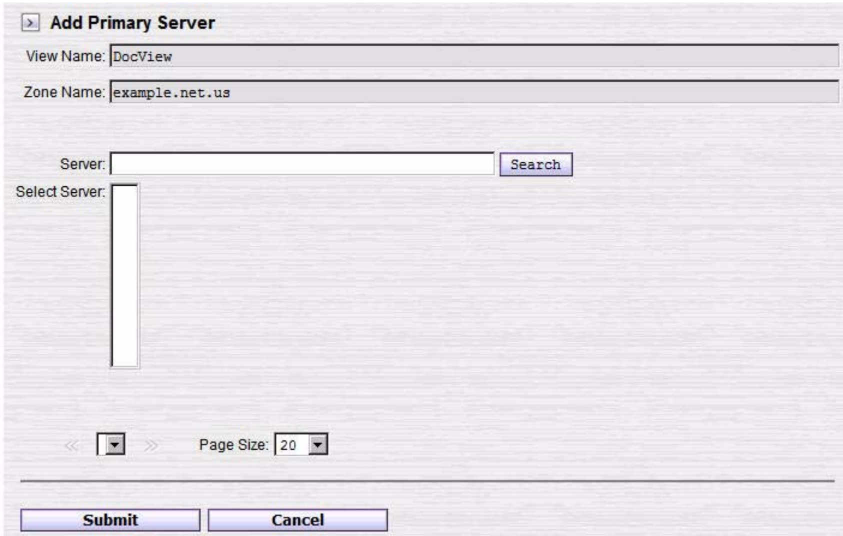
2 Expand the hierarchy for which you want add a primary server to the zone.

3 Select the zone.

Result: The Zone Properties page opens.

4 Click **Add Primary Server**.

Result: The Add Primary Server page opens.



5 In the **Server** field, enter the first few letters of the server name and the wildcard character (*) as needed. If you leave this field blank, a list of all DNS servers is returned.

6 Click **Search**.

Result: The results appear in the Search Results list.

7 In the **Search Results** list, highlight one or more servers.

8 Click **Submit**.

Result: A dialog box opens that states all servers are added.

END OF STEPS

Remove a primary server from a zone

To remove a primary server from a zone, follow these steps:

1 Expand the Zone hierarchy until you come to the primary server to remove.

2 Select the primary server.

Result: The Primary DNS Server page opens.

3 Click **Remove Server from Zone**.

Result: A dialog box opens with the message **Remove Primary Server from Zone?**

4 Click **OK**.

Result: The server and any secondary servers associated with this server are removed from the zone.

END OF STEPS

Assign/remove a secondary server to/from a zone

Purpose

Use this procedure to assign a secondary server to primary server for a zone in a DNS View.

Before you begin

- Do not assign a secondary server if you are unfamiliar with primary and secondary server relationships.
- A primary server must be assigned to the zone before you can add a seconadary server.
- Make sure the secondary server match the correct DNS View on the primary server for the zone.

Assign a secondary server to a zone

To assign a secondary server, follow these steps:

1 Mouse over **DNS** and click **Zone**.

Result: The Zone Hierarchy page opens.

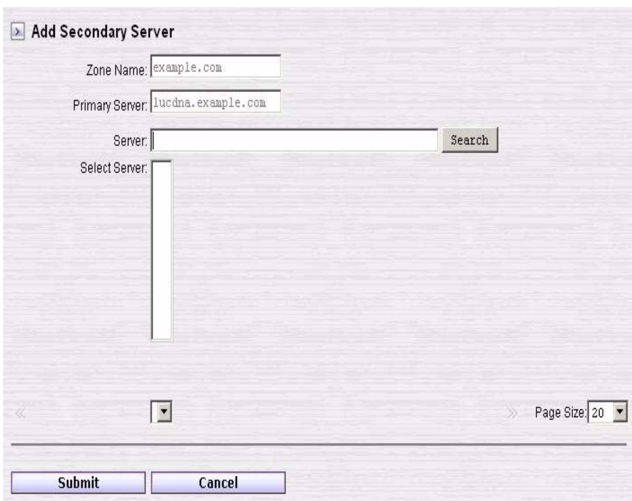
2 Expand the hierarchy until you come to the primary server for which you want to add a secondary server.

3 Select the primary server.

Result: The Primary DNS Server page opens.

4 Select **Add Secondary Server**.

Result: The Secondary DNS Server page opens.



5 In the **Server** field, enter the first few letters of the server name and the wildcard character (*) as needed. If you leave this field blank, a list of all Lucent DNS 4.x and BIND 9.x DNS servers is returned.

6 Click **Search**.

Result: The results appear in the Search Results list.

7 In the **Search Results** list, highlight one or more servers.

8 Click **Submit**.

Result: A dialog box opens that states all servers are added.

END OF STEPS

Remove a secondary server from a zone

To remove a secondary server from a zone, follow these steps:

1 Expand the Zone hierarchy until you come to the secondary server to remove.

2 Select the secondary server.

Result: The Secondary DNS Server page opens.

3 Click **Remove Server from Zone**.

Result: A dialog box opens with the message **Remove Secondary Server from Zone?**

4 Click **OK**.

Result: The server is removed from the zone.

END OF STEPS

Set view and zone options

Purpose

Use this procedure to assign options to the DNS View, zone, and server levels.

Before you begin

- Not all options are valid at every level. Refer to "Option management in DNS Views" (p. 15-9) for more information.
- For descriptions of options, refer to *DNS and BIND* by By Paul Albitz and Cricket Liu.

Procedure

To assign view or zone options, follow these steps:

1 Choose one of the following actions.

If you are setting...	Then...
Zone options for a DNS View	1. Mouse over **DNS** and click **Zone**. **Result:** The Zone Hierarchy page opens. 2. Expand the hierarchy until you come to the a DNS View for which you want to add view options. 3. Select the DNS View. **Result:** The DNS View Properties page opens. 4. Select **View Options**. **Result:** The View Options page opens.
Zone options at the zone level	1. Mouse over **DNS** and click **Zone**. **Result:** The Zone Hierarchy page opens. 2. Expand the hierarchy until you come to the zone for which you want to add zone options. 3. Select the zone. **Result:** The Zone Properties page opens. 4. Select **Zone Options**. **Result:** The Zone Options page opens.
Zone options at the server level	1. Mouse over **DNS** and click **Zone**. **Result:** The Zone Hierarchy page opens. 2. Expand the hierarchy until you come to the primary or secondary server for which you want to add zone options. 3. Select the server. **Result:** The Primary DNS Server or Secondary DNS Server page opens. 4. Select **Server Zone Options**. **Result:** The Zone Options on Primary or Zone Options on Secondary page opens.

2 Set your options.

3 Click **Submit**.

Result: A dialog box opens that states if the zone options where saved.

END OF STEPS

16 IPv6 address management

Overview

Purpose

This chapter describes IPv6 address management.

Contents

This chapter covers these topics.

IPv6 address management

Overview

Purpose

In contrast to IPv4, IPv6 uses 128-bit addresses. IPv6's 128-bit address system creates 340,282,366,920,938,463,463,374,607,431,768,211,456 or 3.4×10^{38} unique addresses.

The huge number of addresses that IPv6 provides should be ample for the estimated billions of new Internet appliances - such as mobile phones and personal digital assistants (PDAs) - that will require IP addresses in the future.

IPv6's new capabilities should provide better quality of service. For example, packet-queuing mechanisms will control the flow of traffic on the network.

Certain packets of data - audio or video files, for example - can be labeled so that they are prioritized over other data and users receive real-time service.

The goal of IPsec is to provide security services for IPv4 and IPv6. All IPv6 hosts are required to support IPsec.

IPv6's autoconfiguration feature - known as autodiscovery - should allow systems to connect to an IPv6 network more easily than to an IPv4 network.

IPv6 address structure

Overview

IPv6 addresses are comprised of eight sections, with each section separated from the next by a colon. Each section is represented with a 4-character hexadecimal value. An example IPv6 address follows:

`2001:fecd:ba23:cd1f:dcb1:1010:9234:4088`

While each section can have a maximum of four characters, only one character is required. Allowable characters are 0 to 9 and a to f. Alphabetic characters are not case-sensitive.

Abbreviation of IPv6 addresses

Some IPv6 addresses can have several sections that contain only zeros, such as the following example:

`fec0:1:0:0:0:0:0:1234`

Instead of writing out several sections that contain only a zero, there is a special notation available to abbreviate this type of address. The zeros can be replaced with two colons. The sections containing the zeros must be contiguous, and the two colons can only be used once in any address. The above address can be abbreviated as follows:

`fec0:1::1234`

The number of visible sections, plus the number of sections containing zeros must comprise a total of eight sections.

IPv6 and IPv4 addresses on the same network

Some non-VitalQIP networks contain both IPv4 and IPv6 addresses. In this type of network environment IPv4 addresses are mapped to IPv6 addresses. The addresses used are IPv6, but the last four sections of these addresses contains a valid IPv4 address. An example address is as follows:

`fe:a90::10.1.2.3`

In the previous example, the last four sections of the address are a valid IPv4 address, but the entire address is a valid IPv6 address.

IPv6 hierarchy

Overview

Address management uses a hierarchy that displays the allocation of addresses hierarchically under existing seed pools.

IPv6 address management allows you to add, delete, move or modify IPv6 address ranges or subnets.

Add a seed block

Purpose

Use this procedure to add a seed block. Seed blocks are added in IPv6 Address Management when you do not want to associate an address block with any registry or when you do not want to perform automatic allocation of address blocks using rules. If you want to do either of those things, allocate the seed block in the Address Allocation module.

Procedure

1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

2 Mouse over the **Actions** menu and select **Add Seed Block**.

Result: The Add Seed Block page opens.

3 Enter a valid IPv6 address in the **Start Address** field.

4 Select a value for the **Length** field from the drop-down list. Allowable values are from 8 to 64.

5 Click **Submit**.

Result: A dialog box opens with the message **Seed Block Added - <IP_Address/length>.**

6 Click **OK**.

Result: The seed block is added to the IPv6 Address Hierarchy and the Seed Block Properties page for the block opens.

END OF STEPS

Delete a seed block

Purpose

Use this procedure to delete a seed block created in Address Management.

Before you begin

- If a seed block is created in address allocation, you cannot delete it.
- You also cannot delete a seed block that contains subnets.

Procedure

1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

2 Expand the list of seed blocks and select the one you want to delete.

Result: The Seed Block Properties page opens.

3 Click **Delete**.

Result: A dialog box opens with the message **Are you sure you want to delete the selected Seed Block?**

4 Click **OK**.

Result: A dialog box opens with the message **Seed Block Deleted.**

5 Click **OK**.

Result: The IPv6 Address Hierarchy is updated and the IP Management splash screen opens.

END OF STEPS

Add an address range

Purpose

An address range is a Alcatel-Lucent defined object. It is a way of visually grouping subnets within a seed block. It is defined by its prefix and length and provides a shortcut to allow administrators to visually organize subnets in whichever way they organize, group and manage the address space. There is no business logic associated with an address range and hence it is optional to use them.

Characteristics of the address range include the following:

- Address ranges are defined as a single IPv6 address prefix and length.
- Address space represented by the address range can be of any length from /9 to /128.
- Address ranges have unique prefixes and lengths.
- Address ranges are optional. The user can create subnets directly under the seed block.
- Address ranges are not hierarchical. A subnet appears in the address range with the greatest prefix length.
- Since address ranges are only for visually grouping addresses, when an address range is deleted, the subnets contained within it are not deleted.
- Address ranges can be added to seed blocks created by either address management or in address allocation.

Procedure

To add an address range, use these steps:

1. Mouse over **Address Management** and click **IPv6**.

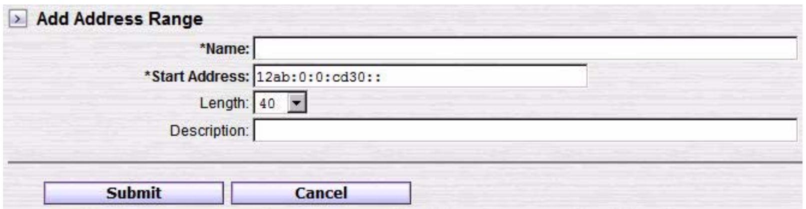
   Result: The IPv6 Hierarchy opens.

2. Expand the list of seed blocks and select the one to which you want to add an address range.

   Result: The Seed Block Properties page opens.

3 Click **Add Address Range**.

Result: The Add Address Range page opens.



4 Enter a name in the **Name** field. This value can be alphanumeric, and up to 64-characters long.

5 Enter a valid IP address in the **Address** field.

6 Select a value from the drop-down list for the **Length** field. Allowable values are from 9 to 128.

7 Optionally, enter a text description in the **Description** field.

8 Click **Submit**.

Result: A dialog box opens with the message **Address Range created successfully!**

9 Click **OK**.

Result: The IPv6 Address Hierarchy is updated and the Address Range Properties page opens.

END OF STEPS

Modify an address range

Purpose

Use the following procedure to modify an address range.

Procedure

To modify an address range, follow these steps.

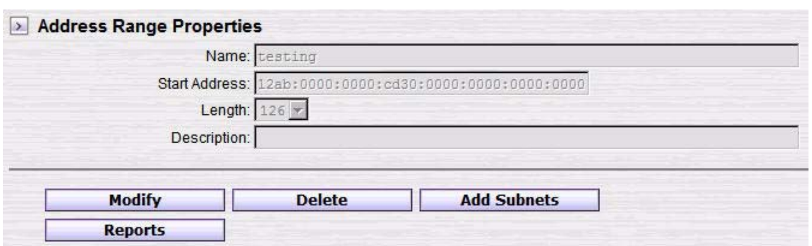
1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

2 Expand the seed block and address ranges until the address range you want to modify is visible.

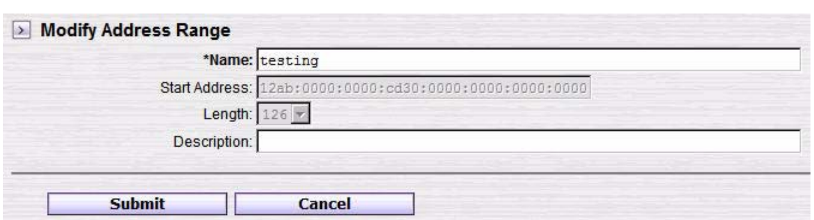
3 Select the address range you want to modify.

Result: The Address Range Properties page opens.



4 Click **Modify**.

Result: The Modify Address Range page opens.



5 Modify the **Name** or **Description** fields. These are the only fields you can modify in address range after it is created. Refer to "Add an address range" (p. 16-7) for descriptions of these fields.

6 When you have finished modifying the address range, click **Submit**.

Result: A dialog box opens with the message: **Address Range Modified successfully!**

7 Click **OK**.

Result: The IPv6 Address Hierarchy is updated and the Address Range Properties page opens.

END OF STEPS

Delete an address range

Purpose

Use the following procedure to delete an address range.

Procedure

To delete an address range, follow these steps.

1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

2 Expand the seed block and address ranges until the address range you want to delete is visible.

3 Select the address range you want to delete.

Result: The Address Range Properties page opens.

4 Click **Delete**.

Result: A dialog box opens with the message **Are you sure you want to delete the selected address range?**

5 Click **OK**.

Result: A dialog box opens with the message **Address Range Deleted successfully!**

6 Click **OK**.

Result: The address range is removed from the IPv6 Address Hierarchy and the IP Management splash screen opens. Subnets that previously appeared in the hierarchy under that address range now appear in the next most specific address range.

END OF STEPS

Add a subnet

Purpose

Use the following procedure to add a subnet to a seed pool or address range.

Procedure

To add a subnet, follow these steps.

1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

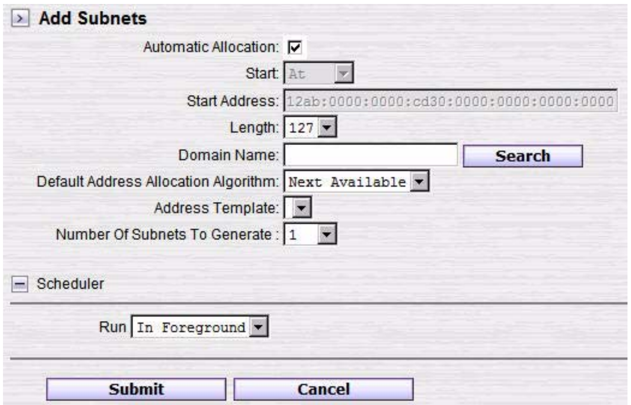
2 Expand the seed block and address ranges until either the seed pool or the address range to which you want to add subnets is visible.

3 Select the seed pool or address range to which you want to add a subnet.

Result: The Seed Pool Properties page or the Address Range Properties page opens.

4 Click **Add Subnets**.

Result: The Add Subnets page opens.



5 Review the following table and fill in the fields as necessary.

Table 16-1 Add subnet fields

Field	Description
Automatic Allocation	***Optional.*** If this box is checked, the Start and Start Address fields are not editable. VitalQIP uses the Best From Start (BFS) contiguous address blocks algorithm and generates contiguous addresses. If the contiguous space is not available, it allocates the next best address that is available. If this box is not checked, you are using explicit allocation, and you must enter a value in the **Start** and **Start Address** fields.
Start	***Required if the Automatic Allocation is checked.*** Only available if the Automatic Allocation box is not checked. Select a value from the drop-down list. • **At** - Subnet starts at this address. • **After** - Subnet starts after this address.
Start Address	***Required.*** if the Automatic Allocation box is not checked. Enter a valid IPv6 address. Defaults to the starting address of the current address range or seed block.
Length	***Optional***. Length of the new subnet. Select a value from the drop-down list. Allowable values are 9 to 128. Defaults to 64.

Field	Description
Domain Name	***Optional***. The Default Domain name for all nodes created in this subnet. Enter the name of the domain you want to use. If you want to search for a list of domains, refer to "Search for a domain" (p. 16-29) for information on this function.
Default Address Allocation Algorithm	***Optional***. Used when creating IP addresses within this subnet. Select a value from the drop-down list. Allowable values are as follows: • **Next Available** (default) • **Last Available** • **Random** • **Specific**
Address Template	***Optional***. Select an address template from the drop-down list to specify nodes to automatically create when this subnet is created.
Number of Subnets to Generate	***Required***. Number of subnets to be created. Allowable values are from 1 to 256. The default is 1.

6 Choose when to add subnets in the **Scheduler** section. Refer to "Schedule subnet configuration" (p. 16-13) for more information.

7 Click **Submit**.

Result: Choose from the following results.

If...	Then...
The job is scheduled in foreground	The report opens.
The job is scheduled in background or at a later time.	The Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Schedule subnet configuration

Purpose

Use this procedure to schedule jobs when you need to perform the following actions:

- Add subnets
- Split subnets
- Renumber blocks in a subnet

Procedure

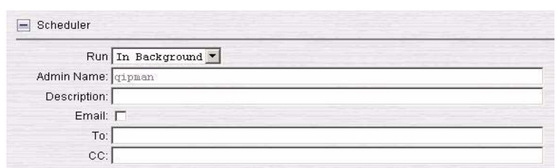
To schedule a job if you are adding, splitting, or renumbering a subnet, follow these steps.

1 Expand the **Scheduler** section, if necessary.

2 Choose one of the following actions.

<table>
<tr><th>If you want to…</th><th>Then…</th></tr>
<tr><td>Run the job immediately</td><td>Ensure that In Foreground is selected in the Run drop-down list.</td></tr>
<tr><td>Run the job in background</td><td>1. Select In Background from the Run drop-down list.

Result: The Scheduler section expands to display additional fields.



The Admin field displays the login ID of the administrator who is scheduling the job.

2. Enter a description of the job in the Description field. If you do not enter a description, a description of <Job Name>:<Run Mode> is used. You may enter up to 255 characters.
3. If you want an e-mail to be sent when the job completes, place a check in the Email check box.

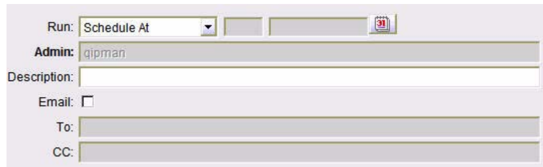
Result: The To and CC fields are enabled.

4. Enter an e-mail address of up to 255 characters in the To field. If an e-mail address has been entered in the Contact Profile for the administrator, it appears by default.
5. If desired, enter a CC e-mail address.</td></tr>
</table>

<table>
<tr><th>If you want to...</th><th>Then...</th></tr>
<tr><td>Schedule the job for a later time</td><td>

1. Select **Scheduled At** from the **Run** drop-down list.

Result: The Scheduler section expands to display additional fields, including a calendar icon.



The **Admin** field displays the login ID of the administrator who is scheduling the job.

2. Click the Calendar icon ( ).

Result: The Calendar widget opens with the scheduled date default of 10 days from the current date.

3. Choose from the following actions.
   a. To choose a different time, click in the hour and minute fields and enter a new time in 24-hour format.
   b. To choose a different month, choose a later month from the month drop-down list.
   c. To choose a different year, click > to enter a future year or < to return to a prior year.
   d. To choose a different day, click another day in the month.

Result: After a different day is clicked, the calendar widget closes and a new run date and/or time are displayed.

4. Enter a description of the job in the **Description** field. If you do not enter a description, a description of `<Job Name>:<Run Mode>` is used. You may enter up to 255 characters.

</td></tr>
</table>

If you want to...	Then...
	1. If you want an e-mail to be sent when the job completes, place a check in the **Email** check box. **Result:** The **To** and **CC** fields are enabled. 2. Enter an e-mail address of up to 255 characters in the **To** field. If an e-mail address has been entered in the **Contact Profile** for the administrator, it appears by default. 3. If desired, enter a **CC** e-mail address.

3 Click **Submit**.

Result: The result depends on which Run option you chose and which subnet function you were performing. Refer to:

- "Add a subnet" (p. 16-11)
- "Split a subnet" (p. 16-18)
- "Renumber a subnet" (p. 16-21)

END OF STEPS

Modify a subnet

Purpose

Use the following procedure to modify subnets.

Procedure

To modify a subnet, follow these steps.

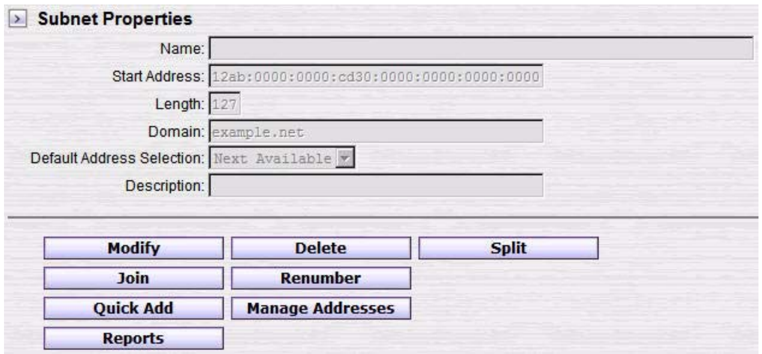
1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

2 Expand the seed block and address ranges until the subnet you want to modify is visible.

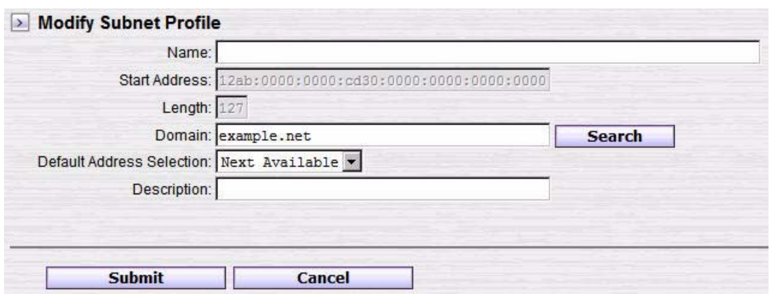
3 Select the subnet you want to modify.

Result: The Subnet Properties page opens.



4 Click **Modify**.

Result: The Modify Subnet Profile page opens.



5 You can modify the Name, Domain, Default Address Selection, Description, and any Attributes associated with the subnet. Refer to Table 16-1, "Add subnet fields" (p. 16-12) for a detailed description of these fields.

6 Click **Submit** when you are finished.

Result: A dialog box opens with the message **Subnet modified.** The IPv6 Hierarchy is updated.

7 Click **OK**.

Result: The Subnet Properties page opens.

END OF STEPS

Split a subnet

Purpose

Use the following procedure to split a subnet.

Procedure

To split a subnet, follow these steps.

1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

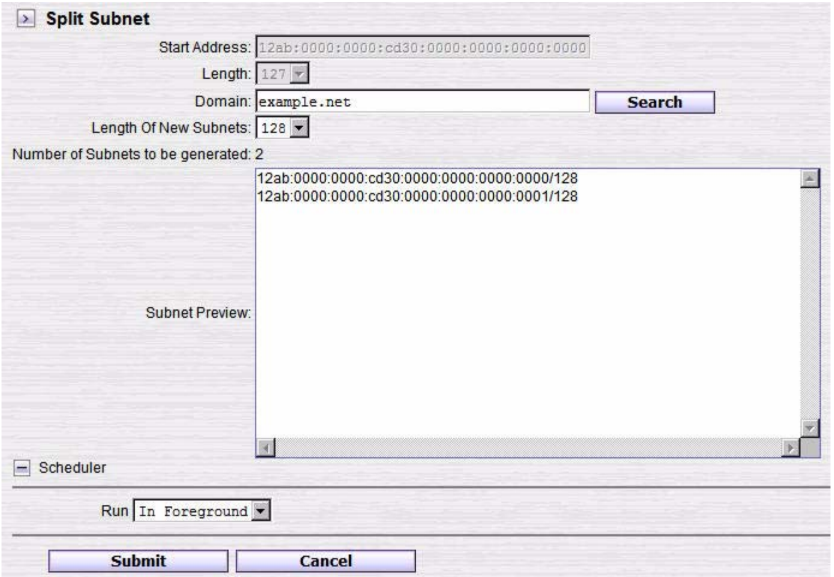
2 Expand the seed block and address ranges until the subnet you want to split is visible.

3 Select the subnet you want to split.

Result: The Subnet Properties page opens.

4 Click **Split**.

Result: The Split Subnet page opens.



5 Select a value from the **Length of New Subnets** drop-down list. This drop-down list contains only values smaller than the subnet you are currently splitting.

Result: The value next to **Number of Subnets to Be Generated** and the list of subnet addresses in **Subnet Preview** change to reflect the length you selected.

6 Choose when to split the subnet in the **Scheduler** section. Refer to "Schedule subnet configuration" (p. 16-13) for more information.

7 Click **Submit**.

Result: Choose from the following results.

If...	Then...
The job is scheduled in foreground	1. A confirmation box opens with the message **Subnet split successfully**. 2. Click **OK**. **Result:** The subnets appear in the IPv6 Address Hierarchy.
The job is scheduled in background or at a later time	1. A confirmation box opens with the message **Job is scheduled. Job ID is <###>. Continue to the job scheduler page?** 2. If you wish to review the job scheduler page, click **OK**. **Result:** The Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information. 3. If you would rather perform another task, click **Cancel**. **Result:** The IP Management splash screen is displayed.

END OF STEPS

Join subnets

Purpose

Use the following procedure to join subnets.

Procedure

To join subnets, follow these steps.

1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

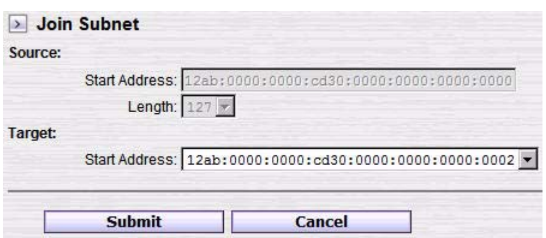
2 Expand the seed block and address ranges until the subnet you want to join with another is visible.

3 Select the subnet you want to join to another.

Result: The Subnet Properties page opens.

4 Click **Join**.

Result: The Join Subnet page opens.



5 Select a start address from the **Target** drop-down list. This drop-down list contains only subnets adjacent to the source subnet.

Note: If there is no adjacent subnet available, a dialog is displayed indicating that there are no available subnets to join with, and the Subnet Properties page is displayed.

6 Click **Submit**.

Result: A dialog box opens with the message **Subnets joined successfully!** and the IPv6 Hierarchy is updated.

7 Click **OK**.

Result: The Subnet Properties page opens.

END OF STEPS

Renumber a subnet

Purpose

Renumber a subnet to change the start address of the subnet. All the IP addresses within the subnet are moved to the same relative position after the new prefix.

Procedure

To renumber subnets, follow these steps.

1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

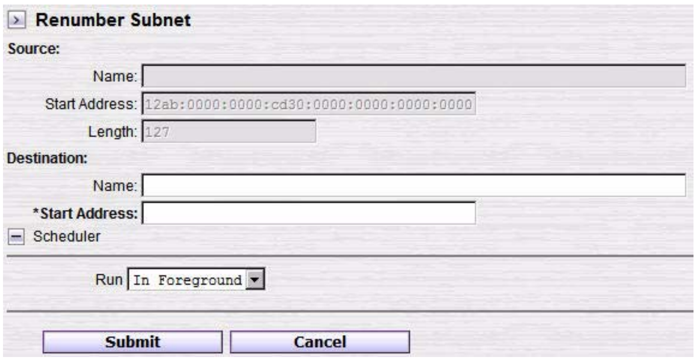
2 Expand the seed block and address ranges until the subnet you want to renumber is visible.

3 Select the subnet you want to renumber.

Result: The Subnet Properties page opens.

4 Click **Renumber**.

Result: The Renumber Subnet page opens.



5 Enter a name in the **Name** field. This field is optional, and defaults to the name of the source subnet.

6 Enter a valid, available IPv6 address in the **Start Address** field. This field is required.

7 Choose when to renumber the subnet in the **Scheduler** section. Refer to "Schedule subnet configuration" (p. 16-13) for more information.

8 Click **Submit**.

Result: Choose from the following results.

If...	Then...
The job is scheduled in foreground	1. A confirmation box opens with the message **Subnet Renumbered Successfully**. 2. Click **OK**. **Result:** The Subnet Properties page is displayed, and the renumbered subnets appear in the IPv6 Address Hierarchy.
The job is scheduled in background or at a later time	1. A confirmation box opens with the message **Job is scheduled. Job ID is <###>. Continue to the job scheduler page?** 2. If you wish to review the job scheduler page, click **OK**. **Result:** The Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information. 3. If you would rather perform another task, click **Cancel**. **Result:** The IP Management splash screen is displayed.

Note: The subnet will have the same length after it is renumbered.

END OF STEPS

Add a node to a subnet

Purpose

Use the following procedure to add a node to a subnet.

Procedure

To add a node to a subnet, follow these steps.

1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

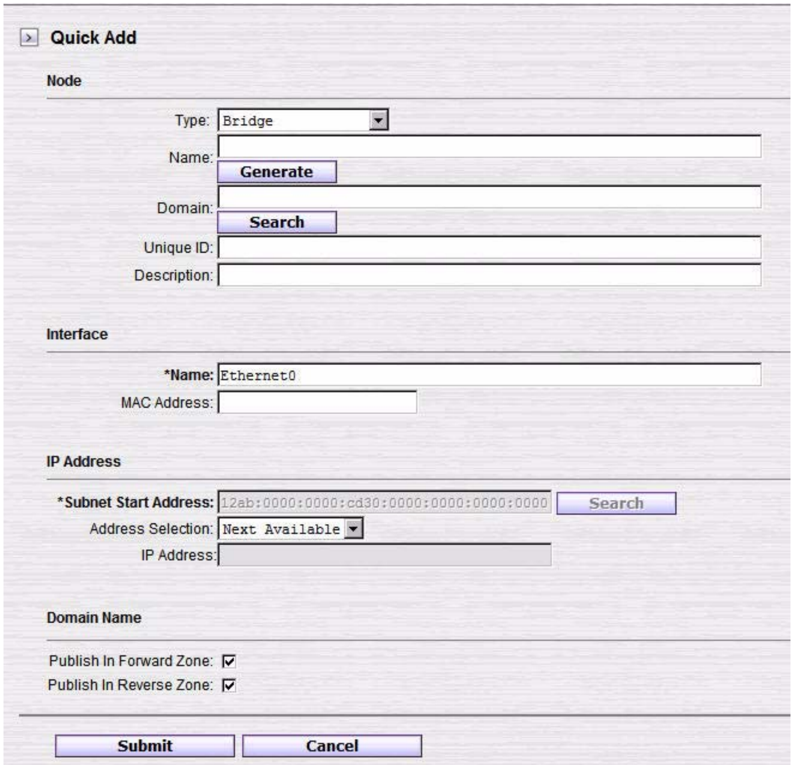
2 Expand the seed block and address ranges until the subnet to which you want to add a node is visible.

3 Select the subnet to which you want to add a node.

Result: The Subnet Properties page opens.

4 Click **Quick Add**.

Result: The Quick Add page opens.



5 Review the following table and fill in the fields as required.

Table 16-2 Quick Add fields

Field	Description
Node	
Type	***Required***. The type of node you are adding. The list of values shown is delivered with VitalQIP, although this list is customizable. The list may therefore contain additional values, or may not contain some values shown in the following list. Allowable values are as follows: • **Workstation** • **X-terminal** • **PC** • **Printer** • **Server** • **Wiring_Hub** • **Router** • **Bridge** • **Terminal_Server** • **Switch** • **Legacy_System** • **Gateway** • **Test_Equipment** • **Undefined** • **Others** • **Partially_Managed**
Name	Name of the node you are adding. You must enter a value in this field, the **Domain** field, or both. You can click **Generate** to automatically generate a node name.
Domain	Domain to which this node is assigned. You can use **Search** to search for a domain. The domain in this field when you first enter it is the default domain for the appropriate subnet. You must enter a value in this field or the **Name** field, or both.
Unique ID	Unique ID assigned to the node. If you do not provide a unique IP address, the system assigns one.
Description	Text description assigned to the node.
Interface	
Name	***Required***. Name of the interface assigned to the node.
Mac Address	MAC address of the interface card assigned to the node.
IP Address	

Field	Description
Subnet Start Address	***Required***. Enter the subnet address that contains the IP address you want to assign to this interface. You can use **Search** to open the Subnet Selection window to select a subnet. If you select a subnet from the Subnet Selection window, this field is populated from that value. When you access this screen from the subnet in the IPv6 Hierarchy as described above, the current subnet start address appears in this field. If you choose **Existing** from the Address Selection field, this field is not editable and **Search** is unavailable.
Address Selection	***Required***. Determines how the address assigned to this interface is determined. Select a value from the drop-down list. Allowable values are as follows: • Next Available • Last Available • Random • Specific If you select **Specific**, you can enter a specific IP address in the **IP Address** field. If you select **Existing**, the **Subnet Start Address**, **Name** and **IP Address** fields are unavailable, and you must select an existing IP Address using **Search** (next to the **Name** field). If you navigated to this screen from a subnet, as described above, the default value is the one defined in the subnet.
IP Address	***Optional***. The IP address you want to add to the interface. You can only enter an IP address if you chose **Specific** in the **Address Selection** field.
Domain Attributes	
Publish in Forward Zone	This checkbox determines if an IPv6 AAAA record for the IPv6 Address is published in a forward zone. The AAAA record is then published in the forward zone for DNS lookups. The default for this value is provided by the Publish AAAA record global policy.
Publish in Reverse Zone	This checkbox determines if a PTR record for the IPv6 Address is published in a reverse zone.. The PTR record is then published in the reverse zone for DNS lookups. The default for this value is provided by the Publish AAAA record global policy.

6 Enter appropriate values for any Attributes.

7 Click **Submit**.

Result: A dialog box opens with the message **Node added successfully!**

8 Click **OK**.

Result: The Manage Addresses in a Subnet page opens. Refer to "Manage addresses in a subnet" (p. 16-27) for additional information.

END OF STEPS

Manage addresses in a subnet

Purpose

Use the following procedure to manage addresses in a subnet.

Procedure

To manage addresses in a subnet, follow these steps.

1 Mouse over **Address Management** and click **IPv6**.

Result: The IPv6 Hierarchy opens.

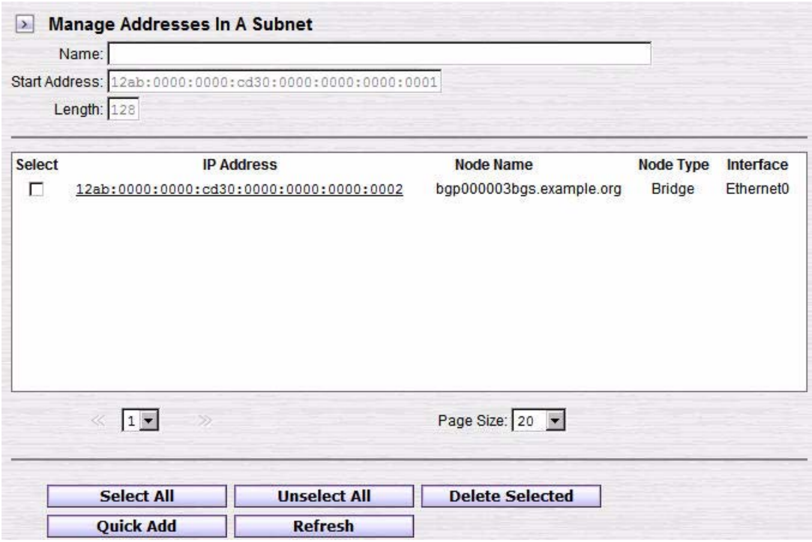
2 Expand the seed block and address ranges until the subnet containing the addresses you want to manage is visible.

3 Select the subnet whose addresses you want to manage.

Result: The Subnet Properties page opens.

4 Click **Manage Addresses**.

Result: The Manage Addresses In A Subnet page opens.



All managed addresses for this subnet (that is, those with a node assigned to them) are displayed on this page.

Delete address from subnet

5 To delete one or more addresses, click the checkbox in the Select column next to the addresses you want to delete, and then click **Delete Selected**.

Result: A dialog box opens with the message **Are you sure you want to delete the selected addresses?**

6 Click **OK**. The addresses are deleted.

7 Click **Refresh** to see an updated list of addresses.

Manage address in subnet

8 To change the properties of an address in a subnet, click the IP address.

Result: A new window opens with the IP address properties. The user can click the **Modify** button to modify the IP Address properties on this new window. The Node Properties page opens. Refer to "Modify a node" (p. 11-17) for details about this screen.

END OF STEPS

Search for a domain

Purpose

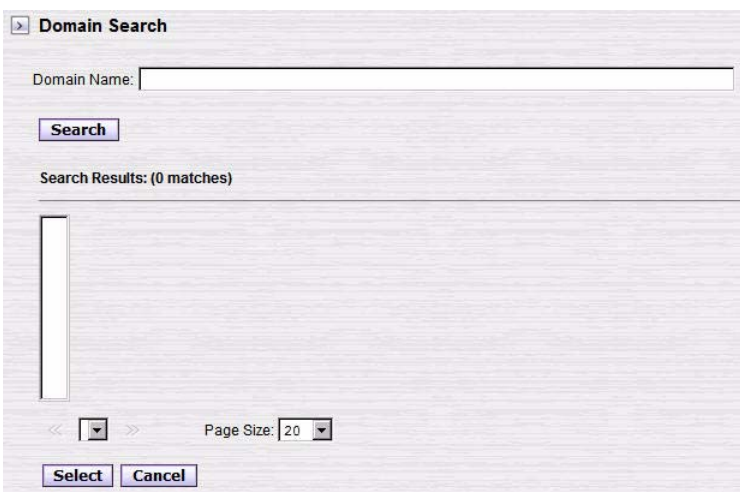
Use this procedure to search for a domain when you are adding subnets.

Procedure

To search for the domain that is associated with a subnet, follow these steps.

1 Click the **Search** button.

Result: The Domain Search dialog box opens.



2 In the **Domain Name** field, enter the first few letters of the domain name. Use the wildcard character (*) as needed. If you enter only the wildcard character, a list of ***all*** domains is returned.

3 Click **Search**.

Result: The results appear in the **Search Results** list.

4 In the **Search Results** list, highlight a domain.

5 Click **Select**.

Result: The Domain Search dialog box closes and the domain you selected is added to the **Domain Name** field.

END OF STEPS

17 DNS configuration file generation

Overview

Purpose

This chapter describes the **DNS Generation** function, which is used to configure, view, and update the policy, data, and configuration files for DNS services.

Contents

This chapter covers these topics.

About DNS file generation

Overview

Purpose

DNS Generation allows you to configure, view, and update the policy, data and configuration files for DNS. Data and configuration files define the behavior of DNS servers through the transmission, or “push” of data to the servers. The information that is transmitted is determined by both the setup of the Infrastructure and the subnet information.

Infrastructure setup

All infrastructure must be set up prior to using **DNS Generation**. A domain, network, DNS server must be defined and configure. Once you have set up the infrastructure and configured the subnets, you can create the necessary files and records required to operate DNS with VitalQIP. **DNS Generation** allows you to update and configure the following:

- DNS configuration and domain zone files, and reverse zone files
- NIS services
- Local host services

DNS generation

Overview

Purpose

Each DNS Server contains Resource Records (RRs), which provide the data that make the DNS system work. The DNS Generation function creates those records and other records required by DNS.

For BIND 8.X and 9.X, DNS generation determines the maximum serial number for the zones being generated across all primary DNS servers for the zones defined in VitalQIP.

The process determines the serial number for the zone on the server on which the DNS generation is being performed. This is obtained by querying the server. If the SOA cannot be queried from the server, the SOA is obtained from the zone file or log file.

The serial number is obtained from all primary servers for the zone that are defined within VitalQIP by querying the SOA for the zone on the server.

If the generation type is **Update**, the maximum serial number for the zone on all the primary DNS servers will be incremented and updated within the VitalQIP database. If the generation type is **Configuration & Data**, the largest serial number is updated within the VitalQIP database. The incremented value will be written to the DNS configuration files being created.

With the generation type **Update**, files are written before touching the running process. The SOA is incremented when the files are written. Lucent 4.X and BIND-9 DNS use rndc commands to reload and the server is never stopped. All other server types are restarted (except AD-integrated Microsoft DNS, where VitalQIP uses **dnscmd** to make the server reload its zones).

The generation type **Configuration & Data** generates the configuration files and the data files for the DNS server without telling the server to reload its files.

> **Note:** **Update** and **Configuration & Data** are not valid generation types for Microsoft DNS.

Modifying an object affects the domains and the reverse zones. If only a few objects have been modified, you can update only the configuration and data files of those zones that contain changes. The **Changed Zones Only** option allows you to update configuration and data files of only those zones that have changed since the last time you performed a DNS generation. **Changed Zones Only** is only availabl for Windows DNS servers. On Lucent DNS 4.X servers, the **Selected Zones Only** option allows you to select specific zones in the DNS Server List.

DNS configuration files

When you perform a DNS Generation with the Type “Configuration & Data” and Destination “Local”, the files described in the following table are created on the GUI client.

The **Configuration & Data** files are created and updated. The following table describes the files included for the DNS servers:

Table 17-1 Configuration and data files for DNS servers

File name	Definition
named.conf (BIND 8.X and 9.X)	Generates the *named* directory, cache, and so on. The “Corporate Extension” information defined in **DNS** > **DNS Server** is added to the beginning of this file.
boot (Microsoft only)	In Windows 2000/2003, the **`dnscmd`** directives in the “Prefix Corporate Extension” and “Suffix Corporate Extension” parameters are executed at push time.
db.127.0.0	Generates the SOA, NS and A records for the 127.0.0 network.
db.cache	Generates NS and A records for the root “.”, if it is the root server. It also puts all NS and A records for the primary and secondary servers of the root domain.
db.root	Generates the SOA, and NS records for the root domain.
db.domainname	Generates all resource records for the domain. The domain extension goes to the bottom of this file.
db.reverse zone	Generates all resource records for the reverse zone.

VitalQIP BIND support

In BIND 8.X and 9.X, the main configuration file is called *named.conf*. The data files used by BIND (zone files) have not changed between the 8.X and 9.X versions.

Note: The data files also contain RR information established in the Domain Profile.

For Windows 2000 DNS, all extensions defined in the **Prefix Corporate Extensions** and the **Suffix Corporate Extensions** parameters of the Server Profile are executed at push time.

For BIND 8.X and 9.X, all extensions defined in the **Corporate Extensions** are prepended to the *named.conf* file. If you define global server options, they must appear in an “options” block, for example:

```
//Sample Corporate Extensions Options section
options {
  max-transfer-time-in 60;
  forward only;
  forwarders  {
    123.123.123.111;
    123.123.123.222;
  };
  multiple-cnames yes;
};
//Sample Corporate Extensions ACL section
acl “permitted-servers”  {
     127.0.0.1;
     123.123.123.55;
     123.123.123.110;
     123.123.123.234;
};
   .
   .
   .
```

For Lucent DNS 3.X, Lucent DNS 4.X, BIND 8.X and 9.X only, DNS Generation inserts “directory” options automatically. Do not include the “directory” options in your “options” block.

> **Note:** You must ensure the BIND DNS Server version in the Server Profile matches the version specified for that DNS server at installation/upgrade time. If not, the DNS server does not function properly.

Generate DNS configuration and data files

Purpose

Use this procedure to generate and view or push DNS configuration and data files on a local server, or on a remote DNS server.

Before you begin

When two pushes to the same DNS server occur simultaneously, one of those pushes is locked out to prevent the configuration files from being corrupted. An error message is displayed to this effect.

Procedure

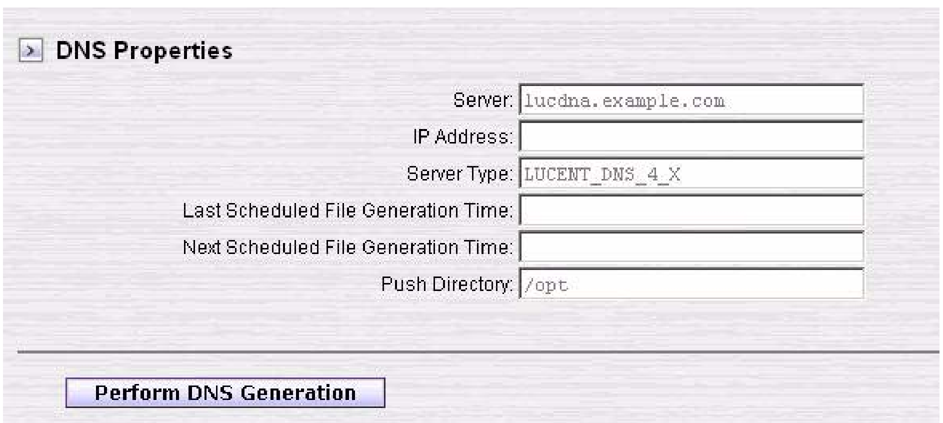
To generate and push DNS configuration and data files on a local server, or on a remote DNS server, follow these steps.

1 Mouse over **DNS** and click **DNS Generation**.

Result: The Generate DNS Generation hierarchy opens.

2 Expand **DNS Generation** and click the server that you want to perform a DNS generation.

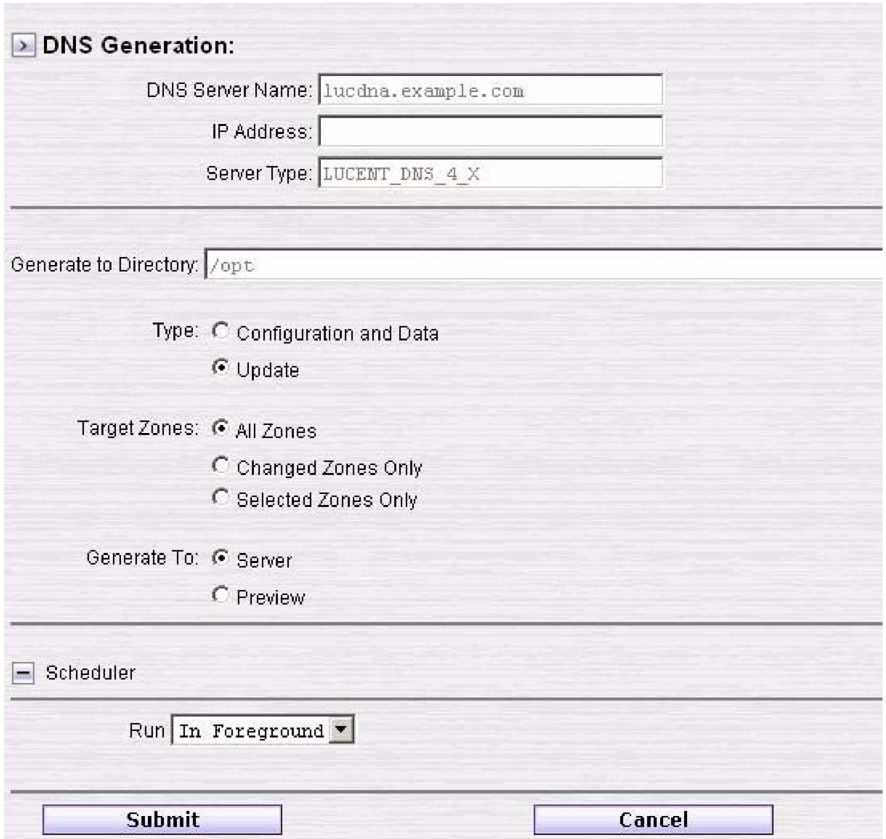
Result: The DNS Properties page opens.



The fields on this screen are read only. They indicate the properties of the DHCP server you have selected. You can change these values using the VitalQIP GUI.

3 Click **Perform DNS Generation**.

Result: The DNS Generation page opens.



The DNS server information appears in the upper portion of this page.

4 Refer to the following table as you determine what files you want to update.

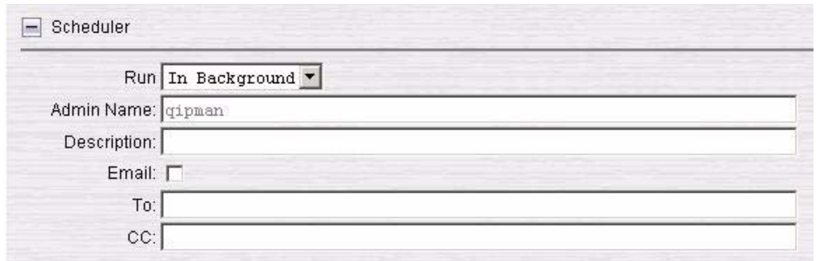
Table 17-2 DNS configuration setup fields

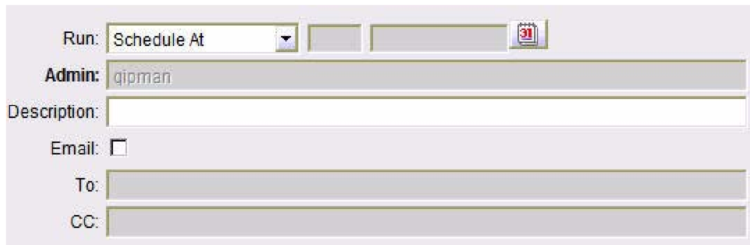
Field	Description
Generate to Directory	***Read only***. Name of the directory where the configuration files will be generated.

Field	Description
Type	Select one of the following options: • **Configuration & Data** - generates the DNS configuration and data files without incrementing the SOA serial number or reloading the server. • **Update** - generates the DNS configuration and data files. It also increments the SOA serial number. If the push is to a server, it also reloads the server. If you have selected a Windows 2000 DNS server, the above options are not displayed. Instead, you can select one of the following: • **All Records** - generates the Windows 2000 DNS configuration and data files, including incrementing the SOA serial number and reloading the server. • **Changed Records Only** - generates files for only changed records. You must perform at least one full push (All records/All zones) before you can perform a Changed Records Only push. If a zone has not been "pushed" previously, the file generation fails. An error message will be displayed explaining the possible problems.
Target Zones	Select one of the following options: • **All Zones** - updates all zones. • **Changed Zones Only** - updates only those zones that have changed since the last push. • **Selected Zones Only** - ***Lucent DNS 4.X servers only.*** Updates only the zones you have selected in the DNS Server List.
Generate to	Select one of the following options: • **Server** - files are generated on the DNS server. • **Preview** - Files are generated on the web server. File can then be downloaded to the web client.

5 Choose when to generate files in the **Scheduler** section. Choose one of the following actions.

If you want to…	Then…
Run the job immediately	Ensure that **In Foreground** is selected in the **Run** drop-down list.

If you want to…	Then…
Run the job in background	1. Select **In Background** from the **Run** drop-down list. **Result:** The Scheduler section expands to display additional fields.  The **Admin** field displays the login ID of the administrator who is scheduling the job, 2. Enter a description of the job in the **Description** field. If you do not enter a description, a description of *`<Job Name>:<Run Mode>`* is used. You may enter up to 255 characters. 3. If you want an email to be sent when the job completes, place a check in the **Email** check box. **Result:** The **To** and **CC** fields are enabled. 4. Enter an email address of up to 255 characters in the **To** field. If an email address has been entered in the **Contact Profile** for the administrator, it appears by default. 5. If desired, enter a **CC** email address.

<table>
<tr><th>If you want to…</th><th>Then…</th></tr>
<tr><td>Schedule the job for a later time</td><td>
1. Select **Scheduled At** from the **Run** drop-down list.
Result: The Scheduler section expands to display additional fields, including a calendar icon.


The **Admin** field displays the login ID of the administrator who is scheduling the job,
2. Click the Calendar icon ( ).
Result: The Calendar widget opens with the current date and time.


3. Choose from the following actions.
a. To choose a different time, click in the hour and minute fields and enter a new time in 24-hour format.
b. To choose a different month, choose a later month from the month drop-down list.
c. To choose a different year, click > to enter a future year or < to return to a prior year.
d. To choose a different day, click another day in the month.
Result: After a different day is clicked, the calendar widget closes and a new run date and/or time are displayed.
4. Enter a description of the job in the **Description** field. If you do not enter a description, a description of `<Job Name>:<Run Mode>` is used. You may enter up to 255 characters.
</td></tr>
</table>

If you want to...	Then...
	5. If you want an email to be sent when the job completes, place a check in the **Email** check box. **Result:** The **To** and **CC** fields are enabled. 6. Enter an email address of up to 255 characters in the **To** field. If an email address has been entered in the **Contact Profile** for the administrator, it appears by default. 7. If desired, enter a **CC** email address.

6 Click **Submit**.

Result: Choose from the following results.

If...	Then...
The job is scheduled in foreground	1. A confirmation box opens with the following messages: – If **Configuration and Data** was selected:**DNS** <*servername*> **successfully configured**. – If **Update** was selected: **DNS** <*servername*> **successfully updated**. 2. Click **OK**. **Result:** The DNS Properties page is displayed.
The job is scheduled in background or at a later time.	1. A confirmation box opens with the message **Job is scheduled. Job ID is** <###>**. Continue to the job scheduler page?** 2. If you wish to review the job scheduler page, click **OK**. **Result:** The Job Scheduler page opens. 3. If you would rather perform another task, click **Cancel**. **Result:** The DNS Properties page is displayed.

Local host generation

Overview

Purpose

If you use Local Host files as part of your naming service, VitalQIP can update those with the **Local Host Generation** option. This option creates files, hosts for all domains, networks, OSPF Areas, Subnet Organizations, Subnets or Corporations.

Local Host Generation generates the */etc/hosts* file.

Note: This only applies to objects created within VitalQIP. It excludes Resource Records and extensions since they are free-form text fields.

Generate local host records

Purpose

Use this procedure to generate local host records.

Procedure

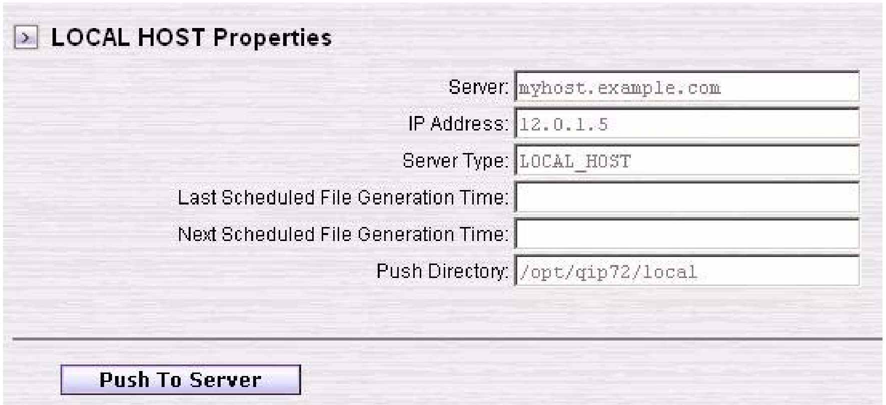
To generate Local Host files, follow these steps.

1 Mouse over **DNS** and click **DNS Generation**.

Result: The Generate DNS Configuration page opens.

2 Expand the list of Localhost servers and click the one that you want to generate a localhost file.

Result: The Local Host Properties page opens.



The fields on this screen are read only. They indicate the properties of the Localhost server you have selected. You can change these values using the VitalQIP GUI.

3 Click **Push To Server**.

Result: The Localhost file is created in the Push directory on the server.

END OF STEPS

NIS generation

Overview

Purpose

If you use NIS as part of your naming service, VitalQIP can update those files with the **NIS Generation** option. NIS Generation creates files, hosts, netmasks and ethers for all domains, networks, OSPF Areas, Subnet Organizations, Subnets or Corporations.

NIS Generation generates the following three files:

- Hosts
- ethers
- netmasks

Note: This only applies to objects created within VitalQIP. It excludes Resource Records and extensions since they are free-form text fields.

Generate NIS files

Purpose

Use this procedure to generate NIS records.

Procedure

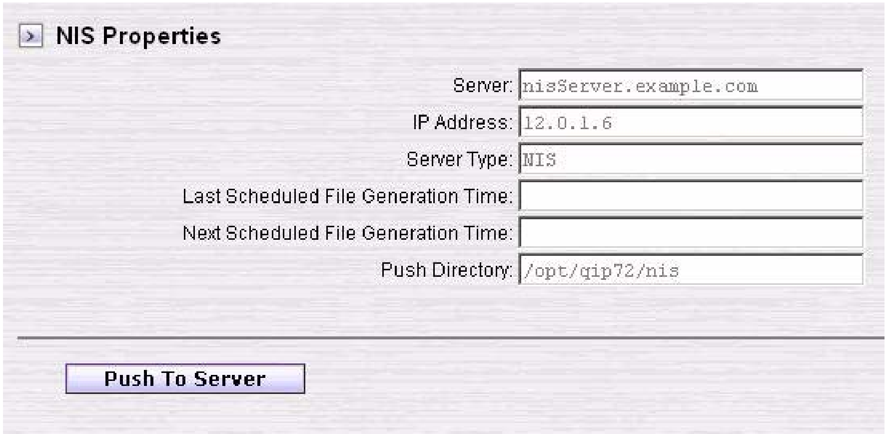
To generate NIS files, follow these steps.

1. Mouse over **DNS** and click **DNS Generation**.

   Result: The Generate DNS Configuration page opens.

2. Expand the list of NIS servers and click the one that you want to generate an NIS file.

Result: The NIS Properties page opens.



The fields on this screen are read only. They indicate the properties of the NIS server you have selected. You can change these values using the VitalQIP GUI.

3 Click **Push To Server**.

Result: The NIS file is created in the Push directory on the server.

END OF STEPS

18 Managed Files

Overview

Purpose

This chapter contains information on setting up VitalQIP to send user specified files to remote servers.

Contents

This chapter covers these topics.

Managed Files administration

Overview

Purpose

VitalQIP provides Managed Files as a mechanism to centrally manage files distributed to remote servers. Managed Files can be used to distribute callouts, scripts, zone files, BIND include files, or any other text based files to remote servers.

Managed Files can be used in conjunction with server side callouts to replace or augment the VitalQIP generated server configuration. Managed Files can be used as DNS include files to publish the same set of relative host names in different zones. The same data get published in multiple zone files and thereby get different FQDNs.

Permissions

Only master or organization administrators are able to configure Managed Files.

The Managed File Hierarchy

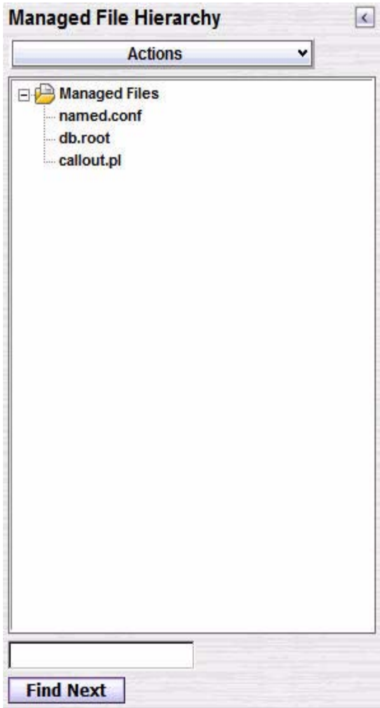
Description

The Managed File Hierarchy displays a list of files that can be pushed to remote servers.

Sample Managed File Hierarchy

The following figure shows an example of a Managed File Hierarchy.

Figure 18-1 Sample Managed File Hierarchy



Search for a managed file

Purpose

Use this procedure to search for a managed file.

Procedure

To search for a managed file, follow these steps:

---

1 Mouse over **DNS** and click **Managed Files**.

Result: The Managed File Hierarchy opens.

---

2 Mouse over the **Actions** menu and select **Search**.

Result: The Managed File Search page opens.

3 In the **File Name** field, enter the first few letters of the managed file and the wildcard character (*) as needed. If you leave this field blank, a list of ***all*** managed files is returned.

4 Click **Search**.

Result: The results appear in the **Search Results** list.

5 In the **Search Results** list, highlight a file.

6 Click **Show in Hierarchy**.

Result: The Managed File Hierarchy is updated with the select file.

END OF STEPS

Add a managed file

Purpose

Use this procedure to add a managed file.

Before you begin

- Two configurable parameters, **`managedFileMaxSizeSoftLimit`** and **`managedFileDisplaySize`**, in the *qip.properties* file restrict the size of the file that can be viewed. Refer to the *VitalQIP Administrator Reference Manual* for information.
- The VitalQIP web user interface enforces a soft limit of 2MB for the maximum size of a managed file. (See **`managedFileMaxSizeSoftLimit`** in the *VitalQIP Administrator Reference Manual*.) VitalQIP does not enforce a hard limit on the maximum size of a managed file, but performance degrades if the managed file is larger than 2MB.

Procedure

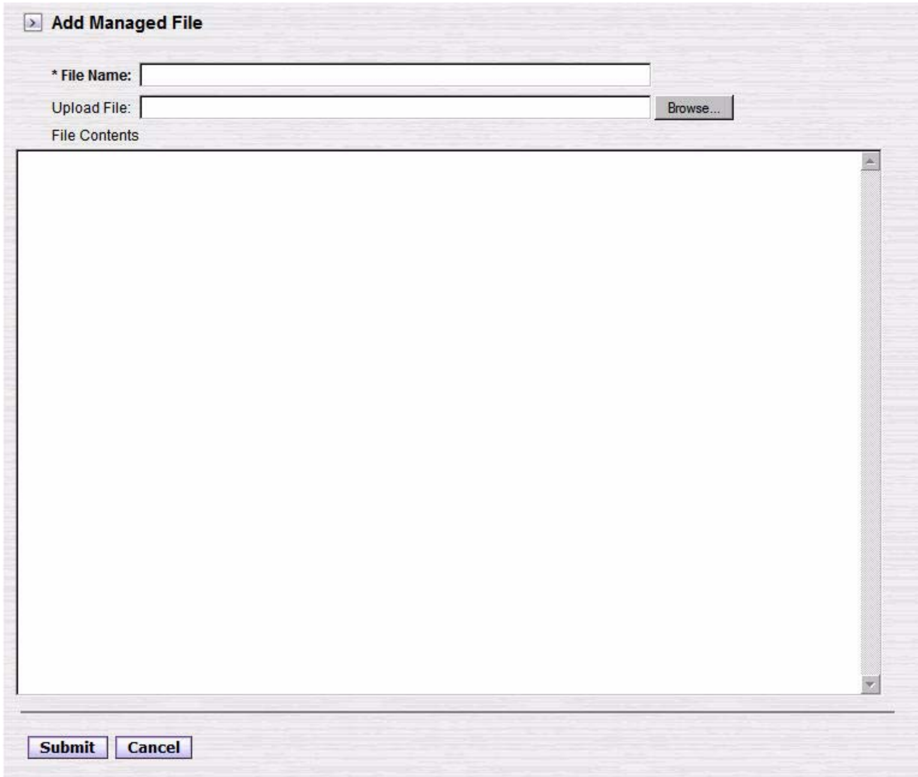
To add a managed file, follow these steps:

1. Mouse over **DNS** and click **Managed Files**.

   Result: The Managed File Hierarchy opens.

2. Mouse over the **Actions** menu and select **Add Managed File**.

Result: The Add Managed File page opens.



3 Enter information in the fields. Refer to the following table for field descriptions.

Table 18-1 Add Managed File fields

Field	Description
Field Name	***Required.*** The name of the file to be managed. The file name: • Cannot contain spaces • Is case insensitive • Is unique in an organization • Is restricted to alphanumeric characters, such as A-B,a-b,0-9,.,_,-
Upload File	***Required only if no text is entered in the File Content field.*** Uploads a file that eventually is sent to remote servers. Either enter the full path location of the file or click **Browse** to add a file.
File Content	***Required only if no path is entered in the Upload File field.*** Enter the content of the file to be created.

4 Click **Submit**.

Result: A dialog box opens that states if the file is created or uploaded successfully.

5 Click **OK**.

END OF STEPS

Associate servers with a managed file

Purpose

Use this procedure to associate servers with a Managed File.

Before you begin

You must have a Managed file created before associating servers with the file.

Procedure

To associate a server, follow these steps:

1 Mouse over **DNS** and click **Managed Files**.

Result: The Managed File Hierarchy opens.

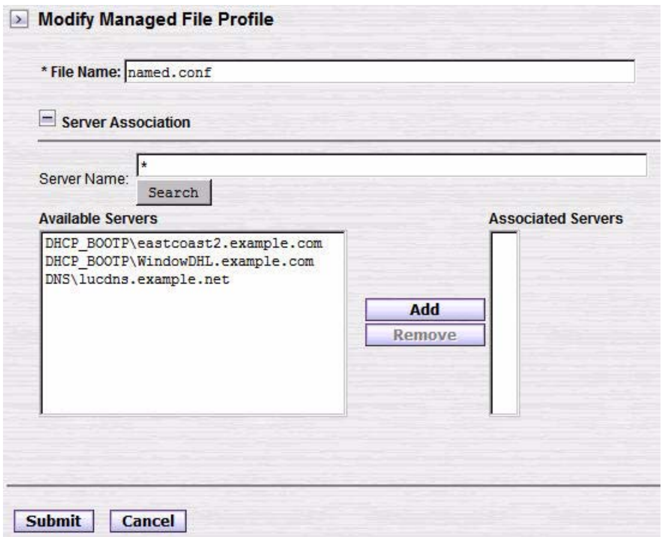
2 Select a Managed File profile.

Result: The Managed File Properties page opens.

Note: The **Modify Contents** button is replaced by a **Download** button if the file size exceeds the **`managedFileDisplaySizeThreshold`** specified in the *qip.properties* file.

3 Click **Modify Profile**.

Result: The Modify Managed File Profile page opens.



4 Choose an action.

If you are...	**Then...**
Searching for server	1. In the **Search** field, enter a few characters or a wildcard. 2. Click **Search**. **Result:** The results are displayed in the **Available Servers** list.
Adding a server	1. From the **Available Servers** list, select a server. 2. Click **Add**. **Result:** The server is added to the **Associated Servers** list.
Deleting a server	1. From the **Associated Servers** list, select a server. 2. Click **Delete**. The server is added to the **Available Servers** list.

5 Click **Submit**.

Result: A dialog box opens that states if the profile is successfully saved.

6 Click **OK**.

END OF STEPS

Modify contents of a managed file

Purpose

Use this procedure to update the contents of the file.

Before you begin

The file size displayed on the Managed Files Properties page is approximate and increases in 8k increments. An update to a file may not cause a change to the file size displayed on the Managed Files Properties page.

Procedure

To update the content of a file, follow these steps:

1 Mouse over **DNS** and click **Managed Files**.

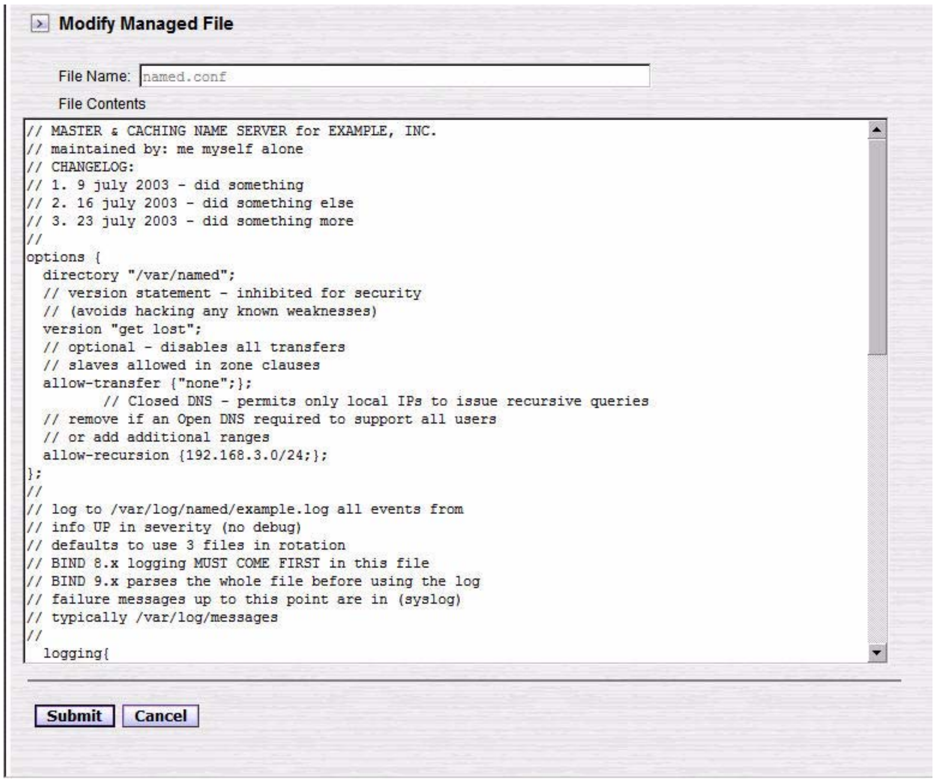
Result: The Managed File Hierarchy opens.

2 Select a Managed File profile.

Result: The Managed File Properties page opens.

3 Click **Modify File Contents**.

Result: The Modify Managed File page opens.



4 Change the content of the file.

5 Click **Submit**.

Result: A dialog box open that states if the file is successfully updated.

6 Click **OK**.

END OF STEPS

Replace the content of a managed file

Purpose

Use this procedure to replace a file.

Before you begin

The file size displayed on the Managed Files Properties page is approximate and increases in 8k increments. An update to a file may not cause a change to the file size displayed on the Managed Files Properties page.

Procedure

To replace a file, follow these steps:

1 Mouse over **DNS** and click **Managed Files**.

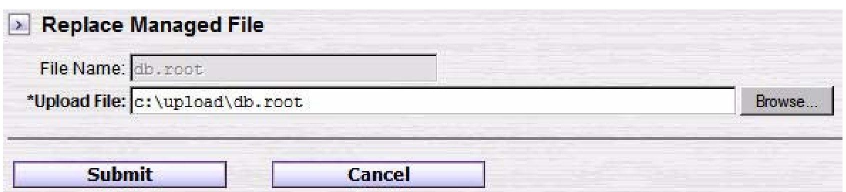
Result: The Managed File Hierarchy opens.

2 Select a Managed File profile.

Result: The Managed File Properties page opens.

3 Click **Replace File Contents**.

Result: The Replace Managed File page opens.



4 In the **Upload File** field, enter the path to the updated file.

5 Click **Submit**.

Result: A dialog box open that states if the file is successfully updated.

6 Click **OK**.

END OF STEPS

Delete a managed file

Purpose

Use this procedure to delete a Managed File.

Procedure

To delete a managed file, follow these steps:

1. Mouse over **DNS** and click **Managed Files**.

   Result: The Managed File Hierarchy opens.

2. Select a Managed File profile.

   Result: The Managed File Properties page opens.

3. Click **Delete Profile**.

   Result: A dialog box opens with the message **You are about to delete Manage File - <file name>. Are you sure you want to proceed?**

4. Click **OK**.

   Result: A dialog box opens that states if the profile is successfully deleted.

5. Click **OK**.

END OF STEPS

Part IV: DHCP administration

Overview

Purpose

This part of the Web Client User's Guide covers DHCP administration in VitalQIP.

Contents

This part includes these chapters.

19 DHCP server

Overview

Purpose

The purpose is to describe how to setup the DHCP servers in VitalQIP.

Contents

This chapter covers these topics.

DHCP Server Hierarchy

Overview

Purpose

The purpose is to describe how to set up your servers in VitalQIP. It also contains information on how DHCP servers operate, and the various types of DHCP servers that are supported by VitalQIP.

DHCP server setup

If your network includes DHCP servers, the VitalQIP remote server software must be installed on the respective servers before pushing your files from your enterprise to those servers (refer to the *VitalQIP Installation Guide*).

The remote service software transfers DHCP and configuration files from a server running the File Generation Service (FGS) to your remote servers. The File Generation Service may run on your enterprise server or on a distributed server, and controls the generation of files for remote servers. Since this service acts as a go-between for the remote and enterprise servers, it prevents actual database communication between the two servers, thereby reducing overall traffic and improving file generation times.

The VitalQIP Remote Service (**`qip-rmtd`**) must be loaded and running on the remote DHCP servers. Refer to the *Administrator Reference Manual* for information on configuring the VitalQIP Remote Service and the two services that comprise the File Generation Service: the VitalQIP RMI Scheduler Service (**`qiprmisched`**) and VitalQIP RMI QAPI Service (**`qapi`**).

> **Note:** Before you define a server other than a DNS server, you must first define the domain for the server.

Add a DHCP server

Purpose

Use this procedure to add a server profile.

Before you begin

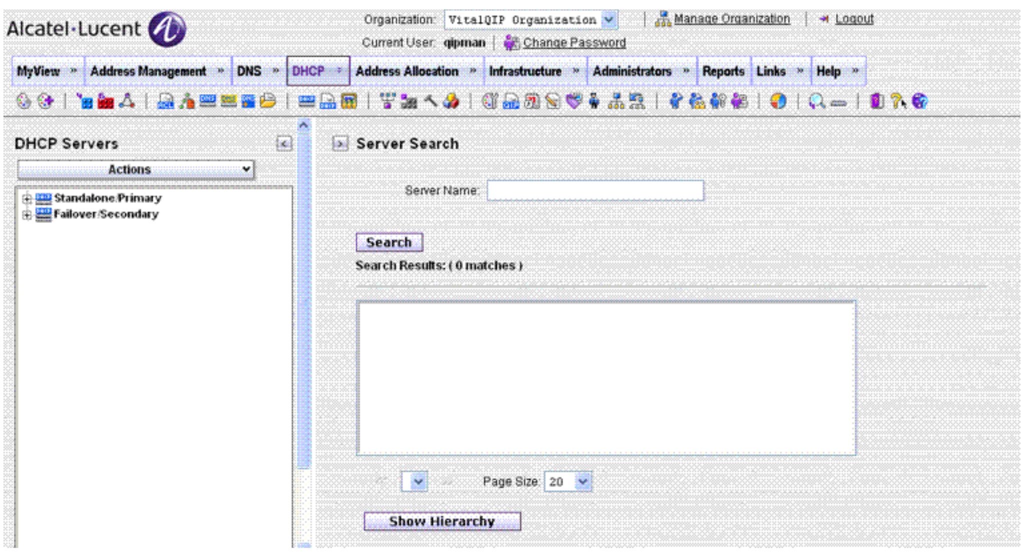
- When you select the **Server Class** of DHCP and select "Domain" as the value for **Managed Range**, the **Existing Domain List** opens as a hierarchical display. If the **Display Domain Folders** option is set to True in the Administrator Profile **Customize** tab, you see domains under their associated folders. For more information on this option, refer to *VitalQIP User's Guide*.
- The default directory, DHCP template, and PingDelay are selected by default from the *qip.properties* file.

Procedure

To set up a server, follow these steps:

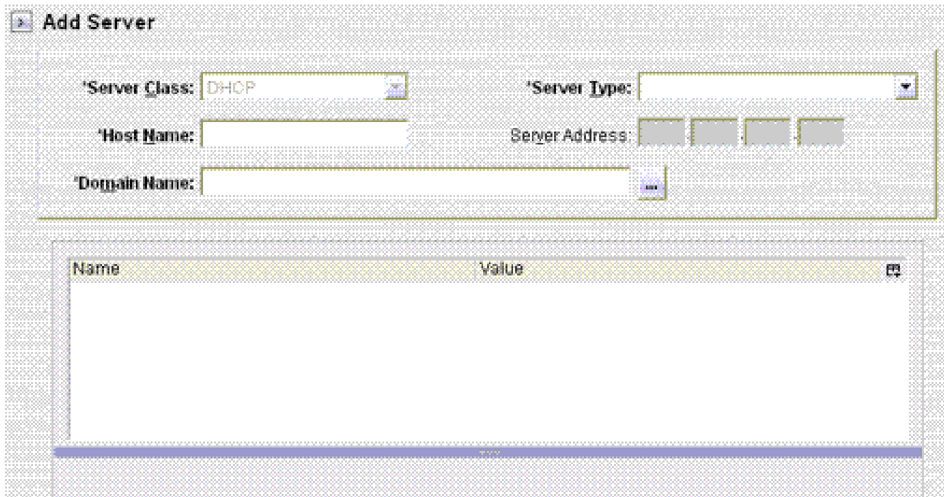
1 Select **DHCP Server** from the **DHCP** menu.

Result: The DHCP Servers page opens.



2 Select **Add Server** from the **Actions** menu.

Result: The Add Server page opens.



3 The DHCP Server is listed in the **Server Class** field. You cannot change this selection.

4 Select a server type from the **Server Type** field in the following table.

Table 19-1 Server types and parameter tables

Server type	Parameter tables
WINDOWS 2003 DHCP	Table 19-2, "Windows 2003 DHCP parameters" (p. 19-21)
LUCENT DHCP 5.4	Table 19-3, "Lucent DHCP 5.4, Lucent DHCP 5.5, and Lucent DHCP 5.6 parameters" (p. 19-23)
LUCENT DHCP 5.5	Table 19-3, "Lucent DHCP 5.4, Lucent DHCP 5.5, and Lucent DHCP 5.6 parameters" (p. 19-23)
LUCENT DHCP 5.6	Table 19-3, "Lucent DHCP 5.4, Lucent DHCP 5.5, and Lucent DHCP 5.6 parameters" (p. 19-23)

5 In the **Host Name** field, enter a new server host name. You can enter a maximum of 63 alphanumeric characters beginning with an alphanumeric. The host name can include the dash (-) character, but cannot contain plus signs (+), exclamation marks (!), or underscores (_).

6 Enter a domain in the **Domain Name** field by clicking  to open the Domain Search window and select a domain from the search results.

7 A set of parameters appears in the **Parameters/Values** list. All server parameters display their default values. The administrator can review the parameters or click **Submit**.

END OF STEPS

Modify a DHCP server

Purpose

Use this procedure to modify a DHCP server.

Procedure

To modify an existing DHCP server, follow these steps:

1 Select **DHCP Server** from the **DHCP** menu.

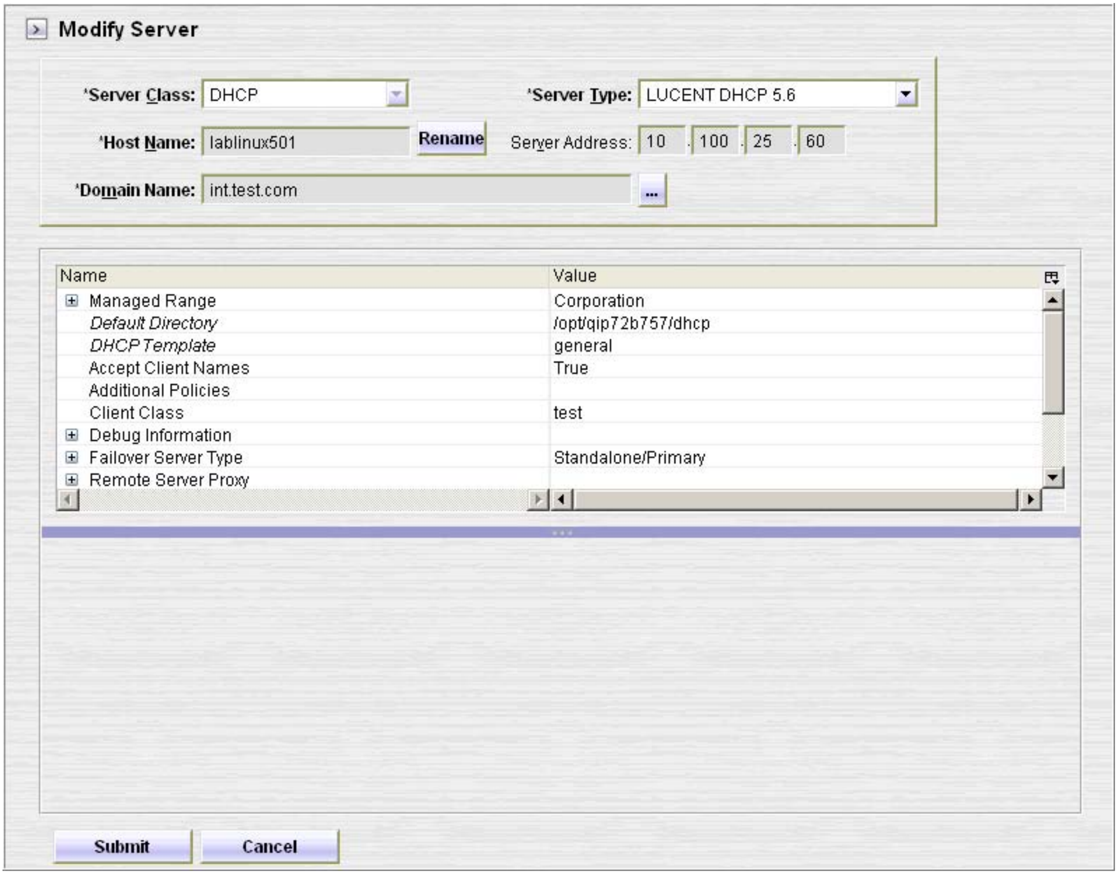
Result: The DHCP Servers page opens.

2 Select the DHCP server that you need to modify.

Result: The DHCP Properties page opens.

3 Click **Modify**.

Result: The Modify Server page opens.



4 Modify the DHCP server parameters as necessary and click **Submit** to save your changes. Refer to Table 19-2 and Table 19-3 for information on any of the server properties you wish to change.

Result: A confirmation dialog box opens.

5 Click **OK**.

Result: The DHCP Properties page opens.

END OF STEPS

Clone a DHCP server

Purpose

To clone a DHCP server.

Before you begin

- A server can be cloned by master and organization administrators, as well as by normal administrators with write privileges for the server being cloned and a Create Infrastructure privilege setting of True.
- All DHCP server options, including managed ranges and user-defined attributes (UDAs), are cloned.
- Secondary DHCP servers cannot be cloned.
- User-defined fields (UDFs) cannot be cloned since they are associated with the IP address of the server, not the server itself.
- DHCP Option template and DHCP Scope template data from the source server are not cloned to the cloned server.

Procedure

To clone a DHCP server, follow these steps.

1 Select **DHCP Server** from the **DHCP** menu.

Result: The DHCP Servers hierarchy opens.

2 Select the DHCP server that you wish to clone.

Result: The DHCP Properties page opens.

3 Click **Clone**.

Result: The Clone Server page opens.

4 Enter either a new or existing server host name in the **New Host Name** field. You can enter a maximum of 63 characters, beginning with an alphanumeric. The host name can include the dash (-) character, but cannot contain plus signs (+), exclamation marks (!), or underscores (_).

5 Click ... to open the Domain Search window and select a domain from the search results.

6 Choose one of the **Run** options in the **Scheduler** section.

7 Click **Submit**.

Result: If run in foreground, the server is cloned, the hierarchy is updated, and the properties of the new server are displayed. A dialog opens with the message **Server <server name> cloned successfully**.

Result: If run in background or scheduled for a later time/date, a dialog opens with the message **Cloning of server <server name> scheduled. Schedule Id=<##>. Continue to the job scheduler page? Click OK to proceed to the job scheduler or Cancel**.

END OF STEPS

Define global MAC address pools

Purpose

Use this procedure to define global MAC address pools.

MAC Address Pools are used by DHCP servers to define which systems in your network can receive an IP address from a DHCP server. This is typically used for security purposes. You can force the DHCP server to only give out leases to MAC addresses that are entered in this pool, by specifying the **RegisteredClientsOnly** policy in the DHCP server definition window or in a DHCP Server Policies template assigned to the server. For more information on the **RegisteredClientsOnly** policy, refer to Table 20-8, “DHCP server policies” (p. 20-23).

Before you begin

- Wildcards (displayed as ‘*’) can be used but only as the last character. At least one hex digit is required before the wildcard.
- If the **Allow 16 Character MAC Address** global policy is set to True, you can enter 12 or 16 character MAC addresses in the **MAC Address** field.
- 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 and are not permitted (even if one is included and one is excluded).

Procedure

To define global MAC address pools, follow these steps:

1 Select **DHCP Server** from the **DHCP** menu.

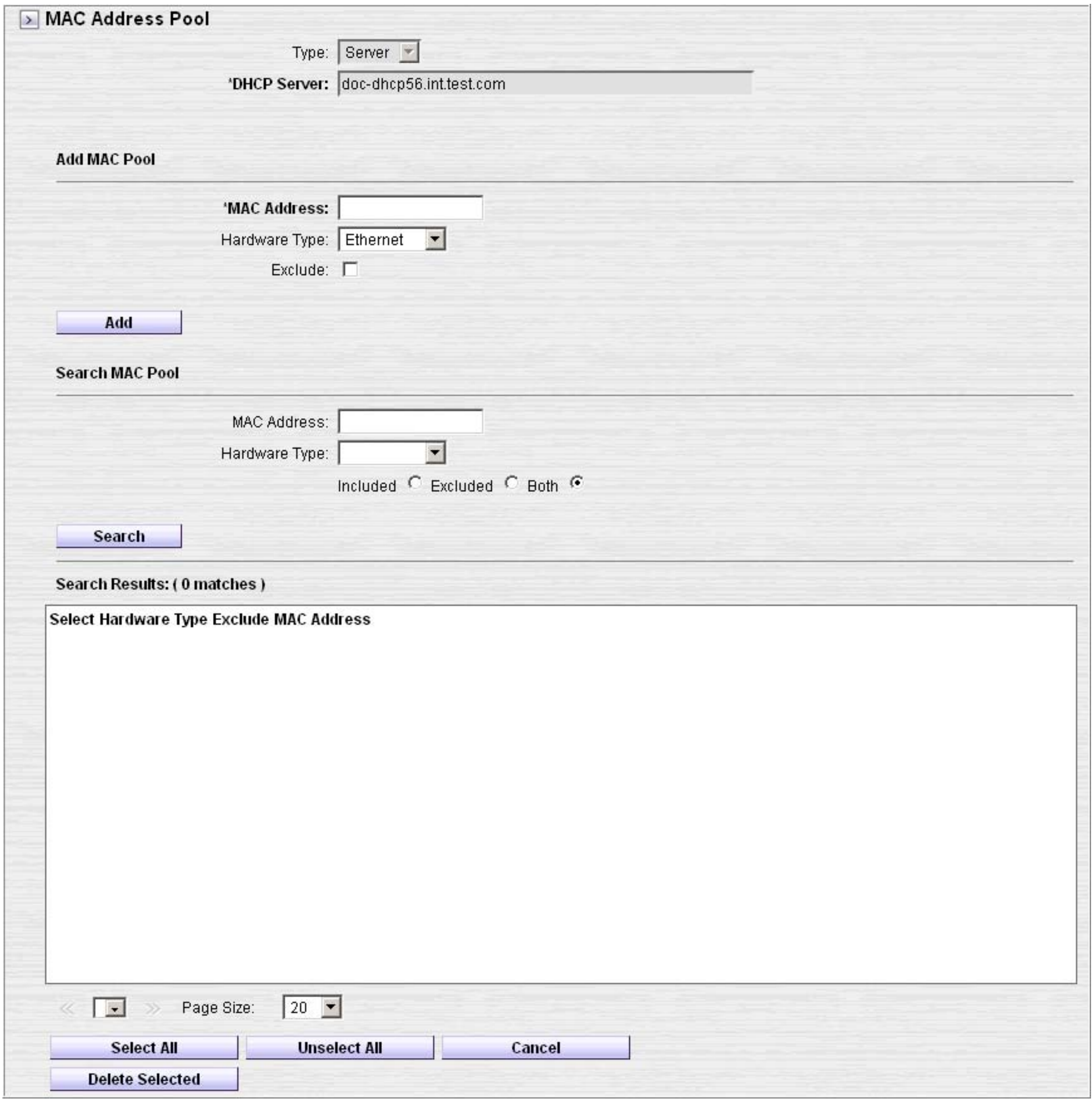
Result: The DHCP Servers Hierarchy page opens.

2 Select a DHCP server.

Result: The DHCP Properties page opens.

3 Click **Maintain MAC Pools**.

Result: The MAC Address Pool page opens.



4 Choose from the following actions.

If you want to …	**Then …**
Add a MAC address to the server pool	1. In the **Add MAC Pool** section, enter a MAC address in the **MAC Address** field. 2. Select the hardware type from the **Hardware Type** field. 3. 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. 4. In the **Search MAC Pool** section, enter the wildcard character (*) in the **MAC Address** field. **Note:** This step avoids an unintended **The search returned no results** message. 5. Click **Add**. **Result:** A confirmation dialog box opens with the message **MAC Pool added successfully**. 6. Click **OK**. **Result:** The MAC address is added to the **Search Results** list for the selected DHCP server.
Search for an existing MAC address	1. In the **Search MAC Pool** section, enter the MAC address in the **MAC Address** field. Use the wildcard character as needed. 2. Select the hardware type from the **Hardware Type** field. 3. Click **Included**, **Excluded**, or **Both**, depending on whether you need to search for the MAC address that is either included or excluded in the pool, or to search for MAC addresses regardless of their inclusion in the pool. 4. Click **Search**. **Result:** The MAC addresses are listed in the search results.

If you want to …	Then …
Unassign one or more MAC addresses from the selected DHCP server	1. Search for the MAC addresses, following the steps above. 2. Place checkmarks beside the addresses in the **Search Results** list that you wish to remove. Use **Select All** and **Unselect All** as needed. 3. Click **Delete Selected**. **Result:** A dialog opens with the message **MAC Pools deleted successfully**. 4. Click **OK**. **Result:** The selected MAC addresses are removed.

END OF STEPS

Delete a DHCP server

Purpose

Use this procedure to delete a DHCP server.

Before you begin

- DHCP servers cannot be deleted if any ranges/scopes are defined for the server. You must first remove the ranges/scopes before deleting the DHCP servers. If you need to delete a DHCP server, you can define a new DHCP server and change the DHCP server entry for all the scopes in each subnet (this can be done in the Subnet Profile or via **Edit Object Properties**), and then delete the original DHCP server entry.

Procedure

To delete an existing DHCP server, follow these steps:

1 Select **DHCP Server** from the **DHCP** menu.

Result: The DHCP Servers page opens.

2 Select the DHCP server that you need to delete.

Result: The DHCP Properties page opens.

3 Click **Delete**.

Result: A confirmation prompt opens.

4 Click **OK**.

END OF STEPS

DHCP servers

Overview

Purpose

The DHCP protocol automatically assigns IP addresses and configures the operating environment of devices represented by objects in VitalQIP. DHCP Servers can be defined at the corporate, domain, network, OSPF area, subnet organization, or subnet level. This provides the flexibility to adopt a corporate, regional (for example, network or OSPF area), or individual subnet DHCP methodology.

VitalQIP supports the Lucent DHCP server on the Windows 2003/2008, Solaris, and Linux platforms. It optionally supports dynamic updates to all authoritative DNS servers. The DHCP service supports specific DHCP parameters. Establishment of DHCP servers occurs during the installation of VitalQIP. The configuration files used by the DHCP server are created via **DHCP|DHCP Generation|Server**. These files reside on the remote machine where the DHCP server is running.

Lucent DHCP server policies are established via the VitalQIP Interface. You can decide between adding them on a per server basis in the Server Profile, or you can establish a server policy template and apply it. A policy called "Additional Policies" allows you to add other policies if necessary, as discussed in the *Administrator Reference Manual*.

Lucent DHCP server configuration files

The files needed for a full Lucent DHCP configuration include the following:

- *%QIPHOME%\x.ddns.conf*
  (Where 'X' is a number representing the Organization that the administrator is using in the VitalQIP database.) This file is used to hold information for dynamic updates to DNS, such as flags that control when DNS servers should be updated, and the IP addresses of authoritative DNS servers. It is also the file that **`qip-dnsupdated`** reads to determine where to send the DNS updates. If you are using DHCP but not DNS, this file is not necessary. In this file, the DNS server's IP address is followed by these values:
  – **8** or **9** indicates the BIND version the DNS server is using.
  – **Clear** or **Signed** indicates the secure update settings. If set to Clear, updates are sent unsigned. If set to Signed, updates are sent Kerberized.
  – **Draft** indicates that updates adhere to the draft for Kerberized dynamic updates.

– **Principal Name** indicates the principal name assigned when you set up the Lucent DNS server. Refer to the Table 13-3, "LUCENT DNS 4.X parameters" (p. 13-11) table for further information on the **Secure DNS Updates** parameter.

The DNS Type is determined in the Server Profile window. During the installation process of the Lucent DHCP server, a skeleton version of the *x.ddns.conf* file is created. During DNS Generation or DHCP Generation processing (on the **Network Services** menu), this file is further updated with domain and DNS server information.

Note: The *x.ddns.conf* file is also created by stopping and starting **`qip-dnsupdated`**.

- *%QDHCPCONFIG%\dhcpd.conf*
  This file holds all DHCP scope and IP address range definitions generated by VitalQIP and is created/updated using the **DHCP Generation** function on the **Network Services** menu.
- *%QDHCPCONFIG%\dhcpd.pcy*
  This file holds the DHCP policy settings supplied by you when you set up servers in the **Servers** function on the **Infrastructure** menu, and is created/updated using the **DHCP Generation** function on the **Network Services** menu.

Note: The VitalQIP CLI command, **`qip-dhcpgen`** can also create/update the *dhcpd.conf* and *dhcpd.pcy* files.

The VitalQIP RMI Scheduler Service gets the information from the enterprise server and the VitalQIP remote server initiates the updates for both DNS and DHCP files.

- Once the configuration information has been set, the DHCP Service can be started. The DHCP Service reads the *dhcpd.pcy* file in the *%QDHCPCONFIG%* directory to obtain server policies. The DHCP Service will fail if the *dhcpd.conf* and *dhcpd.pcy* files do not exist yet (because DHCP Generation has not yet been done) or if the files are in the wrong directory.

Since the *dhcpd.pcy* and *dhcpd.conf* files are overwritten each time a DHCP Generation is performed, it is recommended that you do not manually modify these files.

Client naming policy

When you are configuring a Lucent DHCP server, it is very important to decide how it should handle Client names.

When a DHCP Server, configured with the parameter "Accept Client Names" set to "True", receives a lease request from a client, it accepts a hostname from the client and the first lease granted is associated with that hostname. Subsequent requests from different MAC Addresses get a system-generated name. This scheme is called "FIRST_IN".

A second option, called “LAST_IN”, allows the most recent host requesting a name (with a unique MAC address) to get the name. Any host that had requested that name previously has its name converted to a system-generated name in VitalQIP.

If VitalQIP is configured to update DNS with the VitalQIP QIP Update Service (**qip-qipupdated**), DNS is updated with the appropriate hostnames from the VitalQIP database. If DNS is updated by the DNS Update Service directly from the Message Service (**qip-msgd**), DNS is updated with the client’s hostname without reference to the FIRST_IN/LAST_IN rules. The FIRST_IN/LAST_IN rule applies only to hostnames that have different MAC addresses, not those with the same MAC address/hostname combination. In other words, if a host moves from one subnet to another (getting a different host address from the DHCP server), the hostname moves with the host to the different IP address.

The system-generated name in VitalQIP is the combination of the client-supplied hostname, followed by a hyphen (“-”) and the VitalQIP-generated default name assigned when the dynamic object was first created in VitalQIP. All routines handling the FIRST_IN/LAST_IN rule have been modified to incorporate dashes. They check for names with dashes or underscores, then modify them to remove the underscores and use dashes from that point forward.

The main application for setting LAST_IN is for organizations that have notebook computers that move among subnets. When the notebook user attaches to the network in one location, the user gets an IP address in the subnet at that location. If FIRST_IN/LAST_IN is set to LAST_IN, the user keeps the desired hostname, but if it is FIRST_IN, the user gets a modified hostname at the new subnet, since the hostname is already reserved on the original subnet.

To configure the FIRST_IN/LAST_IN host naming support for Lucent DHCP servers, set the **FirstIn-LastIn** global policy in **Global Policies** on the **Policies** menu. This policy only affects dynamic clients. A static client can never be overridden by a dynamic name.

VitalQIP interface

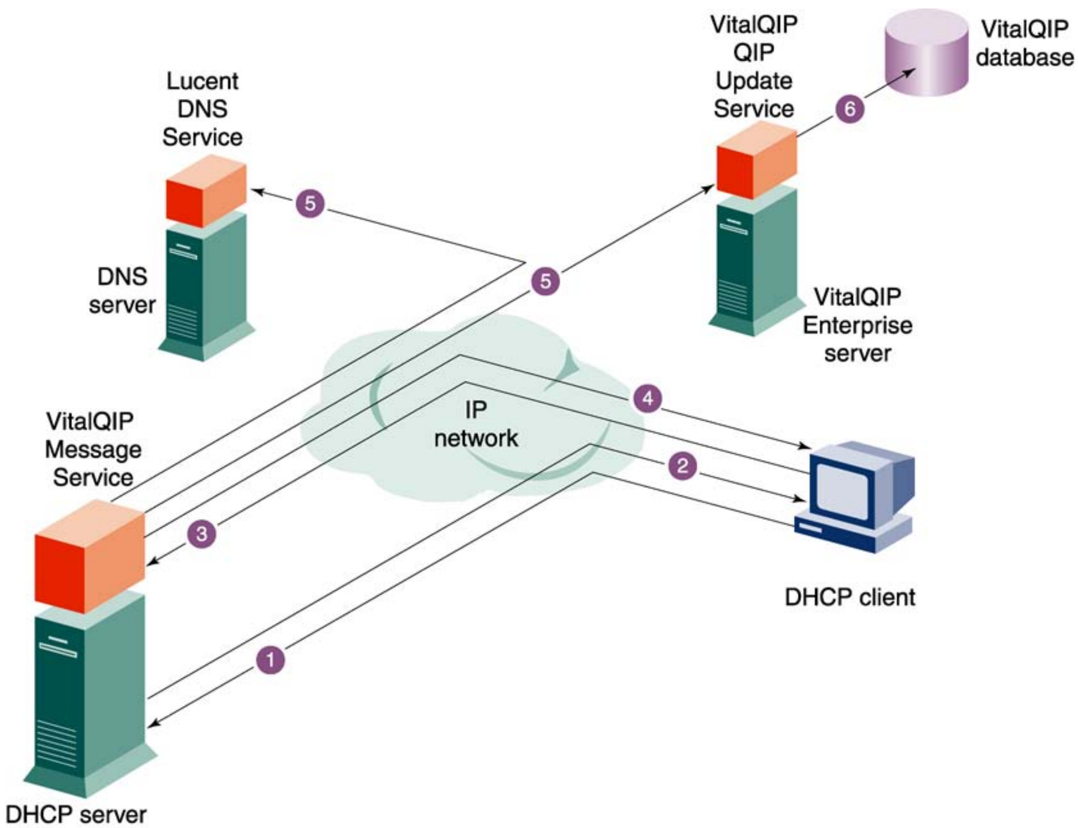
IP Manage and **qip-dhcpgen** (the command line equivalent of the **DHCP Generation** function on the **Network Services** menu) can create the *dhcpd.conf* and *dhcpd.pcy* files, and signal the DHCP server to reread its configuration and policy information. The VitalQIP Remote Service (**qip-rmtd**) is the daemon that receives the information and puts it in place.

The VitalQIP DHCP Active Lease Service (**qip-netd**) is used to obtain Active Lease information from the DHCP server. A request is sent to the Active Lease Service, which reads the environment variable that contains the location of DHCP Lease information. (The Active Lease information is located in *%QDHCPCONFIG%*.)

When a DHCP client requests a lease from the DHCP server, the server offers a lease from its configured pools, after pinging the IP address first to make sure it is not in use.

The Lucent DHCP server then sends a message to the VitalQIP Message Service. These two processes may reside on the same DHCP server. VitalQIP Message Service sends a message to the VitalQIP QIP Update Service (**qip-qipupdated**) to update the lease information on the enterprise server and thus the VitalQIP database. To understand this process more clearly, look at the following illustration.

Figure 19-1 Interactions between DHCP Message Service & VitalQIP QIP Update Service



In the above illustration, information is processed as follows:

1. A request for an address is sent. The Lucent DHCP server searches its database for an address that corresponds to the DHCP client's request. If a valid address is not found, the server does not respond to the request.
2. If an address is free, an ACK is sent, and the address is marked as used.

3. A message that the client has accepted an address is sent.
4. A DHCPACK message is sent back to the client.
5. A message is sent to the QIP Update Service and may also be sent to updated DNS, depending on the policies set in the *qip.pcy* file.
6. The database is updated with new lease information.

Server policies

dhcpd.pcy file

The *%QDHCPCONFIG%\dhcpd.pcy* file is the VitalQIP DHCP policy file that configures the behavior of the server. It describes various aspects of the server, such as how long address conflict checking will take and other policies. These policies can be set either by creating policy templates in the DHCP Template Hierarchy (from the **Actions |Add Policy Template** option on the **DHCP | DHCP Template** menu - refer to Table 20-8, “DHCP server policies” (p. 20-23) or by applying policies to specific Lucent DHCP server profiles.

The most commonly used of the policy options in Lucent DHCP are **ClientHostNameProcessing** and the two policy options used in the process associated with sharing the Automatic Bootp and Dynamic DHCP address pools, as shown in the *dhcpd.pcy* file.

- The **ShareAutoBootpAndDynDhcp** option determines whether the server should share address ranges defined as D-DHCP (Dynamic DHCP) with those defined as A-BOOTP (Automatic Bootp).
- The **SearchDynamicFirst** option tells the server to give out addresses from the D-DHCP ranges first, then when those addresses have been exhausted, to give out addresses from the A-DHCP ranges.

The **Additional Policies** text field defined in the DHCP Server Profile is used to establish parameters not included in the interface. The contents of this field will be appended to the DHCP policy file when you click **Perform DHCP Generation** in the DHCP Properties window.

qip-msgd.pcy file

The VitalQIP Message Service (**`qip-msgd`**) defaults to queueing messages that currently cannot be sent to the VitalQIP QIP Update Service (**`qip-qipupdated`**) due to a network or server outage. There are specific policies defined in the *qip.pcy* file that define the DHCP server and its relation to the QIP Update Service. For more information about VitalQIP Services Policy Files, refer to the *Administrator Reference Manual*.

Windows 2003 DHCP type

The following table shows the parameters for the Windows 2003 DHCP server type. Items in **bold** in the Options column of the table are defaults.

Table 19-2 Windows 2003 DHCP parameters

Parameters	Value type	Options	Usage
Managed Range	Selection	(**Corporation**, Domain, Network, OSPF Area, Subnet, Subnet Organization)	Allows you to establish boundaries for where a server is selectable in a network. If a DHCP server is assigned the default managed range of “Corporation”, it can be selected from any point within VitalQIP. If the server is assigned any of the other options, a managed list of available values opens and values must be added to an **Active Values** list. The selected values can now be associated with the server.
Active Directory Server	Select from List	**User Defined** or Domain Controller List	If User Defined is selected, specify the IP address of the Domain Controller where the Active Directory information for the DHCP server resides. If Domain Controller List is selected, select a Windows 2000 Domain Controller from the list of Domain Controllers. **Note:** Microsoft recommends that you do not place your DHCP server on the same machine as your Domain Controller running Active Directory.
DHCP Template	Select from List	Select from list	Select a DHCP template for this server.
Scheduled Automatic Updates	Time Interval or Time of Day	By Day, By Interval, None	Selecting By Day allows users to push policy and configuration files on a daily basis. Selecting By Interval allows users to push at a certain time interval (the default is 1 hour, which is also the minimum permitted).

Parameters	Value type	Options	Usage
Accept Client Names	Boolean	**True** or False	Choose True to have the server automatically accept the name a client suggests for itself. However, the server will only accept the client-suggested name if the name does not conflict with the hardware or IP addresses, and if the name is not used elsewhere in the network. If the “Accept Client Names” value is False, the Object Host Names will not be updated when a DHCP lease is granted. If a client does not have an assigned name, one is assigned from the hostnames list when the client requests an IP address.
Additional Policies	Multi-line Text	Free Text Area	Additional text area requires NetSh DHCP format. Commands are to be executed on a push. Refer to Microsoft documentation for NetSh syntax.
Remote Server Proxy	IP Address List	0.0.0.0	When a firewall prevents a client from pushing to a remote server, enter IP address(es) to a remote proxy server that has access to the remote server through the firewall. Use the **Description** field to describe how the remote server is used. You can enter up to 255 characters. You can use this field, for example, to keep track of which proxies are configured to accept secure connections.

Lucent DHCP 5.4, Lucent DHCP 5.5, and Lucent DHCP 5.6 server types

The following table shows the parameters for the Lucent DHCP 5.4, Lucent DHCP 5.5, and Lucent DHCP 5.6 server types. Items in **bold** in the Options column of the table are defaults.

Table 19-3 Lucent DHCP 5.4, Lucent DHCP 5.5, and Lucent DHCP 5.6 parameters

Parameters	Value type	Options	Usage
Managed Range	Selection	(**Corporation**, Domain, Network, OSPF, Subnet, Subnet Organization)	Allows you to establish boundaries for where a server is selectable in a network. If a DHCP server is assigned the default managed range of "Corporation", it can be selected from any point within VitalQIP. If the server is assigned any of the other options, a managed list of available values opens and values must be added to an **Active Values** list. The selected values can now be associated with the server.
Default Directory	Text	This value is prepopulated.	***Required***. Configuration files are created in this directory. On Windows-based systems, this includes the drive letter, (for example, *c:\qip\dhcp*).
DHCP Template	Select From List	Select From List	Select a DHCP template for this server.
Accept Client Names	Boolean	**True** or False	Choose True to have the server automatically accept the name a client suggests for itself. However, the server will only accept the client-suggested name if the name does not conflict with the hardware or IP addresses, and if the name is not used elsewhere in the network. If the "Accept Client Names" value is False, the Object Host Names will not be updated when a DHCP lease is granted. If a client does not have an assigned name, one is assigned from the hostnames list when the client requests an IP address.

Parameters	**Value type**	**Options**	**Usage**
Additional Policies	Multi-Line Text	Free Text Area	An additional text area that is appended to the *dhcpd.pcy* file. Enter a name-value pair on one line at a time in **`name=value`** format. Although the policies are case insensitive, do not enclose string values with quotes. For information on additional policies that can be set, refer to the *Administrator Reference Manual*.
Client Class	Parameter List		Allows you to apply one or more Client Classes (previously defined in the **Client Class** function on the **Policies** menu) at the server level. Select the Client Class you wish to apply and click **Add**.
Debug Information	Sub-parameters		**Debug**–Sets the debug level. Refer to the *Administrator Reference Manual* for more information about the Debug policy. **DebugFile**–Sets the debug file name. The default is *dhcpd.log*. **MaxDebugFileSize**–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. The server considers values lesser than 65535 as 65535 bytes. 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.

Parameters	Value type	Options	Usage
Failover Server Type	Select type from the picklist.	Standalone/ Primary Failover/ Secondary	Select the option of whether you want this DHCP server to be a Primary server or a Failover server. If you specify that the server is to be a Primary server, you must select a DHCP server to be its Failover server from the list. Additional policies for defining a Failover server are also made. Refer to Table 19-4, "Failover parameters for the primary DHCP server" (p. 19-28) if you wish to modify default values assigned by VitalQIP. If you specify that the server is to be a Failover/Secondary server, default policies are applied.
Remote Server Proxy	IP Address List	0.0.0.0	When a firewall prevents a client from pushing to a remote server, enter IP address(es) to a remote proxy server that has access to the remote server through the firewall. Use the **Description** field to describe how the remote server is used. You can enter up to 255 characters. You can use this field, for example, to keep track of which proxies are configured to accept secure connections.
Support Bootp	Boolean	**True** or False	Select True to have this server support both manual bootp and automatic bootp (addresses are defined as using Bootp where the individual MAC addresses are not known), or False if you do not want the server to support it.
Scheduled Automatic Updates	Time Interval or Time of Day	By Day, By Interval, None	Selecting By Day allows users to push policy and configuration files on a daily basis. Selecting By Interval allows users to push at a certain time interval (the default is 1 hour, which is also the minimum permitted).

Parameters	Value type	Options	Usage
Use Server Policy Template	Boolean, Sub-parameters	True or **False**	When set to False, you can expand the **DHCP Server Policies** sub-parameter and then apply server policies for this specific server. Refer to “DHCP server policies” (p. 20-23) for information on specific policies. When set to True, select a **Server Policy Template** from the list.

Support for DHCP failover server

Overview

Purpose

VitalQIP provides support for many-to-one DHCP failover servers, which provides a high level of redundancy for dynamic IP environments. Using a DHCP failover server allows an organization to design a DHCP server network through parameters that can provide uninterrupted service for DHCP clients. DHCP failover policies can be defined in the *dhcpd.pcy* file on the primary server and the failover servers and thereby allow you to create a failover environment specific to your needs. (Refer to “Configuration of failover parameters on primary DHCP server” (p. 19-27) to learn how to define the options through the VitalQIP GUI.)

Although VitalQIP does not limit the number of primary DHCP servers that are assigned to handle a single failover DHCP server, there are practical limits for the many-to-one configuration. From the outset, it has always been recommended that the ratio not exceed the 1-to-5 ratio.

The 1-to-5 ratio is recommended for several reasons. In the event of catastrophic failure, such as all primary servers are down or the failover server cannot communicate with the primary servers, there may not be enough processing power for the secondary server to reliably service all primary servers. For each primary server that is backed up by a failover server, a separate thread is created to manage communication between servers. The failover server manages approximately 17 threads under normal standalone operation. Additional threads for each failover channel causes additional context switching by the operational system. Performance can be severely hampered. In some cases, massive context switching can degrade the server to inoperable levels.

You can back up primary servers with DHCP many-to-one failover server support, and you can specify failover policies for each primary. This allows the failover server to “poll” the primaries at different intervals and maintain different options for retries, synchronization, and so on.

DHCP failover limitations

The following are DHCP failover server limitations:

- When a DHCP client performs an explicit release of an address, the DHCP protocol requires that the DHCPRelease message be unicast to the server that issued the lease originally. If the client obtains a lease from a primary server, which then goes down, this causes the secondary to take over. If the client then issues a release, the packet is unicast to the primary (which is not up), and is not seen at all by the secondary. Thus, it is not reflected in the lease database of the secondary. This “released” address is not reflected as released in either server until the original lease time expires.
- A secondary server cannot serve as a failover for two primary servers that service the same subnet. For example, assume primary A server is managing address 1-100 on the 10.200.50.0/24 subnet and primary B server is managing addresses 101-200 on the same subnet 10.200.50.0/24. A secondary server cannot serve as failover for both primary A and B servers. Typically, two primary servers are configured in this way to back up each other. This configuration is known as ***split scopes***. A secondary server usually is not required for this subnet.
- After the installation of the Remote Server, including the DHCP Server, that is intended to be configured as a Primary DHCP server in a failover configuration, for which there is an actively running secondary/failover DHCP server, the primary DHCP server/daemon should not be started until after a DHCP generation has been performed to push the correct configuration and policy files to the server. The primary DHCP server must then be started following the push, so that the lease synchronization properly occurs between the secondary DHCP server and the newly installed primary DHCP server.

Configuration of failover parameters on primary DHCP server

The *dhcpd.pcy* file is created automatically on the primary DHCP server when you establish the server as a Lucent DHCP Primary server and perform a “push” to the server. The additions to the *dhcpd.pcy* file to accommodate DHCP failover are discussed in this section.

A primary Lucent DHCP server and a secondary (or failover) DHCP server need to be on the same version of Lucent DHCP; you might encounter many problems if a DHCP 5.5 server were to be defined as a secondary to a DHCP 5.4 primary and vice versa.

Additional parameters ***applicable to DHCP failover*** must be specified in the *dhcpd.pcy* file in order for the failover to work properly. The **SecondaryIpAddr** option is added by VitalQIP during the push when the Failover Server Type parameter is set to 'Standalone/Primary' in the Server Profile. The Lucent DHCP server provides defaults, as shown in the following table, which you can modify as needed.

When configuring the primary server to support only registered clients in a many-to-one failover environment, MAC address pools must be configured at the subnet level, not globally.

Table 19-4 Failover parameters for the primary DHCP server

Parameter name	Value type	Default value	Description
CtlReqRetryMax	Numeric	3	If no CtlRet message is received from the failover server in the time specified by **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 **SecondaryIpAddr** parameter, even though that server may not be up. The recommended maximum value is 10. **Note:** If both the **CtrlReqRetryMax** and **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.
PollDelay	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 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).
SyncBindRetryMax	Numeric	3	The number of times the server should resend a binding update if an Ack is not received within WaitSyncBindAckSecs.

Parameter name	Value type	Default value	Description
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 same on ***both*** servers. The minimum value is 64. The maximum value is 4096.
Use Failover Server	True, False	False	If set to True, the Failover Server parameter appears, where you can select the fully qualified host name of the failover server to be used by the primary server. If set to False, no failover server is associated with the primary server.
WaitCtlRetSecs	Numeric in seconds	5	The number of seconds that this 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. **Note:** If both the **CtlReqRetryMax** and **WaitCtlRetSecs** parameters are specified, while the DHCP server is waiting, no addresses are given out.
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.
WaitSyncBindUpdateSecs	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.

Configuration of dhcpd.pcy on failover DHCP server

The policies in the *dhcpd.pcy* file to accommodate DHCP failover on the failover server are described in the following table.

Policies applicable to failover DHCP server must be specified in the *dhcpd.pcy* file if the failover is to work properly. These options are added automatically by VitalQIP during the push when the failover server type is set to “Failover/Secondary” in the Server Profile.

The *dhcpd.pcy* file on the failover DHCP server can contain *any* policy (as discussed for the *dhcpd.pcy* on the primary DHCP server) except the failover policies that are specific to the primary server.

Note: Remember to include the regular *dhcpd.pcy* policies, along with the policies specific to the failover server. Otherwise, the failover server does not know its basic parameters of operation.

Table 19-5 Failover parameters for the secondary DHCP server

Parameter name	Value type	Default value	Description
PollRetryMax	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.
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.
SyncBindings	True, False	True	If this policy is True, this failover server requests all current binding information from the primary at startup.
SyncBindRetryMax	Numeric	3	The number of times the server should resend a binding update if an Ack is not received within **WaitSyncBindAckSecs**.
SyncFailCritical	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 **SyncBindings** option is True.

Parameter name	Value type	Default value	Description
SyncReqRetryMax	Numeric	3	If no SyncStart message is received from the primary server in the time specified by **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 **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.
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).
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.
WaitSyncBindUpdateSecs	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.
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).

The *dhcpd.pcy* policy file on the primary server must contain an entry exist for the failover server. Similarly, each primary server is defined on the failover server in the *dhcpd.pcy* policy file with a sequential number following the parameter, as indicated by the following example:

```
PrimaryIpAddr1=198.200.138.207
PrimaryIpAddr2=198.200.138.243
PrimaryIpAddr3=198.200.138.205
```

20 DHCP policies and templates

Overview

Purpose

When planning networks, it is essential to establish standards that are applied throughout the network for how IP services are expected to function and operate.

Contents

This chapter covers these topics.

DHCP Template Management

Overview

Purpose

This section covers information about DHCP templates.

DHCP Template Hierarchy

Description

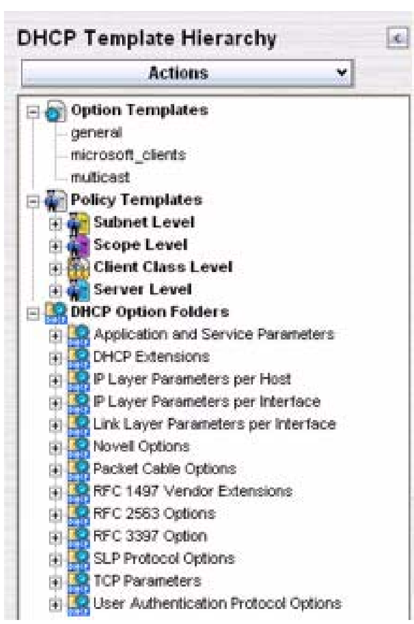
The DHCP Template Hierarchy is a hierarchical list of organizations. The hierarchy displays:

- Option Templates
- Policy Templates
- DHCP Option Folders

Sample DHCP Template Hierarchy

The following figure is a sample of a sample DHCP Template Hierarchy.

Figure 20-1 Sample DHCP Template Hierarchy



DHCP option templates

This section describes the DHCP option templates that are offered as standard with VitalQIP, as well as how to set up your own templates.

A template is a set of rules which define the way by which an address or set of addresses is supposed to operate. Once the template is defined, it can be used repeatedly and assigned to one or more pools of addresses (known as a scope) through the Subnet Profile option in the Object Management function.

Once a DHCP server has been assigned a scope, it can begin assigning addresses to clients when they are requested. When an address assignment is given to a client, a lease is attached to it.

Although the lease parameters can be defined in the Option Templates function, they are normally defined in the dynamic allocation of an object in the Object Management function.

Lease time

Like any other kind of lease, DHCP leases are valid for a limited time. Lease times are a large part of the DHCP model, and help the administrator use IP address space efficiently, especially for networks where there is a shortage of IP addresses.

> **Note:** When an option template is associated with an object, and that template has a lease time defined within it (that is, it includes DHCP option 51), the lease time of the option template always overrides any lease time set at the object. The only time the object lease time is used is if the option template does not have a lease time. Also, be aware that some non-Windows DHCP clients can request Unlimited Leases or other lease times that are different from the DHCP Server’s configuration, and that by default the “HonorRequestedLeaseTime” DHCP Server Policy is set to True.

The default lease time policy specified in the server profile is only pushed to the DHCP server in the *dhcpd.pcy* file and used by the server if there is no lease time defined for a particular scope. VitalQIP will not push a scope without a lease time. The default is a value of 3 months.

DHCP option template description

DHCP option templates allow you to create a generic set of operating environments for your network hosts. These sets of operating environments can be tailored for host characteristics, network characteristics, business characteristics, and so on. The following table describes the locations where DHCP and Bootp options can be assigned.

Table 20-1 Locations where DHCP options are assigned

Location	Application to location
Server	Assigned to specific DHCP servers. This template is assigned to a DHCP server when it is defined. This is also the default template that is assigned to all subnets when they are created.
Subnet Organization	Assigned to specific subnet organizations. This template applies to all subnets managed by the DHCP server selected in the Subnet Organization Profile.
Subnets	Assigned to specific subnets. This option template is assigned in the Subnet Profile. Changing the DHCP option template of a subnet profile only affects new IP objects and does not change the IP objects that already exist within the subnet.
Object	Assigned to a set of objects within a subnet (for example, an address scope). This template is assigned in the Dynamic Allocation: Add window in the Object Profile.
Client Class Templates	***Lucent DHCP server only.*** Associated with a particular vendor class, or one or more user classes, or option 82 relay agent information option device class. A DHCP option template can be assigned to a DHCP server without being assigned to a specific address scope.

The purpose of the DHCP template definition in the server profile is to serve as a default for the option template that is defined in the subnet profile. Likewise, the DHCP template in the subnet profile is the default at the dynamic range level. At each of these levels, you can specify an option template other than the default, but when the options are pushed, there is only one option template from which the options are defined - and that is what is at the object level.

If there are client class option definitions that are address scope independent (that is, device class, user class, or vendor class) to which a client belongs (based upon option 82, user class and vendor class options specified in a DHCPDISCOVER), the server gives precedence to these options over the same options that appear in the address scope. The option assignment sent to the DHCP client is “hierarchical”, in that an option that appears only in the scope template will be sent. The order of precedence when a particular option type appears in more than one option block in *dhcpd.conf* (that all apply to a particular client) is device class, user class, vendor class, and lastly address scope.

Each DHCP option template may define options from the following option folders:

- PacketCable options
- RFC 1497 Vendor Extensions
- IP Layer Parameters per Host
- IP Layer Parameters per Interface

- Link Layer Parameters per Interface
- TCP Parameters
- Application and Service Parameters
- DHCP/Bootp extensions
- Novell options
- RFC 2563 options
- SLP Protocol options
- User Authentication Protocol options
- Domain Search option

Each option folder has a set of options associated with it and a unique option number. Template options can inherit default values from the VitalQIP infrastructure or you can assign them static values.

The **DHCP Template** function is used to define and modify templates for DHCP servers, allowing you to define DHCP client options according to specifications contained in the RFCs listed in the following table.

Table 20-2 DHCP Request for Comments (RFCs)

RFC number	RFC description
2132	DHCP Options and BOOTP Vendor Extensions
2241	DHCP Options for Novell Directory Services
2242	NetWare/IP Domain Name and Information
2485	DHCP Option for The Open Group's User Authentication Protocol
2563	DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients
2610	DHCP Options for Service Location Protocol
3397	DHCP Domain Search option
3442	Classless Static Route Option
3495	DHCP Option for CableLabs Client Configuration

A few things to keep in mind

- A global DHCP option template can be assigned to a DHCP server. However, users can assign a different template via the subnet profile. This is also true for individual IP addresses, where a template can be assigned to override the subnet template. Multiple templates can also be defined on the same subnet, distinguished by the vendor class.

- Define the addresses on the subnets as necessary. Some addresses are static and used for servers and network equipment like routers and hubs. Other protocols for IP address assignment are dynamic, requiring either Bootp or DHCP. This is accomplished in the Object Management function.
- When a DHCP template is created with the **Same as in subnet profile** option specified with option 15 {domain name}, the domain in the subnet profile uses the subnet's default domain name, not the domain associated with the current range, for dynamic DHCP objects.

Standard templates offered with VitalQIP

VitalQIP offers three standard option templates with the product:

- a **general** template
- **microsoft_clients** template for use with Microsoft Windows clients
- **multicast** template for Multicasting

Note: "Multicast" templates can be used with scopes in the multicast range (224.0.0.0 to 239.255.255.255). Such templates are applicable to Windows DHCP only.

Selecting one of the VitalQIP supplied option templates forces certain information to be provided to specific DHCP servers so that they can operate properly. That information is shown in the **Active Options** list in the DHCP Option Template Properties page.

You can modify the current setting for the **Active Options** and also extend a template with any option previously, even if the option is not defined in an RFC. For more information on how to create new DHCP options, refer to "Add a new option to a DHCP option folder" (p. 20-43). For information on how to create your own option templates, refer to "Create a new DHCP option template" (p. 20-9).

The general template

Selecting the **general** template from the DHCP Template Hierarchy pages opens a general set of **Active Options** that must be supplied for the DHCP server to operate properly. The information in the following table outlines the most common general parameters that are passed to the DHCP client. Your environment may require different or additional options. The descriptions are discussed in the specific template class section referenced in the Template column of the table.

Table 20-3 general template options

Option name	Tag key	Option code	Template folder
Subnet Mask	sm	1	RFC 1497 Vendor Extensions
Router	gw	3	RFC 1497 Vendor Extensions
Domain Name Server	ds	6	RFC 1497 Vendor Extensions
Domain Name	dn	15	RFC 1497 Vendor Extensions

The microsoft_clients template

Selecting the **microsoft_clients** template in the DHCP Template Hierarchy page opens an expanded set of **Active Options** that must be supplied for the DHCP server to operate properly with Microsoft clients. The information in the following table lists the options that are passed to a Microsoft DHCP client using the "**microsoft_clients**" template. Your environment may require different or additional options. The descriptions are discussed in the specific template class section referenced in the Template class column of the table.

Note: "NetBIOS over TCP/IP" is also known as WINS (Windows Internet Naming System). Not all Microsoft networks use WINS.

Table 20-4 microsoft_clients template options

Option name	Tag key	Option code	Template folders
Subnet Mask	sm	1	RFC 1497 Vendor Extensions
Router	gw	3	RFC 1497 Vendor Extensions
Domain Name Server	ds	6	RFC 1497 Vendor Extensions
Domain Name	dn	15	RFC 1497 Vendor Extensions
NetBIOS over TCP/IP Name Server	bw	44	Application and Service Parameters
NetBIOS over TCP/IP Node Type	by	46	Application and Service Parameters
NetBIOS over TCP/IP Scope	bz	47	Application and Service Parameters

The Windows multicast template

Purpose

Selecting the **multicast** template in the DHCP Template Hierarchy page opens a set of **Active Options** that must be supplied for the DHCP server to operate properly.

Note: This template can only be used by Windows DHCP servers, not by Lucent DHCP servers. It is also known as MADCAP (Multicast Address Dynamic Client Allocation Protocol).

Table 20-5 Windows multicast template options

Option name	Tag key	Option code	Template folder
Scope Life	513	m513	Application and Service Parameters
Multicast TTL	514	m514	Application and Service Parameters

Procedure

To allow multicasting on your network, follow these steps:

1 Supply a value for **Scope Life** and **Multcast TTL** options.

2 Define a multicast scope within a range of addresses by selecting a subnet, then its subnet profile, and associating the "multicast" template with the subnet. Any address or range of addresses defined within this subnet will automatically be associated with the multicast template.

END OF STEPS

Create a new DHCP option template

Purpose

Use this procedure to create a new DHCP option template.

Before you begin

The VitalQIP "push" logic for the Lucent DHCP server is as follows:

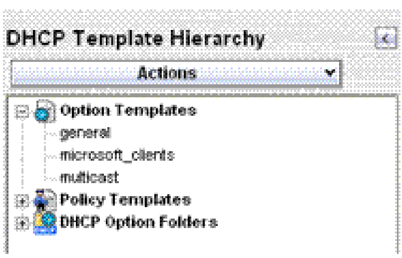
- ***For D-DHCP, A-DHCP, M-DHCP, and A-BOOTP objects:*** If the DHCP template associated with the object uses **Same as in Subnet Profile** for routers (gateways), or DNS servers, the *dhcpd.conf* file is generated with the values from the Subnet, even if other values have been assigned at the object level. If they are **User Defined**, the user-defined values are pushed.
- ***For M-BOOTP objects:*** The values for routers, time servers, and DNS servers are taken from the object. For these objects, the values from the subnet are copied to the object when the object is created, and then the M-Bootp object can be further modified in the Object Profile.

Procedure

To create a new option template, follow these steps:

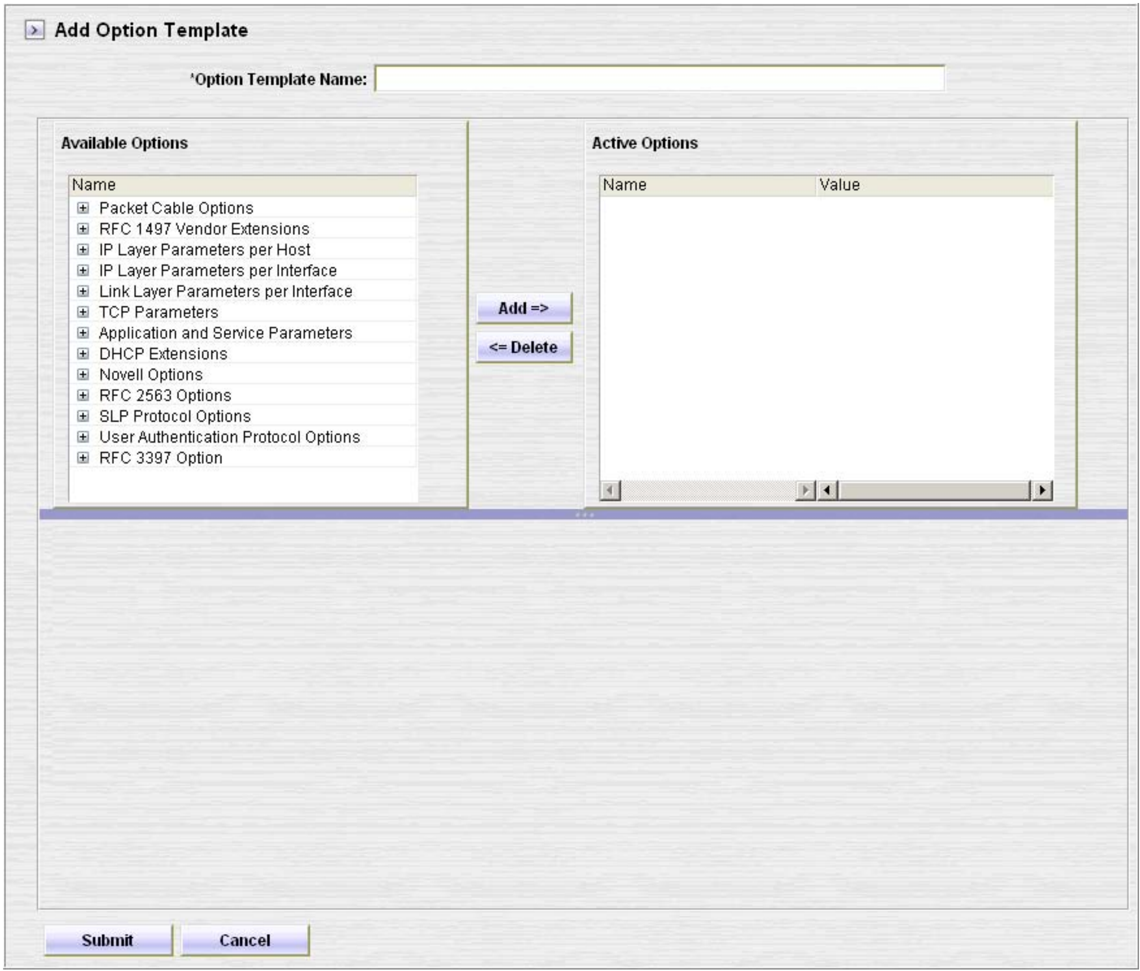
1 Select **DHCP Template** from the **DHCP** menu.

Result: The DHCP Template Hierarchy page opens.



2 Mouse over the **Actions** menu and select **Add Option Template**.

Result: The Add Option Template page opens.



3 Enter a name of up to 64 characters (no spaces) in the **Option Template Name** field.

4 The **Available Options** list displays a set of template class folders supplied by VitalQIP, as well as classes you may have created. For each template class, there is a list of available options. Choose one of the following actions to select options for your DHCP option template.

If you want to…	Then…
Select the entire set of options within a class folder	Select the desired folder and click **Add**. **Result:** All the options within the class folder appear in the **Active Options** list.

If you want to...	Then...
Select one or only a few options within a folder	1. Expand the class folder. 2. Use standard Windows selection techniques (click, shift-click, and control-click) to select the desired options. 3. Click **Add**. **Result:** The options appear in the **Active Options** list.

5 After the options you want in your DHCP option template appear in the **Active Options** list, review the values associated with each option and modify them as necessary. Use the links in the following table to review valid option values.

Table 20-6 Option folders

Option folder	Link
Packet Cable Options	Table 20-10, "Sub-options for CableLabs Client Configuration (CCC)" (p. 20-50)
RFC 1497 Vendor Extensions	Table 20-12, "Options for RFC 1497 Vendor Extensions" (p. 20-53)
IP Layer Parameters per Host	Table 20-13, "Options for IP Layer Parameters per Host" (p. 20-55)
IP Layer Parameters per Interface	Table 20-14, "Options for IP Layer Parameter per Interface" (p. 20-57)
Link Layer Parameters per Interface	Table 20-15, "Options for Links Layer Parameters per Interface" (p. 20-58)
TCP Parameters	Table 20-16, "Options for TCP Parameters" (p. 20-59)
Application and Service Parameters	Table 20-17, "Options for Application and Service Parameters" (p. 20-60)
DHCP Extensions	Table 20-18, "Options for DHCP Extensions" (p. 20-67)
Novell Options	Table 20-19, "RFC 2241 and 2242 Novell options" (p. 20-69)
RFC 2563 Options	Table 20-21, "RFC 2563 options" (p. 20-72)
SLP Protocol Options	Table 20-22, "SLP Protocol options" (p. 20-73)
User Authentication Protocol Options	Table 20-23, "User Authentication Protocol options" (p. 20-74)

Option folder	**Link**
RFC 3397 Option	Table 20-24, "Domain Search/RFC 3397option" (p. 20-74)

6 Choose one of the following actions.

If you want to...	**Then...**
Change a value for an option	1. From the **Active Options** list, select the option. **Result:** A value field appears in the the lower part of the page. 2. In the value field, enter the value. **Result:** The value is displayed in the Value column of the **Active Options** list. **Note:** Some options have the following values: – **Same as in Subnet Profile** - the value for the option is the same value as defined in the subnet profile. – **User Defined** - The procedure for changing the default to a user-defined value is described below.
Enter a user defined value for an option	1. From the **Active Options** list, select the option. **Result:** A value field appears in the the lower part of the page. 2. In the value field, select **User Defined**. **Result:** The User Defined is displayed in the Value column of the **Active Options** list. **User Defined** option appears under the selected option. 3. From the **Active Options** list, select **User Defined**. **Result:** The **User Defined** field appears in the lower part of the page. 4. Enter a value. **Result:** The value is displayed in the Value column of the **Active Options** list.

7 When you have finished selecting the options you want in your DHCP option template and have assigned them values, click **Submit**.

Result: A confirmation dialog opens with the message **Saved DHCP Option Template**.

8 Click **OK**.

Result: The DHCP Template Hierarchy is updated and the properties page opens for the template you just created.

END OF STEPS

Modify a DHCP option template

Purpose

Use this procedure to modify a DHCP option template.

Procedure

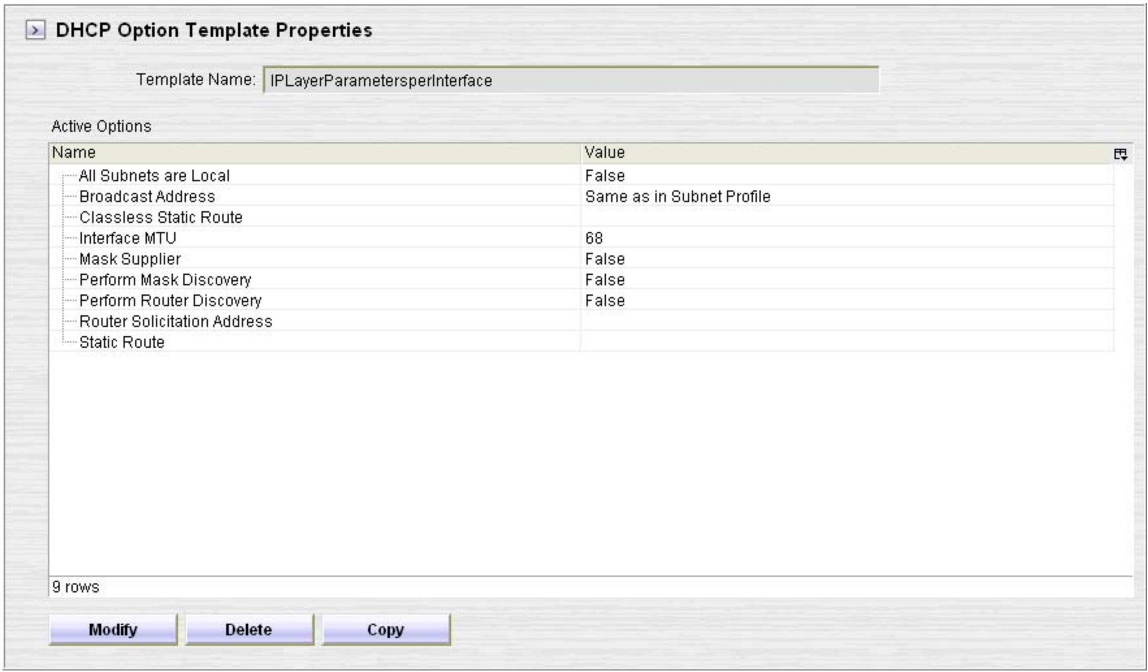
To modify a DHCP option template, follow these steps:

1 Select **DHCP Template** from the **DHCP** menu.

Result: The DHCP Template Hierarchy page opens.

2 Expand the **Option Templates** node and select the required option template.

Result: The DHCP Option Template Properties page opens.



3 Click **Modify**.

4 Add, delete, or modify options and their values in the template as necessary. For more information on the options and their values, refer to Table 20-6, "Option folders" (p. 20-12).

5 Click **Submit** to save the changes.

Result: A confirmation dialog box opens with the message **Saved DHCP Option Template**.

6 Click **OK**.

Result: The DHCP Template Hierarchy is updated and the properties page opens for the template you just modified.

END OF STEPS

Delete a DHCP option template

Purpose

Use this procedure to delete a DHCP option template.

Before you begin

You cannot delete a template if it is in use.

Procedure

To delete a DHCP option template, follow these steps:

1. Select **DHCP Template** from the **DHCP** menu.

   Result: The DHCP Template Hierarchy page opens.

2. Expand the **Option Templates** node and select the option template you wish to delete.

   Result: The DHCP Option Template Properties page opens.

3. Click **Delete**.

   Result: A confirmation dialog box opens with message **Are you sure you want to delete DHCP Template** <*option template*>**?**

4. Click **OK**.

   Result: The option template is removed from the DHCP Template Hierarchy.

END OF STEPS

Copy a DHCP option template

Purpose

To copy a DHCP option template.

Procedure

To copy a DHCP option template, follow these steps:

1 Select **DHCP Template** from the **DHCP** menu.

Result: The DHCP Template Hierarchy page opens.

2 Expand the Option Templates node and select the template you wish to copy.

Result: The DHCP Option Template Properties page opens.

3 Select **Copy**.

4 Add, delete, or modify values in the template as necessary. For more information on the options and their values, refer to Table 20-6, "Option folders" (p. 20-12).

5 Enter a different name for the template in the **Template Name** field.

6 Click **OK**.

Result: A confirmation dialog box opens with the message **Saved DHCP Option Template**.

7 Click **OK**.

Result: The DHCP Template Hierarchy is updated and the properties page opens for the template you just copied.

END OF STEPS

DHCP policy templates

DHCP policy templates allow you to establish standardized settings and thereby avoid having to duplicate your work across servers, subnets, scopes, and client classes. Two basic types of policy templates are available.

1. **DHCP Server Policies** that are set at the server level and help you define the contents of the *dhcpd.pcy* file.
2. **DHCP Configuration File Policies** that are set at the subnet, client class, or scope levels and define settings in the *dhcpd.conf* file such as:
   - DHCP Address Shuffling
   - DHCP lease query message hardware override
   - Subnet Selection Option
   - SNMP usage thresholds at the subnet level
   - Excluded vendor and user classes at the scope level

Create a DHCP policy template

Purpose

You can set policy templates for four different levels - server, client class, subnet, and scope.

Procedure

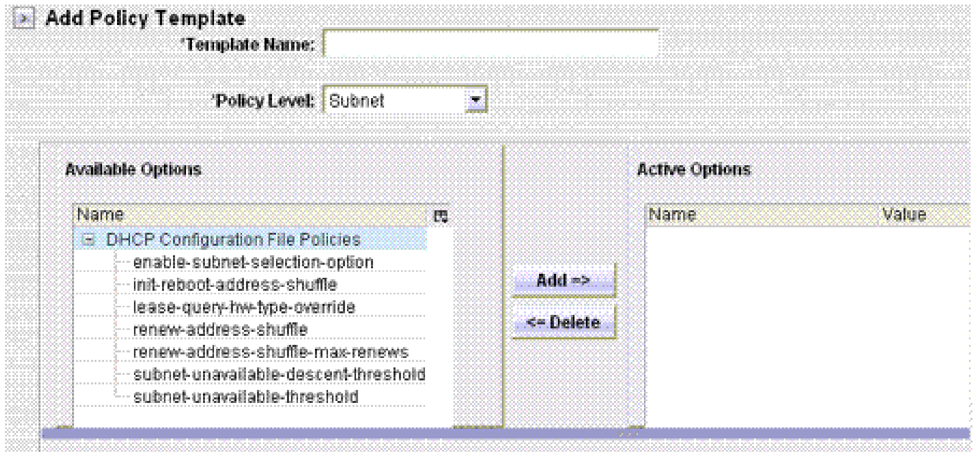
To add a new policy template, follow these steps:

1 Select **DHCP Template** from the **DHCP** menu.

Result: The DHCP Template Hierarchy page opens.

2 Mouse over the **Actions** menu and select **Add Policy Template**.

Result: The Add Policy Template page opens.



3 In the **Template Name** field, enter a name for the DHCP policy template.

4 The Subnet Policy Level is the default, with the DHCP Configuration File Policies folder displayed in the **Available Options** list.

5 To define a different policy level, select **Client Class, Scope**, or **Server** from the **Policy Level** drop-down list.

Note: If you select **Server**, the folder in the **Available Options** list changes to DHCP Server Policies.

6 To add policies, follow one of these steps:

- To select the entire set of policies within a Policy folder, click **Add**. All the policies within a Policy folder appear in the **Active Options** list.
- To select one or only a few policies within a Policy folder, click the plus sign to expand the folder. Use standard selection techniques (click, **Shift**-click, and **Ctrl**-click) to select the desired options. Click **Add** and the options appear in the **Active Options** list.

7 When the policy appears in the **Active Options** list, highlight the policy whose default value you wish to change. The values for the selected option are listed below and you can select the desired value from the drop-down list (or type a value if the data type is text or numeric).

8 When you have finished making selections and establishing values, click **Submit**.

9 Click **OK**.

END OF STEPS

DHCP configuration file policies

The policies that are supported in the policy template for DHCP configuration file policies are described in the following table. These policies update the *dhcpd.conf* file.

Note: The configuration file policies described in the following table are unique to Lucent DHCP and may not be used with third-party DHCP products.

Table 20-7 DHCP configuration file policies

Policy name	Values	Default value	Usage
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, scope, vendor class and/or user class 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, scope, vendor class and/or user class 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.
lease-query-hw-type-override	numeric	0	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 applies only to Lucent DHCP 5.5 and above servers.
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.

Policy name	Values	Default value	Usage
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 dhcpServerSubnetThresholdExceeded 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 dhcpServerSubnetThresholdExceeded 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.
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.

DHCP server policies

The policies that are supported in the policy template for DHCP server policies are described in the following table. These policies update the *dhcpd.pcy* file.

Table 20-8 DHCP server 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.
AbusiveClientMonitorPeriod	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.
AbusiveClientWarningCount	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.

Policy name	**Values**	**Default value**	**Usage**
Access Control	Expands to Access Control Enabled		***Lucent DHCP 5.6 server and above only.***
Access Control Enabled	True False	False	***Lucent DHCP 5.6 server and above only.*** When set to True, exposes the following policies that are unique to the Access Control library: DefaultClass and ReceiveTimeout. Also permits a DHCP callout configuration file (*Qdhcplib_AC.pcy*) to be generated, as well as a MAC-User Class mapping file for the DHCP AC Cache Service (*dhcpac.conf*).
DefaultClass	Existing user class	None	***Lucent DHCP 5.6 server and above only. Required***. Defines the DHCP user class that the AC API callout library will assign to a DHCP client whenever the AC Cache Service returns `Authorize=false`, or is unable to respond to a request from the DHCP server, following the receipt of a DHCPDISCOVER or DHCPREQUEST message. To enter a default user class, follow these steps. 1. Click . **Result:** The Default User Class Search window opens. 2. Click **Search**. **Result:** The **Search Results** field lists existing user classes. 3. Highlight the user class you wish to use as the default and click **Select**. For information on how to add a user class, refer to “Add a User Class” (p. 21-17).
ReceiveTimeout	Numeric	2000	***Lucent DHCP 5.6 server and above only.*** Defines the number of milliseconds the AC callout library will wait for a response from the AC Cache Service before assigning the DefaultClass value. The value should not be less than 1000 nor more than 10000.

Policy name	Values	Default value	Usage
AckRenewForUnusedAddress	True False	False	If set to True, the DHCP server will acknowledge a renew request for an IP address even if the server thinks the address is unused, provided the address is in the server's managed ranges. **Important!** Enabling this policy is particularly useful when transitioning from a different type of DHCP server to the Lucent DHCP server when DHCP clients will be attempting to renew leases that are not in the server's active lease database.
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 server(s). A failover (secondary) server should have this options set to "off" (default).

Policy name	**Values**	**Default value**	**Usage**
Bootfile	Default Hwaddr	Default	The following options are available: **Default** - used if nothing is set for this policy. It indicates that the service operates as in builds prior to build 60. That is, 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.
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.

Policy name	Values	Default value	Usage
ClientHostNameProcessing	Ignore Reject Correct	Ignore	This policy determines how the service handles DHCP client requests that have invalid DNS hostnames. The following values are available: **Ignore** - the service 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 service 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.
DefaultDescentThreshold	0-100	0	***Used with VitalQIP SNMP Module only***. This policy determines the subnet lease percent unavailable value, which when passed, causes the SNMP trap **`dhcpServerSubnet ThresholdDescent`** to be issued. A value of zero disables the monitoring of lease percent unavailable for the server. If the value is non-zero, the percentage can be overridden with the **subnet-unavailable-descent-threshold** configuration file policy on a subnet-by-subnet basis.

Policy name	Values	Default value	Usage
DefaultLease	Numeric	7776000 (3 months)	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).
DefaultUnavailableThreshold	0 - 100	0	***Used with VitalQIP SNMP Module only.*** This policy determines the subnet lease percent unavailable, which when exceeded, causes the SNMP trap **dhcpServerSubnet ThresholdExceeded** to be issued. A value of zero disables the monitoring of lease percent unavailable for the server. If the value is non-zero, the percentage can be overridden with the **subnet-unavailable-threshold** configuration file policy on a subnet-by-subnet basis.
DropAllDhcpInformPackets	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.
DropZeroMacAddressPackets	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.
Enable LDRM Interface			The interface between the Lucent DHCP Service and the LDRM (Lucent DHCP Rules Manager) Service are enabled/disabled by a set of server level policies. Expand the Enable LDRM Interface parameter to display the Use LDRMCallout policy. For more information about Lucent DHCP Rules Manager, Refer to the *LDRM Administrator Guide*.

Policy name	Values	Default value	Usage
UseLDRMCallout	True False	False	***Lucent DHCP 5.4 Server Only***. When set to True, the DHCP service attempts to load the LDRM callout library at startup. The server policy tags are as follows. All default to False: • PacketReceiptLDRMCallout • DiscoverLDRMCallout • RequestLDRMCallout • BootpRequestLDRMCallout • AckLDRMCallout These individual callout policies should be set to True only when LDRM Service rules exist to process DHCP packets sent from these callouts. Refer to the *LDRM Administrator Guide* for more information. **Note:** Enabling the LDRM interface automatically disables the use of the pre-existing DHCP Service API callouts for Registration Manager. ***Lucent DHCP 5.5/5.6 Server Only***. When set to True, the LDRM server policy tags listed above are exposed. All default to False. The DHCP service attempts to load the LDRM callout library at startup only if the **`APICalloutLibraryName*= libldrm_api`** policy is set in the Additional Policies section of the server properties, where * = the numerical index (1 - 9) of the LDRM library. Refer to “Multiple callout library feature”, in Chapter 2 of the *API Toolkit User's Guide*. **Note:** For Lucent DHCP 5.5/5.6, the multiple callout feature allows for LDRM usage with Registration Manager as well as custom API callout libraries.
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.

Policy name	Values	Default value	Usage
ForceClass	None Both Vendor User	None	Determines if the service 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 service to require a match for both user and vendor class against those defined for a particular scope. **Vendor** - causes the service to require a match on vendor class only. **User** - causes the service 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."
HonorRequestedLeaseTime	True False	True	If this policy is True, the service 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, scope, vendor class, or user class 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.
IssueDropUnknownClientTrap	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.
LeaseExpirationSleepTime	Milliseconds	60000	A specified time interval at which lease expiration processing occurs.
LeaveBootpParametersInOptions	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.
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.
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) or syslog (UNIX).

Policy name	Values	Default value	Usage
MaxOutgoingDhcpMessageSize	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.
NackDhcpRequestsForDuplicates	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.
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 subnet(s) (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.

Policy name	Values	Default value	Usage
OfferOnlyApiRequestedAddress	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.
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 service 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 service to perform both the A and PTR record updates, using the FQDN contained in option 81. **Ignore** - causes the service 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.

Policy name	Values	Default value	Usage
PadBootpReply	True False	True	This policy causes the service 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.
PingDelay	Milliseconds	500	This value determines the amount of time the DHCP Service waits for a response regarding the availability of an IP address. **Note:** DHCP servers set up on older versions of VitalQIP may not have the PingDelay policy set. Refer to "Set PingDelay policy" (p. 20-40) for further information.
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.

Policy name	Values	Default value	Usage
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.
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, scope, vendor class, or user class 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.

Policy name	**Values**	**Default value**	**Usage**
RenewAddressShuffleMaxCount	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, scope, vendor class, or user class 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.
SendRequestedParamsOnly	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.
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.

Policy name	Values	Default value	Usage
ShareAutoBootpAndDynDhcp	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 will perform threshold monitor processing for a shared network as a single entity rather than on each individual subnet within the shared network. The server will continue 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, will be 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.
SupportAutoRelease	True False	True	Releases any previous leases for a client (based on the MAC address) when the client receives a new lease.
SupportBootpAutoRelease	True False	True	Releases any previous leases for a client (based on the MAC address) when the client receives a new lease. Used for Bootp clients only.

Policy name	**Values**	**Default value**	**Usage**
SupportClientID	True False	False	***Lucent DHCP 5.6 server and above only.*** When set to True, the Lucent DHCP server will assign and track dynamic DHCP addresses according to the Client ID value, when provided by DHCP clients in option 61, as described in RFC 4361. DHCP clients that do not provide a Client ID value, as well as clients that have an existing lease tracked by MAC address, will continue to have their leases tracked by MAC address. When set to False, the DHCP server will only assign and track addresses by MAC address.
SupportEncodingLongOptions	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.
SupportRelayAgentDeviceClass	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 service to support the Relay Agent Option (82). This policy causes the service to echo the contents of option 82, if present, into all outgoing packets.

Policy name	Values	Default value	Usage
SupportRelayAgentServer Override		False	This enables the server to process the **Server Override** suboption of the **Relay Agent** option (option 82) according to RFC 5107.
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.
ThresholdMonitorSleepTime	Seconds	60	Used with SNMP Module only. This policy specifies the time interval at which lease percent unavailable monitoring occurs.
Update QIP Operations	Expands to display the following keywords: Grant Renew Release Decline Bootp Autorelease Delete Expiration	True	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: **Grant** - grants a new lease **Renew** - renews an existing lease **Release** - releases an existing lease **Decline** - refuses a lease **Bootp** - Bootp client gets a lease **Autorelease** - release is performed by the server when a client changes subnets **Delete** - Administrator deletes a lease through the GUI **Expiration** - lease expiration detected by active lease expiration processing

Policy name	Values	Default value	Usage
UpdatePreclusionDuration	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.
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 service fills in "ciaddr" with 0.0.0.0 on reply (ACK) packets. **Note:** 0.0.0.0 is always in OFFERs.

Set PingDelay policy

Purpose

To assign a value to the PingDelay policy so that an object can be pinged before being assigned an IP address. This policy defaulted to being disabled in earlier releases of the Lucent DHCP server.

Procedure

Some Lucent DHCP servers need to be configured to perform a ping before assign. To do so, follow these steps:

1 Select **DHCP Server** from the **DHCP** menu.

Result: The DHCP Servers hierarchy opens.

2 Select the Lucent DHCP server which might have been created in previous VitalQIP versions.

Result: The DHCP Properties page appears.

3 Click **Modify**. The Modify Server page opens.

4 From the list of values, click **+** to expand **Use Server Policy Template** (if it is set to **False**).

5 Click **+** to expand **DHCP Server Policies**.

6 If **PingDelay** is set to null, reset the value to a non-null value to enable ping before assign. The Lucent DHCP server will ping addresses before assigning addresses.

7 Click **Submit** to save the change.

8 In the DHCP Properties page, perform DHCP file generation by clicking **Perform DHCP Generation** and verify that a line with the `PingDelay` policy exists in the *dhcpd.pcy* file.

END OF STEPS

DHCP options

VitalQIP supplies a set of default DHCP options, based on RFCs listed in the DHCP Request for Comments (RFCs) table. These options allow you to organize DHCP options within VitalQIP and have no effect on the operation of the DHCP server. Additionally, you can define your own classes and add customized options to them. Unlike the default DHCP options, you can modify and delete your custom folders as needed.

Add a new DHCP Option Folder

Purpose

Use this procedure to add a new DHCP Option Folder.

Procedure

To add a new DHCP Template Class, follow these steps:

1 Select **DHCP Template** from the **DHCP** Menu.

Result: The DHCP Template Hierarchy page opens.

2 Mouse over the **Actions** menu and select **Add Option Folder**.

Result: The Add DHCP Option Folder page opens.

3 Enter a name for the option folder in the **Option Folder Name** field.

4 Click **Submit**.

5 A dialog opens with the message **DHCP Folder saved**.

6 Click **OK**.

Result: The new option folder appears at the bottom of the DHCP Template Hierarchy.

END OF STEPS

Add a new option to a DHCP option folder

Purpose

Use this procedure to add a new option to a DHCP option folder.

Procedure

To add a new option, follow these steps:

1 Select **DHCP Template** from the **DHCP** menu.

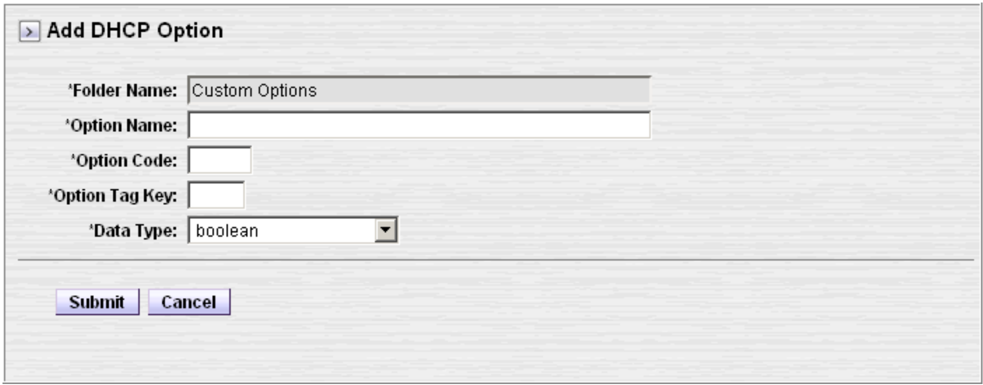
Result: The DHCP Template Hierarchy page opens.

2 Expand the **DHCP Option Folders** node and select an option folder.

Result: The DHCP Option Folder Properties page opens.

3 Click **Add Option**.

Result: The Add DHCP Option page opens.



4 Fill in the following fields:

- **Option Name** - Enter a name to identify the option. This name appears as an option of the selected class.
- **Option Code** - Enter an option number. According to RFC 2132, option codes 128 to 254 are reserved for site-specific options. It cannot be an existing option number.
- **Tag Key** - Enter a two-letter code to identify this option. It cannot be an existing tag key.
- **Data Type** - Select the type of data for this option from the drop-down list. The Data Type affects the input fields that appear when you are adding or modifying DHCP templates and choose an option from the Available Classes/Options list.

The following table describes the functions that are associated with each data type.

Table 20-9 Data types

Data type	Description
boolean	**True/False** option buttons permit the use of Boolean logic.
ip_address	An IP address field is displayed (for example, 196.123.123.10). Numbers between 0 and 255 are accepted.
ip_address_list	An IP address field is displayed in which an IP address can be entered (for example, 196.123.123.10). Numbers between 0 and 255 can be entered in each of this field's octets. You can add or delete IP addresses to the list as needed.

Data type	Description
ip_address_mask_list	An **Address** field and **Mask** field are displayed. The **Mask** field uses a slide rule to add a mask. The **Address** field accepts integers in a four octet format (for example, 123.222.123.10). The IP address and mask can be deleted or added to the list as needed. Both fields accept numbers between 0 and 255 in each octet. The IP address and mask appear side by side in the list.
ip_address_pair_list	Two IP address fields, **Address1** and **Address 2**, are displayed. (for example, 196.123.123.5 and 196.200.23.10). Numbers between 0 and 255 can be entered in each of this field's octets. **Add** and **Delete** permit you to add or delete an IP address pair from the list. The IP addresses appear next to each other in the list.
ip_mask	An IP Mask field and a slider are displayed. The first field is 255 and valid mask values can be entered in the remaining three fields.
ip_mask_ip_list	A Subnet Address field, a Router Address field, and a Mask field are displayed. The Mask field uses a slide rule to add a mask. The address fields accept integers in a four octet format (for example, 123.222.123.10). The subnet address, router address, and mask can be deleted or added to the list as needed. All fields accept numbers between 0 and 255 in each octet. The IP addresses and mask appear side by side in the list.
multi-lined_text	A text area is displayed in which multi-line text can be entered.
numeric	A field that allows you to enter any number between 0 and 128.
numeric_list	A field that allows you to enter any number between 0 and 2,147,483,647. **Add** and **Delete** allow you to add or delete integers from the list.
numeric_signed	A field that allows you to enter any number between -2,147,483,647 to 2,147,483,647.
password	A text field is displayed in which a password can be entered. Characters entered are converted to '*' automatically.
text	A field is displayed which permits you to enter any character, such as `Lucent12345.com`. A maximum of 128 characters can be entered.
text_list	A text field is displayed in which a text string can be entered. A maximum of 128 characters can be entered in the field. You can add or delete text string from the list as needed.

Data type	Description
time_interval	A **Days** field, an **Hours** field, and a **Minutes** field are displayed. Numbers between 0 and 999 are accepted in the **Days** field, and any number in the **Hours** and **Minutes** fields, so long as the total number of days when all fields are calculated does not exceed 999 days.
time_of_day_list	An **Hour** field and a **Minute** field are displayed. Enter a number between 0 and 23 in the **Hour** field. Enter a number between 0 and 59 in the **Minute** field. You can add or delete a text string from the list as needed.

5 Click **Submit**.

Result: A dialog opens with the message **DHCP Option saved.**

6 Click **OK**.

Result: The new DHCP option is added to the selected DHCP option folder.

Note: If you have an option selected when you click **Add Option**, the new option is added under the same folder as the selected option. If you have a sub-option selected, the new option is added as another sub-option.

END OF STEPS

Rename a DHCP option folder

Purpose

Use this procedure to rename a DHCP option folder.

Procedure

To rename an option folder, follow these steps:

1 Select **DHCP Template** from the **DHCP** menu.

Result: The DHCP Template Hierarchy page opens.

2 Expand the **DHCP Option Folders** node and select an option folder.

Result: The DHCP Option Folder Properties page opens.

3 Click **Modify**.

4 Change the name of the DHCP option folder and click **Submit**.

Result: A dialog opens with the message **DHCP Option saved.**

5 Click **OK**.

Result: The renamed DHCP folder reappears in the DHCP Template Hierarchy.

END OF STEPS

Modify a DHCP option folder

Purpose

Use this procedure to modify a DHCP option folder.

Procedure

To modify a DHCP option folder, follow these steps:

1 Select **DHCP Template** from the **DHCP** menu.

Result: The DHCP Template Hierarchy page opens.

2 Expand the **DHCP Option Folders** node and select an option folder.

Result: The DHCP Option Folder Properties page opens.

3 Click **Modify**.

4 Make the desired changes to any of the fields and click **Submit**.

Result: A dialog opens with the message **DHCP Option saved.**

5 Click **OK**.

Result: The modified option folder reappears in the DHCP Template Hierarchy.

END OF STEPS

Delete a DHCP option folder

Purpose

Use this procedure to delete a DHCP option folder.

Before you begin

- You can only delete DHCP option folders that have been added; you cannot delete the default DHCP option folders.
- If you delete a DHCP option folder, it will be deleted from all templates even if the templates are in use.
- When a DHCP option folder is deleted, all options within that folder are also deleted.

Procedure

To delete a DHCP option folder, follow these steps:

1 Select **DHCP Template** from the **DHCP** menu.

Result: The DHCP Template Hierarchy page opens.

2 Expand the **DHCP Option Folders** node and select the option folder you wish to delete.

Result: The DHCP Option Folder Properties page opens.

3 Click **Delete**.

Result: A confirmation dialog box opens with the message **Are you sure you want to delete the selected DHCP Folder?**

4 Click **OK**.

Result: A dialog opens with the message DHCP Folder deleted.

5 Click **OK**.

Result: The DHCP option folder is removed from the DHCP Template Hierarchy.

END OF STEPS

DHCP option folder values

A DHCP option template is a set of DHCP options that defines what information is given out for a particular IP address or a particular range of IP addresses. Although each option was defined by a particular RFC standard, in VitalQIP they are organized into classes based on the RFCs. DHCP options are assigned to templates, which are then associated with subnets and DHCP objects. You can create new options with the Add Option Folder function in the DHCP Template Hierarchy, although your new options must be ones that your DHCP clients can understand. You can create DHCP templates using the existing standard DHCP options and/or user-defined ones.

When DHCP options are assigned to templates, they must be given values. In some cases the values can be set to “Same as Subnet Profile”, in other cases they must be given static values. You can create your own DHCP templates, or you can use one of three pre-defined DHCP option templates that are included in VitalQIP. As you create your own option template or modify an existing one, it is important that you understand the DHCP template values and what they mean ***before you make a selection***.

The tables in the following sections explain the options available in each option folder. Use these tables as a reference when assigning values to the options in an option template.

Note: For Bootptab file support, the value of the tag **nw** is the subnet address (for instance, 144.249.64.128). Tags may appear in any order with one exception: the hardware type (tag **ht**) must precede the hardware address (tag **ha**).

Packet Cable options

The following table describes the CableLabs Client Configuration 122 sub-options, specified in RFC 3495:

Table 20-10 Sub-options for CableLabs Client Configuration (CCC)

Sub-option name	Data type	Default value	Usage
TSP AP-REQ/AP-REP Backoff and Retry	sub_option	N/A	Configures an MTA’s Kerberos AP-REQ/AP-REP timeout, backoff, and retry mechanism. Enter a **Nominal Timeout** value in milliseconds, a **Maximum Timeout** value in seconds and a **Maximum Retry** value. All these values are unsigned

Sub-option name	Data type	Default value	Usage
TSP AS-REQ/AS-REP Backoff and Retry	sub_option	N/A	Configures an MTA's Kerberos AS-REQ/AS-REP timeout, backoff, and retry mechanism. Enter a **Nominal Timeout** value in milliseconds, a **Maximum Timeout** value in seconds and a **Maximum Retry** value. All these values are unsigned.
TSP Kerberos Realm Name	text	N/	The PacketCable architecture requires an MTA to authenticate itself to the TSP's network via the Kerberos protocol. A Kerberos Realm name is required at the MTA to permit a DNS lookup for the address of the TSP's Kerberos Key Distribution Center (KDC) entity. The realm name must be all capital letters and conform to domain name syntax (HOST.SUBDOMAIN.DOMAIN).
TSP Primary DHCP Server Address	ip_address	N/A	Enter the IP address of the TSP's primary DHCP server from which an MTA is permitted to accept a DHCP OFFER.
TSP Provisioning Server Address	static_drop_down_list	IP Address	MTAs communicate with the Provisioning server at various stages in their provisioning process. Enter either the IP address or the FQDN of the TSP's Provisioning server.
TSP Provisioning Timer	numeric	0	Defines the maximum time allowed for the MTA provisioning process to complete. If this timer expires before the MTA has completed the provisioning process, the MTA should reset the timer and re-start its provisioning process from the beginning. Enter a value from `0` to `255`, where 0 means the timer is disabled.
TSP Secondary DHCP Server Address	ip_address	N/A	Enter the IP address of the TSP's secondary DHCP server from which an MTA is permitted to accept a DHCP OFFER.
TSP Ticket Granting Server Utilization	boolean	False	Determines whether an MTA should use a Ticket Granting Ticket (TGT) when obtaining a service ticket for one of the PacketCable application servers. Select True to indicate that the MTA should get its TGT.

Although replaced by code 122 since RFC 3495 was issued, VitalQIP includes code 177 sub-options because some vendors may support the temporary format of the CableLabs Client Configuration sub-options.

The following table describes the CableLabs Client Configuration site-specific sub-options:

Note: Some data fields permit entry of an FQDN or an IPv4 address. You must therefore enter an address using bracketed IP address notation as specified in RFC 821, for example, [xxx.xxx.xxx.xxx]. Additionally, you can specify port numbers if a port other than the standard is required, for example [xxx.xxx.xxx.xxx]:NNNN, where NNNN is an optional UDP port number.

Table 20-11 Sub-options for Site-specific CableLabs Client Configuration (CC)

Sub-option name	Data type	Default value	Usage
CMS FQDN	text	N/A	***Required to provide primary line service.*** Enter the fully qualified domain name of the Call Management Server (CMS). The Call Management Server (CMS) provides call control and signaling related services for the MTA and other gateways in the PacketCable network.
Kerberos Realm	text	N/A	***Required.*** The PacketCable architecture requires an MTA to authenticate itself to the SP’s network via the Kerberos protocol. A Kerberos Realm name is required at the MTA to permit a DNS lookup for the address of the TSP’s Kerberos Key Distribution Center (KDC) entity. Enter the realm name of the SNMP Entity in capital letters and conform to domain name syntax (HOST.SUBDOMAIN.DOMAIN).
Provisioning Timer	numeric	0	Defines the maximum time allowed for the MTA provisioning process to complete. If this timer expires before the MTA has completed the provisioning process, the MTA should reset the timer and restart its provisioning process from the beginning. Enter a value from **`0`** to **`255`**, where 0 means the timer is disabled.
SP Primary DHCP Server Address	text	N/A	***Required.*** Enter the bracketed IP address of the SP’s primary DHCP server from which an MTA is permitted to accept a DHCP OFFER.
SP Primary DNS Server Address	text	N/A	***Required.*** The Service Provider’s DNS server is required to resolve a PacketCable device’s FQDN into an IP address. Enter the DNS server’s address in bracketed IP address format.
SP Secondary DHCP Server Address	text	N/A	Enter the bracketed IP address of the SP’s secondary DHCP server from which an MTA is permitted to accept a DHCP OFFER.

Sub-option name	Data type	Default value	Usage
SP Secondary DNS Server Address	text	N/A	To identify a redundant or backup DNS server, enter the bracketed IP address of the Service Provider's secondary DNS Server.
SP SNMP Entity Address	text	N/A	***Required.*** Enter the network address (in either all-capital FQDN or bracketed IP address format) of the default server for a service provider's network administrative domain. The service provider's SNMP Entity Address component must be capable of accepting SNMP traps.
Use Ticket-Granting Ticket	boolean	False	Determines whether an MTA should use a Ticket Granting Ticket (TGT) when obtaining a service ticket for one of the PacketCable application servers. Select True to indicate that the MTA should get its TGT.

RFC 1497 Vendor Extensions

The following table describes the options for RFC 1497 Vendor Extensions.

Note: Consult your Client vendor documentation for specific information on the support and usage of these options.

Table 20-12 Options for RFC 1497 Vendor Extensions

Option name	Option code	Tag key	Data type	Default value	Usage
Boot File Size	13	bs	numeric	N/A	Enter the length of the client's default boot image. The maximum file length is 65,535 bytes.
Cookie Server	8	cs	ip_address_list	N/A	Enter the IP address of the RFC 865 cookie server available to the client.
Domain Name	15	dn	static_drop_down_list	Same as in Subnet Profile	Enter the domain name you wish to use to resolve hostnames via the Domain Name Service (DNS).
Domain Name Server	6	ds	static_drop_down_list	Same as in Subnet Profile	List the DNS (STD 13, RFC 1035) name server IP addresses available to the client. Servers should be listed in order of preference.

Option name	Option code	Tag key	Data type	Default value	Usage
Extensions Path	18	ep	text	N/A	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	12	ho	static_drop_down_list	Same as in Object Profile	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	10	im	ip_address_list	N/A	Enter the IP address of the Imagen Impress server available to the client.
Log Server	7	lg	ip_address_list	N/A	Enter the IP address of the MIT-LCS UDP log server available to the client.
LPR Server	9	lp	ip_address_list	N/A	Enter the IP address of the RFC 1179 line printer server available to the client.
Merit Dump File	14	df	text	N/A	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	5	ns	ip_address_list	N/A	Enter the IP address of the IEN-116 name server available to the client.
Resource Location Server	11	rl	ip_address_list	N/A	Enter the IP address of the RFC 887 Resource Location server available to the client.
Root Path	17	rp	text	N/A	Enter the pathname that contains the client's root directory or partition. The path is formatted as an NVT ASCII character string.

Option name	Option code	Tag key	Data type	Default value	Usage
Router	3	gw	static_drop_down_list	Same as in Subnet Profile	List the IP addresses for the routers on the client's subnet. Routers should be listed in order of preference.
Subnet Mask	1	sm	static_drop_down_list	Same as in Subnet Profile	Specify the client's subnet mask as per RFC 950. If both the subnet mask and the router option are specified in a DHCP reply, the subnet mask option ***must*** be first.
Swap Server	16	sw	ip address	N/A	Enter the IP address of the client's swap server.
Time Offset	2	to	numeric_signed	N/A	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	4	ts	static_drop_down_list	Same as in Subnet Profile	Enter the IP address of the RFC 868 time server available to the client.

IP Layer Parameters per Host

The following table describes the RFC 2132 options for IP Layer Parameters per Host.

Table 20-13 Options for IP Layer Parameters per Host

Option name	Option code	Tag key	Data type	Default value	Usage
Default IP Time-to-Live	23	it	numeric	N/A	Enter the default time-to-live (in seconds) to use on outgoing datagrams as an octet between 1 and 255, inclusive.

Option name	Option code	Tag key	Data type	Default value	Usage
IP Forwarding Enable/Disable	19	br	boolean	False	Selecting True allows you to configure the IP layer to enable packet forwarding. False disables packet-forwarding.
Maximum Datagram Reassembly Size	22	as	numeric	N/A	Enter the maximum reassembly size of the datagram. Enter a value between 576 and 65,535.
Non-Local Source Routing Enable/ Disable	20	fn	boolean	False	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.
Path MTU Aging Timeout	24	pt	numeric	N/A	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	25	pl	numeric_list	N/A	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	21	pf	ip_address_mask_list	N/A	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.

IP Layer Parameters per Interface

IP layer parameters affect the operation of the IP layer on a per-host basis. Additionally, it describes the options that affect the operation of the IP layer on a per-interface basis. It is assumed that clients can issue multiple requests, one per interface, in order to configure interfaces with their specific parameters. The following table describes the RFC 2132 options for IP Layer Parameters per Interface.

Table 20-14 Options for IP Layer Parameter per Interface

Option name	Option code	Tag key	Data type	Default value	Usage
All Subnets are Local	27	sl	boolean	False	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	28	ba	static_drop_down_list	Same as in Subnet Profile	Enter the broadcast address in use on the client's subnet.
Classless Static Route	121	sr	ip_mask_ip_list	N/A	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	26	tu	numeric	N/A	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	30	ms	boolean	False	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.

Option name	Option code	Tag key	Data type	Default value	Usage
Perform Mask Discovery	29	md	boolean	False	Selecting True establishes that the client should perform subnet mask discovery. Selecting False indicates no mask discovery should be performed.
Perform Router Discovery	31	rd	boolean	False	Selecting True allows router discovery to be performed as defined in RFC 1256. Selecting False indicates no router discovery to be performed.
Router Solicitation Address	32	rs	ip_address	N/A	Name the IP address where router solicitation requests should be transmitted.
Static Route	33	sr	ip_address_pair_list	N/A	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.

Link Layer Parameters per Interface

The following table describes the RFC 2132 options for Link Layer Parameters per Interface. These options affect the operation of data link layer on a per-interface basis.

Table 20-15 Options for Links Layer Parameters per Interface

Option name	Option code	Tag key	Data type	Default value	Usage
ARP Cache Timeout	35	at	numeric	N/A	Enter the timeout in seconds for ARP cache entries, from 0 to 2,147,483,647.

Option name	Option code	Tag key	Data type	Default value	Usage
Ethernet Encapsulation	36	ec	boolean	False	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	34	tr	boolean	False	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.

TCP Parameters

The following table describes the RFC 2132 options for TCP. These options affect the operation of the TCP layer on a per-interface basis.

Table 20-16 Options for TCP Parameters

Option name	Option code	Tag key	Data type	Default value	Usage
TCP Default TTL	37	tt	numeric	N/A	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	39	ko	boolean	False	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.
TCP Keepalive Interval	38	ki	numeric	N/A	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.

Application and Service Parameters

The following table describes the RFC 2132 options for Application and Service Parameters. The network parameters require that you identify the static IP addresses for the servers on your network, if applicable.

Table 20-17 Options for Application and Service Parameters

Option name	Option code	Tag key	Data type	Default value	Usage
Default Finger Server	73	fi	ip_address_ list	N/A	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	74	ir	ip_address_ list	N/A	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	72	ww	ip_address_ list	N/A	The WWW server option specifies a list of WWW servers available to the client. Servers should be listed in order of preference.
Microsoft Default Router Metric Base			numeric	N/A	This option can be used to set the default base metric for Windows DHCP clients. When this option is set, the DHCP Client service uses the value configured here as the base metric for its default gateways. This value can be assigned as an integer cost metric ranging from 1 through 9,999. It is used in calculating the fastest, most reliable, and least expensive routes. If a value is not specified, a default of either 1 or the currently set interface-specific metric is used.
Microsoft Disable NetBios			numeric	N/A	This option can be used to selectively enable or disable NetBios for DHCP-enabled computers running Windows 2003 only. By installation default, if this option is not present, Windows 2003 enables the use of NetBios for network connections that are configured to use TCP/IP. Earlier Windows clients require NetBios and do not support this option.

Option name	Option code	Tag key	Data type	Default value	Usage
Microsoft Release DHCP Lease on Shutdown			numeric	N/A	This option can be used to control whether DHCP-enabled computers running Windows 2003 send a release for their current DHCP lease to the DHCP server when they are shutdown. It is actually implemented and interpreted as a bit masked value by the DHCP client service. In most cases, the default (that is, the functional equivalent to this option value not being used or present in the DHCP message) is that Windows 2003 clients do not send DHCP release messages on a proper shutdown.
Mobile IP Home Agent	68	mh	ip_address_list	N/A	This option specifies an IP address list indicating mobile IP home agents available to the client. Agents should be listed in order of preference.
Multicast TTL			numeric	N/A	Number of routers (from 0 to 255) that multicast traffic is permitted to pass through before expiring on the network.
NetBIOS over TCP/IP Datagram Distribution Server	45	bx	ip_address_list	N/A	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	44	bw	ip_address_list	N/A	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	46	by	static_drop_down_list	N/A	The NetBIOS node type option allows NetBIOS over TCP/IP clients, which are configurable as described in RFC 1001/1002. The value is specified as a single octet, which identifies the client type, as follows: **Value** **Node type** 0x1 B-node 0x2 P-node 0x4 M-node 0x8 H-node

Option name	Option code	Tag key	Data type	Default value	Usage
NetBIOS over TCP/IP Scope	47	bz	text	N/A	The NetBIOS scope option specifies the NetBIOS over TCP/IP scope parameter for the client, as specified in RFC 1001/1002.
Network Information Servers	41	ys	ip_address_list	Same as in Subnet Profile	List the IP addresses (in order of preference) identifying the NIS (Network Information Service) servers available to the client.
Network Information Service Domain	40	yd	text	Same as in Subnet Profile	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	64	zd	text	N/A	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	65	zs	ip_address_list	N/A	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	71	nn	ip_address_list	N/A	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	42	nt	ip_address_list	Same as in Subnet Profile	List the IP addresses (in order of preference) indicating NTP (RFC 868) servers available to the client.
Post Office Protocol (POP3) Server	70	po	ip_address_list	N/A	The POP3 server option specifies a list of POP3 servers available to the client. Servers should be listed in order of preference.
Scope Life			numeric	N/A	Number of hours before the multicast scope expires.

Option name	Option code	Tag key	Data type	Default value	Usage
Simple Mail Transport Protocol (SMTP) Server	69	sp	ip_address_list	N/A	The SMTP server option specifies a list of SMTP servers available to the client. Servers should be listed in order of preference.
StreetTalk Directory Assistance (STDA) Server	76	da	ip_address_list	N/A	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	75	st	ip_address_list	N/A	The StreetTalk server option specifies a list of StreetTalk servers available to the client. Servers should be listed in order of preference.
Broadcast and Multicast Control Service Domain List	88	bmdl	text_list	N/A	Lists server names that host the Broadcast and Multicast services that are specified as domain names.
Broadcast and Multicast Control Service Address List	89	bmal	ip_address_list	N/A	Lists server names that host the Broadcast and Multicast services that are specified as IPV4 addresses.
Timezone specified as IEEE 1003.1 String	100	tzie	text	255	Specifies a DHCP client’s timezone specified as a POSIX 1003.1 timezone string.
Timezone specified as TZ Database String	101	tzdb	text	255	Specifies a DHCP client’s timezone specified as a TZ database string.

Option name	Option code	Tag key	Data type	Default value	Usage
SIP Server Address List	120	ssal	ip_address_list	N/A	Lists the SIP servers specified as IPV4 addresses.
SIP Server Domain List	120	ssdl	text_list	N/A	Lists the SIP servers specified as domain names.

Option name	Option code	Tag key	Data type	Default value	Usage
Vendor Specific Information	43	vs	hexa decimal_ text	N/A	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	49	xd	ip_address_ list	N/A	This option specifies a IP address list of systems that are running the X Window System Display Manager and are available to the client.

Option name	Option code	Tag key	Data type	Default value	Usage
X Window System Font Server	48	xf	ip_address_ list	N/A	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 octet
`c6c88afe`	IP address 198.200.138.254 in hex
`21`	Second sub-option
`0b`	Length of 11 octets
`7375626f7074696f6e3200`	"suboption2" in hex, null terminated

DHCP Extensions

The following table describes the options for DHCP Extensions.

Table 20-18 Options for DHCP Extensions

Option name	Option code	Tag key	Data type	Default value	Usage
Bootfile Name	67	bf	text	N/A	This option is used to identify a bootfile when the **`file`** field in the DHCP header has been used for DHCP options.
Client Identifier	61	id	text	N/A	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.
IP Address Lease Time	51	lt	time_interval	Unlimited	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. Selecting Limited allows you to set a lease time of up to 999 days, 999 hours, and 999 minutes.

Option name	Option code	Tag key	Data type	Default value	Usage
Option Overload	52	ov	1, 2, or 3	N/A	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	59	t2	numeric	N/A	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	58	t1	numeric	N/A	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	66	sn	text	N/A	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.

Option name	Option code	Tag key	Data type	Default value	Usage
Vendor Class Identifier	60	ck	text	N/A	This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a text string of ***n*** octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client. For example, the identifier may encode the client's hardware configuration. Servers not equipped to interpret the class-specific information sent by a client must ignore it (although it may be reported). Servers that respond should only use option 43 (Vendor Specific Information) to return the vendor-specific information to the client.

Novell options

The Novell options (described in the following table) define three DHCP options for delivering configuration information to clients of the Novell Directory Services (NDS). These options provide an NDS client with enough information to connect to an NDS tree without manual configuration of the client. Additionally, options that carry NetWare/IP domain name and NetWare/IP sub-options to DHCP clients are defined in the following table.

Table 20-19 RFC 2241 and 2242 Novell options

Option name	Option code	Tag key	Data type	Default value	Usage
NDS Context	87	nc	text	N/A	This option specifies the initial NDS context the client should use. You can enter up to 255 characters.
NDS Servers	85	nv	ip_address_list	N/A	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.

Option name	Option code	Tag key	Data type	Default value	Usage
NDS Tree Name	86	na	text	N/A	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	62	nd	text	N/A	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.
Netware/IP Information	63	ni	sub-option	N/A	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 will be conveyed using this option code. If NWIP_EXIST_IN_OPTIONS_AREA sub-option is set, one or more of the other sub-options may be present.

Table 20-20 Netware/IP Information sub-options

Sub-option name	Data type	Default value	Usage
AUTORETRIES	numeric		The value is an integer value indicating the number of times a NetWare/IP client should attempt to communicate with a given DSS server at startup.
AUTORETRY_SECS	numeric		The value is an integer value indicating the amount of delay in seconds in between each NetWare/IP client attempt to communicate with a given DSS server at startup.
NEAREST_NWIP_SERVER	ip_address_list		The list contains the IP addresses of up to 5 Nearest NetWare/IP servers.
NSQ_BROADCAST	boolean	False	If the value is True, the client ***should*** perform a NetWare Nearest Server Query to find out its nearest NetWare/IP server.

Sub-option name	Data type	Default value	Usage
NWIP Setting	static_drop_down_list	NWIP_DOES_NOT_EXIST	**NWIP_DOES_NOT_EXIST** - The responding DHCP server does not have any NetWare/IP information configured. **NWIP_EXIST_IN_OPTIONS_AREA** - All NetWare/IP information is present in the 'options' area of the DHCP response packet. **NWIP_EXIST_BUT_TOO_BIG** - Neither 'options' area nor 'sname' field can accommodate the NetWare/IP information.
NWIP_1_1	boolean	False	If the value is True, the NetWare/IP client ***should*** support NetWare/IP Version 1.1 compatibility. A NetWare/IP client only needs this compatibility if it will contact a NetWare/IP version 1.1 server.
PREFERRED_DSS	ip_address_list		The list contains the IP addresses of up to 5 NetWare Domain SAP/RIP Servers (DSS).
PRIMARY_DSS	ip_address		The value is a single IP address. This field identifies the Primary Domain SAP/RIP Service server (DSS) for this NetWare/IP domain. The NetWare/IP administration utility uses this value as Primary DSS server when configuring a secondary DSS server.

RFC 2563 options

Operating Systems are now attempting to support ad-hoc networks of two or more systems, while keeping user configuration at a minimum. To accommodate this, in the absence of a central configuration mechanism (DHCP), some operating systems are automatically choosing a link-local IP address which will allow them to communicate only with other hosts on the same link. This address will not allow the operation systemA to communicate with anything beyond a router. However, some sites depend on the fact that a host with no DHCP response will have no IP address. RFC 2563 describes a mechanism by which DHCP servers are able to tell clients that they do not have an IP address to offer, and that the client should not generate an IP address of its own.

The following table describes the option for RFC 2563 options.

Table 20-21 RFC 2563 options

Option name	Option code	Tag key	Data type	Default value	Usage
Auto Configuration of Ipv4 Clients	116	ac	boolean	False	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.

SLP Protocol options

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Entities using the Service Location Protocol (SLP), Version 1 and 2 need to obtain the address of Directory Agents and Scope configuration. SLP provides a default configuration for Scopes and Directory Agents, which may be discovered using multicast or broadcast. It is useful in a larger deployment to be able to configure SLP Agents using DHCP, so as to centralize the administration and to deploy SLP in networks where multicast routing is not available.

The DHCP options described below are used to configure Agents using the Service Location Protocol, Version 1 and 2. The SLP Directory Agent option is used to configure User Agents and Service Agents with the location of Directory Agents in the network. The SLP Scope option takes precedence over both default and static scope configuration of SLP agents.

The following table describes the RFC 2610 options for SLP Protocol options.

Table 20-22 SLP Protocol options

Option/sub-option name	Option code	Tag key	Data type	Default value	Usage
SLP Directory Agent	78	sd	sub-option		This option specifies the location of one or more SLP Directory Agents. The SLP Directory Agent option contains the following sub-options:
Directory Agent Address			ip_address_list	N/A	This sub-option allows a IP address list to be specified. The list must be in order of preference, if an order of preference is desired.
Mandatory			boolean	False	This sub-option may be set to either True or False. If it is set to True, the SLP User Agent or Service Agent so configured ***must not*** employ either active or passive multicast discovery of Directory Agents.
SLP Service Scope	79	ss	sub-option		This option indicates the scopes that a SLP Agent is configured to use. It contains the following sub-options:
Mandatory			boolean	False	This sub-option determines whether SLP Agents override their static configuration for scopes in the Scope List. This allows DHCP administrators to implement a policy of assigning a set of scopes to Agents for service provision. If set to False, static configuration takes precedence over the DHCP-provided scope list. If set to True, the entries in the Scope List ***must*** be used by the SLP Agent.
Scope List			text	N/A	This sub-option is a comma-delimited list of scopes. The list is case insensitive.

User Authentication Protocol options

The DHCP option for The Open Group's User Authentication Protocol (UAP) defines an option that contains a list of pointers to User Authentication Protocol servers, which in turn provide user authentication services for clients that conform to The Open Group Network Computing Client Technical Standard.

The following table describes the RFC 2485 options for User Authentication Protocol options.

Table 20-23 User Authentication Protocol options

Option name	Option code	Tag key	Data type	Default value	Usage
User Authentication Protocol	98	ua	text_list	N/A	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.

Domain Search option

VitalQIP supports the RFC 3397 option which is passed from the DHCP Server to the DHCP Client to specify the domain search list used when resolving hostnames with DNS. This option applies only to DNS and does not apply to other name resolution mechanisms.

The following table describes the RFC 3397 option.

Table 20-24 Domain Search/RFC 3397option

Option name	Option code	Tag key	Data type	Default value	Usage
Domain Search Option	119	do	text_list	N/A	Passes the domains in the search list from the DHCP Server to the DHCP Client to use when resolving hostnames using DNS. Enter a domain name in the **New Value** field and click **Add**.

21 DHCP Client Class

Overview

Purpose

This chapter describes how to manage DHCP Client Classes.

Contents

This chapter covers these topics.

DHCP Client Class Management

A DHCP Client Class allows you to assign DHCP option templates and/or policy templates specifically to a Vendor, Device, or User class, without the class having to be associated with a specific address scope. The options and policies assigned to a DHCP Client Class are applied to any DHCP client that specifies the matching vendor, user class (refer to Option 60 in RFC 2132 and Option 77 in RFC 3004, respectively), or device class (refer to RFC 3256).

Options and policies applied to a DHCP client from a DHCP Client Class take precedence for that client, over the same options and policies that may also be associated with the dynamic address scope from which the client lease is assigned. Configuration parameters associated with a device class in the DHCP configuration file take precedence over a similar configuration option with different values specified in a user class client class, which in turn take precedence over the same specified value in a vendor class client class.

A DHCP Client Class can have one vendor class, one device class, or one or more user classes and must have an option template or a client class policy template attached. Multiple client classes can be assigned to a DHCP server and any class can be used on multiple servers. Client classes can also be assigned to individual subnets, in which case those particular client classes should not be assigned to the DHCP server that is managing that subnet.

Add/Modify/Delete Device Class

Although functionality to add/modify and delete a device class is available, it does not affect the **Device Class** drop-down list for a device class client class because available devices classes are defined only by RFC and the only current device class is CCCM.

Add a new User Class Client Class

Purpose

Use this procedure to add a new User Class Client Class.

Procedure

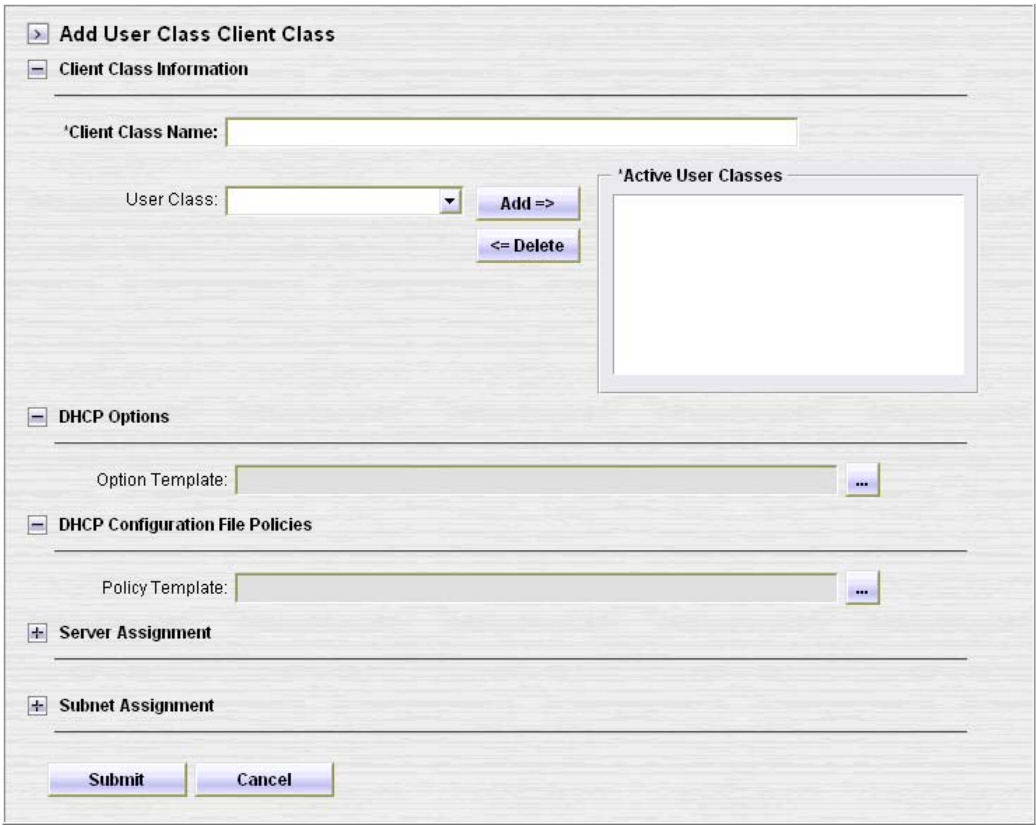
To add a new User Class Client Class, follow these steps:

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

2 Mouse over the **Actions** menu and select **Add User Class Client Class**.

Result: The Add User Class Client Class page opens.



3 Enter an alphanumeric name in the **Client Class Name** field.

4 In the **User Class** field, enter an alphanumeric name for the user class or select an existing user class from the drop-down list and click **Add =>**. The user class is displayed in the **Active User Classes** list.

5 A client class must have an option template and/or a policy template.

If you want to ...	**Then ...**
Assign an option template	1. In the **DHCP Options** section, click ... beside the **Option Template** field. **Result:** The DHCP Option Template Search window opens. 2. Enter search criteria in the **DHCP Option Template** field and click **Search**. To return all currently defined option templates, enter *****. 3. From the search results, select an option template and click **OK**. **Result:** The option template appears in the **Option Template** field.
Assign a policy template	1. In the **DHCP Configuration File Policies** section, click ... beside the **Policy Template** field. **Result:** The DHCP Policy Template Search window opens. 2. Enter search criteria in the **DHCP Policy Template** field and click **Search**. To return all currently defined option templates, enter *****. 3. From the search results, select a policy template and click **OK**. **Result:** The policy template appears in the **Policy Template** field.

6 A client class can also optionally be assigned to a DHCP server and/or a subnet.

If you want to …	Then …
Assign a DHCP server to the client class	1. Expand the **Server Assignment** section and enter search criteria in the **Available DHCP Servers** field. To return all currently defined DHCP servers, enter *. 2. Click **Search**. 3. Select one or more DHCP servers from the search results and click **Add=>**. **Result:** The DHCP servers appear in the **Assigned DHCP Servers** list.
Assign subnets to the client class	1. Expand the **Subnet Assignment** section. 2. Expand the Networks node in the **Available Subnets** list. 3. Select one or more subnets. 4. Click **Add=>**. **Result:** The subnets appears in the **Assigned Subnets** list.

7 Click **Submit**.

Result: A confirmation dialog opens with the message **Client class saved**.

8 Click **OK**.

Result: The User Class Client Class Properties page opens.

END OF STEPS

Modify a User Class Client Class

Purpose

Use this procedure to modify a User Class Client Class.

Procedure

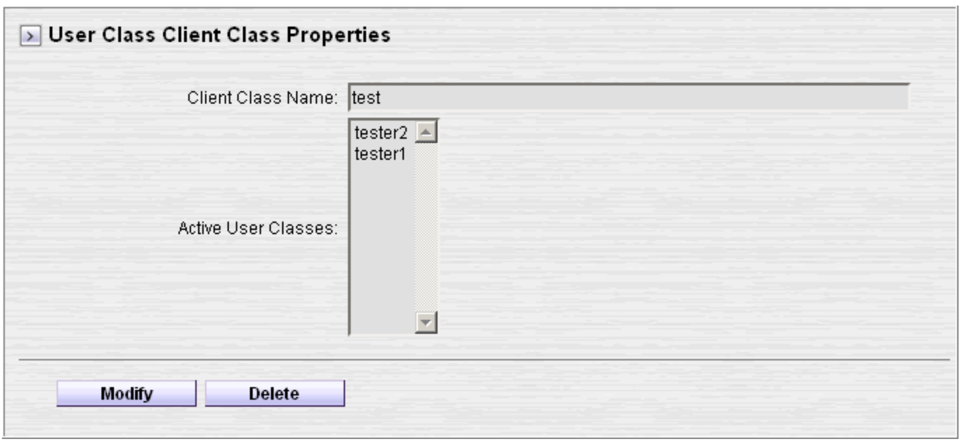
To modify a User Class Client Class, follow these steps:

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy opens.

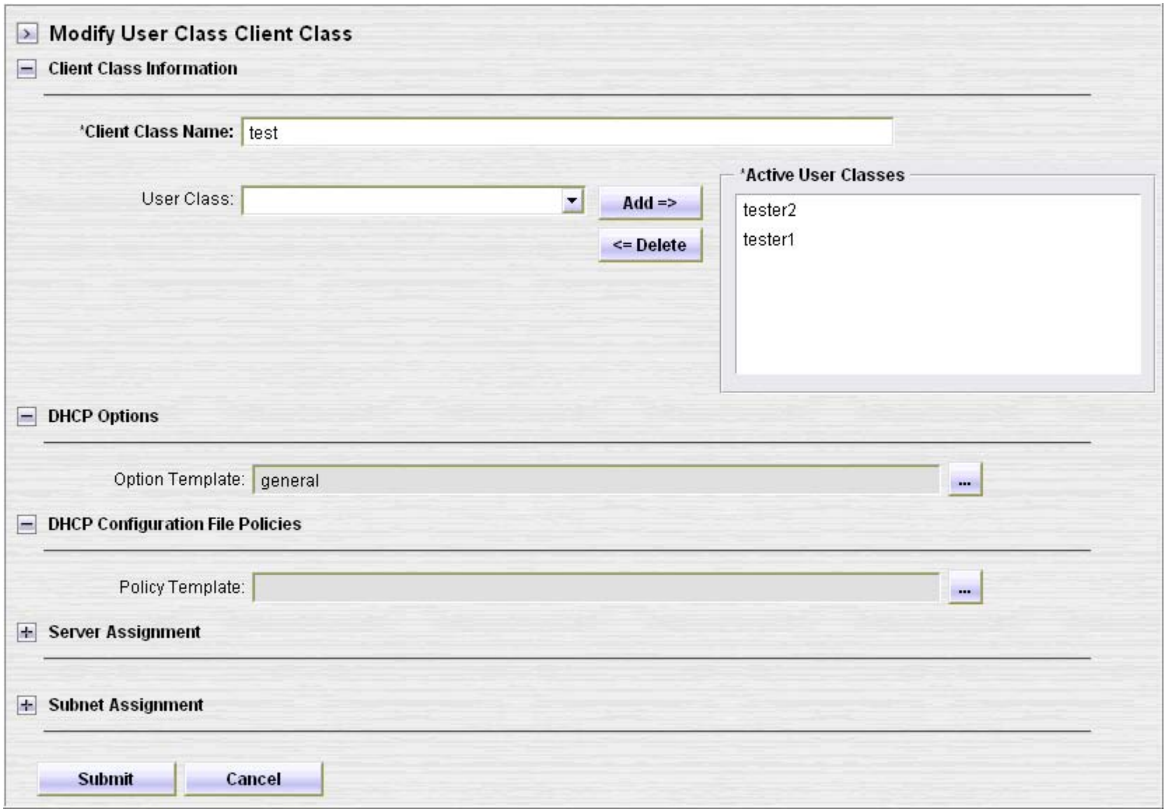
2 From the DHCP Client Class Hierarchy, expand User Class Client Classes and select a user class client class.

Result: The User Class Client Class Properties page opens.



3 Click **Modify**.

Result: The Modify User Class Client Class page opens.



4 Make changes as needed. For more information on DHCP Options, DHCP Configuration Policies, DHCP server assignment, and subnet assignment, refer to steps 5 and 6 in "Add a new User Class Client Class" (p. 21-2).

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

Result: A confirmation dialog opens with the message **Client class saved**.

6 Click **OK**.

Result: The User Class Client Class Properties page opens.

END OF STEPS

Delete a User Class Client Class

Purpose

Use this procedure to delete a User Class Client Class.

Before you begin

DHCP server assignments and subnet assignments must be removed from a user class client class (with the Modify function) before you can successfully delete it.

Procedure

To delete a User Class Client Class, follow these steps:

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

2 From the DHCP Client Class Hierarchy, expand User Class Client Classes and select a user class client class you want to delete.

Result: The User Class Client Class Properties page opens.

3 Click **Delete**.

Result: A confirmation dialog opens with the message **Are you sure you want to delete the selected Client Class?**

4 Click **OK**.

Result: A confirmation dialog opens with the message **Client Class deleted**.

5 Click **OK**.

END OF STEPS

Add a new Vendor Class Client Class

Purpose

Use this procedure to add a new Vendor Class Client Class.

Procedure

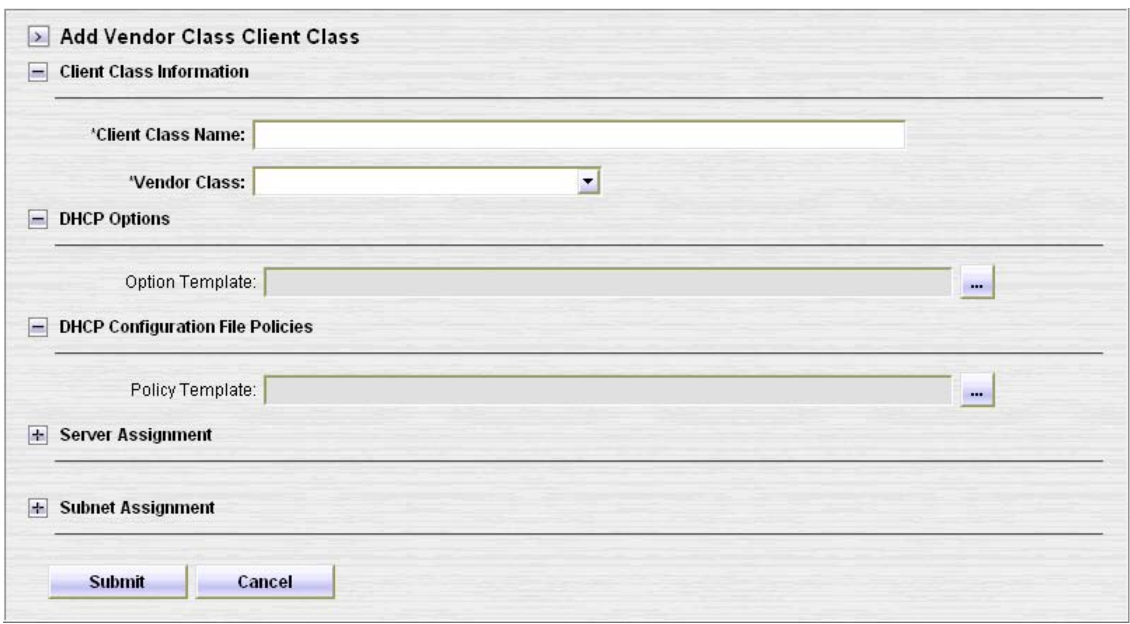
To add a new Vendor Class Client Class, follow these steps:

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

2 From the **Actions** menu, select **Add Vendor Class Client Class**.

Result: The Add Vendor Class Client Class page opens.



3 In the **Client Class Name** field, enter a name for the client class.

4 In the **Vendor Class** field, enter a name for the vendor class or select an existing vendor class.

5 Assign DHCP Options and/or DHCP Configuration Policies, and (optionally) make server and subnet assignments as required. For more information, refer to steps 5 and 6 in "Add a new User Class Client Class" (p. 21-2).

6 To save your changes, click **Submit**.

Result: A confirmation dialog opens with the message **Client class saved**.

7 Click **OK**.

Result: The Vendor Class Client Class Properties page opens.

END OF STEPS

Modify a Vendor Class Client Class

Purpose

Use this procedure to modify a Vendor Class Client Class.

Procedure

To modify a Vendor Class Client Class, follow these steps:

1 Select **DHCP Client Class** from the **DHCP** menu.

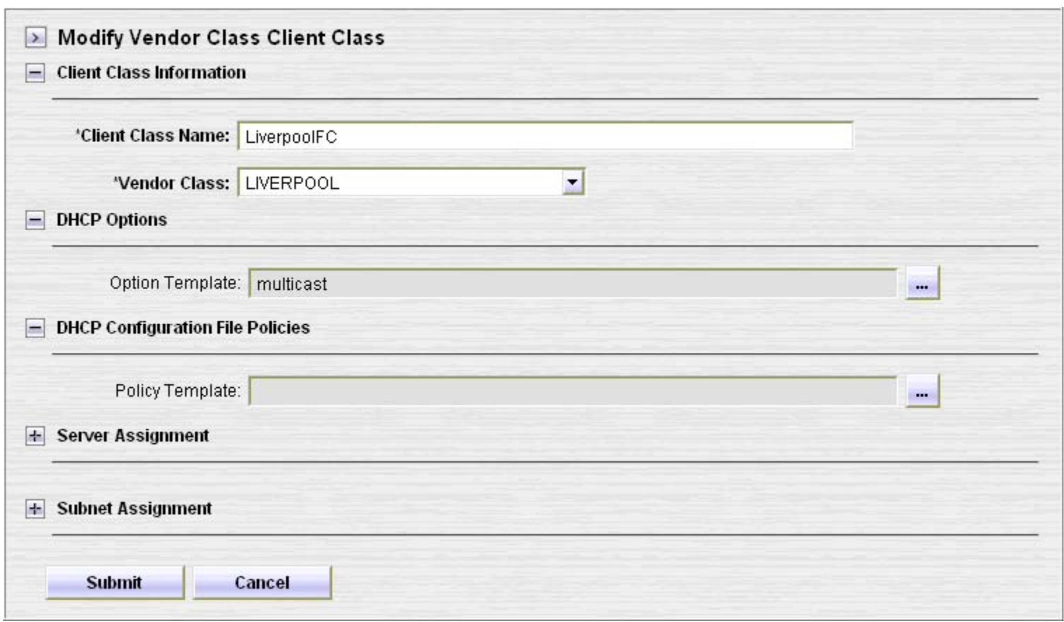
Result: The DHCP Client Class Hierarchy opens.

2 Expand the **Vendor Class Client Classes** node and select the vendor class client class you wish to modify.

Result: The Vendor Class Client Class Properties window opens.

3 Click **Modify**.

4 The Modify Vendor Class Client Class page opens.



5 Make changes as needed. For more information on DHCP Options, DHCP Configuration Policies, DHCP server assignment, and subnet assignment, refer to steps 5 and 6 in "Add a new User Class Client Class" (p. 21-2).

6 To save your changes, click **Submit**.

Result: A confirmation dialog opens with the message **Client class saved**.

7 Click **OK**.

Result: The Vendor Class Client Class Properties page opens.

END OF STEPS

Delete a Vendor Class Client Class

Purpose

Use this procedure to delete a Vendor Class Client Class.

Before you begin

DHCP server assignments and subnet assignments must be removed from a vendor class client class (with the Modify function) before you can successfully delete it.

Procedure

To delete a Vendor Class Client Class, follow these steps:

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

2 Expand the Vendor Class Client Classes node and select a vendor class client class you want to delete.

Result: The Vendor Class Client Class Properties page opens.

3 Click **Delete**.

Result: A confirmation dialog opens with the message **Are you sure you want to delete the selected Client Class?**

4 Click **OK**.

Result: A confirmation dialog opens with the message **Client Class deleted**.

5 Click **OK**.

END OF STEPS

Add a new Device Class Client Class

Purpose

Use this procedure to add a new Device Class Client Class.

Procedure

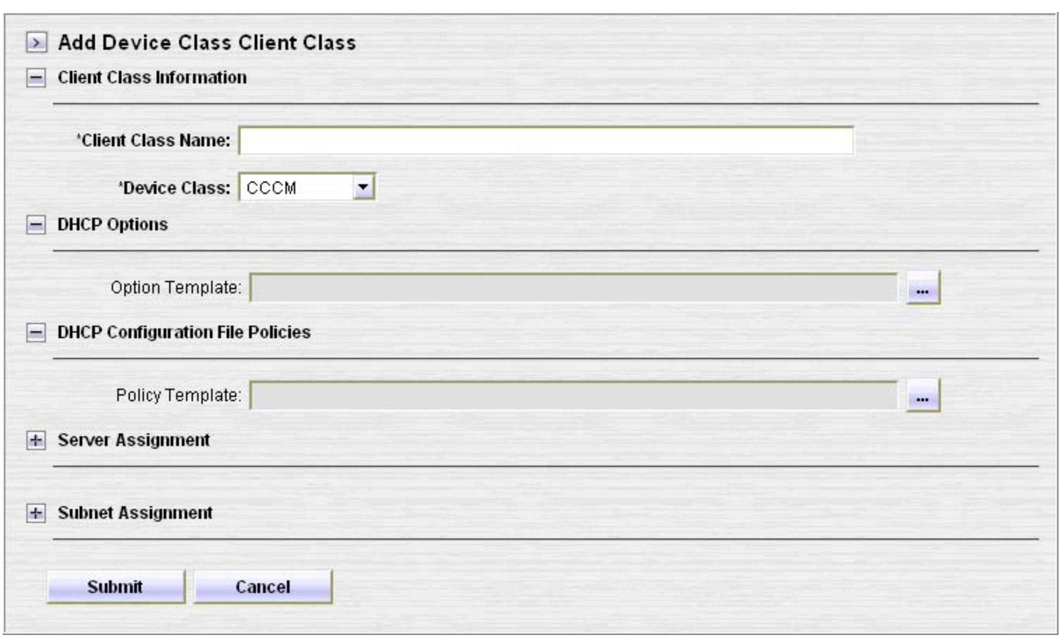
To add a new Device Class Client Class, follow these steps:

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

2 From the **Actions** menu, select **Add Device Class Client Class**.

Result: The Add Vendor Class Client Class page opens.



3 In the **Client Class Name** field, enter a name for the client class.

4 From the **Device Class** drop-down list, select the only available device class, **CCCM**.

5 Assign a DHCP option template and/or DHCP policy template, and (optionally) a DHCP server, and subnet. For more information, see steps 5 and 6 in "Add a new User Class Client Class" (p. 21-2).

6 Click **Submit**.

Result: A confirmation dialog opens with the message **Client class saved**.

7 Click **OK**.

Result: The Device Class Client Class Properties page opens.

END OF STEPS

Modify a Device Class Client Class

Purpose

Use this procedure to modify a Device Class Client Class.

Procedure

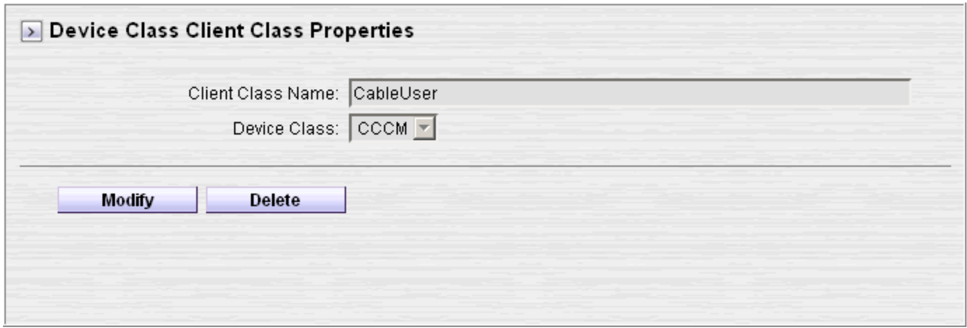
To modify a Device Class Client Class, follow these steps:

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

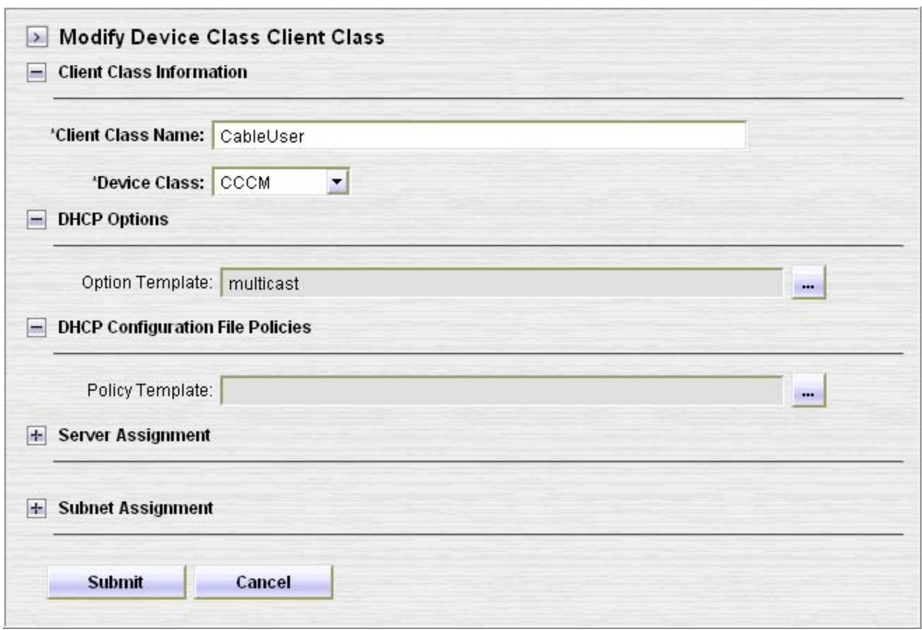
2 Expand the Device Class Client Classes node and select a device class client class.

Result: The Device Class Client Class Properties page opens.



3 Click **Modify**.

Result: The Modify Device Class Client Class page opens.



4 Make changes as needed. For more information on DHCP Options, DHCP Configuration Policies, DHCP server assignment, and subnet assignment, refer to steps 5 through 8 in "Add a new User Class Client Class" (p. 21-2).

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

Result: A confirmation dialog opens with the message **Client class saved**.

6 Click **OK**.

Result: The Device Class Client Class Properties page opens.

END OF STEPS

Delete a Device Class Client Class

Purpose

Use this procedure to delete a Device Class Client Class.

Before you begin

DHCP server assignments and subnet assignments must be removed from a device class client class (with the Modify function) before you can successfully delete it.

Procedure

To delete a Device Class Client Class, follow these steps:

1 Select **DHCP Client Class** from the **DHCP** menu. The DHCP Client Class Hierarchy opens.

2 From the DHCP Client Class Hierarchy, expand Device Class Client Classes and select a device class client class you want to delete. The Device Class Client Class Properties window opens.

3 Click **Delete**.

Result: A confirmation dialog opens with the message **Are you sure you want to delete the selected Client Class?**

4 Click **OK**.

Result: A confirmation dialog opens with the message **Client Class deleted**.

5 Click **OK**.

END OF STEPS

Add a User Class

Purpose

To create a user class.

Procedure

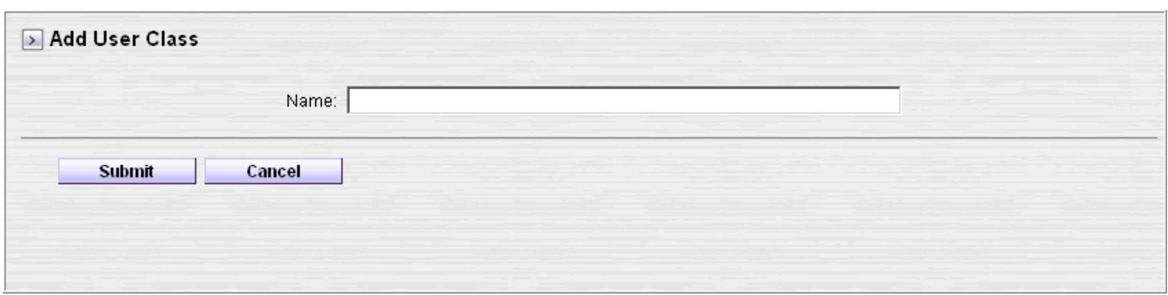
To create a user class, follow these steps.

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

2 Mouse over the **Actions** menu and select **Add User Class**.

Result: The Add User Class page opens.



3 Enter an alphanumeric name for the user class in the **Name** field.

4 Click **Submit**.

Result: A confirmation dialog opens with the message **User Class - <user class name> saved.**

5 Click **OK**.

Result: The User Class Properties page opens.

End of Steps

Modify a User Class

Purpose

To modify a user class.

Procedure

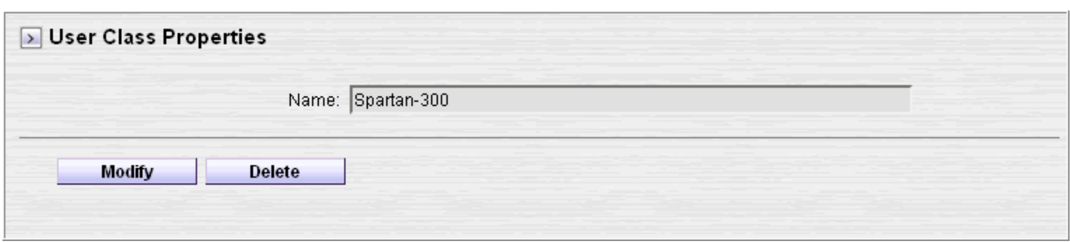
To modify a user class, follow these steps.

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

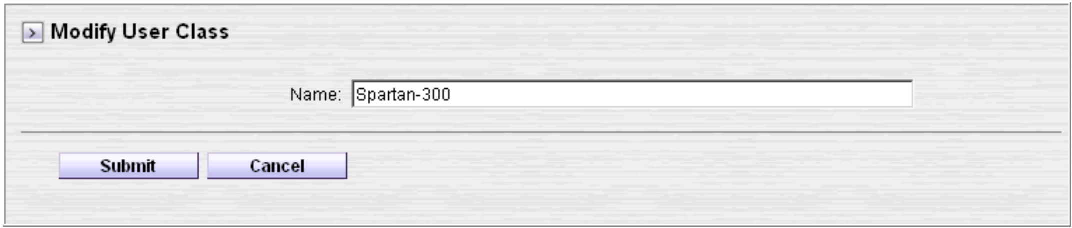
2 Expand the **User Classes** node and select the user class you want to modify.

Result: The User Class Properties page opens.



3 Click **Modify**.

Result: The Modify User Class page opens.



4 Change the user class name as required and click **Submit**.

Result: A confirmation dialog opens with the message **User Class - <user class name> saved.**

5 Click **OK**.

Result: The User Class Properties page opens.

END OF STEPS

Delete a User Class

Purpose

To delete a user class.

Before you begin

You cannot delete a user class until its association with a client class has been removed.

Procedure

To delete a user class, follow these steps.

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

2 Expand the **User Classes** node and select the user class you want to delete.

Result: The User Class Properties page opens.

3 Click **Delete**.

Result: A confirmation dialog opens with the message **You are about to delete User Class - <user class name>. Are you sure you want to proceed?**

4 Click **OK**.

Result: A confirmation dialog opens with the message **User Class - <user class name> deleted.**

Note: An additional confirmation dialog opens if the user class is also associated with an object/address template.

5 Click **OK**.

END OF STEPS

Add a Vendor Class

Purpose

To add a vendor class.

Procedure

To add a vendor class, follow these steps.

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

2 Mouse over the **Actions** menu and select **Add Vendor Class**.

Result: The Add Vendor Class page opens.

3 Enter an alphanumeric name for the vendor class in the **Name** field.

4 Click **Submit**.

Result: A confirmation dialog opens with the message **Vendor Class - <vendor class name> saved.**

5 Click **OK**.

Result: The Vendor Class Properties page opens.

END OF STEPS

Modify a Vendor Class

Purpose

To modify a vendor class.

Procedure

To modify a vendor class, follow these steps.

1 Select **DHCP Client Class** from the **DHCP** menu.

Result: The DHCP Client Class Hierarchy page opens.

2 Expand the **Vendor Classes** node and select the vendor class you want to modify.

Result: The Vendor Class Properties page opens.

3 Click **Modify**.

Result: The Modify Vendor Class page opens.

4 Change the vendor class name as required and click **Submit**.

Result: A confirmation dialog opens with the message **Vendor Class - <vendor class name> saved.**

5 Click **OK**.

Result: The Vendor Class Properties page opens.

END OF STEPS

Delete a Vendor Class

Purpose

To delete a vendor class.

Before you begin

You cannot delete a vendor class until its association with a client class has been removed.

Procedure

To delete a vendor class, follow these steps.

1. Select **DHCP Client Class** from the **DHCP** menu.

   Result: The DHCP Client Class Hierarchy page opens.

2. Expand the **Vendor Classes** node and select the vendor class you want to delete.

   Result: The User Class Properties page opens.

3. Click **Delete**.

   Result: A confirmation dialog opens with the message **You are about to delete Vendor Class - <vendor class name>. Are you sure you want to proceed?**

4. Click **OK**.

   Result: A confirmation dialog opens with the message **Vendor Class - <vendor class name> deleted.**

   Note: An additional confirmation dialog opens if the vendor class is also associated with an object/address template.

5. Click **OK**.

END OF STEPS

22 DHCP configuration file generation

Overview

Purpose

This chapter describes the **Generation DHCP Configuration** function, which is used to configure, view, and update the policy, data, and configuration files for DHCP.

Contents

This chapter covers these topics.

About DHCP configuration file generation

Overview

Purpose

Generate DHCP Configuration allows you to configure, view, and update the policy, data and configuration files of DHCP. Data and configuration files define the behavior of DNS and DHCP servers through the transmission, or "push" of data to the servers. The information that is transmitted is determined by both the setup of the infrastructure and the subnet information.

Infrastructure setup

All infrastructure must be set up prior to using **Generate DHCP Configuration**, which includes a domain, a network, a DHCP server, and a DHCP/Bootp template for your system.

Once you have set up the infrastructure and configured the subnets, you can create the necessary files and records required to operate DHCP with VitalQIP.

Generate DHCP Configuration allows you to update and configure the following:

- DNS Configuration and Domain Zone files, and Reverse Zone files
- DHCP Configuration and Policy files
- Bootp services
- Active leases for a DHCP server or a specific subnet of a DHCP server

DHCP generation

Overview

Purpose

This function enables you to generate the DHCP configuration and data files appropriate to the type of DHCP server selected. You can only generate DHCP files for DHCP servers. (Note that the server may be a Bootp server as well, depending on the server vendor.)

When a DHCP Generation is performed, the DHCP configuration files are generated, based on your Server Type, as described in the following table.

Table 22-1 Generated DHCP configuration files

Server Type	Files
Lucent DHCP	*dhcpd.conf, dhcpd.pcy, x.ddns.conf* (Refer to the note below), and *dhcp.db*
Microsoft DHCP	Data is written to the Registry

Note: "x" is 1, 2, 3… representing the Organization ID number. By default, if only one organization defined, the generated file is *1.ddns.conf*. The *1.ddns.conf* file lists the configured domains and the primary and secondary DNS servers to dynamically update.

VitalQIP push logic

The VitalQIP "push" logic for the Lucent DHCP server is as follows:

- For D-DHCP, A-DHCP, M-DHCP, and A-BOOTP objects: If the DHCP template associated with the object uses **Same as Subnet Profile** for routers (gateways), DNS servers, or TFTP servers, then the *dhcpd.conf* file is generated with the values from the subnet, whether or not those values have been overridden at the object level. There is no DHCP template option for **Same as Object Profile** for these three DHCP options. If they are **User Defined**, then the user-defined value(s) are pushed. Otherwise, the values associated with the subnet are used.
- For M-BOOTP objects: The values for routers, time-servers, and DNS servers are taken from the object. For these objects, the values from the subnet are copied to the object when the object is created, and then can be further modified in the M-BOOTP setup window/tab in the Object Profile.

When an administrator attempts to “push” DHCP configuration files to a DHCP server, a “Privilege Denied” error message appears if a failover server has been configured and has not been assigned to the administrator. To resolve this problem, use the thick client to add the failover server to the administrator’s Managed List in the Administrator Profile.

Control debug levels for Lucent DHCP servers

The DHCP Generation screen provides a way to push requests to Lucent DHCP servers to reinitialize the debug log, or change the debug level, or stop the debug logging all together, all without restarting the server.

The primary intent of this functionality is to provide a means for generating additional log data to assist in troubleshooting DHCP server problems without restarting the server, as was previously required by Lucent servers, to change the debug level or clear the debug log. The debug level selected with this new functionality does not affect the debug level defined for the server in the Server Profile. The debug level specified therefore only applies until the next DHCP file generation, or until superseded by a subsequent enhanced debug request: the selected debug level does not get saved as the server’s debug level, and the level of debugging in the debug log can be reset with the next File Generation/push.

A file named *%QDHCPCONFIG%/qdhcp_logaction.txt* is pushed to the Lucent DHCP server by VitalQIP, instructing the server how to respond to the receipt of the control/signal.

Generate DHCP configuration files

Purpose

Use this procedure to generate DHCP configuration files.

Before you begin

For Lucent DHCP servers, the server’s current debug level is selected in the drop-down list (if set to **None** in the Server Profile, the first setting in the **Change Debug Level** drop-down list is displayed even though it is not active). You can change the debug levels by selecting **Debug**.

Procedure

To generate DHCP configuration files, follow these steps.

1 Mouse over **DHCP** and click **DHCP Server**.

Result: The DHCP Server hierarchy opens.

2 Expand the hierarchy until you come to the DHCP that you want to generate configuration files.

3 Expand the list of DHCP servers and click the one that you want to perform a DHCP push.

Result: The DHCP Properties page opens.

The fields on this page are read only. They indicate the properties of the DHCP server you have selected.

4 Click **Perform DHCP Generation**.

Result: The Generate DHCP Configuration File page opens.

The DHCP server information appears in the upper portion of this page. The fields on the remaining portion of this page are as follows.

Table 22-2 DHCP configuration setup fields

Field	Description
Generate to Directory	***Read only***. Name of the directory where the configuration files will be generated.

Field	Description
Type	***Required***. Check the radio button to specify where you want the files to go. Allowable values are: • **Server** – Perform DHCP generation (default). • **Preview** - Preview the generated DHCP. • **Debug** – Change the Debug options for this server. This option is only available if the server is a Lucent DHCP server.
Debug Options	If Type is set to **Debug**, you can select one of the following options for this server: • **Change Debug Level** - Changes the debug level. This option enables **Debug Level** options when selected. • **Clear Debug Log** - Clears the debug log • **Stop Debug Log** - Stops debugging.
Debug Level	If Debug is set to **Change Debug Level**, you can select one of the following options for the debug level for this server: • **LevelCritical** – The default value. A critical error is one that shuts down the program. Only critical messages are logged. • **LevelError** – An error has occurred, but the program should continue. Critical messages are included. • **LevelWarning** – The program has encountered an unexpected issue but continues. Errors and critical messages are included with these warnings. • **LevelInfo** – These are informational messages about the program events and flow. These messages include critical messages, errors, and warnings. • **LevelDebug** – Indicates that all levels should be logged. **Note:** The current debug level for the server is the one that is initially selected when you open the Generate DHCP Configuration File page.

5 In the **Scheduler** area, select a schedule for DHCP configuration file generation. For more information about scheduling the DHCP configuration file generation, see "Schedule a report" (p. 29-6).

6 Click **Submit**.

Result: If you selected **Server**, the DHCP files are exported to the specified directory on the server. The DHCP generation is performed, or the Debug level is set.

END OF STEPS

DHCP user exit

The section describes the default user exits. You can rename user exits if desired. See the *VitalQIP Administrator Reference Manual* for more information. VitalQIP provides a user exit (**`qipdhcpuserexit`**) that allows you to manipulate the DHCP configuration file after it has been created. The user exit is called after the *dhcpd.pcy* and *dhcpd.conf* files are created, but before the DHCP Service is notified to refresh the configuration files. The user exit is run if it exists and has the five parameters listed below. Create the user exit script in the *%QIPHOME%\userexits* directory.

Note: Use full path names within user exit routines. Otherwise, output files are directed to *%QIPHOME%*.

Synopsis

```
%QIPHOME%\userexits\qipdhcpuserexit(.bat, .exe, .cmd, .pl)
   [server_name] [server_IP] [current_push_directory]
   [remote_push_directory] [SERVER or LOCAL]
```

Parameters

The following parameters are passed to **`qipdhcpuserexit`**:

server_name	The name of the server where the user exit is being pushed
server_IP	The IP address of the server to which the user exit is being pushed
current_push_directory	The directory where files are currently stored. This will only be different from the remote_push_directory if this user exit is being run on the File Generation Service. **Note:** The directory may be set to NONE if the directory is not available.
remote_push_directory	The directory on the Remote Service where files will be placed. **Note:** The directory may be set to NONE if the directory is not available.
`Server` or **`Local`**	Specifies the type of push.

When a server push user exit runs on the File Generation Service, the user exit name must be amended to include the “fgs” suffix, for example **`qipdhcpuserexitfgs`**.

View active DHCP leases

Purpose

Use this procedure to view active DHCP leases.

Before you begin

- Lease Information is retrieved directly from the DHCP server's lease database, not the VitalQIP database.
- The items listed in the Active Leases Information page are listed in ascending IP address order. The Object and Domain Name which appear in the listing are generated as follows:
  - If the Object Name or Domain Name exists in the DHCP database, that name is used.
  - If the Object Name or Domain Name does not exist in the DHCP database, the system uses the name stored within VitalQIP if the object is defined. However, the Object Name and/or Domain Name are prefixed with an asterisk (*) to indicate that the name was taken from VitalQIP.
  - If the Object Name or Domain Name does not exist in the DHCP database, and there is no Object Name or Domain Name within VitalQIP (for example, the object has not been defined), the Object Name and/or Domain Name are blank.

Procedure

To view active DHCP leases, follow these steps.

1 Mouse over **DHCP** and click **DHCP Server**.

Result: The DHCP Server hierarchy opens.

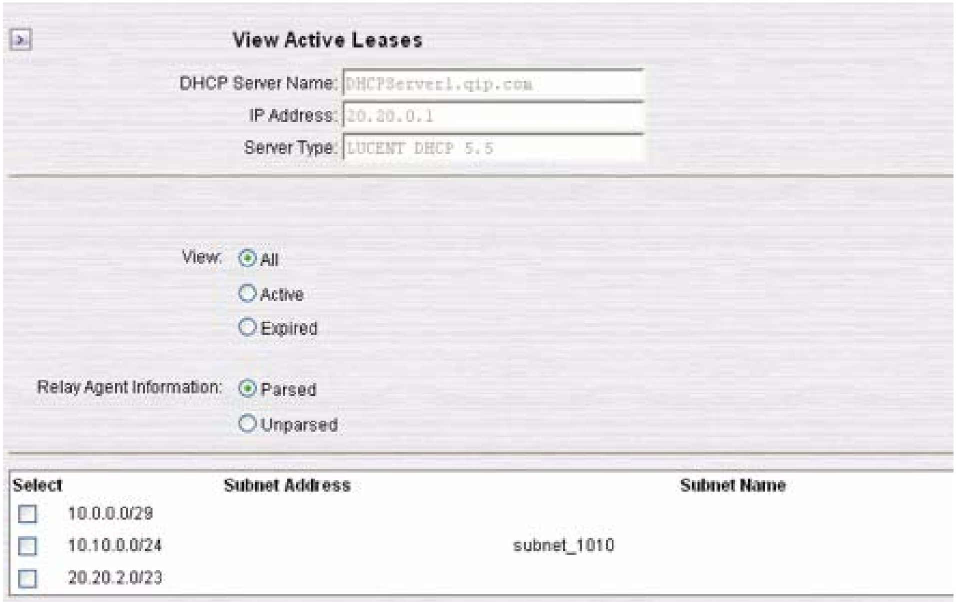
2 Expand the list of DHCP servers and click the one whose active leases you want to view.

Result: The DHCP Properties page opens.

The fields on this page are read only. They indicate the properties of the DHCP server you have selected.

3 Click **View Active Leases**.

Result: The View Active Leases page opens.



4 Select the appropriate radio button for the type of leases you want to view.

- **All** – Displays both active and expired leases
- **Active** – Displays only those leases that are active
- **Expired** – Displays only those leases that have expired.

5 Relay Agent information options are those associated with DHCP Option 82. Select the appropriate radio button to display **Relay Agent Information**:

- **Parsed** – Include the Relay Agent information in the active lease view
- **Unparsed** – Do not include the Relay Agent information in the active lease view.

6 Chose one of the following action if you need to work with the list.

If you want to...	Refer to...
Select all subnets	Click **Select All**. **Result:** All subnets are selected.
Unselect subnet	Click **Unselect All**. **Result:** Selected subnets are unselected.

If you want to...	Refer to...
Refresh the list	Click **Refresh**. **Result:** The list is updated.

7 Click **Submit**.

Result: The list of leases opens.

8 To delete an active lease, do the following:

a. Select a lease from the list.

Result: The **Delete Lease** button are enabled.

b. Click **Delete Lease**.

Result: A dialog box opens that ask if you want to delete the lease.

c. Click **OK**.

Result: The lease is deleted from the list.

END OF STEPS

23 Access Control

Overview

Purpose

This chapter describes how to configure and manage the Access Control (AC) feature.

Contents

This chapter covers these topics.

Access Control

Overview

Purpose

Access Control (AC) is a feature that allows a network administrator to control which machines are allowed access to which subnets, based on subscriber and device information. This is implemented by mapping a User Class to these devices (via MAC address) and subscribers.

Subscribers and devices are added by an administrator (Administrator registration). In a future release, automatic registration will be supported (the system will automatically add a subscriber when he or she comes online and authenticates him- or herself), as well as manual self-registration (where users can manage their devices themselves).

For Administrator device registration, an administrator selects Access Control in the web client GUI and creates the subscriber, then creates the device, associates them both, and assigns a User Class. At this point, VitalQIP will update the DHCP cache with the MAC-User Class mapping. When the device comes onto the network, it already exists in the DHCP server cache, and thus automatically gets service.

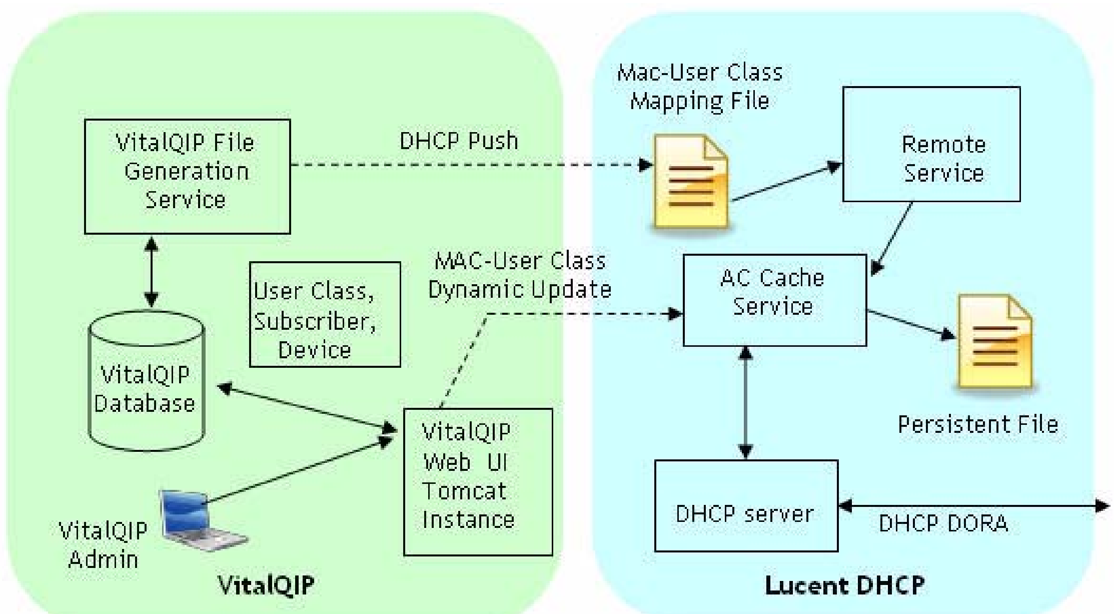


Figure 23-1 Administrator registration architecture

Several major architectural changes have been made to VitalQIP to support this new feature:

- VitalQIP File Generation Service has been enhanced to generate the Mac to User Class mapping file on a DHCP generation for any DHCP server with AC functionality enabled. The remote service reads this file and applies the configuration to the AC Cache Service.
- The VitalQIP Web UI allows administrators to create, modify, and delete subscribers, devices, and the relationships between them, as well as to assign User Classes to subscribers and devices. The Access Control feature is only available to administrators who have permission (in their administrator profile) to manage AC infrastructure. Refer to "Allow AC Management" (p. 6-10).
- The DHCP server is able to query the AC Cache Service for the appropriate user class for a request from an incoming MAC address if AC functionality is enabled on that DHCP server. Refer to Table 20-8, "DHCP server policies" (p. 20-23) for information on policies that enable AC functionality.
- VitalQIP supports dynamic updates to the MAC-User class mappings used by the DHCP server by allowing dynamic update messages to be sent to the AC Cache Service. This behavior can be controlled from the web UI with the **Send AC Updates to DHCP** global policy. Refer to "Send AC Updates to DHCP" (p. 2-30).
- The AC Cache Service manages the MAC to User Class mappings. These mappings are updated from the file that gets pushed out from the FGS on a file generation, as well as from dynamic updates that get sent from the VitalQIP web UI whenever administrators and users change the device and User Class data. The AC Cache Service is responsible for maintaining a current list of these mappings, and responding when the DHCP server requests this information. For more information on policies that control the AC Cache Service, refer to "VitalQIP Access Control policies", in the *VitalQIP Administrator Reference Manual*.
- Devices and Subscribers are available as infrastructure types for use with User Defined Attributes, as described in Chapter 7, "Attributes".

Access Control configuration

Overview

The functionality to support AC in the DHCP 5.6 server is provided through a dynamically loaded callout library named *Qdhcplib_AC*. To support this, three additional policies are automatically added in the "Additional Policies" section when the DHCP server policy **Access Control Enabled** is set to True.

- **`APICalloutLibraryName1=Qdhcplib_AC`**
- **`APIDiscoverCallout1=1`**
- **`APIRequestCallout1=1`**

Note: When the DHCP server has to support additional libraries, the numerical suffix in the policy names is used to distinguish between the multiple libraries. Up to nine different libraries can be supported in the DHCP 5.6 server. For further information, refer to "Multiple callout library feature", in Chapter 2 of the *VitalQIP API Toolkit User's Guide*.

When the DHCP 5.6 server policy **Access Control Enabled** is set to True, the following sub-parameters are required. Refer to Table 20-8, "DHCP server policies" (p. 20-23).

- **DefaultClass** – allows you to define a default User Class in VitalQIP that the AC API callout library can assign to a DHCP client whenever the AC Cache Service is unable to respond to a request from the DHCP server, such as when the AC Cache Service does not find the requested MAC in its cache.
- **ReceiveTimeout** – defines how many milliseconds the DHCP server waits for a response from the AC Cache Service. The default value for this policy is 2000 milliseconds.

Additionally, the **ForceClass** policy should be set to User.

Search subscribers

Purpose

To search for current Access Control subscribers.

Before you begin

- Search results are paged according to the **`SubscriberPageSize`** property in the *qip.properties* file.
- Search criteria for the **Login Name** and **Last Name** fields are not case sensitive.

Procedure

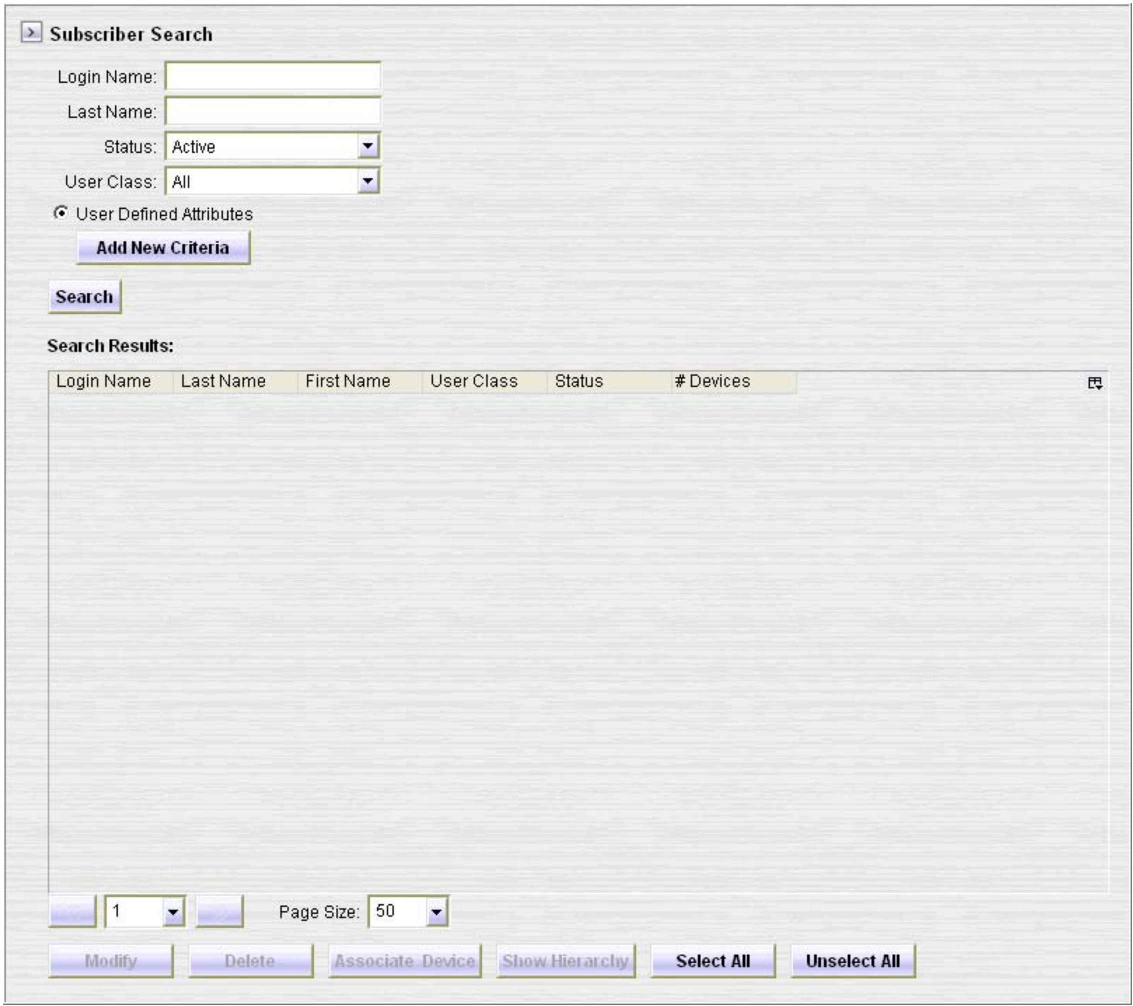
To search for current Access Control subscribers, follow these steps.

---

1 Select **Access Control** from the **DHCP** menu.

If you are already using the Access Control function, mouse over the **Actions** menu and select **View Subscribers**.

Result: The Access Control Hierarchy opens with the Search Subscriber page.



2 Enter search criteria as needed to locate one or more subscribers. Refer to Table 23-1, "Subscriber properties" (p. 23-7) for information on field values.

3 To search on User Defined Attributes, click **Add New Criteria**. Refer to Table 7-2, "User Defined Attribute fields" (p. 7-27) for information on specifying search criteria for UDAs.

4 Click **Search**.

Result: The **Search Results** list displays the results of your search.

5 Choose from the following actions.

If you want to ...	Then ...
Refresh the hierarchy to display a specific subscriber.	Highlight the subscriber in the **Search Results** list and click **Show Hierarchy**.
Modify a subscriber record.	Highlight the subscriber in the **Search Results** list and click **Modify**. Refer to "Modify subscriber" (p. 23-8).
Associate a device with a subscriber.	Highlight the subscriber in the **Search Results** list and click **Associate Device**. Refer to "Associate device with subscriber" (p. 23-10).
Delete one or more subscriber records	Highlight one or more subscribers in the **Search Results** list and click **Delete**. (To select all subscribers in the list, click **Select All**.) Refer to "Delete a subscriber" (p. 23-13).

END OF STEPS

Add subscriber

Purpose

To add an Access Control subscriber.

Procedure

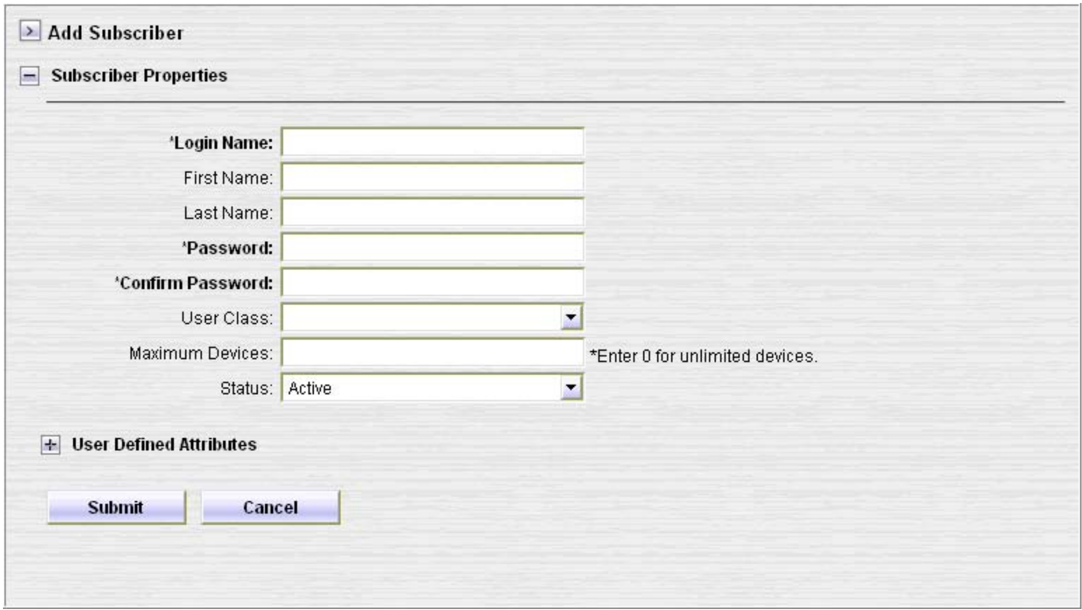
To add an Access Control subscriber, follow these steps.

1 Select **Access Control** from the **DHCP** menu.

Result: The Access Control Hierarchy opens.

2 Mouse over the **Actions** menu and select **Add Subscriber**.

Result: The Add Subscriber page opens.



3 Refer to the following table as you fill in the fields of a subscriber record.

Table 23-1 Subscriber properties

Field	Description
Login Name	***Required***. Enter an alphanumeric subscriber login of up to 255 characters.
First Name	Enter up to 255 characters for the subscriber's first name.
Last Name	Enter up to 255 characters for the subscriber's last name.
Password	***Required***. Enter up to 255 alphanumeric characters for the subscriber's password. Data entry is masked and is stored in encrypted format in the database.
Confirm Password	***Required***. Re-enter the subscriber's password to validate it.
User Class	Select a pre-defined user class from the drop-down list. For information on adding a user class, refer to "Add a User Class" (p. 21-17).

Field	Description
Maximum Devices	Enter the maximum number of devices that can be associated with the subscriber. The maximum number is 2147483647, although you can enter 0 for an unlimited number of devices.
Status	Choose one of the following values from the drop-down list: • **Active** - Authenticate subscriber and go ahead with registration. After registration, an IP address from a registered subnet will be given to the subscriber device. • **Inactive** - User is not currently active and mappings are not sent to the DHCP server for this user's devices. • **Pending** - Subscriber cannot login or register. An IP address from the default subnet is given to the subscriber and the subscriber devices are deleted from cache.

4 Enter User Defined Attributes if any have been defined for the Subscriber Infrastructure Type.

5 Click **Submit**.

Result: A confirmation dialog opens with the message **Subscriber** *<login name>* **Added Successfully**.

6 Click **OK**.

END OF STEPS

Modify subscriber

Purpose

To modify an Access Control subscriber.

Procedure

To modify an Access Control subscriber, follow these steps.

1 Select **Access Control** from the **DHCP** menu.

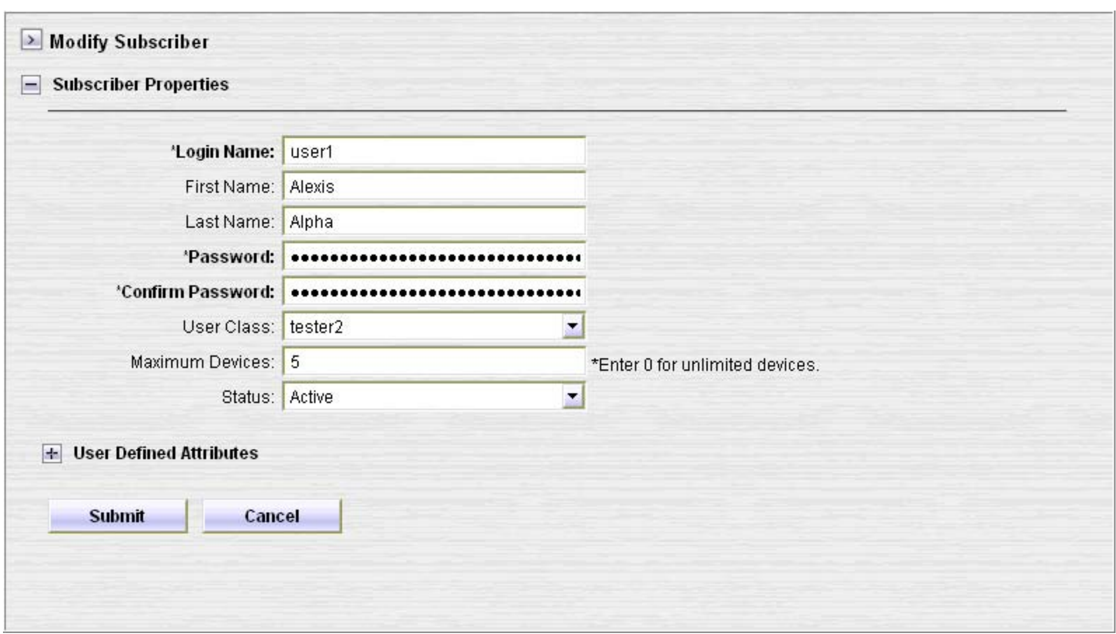
Result: The Access Control Hierarchy opens.

2 Choose one of the following actions.

If you want to ...	Then ...
Locate a subscriber in the hierarchy	Select the subscriber in the Subscribers hierarchy (expand folder if necessary). **Result:** The Subscriber Properties page opens.
Search for a subscriber	1. Enter search criteria in the Search Subscriber page. 2. Select the subscriber in the **Search Results** list.

3 Click **Modify**.

Result: The Modify Subscriber page opens.



4 Modify the subscriber information as required. Refer to Table 23-1, “Subscriber properties” (p. 23-7) for information on the fields.

5 Click **Submit**.

Result: A confirmation dialog opens with the message **Subscriber** *<login name>* **Modified Successfully**.

6 Click **OK**.

END OF STEPS

Associate device with subscriber

Purpose

To associate a device with a subscriber.

Procedure

To associate a device with a subscriber, follow these steps.

1 Select **Access Control** from the **DHCP** menu.

Result: The Access Control Hierarchy opens.

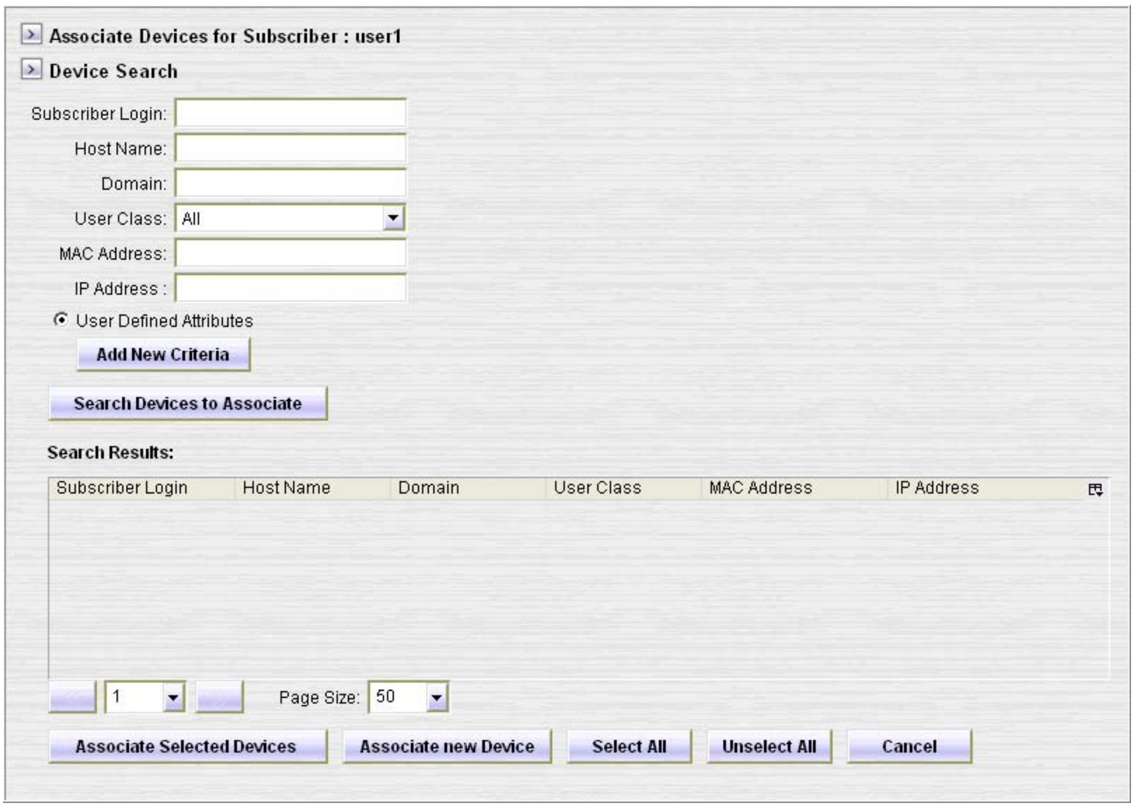
2 Choose one of the following actions.

If you want to …	Then …
Locate a subscriber in the hierarchy	Select the subscriber in the Subscribers hierarchy (expand folder if necessary). **Result:** The Subscriber Properties page opens.

If you want to …	Then …
Search for a subscriber	1. Enter search criteria in the Search Subscriber page. 2. Select the subscriber in the **Search Results** list. **Result:** The Subscriber Properties page opens.

3 Click **Associate Device**.

Result: The Associate Devices for Subscriber page opens.



4 Choose one of the following actions.

If you want to ...	**Then ...**
Search for an existing device to associate	1. Enter search criteria for the device you wish to associate with subscriber. 2. Click **Search Devices to Associate**. **Result:** A list of devices that match your criteria opens in the **Search Results** list. 3. Select one or more devices to associate with the subscriber. 4. Click **Associate Selected Devices**. **Result:** A confirmation dialog opens with the message **Device Association done**. 5. Click **OK**.
Create a new device to associate	Click **Associate new Device**. For more information, refer to "Add device" (p. 23-16).

END OF STEPS

View devices assigned to subscriber

Purpose

To check what devices are currently assigned to a subscriber.

Procedure

To determine what devices are assigned to a subscriber, follow these steps.

1 Select **Access Control** from the **DHCP** menu.

Result: The Access Control Hierarchy opens.

2 Choose one of the following actions.

If you want to ...	Then ...
Locate a subscriber in the hierarchy	1. Expand the **Subscribers** node (expand folder if necessary). **Result:** A list of subscribers opens. 2. Expand the subscriber node whose devices you want to review. 3. Expand the **Devices** node. **Result:** A list of devices assigned to that subscriber opens.
Search for a subscriber	1. Enter search criteria in the Search Subscriber page. 2. Select the subscriber in the **Search Results** list. **Result:** The Subscriber Properties page opens. 3. Click **Show Hierarchy**. **Result:** The subscriber node opens, 4. Expand the subscriber node whose devices you want to review. 5. Expand the **Devices** node. **Result:** A list of devices assigned to that subscriber opens.

END OF STEPS

Delete a subscriber

Purpose

To delete a subscriber record.

Procedure

To delete a subscriber record, follow these steps.

1 Choose one of the following actions.

If you want to ...	**Then ...**
Locate a subscriber in the hierarchy	Select the subscriber in the Subscribers hierarchy (expand folder if necessary). **Result:** The Subscriber Properties page opens.
Search for a subscriber	1. Enter search criteria in the Search Subscriber page. 2. Select the subscriber in the **Search Results** list. **Result:** The Subscriber Properties page opens.

2 Click **Delete**.

Result: A confirmation dialog opens with the message **Delete Subscriber?**

3 Click **Yes**.

Result: A confirmation dialog opens with the message **Subscriber Deleted Successfully**.

4 Click **OK**.

Result: All devices registered for this subscriber are removed from the database and the DHCP cache.

END OF STEPS

Search devices

Purpose

To search for an Access Control device.

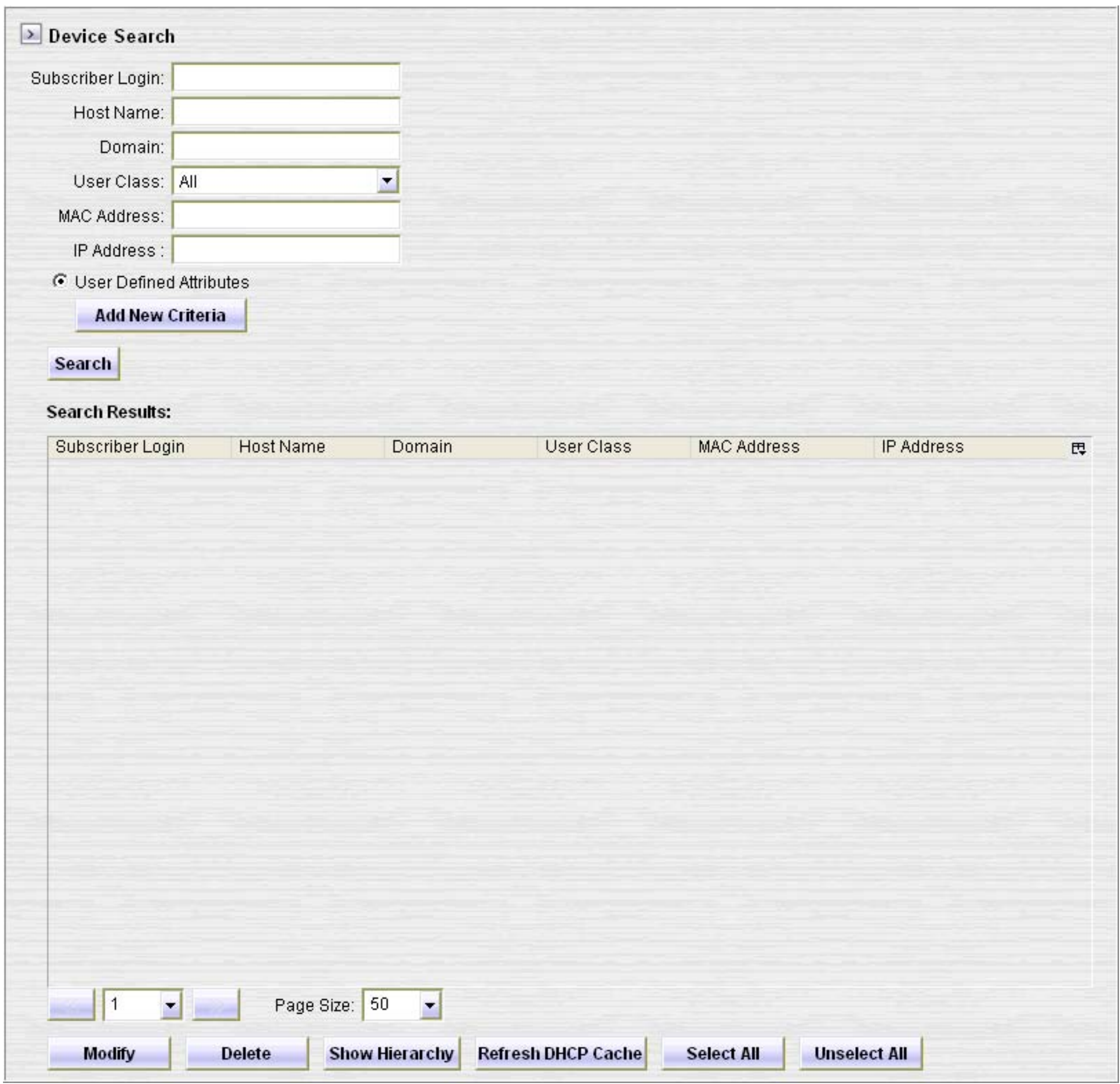
Procedure

To search for an Access Control device, follow these steps.

1 Select **Access Control** from the **DHCP** menu.

2 Mouse over the **Actions** menu and select **View Devices**.

Result: The Device Search page opens.



3 Enter search criteria as needed to locate one or more devices. Refer to Table 23-1, "Subscriber properties" (p. 23-7) for information on field values.

4 To search on User Defined Attributes, click **Add New Criteria**. Refer to Table 7-2, "User Defined Attribute fields" (p. 7-27) for information on specifying search criteria for UDAs.

5 Click **Search**.

Result: The **Search Results** list displays the results of your search.

6 Choose from the following actions.

If you want to ...	Then ...
Refresh the hierarchy to display a specific device	Highlight a device in the **Search Results** list and click **Show Hierarchy**.
Modify a device record	Highlight a device in the **Search Results** list and click **Modify**. Refer to "Modify device" (p. 23-18).
Refresh DHCP cache for one or more devices	Highlight the device(s) in the **Search Results** list and click **Refresh DHCP Cache**. MAC-User Class mappings are then sent to all DHCP servers for the selected devices. Use this feature if a device is not known to the DHCP server for some reason. The information can be resent and makes a push to the DHCP server unnecessary.
Delete one or more device records	Highlight one or more devices in the **Search Results** list and click **Delete**. (To select all devices in the list, click **Select All**.) Refer to "Delete device" (p. 23-20).

END OF STEPS

Add device

Purpose

To add an Access Control device.

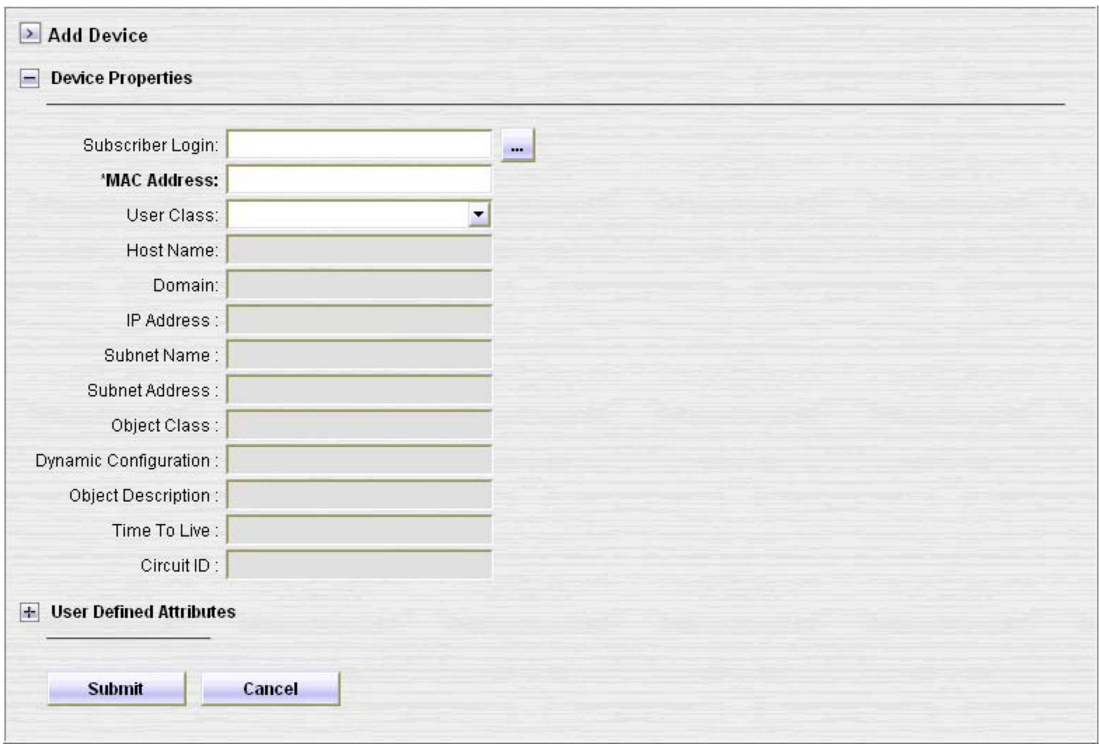
Procedure

To add an Access Control device, follow these steps.

1 Select **Access Control** from the **DHCP** menu.

2 Mouse over the **Actions** menu and select **Add Device**.

Result: The Add Device page opens.



3 Refer to the following table as you fill in the fields of a device record.

Table 23-2 Device properties

Field	Description
Subscriber Login	Enter an existing subscriber login. To search for a subscriber, click ... and enter search criteria to locate the subscriber login to associate with the device you are adding.
MAC Address	Enter a valid MAC address

Field	Description
User Class	Select a pre-defined user class from the drop-down list. For information on adding a user class, refer to "Add a User Class" (p. 21-17). **Note:** If a user class is defined for the device, the subscriber user class (if any) is ignored.

4 Enter User Defined Attributes if any have been defined for the Device Infrastructure Type.

5 Click **Submit**.

Result: A confirmation dialog opens with the message **Device** *<login name>* **Added Successfully**.

6 Click **OK**.

END OF STEPS

Modify device

Purpose

To modify an Access Control device.

Procedure

To modify an Access Control device, follow these steps.

1 Select **Access Control** from the **DHCP** menu.

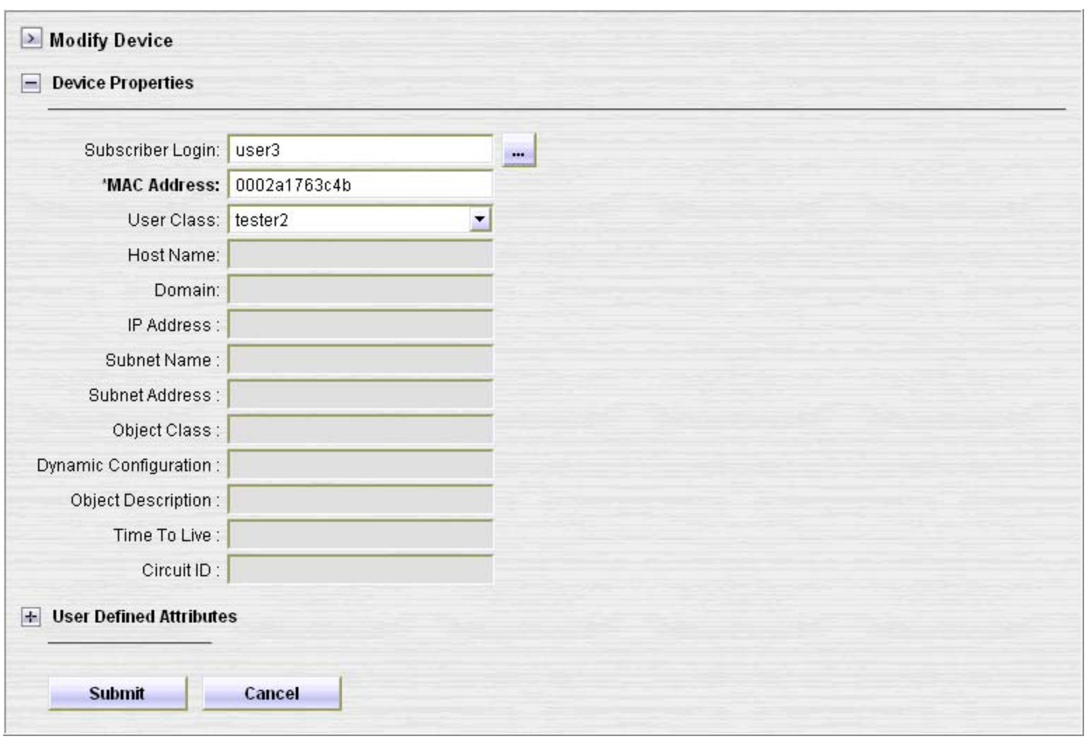
Result: The Access Control Hierarchy opens.

2 Choose one of the following actions.

If you want to …	Then …
Locate a device in the hierarchy	1. Select the subscriber who is associated with the device in the Subscribers hierarchy. 2. Expand **Devices**. 3. Select the device you want to modify. **Result:** The Device Properties page opens.
Search for a device	1. Mouse over the **Actions** menu and select **View Devices**. 2. Select the device you want to modify in the **Search Results** list. **Result:** The Device Properties page opens.

3 Click **Modify**.

Result: The Modify Device page opens.



4 Modify the device information as required. Refer to Table 23-2, "Device properties" (p. 23-17) for information on the fields.

5 Click **Submit**.

Result: A confirmation dialog opens with the message **Device** *<login name>* **Modified Successfully**.

6 Click **OK**.

END OF STEPS

Delete device

Purpose

To delete one of more devices.

Procedure

To delete a device, follow these steps.

1 Select **Access Control** from the **DHCP** menu.

Result: The Access Control Hierarchy opens.

2 Choose one of the following actions.

If you want to ...	Then ...
Locate a device in the hierarchy	1. Select the subscriber who is associated with the device in the Subscribers hierarchy. 2. Expand **Devices**. 3. Select the device you want to delete. **Result:** The Device Properties page opens.

If you want to …	Then …
Search for one or more devices	1. Mouse over the **Actions** menu and select **View Devices**. 2. Enter search criteria for the device(s) you wish to delete. 3. Select the device(s) in the **Search Results** list.

3 Click **Delete**.

Result: A confirmation dialog opens with the message **Delete device(s)?** *<MAC address>.*

4 Click **OK**.

Result: A confirmation dialog opens with the message **Device(s) deleted Successfully**.

END OF STEPS

Part V: Address allocation

Overview

Purpose

The purpose is to provide information for address allocation.

Contents

This part includes these chapters.

24 Address allocation templates

Overview

Purpose

This chapter describes how to manage address templates in VitalQIP.

Contents

This chapter covers these topics.

Address allocation template administration

Overview

Purpose

VitalQIP allows users to configure address templates for use with allocation rules so objects can be automatically created when a block is allocated and when a subnet is consequently created in VitalQIP.

VitalQIP offers several templates to assist in the allocation process.

- An address template is offered that automatically creates objects when a block is created.
- A reverse zone template is offered that automatically configures a reverse zone when a network is created.
- A subnet profile template is offered that automatically configure subnet profile when a subnet is created in VitalQIP.

Administrator privileges

Only a Master type administrator, or a Normal type administrator with Organization access and Access Address Allocation and Maintain Address Templates can add, modify, or delete Address Templates, Subnet Profile Templates, and Reverse Zone Templates.

Static address templates

Static address templates can only contain static object definitions. For a static object definition, you must supply a **Start Offset**, an **End Offset**, and an **Object Class**. You cannot specify a DHCP server when you create a static address template.

Dynamic address templates

Dynamic address templates are only available in the organization in which they are created. A dynamic address template can have both static and dynamic object definitions.

For a dynamic object definition, you must supply a **Start Offset**, an **End Offset**, an **Object Class**, and a **DHCP Server** to be associated with the dynamic scope when it is created. You can optionally supply a **DHCP Scope Policy Template** and/or a **User Class**.

How address templates work

Overview

Address templates are associated with rules. When a block is allocated using a rule with an address template associated with it, the address template is read to determine what objects can be created. An address template can only be associated with a Used rule type. This is the only rule type that creates VitalQIP subnets, and is therefore the only type that can use an address template.

The address template defines what objects can be created during a block allocation. You have the option of not creating all the objects and may enter a smaller number than the template allows. You cannot increase the number of objects to be created, however. During the allocation process, you are prompted to specify how many objects should be created for each object definition in the address template. The default value is to create all the objects listed in the **Number of Objects to be Created** fields.

For static objects, you are prompted to specify the name of the object. You do not have to enter a name. You can leave the <DEFAULT> value as the name of the object. This tells VitalQIP to use the VitalQIP naming policies when creating the object.

Add an address template

Purpose

A managed range is a range of IP addresses in a subnet that is designated for a specific object class. When managed ranges are defined in an address template, they can be automatically assigned IP addresses during the block allocation process. Use this procedure to create an address template.

Procedure

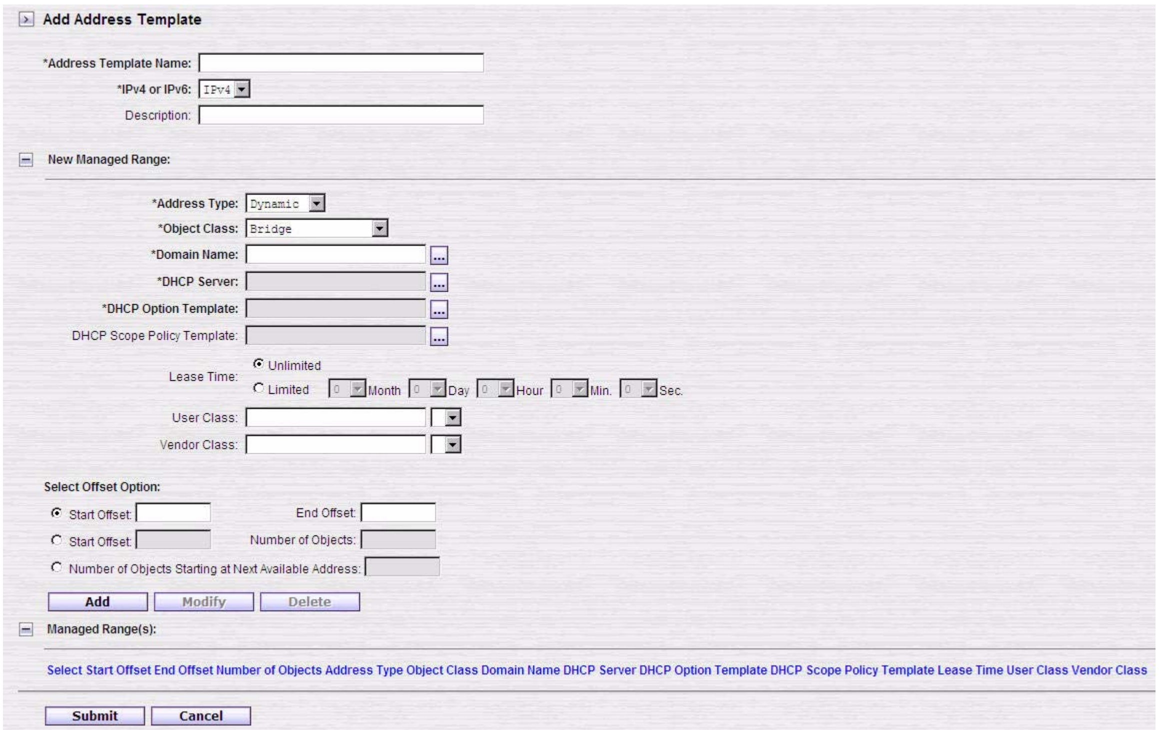
To add an address template, follow these steps.

1. Select **Templates** from the **Infrastructure** menu.

   Result: The Template Hierarchy opens.

2. Mouse over the **Actions** menu and select **Add Address Template**.

Result: The Add Address Template page opens.



3 Fill in the fields after reviewing the following table.

Table 24-1 Address template information fields

Field	Description
Address Template Name	***Required***. Enter up to 32 alphanumeric characters as the template's name.
Description	***Optional***. Enter up to 255 alphanumeric characters of descriptive information.
New Managed Range	
Address Type	***Required***. Establishes which object types are created. The values are: • **Static** – only static objects are created. This is the only value for IPv6 addresses. • **Dynamic** – only dynamic objects are created. • **Reserved** – only reserved objects are created.
Object Class	***Required***. Determines how objects are assigned in a managed range. For a definition of the available object classes, refer to Table 24-2, "Object classes" (p. 24-6).

Field	Description
Domain Name	***Required***. Specifies the domain associated with the address template. Refer to "Search for a domain" (p. 24-9) for additional information about specifying a domain.
Interface Name	***IPv6 only***. Enter up to 64 characters for he interface name (on each of the Nodes), with which the IP Address will be associated.
The following fields only display if the Address Type is set to Dynamic	
DHCP Server	***Required***. If the **Object Type** field is set to **Dynamic**. Select a DHCP server to be associated with the managed range. **Note:** Normal Administrators must have access to the list of DHCP servers in their VitalQIP Administrator profile to select from this field.
DHCP Option Template	***Required***. If the **Object Type** field is set to **Dynamic**, select a DHCP Option Template to be associated with the managed range.
DHCP Scope Policy Template	***Optional***. If the **Object Type** field is set to **Dynamic**, you can select a DHCP Scope Policy Template to be associated with the managed range.
Lease Time	***Optional***. If the **Object Type** field is set to **Dynamic**, you can enter the amount of time in seconds that the lease can exist for the objects in the managed range.
User Class	***Optional***. If the **Object Type** field is set to **Dynamic**, you can create or select a user class to be associated with the managed range. Either enter a user class or select a user class from the drop-down list. **Note:** You can also create a user class in the DHCP Client Class Hierarchy. Refer to "Add a User Class" (p. 21-17).
Vendor Class	***Optional***. Select a vendor class to be associated with the managed range. Either enter a vendor class or select a vendor class from the drop-down list. **Note:** You can also create a vendor class in the DHCP Client Class Hierarchy. Refer to "Add a Vendor Class" (p. 21-20).

Table 24-2 Object classes

Object class	Description
Bridge	Device that forwards traffic between network segments based on data link layer information.
Dynamic_Allocation	Dynamically allocated object.
External	Created by dynamic DNS updates from some product to a DNS server managed by VitalQIP.
Gateway	Device that enables data to flow between different networks.

Object class	Description
Legacy_System	Database management system running on mainframes or minicomputers.
Others	Something other than object types listed here.
Partially_Managed	Allows an object to be managed by VitalQIP administrators and externally modified by Windows administrators. **Note:** For more information, refer to the “Support for External Objects and Resource Records” in Chapter 23, “Advanced DNS Configurations” in the *VitalQIP Administrator Reference Manual*.
PC	Personal computer.
Printer	Device that prints text or graphics on paper.
Router	Device in a network that handles message transfers between computers.
Server	Computer that provides a service(s) for other computers connected to it via a network.
Switch	Packet or circuit switch.
Terminal_Server	Hardware device or server that provides terminals (PCs, printers, and so on) with a common connection point to a local or wide area network.
Test_Equipment	Equipment used for testing.
Undefined	Unknown devices.
Wiring_Hub	Hub at a point where a wiring system in a building or a room is connected to a main concentrator.
Workstation	General-purpose computer used by one person at a time and offers higher performance than normally found in a personal computer.
X-terminal	Intelligent terminal, which operates as an X server directly connected to Ethernet.

Managed Ranges

Use the following fields to define the managed ranges for the address template. You can define managed ranges in one of following ways:

- By Start Offset and End Offset
- By Start Offset and number of objects in the range
- By the number of objects in the offset, regardless of where it starts.

4 Select the radio button next to the method you want to use to define a managed range.

5 On the same line where you selected the radio button, enter values in the appropriate fields, as described in the following table.

Table 24-3 Address template managed ranges

Field	Description
Start Offset	Enter a number that establishes the start address in the subnet where the objects are created. This field, along with the **End Offset** field, establishes the range of objects to be created. Both the start and end offsets are referenced from the beginning of the subnet.
End Offset	Enter a number that establishes the end address in the subnet where objects are created. This field, along with the **Start Offset** field, establishes the range of objects to be created. Both the start and end offsets are referenced from the beginning of the subnet.
Number of Objects	Enter the number of objects contained in the managed range. If you use this field, the end offset of the range is calculated based on this number.
Number of Objects Starting at Next Available Address	Enter the number of objects starting at the next available address.

6 After you enter values for a managed range, click **Add**.

Result: The managed range is added to the **Managed Range(s)** list.

To remove an entry from the list, select the entry and click **Delete**.

7 To add additional ranges to the template, repeat Step 4 through Step 6.

8 Click **Submit** when you have finished.

Result: A confirmation dialog box opens with the message **Address Template Saved**.

9 Click **OK**.

Result: The address template appears in the hierarchy and the Address Template Properties page opens.

END OF STEPS

Search for a domain

Purpose

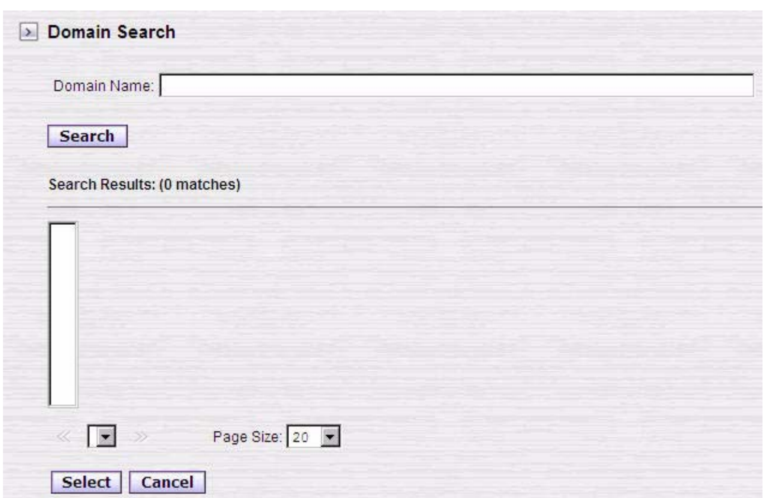
Use this procedure to search for a domain.

Procedure

To search for the domain that is associated with a template, follow these steps.

1 Click the ellipsis button (...) that appears next to the **Domain** field.

Result: The Domain Search dialog box opens.



2 In the **Domain Name** field, enter the first few letters of the domain name and the wildcard character (*) as needed. If you leave this field blank, a list of ***all*** domains is returned.

3 Click **Search**.

Result: The results appear in the **Search Results** list.

4 In the **Search Results** list, highlight a domain.

5 Click **Select**.

Result: The Domain Search dialog box closes and the domain you selected is added to the **Domain Name** field.

END OF STEPS

Modify an address template

Purpose

Use this procedure to modify an address template.

Procedure

To modify an address template, follow these steps.

1 Select **Templates** from the **Infrastructure** menu.

Result: The Template Hierarchy opens.

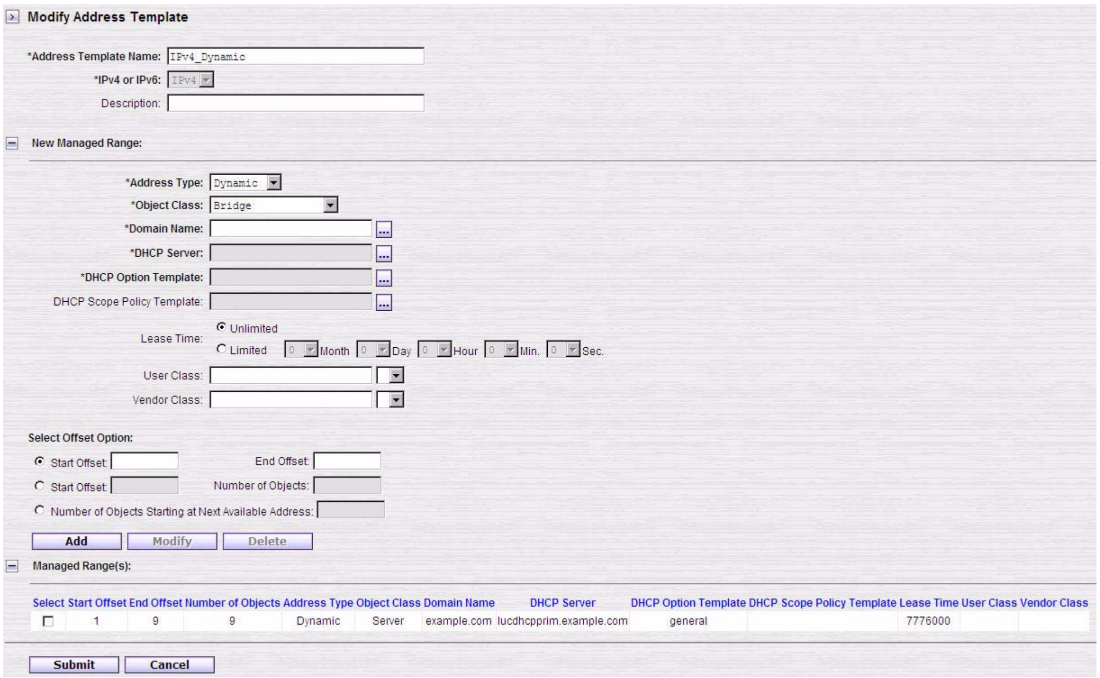
2 Expand the list of address templates until the one you want to modify is visible.

3 Click the address template you want to modify.

Result: The Address Template Properties page opens.

4 Click **Modify**.

Result: The Modify Address Template page opens.



5 Modify the template by changing the values in the appropriate fields. Refer to Table 24-1, "Address template information fields" (p. 24-5) and Table 24-3, "Address template managed ranges" (p. 24-8)Address template managed ranges for information on valuing these fields.

6 When you are done, click **Submit**.

Result: Your changes are saved and Subnet Template Saved dialog box opens.

7 Click **OK** to close the dialog box.

END OF STEPS

Copy an address template

Purpose

Use this procedure to copy an address template.

Procedure

To copy an address template, follow these steps.

1 Select **Templates** from the **Infrastructure** menu.

Result: The Template Hierarchy opens.

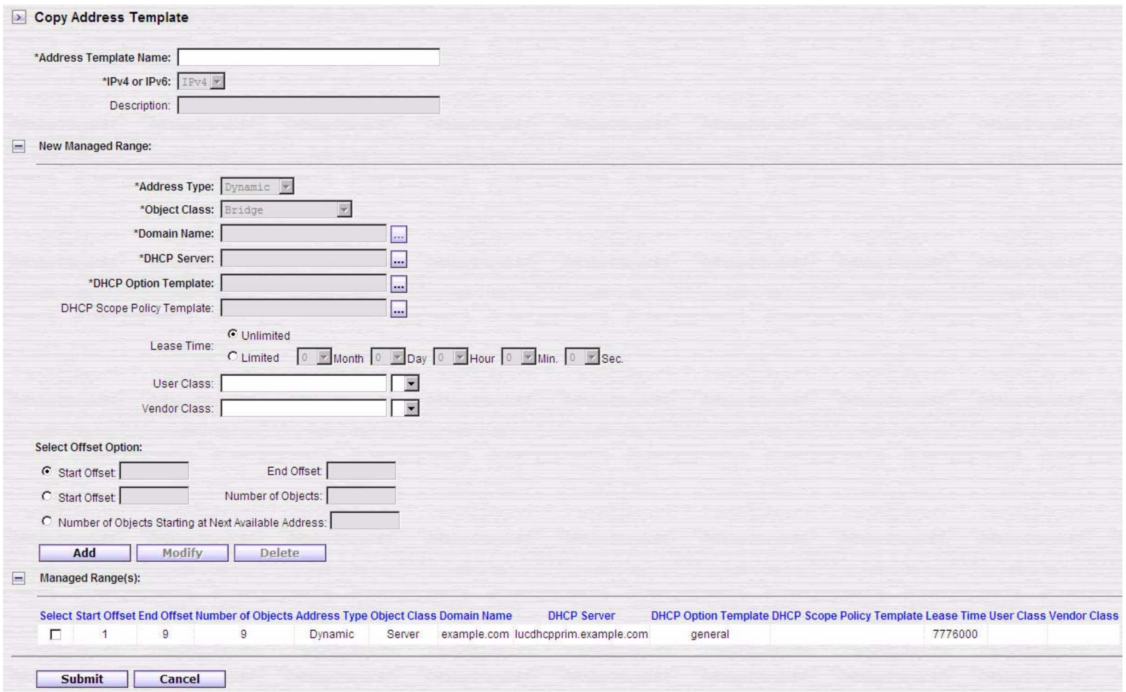
2 Expand the list of address templates until the one you want to copy is visible.

3 Click the address template you want to copy.

Result: The Address Template Properties page opens.

4 Click **Copy**.

Result: The Copy Address Template page opens.



5 Enter a ***unique*** name for the new address template. You cannot modify any other fields. After you copy the template, you can modify it if you want to make additional changes. Refer to "Modify an address template" (p. 24-10) for information on modifying a template.

6 Click **Submit** when you have finished.

END OF STEPS

Associate an address template with a rule

Purpose

You can associate an address template with any "Used" allocation rule. You can make this association when you create or modify a rule, or when you create or modify an address template.

Procedure

To associate an address template with a rule, follow these steps.

1 Select **Templates** from the **Infrastructure** menu.

Result: The Template Hierarchy opens.

2 Expand the list of address templates until the one you want to associate with a rule is visible.

3 Click the address template you want to associate with a rule.

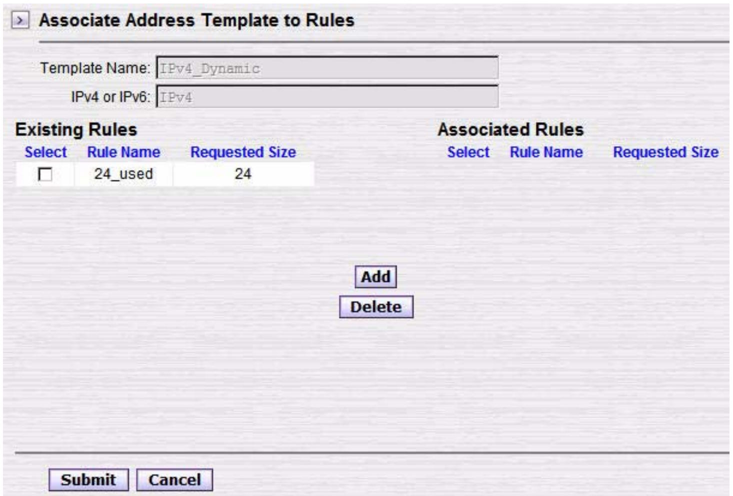
Result: The Address Template Properties page opens.

4 Click **Rule Associations**.

Result: The Associate Address Template to Rules page opens.

Note: This page lists all “Used” rules that are not associated with an address template as well as those rules that are large enough to handle the template size.

5 Select the rule or rules you want to associate with the address template by clicking the checkbox.



6 Click **Add**. The rule moves to the Associated Rules column of the screen and is now associated with this address template.

To disassociate a rule from this address template, click the checkbox next to any rule (or rules) in the Associated Rules column and click **Delete**.

7 Click **Submit** to complete associating the address template with the rule.

END OF STEPS

Delete an address template

Purpose

Use this procedure to delete an address template.

Before you begin

You cannot delete an address template if it is attached to a rule. You need to run a Rule Summary report and note which rules are using the template. Modify each rule to use another template before you return to the Maintain Address Template function and delete the template. The rule must be modified and the address template removed before deleting the address template.

Procedure

To delete an address template, follow these steps.

1 Select **Templates** from the **Infrastructure** menu.

Result: The Template Hierarchy opens.

2 Expand the list of address templates until the one you want to delete is visible.

3 Click the address template you want to delete. The Address Template Properties page opens.

4 Click **Delete**. A dialog box opens with the message **You are about to delete address template '*nnnnnnn*'. Are you sure you want to proceed?**

5 Click **OK**.

Result: The address template is deleted and a confirmation dialog box opens with the message **Address Template Deleted**.

6 Click **OK**.

Result: The address template that was deleted is removed from the infrastructure hierarchy.

END OF STEPS

Reverse zone templates

Overview

VitalQIP allows users to configure reverse zone templates that automatically configure a reverse zone when a network is created. The reverse zone template contains a list of primary and secondary DNS servers. When the reverse zone template is selected during the allocation process, all primary and secondary DNS servers assigned to the reverse zone template are assigned to the reverse zone.

How reverse zone templates work

Reverse zone templates are associated with pools. When a block is allocated to a pool, VitalQIP traverses up the pool hierarchy to find the first pool with a reverse zone template. VitalQIP then uses the first pool with reverse zone template to configure reverse zones when a network is created.

Add a reverse zone template

Purpose

Use this procedure to add a reverse zone template.

Procedure

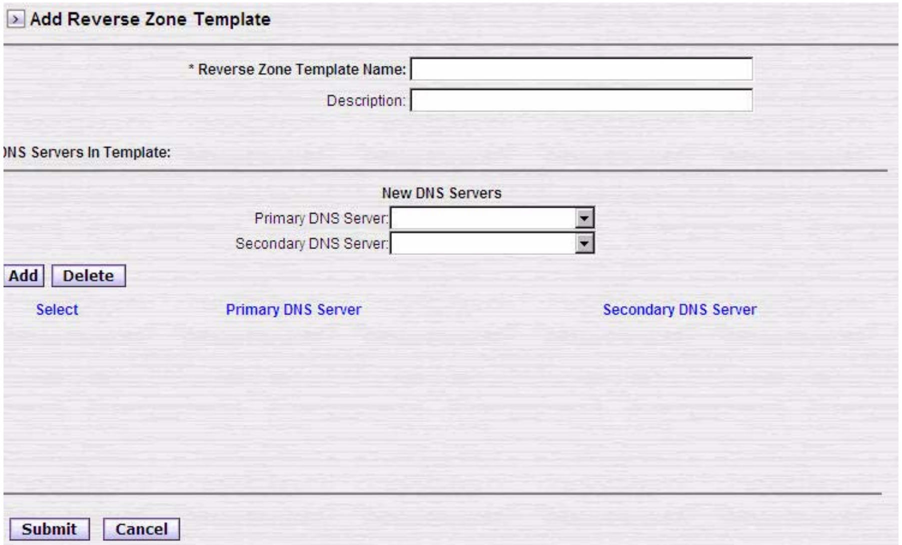
To add reverse zone template, follow these steps.

1. Select **Templates** from the **Infrastructure** menu.

   Result: The Template Hierarchy opens.

2. Mouse over the **Actions** menu and select **Add Reverse Zone Template**.

Result: The Add Reverse Zone Template page opens.



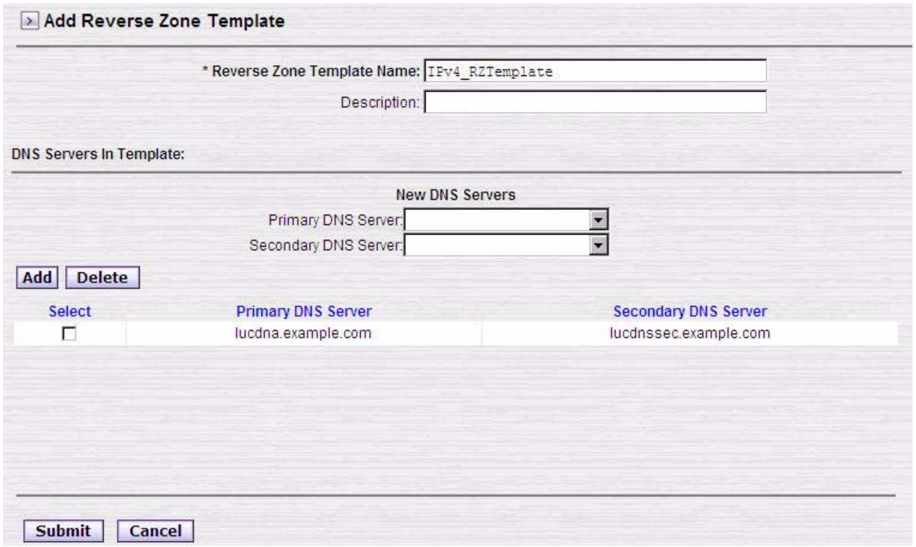
3 Fill in the fields after reviewing the following table.

Table 24-4 Add reverse zone template fields

Field	Description
Template Name	***Required***. Enter the name of the reverse zone template.
Description	***Optional***. You can enter a description for the reverse zone template.
Primary DNS Server	***Required***. Select the primary DNS server to be assigned to the template.
Secondary DNS Server	***Optional***. Select the secondary DNS server to be assigned to the template.

4 Add and delete DNS servers to the template, as follows:

- To add a DNS server to the template, select a primary and/or secondary server and click **Add**. The DNS server appears in the **DNS Servers in Template** list.



- To delete DNS servers from the **DNS Servers in Template** list, select a DNS server by clicking the checkbox next to it and then click **Delete**. The DNS server is removed from the **DNS Servers in Template** list.

5 Repeat Step 3 as needed.

6 Click **Submit** when you are finished.

Result: The Reverse Zone Template Saved dialog box opens.

7 Click **OK** to close the dialog box.

Result: The template you added appears in the Infrastructure Hierarchy.

END OF STEPS

Modify a reverse zone template

Purpose

Use this procedure to modify a reverse zone template.

Procedure

To modify a reverse zone template, follow these steps.

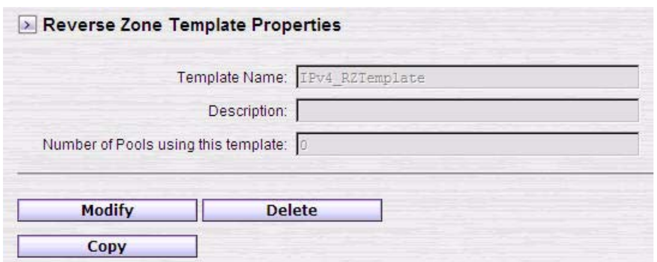
1 Select **Templates** from the **Infrastructure** menu.

Result: The Template Hierarchy opens.

2 Expand the list of reverse zone templates until the one you want to modify is visible.

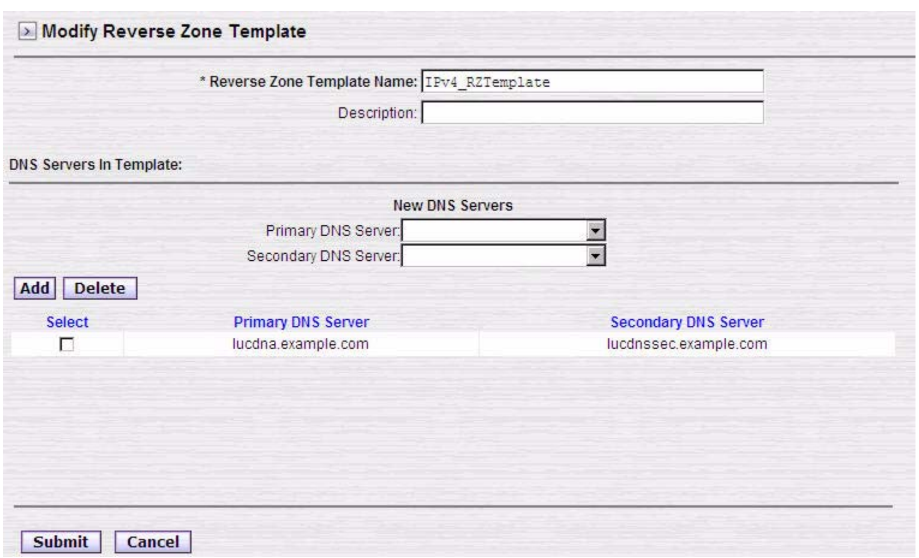
3 Click the reverse zone template you want to modify.

Result: The Reverse Zone Template Properties page opens.



4 Click **Modify**.

Result: The Modify Reverse Zone Template page opens.



5 Make the necessary changes. Refer to Table 24-4, "Add reverse zone template fields" (p. 24-18) for descriptions of the fields.

6 DNS servers can be added and deleted from the reverse zone template:

- To add a DNS server to the template, select a primary and/or secondary server and click **Add**. The DNS server appears in the **DNS Servers in Template** list.
- To delete DNS servers from the **DNS Servers in Template** list, select a DNS server by clicking the checkbox next to it and then click **Delete**. The DNS server is removed from the **DNS Servers in Template** list.

7 Click **Submit** when you are finished.

Result: The Reverse Zone Template Saved dialog box opens.

8 Click **OK** to close the dialog box.

END OF STEPS

Copy a reverse zone template

Purpose

Use this procedure to copy a reverse zone template.

Procedure

To copy a reverse zone template, follow these steps.

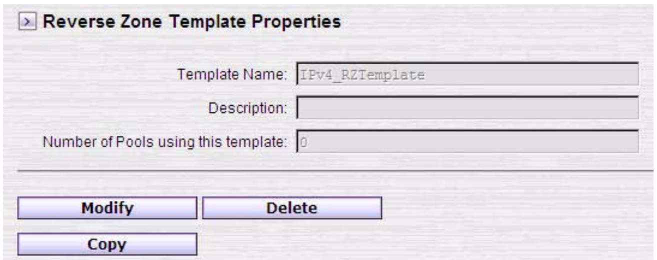
1 Select **Templates** from the **Infrastructure** menu.

Result: The Template Hierarchy opens.

2 Expand the list of reverse zone templates until the one you want to copy is visible.

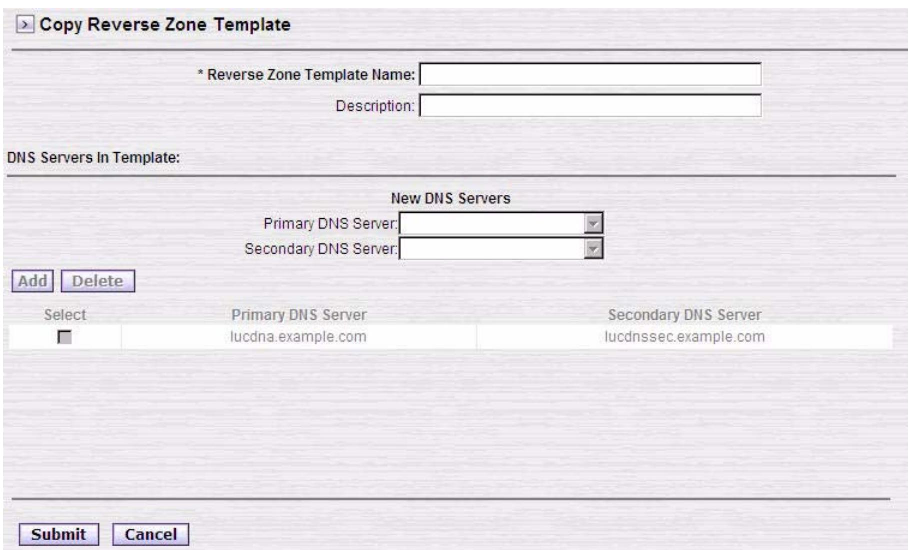
3 Click the reverse zone template you want to modify.

Result: The Reverse Zone Template Properties page opens.



4 Click **Copy**.

Result: The Copy Reverse Zone Template page opens.



5 Make the necessary changes. Refer to the following table for descriptions of the fields.

Table 24-5 Copy Reverse Zone Template Fields

Field	Description
Reverse Zone Template Name	***Required***. Enter the name of the new reverse zone template.
Description	***Optional***. You can enter a description for the reverse zone template.

Field	Description
Primary DNS Server	***Required***. Select the primary DNS server to be assigned to the template.
Secondary DNS Server	***Optional***. Select the secondary DNS server to be assigned to the template.

6 DNS servers can be added and deleted from the reverse zone template:

- To add a DNS server to the template, select a primary and/or secondary server and click **Add**. The DNS server appears in the **DNS Servers in Template** list.
- To delete DNS servers from the **DNS Servers in Template** list, select a DNS server by clicking the checkbox next to it and then click **Delete**. The DNS server is removed from the **DNS Servers in Template** list.

Note: If there is only one DNS server assigned to the reverse zone template, you cannot delete it until you assign an additional DNS server.

7 Click **Submit** when you are finished.

Result: The Reverse Zone Template Copied dialog box opens.

8 Click **OK** to close the dialog box.

END OF STEPS

Delete a reverse zone template

Purpose

Use this procedure to delete a reverse zone template.

Before you begin

A reverse zone template cannot be deleted if is associated with pool.

Procedure

To delete an object template, follow these steps.

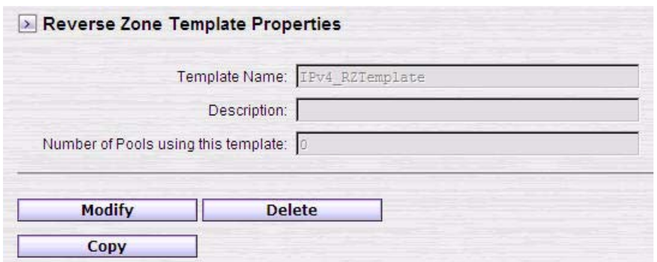
1 Select **Templates** from the **Infrastructure** menu.

Result: The Template Hierarchy opens.

2 Expand the list of reverse zone templates until the one you want to delete is visible.

3 Click the reverse zone template you want to delete.

Result: The Reverse Zone Template Properties page opens.



4 Click **Delete**.

Result: A dialog box opens with the message **You are about to delete reverse zone template <*templatename*>. Are you sure you want to proceed?**

5 Click **OK**.

Result: The reverse zone template is deleted, and a confirmation dialog box opens with the message **Reverse Zone Template Deleted**.

6 Click **OK**.

Result: The reverse zone template that was deleted is removed from the infrastructure hierarchy.

END OF STEPS

Subnet profile templates

Overview

VitalQIP allows users to configure subnet profile templates. A subnet profile template is used to configure a Subnet Profile in VitalQIP when VitalQIP creates a subnet.

How subnet profile templates work

Subnet profile templates are associated with rules. When a rule with a subnet profile template associated with it is used during the allocation process, VitalQIP uses the subnet profile template to configure the Subnet Profile in VitalQIP.

Add a subnet profile template

Purpose

Use this procedure to create a subnet profile template.

Procedure

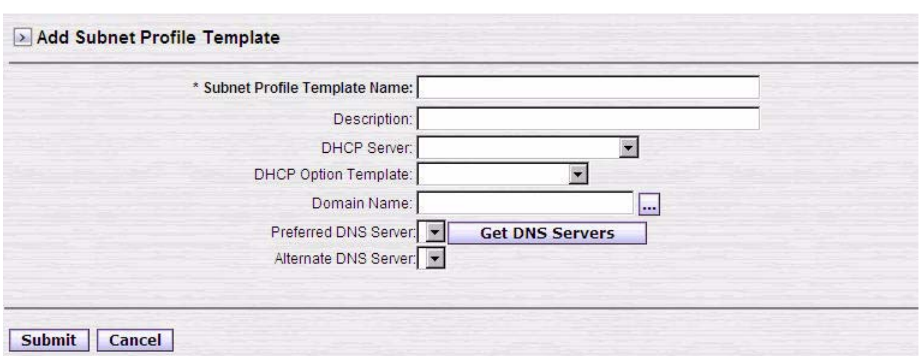
To add a subnet profile template, follow these steps.

1 Select **Templates** from the **Infrastructure** menu.

Result: The Template Hierarchy opens.

2 Mouse over the **Actions** menu and select **Add Subnet Profile Template**.

Result: The Add Subnet Profile Template page opens.



3 Fill in the fields after reviewing the following table.

Note: Note that either the **DHCP Server** or **Domain Name** and **Primary DNS Server** fields must be populated.

Table 24-6 Subnet Profile Template fields

Field	Description
Subnet Profile Name	***Required***. Enter the name of the subnet profile template.
Description	***Optional***. A description can be entered for the template.
DHCP Server	***Optional***. A DHCP server can be assigned to the template.
DHCP Template	***Optional***. A DHCP template can be assigned to the subnet profile template.
Domain Name	***Optional***. A domain can be added to the subnet profile template by searching for a domain. You must specify a domain if you are specifying preferred or alternate DNS servers. Refer to "Search for a domain" (p. 24-9) for additional information about specifying a domain.
Preferred DNS Server	***Optional***. A primary DNS server can be selected. This field and the **Alternate DNS Server** field can be refreshed with a DNS server list for a specific domain. To do so, ensure a domain is entered in the **Domain** field and click **Get DNS Server List**.
Alternate DNS Server	***Optional***. An alternate server can be selected.

4 Click **Submit** when you are finished.

Result: A dialog box opens with the message **Subnet Profile Template Saved**.

5 Click **OK** to close the dialog box.

Result: The subnet profile template appears in the Infrastructure Hierarchy.

END OF STEPS

Modify a subnet profile template

Purpose

Use this procedure to modify a subnet profile template.

Procedure

To modify a subnet profile template, follow these steps.

1 Select **Templates** from the **Infrastructure** menu.

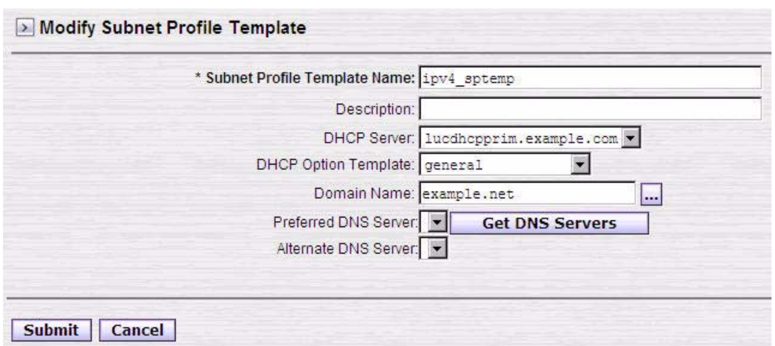
Result: The Template Hierarchy opens.

2 Expand the list of subnet profile templates until the one you want to modify is visible.

Result: The Subnet Profile Template Properties page opens.

3 Click **Modify**.

Result: The Modify Subnet Profile Template page opens.



4 Make any changes to the subnet profile template. Refer to Table 24-6, "Subnet Profile Template fields" (p. 24-26) for information about subnet profile template fields.

5 Click **Submit** when you are done.

Result: A dialog box opens with the message Subnet Profile Template Saved.

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

END OF STEPS

Copy a subnet profile template

Purpose

Use this procedure to copy a subnet profile template.

Procedure

To copy a subnet profile template, follow these steps.

1 Select **Templates** from the **Infrastructure** menu.

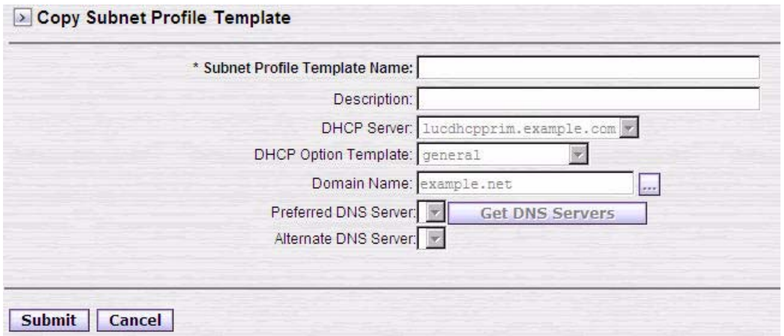
Result: The Template Hierarchy opens.

2 Expand the list of subnet profile templates and click the one you want to copy.

Result: The Subnet Profile Template Properties page opens.

3 Click **Copy**.

Result: The Copy Subnet Profile Template page opens.



4 Make any changes to the subnet profile template. Refer to Table 24-6, "Subnet Profile Template fields" (p. 24-26) for information about subnet profile template fields.

5 Click **Submit** when you are done.

Result: A dialog box opens with the message **Subnet Profile Template Copied**.

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

END OF STEPS

Associate a subnet profile template with a rule

Purpose

You can associate an subnet profile template with any "Used" allocation rule. You can make this association when you create or modify a rule, or when you create or modify an address template.

Procedure

To associate a subnet profile template with a rule, follow these steps.

1 Select **Templates** from the **Infrastructure** menu.

Result: The Template Hierarchy opens.

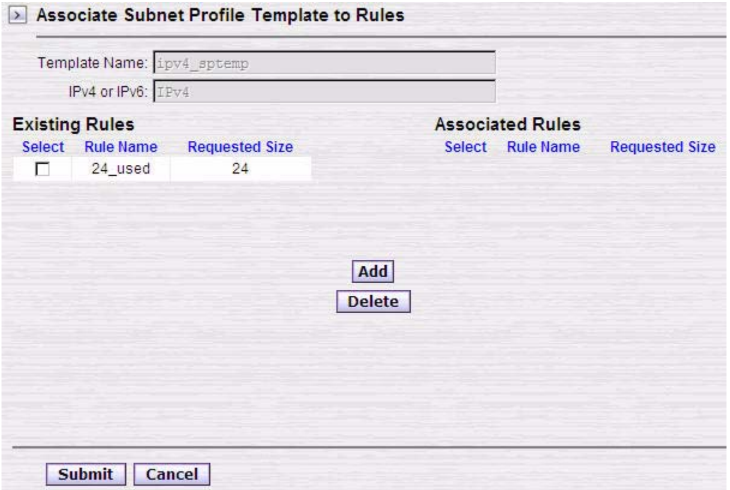
2 Expand the list of subnet profile templates until the one you want to associate with a rule is visible.

3 Click the subnet profile template you want to associate with a rule.

Result: The Subnet Profile Template Properties page opens.

4 Click **Rule Associations**.

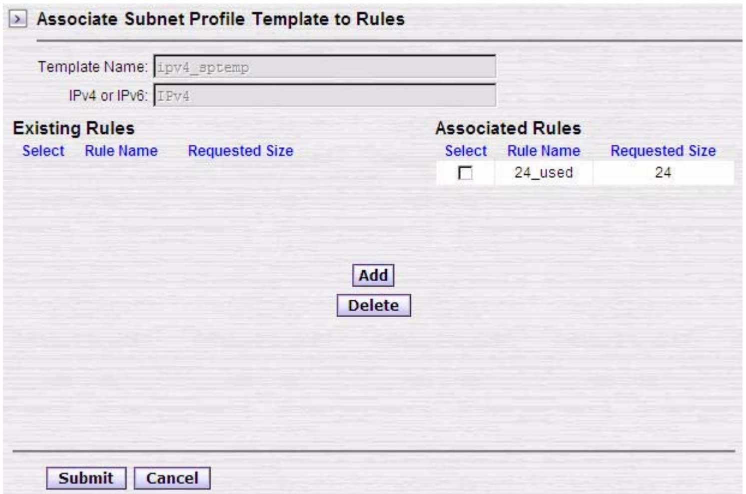
Result: The Associate Subnet Profile Template to Rules page opens.



The **Existing Rules** column lists all "Used" rules that are not associated with a subnet profile template.

5 Select the rule or rules you want to associate with the subnet profile template by clicking the appropriate checkbox.

6 Click **Add**. The rules you selected appear in the **Associated Rules** column.



To disassociate a subnet profile template from a rule, select the checkbox next to the rule name in the **Associated Rules** column, and click **Delete**.

Result: The rule appears in the **Existing Rules** column.

7 Click **Save** when you are done.

Result: The rule associations are saved with the subnet profile template and a confirmation dialog box opens with the message **Successfully modified association of template to rules**.

8 Click **OK** to close the dialog box.

END OF STEPS

Delete a subnet profile template

Purpose

Use this procedure to delete a subnet profile template.

Before you begin

If a subnet profile template is associated with a rule (via the Maintain Rule screen), the template cannot be deleted.

Procedure

To delete a subnet profile template, follow these steps.

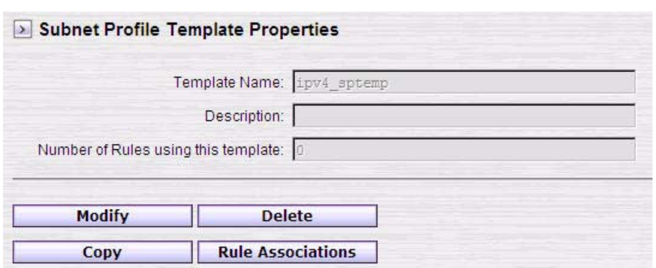
1 Select **Templates** from the **Infrastructure** menu.

Result: The Template Hierarchy opens.

2 Expand the list of subnet profile templates until the one you want to delete is visible.

3 Click the subnet profile template you want to delete.

Result: The Subnet Template Properties page opens.



4 Click **Delete**.

Result: A dialog box opens with the message **You are about to delete subnet profile template *<templatename>*. Are you sure you want to proceed?**

5 Click **OK**.

Result: A confirmation dialog box opens with the message **Subnet Profile Template Deleted**.

6 Click **OK**.

Result: The Subnet Profile Template that was deleted is removed from the infrastructure hierarchy.

END OF STEPS

25 Address allocation rules

Purpose

This chapter describes how to use allocation rules.

Contents

This chapter covers these topics.

Rules

Overview

Purpose

Rules allow you to automate the process of allocating blocks. Rules control how a pool obtains space from its parent and what to do with that space after it has been allocated. If a pool is running out of space, rules also determine how that pool obtains additional space.

Rules that create a block of Used address space allow subnets to be created. Such rules can have an address template associated with them which will define what objects can be created during a block allocation.

Administrator privileges

Only a Master type administrator or a Normal type administrator with Organization access and Access Address Allocation and Maintain Rules privilege set to **True** is allowed to add, modify, or delete a rule.

Site rules

Overview

When you specify a Rule Type of **Site**, then any pool you create using this rule is a unique site. You can optionally specify address templates or subnet profile templates to be used for each range in your site.

When you create a Site rule, VitalQIP finds the specified Parent Pool and creates a new child pool with the Site parameters you specify. Any rule assigned to the site is associated with the new child pool. The rule is processed to retrieve a block of the requested size from the parent pool.

If the block allocation is successful, a network is created in VitalQIP with the same start address and size of the block.

VitalQIP looks at the subnet offsets and sizes you specify for the site. Beginning at the start address of the initial block, an explicit block allocation is performed against the initial block that was allocated for each of the subnet offsets you specify in the site parameters. The explicit block allocation also creates a subnet in VitalQIP corresponding to the block.

If any records in the site also have a subnet profile template or an object template associated with them, these templates are processed when the subnet is created. Blocks and pools are useful tools for managing IP address space. However, by themselves, they do not automate the process of provisioning.

VitalQIP addresses this problem by allowing an administrator to define rules for each pool. Rules govern how a pool obtains space from its parent and what to do with that space once allocated. This capability allows the administrators to automate allocations that are typical for their organization. Unusual allocations can then be managed by exception.

Add a rule

Purpose

Use this procedure to add a rule.

Procedure

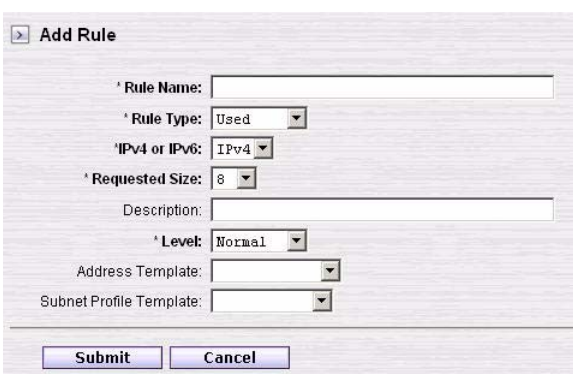
To add a rule, follow these steps.

1 Mouse over the **Address Allocation** tab and click **Rules**.

Result: The Rule Hierarchy opens.

2 Mouse over the **Actions** menu and select **Add Rule**.

Result: The Add Rule page opens.



3 Enter values for the fields, as described in the following table.

Table 25-1 Add Rule fields

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Rule Name</td><td>Required. Enter a unique name of up to 32 alphanumeric characters for the rule.</td></tr>
<tr><td>Rule Type</td><td>Required. This field defines the type of rule. Select one of the following values:

Used – triggers the RIR Reporting mechanism if the seed pool is associated with an Internet registry and the rule size is larger or equal to the minimum IPv4 or IPv6 block size for their respective rules. A Used Rule also allows the user to specify the following:

Which Subnet Templates to use for the subnet to be created
Which Address Templates to use for the IP objects to be created during the allocation process

Reserved – indicates that when a block is allocated using this rule, the block cannot be assigned to a pool until its status is changed.
Free – indicates that when a block is allocated using this rule, the block is available for assignment to a pool.
Site – suballocates the address block further to a specified pool. The subnets corresponding to these sub-blocks are then created in VitalQIP.
</td></tr>
<tr><td>IPv4 or IPv6</td><td>Required. Select the type of address pool to which this rule applies.</td></tr>
<tr><td>Requested Size</td><td>Required. Determines the CIDR size of the block that is requested by this rule. Select from the available values of 8 through 32 for IPv4 or 9 through 128 for IPv6.</td></tr>
<tr><td>Description</td><td>Optional. Text description of the rule’s function.</td></tr>
<tr><td>Level</td><td>Required. Limits what rule is available to an administrator for block allocation. Administrators can only process rules that are at or below their specified level (defined in the Administrator Profile). Select one of the following:

Normal – administrators who have the ability to allocate blocks can process rules.
Advanced – rules can only be processed by Master, Organization, and Normal administrator with a rule level set to Advanced or Expert.
Expert – Master, Organization, and Normal administrators with a rule level set to Expert can process rules.
</td></tr>
</table>

Field	Description
Address Template	***Optional***. The name of an address template to be associated with the rule. Only **Used** rules can have address templates associated with them.
Subnet Profile Template	***Optional***. Select the subnet profile template to be assigned to the rule. Only a **Used** rule can have a subnet profile template assigned to it.
Site Information	The following fields only display if the Rule Type is set to **Site**.
Size	The CIDR size of the sub-block to be created. This field must be no larger than the total address block length.
Status	Select an option from the drop-down list. Allowable values are: • **Used** • **Reserved**
Address Template	The template to be used for creating IP objects in the subnet to be created.
Subnet Profile Template	The template for the creating the subnet profile of the subnet to be created.

4 For site rules only, value the fields for each site rule and click **Add**.

Result: The site rule is added to the site information at the bottom of the page. You can add multiple site rules as necessary. You must enter information for at least one site.

5 Click **Submit**.

Result: The rule is saved. You can see the rule by expanding the rule hierarchy on the left side of the screen. The new rule appears under its address type and its rule type.

END OF STEPS

Modify a rule

Purpose

Use this procedure to modify a rule.

Procedure

To modify a rule, follow these steps.

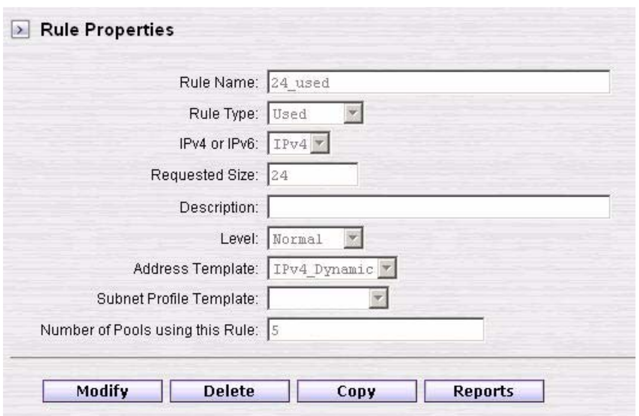
1 Mouse over the **Address Allocation** tab and click **Rules**.

Result: The Rule Hierarchy Hierarchy opens.

2 Expand the hierarchy until you see the rule you want to modify.

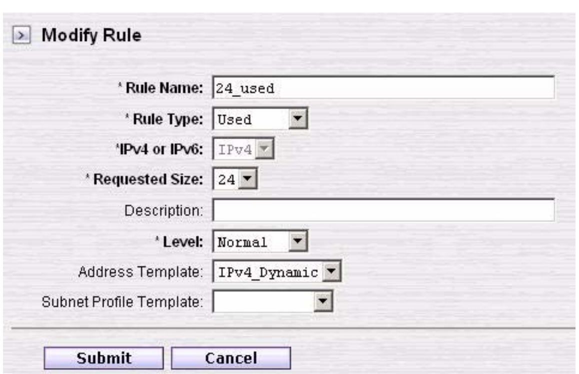
3 Click a rule.

Result: The Rule Properties page opens.



4 Click **Modify**.

Result: The Modify Rule page opens.



5 Make any changes as needed. Refer to Table 25-1, "Add Rule fields" (p. 25-4) for information on the fields and options.

6 Click **Submit**.

Result: The rule is modified.

END OF STEPS

Copy a rule

Purpose

Use this procedure to copy a rule.

Procedure

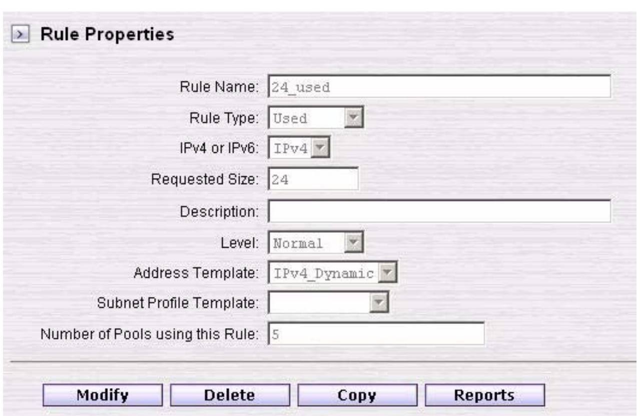
To copy a rule, follow these steps.

1 Mouse over the **Address Allocation** tab and click **Rules**.

Result: The Rule Hierarchy Hierarchy opens.

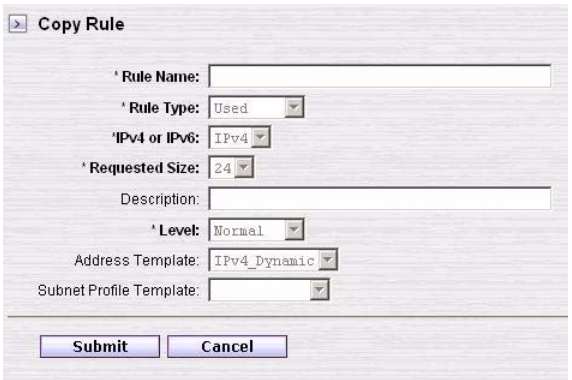
2 Expand the list of rules and click the rule you want to copy.

Result: The Rule Properties page opens.



3 Click **Copy**.

Result: The Copy Rule page opens. All the fields in the screen contain the values from the original rule, except for the **Rule Name** field, which is blank.



4 Enter a ***unique*** rule name in the **Rule Name** field. This is the name of the new rule you are creating. Make any other changes to the values on the screen.

5 Click **Submit**.

Result: A new rule with the name and values you specified is created.

END OF STEPS

Delete a rule

Purpose

Use this procedure to delete a rule.

Before you begin

You can delete any rule that is not currently assigned to a pool. You must assign pools associated with the rule to a different rule first. Run one of the Pool reports to determine which pools are using the rule you want to delete.

Procedure

To delete a rule, follow these steps.

1 Mouse over the **Address Allocation** tab and click **Rules**.

Result: The Rule Hierarchy Hierarchy opens.

2 Expand the list of rules and click the one you want to delete.

Result: The Rule Properties page opens.

3 Click **Delete**.

Result: A dialog box opens with the message **You are about to delete <rulename>. Are you sure want to proceed?**

4 Click **OK**.

Result: The rule is deleted and the a confirmation dialog box opens with the message **Rule Deleted.**

5 Click **OK**.

Result: The rule that was deleted is removed from the infrastructure hierarchy.

END OF STEPS

26 Internet registries

Overview

Purpose

This chapter describes how to use Internet Registries.

Contents

This chapter covers these topics.

Regional Internet Registries

Overview

Purpose

These Regional Internet Registries (RIR) are supported in VitalQIP:

- ARIN
- APNIC
- RIPE
- AFRINIC

Regional Internet Registries require Local Internet Registries such as Internet Service Providers (ISPs) to register all the allocations and assignments of IP addresses that are greater than /29 for IPv4 or /48 for IPv6. Registration is made in the "WhoIs" database of the RIR. VitalQIP sends the required registration format for the various types of address assignments to the RIR using email. The registration is done after the necessary approvals are received from the RIR granting the usage of an address space.

The registration guidelines vary between the RIRs, especially between ARIN and other RIRs, for the IPv4 address assignments. In ARIN, the ISPs are expected to follow the Shared WhoIS Project (SWIP) reporting guidelines that are unlike the other RIRs. There is enough similarity in the reporting guidelines between RIPE and APNIC, especially since the APNIC WhoIs database is based on RIPE v3 database software. For IPv6 addresses, the allocation and assignment policies (**http://www.iana.org/reports/2002/ipv6-allocation-policy-26jun02**) are uniform among all RIRs, but the registration procedures vary.

Add a maintainer

Purpose

When you register a block of addresses, you must specify a maintainer. The maintainer is the person responsible for tracking which addresses in the block are used. You must specify a maintainer when obtaining addresses from an Internet registry. It is a requirement for all Internet registries.

Before you begin

You must define at least one maintainer for each Internet Registry you use. You can specify the same person for multiple registries, or different ones for each.

Procedure

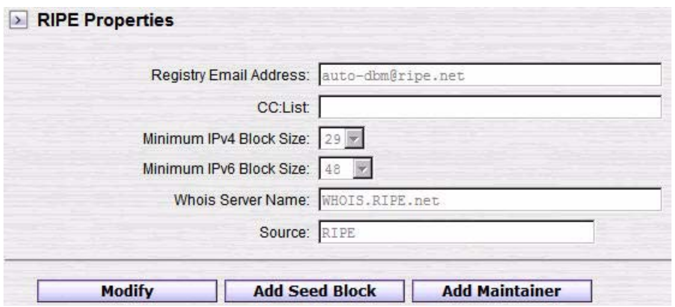
To add a maintainer, follow these steps.

1 Mouse over the **Address Allocation** tab and click **Internet Registries**.

Result: The Internet Registry Hierarchy opens.

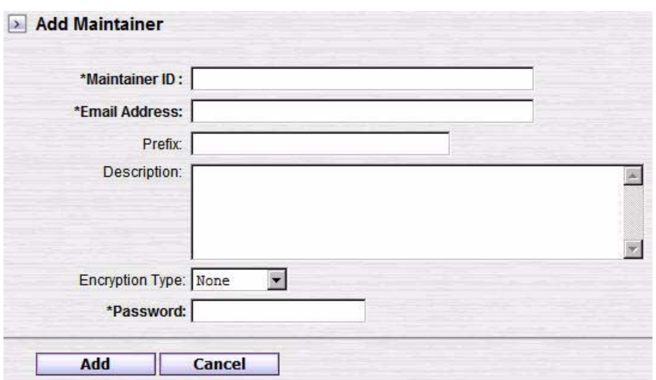
2 Expand the hierarchy and click on the registry to which you want to add a maintainer.

Result: The Internet Registry Properties page opens.



3 Click **Add Maintainer**.

Result: The Add Maintainer page opens.



4 Enter values in the fields on this page, as described in the following table.

Table 26-1 Maintainer fields

Field	Description
Maintainer ID	***Required***. Enter the name or other identifier for the maintainer. Alphanumeric, up to 10-characters.
Email Address	***Required***. Enter the email address of the maintainer (up to 255 characters).
Prefix	***Optional***. Enter the prefix of the network name in the RIR report. Alphanumeric, up to 32 characters. For APNIC and RIPE, the first character must be alphabetic.
Description	***Optional***. Enter a text description for the maintainer, such as job responsibilities, or organizations the person manages. Alphanumeric, up to 256 characters.
Encryption Type	***Required for APNIC and RIPE***. Select one of the following from the drop-down list. • **None** - RIPE only • **Cryptic PW** - Encryption method used at RIPE and APNIC. • **MD5-PW** - Encryption method used at RIPE and APNIC.
Password	***Required for APNIC, RIPE and AFRINIC***.

5 Click **Add** when you are finished.

Result: The maintainer is added to the VitalQIP database and a confirmation dialog box opens with the message **Maintainer saved!**

6 Click **OK** to close the confirmation dialog box.

END OF STEPS

Modify a maintainer

Purpose

Use this procedure to modify a maintainer assigned to an Internet Registry.

Procedure

To modify a maintainer, follow these steps.

1 Mouse over the **Address Allocation** tab and click **Internet Registries**.

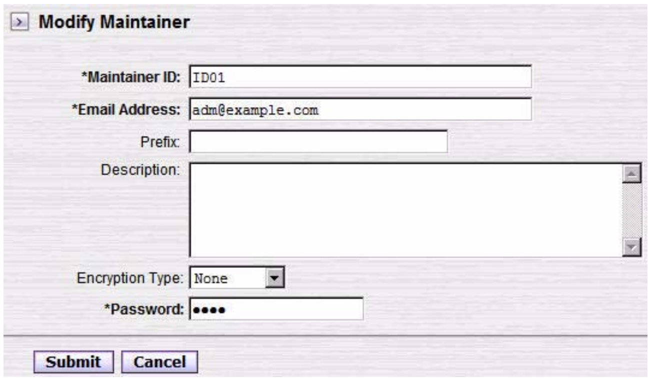
Result: The Internet Registry Hierarchy opens.

2 Expand the hierarchy and then expand the registry where you want to modify a maintainer.

Result: A list of Maintainer IDs displays below the registry.

3 Select the **Maintainer ID** you want to modify and click **Modify**.

Result: The Modify Maintainer page opens.



4 Modify field values as needed. Refer to Table 26-1, “Maintainer fields” (p. 26-4) for field descriptions.

5 Click **Submit** when you are finished.

Result: The maintainer is modified in the VitalQIP database and a confirmation dialog opens with the message **Maintainer saved!**

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

END OF STEPS

Delete a maintainer

Purpose

Use this procedure to delete a maintainer assigned to an Internet Registry.

Note: You cannot delete a maintainer associated with a seed block.

Procedure

To delete a maintainer, follow these steps.

1 Mouse over the **Address Allocation** tab and click **Internet Registries**.

Result: The Internet Registry Hierarchy opens.

2 Expand expand the hierarchy until you reach the the registry from where you want to delete a maintainer.

Result: A list of Maintainer IDs displays below the registry.

3 Click the Maintainer ID you want to delete.

Result: The Maintainer Properties page opens.

4 Click **Delete**.

Result: A dialog box opens with the message **Delete the Maintainer?**

5 Click **OK**.

Result: A confirmation dialog box opens with the message **Maintainer deleted**!

6 Click **OK**.

Result: The dialog box closes and the IP Management splash screen opens.

END OF STEPS

Modify Internet Registry properties

Purpose

Use this procedure to change your site's settings for each Internet Registry.

Before you begin

Do not change the default settings supplied with VitalQIP unless you are doing internal testing.

Procedure

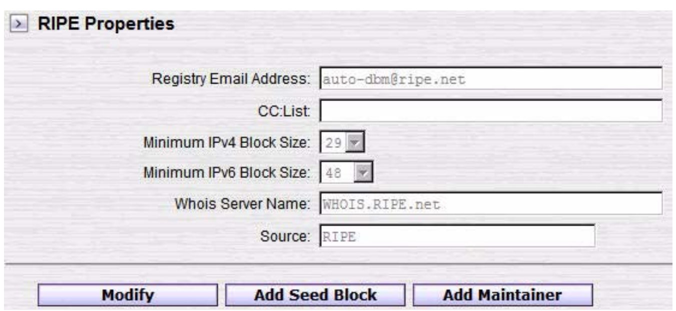
To modify Internet Registry Properties, follow these steps.

1 Mouse over the **Address Allocation** tab and click **Internet Registries**.

Result: The Internet Registry Hierarchy opens.

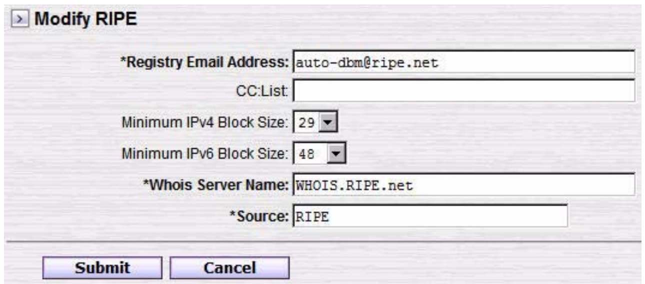
2 Expand the hierarchy and click on the Internet Registry you want to modify.

Result: The Internet Registry Properties page opens.



3 Click **Modify**.

Result: The Modify Internet Registry Properties page opens.



4 Enter values in the fields, as described in the following table.

Table 26-2 Internet Registry properties

Field	Description
Registry Email Address	The email address where reports are sent. The initial default should not be changed except for testing purposes.
CC: List	Additional email addresses where reports are sent.
Minimum IPV4 Block Size	Minimum IPV4 Block Size used for reporting purposes (defaults to /29).
Minimum IPV6 Block Size	Minimum IPV6 Block Size used for reporting purposes (default to /48).
Whois Server Name	The default server name for the Internet registry. This specifies what server to check for “WHOIS” database block information and this field is the FQDN of the Whois Server. The initial default should not be changed except for testing purposes.
Source	Source of data for the Internet Registry. Only displays for RIPE and APNIC.

5 Click **Submit** when you are finished.

Result: The Internet registry is modified in the VitalQIP database.

END OF STEPS

Seed block maintenance

Overview

Each Internet Registry allows you to add, modify and delete seed blocks associated with it. Refer to "Associate seed blocks with a seed pool" (p. 27-9) for information on block maintenance.

27 Pool management

Overview

Purpose

VitalQIP uses pools to manage large areas of address space. This chapter contains information on designing a pool hierarchy, creating, pools, and managing pools. In addition, you can find information on using rules to manage the allocation process.

Contents

This chapter covers these topics.

Pool hierarchy design

Overview

Purpose

The first decision you must make is how to structure your pool hierarchy. Pools should mirror your organizational or administrative structure.

Pool hierarchy guidelines

To structure your pool hierarchy, follow these guidelines:

- Define at least one seed pool to represent the top level within the organizational hierarchy.
- Use mid-level pools that reflect how IP addresses are allocated by the involved organizations. For a large corporation, pools for regional or divisional allocation might be appropriate. For ISPs, pools for large customers or Service Types should be defined.
- Define the lowest level pools that reflect how the actual subnets are deployed. For a large company, a lowest level pool might be appropriate for a department, branch, or small campus. For an ISP, a lowest level pool might be appropriate for a small customer.

Seed pools

Overview

A seed pool is the top (or root) pool in the VitalQIP hierarchy. All address space that you manage with VitalQIP must be manually entered into a seed pool. Because a seed pool has no parent, it does not have a rule associated with it (since rules are designed to tell child pools how to request space from a parent pool).

The addresses within the seed pool can be internal or supplied by a regional Internet registry (such as ARIN, RIPE or APNIC). If the address source is internal, it means that address space added to the seed pool is managed internally by the customer and no reporting to Internet registries occurs. If the address space is supplied by an Internet registry, VitalQIP sends reports to the Internet registry as the address space is allocated or freed.

Administrator privileges

Only an administrator with a Master type administrator or a Normal type administrator with Organization Access and Maintain Seed Pool privilege set to **True** is allowed to add, modify, or delete a seed pool. You can define a seed pool without providing an initial block address in case you are designing your infrastructure while waiting for an address from an Internet registry. You can later enter a seed block with the Add Seed Block function.

Add a seed pool

Purpose

Use this procedure to add a seed pool.

Procedure

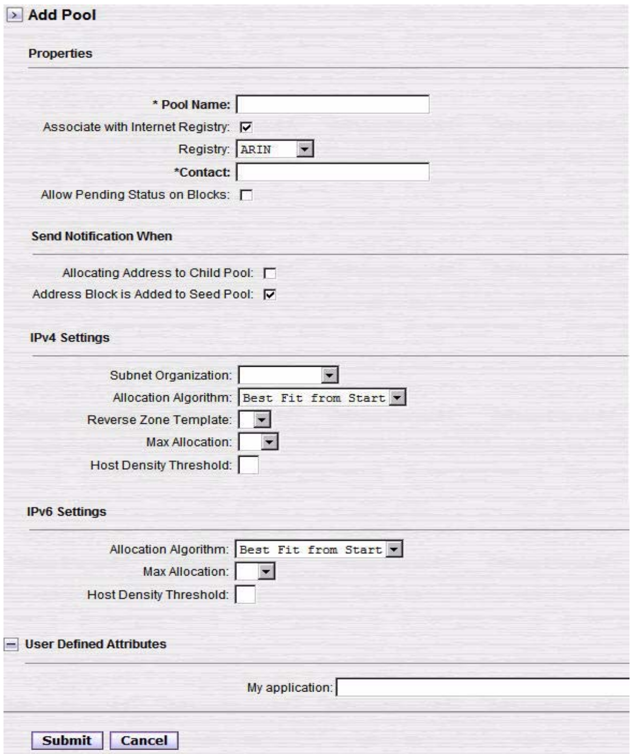
To add a seed pool, follow these steps.

1. Mouse over **Address Allocation** and click **Pool Hierarchy**.

   Result: The Pool Hierarchy opens.

2. Mouse over the **Actions** menu and select **Add Seed Pool**.

Result: The Add Pool page opens.



3 Review the following table and fill in the fields as necessary.

Table 27-1 Add pool fields

Field	Description
Properties	
Pool Name	***Required***. Enter up to 64 alphanumeric characters to define the name of the pool. Seed pool names must be unique across the organization. Child pool names must be unique among its sibling pools.
Associate with Internet Registry	***Optional for seed pools only***. If this box is checked, the Registry field appears immediately below it. This field is not modifiable after the seed pool is created.

Field	Description
Registry	***Optional***. Select the Internet registry from the drop-down list from which this seed pool is obtaining addresses. The list contains the following values: • **ARIN** (default) • **RIPE** • **APNIC** • **AFRINIC** This field is only available if the **Associate with Internet Registry** field is checked. This field is not modifiable after the pool is created.
Contact	***Required***. Enter the email address of the administrator who receives notifications about activity in the seed pool (for example, whenever blocks are allocated). Email messages are sent based on the **Send Notification When** checkboxes described below. Multiple email addresses are permitted, separated from each other by a semicolon (;). **Note:** A default value may be set for this field using the **`poolcontact`** parameter in the *qip.properties* file. Refer to Chapter 3 of the *VitalQIP Administrator Reference Manual* for details on this parameter.
Request Address from Parent Pool	***Optional***. If checked, this pool requests additional addresses from the parent if it cannot meet a request from its child. Not applicable for seed pools.
Allow Pending Status on Blocks	***Optional***. Applicable for seed pools only. Not applicable if the pool is not associated with an Internet registry.
Change Pending Block to Free Status When	This field only displays if **Allow Pending Status on Blocks** is checked. If it is displayed, it is required. Allowable values are: • Free After Days • Free after removal from Whois DB • Free After Days or After Removal from Whois DB • Free After Days and After Removal from Whois DB
Change Pending Block to Free Status After	Required if **Change Pending Block to Free Status When** contains a value that requires you to specify a number of days. Select a value from 1 to 30 from the drop-down list.
Send notification when	

Field	Description
Allocating Address to Child Pool	***Optional***. Check this box if you want the contact person to receive email when this pool allocates an address to a child pool.
Address Block is Added to Seed Pool	***Optional***. Check this box if you want the contact person to receive email when an address block is added to a seed pool.
Requesting Address from Parent Pool	***Optional***. Check this box if you want the contact person to receive email when an address request is made to the parent pool from this pool. Not applicable for seed pools.
IPV4/IPV6 settings	
Subnet Organization	***Optional***. Available for IPv4 pools only. Associates the pool with a subnet organization. You can select an existing subnet organization from the drop-down list, which contains the available subnet organizations in VitalQIP.
Allocation Algorithm	This field cannot be modified after the pool has been created. Select one of the following from the drop-down list: • **Best Fit from Start** - Allocate the smallest block possible using the block closest to the parent block’s starting address. • **Best Fit from End** - Allocate the smallest block possible using block closest to the parent block’s ending address. • **Sparse Allocation** - Allocate the block using left bit manipulation. The requested block size must be larger or equal to the minimum sparse allocation size defined in parent pool. The user cannnot modify this field if the allocation algorithm for this seed pool is sparse allocation.
Sparse Allocation:Minimum Size	***Required if Sparse Allocation is selected for this pool. Optional otherwise***. Minimum Block size, applicable only if the Allocation Algorithm selected is **Sparse Allocation**. For IPv4, select a value from 8 to 32 from the drop-down list. For IPv6, select a value from 8 to 64 from the drop-down list.
Allocation Rule	***Optional for child pools***. Not available for seed pools. Select an Allocation Rule from the drop-down list. Rules are unique to your enterprise. Only IPv4 or IPv6 rules display depending on the address type of this pool.
Reverse Zone Template	***Optional***. Available for IPv4 pools only. Select the template for creating the reverse zone when a Network/Subnet is created (specifies primary and secondary DNS servers). Select the reverse zone template to be assigned to the seed pool.

Field	Description
Max Allocation	***Optional.*** Allocation requests from the child pools cannot exceed this size.
Host Density Threshold	***Optional.*** When the Host Density (HD) ratio reaches this ratio, the user will be notified. HD is calculated as follows: HD = log (number of allocated objects) / log (maximum number of allocatable objects)

4 Click **Submit**.

Result: A dialog box opens with the message **Pool saved**.

5 Click **OK**.

Result: The seed pool appears in the Pool Hierarchy and a dialog box opens with the message **Do you want to add Seed Block to this Pool-*<poolname>*?**

6 Choose one of the following actions.

If you want to...	Then...
Add a seed block to the seed pool	Click **OK**. The Add Seed Block page opens. For information on adding a seed block, refer to “Associate seed blocks with a seed pool” (p. 27-9).
Add a seed block at some other time	Click **Cancel**. The Pool Properties page for the Seed Pool you just added opens.

END OF STEPS

Seed blocks

Overview

After you successfully add a seed pool, VitalQIP prompts you to add a seed block. Seed blocks are the blocks of address space that are manually added to a seed pool. A seed block can only be added to a seed pool. It initially has a status of Free. Seed blocks can be added when a seed pool is created, or by using the **Add Seed Block** function in the Maintain Seed Pool screen.

Some address blocks may already be created in the system as part of the Internet Registry setup. If that is the case, a list displays of "available" address blocks (not associated with an address pool) within the Internet Registry that are not associated with the pool. You can choose one of the available address blocks to add to the pool, or create a new address block. If there are no available address blocks, the Add Seed Block page opens.

Associate seed blocks with a seed pool

Use the following procedure to associate seed blocks that were added in the Internet Registry Properties page without being assigned to a seed pool.

Before you begin

The only differences between a seed block and a regular block are:

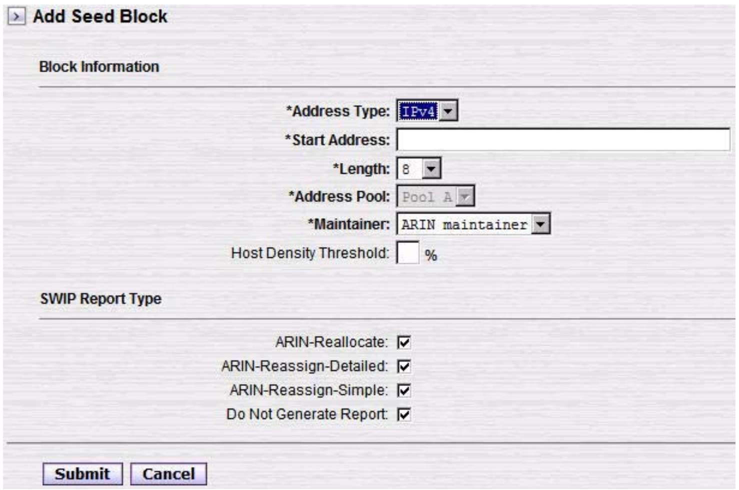
- Seed blocks are manually added to VitalQIP.
- When you delete a Free seed block or delete a seed pool with a Free seed block, the seed block is removed from the database. The regular blocks cannot be added to a pool - they must be allocated using the "allocate block" function.

Procedure

If unassociated seed blocks already exist in the database when you decide to add blocks to a seed pool, the Associate Seed Blocks with Pool page opens. This occurs under the following circumstances:

- After you create a seed pool and click OK in response to the message **Do you want to add Seed Block to this Pool-*<poolname>*?**

- After you click **Add Seed Block** in the Pool Properties page.



To associate an available seed block with a seed pool, follow these steps.

1 Click the **Select** checkbox next to each block you want to add to the seed pool.

2 Click **Associate Selected Blocks to Pool**.

Result: The blocks are added to the seed pool and appear in the Pool Hierarchy.

Note: If you decide that you would rather add a seed block that does not exist to the selected seed pool, click **Add New Block**. The Add Block page opens. Refer to "Add a seed block to a pool" (p. 27-10).

END OF STEPS

Add a seed block to a pool

Purpose

Use this procedure to add a seed block to a seed pool.

Before you begin

The only differences between a seed block and a regular block are:

- Seed blocks are manually added to VitalQIP.

- When you delete a Free seed block or delete a seed pool with a Free seed block, the seed block is removed from the database. The regular blocks cannot be added to a pool - they must be allocated using the "allocate block" function.

Procedure

To add a seed block to a seed pool, follow these steps.

1 Mouse over **Address Allocation** and click **Pool Hierarchy**.

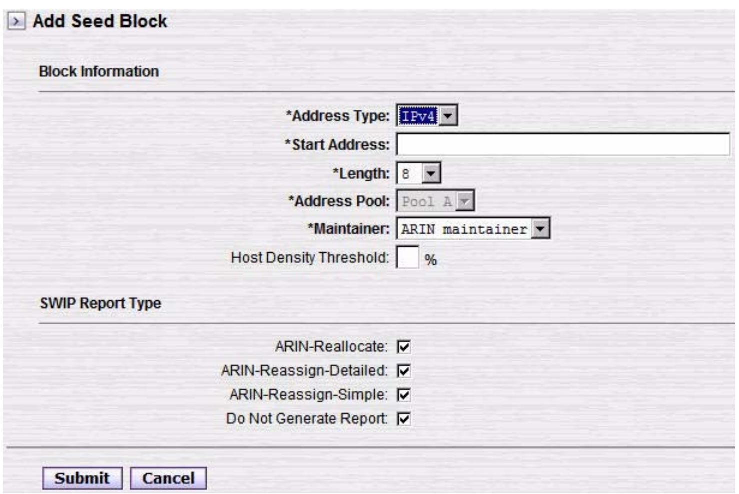
2 The Pool Hierarchy opens.

3 Expand the list of seed pools and select the seed pool to which you want to add a block.

Result: The Pool Properties page opens.

4 Click **Add Seed Block**.

Result: If there are associated seed blocks, the Associate Seed Blocks with Pool page opens. Refer to "Associate seed blocks with a seed pool" (p. 27-9). If there are no unassociated seed blocks, the Add Seed Block page opens.



5 Review Table 28-9, "Block allocation fields" (p. 28-18), and fill in the **Block Information** section fields.

6 Click **Submit**.

Result: A dialog box opens with the message **Seed block added -<*blockname*>**.

7 Click **OK**.

Result: The seed block appears in the Pool Hierarchy.

END OF STEPS

Modify a pool

Purpose

Use this procedure to modify a pool.

Procedure

To modify a pool, follow these steps.

1 Mouse over **Address Allocation** and click **Pool Hierarchy**.

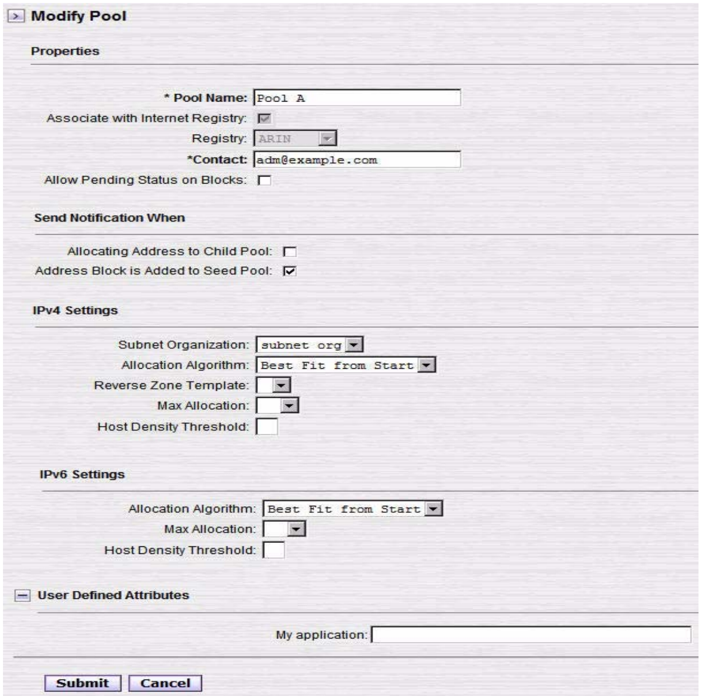
Result: The Pool Hierarchy opens.

2 Expand the list of pools and select the pool you want to modify.

Result: The Pool Properties page opens.

3 Click **Modify Pool**.

Result: The Modify Pool page opens.



Make any changes to the pool's properties. Refer to Table 27-1, "Add pool fields" (p. 27-5) for descriptions of these fields.

> **Note:** Not all fields are modifiable for all types of pools. The user can change the **Allocation Algorithm** from **Best fit from start** to **Best fit from end** and vice versa. However, the user cannot to modify the allocation algorithm if it is set to **Sparse allocation**.

4 Click **Submit**.

END OF STEPS

Delete a pool

Purpose

Use this procedure to delete a pool.

Before you begin

If you delete blocks that were originally reported to ARIN without sending any SWIP reports, remember that later you will have to send SWIP reports manually to ARIN to have the WHOIS database updated.

Procedure

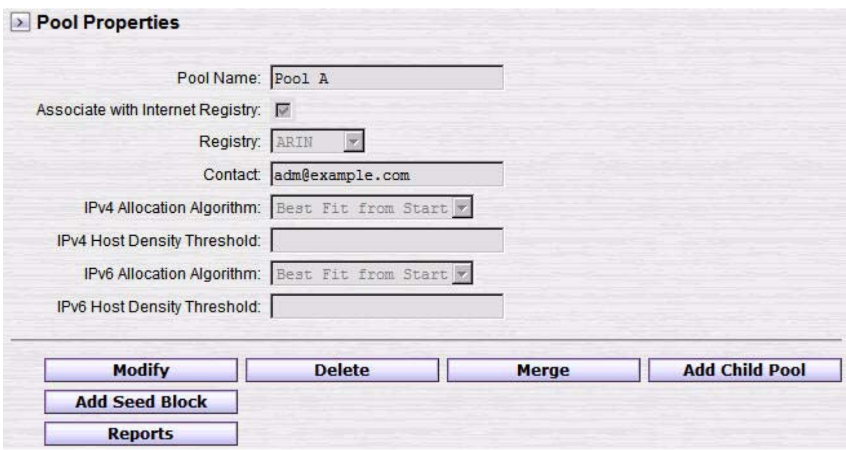
To delete a pool, follow these steps.

1 Mouse over **Address Allocation** and click **Pool Hierarchy**.

Result: The Pool Hierarchy opens.

2 Expand the list of pools and click the one you want to delete.

Result: The Pool Properties page for that pool opens.



3 Click **Delete**.

Result: A dialog box opens with the message **Are you sure you want to delete** ***<poolname>*** **pool?**

4 Click **OK**.

Result: If there are no child pools, the pool is deleted.

Note: Deleting a pool removes the pool and all children of the pool. You can only delete a pool if all blocks under the pool (anywhere in the hierarchy) have a status of Free.

END OF STEPS

Pools

Overview

VitalQIP groups address blocks together into "buckets" known as pools. Pools conform to a tree structure, starting at the root pool, known as the seed pool. Pools are created below the seed pools and can be layered as deep as you need them. Typically, pool hierarchies are from three to six layers. Address blocks are added to pools either by performing a block allocation (or explicit allocation) against the pool or by performing an allocation against a pool below the pool in the pool hierarchy.

Administrator privileges

A Master administrator can perform any operation for pools and blocks. A Normal administrator with Organization Access and Access Address Allocation privilege set to True, can do various operations as shown in the following table:

Table 27-2 Administrator privileges for pools

If value is True	Then the administrator has this capability
Maintain Address Template	Add/modify/delete address template.

<table>
<tr><th>If value is True</th><th>Then the administrator has this capability</th></tr>
<tr><td>Maintain Blocks</td><td>Allocate a block, explicit allocation and all block management actions.
If Maintain Blocks is set to True, the following sub-privileges can be set for each administrator:
• Allocate Block (default is true)
  • Run Level - Normal (default) Allocate blocks using Normal level of rules
  • Run Level - Advanced Allocate blocks using both Advanced and Normal level of rules
  • Run Level - Expert Allocate blocks using all level of rules
• Expand Blocks (default is true)
• Explicitly Create Blocks (default is true)
• Free Blocks (default is true)
• Move Blocks (default is true)
• Renumber Blocks (default is true)
• Split/Merge Block (default is true)</td></tr>
<tr><td>Maintain Pools</td><td>Add/modify/delete child pools.</td></tr>
<tr><td>Maintain Reverse Zone Template</td><td>Add/modify/delete/copy reverse zone templates.</td></tr>
<tr><td>Maintain Rules</td><td>Add/modify/delete/copy rules.</td></tr>
<tr><td>Maintain Seed Pool</td><td>Add/modify/delete seed pools and seed blocks.</td></tr>
<tr><td>Maintain Subnet Profile Template</td><td>Add/modify/delete/copy subnet profile templates.</td></tr>
<tr><td>Rule Override</td><td>Use different rule (other than the one assigned in the child pool) to allocate a block.</td></tr>
<tr><td>Write new infrastructure to managed list</td><td>Create new infrastructure including networks and subnets. Only for IPv4 blocks.</td></tr>
</table>

Add a child pool

Purpose

Use this procedure to add a child pool.

Procedure

To add a child pool to a seed pool, use the following steps:

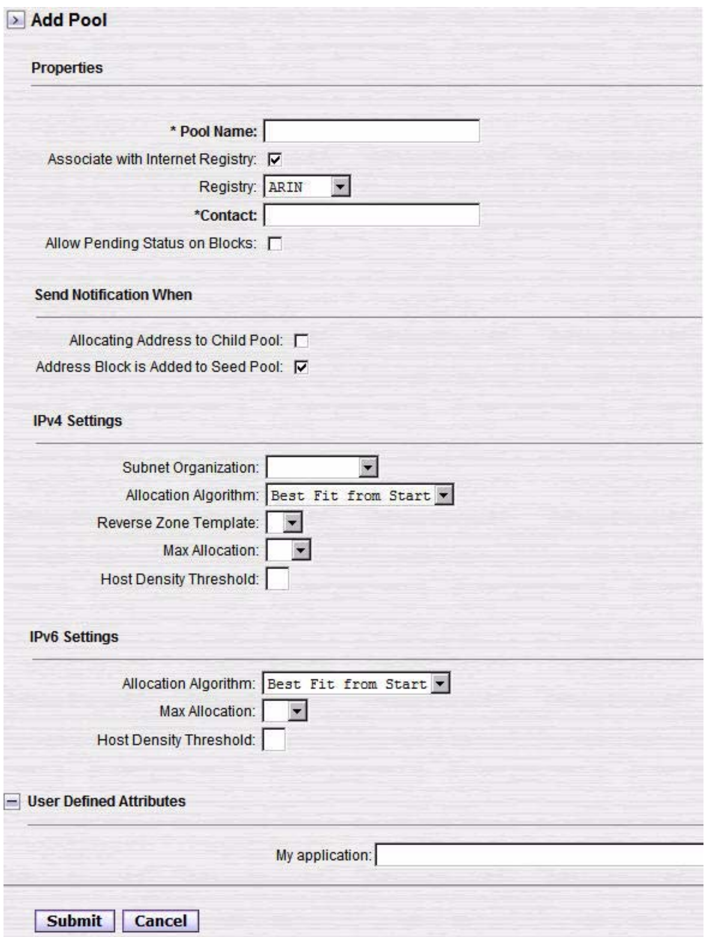
1 Mouse over **Address Allocation** and click **Pool Hierarchy**.

Result: The Pool Hierarchy opens.

2 Select the seed pool to which you are adding the child pool.

3 Click **Add Child Pool**.

Result: The Add Pool page opens.



4 Refer to Table 27-1, "Add pool fields" (p. 27-5)as you fill in the values of the fields.

5 Click **Submit** to save your changes.

END OF STEPS

Quickly allocate a child pool

Purpose

This procedure allows you quickly allocate an address block and optionally add a child pool.

Procedure

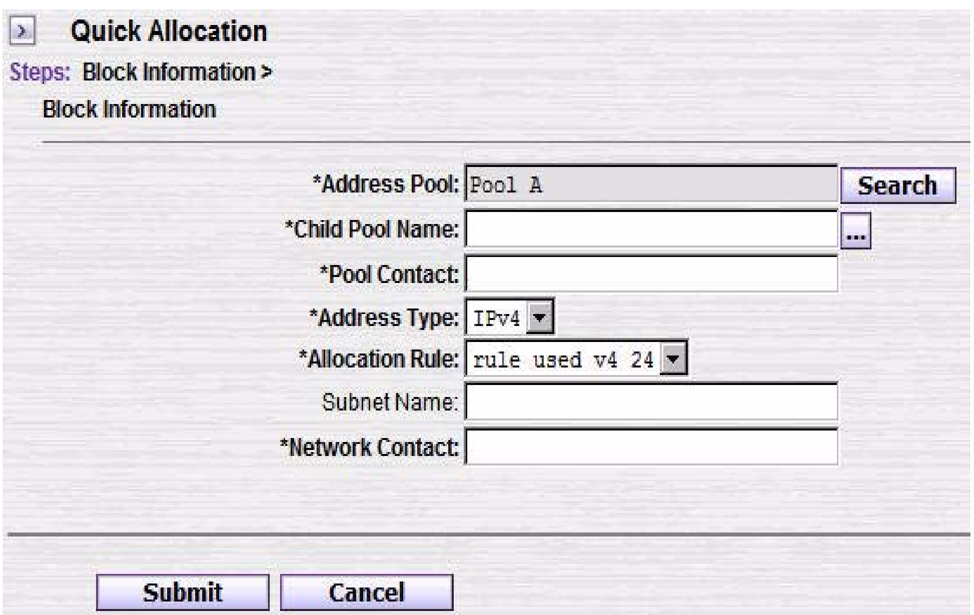
To quickly allocate blocks, use the following steps:

1 Mouse over **Address Allocation** and click **Pool Hierarchy**.

Result: The Pool Hierarchy opens.

2 From the **Actions** menu, select **Quick Allocation**.

Result: The Quick Allocation page opens:



3 Review the following table and fill in the Quick Allocate fields:

Note: Not all fields display on this screen depending on the type of block you are allocating.

Table 27-3 Quick allocate fields

Field	Description
Address Pool	***Required.*** Contains the name of the address pool to which this block is being allocated. • If a pool's properties page is displayed when you select **Quick Allocation**, this field is valued with the pool name and is not modifiable. • If no pool's property page is displayed you select **Quick Allocation**, this field is blank. You must click the **Search** button to search for and select a pool.
Child Pool Name	***Required***. Select an existing child pool under this parent by clicking the **...** button, or type in a pool name. If the pool does not exist, it will be created.
Pool Contact	***Required***. If you use the search feature to select an existing child pool, this field is automatically populated with the pool contact and is not displayed. If you enter a new pool name, you must enter a valid pool contact in this field. **Note:** A default value may be set for this field using the **`poolcontact`** parameter in the *qip.properties* file. Refer to Chapter 3 of the *VitalQIP Administrator Reference Manual* for details on this parameter.
Address Type	***Required***. Select a value from the drop-down list. Allowable values are as follows: • **IPv4** (default) • **IPv6**
Allocation Rule	***Required***. Select an allocation rule from the drop-down list.
Subnet Name	***Optional***. If the allocation rule is ***Used***, this field displays. It allows you to assign a name to the subnet in VitalQIP.
Network Contact	***Required for IPv4 addresses only***. If the allocation rule is ***Used***, this field displays. You must enter a valid network contact

Field	Description
Use Default Address Template	***Optional*** if the allocation rule is ***Used*** and the rule has been associated with an address template, this checkbox displays. If this box is checked, (default), the address template creates infrastructure using the default addresses and names. If the box is unchecked, you are prompted to view and optionally edit the infrastructure to be created.

4 Click **Submit**.

Result: Results vary depending on the options you have selected.

- If you have allocated a block with a Used status an address template, and you unchecked the **Use Default Address Template** checkbox, you are prompted to confirm the block's infrastructure. Refer to "Address allocation templates" (p. 24-1) for information about setting up a block's infrastructure.
- If you have allocated a block using any other combination values, you see a dialog box telling you the allocation was successful the number of objects created, if you used a rule, and what the associated address template is.

END OF STEPS

Allocate a block to a child pool using its allocation rule

Purpose

Each child pool has an allocation rule associated with it when it is created. This rule determines the default settings for the size of each block allocated to it as well as other attributes. Use this procedure to allocate a block to a child pool using its allocation rule.

Procedure

To allocate a block to a child pool using its default allocation rule, follow these steps.

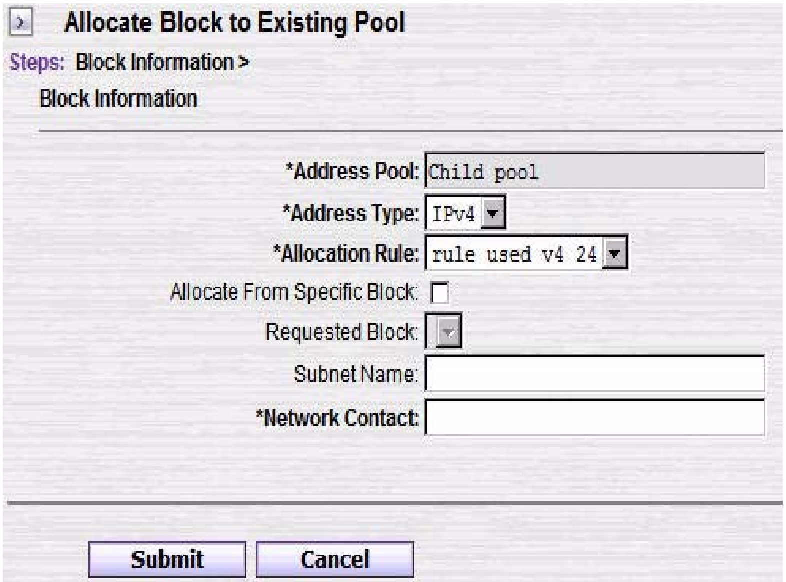
1 Mouse over **Address Allocation** and click **Pool Hierarchy**.

Result: The Pool Hierarchy opens.

2 Select the child pool to which you want to allocate a block.

3 Click **Allocate a Block**.

Result: The Allocate Block to Existing Pool page opens.



4 Review the following table and fill in the Allocate Block to Existing Pool fields:

Table 27-4 Allocate block to existing pool fields

Field	Description
Address Pool	***Read only.*** Contains the name of the address pool to which this block is being allocated.
Address Type	***Read only.*** Contains the type of IP addresses in this block. Allowable values are either IPv4 or IPv6.
Allocate from Specific Block	***Optional.*** Check this option if to allocate space from a specific block. If this option is selected, select a block from the **Requested Block** field.
Requested Block	***Required if Allocate from Specific Block is checked.*** Select the block from which space is allocated.
Allocation Rule	***Required.*** Select the allocation rule you want to use for this block. The default allocation rule initially appears selected in the drop-down list.
Subnet Name	***Optional.*** Enter the name of the subnet to which you are allocating this block.

Field	Description
Network Contact	***Required for IPv4 blocks. Unavailable for IPv6 blocks.*** Enter the network contact's email address for the block you are allocating.
Use Default Address Template	If you check this box, this block uses the default address template associated with the pool. Otherwise, no addresses are created.

5 Click **Submit**.

Result: The block is allocated.

The allocated block has properties based on the type of rule you used. For all blocks, the block size is the same size specified in the allocation rule.

Used rule

- The block status is Used.
- RIR reporting GUI displays if allocation size is larger than or equal to the minimum block size (IPv4 or IPv6) defined in Internet Registry properties.

Free rule

- Block status is Free.

Reserved rule

- Block status is Reserved

Site rule

- Main block size is the same size specified in the allocation rule
- Main block status is Origin
- Sub-blocks' size and status (Used or Reserved) are the same as defined in the site information of the site rule.

END OF STEPS

Allocate a block explicitly

Purpose

Use explicit block allocation when you want to allocate a block of a specific size with a specific start address. When you allocate a block explicitly, you do not specify an allocation rule.

- You can optionally allocate a block explicitly to a child pool. Child pools always have an allocation rule associated with them, but explicit allocation allows you to specify a start address or size that differs from the rule.
- For IPv4 blocks, you have the option to enter other attributes such as subnet creation option, subnet name, address template, and subnet profile template.

Procedure

Follow these steps to explicitly allocate a block:

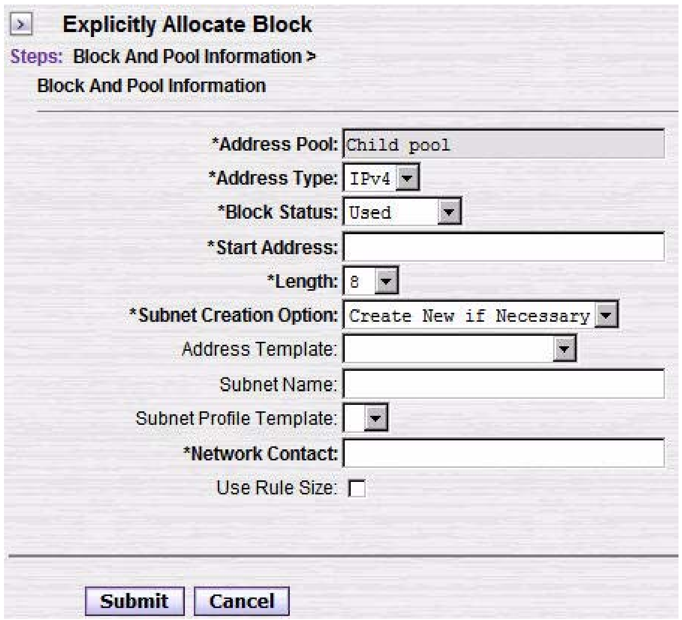
1 Mouse over **Address Allocation** and click **Pool Hierarchy**.

Result: The Pool Hierarchy opens.

2 Select the child pool to which you want to allocate a block.

3 Click **Explicit Allocation**.

Result: The Explicitly Allocate Block page opens.



4 Review the following table and enter values in the fields as appropriate.

Table 27-5 Explicitly allocate block fields

Field	Description
Address Pool	***Read only.*** Contains the name of the address pool to which this block is being allocated.
Address Type	***Read only.*** Contains the type of IP addresses in this block. Allowable values are either IPv4 or IPv6.
Block Status	***Required.*** Status of the Blocks. Allowable values are: • **Allocated** • **Used** • **Free** • **Reserved** • **Site**
Start Address	***Required.*** Enter a valid IP address in either IPv4 or IPv6 format as specified in the Address Type field.
Length	***Required.*** Select a length from the drop-down list. For IPv4, select a value from 8 to 32. For IPv6, select a value from 9 to 128.

Field	Description
Subnet Creation Option	***Required only if the Block status is Used.*** This option determines how the block is associated with the existing/new subnet in VitalQIP. Select a value from the drop-down list. Allowable values are: • **Create New** – Attempt to create a subnet at the address and size of the block. If the subnet already exists, the process fails. If the subnet is created, all post allocation processing will be performed. • **Link to existing** – Requires that a subnet exist in VitalQIP at the address and size of the allocated block. If such a subnet does not exist, the process fails. If the subnet is found, the block is associated with this subnet. Since the subnet already exists, VitalQIP does not perform other post allocation processing on the subnet (for example, the Address Template is not processed, the domain is ignored, and so on). • **Create New if necessary** – Check if a VitalQIP subnet exists, and if it does, links the block with the subnet. If the subnet does not exist, VitalQIP creates it and performs all post allocation processing. • **Do not Create or Link** – Subnets are not created or linked to in the Address Management module. VitalQIP attempts the creation of individual objects or IP Addresses in Address Management in either of these cases.
Address Template	***Optional.*** Select an address template from the drop-down list. Valid for Used status only.
Subnet Name	***Optional.*** If you are creating a new subnet, you can enter the name in this field.
Subnet Profile Template	***Optional.*** Select a subnet profile template from the drop-down list. Valid for Used status only.
Network Contact	***Required only for IPv4 Used blocks.*** Enter the e-mail address of the network administrator responsible for this block.
Use Rule Size	***Optional.*** If this field is selected, then the default rule size for the pool is used when the Pools make address requests to their parent pools.

5 Click **Submit**.

Result: The block is allocated.

END OF STEPS

Search for a pool or a block

Purpose

Use this procedure to search for a specific pool or block.

Before you begin

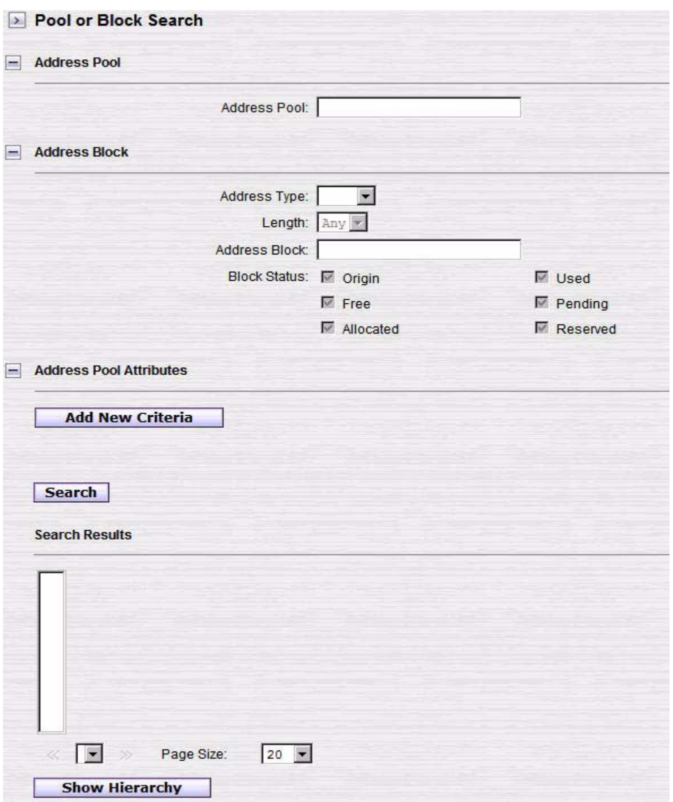
Always try to limit the search criteria whenever possible. Searching for all pools in a large database could take a long time to return results.

Procedure

To find the location of a specific pool, follow these steps.

1 From either the Pool Hierarchy or the Block Hierarchy, mouse over the **Actions** menu and select **Search**. You can search pools only, or you can search both pools and blocks.

Result: The Search Criteria page opens.



2 Enter search criteria as needed. The Search fields are described in the following table.

Table 27-6 Search fields

Field	Description
Address Pool	***Required***. Enter the name of the pool for which you are searching. This field is case-sensitive. You can enter a partial name by using the asterisk (*) as a wildcard, or you can search all pools by entering only an asterisk.
Address Type	***Optional***. You can select IPv4 or IPv6 from the drop-down list. If you do not select either, then all address types are shown.
Length	***Optional***. Select a length from the drop-down list. For IPv4, allowable values are 8 to 32. For IPv6, allowable values are 9 to 128.
Address Block	***Optional***. Enter the IP address of the address block for which you are searching. You can enter a partial address by using the asterisk (*) as a wildcard.
Block Status	***Optional***. Click a checkbox to limit your search to only blocks with that status. If no block statuses are checked, the search looks for all blocks.
Address pool attributes	
Number of Attributes	***Optional***. Select the number of address pool attributes to include in the search. If you select 0, then the following two fields do not display.
Attribute Group	***Required if visible***. If specified, the search is limited to this pool attribute group. You can specify any attribute groups currently associated with the Pool or one of two pre-defined entries: • **<NONE>** – Select this entry to exclude Pool Attribute Group from this search criteria row. • **<IGNORE>** – Select this entry if, for this search criteria row, you do not care if a UDA is in a group or not. • **<ANY>** – Select this entry to include all Pool Attribute Group(s) in this search criteria row.
Attribute Name	***Required if visible***. If specified, the search is limited to this pool attribute value. Values in this column are based on the value in the **Attribute Group** column. The available values are: • All Attributes that do not attach to any Attribute Group, plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<NONE>**. • All Attributes of Pool, plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<IGNORE>**. • All Attributes attached to the specified Attribute Group, plus the pre-defined entry **<ALL>** – if an Attribute Group is selected. • All Attributes attached to at least one Attribute Group, plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<ANY>**.

Field	Description
Attribute Value	Full or partial name (with wildcard) of the attribute. To search for an attribute with a null value, enter two double quotes (“ ”).
Address block attributes	
Number of Attributes	***Optional***. Select the number of address block attributes to include in the search. If you select 0, the following two fields do not display.
Attribute Group	***Required if visible***. If specified, the search is limited to this block attribute group. You can specify any attribute group(s) currently associated with the block or one of two pre-defined entries: • **<NONE>** – Select this entry to exclude Block Attribute Group from this search criteria row. • **<IGNORE>** – Select this entry if, for this search criteria row, you do not care if a UDA is in a group or not. • **<ANY>** – Select this entry to include all Block Attribute Group(s) in this search criteria row.
Attribute Name	***Required if visible***. If specified, the search is limited to this block attribute value. Values in this column are based on the value in the **Attribute Group** column. The available values are: • All Attributes that do not attach to any Attribute Group, plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<NONE>**. • All Attributes of Block, plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<IGNORE>**. • All Attributes attached to the specified Attribute Group, plus the pre-defined entry **<ALL>** – if an Attribute Group is selected. • All Attributes attached to at least one Attribute Group, plus the pre-defined entry **<ALL>**.
Attribute Value	Full or partial name (with wildcard) of the attribute. To search for an attribute with a null value, enter two double quotes (“ ”).

3 Click **Search**.

Result: The results appear in the **Search Results** list.

4 Click the pool or block whose hierarchy you want to view, then click **Show Hierarchy**.

Note: If there are multiple pages of matching objects, use the arrows or the drop-down list to select another page of search results.

Result: The object's hierarchy appears.

END OF STEPS

Merge pools

Overview

You can use the Merge Pools function to merge two pools together, as long as they are at the same level in the pool hierarchy and have the same parent. The function moves all the blocks contained in the selected source pool and places them in the destination pool. All child pools of the source pool become children of the destination pool. The source pool is then removed.

When two pools are merged, Attribute values in the source pool (which is eventually removed) are not used in the operation, and Attribute values in the target pool remain.

Merge pools

Purpose

Use this procedure to merge a pool with another pool in the Pool Hierarchy.

Before you begin

- Only a Master type administrator or a Normal type administrator with Organization Access and Maintain Pools privilege set to **True** (for merging child pools) or Maintain Seed Pool privilege set to **True** (for merging seed pools) is allowed to merge pools.
- When merging pools, both the source and target pools must belong to the same Internet registry.

Procedure

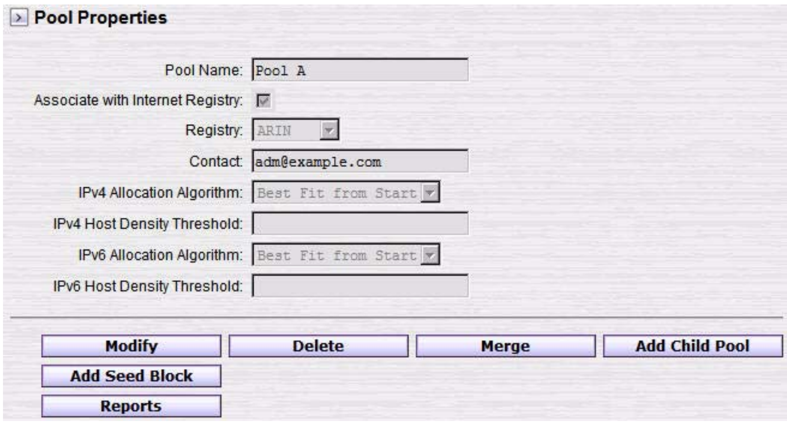
To merge pools, follow these steps.

1 Mouse over **Address Allocation** and click **Pool Hierarchy**.

Result: The Pool Hierarchy opens.

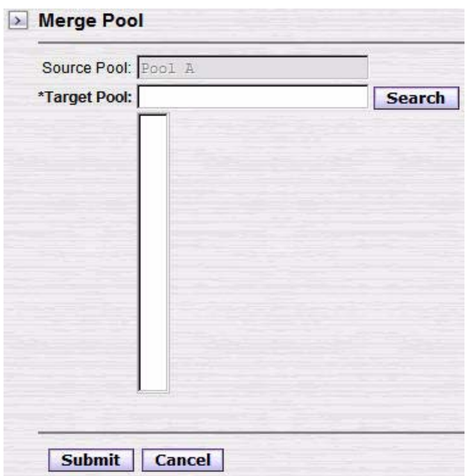
2 Expand the list of pools and select the pool you want to be the source pool.

Result: The Pool Properties page for that pool opens.



3 Click **Merge Pool**.

Result: The Merge Pool page opens.

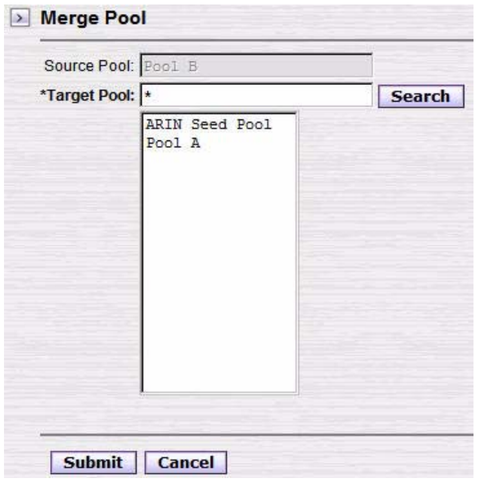


.

4 Enter the name of the target pool you want to merge with the source pool. If you want to see a list of all available pools, enter an asterisk.

5 Click **Search** to see a list of available pools.

Result: A list of available pools is shown.



6 Click the name of the pool you want to combine with the source pool, and click **Submit**.

Result: The pools are merged.

END OF STEPS

Subnet organizations

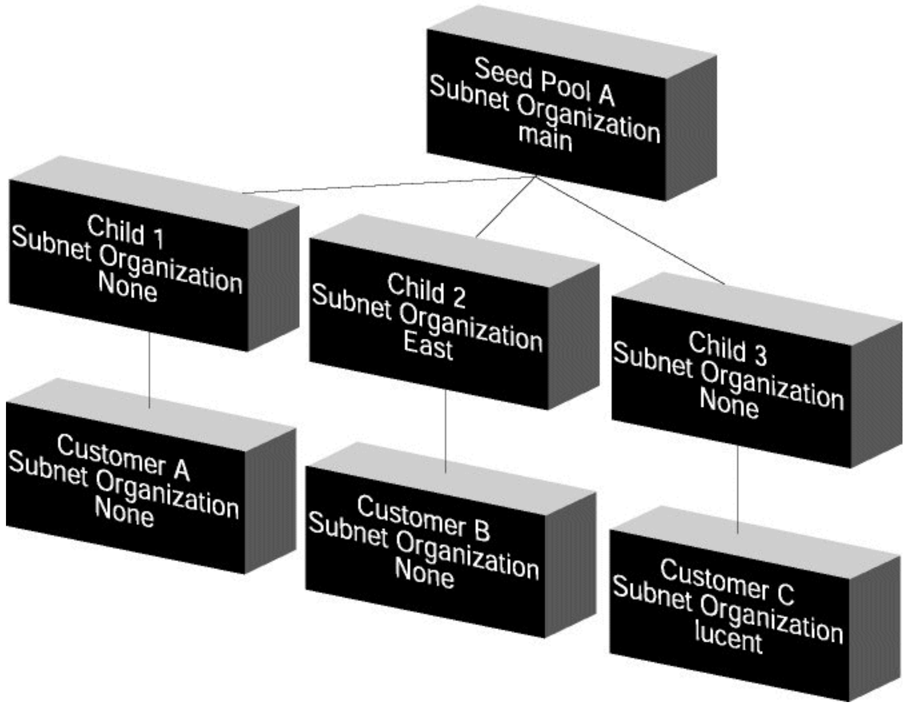
Overview

You can use the pool hierarchy to create a subnet in VitalQIP. At the time the subnet is created, VitalQIP can also be configured to put the subnet into a subnet organization. You can assign any pool to a subnet organization, but typically, you would assign a pool to a subnet organization somewhere higher up the pool hierarchy above the pool where the block is being allocated.

Note: Refer to "Subnet organization management" (p. 9-73) for information on subnet organization management.

To demonstrate, assume the pool hierarchy shown:

Figure 27-1 Subnet organizations in pool hierarchy



In this example, assume the pools Customer A, Customer B, and Customer C are all associated with Contiguous Used rules and associate all blocks assigned to them with VitalQIP subnets.

When a block is allocated to Customer A, the subnet created will be placed into the "main" subnet organization. This can be determined by following the pool hierarchy upward until a subnet organization is found. Since Customer A does not have a subnet organization associated with it, VitalQIP looks at its parent pool, which is Child 1. Child 1 does not have a subnet organization associated with it, so the process continues up to Seed Pool A. Seed Pool A has the "main" subnet organization associated with it, so this is where the subnet for Customer A is placed.

Using a similar process, Customer B would assign subnets to the "East" subnet organization (associated with Child 2). Customer C assigns subnets to the "lucent" subnet organization since it is associated with that organization. No parent flow is necessary.

A subnet does not have to be placed in a subnet organization. If there is no pool higher up in the hierarchy associated with a subnet organization, the subnet will still be created but will not be placed into a subnet organization. For example, if the "main" subnet organization were removed from the Seed Pool A profile, blocks assigned to Customer A would not be placed into a subnet organization.

Note: Subnets cannot belong to more than one subnet organization.

END OF STEPS

28 Block allocation

Overview

Purpose

This chapter discusses the way VitalQIP uses blocks and how blocks are allocated. It also discusses block maintenance and an automated process to allocate blocks.

You can access block maintenance from either the block hierarchy or the pool hierarchy in the VitalQIP Web GUI.

Contents

This chapter covers these topics.

The block allocation process

Overview

Purpose

Block allocation is the process of assigning an additional block to a pool. VitalQIP assigns the address space based on the configuration of rules and pools in the hierarchy.

Administrator privileges

Only an administrator with a VitalQIP **Rule Override** privilege set to **True** is allowed to select a rule other than the rule associated with the existing pool. If your VitalQIP **Rule Override** privilege is set to **False**, the **Rule Name** field in the Allocate Block to Existing Pool page is set to Read Only.

Block allocation and child pools

A block can be allocated to a child pool via an allocation rule. The allocation rule associated with the child pool determines the default settings for the size of each block allocated to it as well as other attributes. Refer to "Allocate a block to a child pool using its allocation rule" (p. 27-20) for instructions for how to allocate a block to a child pool.

SWIP reporting

Introduction

VitalQIP contains optional support for registering address space with ARIN. The configuration parameters for ARIN are available at the seed pool level. Each seed pool can be configured differently (one seed pool might use ARIN and another may not).

Enable ARIN support

ARIN support is turned on by selecting **ARIN** as the **Registry Name** in the Add Seed Pool page. Refer to "Associate seed blocks with a seed pool" (p. 27-9) for information on the fields that support ARIN.

What is ARIN

ARIN maintains a database (WHOIS) of all registered IP address blocks and information about who is using this address space. When an ISP allocates address space to another company, it registers this allocation by sending a SWIP report to ARIN.

VitalQIP support of ARIN

If a seed pool is configured with ARIN support turned on, any block allocation that creates a VitalQIP subnet anywhere below the seed pool in the hierarchy will generate a SWIP report. Based on the SWIP report type that the administrator chooses, VitalQIP prompts for various pieces of information needed in the SWIP report. This information will be formatted into the selected SWIP template and mailed to the **ARIN Email** address specified on the seed pool.

> **Note:** VitalQIP does not generate SWIP reports for block allocations that are smaller than a /29 because ARIN does not wish to be notified about such block sizes. If you allocate a block that is smaller than a /29 in a seed pool where ARIN reporting is enabled, you will see the SWIP Reporting screen during the Allocation process. In such circumstances, it is recommended that you leave the SWIP template information empty, and click **Allocate** to proceed. Select **Do Not generate Report** and click **Cancel**. If any information is entered, it will be ignored.

For IPv4 address blocks, ARIN SWIP templates that are supported in VitalQIP include:

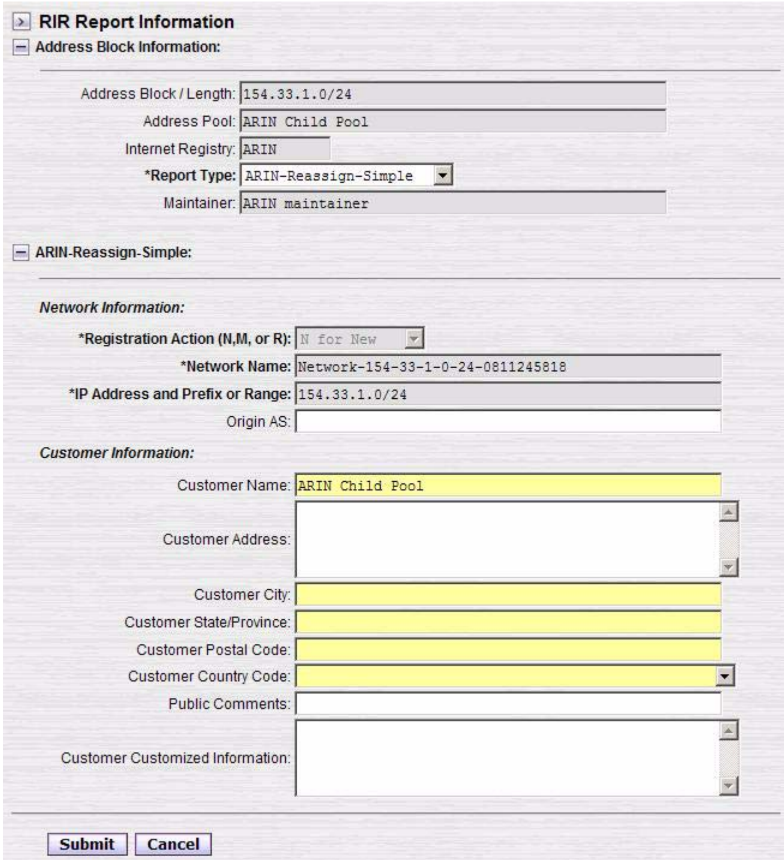
- ARIN-REALLOCATE-4.2
- ARIN-REASSIGN-SIMPLE-4.1
- ARIN-REASSIGN-DETAILED-4.2

For IPv6 address blocks, ARIN SWIP templates that are supported in VitalQIP include:

- ARIN-IPv6-REALLOCATE-4.2
- ARIN-IPv6-REASSIGN-4.2

For more information on these SWIP templates, please access **www.arin.net**. A sample SWIP reporting screen is shown as follows.

Table 28-1 Sample SWIP reporting screen



Whenever a SWIP report is sent after a block has been allocated, VitalQIP stores the following as part of the block information:

- The type of SWIP report that was generated.
- The value of the **network name** field (a unique name that includes the **Network Prefix** value defined in the Seed Pool function. Refer to "Add a seed pool" (p. 27-4).

Support for SWIP report template changes

Because SWIP report templates can change between VitalQIP releases, free text fields are available that allow for you to add values to the SWIP report. The information in these fields is placed verbatim in the RIR email that is sent.

Values are entered in the following format:

`tag: value`

For example:

`testtag: testvalue`

`another test tag: my test value`

All tags and values entered must be valid and supported by RIR. If tags and value are not supported by the RIR, a syntax error is returned from RIR.

The following table shows the available free text fields associated with each report template.

Table 28-2 SWIP report templates and associated free text fields

SWIP report template	Associated free text fields
ARIN-REALLOCATE	Org Customized Information Org POC Customized Information Net POC Customized Information
ARIN-REASSIGN-SIMPLE	Customer Customized Information
ARIN-REASSIGN-DETAILED	Org Customized Information Org POC Customized Information Network Customized Information Net POC Customized Information Others Customized Information
ARIN-IPv6-REALLOCATE	Org Customized Information Org POC Customized Information Network Customized Information Net POC Customized Information Others Customized Information
ARIN-IPv6-REASSIGN	Org Customized Information Org POC Customized Information Network Customized Information Net POC Customized Information Others Customized Information

SWIP reporting after Freeing a Block

Whenever a Free Block operation is performed on a block that contains a valid SWIP type and **network name**, a corresponding Free SWIP report is sent ***automatically***.

- For a block allocated with an ARIN-REASSIGN-SIMPLE template, it is freed by sending another ARIN-REASSIGN-SIMPLE template and specifying `R` for Registration Action in the template.

- For a block allocated with an ARIN-REASSIGN-DETAILED template or an ARIN-REALLOCATE template, it is freed by sending an ARIN-NET-MOD template and specifying **R** for Registration Action in the template.
- For a block allocated with an ARIN-REASSIGN-SIMPLE-4.1 template, it is freed by sending another ARIN-NET-MOD-4.1 template and specifying **R** for Registration Action in the template.

For further information on freeing a block, refer to "The free block function" (p. 28-32).

APNIC reporting

Introduction

VitalQIP contains optional support for registering address space with APNIC and RIPE. The configuration parameters for APNIC are available at the seed block level. Each seed block can be configured differently (one seed pool might use APNIC and another may not).

Enable APNIC support

APNIC support is turned on by selecting **APNIC** as the **Registry Name** in the Add Seed Pool page. Refer to Table 28-9, "Block allocation fields" (p. 28-18) for information on the fields that support APNIC.

What is APNIC

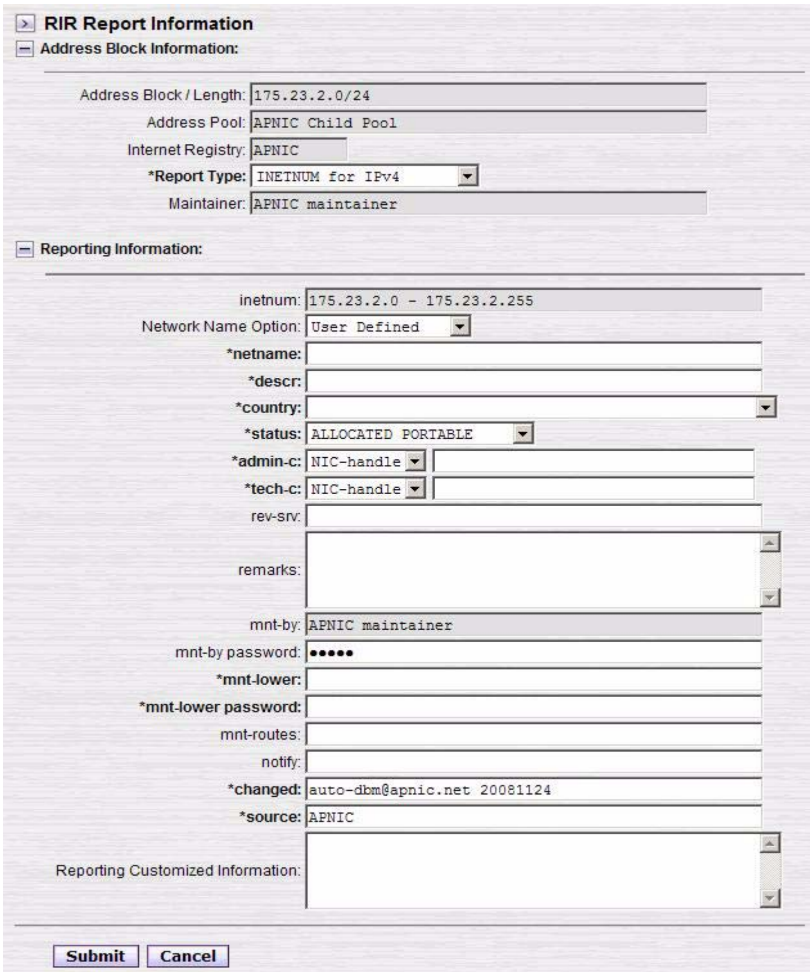
APNIC maintains a database (WHOIS) of all registered IP address blocks and information about who is using this address space in Asian Pacific. When an ISP allocates address space to another company, it registers this allocation by sending an APNIC report to Whois.

VitalQIP's support of APNIC

If a seed pool is configured with APNIC support turned on, any block allocation that creates a VitalQIP subnet anywhere below the seed pool in the hierarchy will generate an inetnum report associated with the maintainer ID specified on the seed pool. VitalQIP does not generate inetnum reports for block allocations that are smaller than the minimum block size specified on the seed pool because APNIC does not wish to be notified about such block sizes. If you allocate a block that is smaller than the specified minimum block size in a seed pool where inetnum reporting is enabled, you will see the APNIC Reporting screen during the Allocation process. In such circumstances, it is recommended that you leave the inetnum template information empty, and click **Allocate** to proceed. Select **Do Not generate Report** and click **Cancel**. If any information is entered, it will be ignored.

For information on the APNIC inetnum report, please access **www.apnic.net**. The following is a sample APNIC reporting screen.

Table 28-3 Sample APNIC reporting screen



Note: Administrators for the **admin-c** and **tech-c** fields must be defined before inetnum report can be generated.

Whenever an APNIC inetnum report is sent after a block has been allocated, VitalQIP stores the following as part of the block information:

- The type of APNIC inetnum report that was generated.
- The value of the **network name** field.

For IPv4 address blocks, the status for inetnum report is one of the following:

- ALLOCATED PORTABLE
- ALLOCATED NON-PORTABLE
- ASSIGNED PORTABLE

- ASSIGNED NON-PORTABLE

For IPv6 address blocks, the status for inet6num report is one of the following:

- ALLOCATED PORTABLE
- ALLOCATED NON-PORTABLE
- ASSIGNED PORTABLE
- ASSIGNED NON-PORTABLE

Support for APNIC report template changes

Because APNIC report templates can change between VitalQIP releases, free text fields are available that allow for you to add values to the APNIC report. The information in these fields is placed verbatim in the RIR email that is sent.

Values are entered in the following format:

`tag: value`

For example:

`testtag: testvalue`

`another test tag: my test value`

All tags and values entered must be valid and supported by RIR. If tags and value are note supported by the RIR, a syntax error is returned from RIR.

The following table shows the available free text fields associated with each report template.

Table 28-4 APNIC report templates and associated free text fields

SWIP report template	Associated free text fields
INETNUM for IPv4	Reporting Customized Information Org Customized Information Admin Contact Customized Information Technical Customized Information
INETNUM for IPv6	Reporting Customized Information Org Customized Information: Admin Contact Customized Information Technical Customized Information

Inetnum reporting after freeing a block

Whenever a Free Block operation is performed on a block that contains a valid inetnum report type and network name, a corresponding Free inetnum report is sent ***automatically***. For further information on freeing a block, refer to "The free block function" (p. 28-32).

RIPE reporting

Introduction

VitalQIP contains optional support for registering address space with RIPE. The configuration parameters for RIPE are available at the seed block level. Each seed block can be configured differently (one seed block might use RIPE and another may not).

Enable RIPE support

RIPE support is turned on by selecting **RIPE** as the **Address Source** in the Add Seed Pool screen. Refer to "Add a seed pool" (p. 27-4) for information on the additional fields that support RIPE.

What is RIPE

RIPE maintains a database (WHOIS) of all registered IP address blocks and information about who is using this address space in Europe and the Middle-East. When an ISP allocates address space to another company, it registers this allocation by sending an RIPE report to Whois.

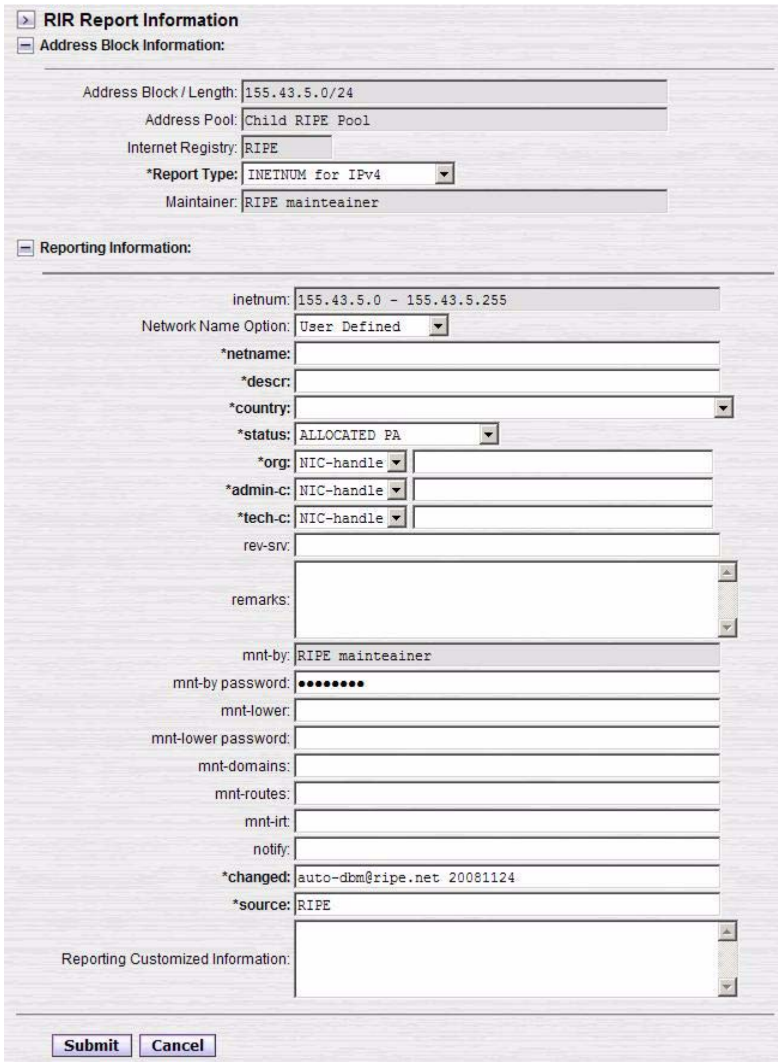
VitalQIP's support of RIPE

If a seed pool is configured with RIPE support turned on, any block allocation that creates a VitalQIP subnet anywhere below the seed pool in the hierarchy will generate an inetnum report associated with a maintainer ID specified on the seed pool. VitalQIP will prompt for various pieces of information needed in the inetnum report. This information will be formatted into the selected inetnum report and emailed to the **RIPE Email** address specified on the seed pool.

> **Note:** VitalQIP does not generate inetnum reports for block allocations that are smaller than the minimum block size specified on the seed pool because RIPE does not wish to be notified about such block sizes. If you allocate a block that is smaller than the minimum block size specified on the seed pool in a seed pool where inetnum reporting is enabled, you will see the RIPE Reporting screen during the Allocation process. In such circumstances, Alcatel-Lucent recommends that you leave the inetnum template information empty, and click **Allocate** to proceed. Select **Do Not generate Report** and click **Cancel**. If any information is entered, it will be ignored.

For information on the RIPE inetnum report, please access **www.ripe.net**. The following is a sample RIPE reporting screen.

Table 28-5 Sample RIPE reporting screen



> **Note:** Administrators for the **admin-c** and **tech-c** fields must be defined before inetnum report can be sent.

The **Whois Report Information** section of the RIPE inetnum report screen is a freeform interface. It does not place any restrictions on the field lengths or the values entered into the fields. In some cases, some fields are not applicable if other fields have a value. Some fields also may have length or content limitations although VitalQIP does not enforce any restrictions. This is by design since the format of the RIPE inetnum report is subject to change by RIPE. When the RIPE inetnum report email is generated, any non-applicable fields are ignored.

Whenever a RIPE inetnum report is sent after a block has been allocated, VitalQIP stores the following as part of the block information:

- The type of RIPE inetnum report that was generated.
- The value of the **network name** field.

For IPv4 address blocks, the status for inetnum report, is one of the following:

- ALLOCATED PA
- ALLOCATED PI
- ALLOCATED UNSPECIFIED
- ASSIGNED PA
- ASSIGNED PI
- LIR-PARTITIONED PA
- LIR-PARTITIONED PI
- SUB-ALLOCATED PA
- ASSIGNED ANYCAST
- EARLY-REGISTRATION
- NOT-SET

For IPv6 address blocks, the status for inet6num report is one of the following:

- ALLOCATED-BY-LIR
- ALLOCATED-BY-RIR
- ASSIGNED
- ASSIGNED ANYCAST

Support for RIPE report template changes

Because RIPE report templates can change between VitalQIP releases, free text fields are available that allow for you to add values to the RIPE report. The information in these fields is placed verbatim in the RIR email that is sent.

Values are entered in the following format:

`tag: value`

For example:

`testtag: testvalue`

`another test tag: my test value`

All tags and values entered must be valid and supported by RIR. If tags and value are note supported by the RIR, a syntax error is returned from RIR.

The following table shows the available free text fields associated with each report template.

Table 28-6 RIPE report templates and associated free text fields

SWIP report template	Associated free text fields
INETNUM for IPv4	Reporting Customized Information Org Customized Information Admin Contact Customized Information Technical Customized Information
INETNUM for IPv6	Reporting Customized Information Org Customized Information: Admin Contact Customized Information Technical Customized Information

Inetnum reporting after freeing a block

Whenever a Free Block operation is performed on a block that contains a valid inetnum report type and network name, a corresponding Free inetnum report is sent ***automatically***. For further information on freeing a block, refer to “The free block function” (p. 28-32).

AfriNIC reporting

Introduction

VitalQIP contains optional support for registering address space with AfriNIC. The configuration parameters for AfriNIC are available at the seed block level. Each seed block can be configured differently (one seed block might use AfriNIC and another may not).

Enable AfriNIC support

AfriNIC support is turned on by selecting **AfriNIC** as the **Address Source** in the Add Seed Pool screen. Refer to “Add a seed pool” (p. 27-4) for information on the additional fields that support AfriNIC.

What is AfriNIC

AfriNIC maintains a database (WHOIS) of all registered IP address blocks and information about who is using this address space in Africa. When an ISP allocates address space to another company, it registers this allocation by sending an AfriNIC report to Whois.

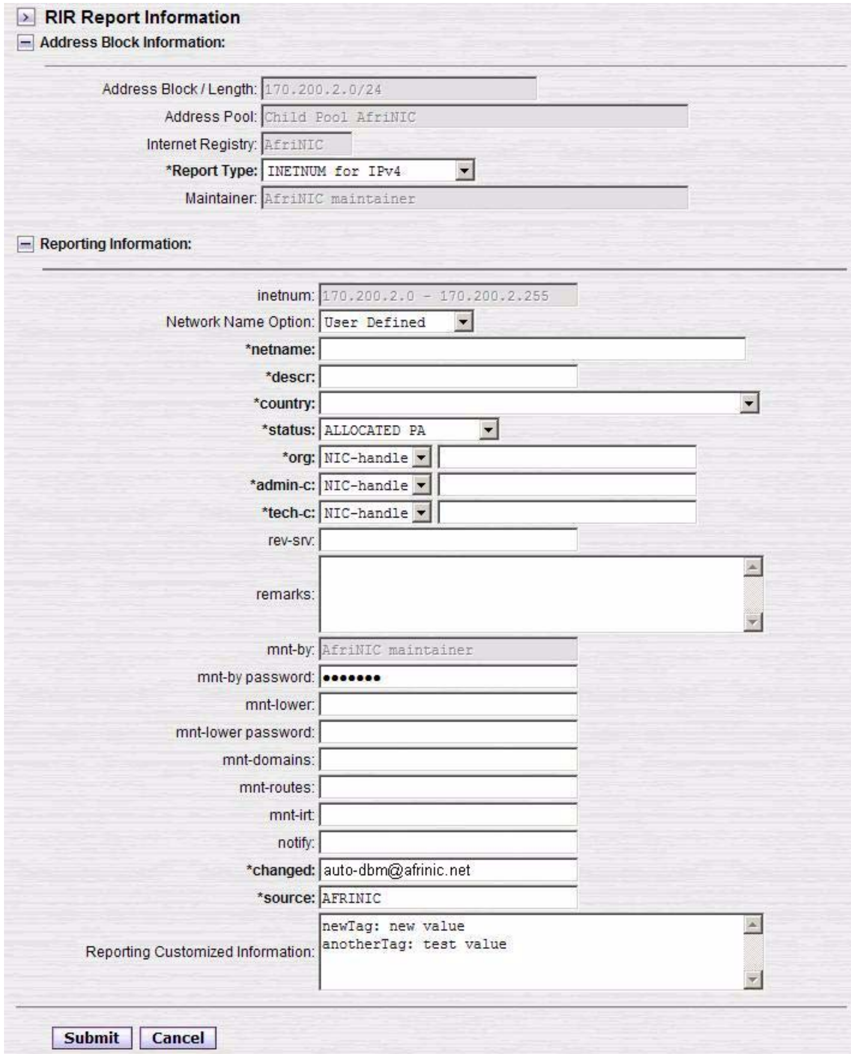
VitalQIP's support of AfriNIC

If a seed pool is configured with AfriNIC support turned on, any block allocation that creates a VitalQIP subnet anywhere below the seed pool in the hierarchy will generate an inetnum report associated with a maintainer ID specified on the seed pool. VitalQIP will prompt for various pieces of information needed in the inetnum report. This information will be formatted into the selected inetnum report and emailed to the **AfriNIC Email** address specified on the seed pool.

> **Note:** VitalQIP does not generate inetnum reports for block allocations that are smaller than the minimum block size specified on the seed pool because AfriNIC does not wish to be notified about such block sizes. If you allocate a block that is smaller than the minimum block size specified on the seed pool in a seed pool where inetnum reporting is enabled, you will see the AfriNIC Reporting screen during the Allocation process. In such circumstances, Alcatel-Lucent recommends that you leave the inetnum template information empty, and click **Allocate** to proceed. Select **Do Not generate Report** and click **Cancel**. If any information is entered, it will be ignored.

For information on the AfriNIC inetnum report, please access **www.AfriNIC.net**. The following is a sample AfriNIC reporting screen.

Table 28-7 Sample AfriNIC reporting screen



Note: Administrators for the **admin-c** and **tech-c** fields must be defined before inetnum report can be sent.

The **Whois Report Information** section of the AfriNIC inetnum report screen is a freeform interface. It does not place any restrictions on the field lengths or the values entered into the fields. In some cases, some fields are not applicable if other fields have a value. Some fields also may have length or content limitations although VitalQIP does not enforce any restrictions. This is by design since the format of the AfriNIC inetnum report is subject to change by AfriNIC. When the AfriNIC inetnum report email is generated, any non-applicable fields are ignored.

Whenever a AfriNIC inetnum report is sent after a block has been allocated, VitalQIP stores the following as part of the block information:

- The type of AfriNIC inetnum report that was generated.

- The value of the **network name** field.

For IPv4 address blocks, the status for inetnum report, is one of the following:

- ALLOCATED PA
- ALLOCATED PI
- ALLOCATED UNSPECIFIED
- ASSIGNED PA
- ASSIGNED PI
- LIR-PARTITIONED PA
- LIR-PARTITIONED PI
- SUB-ALLOCATED PA
- ASSIGNED ANYCAST
- EARLY-REGISTRATION
- NOT-SET

For IPv6 address blocks, the status for inet6num report is one of the following:

- ALLOCATED-BY-LIR
- ALLOCATED-BY-RIR
- ASSIGNED
- ASSIGNED ANYCAST

Support for AfriNIC report template changes

Because AfriNIC report templates can change between VitalQIP releases, free text fields are available that allow for you to add values to the AfriNIC report. The information in these fields is placed verbatim in the RIR email that is sent.

Values are entered in the following format:

`tag: value`

For example:

`testtag: testvalue`

`another test tag: my test value`

All tags and values entered must be valid and supported by RIR. If tags and value are note supported by the RIR, a syntax error is returned from RIR.

The following table shows the available free text fields associated with each report template.

Table 28-8 AffriNIC report templates and associated free text fields

SWIP report template	Associated free text fields
INETNUM for IPv4	Reporting Customized Information Org Customized Information Admin Contact Customized Information Technical Customized Information
INETNUM for IPv6	Reporting Customized Information Admin Contact Customized Information Technical Customized Information

Inetnum reporting after freeing a block

Whenever a Free Block operation is performed on a block that contains a valid inetnum report type and network name, a corresponding Free inetnum report is sent ***automatically***. For further information on freeing a block, refer to "The free block function" (p. 28-32).

Add a seed block to a seed pool

Purpose

Use this procedure to add a seed block to a seed pool.

Before you begin

You can also access this function from the Pool Hierarchy.

Procedure

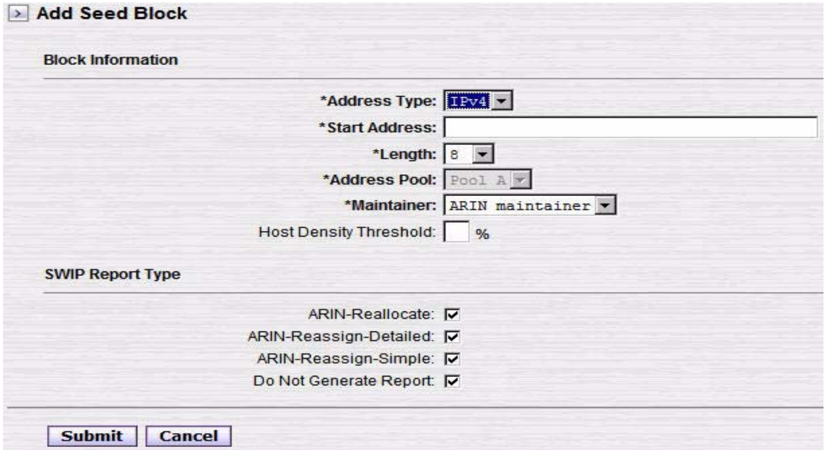
To add a seed block to a seed pool, follow these steps.

1. Mouse over **Address Allocation** and click **Block Hierarchy**.

   Result: The Block Hierarchy opens.

2. Mouse over the **Actions** menu and select **Add Seed Block**.

Result: The Add Seed Block page opens.



3 Review the following table, and fill in the Add Block fields.

Table 28-9 Block allocation fields

Field	Description
Address Type	***Required***. Select IPv4 or IPv6 from the drop-down list. Read only when modifying a block.
Start Address	***Required***. Enter a valid IP address in either IPv4 or IPv6 format as specified in the Address Type field. Read only when modifying a block.
Length	***Required***. Select a length from the drop-down list. Read only when modifying a block.
Address Pool	***Required***. Select the address pool from the drop-down list to which you are allocating this block. Read only when modifying a block.
Maintainer	***Required for seed blocks***. Does not display, but defaults to the maintainer for the seed pool for other blocks. Select the name of the person responsible for this block from the drop-down list. Read only when modifying a non-seed pool block. **Note:** A default value may be set for this field using the **`blocknetworkcontact`** parameter in the *qip.properties* file. Refer to Chapter 3 of the *VitalQIP Administrator Reference Manual* for details on this parameter.
Status	***Required for non-seed blocks***. Is always set to Free for other blocks. Select a status for the block from the drop-down list.

Field	Description
Host Density Threshold	***Optional***. When the Host Density (HD) ratio reaches this ratio, the user will be notified. HD is calculated as follows: HD = log(number of allocated objects) / log(maximum number of allocatable objects)
Report Type	***Optional***. Only displays when the address pool is registered with an Internet registry (ARIN, RIPE, APNIC or AfriNIC). Select the type of report you want VitalQIP to generate when this block is added or deleted.

Modify a block

Purpose

Use this procedure to modify a block.

Before you begin

You can also access this function from the Pool Hierarchy.

Procedure

To modify a block, follow these steps.

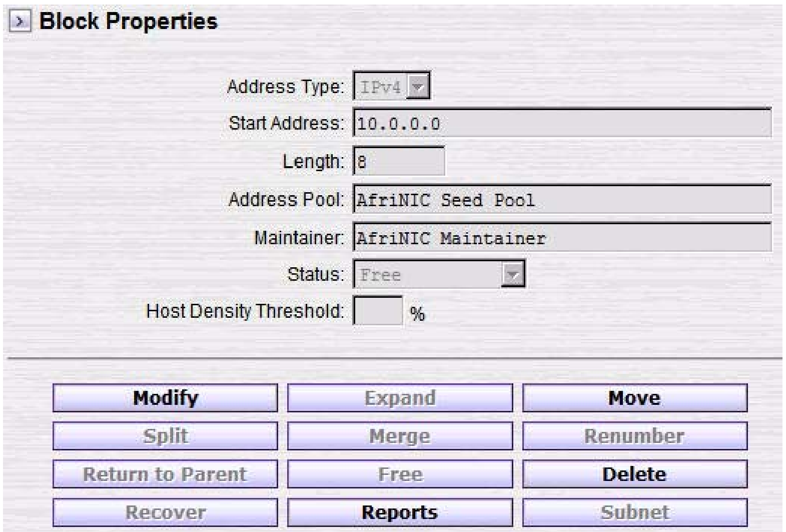
1. Mouse over **Address Allocation** and click **Block Hierarchy**.

   Result: The Block Hierarchy opens.

2. Expand the list of blocks until the one you want to modify is visible.

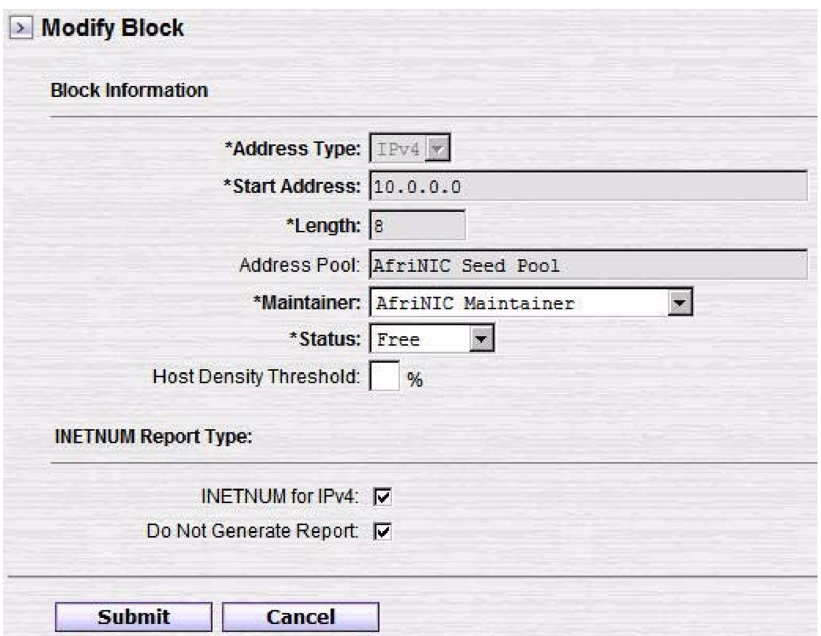
3. Select the block you want to modify.

Result: The Block Properties page opens.



4 Click **Modify**.

Result: The Modify Block page opens.



5 Modify the Block Property fields as necessary.

For seed blocks, you can modify the **Block Status** (from Free to Reserved and vice versa), **Host Density Threshold** and report types. At least one report type must be entered. For a child block, you can modify **Block Status** from Free to Reserved and vice versa.

Refer to Table 28-9, "Block allocation fields" (p. 28-18) and modify the fields as needed.

6 Click **Submit**.

Result: A dialog box opens with the message **Modify Block completed.**

7 Click **OK**.

Result: The dialog box closes and the Block Properties page opens.

END OF STEPS

Block expansion

Overview

Block expansion allows a block to acquire contiguous space from the parent pool. Expansion is limited to double the original size (for example, /48 can be expanded to /47).

Block expansion can be performed on all levels of blocks except for the seed block. The block does not have to be the highest level block within a pool.

Expansion is allowed for all the allocation algorithms, but works best with sparse allocation.

For block expansion, the address can be borrowed from the parent pool, if the pool does not have free address space to expand the block.

Expansion is allowed for the block status values Used, Free, and Reserved.

If the block is Used, and if the subnet was created in VitalQIP (identified by the presence of the associated subnet name) then VitalQIP also expands the size of corresponding subnet.

Expand a block

Purpose

Use this procedure to expand a block.

Before you begin

- If a block has “allocated” status, it cannot be expanded. The expansion request must come from the same block located in the child pool.
- When a block is expanded, if there is a free block that exists that is going to be consumed in the expansion, Attribute values in the free block are not used in the operation, and Attribute values in the block to be expanded remain.
- You can also access this function from the Pool Hierarchy.

Procedure

To expand a block, follow these steps.

1 Mouse over **Address Allocation** and click **Block Hierarchy**.

Result: The Block Hierarchy opens.

2 Expand the list of blocks until the one you want to expand is visible.

3 Select the block you want to expand.

Result: The Block Properties page opens.

4 Click **Expand**.

Result: A dialog box opens with the message **Are you sure you want to double the size of the selected Block?**

5 Click **OK**.

Result: The block is expanded.

END OF STEPS

Move block function

Overview

Moving a block moves the selected block, all of its children in the block hierarchy, and all of the child pools that contain segments of this block to the destination pool. The source pool is deleted after the move is complete.

To move a block, the following conditions must be met:

- The source and destination pools must be siblings
- The block must be highest level block in the pool
- All address space in any child pool that contains a portion of the block to be moved must only contain address space of the block to be moved.

Move a block

Purpose

Use this procedure to move a block.

Before you begin

You can also access this function from the Pool Hierarchy.

Procedure

To move a block, follow these steps.

1. Mouse over **Address Allocation** and click **Block Hierarchy**.

   Result: The Block Hierarchy opens.

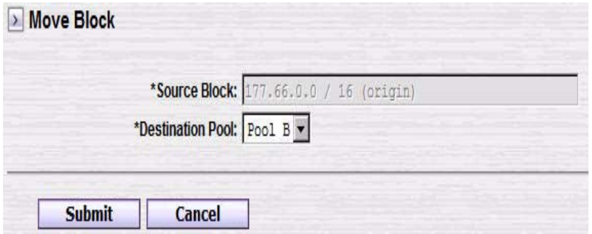
2. Expand the list of blocks until the one you want to move is visible.

3. Select the block you want to move.

   Result: The Block Properties page opens.

4. Click **Move**.

Result: The Move Block page opens.



5 Select a destination pool from the drop-down list and click **Submit**.

Result: A dialog box opens with the message **Are you sure you want to move the Block to the destination Pool?**

6 Click **OK**.

Result: A dialog box opens with the message **Move Block completed**.

7 Click **OK**.

Result: The Block Hierarchy is updated and the Block Properties page for the moved block opens.

END OF STEPS

The split block function

Overview

The Split Block function allows you to create multiple smaller blocks from a specified block. The Split Block function is allowed only on address blocks with a Used status, and with no prior RIR reporting done on them.

If the original Block was the highest level Block within the Pool, VitalQIP changes the status of the original Address Block status to Origin and creates new Address Blocks under it.

If the original Block was the not the highest level Block within the Pool, VitalQIP deletes the original Address Block and creates new Address Blocks in its place.

It also splits the corresponding subnet in the IPv4 address module.

There is no RIR reporting following the Split Block operation.

Split a block

Purpose

Use this procedure to split a block. At most the address block can be advanced 8 bits. For example, for a size /32 IPv6 block, you can split it to 256 size /40 IPv6 blocks.

Before you begin

You can also access this function from the Pool Hierarchy.

Procedure

To split a block, follow these steps.

1. Mouse over **Address Allocation** and click **Block Hierarchy**.

   Result: The Block Hierarchy opens.

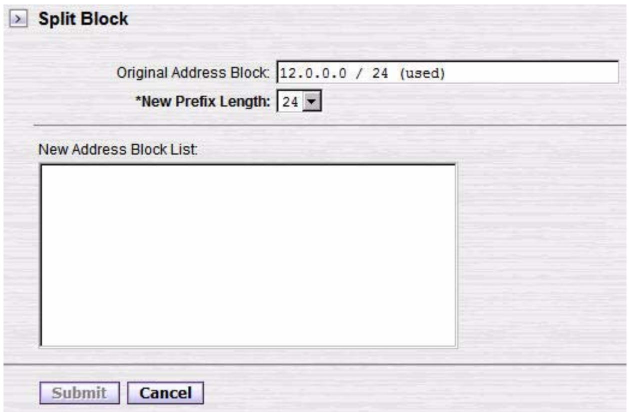
2. Expand the list of blocks until the one you want to split is visible.

3. Select the block you want to split.

   Result: The Block Properties page opens.

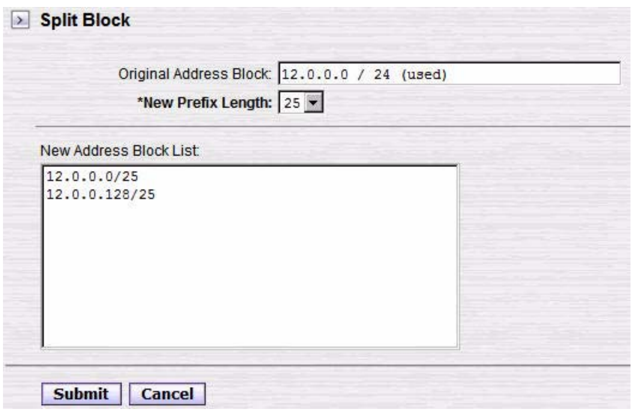
4. Click **Split**.

Result: The Split Block page opens.



5 Select a new prefix length from the drop-down list. This specifies the length of new Address Blocks.

Result: The New Address Block List is populated with the list of address blocks that will be generated when the request is submitted.



6 Click **Submit**.

Result: A dialog box opens with the message **Are you sure you want to split selected block?**

7 Click **OK**.

Result: The block is split.

End of Steps

The merge block function

Overview

Merge Block combines the current block with its contiguous block.

Merging blocks is allowed for the following block status values:

- Used
- Reserved
- Free

Used blocks you are merging cannot have prior RIR reporting.

Both blocks being merged must be siblings within the same pool (If they are in different pools, you can use the Move Block operation to get the blocks into the same pool). Both blocks being merged cannot have Free status. Free blocks should be merged by the "Free Space Consolidation" function. Refer to f"The free block function" (p. 28-32) or more information. If two blocks are being merged with differing status values the resulting status is as follows:

- Used + any status = Used
- Reserved + Free = Reserved

If an IPv4 block is Used, and if the subnet was created in VitalQIP, the size of the corresponding subnet in VitalQIP is also expanded.

There is no RIR reporting after merging blocks.

When two blocks are merged, Attribute values in the source block (which is eventually removed) are not used in the operation, and Attribute values in the target block remain.

Merge a block

Purpose

Use this procedure to merge a block.

Before you begin

You can also access this function from the Pool Hierarchy.

Procedure

To merge a block, follow these steps.

1 Mouse over **Address Allocation** and click **Block Hierarchy**.

Result: The Block Hierarchy opens.

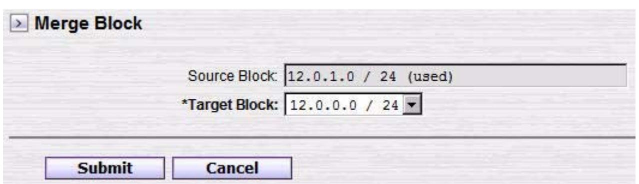
2 Expand the list of blocks until one of the blocks you want to merge is visible.

3 Select the block you want to merge.

Result: The Block Properties page opens.

4 Click **Merge**.

Result: The Merge Block page opens.



5 Select the block with which you want to merge this block from the drop-down list and click **Submit**.

Result: A dialog box opens with the message **Are you sure you want to merge selected Blocks?**

6 Click **OK**.

Result: The blocks are merged.

END OF STEPS

The renumber block function

Overview

The renumber function allows the user to change the prefix of the Address Block, without having to change the IP address component to the right of the prefix (that is, the InterfaceId). The Renumber Block function is allowed only on IPv6 Address Blocks with Used status, and with no prior RIR reporting done on them. The target Block must already exist in Free or Reserved status within the same pool as the source block.

The user selects the Source Block from the hierarchy and clicks on the Renumber Block action. The GUI will present the candidate Blocks (blocks of the same size with Free status, within the same pool,) that can be the potential targets.

There is no RIR reporting after the Renumber operation.

Renumber a block

Purpose

Use this procedure to renumber an IPv6 block.

Procedure

To renumber a block, follow these steps.

---

1 Mouse over **Address Allocation** and click **Block Hierarchy**.

Result: The Block Hierarchy opens.

---

2 Expand the list of blocks until the block you want to renumber is visible.

---

3 Select the block you want to renumber.

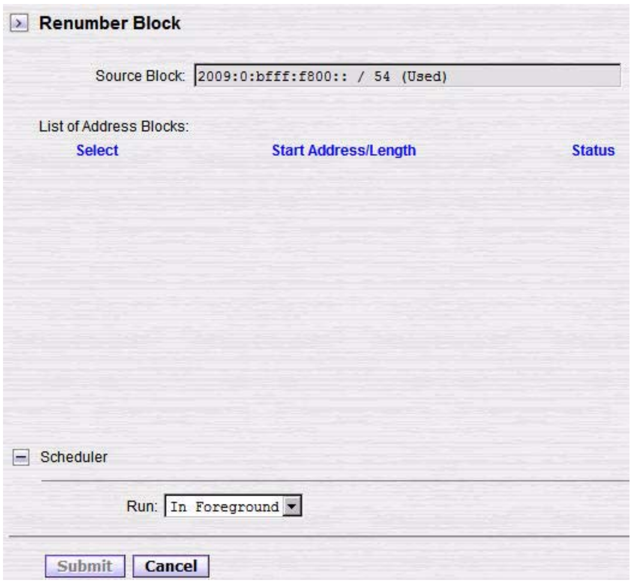
Note: The block must have a status of Used and cannot have had RIR reporting associated with it.

Result: The Block Properties page opens.

---

4 Click **Renumber**.

Result: The Renumber Block page opens. A list of blocks of the same size with a status of free status, within the same pool displays. These are the blocks that can be the potential targets.



5 Select an address block as the target and click **Submit**.

Result: A dialog box opens with the message **Are sure you want to renumber the current Block?**

6 Click **OK**.

Result: The block is renumbered.

END OF STEPS

The return child block to parent function

Overview

This function allows you to return a child block to its parent. You can perform this function if the block status is free, and the block is the highest level block in its pool. The block is removed from the current pool and the corresponding block in the parent pool (that had a status of Allocated) is marked as Free.

Return a block to its parent

Purpose

Use this procedure to return a block to its parent.

Before you begin

The block must be the highest level block in its pool and must have a status of Free or the **Return to Parent** button will not be active.

Before you begin

You can also access this function from the Pool Hierarchy.

Procedure

To return a block to its parent, follow these steps.

1. Mouse over **Address Allocation** and click **Block Hierarchy**.

   Result: The Block Hierarchy opens.

2. Expand the list of blocks until the block you want to return to its parent pool is visible.

3. Select the block you want to return to its parent.

   Result: The Block Properties page opens.

4. Click **Return to Parent**.

   Result: A dialog box opens with the message **Are you sure you want to return the selected Block to parent Pool?**

5. Click **OK**.

   Result: The block is returned to its parent pool.

END OF STEPS

The free block function

Overview

You can only free Used blocks. If a registry report was generated during block allocation, a new one must be generated and sent. For IPv4 blocks, the corresponding subnet in VitalQIP must also be deleted. Once the block is marked Free, VitalQIP runs a Free Space Consolidation routine that consolidates separate contiguous blocks into one larger block, and potentially consolidates all the child blocks into the parent block.

Pending status

The transition of a block from Used to Free might not happen immediately: based on the option set at the pool level (the **Support Pending** field), the block might be set to Pending status for some duration determined by the pool level option. During that period, you may also undo the effects of the Free block function by using the Recover block function. Refer to "Recover a block" (p. 28-34).

Status check of Pending blocks

A scheduled process checks the status of Pending blocks and frees them (it sets the status to Free as necessary). The default schedule for this job to check and free Pending blocks is set to once a day at 1:00 AM. To modify the schedule, open *$QIPHOME/web/conf/schedule.properties* in a text editor and modify the following parameter:

`schedule.free_pending_block_run_time`

> **Note:** The password in *schedule.properties* must be entered as an encrypted string when you set up this job.

At least 6 (and optionally 7) time elements, separated by spaces are used to indicate the time. In order from left to right, the values are defined as follows:

1. Seconds: **`0-59`** (* indicates every second)
2. Minutes: **`0-59`** (* indicates every minute)
3. Hours: **`0-23`** (* indicates every hour)
4. Day of month: **`1-31`** (* indicates every day of the month)
5. Month: **`1-12`** or **`JAN-DEC`** (* indicates every month)
6. Day of week: **`1-7`** or **`SUN-SAT`** (* indicates every day of the week)
7. Year: **`1970-2099`**

The following is an example of a job entry in *schedule.properties*:

```
schedule.run_free_pending_block_job=true
schedule.free_pending_block_run_time=0 0,30 6-22 * * ?
```

This job runs every half hour from 6:00AM to 10:00PM every day.

block,checkpending CLI

The **`block,checkpending`** CLI allows you to query the **whois** database and set Pending blocks to Free if the criteria are matched.

The following is an example of the CLI used to change all Pending blocks to Free under the VitalQIP Organization if the criteria are matched:

```
./qip-cli -c block,checkpending -o "VitalQIP Organization"
   --level=organization
```

DEBUG

If the scheduled jobs are not running, turn on DEBUG in *$QIPHOME/web/conf/log4j.properties* so you can troubleshoot the problem. For example,

```
log4j.threshold = DEBUG
log4j.logger.localized.com.lucent.qip.schedule=DEBUG
```

VitalQIP database updates

Along with freeing the address block, VitalQIP also removes the IPv4 Subnet and all the IP addresses within the subnet. The DNS entries associated with these IP addresses are also deleted. If the address is the only IP address on an interface when the IP address is removed, the interface is removed. Similarly, if the interface being removed is the only one on the node, the node is removed.

Free a block

Purpose

Use this procedure to free a block.

Before you begin

- If the block being freed is the highest level block in the pool, it may be returned to its parent. A dialog box appears with the message **Return the Free Block to Parent?**
- You can also access this function from the Pool Hierarchy.

Procedure

To free a block, follow these steps.

1. Mouse over **Address Allocation** and click **Block Hierarchy**.

Result: The Block Hierarchy opens.

2 Expand the list of blocks until the block you want to free is visible.

3 Select the block you want to free.

Result: The Block Properties page opens.

4 Click **Free**.

Result: A dialog box opens with the message **Are you sure you want to free the selected Block?**

5 Click **OK**.

Result: The block is freed.

END OF STEPS

Recover a block

Purpose

Use this procedure to undo the effects of the Free block function. The recover block function allows you to recover a block after it is freed but still in a Pending state. This occurs because of registry reporting and settings in the seed pool **Allow Pending Status on Blocks** field.

Before you begin

You can also access this function from the Pool Hierarchy.

Procedure

To recover a block, follow these steps.

1 Mouse over **Address Allocation** and click **Block Hierarchy**.

Result: The Block Hierarchy opens.

2 Expand the list of blocks until the Pending block you want to recover is visible.

3 Select the block you want to recover.

Result: The Block Properties page opens.

4 Click **Recover**.

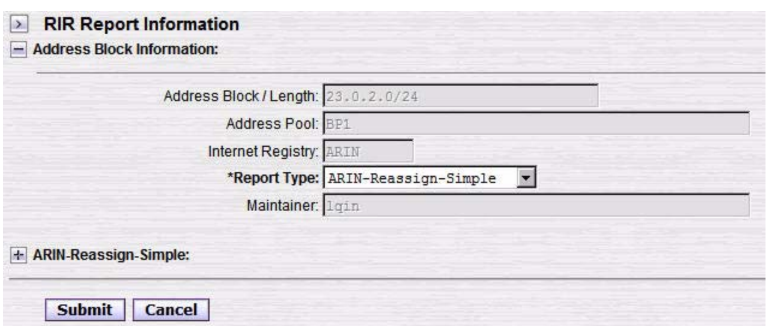
Result: A dialog box opens with the message **Are you sure you want to recover the Selected block?**

5 Click **OK**.

Result: A dialog box opens with the message **Recover Block completed!**

6 Click **OK**.

Result: The RIR Report Information page opens.



7 Fill in the report fields and click **Submit**.

Result: A dialog box opens with the message **RIR Reporting generated succeeded**.

8 Click **OK**.

Result: The block status reverts to Used in the Block Hierarchy and its properties are displayed in the Block Properties page, where the **Status** field reads **Used**. Additionally, a new RIR report is sent to the Internet Registry.

END OF STEPS

Delete a block

Purpose

Use the delete block function to delete a block.

Before you begin

- You can only delete a seed block with a Free status. If you select a block other than a seed block, the **Delete Block** button is inactive.
- All address spaces within that block (everywhere in the hierarchy) must be free.
- You can also access this function from the Pool Hierarchy.

Procedure

To delete a block, follow these steps.

1 Mouse over **Address Allocation** and click **Block Hierarchy**.

Result: The Block Hierarchy opens.

2 Expand the list of blocks until the block you want to delete is visible.

3 Select the block you want to delete.

Result: The Block Properties page opens.

4 Click **Delete**.

Result: A dialog box opens with the message **Are you sure you want to delete the selected Seed Block?**

5 Click **OK**.

Result: A dialog box opens with the message **Seed Block deleted.**

6 Click **OK**

Result: The Block Hierarchy is updated and the IP Management splash screen opens.

END OF STEPS

Manage a subnet assocated with a block

Purpose

Use this procedure to manage a subnet associated with a block.

Before you begin

- The **Subnet** button is only enabled on the Block Properties page if a subnet is associated with a block.
- When a subnet is associated with a block, the subnet cannot be split, joined, or deleted.
- Access to buttons on the Subnet Properties page is dependent on the administrator permissions.

Procedure

To manage a subnet associated with a block, follow these steps.

1 Mouse over **Address Allocation** and click **Block Hierarchy**.

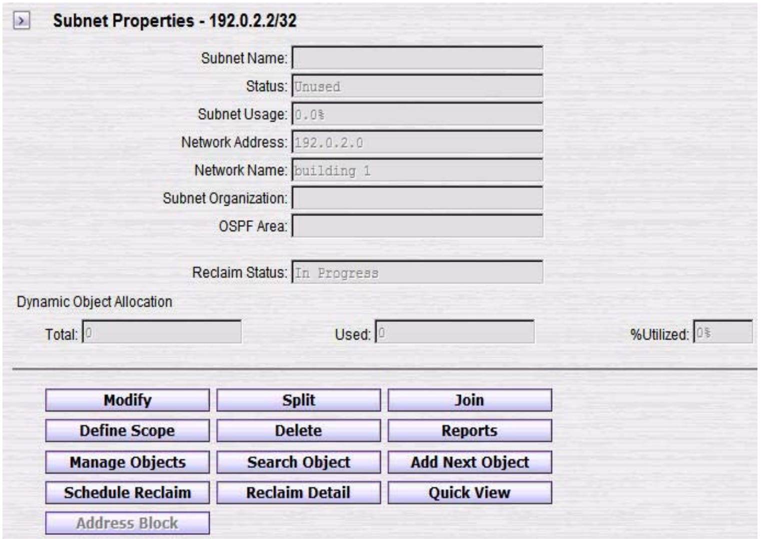
Result: The Block Hierarchy opens.

2 Expand the list of blocks and select the block associated with a subnet.

Result: The Block Properties page opens.

3 Click **Subnet**.

Result: The Subnet Properties page opens.



END OF STEPS

Part VI: Web client administration

Overview

Purpose

This part of the manual provides information on web client administration.

Contents

This part includes these chapters.

29 Reports

Overview

Purpose

This chapter describes the different types of reports VitalQIP can produce for Address Allocation, Address Management, DNS, and Infrastructure.

Contents

This chapter covers these topics.

About Reports

Overview

Purpose

Reports provide the user with information to manage address allocation and management infrastructure, acl template usage and zone resource records, and VitalQIP infrastructure. Each report can be formatted and saved as a file, as well as displayed on the screen.

You can produce reports from the following locations:

- From the Reports tab.
- From the Reports icon in the toolbar.
- From the Properties page of an item selected in the hierarchy.

Note: Report availability is based on administrator privileges. If an administrator does not have access privileges for certain functions, related reports are not displayed.

Types of reports

VitalQIP provides the following reports.

Table 29-1 Report types

Module	Category	Report
Address Allocation	Block	Hierarchy
		Utilization
	Pool	Block Status
		Hierarchy
		Information
		Statistics
		Usage
		View Free Space
	Rule	Summary

Module	Category	Report
Address Management	IPv4	Object Info
		Subnet Info
		Subnet Usage
	IPv6	Managed Addresses
		Subnets
	Node	Hierarchy
DNS	ACL Template	ACL Template Usage
	Zone	Resource Record
Infrastructure	Audit	Administrator Activity
		Administrator Generation
		Administrator Profile
		Administrative Role
		Block
		DC Generation
		DHCP Server Generation
		DNS Server Generation
		DNS View
		IPv4 Network
		IPv4 Subnet
		IPv4 Subnet Organization
		IPv6 Address
		IPv6 Subnet
		Managed Files
		My View
		Organization
		Pool
		Rule
	My View	Hierarchy

Auditing parameter in qip.pcy

Audit reports are only available if auditing is enabled for your system. By default, auditing is enabled when VitalQIP is installed. Auditing is controlled by the **`Auditing`** policy in the Global section of the *qip.pcy* file. Refer to Chapter 3 in the *VitalQIP Administrator Reference Manual* for further information.

> **Note:** The **`Auditing`** policy controls only address allocation and IPv6 address management. Because IPv4 subnet management is controlled by auditing rules in the VitalQIP client, IPv4 subnet reports and an Administrator Activity report of an IPv4 subnet are available when auditing is not enabled.

Record search limit in qip.properties

The **`MAX_FETCH_RECORDS`** property in *qip.properties* limits the number of records that can be displayed in reports to a default of 100,000. It can be set to a different value, or to -1 to remove the restriction altogether.

About user defined attributes, fields, and reports

If user defined attributes or fields are associated with specific reports, an additional section or option is displayed. The sections or options **User Defined Attribute** or **User Define Fields**. Refer to "Working with user defined attributes and fields" (p. 7-23) for more information on working with user defined attributes or fields.

Schedule a report

Purpose

Use this procedure to schedule report generation.

Procedure

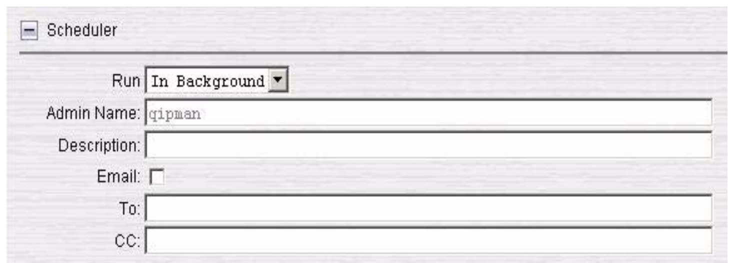
To schedule the generation of a report, follow these steps.

1 Select the report you want to run.

Result: The report setup window opens. For further information on setting up reports, refer to the descriptions of specific reports.

2 Expand the **Scheduler** section, if necessary.

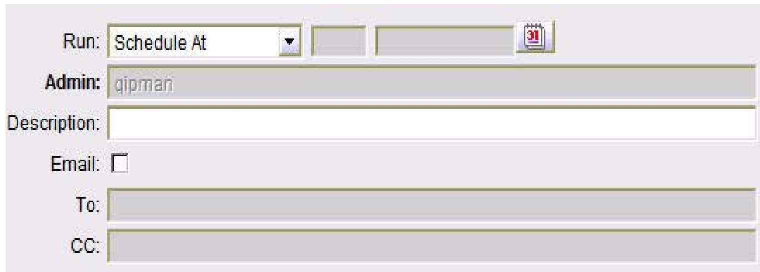
3 Choose one of the following actions.

If you want to...	Then ...
Run the job immediately	Ensure that **In Foreground** is selected in the **Run** drop-down list.
Run the job in background	1. Select **In Background** from the **Run** drop-down list. **Result:** The **Scheduler** section expands to display additional fields.  The **Admin** field displays the login ID of the administrator who is scheduling the job. 2. Enter a description of the job in the **Description** field. If you do not enter a description, a description of *<Job Name>:<Run Mode>* is used. You may enter up to 255 characters. 3. If you want an e-mail to be sent when the job completes, place a check in the **Email** check box. **Result:** The **To** and **CC** fields are enabled. 4. Enter one or more e-mail addresses (comma separated) in the **To** field. If an e-mail address has been entered in the **Contact Profile** for the administrator, it appears by default. The field limit is 255 characters. 5. If desired, enter one or more e-mail addresses in the **CC** field.

<table>
<tr><th>If you want to...</th><th>Then ...</th></tr>
<tr><td>Schedule the job for a later time</td><td>

1. Select **Scheduled At** from the **Run** drop-down list.

Result: The **Scheduler** section expands to display additional fields, including a Calendar icon.



The **Admin** field displays the login ID of the administrator who is scheduling the job.

2. Click the Calendar icon ( ).

Result: The Calendar widget opens with the scheduled date default of 10 days from the current date.

3. Choose from the following actions.
   a. To choose a different time, click in the hour and minute fields and enter a new time in 24-hour format.
   b. To choose a different month, choose a later month from the month drop-down list.
   c. To choose a different year, click ≥ to enter a future year or ≤ to return to a prior year.
   d. To choose a different day, click another day in the month.

Result: After a different day is clicked, the Calendar widget closes and a new run date and/or time are displayed.

4. Enter a description of the job in the **Description** field. If you do not enter a description, a description of `<Job Name>:<Run Mode>` is used. You may enter up to 255 characters.

</td></tr>
</table>

If you want to...	Then ...
	5. If you want an e-mail to be sent when the job completes, place a check in the **Email** check box. **Result:** The **To** and **CC** fields are enabled. 6. Enter one or more e-mail addresses (comma separated) in the **To** field. If an e-mail address has been entered in the **Contact Profile** for the administrator, it appears by default. The field limit is 255 characters. 7. If desired, enter one or more e-mail addresses in the **CC** field.

4 Click **Submit**.

Result: The result depends on which Run option you chose and which report you were generating. For further information on generating reports, refer to the descriptions of specific reports.

END OF STEPS

Address allocation reports

Overview

Purpose

The following reports are available from the **Address Allocation** section of the Reports hierarchy.

- Block Hierarchy Report
- Block Utilization Report
- Pool Block Status Report
- Pool Hierarchy Report
- Pool Info Report
- Pool Statistics Report
- Pool Usage Report
- Pool View Free Space Report
- Rule Summary Report

When accessed from the Reports hierarchy, you need to enter search criteria to locate the block or pool on which to report. For information on the search criteria, refer to "Search for a block" (p. 29-10) and "Search for a pool" (p. 29-13). The report output defaults to html format. You can choose to view the report output either in the html format or as a PDF file.

Search for a block

Purpose

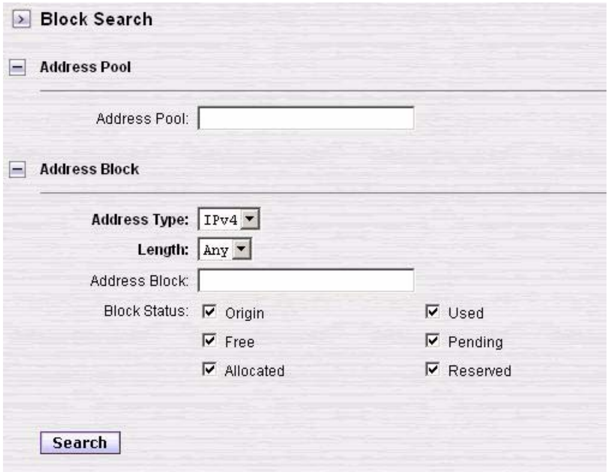
Use this procedure to search for a block on which you want to produce the block hierarchy, block utilization, or block audit reports.

Procedure

To search for a block, follow these steps.

1. Select a block hierarchy, block utilization, or block audit report and click **Search**.

Result: The Block Search Criteria window opens.



2 Review the following table and fill in the fields you need to complete your search.

Table 29-2 Pool/Block search fields

Field	Description
Address Pool	***Required***. Enter the name of the pool for which you are searching. This field is case-sensitive. You can enter a partial name by using the asterisk (*) as a wildcard, or you can leave the field blank to search all pools.
Address Type	Select **IPv4** or **IPv6** from the drop-down list.
Length	***Optional***. Select a length from the drop-down list. To return any address length, select **Any**. Otherwise, choose the exact length for which you are searching.
Address Block	***Optional***. Enter the IP address of the address block for which you are searching. You can enter a partial address by using the asterisk (*) as a wildcard.
Block Status	***Optional***. Click a checkbox to limit your search to only blocks with that status. If all block statuses are checked, the search looks for all blocks.
Attribute Value	Enter the full or partial name (with wildcard) of the attribute. To search for an attribute with a null value, enter two double quotes (“ ”).
Address block attributes	

Field	Description
Attribute Group	***Required if visible***. If specified, the search is limited to this block attribute group. You can specify any attribute groups currently associated with the Pool or one of two pre-defined entries: • **<NONE>** – Select this entry to exclude Block Attribute Group from this search criteria row. • **<IGNORE>** – Select this entry if, for this search criteria row, you do not care if a UDA is in a group or not. • **<ANY>** – Select this entry to include all Block Attribute Group(s) in this search criteria row.
Attribute Name	***Required if visible***. If specified, the search is limited to this block attribute value. Values in this column are based on the value in the **Attribute Group** column. The available values are: • All Attributes that do not attach to any Attribute Group, plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<NONE>**. • All Attributes of Block, plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<IGNORE>**. • All Attributes attached to the specified Attribute Group, plus the pre-defined entry **<ALL>** – if an Attribute Group is selected. • All Attributes attached to at least one Attribute Group, plus the pre-defined entry **<ALL>** – if Attribute Group is set to **<ANY>**.
Attribute Value	Full or partial name (with wildcard) of the attribute. To search for an attribute with a null value, enter two double quotes (“ ”). Do one of the following: • Click **Add New Criteria** to add address block attributes as required. You can add a maximum of five attributes. • Click **Remove** to delete the address block attributes.

3 Click **Search**.

Result: The results appear in the **Search Results** list.

END OF STEPS

Search for a pool

Purpose

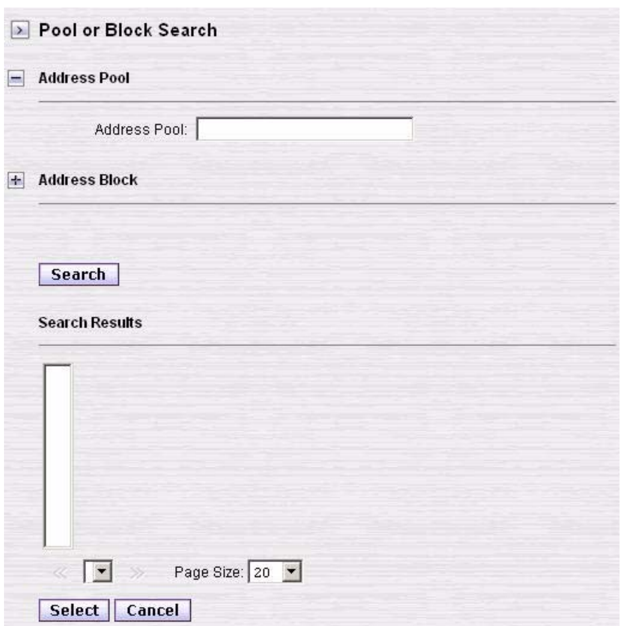
Use this procedure to search for a pool on which you want to produce the Pool Block Status, Pool Hierarchy, Pool Info, Pool Statistics, Pool Usage, Pool Free Space, or the Pool Audit reports.

Procedure

To search for a pool, follow these steps.

1 Select a Pool Block Status, Pool Hierarchy, Pool Info, Pool Statistics, Pool Usage, Pool Free Space, or the Pool Audit report and click **Search**.

Result: The Pool or Block Search window opens.



2 ***Required***. Enter the name of the pool for which you are searching in the **Address Pool** field. This field is case-sensitive. You can enter a partial name followed by an asterisk (*) as a wildcard, or leave the field blank to search all pools.

3 Click **Search**.

Result: The results appear in the **Search Results** list.

END OF STEPS

Produce a Block Hierarchy report

Purpose

This report provides the hierarchy structure within a selected block. Instructions are provided for access from the Reports hierarchy or from the Block Properties page.

From the menu or toolbar

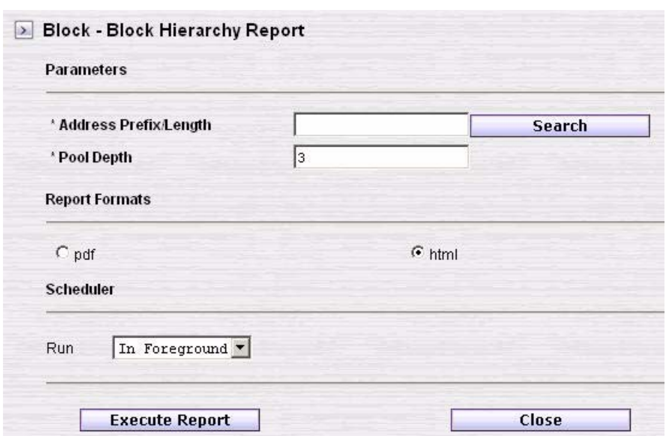
To produce a Block Hierarchy report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Allocation - Block** section, click **Hierarchy**.

Result: The Block - Block Hierarchy Report page opens.



3 Click **Search**.

Result: The Block Search window opens. Refer to "Search for a block" (p. 29-10) for further information.

4 Highlight the block for which you wish to review hierarchy information and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected block appears in the **Address Prefix/Length** field.

5 In the **Pool Depth** field, enter the level of the pool hierarchy for which you want hierarchy information.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Block Properties page

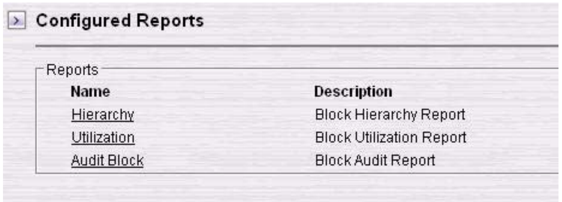
To produce a Block Hierarchy report on a block in the hierarchy, follow these steps.

1 Select the block on which you want to report.

Result: The Block Properties page opens.

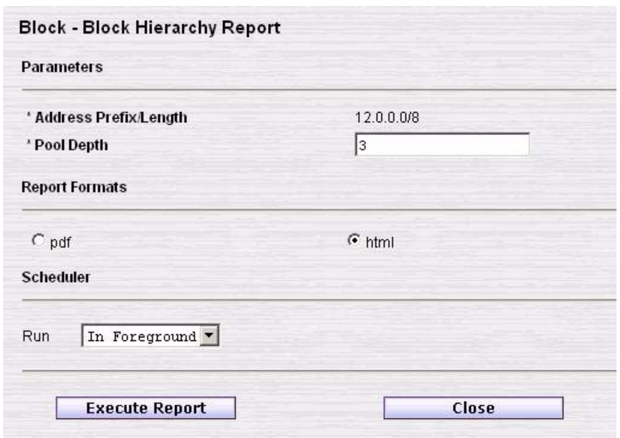
2 Click **Reports**.

Result: The Configured Reports page opens.



3 Click the **Hierarchy** link.

Result: The Block Hierarchy Report page opens in the Report Execution window.



4 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

5 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

6 Click **Execute Report**.

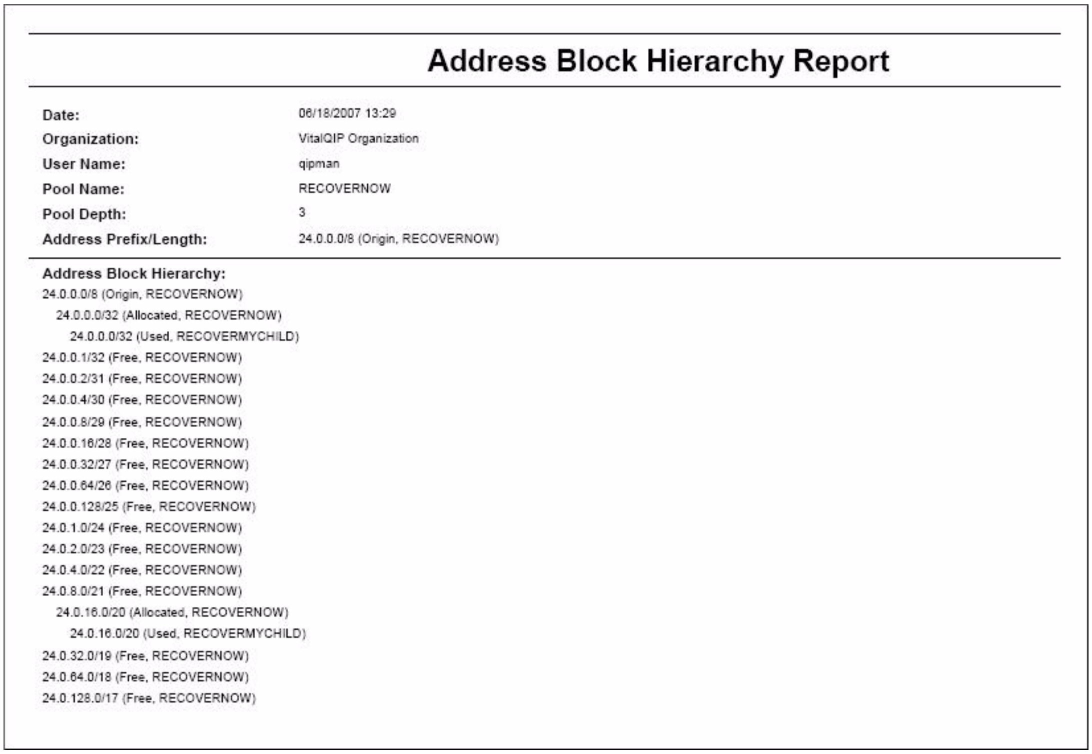
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Block Hierarchy report appears as follows.

Figure 29-1 Sample Address Block Hierarchy report



Address Block Hierarchy Report

Date:	06/18/2007 13:29
Organization:	VitalQIP Organization
User Name:	qipman
Pool Name:	RECOVERNOW
Pool Depth:	3
Address Prefix/Length:	24.0.0.0/8 (Origin, RECOVERNOW)

Address Block Hierarchy:
24.0.0.0/8 (Origin, RECOVERNOW)
  24.0.0.0/32 (Allocated, RECOVERNOW)
    24.0.0.0/32 (Used, RECOVERMYCHILD)
24.0.0.1/32 (Free, RECOVERNOW)
24.0.0.2/31 (Free, RECOVERNOW)
24.0.0.4/30 (Free, RECOVERNOW)
24.0.0.8/29 (Free, RECOVERNOW)
24.0.0.16/28 (Free, RECOVERNOW)
24.0.0.32/27 (Free, RECOVERNOW)
24.0.0.64/26 (Free, RECOVERNOW)
24.0.0.128/25 (Free, RECOVERNOW)
24.0.1.0/24 (Free, RECOVERNOW)
24.0.2.0/23 (Free, RECOVERNOW)
24.0.4.0/22 (Free, RECOVERNOW)
24.0.8.0/21 (Free, RECOVERNOW)
  24.0.16.0/20 (Allocated, RECOVERNOW)
    24.0.16.0/20 (Used, RECOVERMYCHILD)
24.0.32.0/19 (Free, RECOVERNOW)
24.0.64.0/18 (Free, RECOVERNOW)
24.0.128.0/17 (Free, RECOVERNOW)

The following table describes the fields on the report.

Table 29-3 Address Block Hierarchy report fields

Field	Description
Date	Date and time the report was produced.
Organization	Organization where the block is located.
User Name	User who produced the report.
Pool Name	Pool that is the subject of this report.
Pool Depth	The level of the pool hierarchy that this report covers.
Address Prefix/Length	Address of the block, followed by the prefix that indicates its length.
Column headings	
Address Prefix/Lengths	Address of each block, followed by the prefix that indicates its length.

Field	Description
Block Status	Status of each block.
Pool Name	Name of the pool in which this block is located.

Produce a Block Utilization report

Purpose

This report provides a list of all Used and Reserved blocks within a selected block. Instructions are provided for access from the Reports hierarchy or from the Block Properties page.

From the menu or toolbar

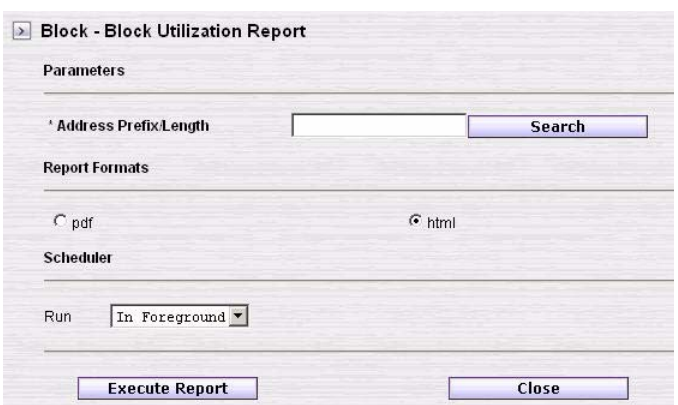
To produce a Block Utilization report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Allocation - Block** section, click **Utilization**.

Result: The Block Utilization Report page opens.



3 Click **Search**.

Result: The Pool/Block Search Criteria window opens. Refer to "Search for a block" (p. 29-10) for further information.

4 Highlight the block for which you wish to review usage and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected block appears in the **Address Prefix/Length** field.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Block Properties page

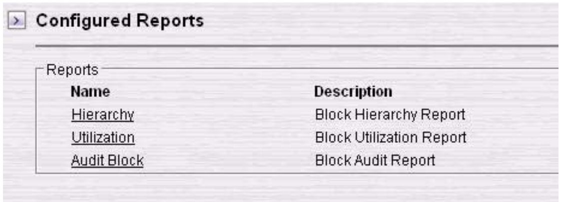
To produce a Block Utilization report, follow these steps.

1 In the hierarchy, click the name of the block for which you want the report.

Result: The Block Properties page opens.

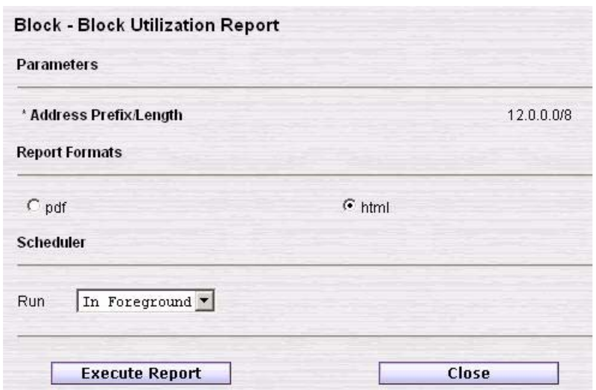
2 Click **Reports**.

Result: The Configured Reports page opens.



3 Click the **Utilization** link.

Result: The Block Utilization Report page opens in the Report Execution window.



4 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

5 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

6 Click **Execute Report**.

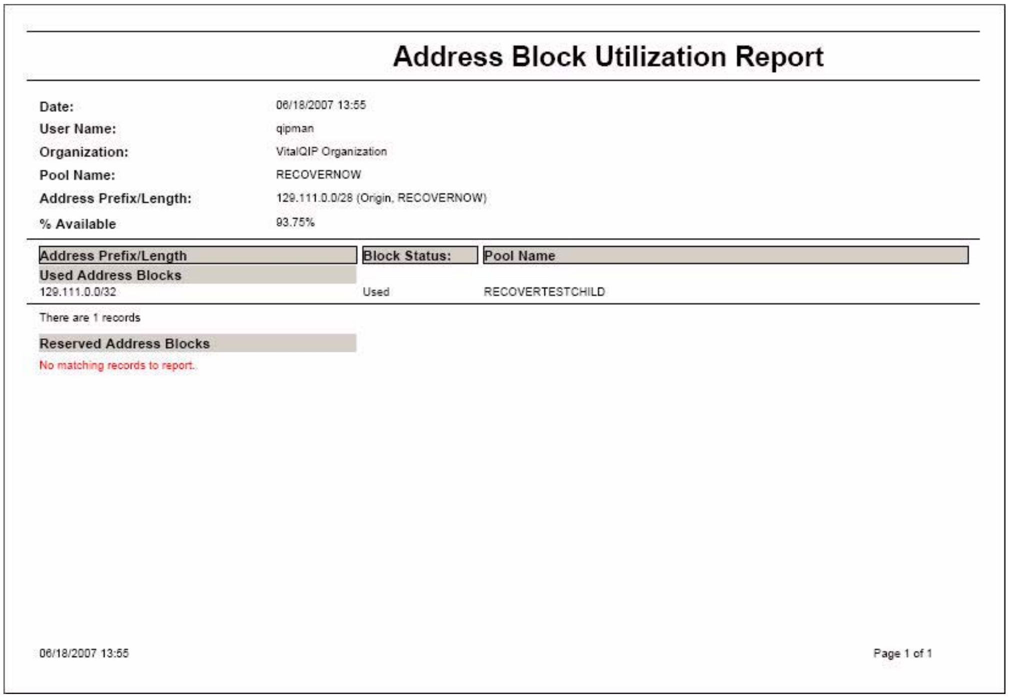
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Block Utilization report appears as follows.

Figure 29-2 Sample Block Utilization report



Address Block Utilization Report

Date:	06/18/2007 13:55
User Name:	qipman
Organization:	VitalQIP Organization
Pool Name:	RECOVERNOW
Address Prefix/Length:	129.111.0.0/28 (Origin, RECOVERNOW)
% Available	93.75%

Address Prefix/Length	Block Status:	Pool Name
Used Address Blocks		
129.111.0.0/32	Used	RECOVERTESTCHILD

There are 1 records

Reserved Address Blocks

No matching records to report.

06/18/2007 13:55 Page 1 of 1

The following table describes the fields on the report.

Table 29-4 Address Block Utilization report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the block is located
Pool Name	Pool that contains the block that is the subject of this report.
Address Prefix/Length	Address of the block, followed by the prefix that indicates its length.
% Available	The percentage of free space available in the block.
Column headings The following column headings appear for used address blocks and reserved address blocks.	
Address Prefix/Length	Address of each block, followed by the prefix that indicates its length.

Field	Description
Block Status	Status of each block.
Pool Name	Name of the pool in which this block is located.

Produce a Pool Block Status report

Purpose

This report provides a list of blocks sorted by status within a selected pool. Instructions are provided for access from the Reports hierarchy or from the Pool Properties page.

From the menu or toolbar

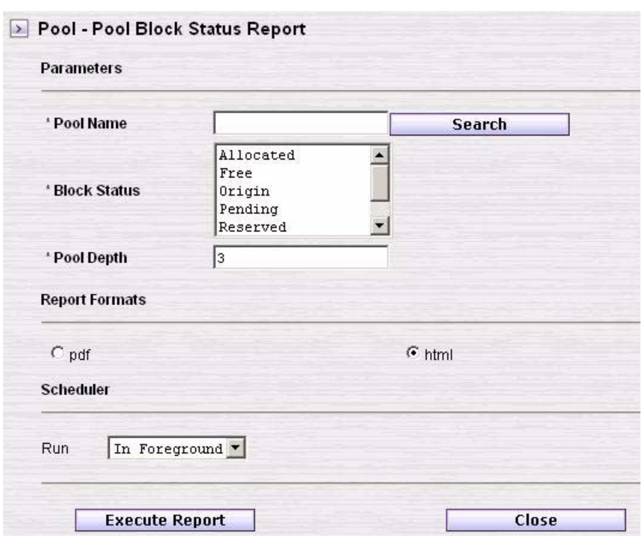
To produce a Pool Block Status report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Allocation - Pool** section, click **Block Status**.

Result: The Pool Block Status Report page opens.



3 Click **Search**.

Result: The Pool/Block Search Criteria window opens. Refer to "Search for a pool" (p. 29-13) for further information.

4 Highlight the pool whose status you want to review and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected pool appears in the **Pool Name** field.

5 Select the statuses of the blocks you want to see. You can select multiple block statuses by holding the **Ctrl** or **Shift** keys as you click the different status types.

6 Enter the level of the pool hierarchy for which you want status information. The default level is set to `3`.

7 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

9 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Pool Properties page

To produce a Pool Block Status report, follow these steps.

1 In the hierarchy, click the name of the pool for which you want the report.

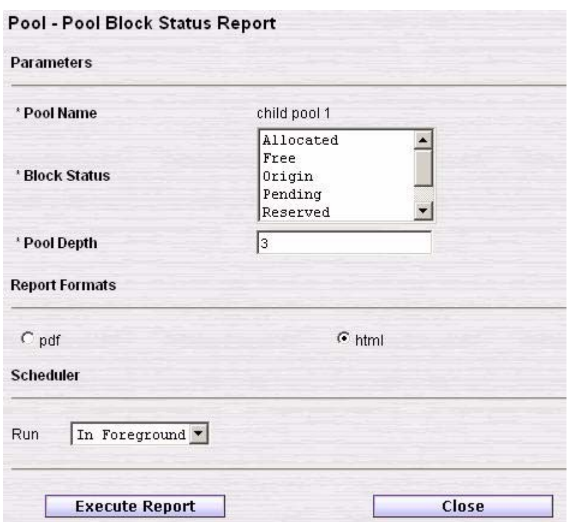
Result: The Pool Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Block Status** link.

Result: The Pool Block Status Report page opens in the Report Execution window.



4 Select the statuses of the blocks you want to see. You can select multiple block statuses by holding the **Ctrl** or **Shift** keys as you click the different status types.

5 Enter the level of the pool hierarchy for which you want pool status information. The default level is set to **3**.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

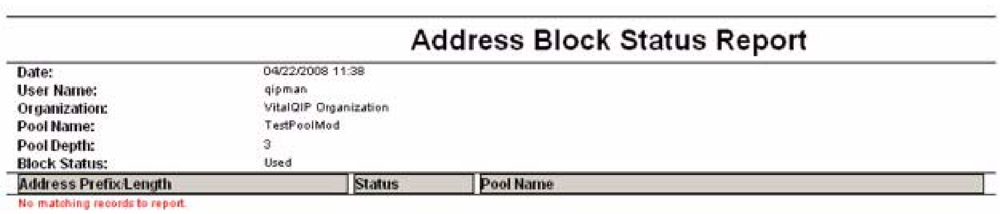
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Pool Block Status report appears as follows.

Figure 29-3 Sample Pool Block Status report


Address Block Status Report

Date: 04/22/2008 11:38
User Name: qipman
Organization: VitalQIP Organization
Pool Name: TestPoolMod
Pool Depth: 3
Block Status: Used

Address Prefix/Length	Status	Pool Name

No matching records to report.

The following table describes the fields on the report.

Table 29-5 Pool Block Status report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the pool is located

Field	Description
Pool Name	Pool that is the subject of this report.
Pool Depth	The level of the pool hierarchy that this report covers.
Block Status	List of all the block statuses specified when the report was produced.
Column headings	
Address Prefix/Length	Address of the block, followed by the prefix that indicates its length.
Status	Status of the block. The only statuses that appear in this column are the ones specified when the report was produced.
Pool Name	Pool where the block is located. Pools display down to the level specified in the pool depth field when the report was produced.

Produce a Pool Hierarchy report

Purpose

This report provides the hierarchy information within a selected pool, allowing you to see the structure of the pools and blocks within them. Instructions are provided for access from the Reports hierarchy or from the Pool Properties page.

From the menu or toolbar

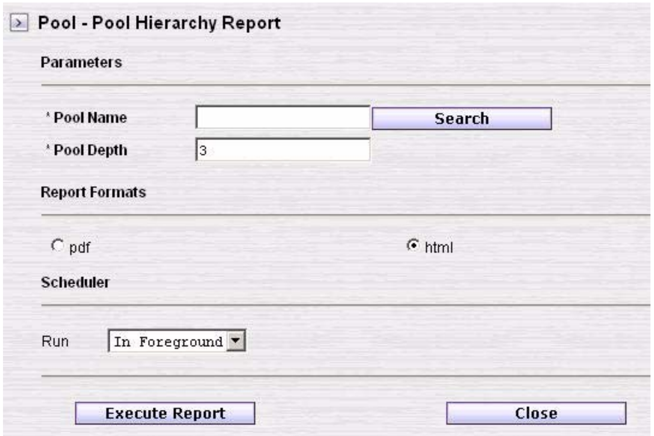
To produce a Pool Hierarchy Status report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Allocation - Pool** section, click **Hierarchy**.

Result: The Pool Hierarchy Report page opens.



3 Click **Search**.

Result: The Pool/Block Search Criteria window opens. Refer to "Search for a pool" (p. 29-13) for further information.

4 Highlight the pool whose hierarchy you wish to review and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected pool appears in the **Pool Name** field.

5 Enter the level of the pool hierarchy for which you want pool hierarchy information. The default level is set to **3**.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Pool Properties page

To produce a Pool Hierarchy report, follow these steps.

1 In the hierarchy, click the name of the pool for which you want the report.

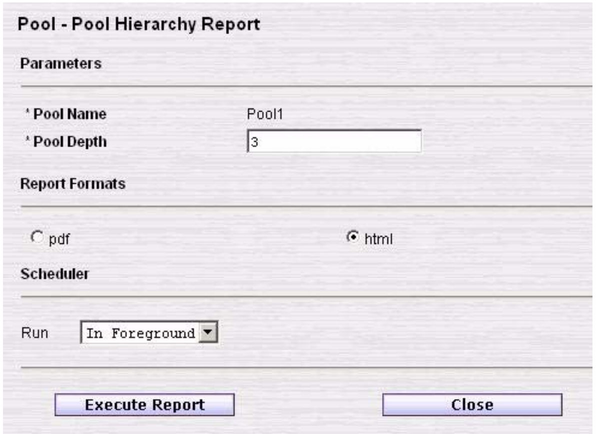
Result: The Pool Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Hierarchy** link.

Result: The Pool Hierarchy Report page opens in the Report Execution window.



---

4 Enter the level of the pool hierarchy for which you want pool hierarchy information. The default level is set to **3**.

---

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

---

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

---

7 Click **Execute Report**.

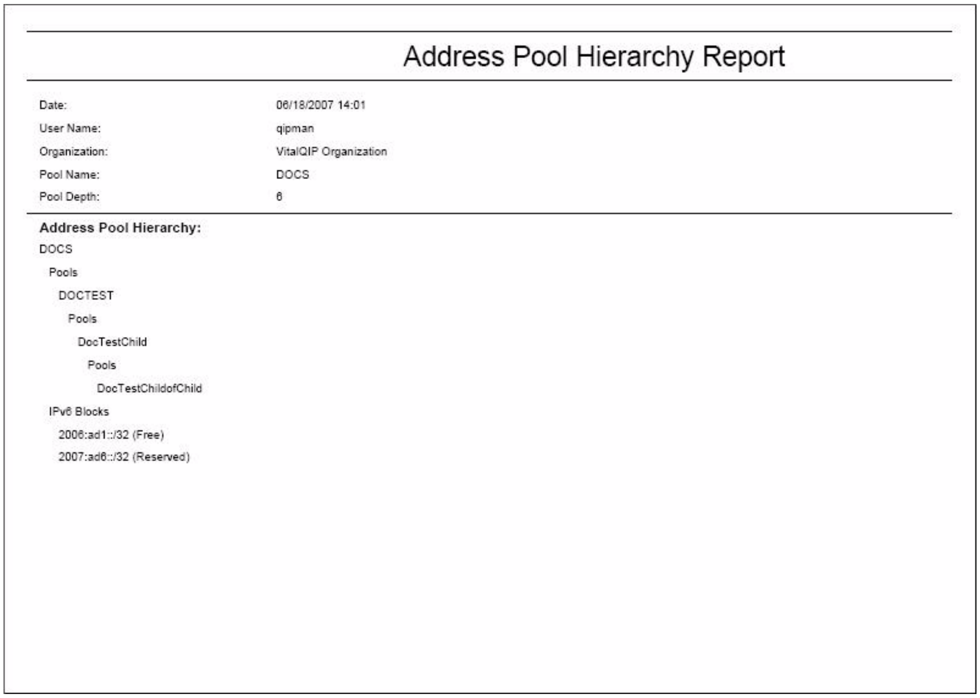
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Pool Hierarchy report appears, as follows.

Figure 29-4 Sample Pool Hierarchy report


Address Pool Hierarchy Report

Date: 06/18/2007 14:01
User Name: qipman
Organization: VitalQIP Organization
Pool Name: DOCS
Pool Depth: 6

Address Pool Hierarchy:
DOCS
Pools
DOCTEST
Pools
DocTestChild
Pools
DocTestChildofChild
IPv6 Blocks
2006:ad1::/32 (Free)
2007:ad6::/32 (Reserved)

The following table describes the fields on the report.

Table 29-6 Pool Hierarchy report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the pool is located
Pool Name	Pool that is the subject of this report.
Pool Depth	The level of the pool hierarchy that this report covers.
Hierarchy headings	
Address Pool Hierarchy	Name of the pool whose hierarchy is being shown

Produce a Pool Statistics report

Purpose

This report provides usage statistics information for a selected pool. Instructions are provided for access from the Reports hierarchy or from the Pool Properties page.

From the menu or toolbar

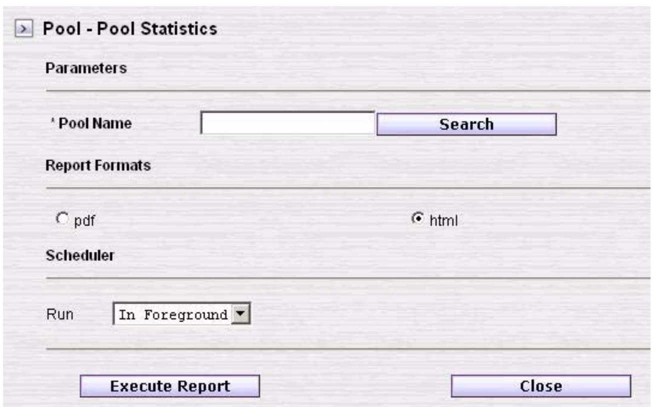
To produce a Pool Statistics report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Allocation - Pool** section, click **Statistics**.

Result: The Pool Statistics Report page opens.



3 Click **Search**.

Result: The Pool or Block Search Criteria window opens. Refer to "Search for a pool" (p. 29-13) for further information.

4 Highlight the pool whose statistics you wish to review and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected pool appears in the **Pool Name** field.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Pool Properties page

To produce a Pool Statistics report, follow these steps.

1 In the hierarchy, click the name of the pool for which you want the report.

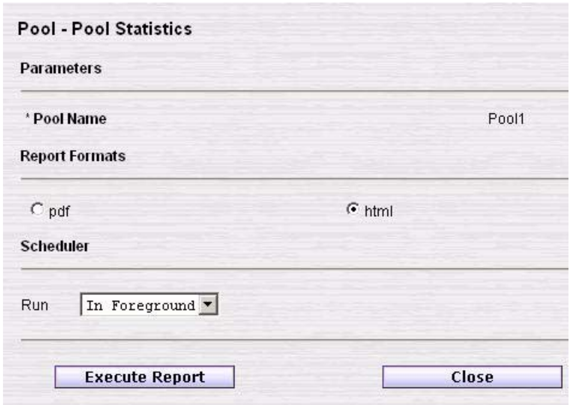
Result: The Pool Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Statistics** link.

Result: The Pool Statistics Report page opens in the Report Execution window.



4 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

5 Choose when to run the report in the **Scheduler** section. Refer to “Schedule a report” (p. 29-6) for more information.

6 Click **Execute Report**.

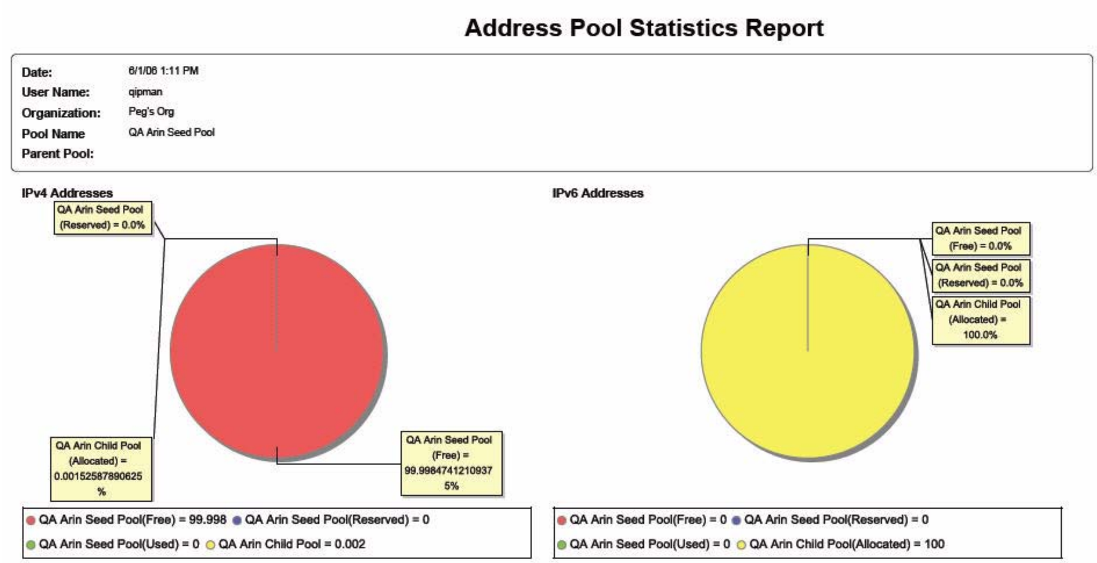
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to “View scheduled jobs” (p. 30-3) for more information.

END OF STEPS

Report format

The Pool Statistics report appears as follows. The charts on this report show the usage statistics for all IPv4 and IPv6 addresses. Each pie chart has both a label on the chart and a legend below it that show the proportion of Free, Reserved and Used blocks, and blocks allocated to child pools.

Figure 29-5 Sample Pool Statistics report



The following table describes the fields on the report.

Table 29-7 Pool Statistics report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the pool is located
Pool Name	Pool that is the subject of this report.
Parent Pool	Name of the parent pool for this pool. Blank indicates that the pool is a seed pool.

Produce a Pool Usage report

Purpose

This report provides the address usage information within a selected pool. Instructions are provided for access from the Reports hierarchy or from the Pool Properties page.

From the menu or toolbar

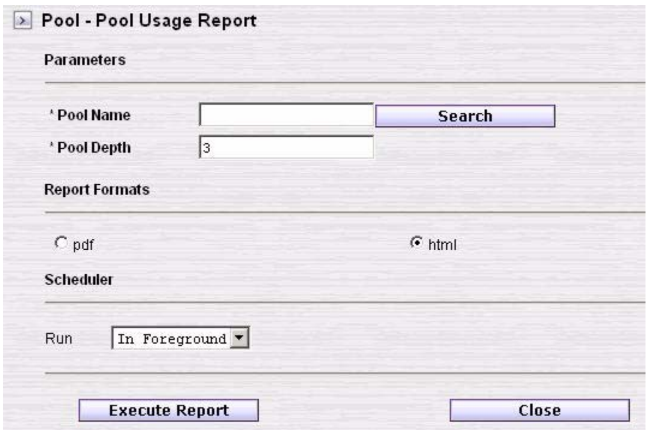
To produce a Pool Usage report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Allocation - Pool** section, click **Usage**.

Result: The Pool Usage Report page opens.



3 Click **Search**.

Result: The Pool or Block Search Criteria window opens. Refer to "Search for a pool" (p. 29-13) for further information.

4 Highlight the pool whose usage you wish to review and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected pool appears in the **Pool Name** field.

5 Enter the level of the pool hierarchy for which you want pool usage information. The default level is set to `3`.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Pool Properties page

To produce a Pool Usage report, follow these steps.

1 In the hierarchy, click the name of the pool for which you want the report.

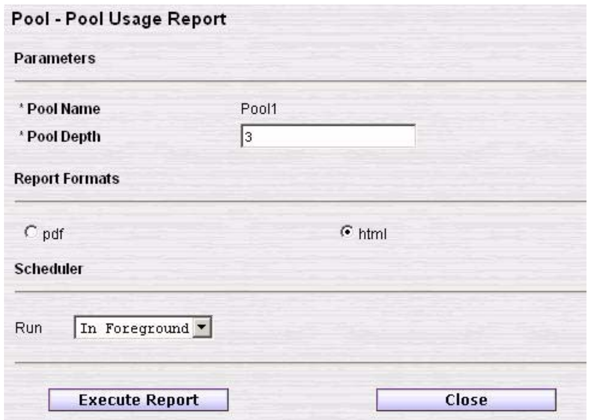
Result: The Pool Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Usage** link.

Result: The Pool Usage Report page opens in the Report Execution window.



4 Enter the level of the pool hierarchy for which you want pool usage information. The default level is set to **3**.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

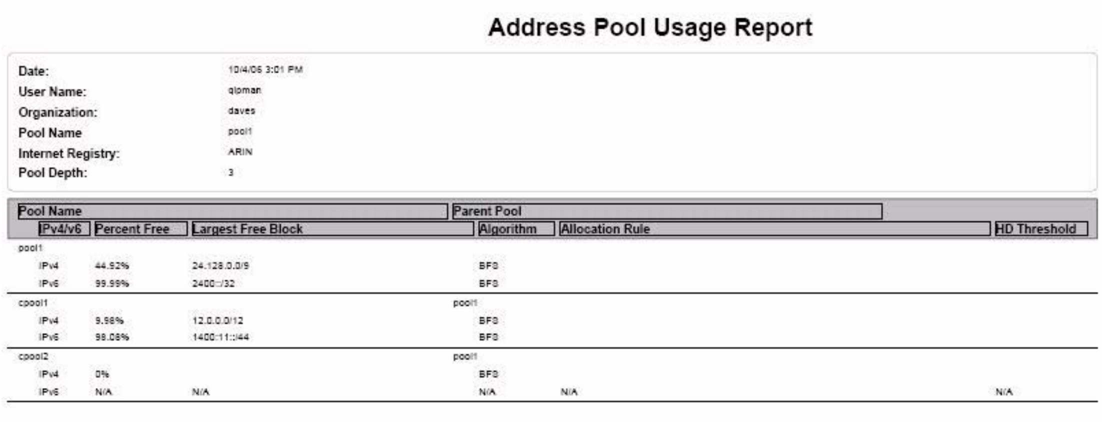
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Pool Usage report appears as follows.

Figure 29-6 Sample Pool Usage report



Address Pool Usage Report

Date: 10/4/06 3:01 PM
User Name: qloman
Organization: daves
Pool Name pool1
Internet Registry: ARIN
Pool Depth: 3

Pool Name				Parent Pool			
	IPv4/v6	Percent Free	Largest Free Block		Algorithm	Allocation Rule	HD Threshold
pool1							
	IPv4	44.92%	24.128.0.0/9		BFS		
	IPv6	99.99%	2400::/32		BFS		
cpool1				pool1			
	IPv4	9.98%	12.0.0.0/12		BFS		
	IPv6	98.08%	1400:11::/44		BFS		
cpool2				pool1			
	IPv4	0%			BFS		
	IPv6	N/A	N/A		N/A	N/A	N/A

The following table describes the fields on the report.

Table 29-8 Pool Usage report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the pool is located
Pool Name	Pool that is the subject of this report.
Internet Registry	Internet registry with which this pool is registered. Blank indicates the pool is not assigned to an Internet registry.
Pool Depth	The level of the pool hierarchy that this report covers.
Column headings	
Pool Name	Name of each pool or child pool down to the pool depth specified when the report was produced.
IPv4/v6	For each pool, there is line with IPv4 statistics and IPv6 statistics.
Free Space	Indicates the amount of free space available in the pool.
Largest Free Block	Address of the largest free block in the pool.
Parent Pool	Name of the parent pool for the pool statistics on a given line. Blank indicates that the pool is a seed pool.

Field	Description
Algorithm	Allocation algorithm used when creating the pool. Allowable values are: BFS: Best fit from start BFE: Best fit from end SPL: Sparse allocation
Allocation Rule	Name of the allocation rule, if applicable, that was used when creating the pool.
HD Threshold	When the Host Density (HD) ratio reaches this ratio, the user is notified. HD is calculated as follows: HD = log(number of allocated objects) / log(maximum number of allocatable objects)

Produce a Pool Free Space report

Purpose

This report provides free space information within a selected pool. Instructions are provided for access from the Reports hierarchy or from the Pool Properties page.

From the menu or toolbar

To produce a Pool Free Space report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Allocation - Pool** section, click **Free Space**.

Result: The Pool Free Space Report page opens.

3 Click **Search**.

Result: The Pool or Block Search Criteria window opens. Refer to "Search for a pool" (p. 29-13) for further information.

4 Highlight the pool whose free space you wish to review and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected pool appears in the **Pool Name** field.

5 Enter the level of the pool hierarchy for which you want pool free space information. The default level is set to `3`.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Pool Properties page

To produce a Pool Free Space report, follow these steps.

1 In the hierarchy, click the name of the pool for which you want the report.

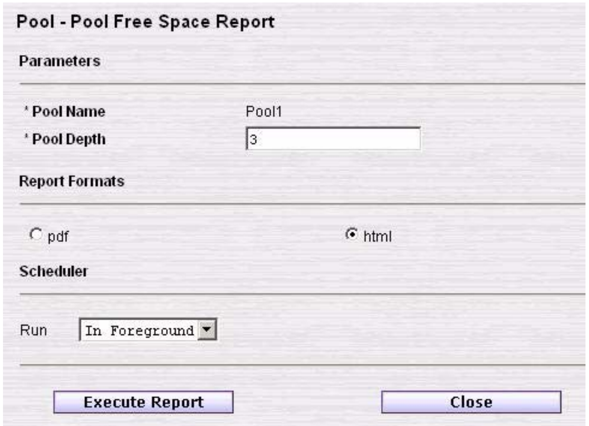
Result: The Pool Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **View Free Space** link.

Result: The Pool Free Space Report page opens in the Report Execution window.



4 Enter the level of the pool hierarchy for which you want pool free space information. The default level is set to **3**.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to “Schedule a report” (p. 29-6) for more information.

7 Click **Execute Report**.

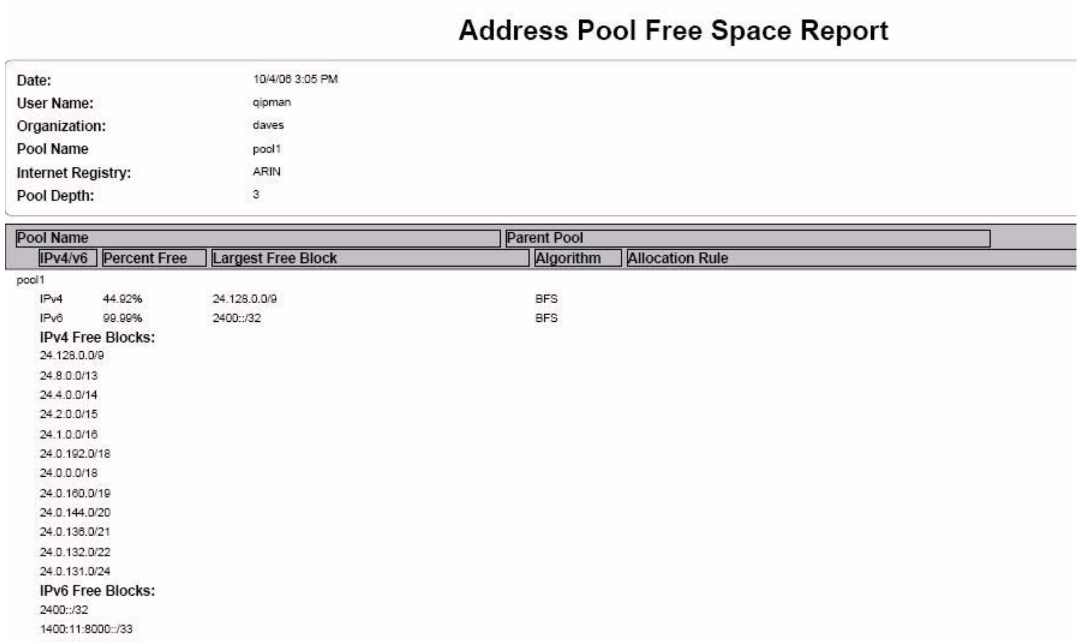
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to “View scheduled jobs” (p. 30-3) for more information.

END OF STEPS

Report format

The Pool Free Space report appears as follows.

Figure 29-7 Sample Pool Free Space report



Address Pool Free Space Report

Date: 10/4/06 3:05 PM
User Name: qipman
Organization: daves
Pool Name pool1
Internet Registry: ARIN
Pool Depth: 3

Pool Name				Parent Pool	
	IPv4/v6	Percent Free	Largest Free Block	Algorithm	Allocation Rule
pool1					
	IPv4	44.92%	24.128.0.0/9	BFS	
	IPv6	99.99%	2400::/32	BFS	

IPv4 Free Blocks:
24.128.0.0/9
24.8.0.0/13
24.4.0.0/14
24.2.0.0/15
24.1.0.0/16
24.0.192.0/18
24.0.0.0/18
24.0.160.0/19
24.0.144.0/20
24.0.136.0/21
24.0.132.0/22
24.0.131.0/24
IPv6 Free Blocks:
2400::/32
1400:11:8000::/33

The following table describes the fields on the report.

Table 29-9 Pool Free Space report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the pool is located
Pool Name	Pool that is the subject of this report.
Internet Registry	Internet registry with which this pool is registered. Blank indicates the pool is not assigned to an Internet registry.
Pool Depth	The level of the pool hierarchy that this report covers.
Column headings	
Pool Name	Name of each pool or child pool down to the pool depth specified when the report was produced.
IPv4/v6	For each pool, there is a line with IPv4 statistics and IPv6 statistics.
Free Space	Indicates the amount of free space available in the pool.
Largest Free Block	Address of the largest free block in the pool.

Field	Description
Parent Pool	Name of the parent pool for the pool statistics on a given line. Blank indicates that the pool is a seed pool.
Algorithm	Allocation algorithm used when the pool was created. Values are: BFS: Best fit from start BFE: Best fit from end SPL: Sparse allocation
Allocation Rule	Name of the allocation rule, if applicable, that was used when the pool was created.

Produce a Rule Summary report

Purpose

This report provides a list of all rules within an organization. Instructions are provided for access from the **Reports** hierarchy or the **Address Allocation** section of the Address Allocation hierarchy.

From the menu or toolbar

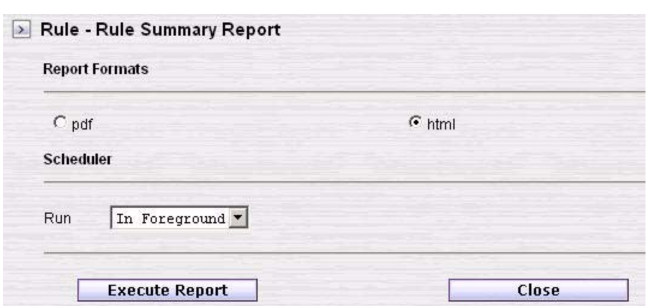
To produce a Rule Summary report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Allocation - Rule** section, click **Summary**.

Result: The Rule Summary Report page opens.



3 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

4 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

5 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From a Properties page

To produce a Rule Summary report on a rule in the Address Allocation hierarchy, follow these steps.

1 Select any rule in the hierarchy.

Result: The Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Summary** link.

Result: The Rule Summary Report page opens in the Report Execution window.

4 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

5 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

6 Click **Execute Report**.

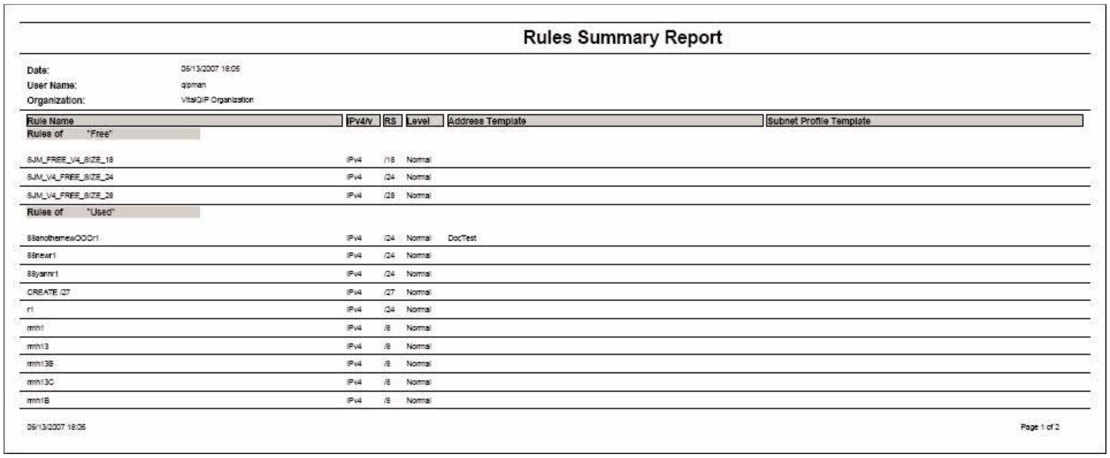
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Rules Summary report appears as follows.

Figure 29-8 Sample Rules Summary report


Rules Summary Report

Date: 06/13/2007 18:06
User Name: qipman
Organization: VitalQIP Organization

Rule Name	IPv4/v	RS	Level	Address Template	Subnet Profile Template
Rules of "Free"					
SJM_FREE_V4_SIZE_18	IPv4	/18	Normal		
SJM_V4_FREE_SIZE_24	IPv4	/24	Normal		
SJM_V4_FREE_SIZE_28	IPv4	/28	Normal		
Rules of "Used"					
88anothernewOOOr1	IPv4	/24	Normal	DocTest	
88newr1	IPv4	/24	Normal		
88yannr1	IPv4	/24	Normal		
CREATE /27	IPv4	/27	Normal		
r1	IPv4	/24	Normal		
rmh1	IPv4	/8	Normal		
rmh13	IPv4	/8	Normal		
rmh13B	IPv4	/8	Normal		
rmh13C	IPv4	/8	Normal		
rmh1B	IPv4	/8	Normal		

06/13/2007 18:06 Page 1 of 2

The following table describes the fields on the report. The report is sorted by rule type: Free, Used, Reserved, and Site. Additional information is displayed if a site rule has been defined.

Table 29-10 Rule Summary report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the rule is located.
Column headings for Free, Used, and Reserved	
Rule Name	Name of the rule.
IPv4/v6	Indicates the type of address block for which the rule is used.
RS	Requested Size. Indicates the length of the block to which the rule applies.
Level	Indicates the user level of the rule. Allowable values are as follows: • Normal • Advanced • Expert
Address Template	The address template, if applicable, assigned to this rule.
Subnet Profile Template	The subnet profile template, if applicable, assigned to this rule.
Additional column headings (second line) for Site	

Field	Description
Status	Indicates whether the status of the site rule is **Used** or **Reserved**.
Size	Indicates the length of the block to which the site rule applies.
Address Template	Address template with which the site rule is associated.
Subnet Profile Template	Subnet profile template with which the site rule is associated.

Address management reports

Overview

Purpose

The following reports are available from the **Address Management** section of the Reports hierarchy.

- IPv4 Objects
- IPv4 Subnets
- IPv4 Subnet Usage
- IPv6 Managed Addresses
- IPv6 Subnets
- Node Hierarchy

When accessed from the Reports hierarchy, you need to enter the search criteria to locate the item on which to report. For information on what criteria you may enter, refer to "Search for an IPv4 hierarchy item" (p. 29-49) and "Search for an IPv6 hierarchy item" (p. 29-67).

Search for an IPv4 hierarchy item

Purpose

Use this procedure to search for an item in the IPv4 hierarchy on which you wish to produce one of the IPv4 Object, IPv4 Subnet, IPv4 Network Audit, or IPv4 Subnet Organization Audit reports.

Before you begin

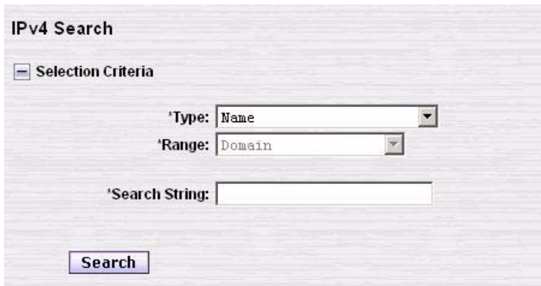
You can use the wildcard character (*) as part of the search string for all searches.

Procedure

To search for an item in the IPv4 hierarchy, follow these steps.

1 Select one of the IPv4 object or subnet reports in the Reports hierarchy and click **Search**.

Result: The IPv4 Search page opens.



2 Review the following table and fill in the fields you need to complete for your search.

Table 29-11 IPv4 search fields

Field	Description
Type	Select whether you are searching for a **Name**, an **Address**, or a **User-Defined Field** from the drop-down list.
Range	Displays the range for which you are searching. The values for this field vary depending on the type of report selected, or the value selected in the **Scope** field.
UDF Field Name	This field is only active if the **Type** is set to **User-Defined Field**. Select the name of any user-defined field from the drop-down list, or select **All** to search all user-defined fields.
User Defined Attributes	This field is only active if the **Type** is set to **User Defined Attributes**. • From the **Attribute Group** drop-down list, select the required attribute group. • From the **Attribute Name** drop-down list, select the required user-defined attribute. • In the **Attribute Value** field, enter text based on the item for which you are searching.
Search String	Enter text in this field based on the type of item for which you are searching. Allowable values are as follows: **Name** – Enter freeform text. You may use the wildcard character for 0 or more characters. **Address** – Enter a valid IP address. You can use the wildcard character, but each octet must be complete. For example 135.106.* is a valid search address. If you enter an invalid IP address, no matches are returned. **User-Defined Field** – Enter freeform text. You may use the wildcard character for 0 or more characters.

3 Click **Search**.

Result: The results appear in the **Search Results** list.

END OF STEPS

Produce an IPv4 Objects report

Purpose

Use this procedure to produce an IPv4 Objects report. Instructions are provided for access from the Reports hierarchy or from the Network, Domain, OSPF Area, Subnet Organization, and Subnet Properties pages. This report lists all the objects for a specific scope based on Object type, Status, User Defined Field value, and User Defined Attribute value.

Before you begin

- The **User Defined Fields** section is displayed if user defined fields are associated with the report.
- The **User Defined Attributes** section is displayed if user defined attributes are associated with the report.
- Only one user defined field can be used in a report.

From the menu or toolbar

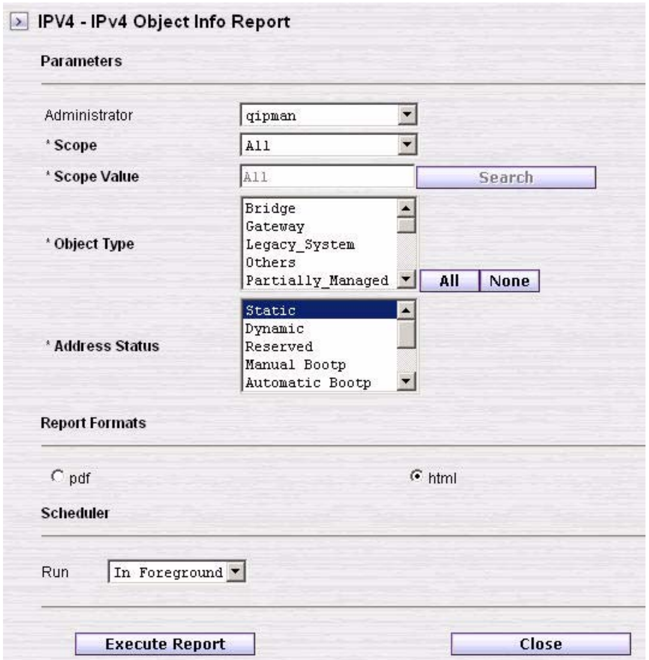
To produce an IPv4 Objects report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Management - IPv4** section, click **Object Info**.

Result: The IPv4 Object Info Report page opens.



3 Select an administrator name from the Administrator drop-down list. This list contains your user ID (default), the names of any other administrators whose information you are authorized to view, and a null selection.

4 Select a scope type from the **Scope** drop-down list. Possible choices are:

- All (only displays if you selected an administrator from the Adminstrator drop-down list)
- Domain
- Network
- OSPF Area
- Subnet Organization
- Subnet

5 Enter a value in the **Scope Value** field. To enter a value, you must click **Search** and select a value, you cannot enter it directly in the field. This field only displays if you accessed this screen from the reports menu rather than from a properties screen. This field has the value set to **All** if you selected an administrator from the Administrator drop-down menu.

6 Click **Search**.

Result: The IPv4 Search window opens. Refer to “Search for an IPv4 hierarchy item” (p. 29-49) for further information.

7 Highlight the required object and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected object appears in the **Scope Value** field.

8 Select the object types you wish to review from the **Object Type** list. You can select multiple object types by holding down the **Ctrl** or **Shift** keys as you click. You can also select all objects in the list by clicking **All**, or you can deselect all objects by clicking **None**.

9 Select the address type you wish to review from the **Address Status** list. You can select multiple types of address by holding down the **Ctrl** or **Shift** keys as you click.

10 Select **User Defined Attributes** or **User Defined Fields** to include either user defined attributes or user defined fields in the search query.

Refer to “Working with user defined attributes and fields” (p. 7-23) for more information on working with user defined attributes or fields.

11 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

12 Choose when to run the report in the **Scheduler** section. Refer to “Schedule a report” (p. 29-6) for more information.

13 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information. The output of the report depends on the selected scope.

END OF STEPS

From the Properties page

You can generate the IPv4 Object Info report from the Network, Domain, Subnet Organization, and Subnet Properties pages. The procedure for generating the IPv4 Object Info report is the same in all these pages.

To produce an IPv4 Object Info report on an item in the IPv4 hierarchy, follow these steps.

1 Select the item on which you want to report.

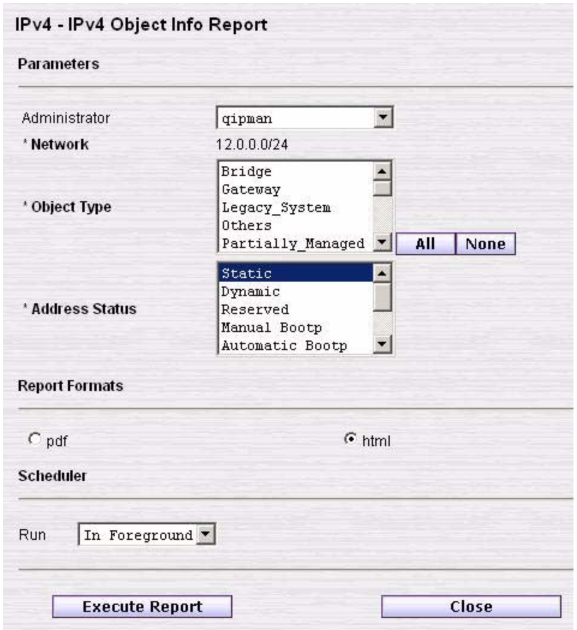
Result: The Properties page for the selected item opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Object Info** link.

Result: The IPv4 Object Info Report page opens in the Report Execution window. This page is generated from the Network Properties page.



4 Select an administrator name from the Administrator drop-down list. This list contains your user ID (default), the names of any other administrators whose information you are authorized to view, and a null selection.

5 Select the object types you wish to review from the **Object Type** list. You can select multiple object types by holding down the **Ctrl** or **Shift** keys as you click. You can select all objects in the list by clicking **All**. You can deselect all objects by clicking **None**.

6 Select the address type you wish to review from the **Address Status** list. You can select multiple types of address by holding down the **Ctrl** or **Shift** keys as you click.

7 Select **User Defined Attributes** or **User Defined Fields** to include either user defined attributes or user defined fields in the search query.

Refer to "Working with user defined attributes and fields" (p. 7-23) for more information on working with user defined attributes or fields.

8 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

9 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

10 Click **Execute Report**.

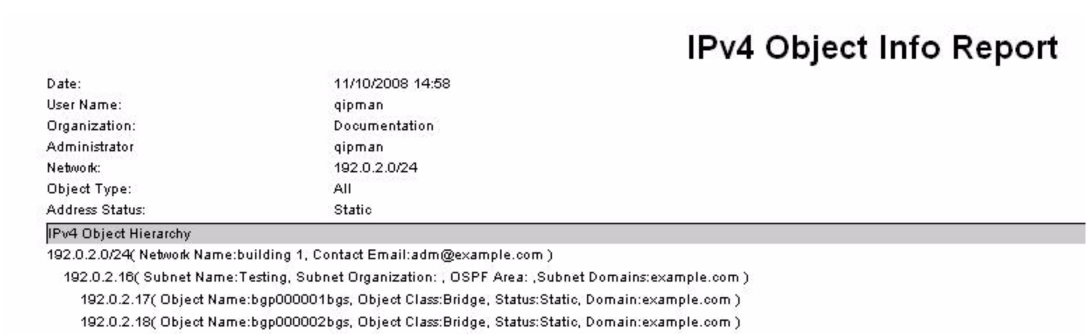
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

When invoked from the Subnet Properties page, the IPv4 Objects report appears as follows.

Figure 29-9 Sample IPv4 Objects report


IPv4 Object Info Report

Date:	11/10/2008 14:58
User Name:	qipman
Organization:	Documentation
Administrator	qipman
Network:	192.0.2.0/24
Object Type:	All
Address Status:	Static

IPv4 Object Hierarchy

192.0.2.0/24(Network Name:building 1, Contact Email:adm@example.com)
192.0.2.16(Subnet Name:Testing, Subnet Organization: , OSPF Area: ,Subnet Domains:example.com)
192.0.2.17(Object Name:bgp000001bgs, Object Class:Bridge, Status:Static, Domain:example.com)
192.0.2.18(Object Name:bgp000002bgs, Object Class:Bridge, Status:Static, Domain:example.com)

The following table describes the fields on the report.

Table 29-12 IPv4 Object Info report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located

Field	Description
Administrator	If selected when the report was generated, the name of the administrator whose IPv4 objects are on this report.
<Scope>	The domain that is the subject of this report. **Note:** This is actually the scope where the subnets/objects are queried. When you invoke this report from the Network Properties page for example, you see Network instead of Subnet in the report. Similarly for Domain, OSPF Area, and Subnet Organization.
Object Type	The types of object selected for this report.
Address Status	The status of the addresses selected for this report.

Produce an IPv4 Subnet Info report

Purpose

Use this procedure to produce an IPv4 Subnet Info report. Instructions are provided for access from the Reports hierarchy or from the Network, Domain, OSPF Area, and Subnet Organization. This report lists all the subnets for a specific scope based on Object type, Status, User Defined Field value, and User Defined Attribute value.

Before you begin

- The **User Defined Fields** section is displayed if user defined fields are associated with the report.
- The **User Defined Attributes** section is displayed if user defined attributes are associated with the report.
- Only one user defined field can be used in a report.

From the menu or toolbar

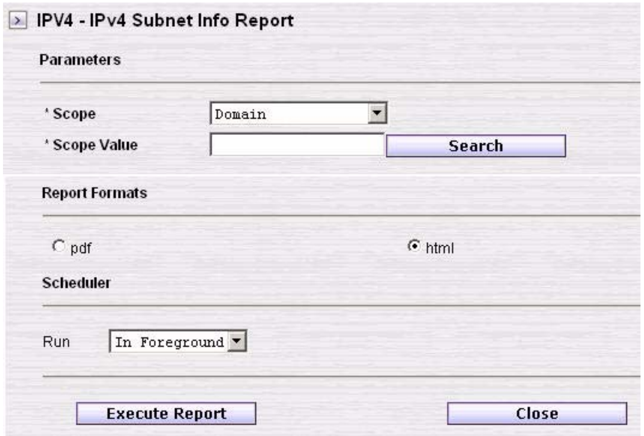
To produce an IPv4 Subnet Info report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Management - IPv4** section, click **Subnet Info**.

Result: The IPv4 Subnet Info Report page opens.



3 Select a scope type from the **Scope** drop-down list. Possible choices are:

- Domain
- Network
- OSPF Area
- Subnet Organization

4 Click **Search**.

Result: The IPv4 Search window opens. Refer to "Search for an IPv4 hierarchy item" (p. 29-49) for further information.

5 Highlight the required object and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected object appears in the **Scope Value** field.

6 Select **User Defined Attributes** or **User Defined Fields** to include either user defined attributes or user defined fields in the search query.

Refer to "Working with user defined attributes and fields" (p. 7-23) for more information on working with user defined attributes or fields.

7 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

9 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Subnet Properties page

To produce an IPv4 Subnet Info report on a subnet in the IPv4 hierarchy, follow these steps.

1 Select the network, domain, or subnet organization which you want to report.

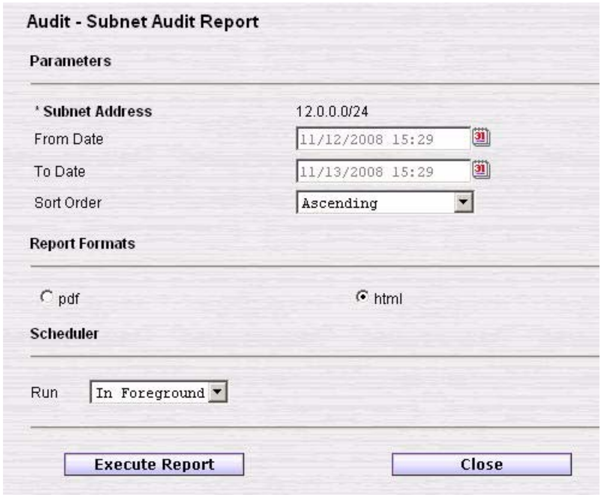
Result: The Properties page for the selected subnet opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Audit IPv4 Subnet** link.

Result: The Subnet Audit Report page opens in the Report Execution window.



4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

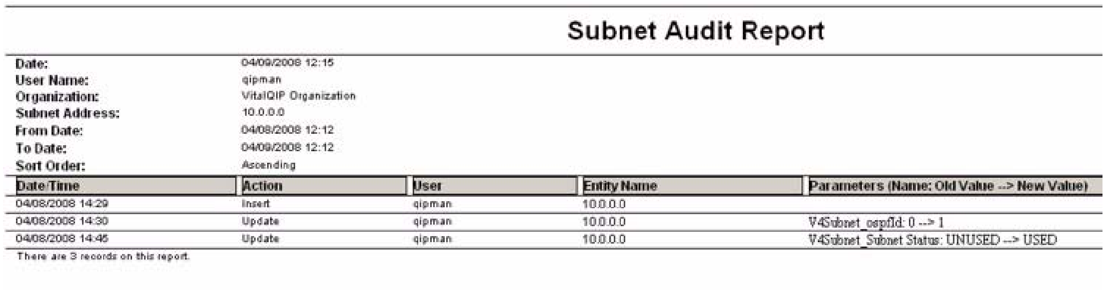
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

When invoked from the Subnet Properties page, the Subnet Audit report appears as follows.

Figure 29-10 Sample Subnet Audit report



Subnet Audit Report

Date:	04/09/2008 12:15
User Name:	qipman
Organization:	VitalQIP Organization
Subnet Address:	10.0.0.0
From Date:	04/08/2008 12:12
To Date:	04/09/2008 12:12
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
04/08/2008 14:29	Insert	qipman	10.0.0.0	
04/08/2008 14:30	Update	qipman	10.0.0.0	V4Subnet_ospfId: 0 --> 1
04/08/2008 14:45	Update	qipman	10.0.0.0	V4Subnet_Subnet Status: UNUSED --> USED

There are 3 records on this report.

The following table describes the fields on the report.

Table 29-13 Subnet Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
Subnet Address	The subnet that is the subject of this report. **Note:** This is actually the scope where the subnets/objects are queried. When you invoke this report from the Network Properties page for example, you see Network instead of Subnet in the report. Similarly for Domain, OSPF Area, and Subnet Organization.
From Date	Starting date for the subnet report date range.
To Date	Ending date for the subnet report date range.
Sort Order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.

Field	Description
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Produce an IPv4 Subnet Usage report

Purpose

Use this report to produce an IPv4 Subnet Usage report. Instructions are provided for access from the Reports hierarchy or from the Network Properties page.

From the menu or toolbar

To produce an IPv4 Subnet Usage report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Management - IPv4** section, click **Subnet Usage**.

Result: The IPv4 Subnet Usage Report page opens.

3 Click **Search**.

Result: The IPv4 Search window opens. Refer to "Search for an IPv4 hierarchy item" (p. 29-49) for further information.

4 Highlight the network on which you wish to report and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected network appears in the **Network** field.

5 Select **Free** or **Used** from the **Status** drop-down list.

- If **Free** is selected, the report lists subnets that can be created for the specified CIDR length and includes the count of free subnets as well as the percentage of free space that the subnets on the list will use up.
- If **Used** is selected, all subnets that are not free (that is, cannot be created) are listed.

6 Select the CIDR length from the **CIDR** drop-down list.

Note: CIDR is applicable only for Free status.

7 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

9 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From a Network Properties page

To produce an IPv4 Subnet Usage report on a network listed in the IPv4 (or MyView) hierarchy, follow these steps.

1 Select the network on which you want to report.

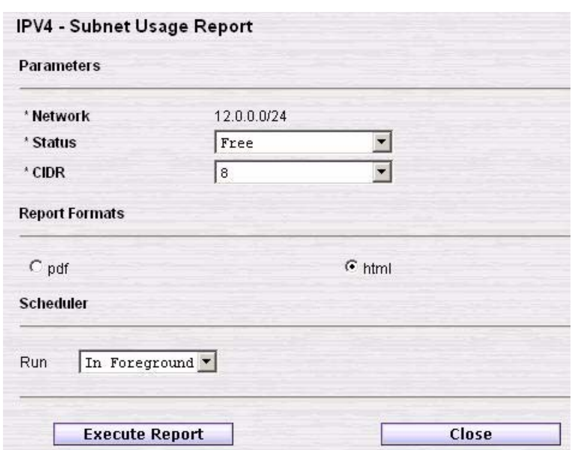
Result: The Properties page for the selected item opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Subnet Usage** link.

Result: The Subnet Usage Report page opens in the Report Execution window.



4 Select **Free** or **In Use** from the **Status** drop-down list.

- If **Free** is selected, the report lists subnets that can be created for the specified CIDR length and includes the count of free subnets as well as the percentage of free space that the subnets on the list will use up.
- If **In Use** is selected, all subnets that are not free (that is, cannot be created) are listed.

5 Select the desired CIDR length from the **CIDR** drop-down list.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

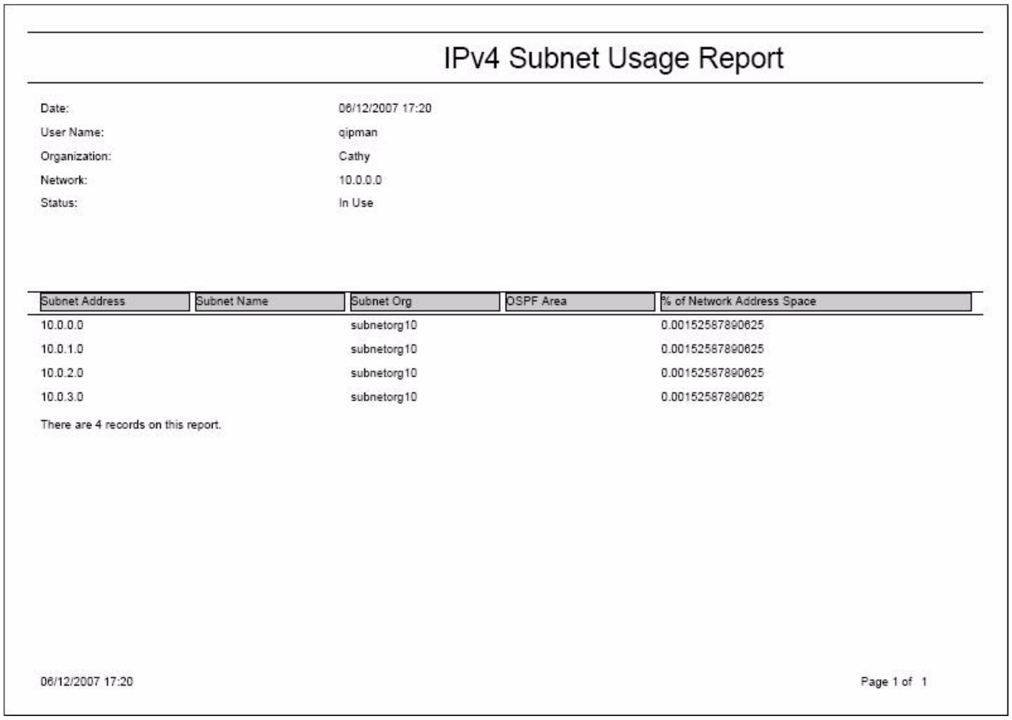
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Subnet Usage report appears as follows.

Figure 29-11 Sample Subnet Usage report - In Use Status



IPv4 Subnet Usage Report

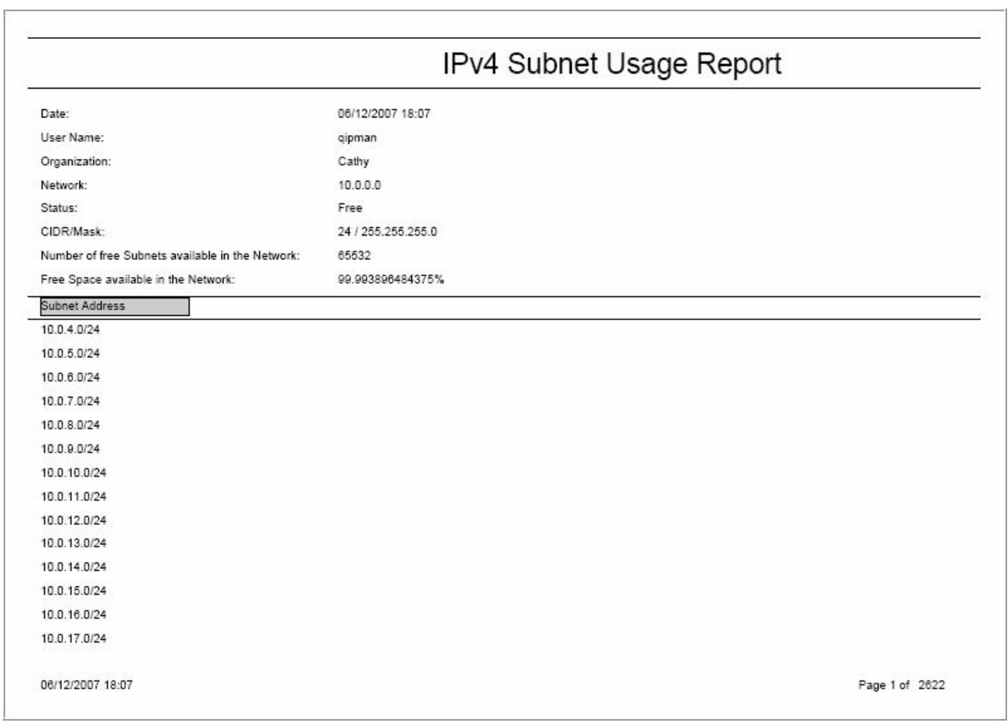
Date:	06/12/2007 17:20
User Name:	qipman
Organization:	Cathy
Network:	10.0.0.0
Status:	In Use

Subnet Address	Subnet Name	Subnet Org	OSPF Area	% of Network Address Space
10.0.0.0		subnetorg10		0.00152587890625
10.0.1.0		subnetorg10		0.00152587890625
10.0.2.0		subnetorg10		0.00152587890625
10.0.3.0		subnetorg10		0.00152587890625

There are 4 records on this report.

06/12/2007 17:20 Page 1 of 1

Figure 29-12 Sample Subnet Usage report - Free Status



IPv4 Subnet Usage Report

Date:	06/12/2007 18:07
User Name:	qipman
Organization:	Cathy
Network:	10.0.0.0
Status:	Free
CIDR/Mask:	24 / 255.255.255.0
Number of free Subnets available in the Network:	65532
Free Space available in the Network:	99.993896484375%

Subnet Address
10.0.4.0/24
10.0.5.0/24
10.0.6.0/24
10.0.7.0/24
10.0.8.0/24
10.0.9.0/24
10.0.10.0/24
10.0.11.0/24
10.0.12.0/24
10.0.13.0/24
10.0.14.0/24
10.0.15.0/24
10.0.16.0/24
10.0.17.0/24

06/12/2007 18:07 Page 1 of 2622

The following table describes the fields on the report.

Table 29-14 IPv4 Subnets report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
Network	The network that is the subject of this report.
Status	Indicates whether the status of the subnets are **In Use** or **Free**.
CIDR/Mask	***Appears if status is Free.*** Indicates the CIDR length and Mask of the subnets in this report.
Number of free Subnets available in the Network	***Appears if status is Free.*** Displays the number of free subnets that are available for the stated CIDR length.
Free Space available in the Network	***Appears if status is Free.*** Indicates the percentage of the total free space that the subnets on the report will use up.
Column heading (if Status is Free or In Use)	
Subnet Address	The address of the subnet that has a status of Used.
Column headings (If Status is in Use	
Subnet Name	The name of the subnet that has a status of Used.
Subnet Org	The subnet organization in which the used subnet is located.
OSPF Area	The OSPF Area in which the used subnet is located.
% of Network Address Space	Indicates the total address space in the used subnet as a percentage of the total address space in the network.

Search for an IPv6 hierarchy item

Purpose

Use this procedure to search for an IPv6 address or subnet when you wish to produce one of the IPv6 Subnet or Address reports.

Before you begin

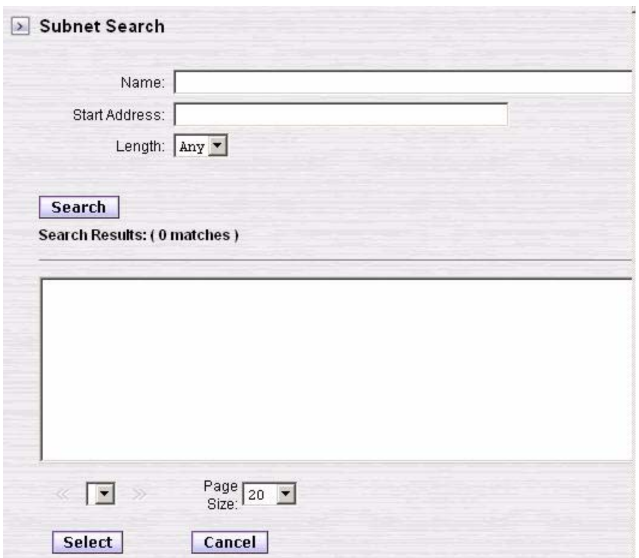
You can use the wildcard character (*) as part of the search string for all searches.

Procedure

To search for an item in the IPv6 hierarchy, follow these steps.

1 Select one of the IPv6 addresses or IPv6 subnet reports in the Reports hierarchy and click **Search**.

Result: The Subnet Search page opens.



2 Review the following table and fill in the fields you need to complete for your search.

Table 29-15 Subnet search fields

Field	Description
Name	***Optional***. Enter the IPv6 subnet name.
Start Address	***Optional***. Enter a valid IPv6 address.
Length	Select the length of the subnet for which you are searching from the drop-down list.

3 Click **Search**.

Result: The results appear in the **Search Results** list.

END OF STEPS

Produce an IPv6 Managed Addresses report

Purpose

This report provides address information within a selected subnet. Instructions are provided for access from the Reports hierarchy or from the IPv6 Hierarchy (or MyView Hierarchy if IPv6 seed blocks, subnets, and address ranges are present).

From the menu or toolbar

To produce an IPv6 Managed Addresses report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Management - IPv6** section, click **Managed Addresses**.

Result: The IPv6 Managed Addresses Report page opens.

3 Click **Search**.

Result: The Subnet Search window opens. Refer to "Search for an IPv6 hierarchy item" (p. 29-67) for further information.

4 Highlight the address on which you wish to report and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected address appears in the **Subnet Address** field.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From a Hierarchy Properties page

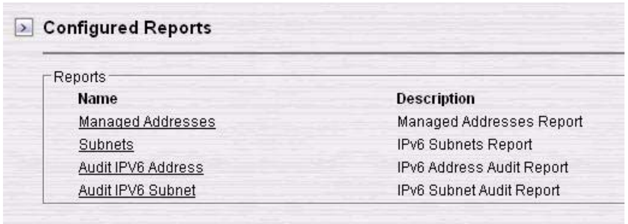
To produce an IPv6 Managed Addresses report on an address in the IPv6 (or MyView) hierarchy, follow these steps.

1 Select the IPv6 item (seed block, address range, or subnet) on which you want to report.

Result: The Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.



3 Click the **Managed Addresses** link.

Result: The IPv6 Managed Addresses Report page opens in the Report Execution window.

4 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

5 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

6 Click **Execute Report**.

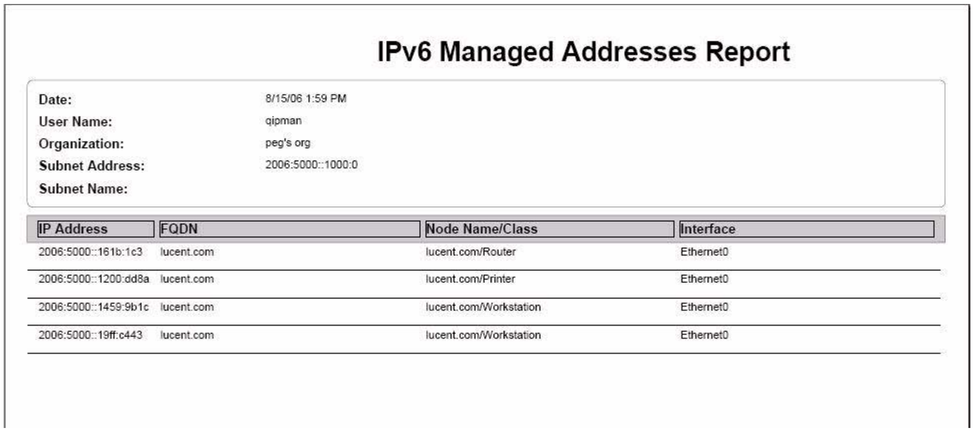
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The IPv6 Managed Addresses report appears as follows.

Figure 29-13 IPv6 Managed Addresses report



IPv6 Managed Addresses Report

Date: 8/15/06 1:59 PM
User Name: qipman
Organization: peg's org
Subnet Address: 2006:5000::1000:0
Subnet Name:

IP Address	FQDN	Node Name/Class	Interface
2006:5000::161b:1c3	lucent.com	lucent.com/Router	Ethernet0
2006:5000::1200:dd8a	lucent.com	lucent.com/Printer	Ethernet0
2006:5000::1459:9b1c	lucent.com	lucent.com/Workstation	Ethernet0
2006:5000::19ff:c443	lucent.com	lucent.com/Workstation	Ethernet0

The following table describes the fields on the report.

Table 29-16 IPv6 Managed Addresses report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the subnet is located.
Subnet Address	IP address of the subnet that is the subject of this report.
Subnet Name	Name of the subnet, if one is assigned.
Column headings	
IP Address	IPv6 address that is assigned to an object or node within the subnet.
FQDN	Fully qualified domain name to which the subnet is allocated.
Node Name/Class	Name of the node and its user class.
Interface	Name of any interfaces associated with the node.

Produce an IPv6 Subnets report

Purpose

This report provides subnet information about a selected IPv6 subnets. Instructions are provided for access from the Reports hierarchy or from the IPv6 hierarchy (or MyView hierarchy if IPv6 seed blocks, subnets, and address ranges are present).

From the menu or toolbar

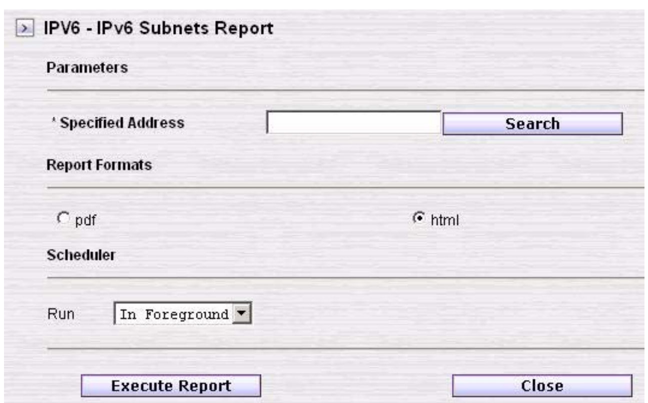
To produce an IPv6 Subnets report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Management - IPv6** section, click **Subnets**.

Result: The IPv6 Subnets Report page opens.



3 Click **Search**.

Result: The Subnet Search window opens. Refer to "Search for an IPv6 hierarchy item" (p. 29-67) for further information.

4 Highlight the address on which you wish to report and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected address appears in the **Specified Address** field.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From a Hierarchy Properties page

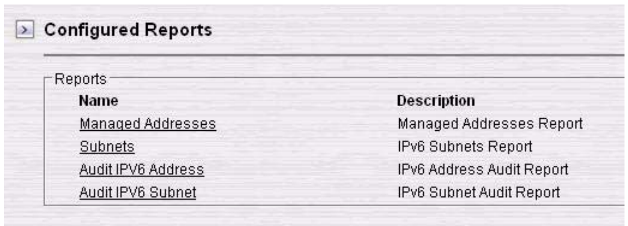
To produce an IPv6 Subnets report on an address in the IPv6 (or MyView) hierarchy, follow these steps.

1 Select the IPv6 item (seed block, address range, or subnet) on which you want to report.

Result: The Properties page opens.

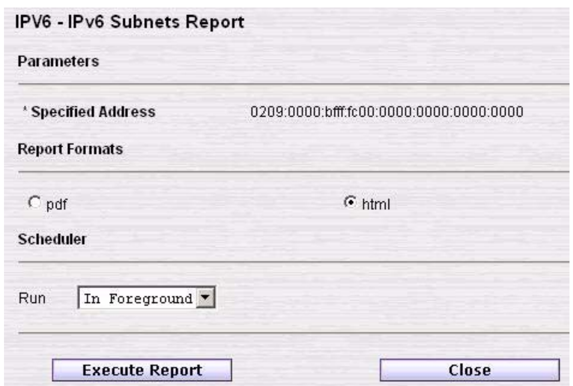
2 Click **Reports**.

Result: The Configured Reports page opens.



3 Click the **Subnets** link.

Result: The IPv6 Subnets Report page opens in the Report Execution window.



4 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

5 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

6 Click **Execute Report**.

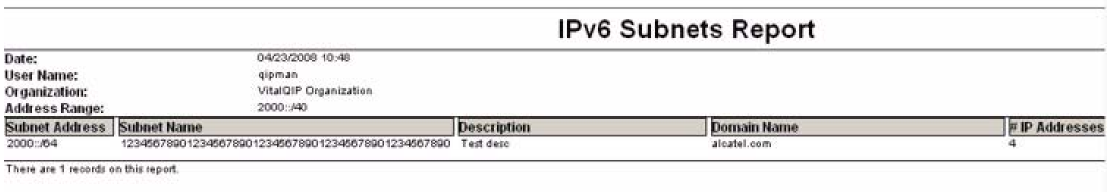
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The IPv6 Subnets report appears as follows.

Figure 29-14 IPv6 Subnets report



The following table describes the fields on the report.

Table 29-17 IPv6 Subnets report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the seed block is located.
Address Range	Address range that is the subject of this report.
Column headings	
Subnet Address	IPv6 address and prefix of the subnet.
Subnet Name	Name of the subnet.
Description	Description, if entered, of the subnet.
Domain Name	Domain with which the subnet is associated.
# IP Addresses	Number of nodes or objects contained within the subnet.

Produce a Node Hierarchy report

Purpose

This report provides address information about a selected node's hierarchy. Instructions are provided for access from the Reports hierarchy or from the Node Properties page.

From the hierarchy or toolbar

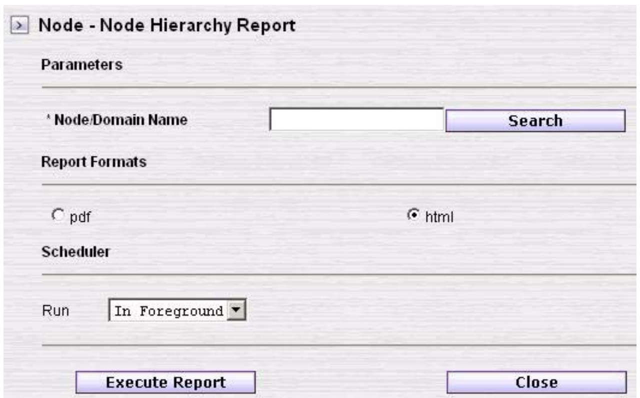
To produce a Node Hierarchy report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Address Management - Node** section, click **Hierarchy**.

Result: The Node Hierarchy Report page opens.



.

3 Click **Search**.

Result: The Node Search window opens. Refer to "Search for a node" (p. 11-3) for further information.

4 Highlight the node on which you wish to report and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected pool appears in the **Node/Domain Name** field.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Node Properties page

To produce a Node Hierarchy report, follow these steps.

1 In the hierarchy, click the name of the node for which you want the report.

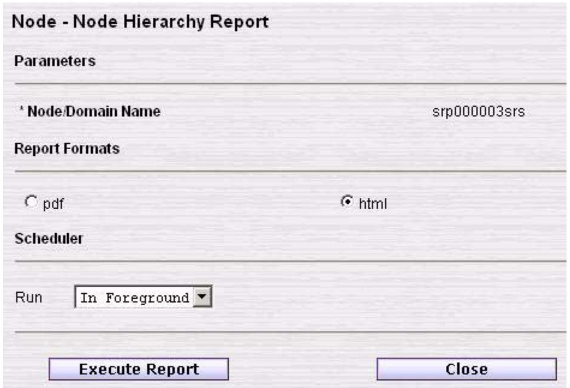
Result: The Node Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Hierarchy** link.

Result: The Node Hierarchy Report page opens in the Report Execution window.



4 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

5 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

6 Click **Execute Report**.

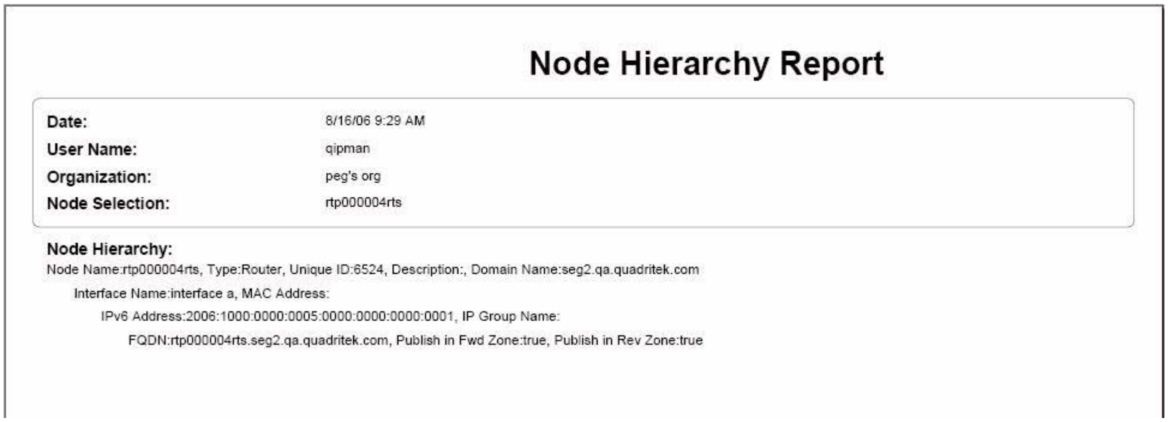
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Node Hierarchy report appears as follows.

Figure 29-15 Sample Node Hierarchy report



Node Hierarchy Report

Date:	8/16/06 9:29 AM
User Name:	qipman
Organization:	peg's org
Node Selection:	rtp000004rts

Node Hierarchy:

Node Name:rtp000004rts, Type:Router, Unique ID:6524, Description:, Domain Name:seg2.qa.quadritek.com

Interface Name:interface a, MAC Address:

IPv6 Address:2006:1000:0000:0005:0000:0000:0000:0001, IP Group Name:

FQDN:rtp000004rts.seg2.qa.quadritek.com, Publish in Fwd Zone:true, Publish in Rev Zone:true

The following table describes the fields on the report.

Table 29-18 Node Hierarchy report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the node is located.
Node Selection	Name of the node whose hierarchy information is displayed.
Node Hierarchy fields	
Node Name	Name assigned to the node when it was created.
Type	Type of hardware (workstation, router, printer, and so on).
Unique ID	Identification number assigned to the node.
Description	Text description assigned to the node, if entered.
Domain Name	Domain name assigned to the node.
Interface Name	Name assigned to each interface contained within the node.
MAC Address	MAC address assigned to each interface contained within the node.
IPv6 Address	IPv6 address assigned to each interface contained within the node.
IP Group Name	Name of the subnet where this node resides.
FQDN	Fully qualified domain name of the node within its domain name.

Field	Description
Publish in Forward Zone	Publish a forward zone record for this domain name in DNS.
Publish in Reverse Zone	Publish a reverse zone record for this domain name in DNS.

DHCP Server reports

Overview

Purpose

The following reports are available from the **DHCP Server** section of the Reports hierarchy.

- Profile
- Utilization

Produce a DHCP Server Profile report

Purpose

Use this procedure to produce a DHCP Server Profile report. The DHCP Server Profile report lists the DHCP parameters configured for a selected DHCP server, its managed objects, and the associated MAC pool and then produces a report.

The DHCP Server Profile report can list the information in an expanded or compressed format.

Procedure

To produce an DHCP Server Profile report, follow these steps.

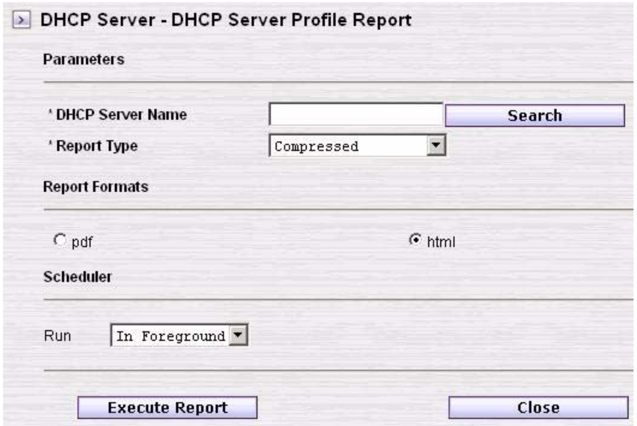
1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **DHCP, DHCP Server** section, click **Profile**.

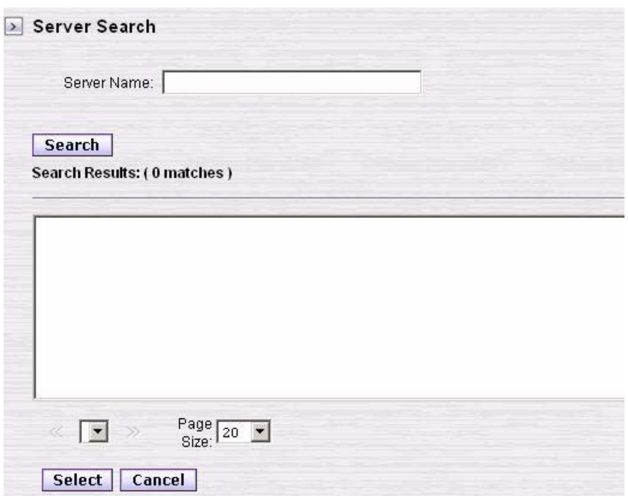
Result: The DHCP Server Profile report opens.

Note: This report is also accessble from the DHCP Server properties screen by clicking **Reports**.



3 Click Search to enter a DHCP server name. You must click Search to enter a value, you cannot enter it directly.

Result: The Server Search window opens.



4 Type a DHCP server name in the **Server Name** field. You can use an asterisk as a wildcard.

5 Click **Search**.

Result: A list of matching DHCP servers displays in the **Search Results** window.

6 Click a DHCP server, and then click **Select**.

Result: The Server Search window closes and the DHCP server you selected displays in the DHCP Server Profile Report page.

7 Select a report type from the **Report Type** drop-down menu. Allowable values are **Compressed** and **Expanded**.

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

9 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The DHCP Server Profile report appears as follows.

Figure 29-16 DHCP Server Profile Report - Expanded

```
  DHCP Server Profile Report

Date:  10/20/2008 11:02
User Name:  qipman
  Organization: Server Audit
DHCP Server Name:  eastcoast1.test.domain.com
Report Type  Expanded

DHCP Server Records

Server Name    -->   eastcoast1.test.domain.com
Accept Client Names    -->   True
Additional Policies
Client Class
```

```
DHCP Template    -->   general
Debug Information
           Debug    -->   None
           DebugFile    -->   dhcpd.log
           MaxDebugFileSize    -->   -1
Default Directory    -->   E:\qip72sp1\dhcp
Failover Server Type    -->   Standalone/Primary
           CtlReqRetryMax    -->   3
           PollDelay    -->   60
           SyncBindRetryMax    -->   3
           SyncBindingBufSize    -->   1024
           Use Failover Server    -->   False
           WaitCtlRetSecs    -->   5
           WaitSyncBindAckSecs    -->   5
           WaitSyncBindUpdateSecs    -->   15
Managed Range    -->   Network
           Managed Network List    -->   56
Remote Server Proxy
           Description
Scheduled Automatic Updates    -->   None
Support Bootp    -->   True
Use Server Policy Template    -->   False
           DHCP Server Policies
                      AckRenewForUnusedAddress    -->   False
                      ActiveLeaseExpiration    -->   Off
                      Bootfile    -->   Default
                      CheckTransactionID    -->   False
                      ClientHostNameProcessing    -->   Ignore
                      CompressedLog    -->   False
                      DefaultDescentThreshold    -->   0
                      DefaultLease    -->   7776000
                      DefaultUnavailableThreshold    -->   0
                      DropAllDhcpInformPackets    -->   False
                      DropZeroMacAddressPackets    -->   True
                      Enable LDRM Interface
                                 UseLDRMCallout    -->   False
                      ExpireAllLeasesOnRestart    -->   True
                      ForceClass    -->   None
                      HonorRequestedLeaseTime    -->   True
                      HonorUnqualifiedBootfile    -->   False
                      InitRebootAddressShuffle    -->   Off
                      IssueDropUnknownClientTrap    -->   False
                      LeaseExpirationSleepTime    -->   60000
                      LeaveBootpParametersInOptions    -->   False
                      LogLeaseGrantAndRenew    -->   True
```

```
                    MacWarningsToEventLog    -->   False
                    MaxOutgoingDhcpMessageSize    -->   1024
                    MaxPendingSeconds    -->   10
                    MaxUnavailableTime    -->   86400
                    NackDhcpRequestsForDuplicates    -->   True
                    NakUnknownClients    -->   True
                    OfferOnlyApiRequestedAddress    -->   False
                    Option81Support    -->   Suppress
                    PadBootpReply    -->   True
                    PingAttempts    -->   1
                    PingBeforeManualBootp    -->   False
                    PingBeforeManualDhcp    -->   True
                    PingDelay    -->   0
                    PingRetention    -->   0
                    PingSendDelay    -->   0
                    RegisteredClientsOnly    -->   False
                    RenewAddressShuffle    -->   Off
                    RenewAddressShuffleMaxCount    -->   0
                    SearchDynamicFirst    -->   False
                    SendRequestedParamsOnly    -->   False
                    SendServerIdLast    -->   False
                    ShareAutoBootpAndDynDhcp    -->   False
                    SharedNetworkThresholdProcessing    -->   False
                    SupportAutoRelease    -->   True
                    SupportBootpAutoRelease    -->   True
                    SupportEncodingLongOptions    -->   False
                    SupportMultiUserClass    -->   False
                    SupportRelayAgentDeviceClass    -->   False
                    SupportRelayAgentOption    -->   True
                    SupportRelayAgentServerOverride    -->   False
                    SupportSubnetSelection    -->   False
                    ThresholdMonitorSleepTime    -->   60
                    Update QIP Operations
                               Autorelease    -->   True
                               Bootp    -->   True
                               Decline    -->   True
                               Delete    -->   True
                               Expiration    -->   True
                               Grant    -->   True
                               Release    -->   True
                               Renew    -->   True
                    UpdatePreclusionDuration    -->   0
                    ZeroCiAddr    -->   False
 Subnet Address: 80.0.1.0
 Subnet Mask: 255.255.255.0
```

```
Subnet Name:
Effective Domain:test.domain.com
Default Routers:
Subnet Mac Pool:
           Scope:
                   80.0.1.11          --80.0.1.15          general
  D-Dhcp                             3days 0hrs 0mints 0secs
  test.domain.com
Option Template:  general
           Domain Name    -->   Same as in Subnet Profile
           Domain Name Server    -->   Same as in Subnet Profile
           Router    -->   Same as in Subnet Profile
           Subnet Mask    -->   Same as in Subnet Profile
Server Mac Pool:
```

Figure 29-17 DHCP Server Profile Report - Compressed

```
DHCP Server Profile Report

 Date:  10/20/2008 11:07
 User Name:  qipman
   Organization: Server Audit
 DHCP Server Name:  eastcoast1.test.domain.com
 Report Type  Compressed

 DHCP Server Records

 Server Name    -->   eastcoast1.test.domain.com
 Subnet Address: 80.0.1.0
 Subnet Mask: 255.255.255.0
 Subnet Name:
 Effective Domain:test.domain.com
 Default Routers:
 Subnet Mac Pool:
            Scope:
                    80.0.1.11          --80.0.1.15          general
   D-Dhcp                             3days 0hrs 0mints 0secs
   test.domain.com
 Option Template:  general
            Domain Name    -->   Same as in Subnet Profile
            Domain Name Server    -->   Same as in Subnet Profile
            Router    -->   Same as in Subnet Profile
            Subnet Mask    -->   Same as in Subnet Profile
 Server Mac Pool:
```

Produce a DHCP Server Utilization report

Purpose

Use this procedure to produce a DHCP Server Utilization report. The DHCP Server Utilization report allows you to monitor the usage levels of a DHCP server on a network or subnet served by primary/standalone DHCP servers.

Procedure

To produce an DHCP Server Utilization report, follow these steps.

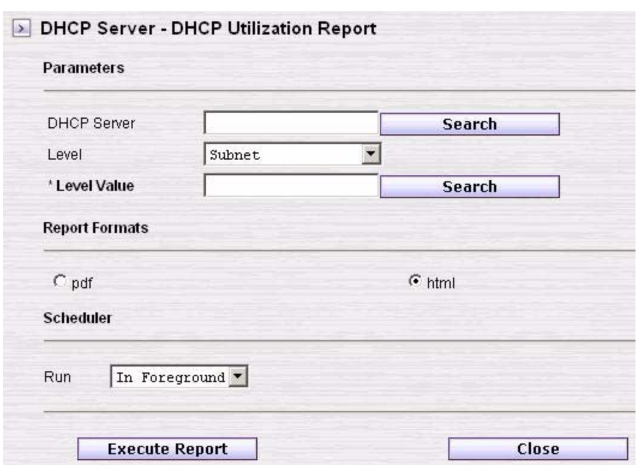
1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **DHCP, DHCP Server** section, click **Utilization**.

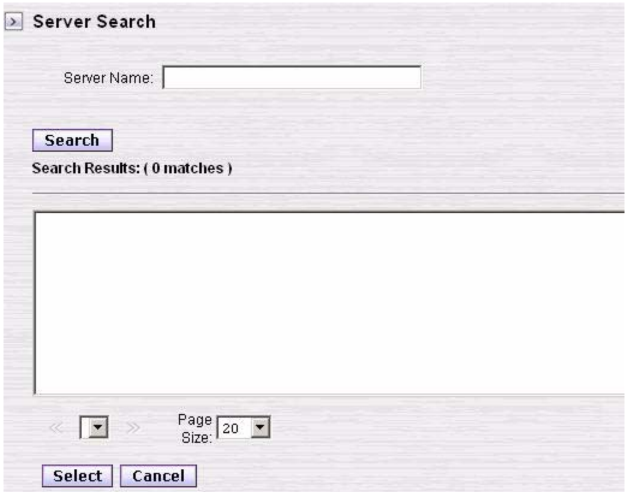
Result: The DHCP Server Utilization report opens.

Note: This report is also accessble from the DHCP Server properties screen the Network properties screen, the Scopes properties screen and the Subnet properties screen by clicking **Reports**.



3 Click **Search** to enter a DHCP server name. You must click **Search** to enter a value, you cannot enter it directly.

Result: The Server Search window opens.



4 Type a DHCP server name in the **Server Name** field. You can use an asterisk as a wildcard.

5 Click **Search**.

Result: A list of matching DHCP servers displays in the **Search Results** window.

6 Click a DHCP server, and then click **Select**.

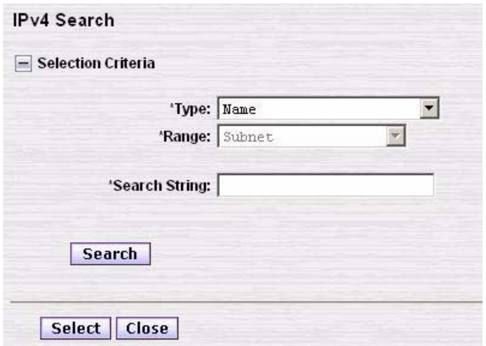
Result: The Server Search window closes and the DHCP server you selected displays in the DHCP Server Utilization Report page.

7 Select a level from the **Level** drop-down menu. Allowable values are **Subnet**, **Network**, and **All**.

Note: If you select **All**, you do not have to select a Level Value. At this point you can click the submit button and continue with Step 12.

8 Click **Search** to select a Level Value.

Result: The IPv4 Search screen opens.



9 Select a type from the **Type** drop-down menu. Allowable values are as follows:

- Name
- Address

Note: The range is not editable and corresponds to the value you selected in the **Level** field.

10 Enter a value in the Search String field and click Search.

Result: Matching values display on the lower half of the page.

11 Select a result by clicking its radio button and then click Select.

Result: The IPv4 Search window closes and the values you selected appear on the DHCP Server Utilization report.

12 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

13 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The DHCP Server Utilization report appears as follows.

Figure 29-18 DHCP Server Utilization report

```
DHCP Utilization Report

 Date:  10/20/2008 12:45
 User Name:  qipman
 Organization: Documentation
 DHCP Server Name:  cosmos.example.com
 NETWORK  128.10.0.0/24

 DHCP Utilization Records

DHCP Server ( Name: COSMOS) Scope: 192.168.0.25 - 192.168.0.28 (Object
   Type:D-Dhcp) [Active:0.0% Expired:0.0% Free:100.0% ] Scope: 192.168.0.30 -
   192.168.0.32 (Object Type:D-Dhcp) [Active:100.0% Expired:0.0% Free:0.0% ]
   Scope: 192.168.0.34 - 192.168.0.34 (Object Type:D-Dhcp) [Active:100.0%
   Expired:0.0% Free:0.0% ] Scope: 192.168.0.41 - 192.168.0.43 (Object
   Type:D-Dhcp) [Active:66.67% Expired:0.0% Free:33.33% ] Scope: 192.168.0.46
   - 192.168.0.46 (Object Type:M-Dhcp) [Active:100.0% Expired:0.0% Free:0.0%
   ] DHCP Server COSMOS Summary:[ Active:0% Expired:0% Free:0% ]
```

The following table describes the fields on the report.

Table 29-19 DHCP Utilization report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the node is located.
DHCP Server Name	Name of the DHCP server whose information is generated.
Level	Network or subnet whose utilization is being generated.
DHCP Utilization Records	
DHCP Server Name	Name of the DHCP server whose information is generated.

Field	Description
DHCP Server Summary	List of the Active, Expired, and Free addresses on the DHCP server, network or subnet.

DNS reports

Overview

Purpose

The following reports are available from the **DNS** section of the Reports hierarchy.

- ACL Template Usage
- Resource Record

When accessed from the Reports hierarchy, you need to enter search criteria to locate the item on which to report. For information on what criteria you may enter, refer to "Search for an ACL Template" (p. 29-93)

Search for an ACL Template

Purpose

Use this procedure to search for an ACL Template when you wish to produce an ACL Template Usage report.

Before you begin

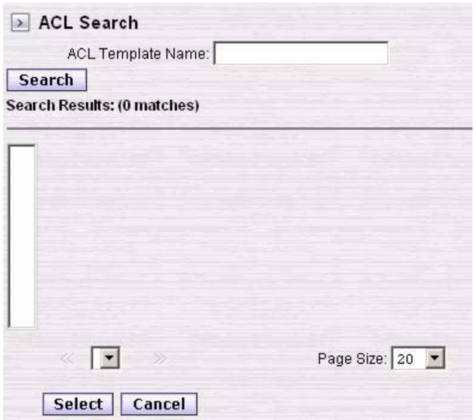
You can use the wildcard character (*) as part of the search string for all searches.

Procedure

To search for an ACL Template, follow these steps.

1 Select an ACL Template Usage report in the Reports hierarchy and click **Search**.

Result: The ACL Search page opens.



2 Enter the name of the ACL Template for which you are searching in the **ACL Template Name** field. This field is case-sensitive. You can enter a partial name followed by an asterisk (*) as a wildcard, or leave the field blank to search all ACL Templates.

3 Click **Search**.

Result: The results appear in the **Search Results** list.

END OF STEPS

Produce an ACL Template Usage report

Purpose

Use this procedure to produce an ACL Template Usage report. ACL Templates are associated with:

- ACL Template
- Zone
- Reverse zone
- DNS View
- View specific zone
- Shared zone
- Shared reverse zone

- Zone server
- Reverse zone server
- View specific zone server
- Shared zone server
- Shared reverse zone server

From the menu or toolbar

To produce an ACL Template Usage report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **DNS - ACL Template** section, click **ACL Template Usage**.

Result: The ACL Template Usage report opens.

3 Click **Search**.

Result: The ACL Search window opens. Refer to "Search for an ACL Template" (p. 29-93) for further information.

4 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

5 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

6 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the ACL Template Properties page

To produce a ACL Template Usage report on a ACL Template in the hierarchy, follow these steps.

1 Select the ACL Template on which you want to report.

Result: The ACL Template Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **ACL Template Usage** link.

Result: The ACL Template Usaget Report page opens in the Report Execution window.

4 Click **Search**.

Result: The ACL Search window opens. Refer to "Search for an ACL Template" (p. 29-93) for further information.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The ACL Template Usage report appears as follows.

Figure 29-19 Sample ACL Template Usage report

ACL Template Usage Report

Date:	04/10/2008 10:12
User Name:	qipman
Organization:	VitalQIP Organization
ACL Template Name:	TestAclTemp

Type	Name	Server	View
Domain	Alcatel.Com		
Domain	TestZone		
Domain Server	lucent.com	test.lucent.com	
Domain Server	Alcatel.Com	test.Alcatel.Com	
ACL Template	New_ACL_Template		
ACL Template	TestTemplate		
ACL Template	myAclTemplate		
ACL Template	oldTemplate		
View	SecondView		
View Specific Zone	SpecificZone		TestDNSViewChnaged
Shared Forward Zone	TestZone		SecondView
V4 Reverse Zone	0.0.10.in-addr.arpa		

There are 12 records on this report.

The following table describes the fields on the report.

Table 29-20 ACL Template Usage report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the ACL template is located.
ACL Template Name	Name of the ACL Template.
Column headings	
Type	Infrastructure type where the ACL is used. For e.g., ACL, Zone, Reverse Zone, View, and so on.
Name	Name of the ACL, Zone, Reverse Zone, View, and so on that use the ACL.
Server	The Zone-Server combination that uses the ACL.
View	The View options that have an ACL or the zone that is part of a view.

Produce a Resource Record report

Purpose

Use this procedure to produce a Resource Record report. The Resource Record report searches the owner and data fields of resource records defined in an object, zone, or reverse zone.

From the menu or toolbar

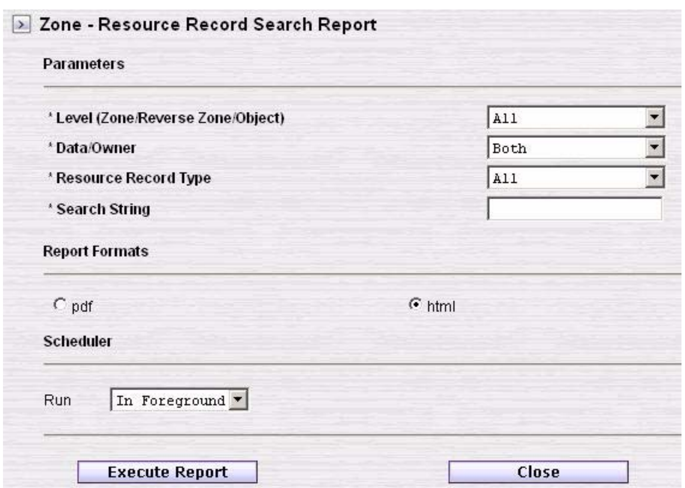
To produce a Resource Record report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **DNS - Zone** section, click **Resource Record**.

Result: The Resource Record report opens.



3 Review the following table and fill in the fields you need to complete for your search.

Table 29-21 Resource Record Report fields

Field	Description
Level	Specifies the level of the resource record. The options are: • All (Default) • Zone • IPv4 Reverse Zone • IPv6 Reverse Zone • Object
Field	Specifies the resource record field to be searched. The options are: • Both (Default) • Owner • Data
Resource Record Type	Specifies the type of the resource record. The options are: • All (Default) • A • CName • MX • NAPTR • NS • PTR • TXT • WKS • AAAA • AFSDB • MB • MG • MINFO • MR • ISDN • SRV • X25
Search String	Enter text in this field based on the type of item for which you are searching.

4 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

5 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

6 Click **Execute Report**.

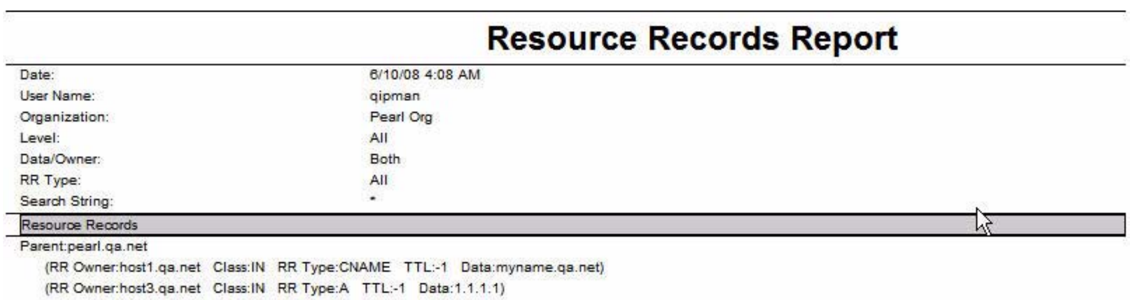
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Resource Record report appears as follows.

Figure 29-20 Sample Resource Record report



Resource Records Report

Date:	6/10/08 4:08 AM
User Name:	qipman
Organization:	Pearl Org
Level:	All
Data/Owner:	Both
RR Type:	All
Search String:	*

Resource Records

Parent:pearl.qa.net

(RR Owner:host1.qa.net Class:IN RR Type:CNAME TTL:-1 Data:myname.qa.net)

(RR Owner:host3.qa.net Class:IN RR Type:A TTL:-1 Data:1.1.1.1)

The following table describes the fields on the report.

Table 29-22 Resource Record report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the resource record is located.
Level	The level of the resource record.
Data/Owner	Resource Record field that is searched.
RR Type	Type of the Resource Record.
Search String	Indicates the search text based on the type of item being searched.

Produce a Resource Record by zone report

Purpose

Use this procedure to produce a Resource Record by zone report. The Resource Record by zone report lists either all or just the selected Resource Record type for a specific selected forward or reverse zone and view-specific or shared zone. It also includes zone extensions..

From the menu or toolbar

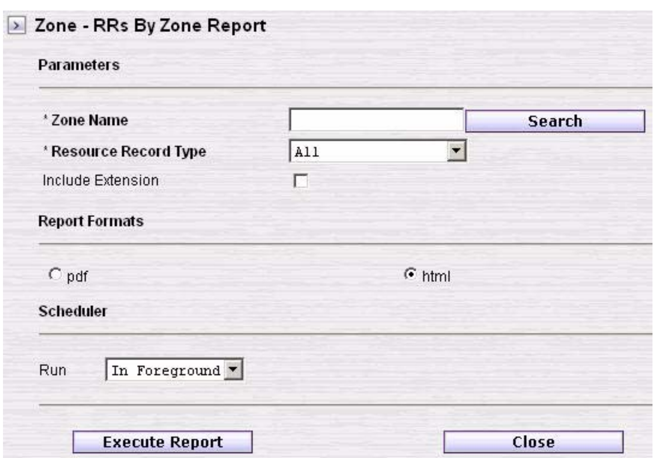
To produce a Resource Record by zone report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **DNS - Zone** section, click **RRs by Zone**.

Result: The RRs By Zone Report page opens.



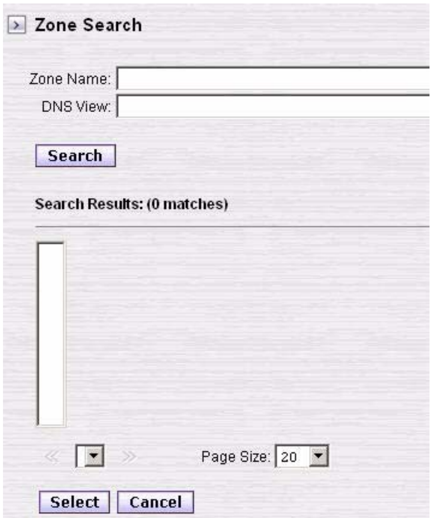
3 Review the following table and fill in the fields you need to complete for your search.

Table 29-23 Resource Records by Zone Report Fields

Field	Description
Zone Name	Click Search to enter a zone name. You must click Search to enter a value, you cannot enter it directly. Allowable values are Any Forward Zone, Reverse Zone, View Specific Zone or Shared Zone.
Resource Record Type	Allowable values are as follows: • All (Default) • A • CName • MX • NAPTR • NS • PTR • TXT • WKS • AAAA • AFSDB • MB • MG • MINFO • MR • ISDN • SRV • X25
Include Extension	Allowable values are as follow:s **False** (Default) (Unchecked) **True** (Checked)

4 Click Search.

Result: The Zone Search window opens.



5 Type a zone name in the **Zone Name** field. You can use an asterisk as a wildcard.

6 Select either **None** or **Any** from the **DNS View** drop-down menu.

7 Click **Search**.

Result: A list of matching zones displays in the **Search Results** window.

8 Click a zone, and then click Select.

Result: The Zone Search window closes and the zone you selected displays in the RRs By Zone Report page.

9 Select a Resource Record type from the **Resource Record Type** drop-down menu.

10 Either check, or leave unchecked, the **Include Extension** checkbox.

11 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

12 Click **Execute Report**.

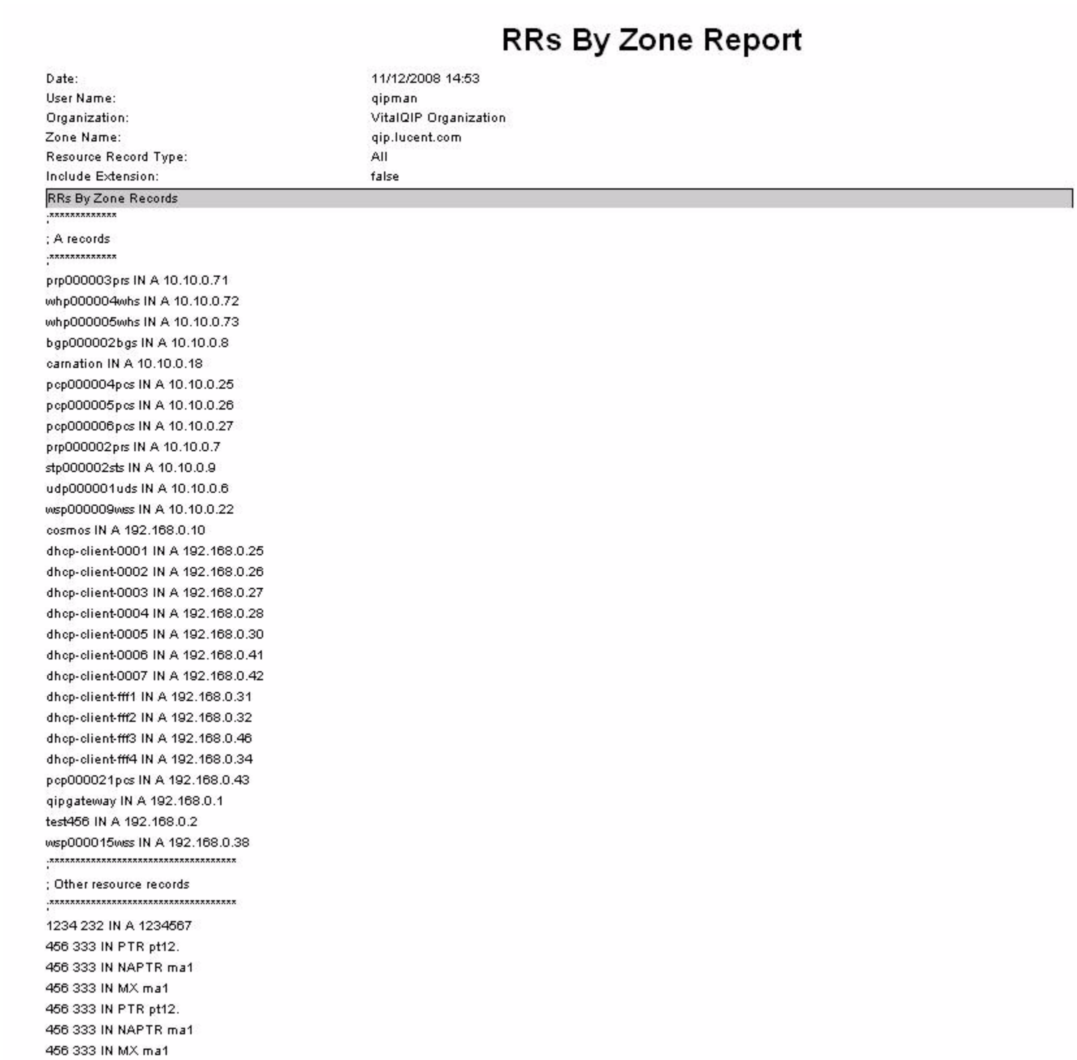
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Resource Record by zone report appears as follows.

Figure 29-21 Sample Resource Records by Zone report



RRs By Zone Report

Date:	11/12/2008 14:53
User Name:	qipman
Organization:	VitalQIP Organization
Zone Name:	qip.lucent.com
Resource Record Type:	All
Include Extension:	false

RRs By Zone Records

```
;*************
; A records
;*************
prp000003prs IN A 10.10.0.71
whp000004whs IN A 10.10.0.72
whp000005whs IN A 10.10.0.73
bgp000002bgs IN A 10.10.0.8
carnation IN A 10.10.0.18
pcp000004pcs IN A 10.10.0.25
pcp000005pcs IN A 10.10.0.26
pcp000006pcs IN A 10.10.0.27
prp000002prs IN A 10.10.0.7
stp000002sts IN A 10.10.0.9
udp000001uds IN A 10.10.0.6
wsp000009wss IN A 10.10.0.22
cosmos IN A 192.168.0.10
dhcp-client-0001 IN A 192.168.0.25
dhcp-client-0002 IN A 192.168.0.26
dhcp-client-0003 IN A 192.168.0.27
dhcp-client-0004 IN A 192.168.0.28
dhcp-client-0005 IN A 192.168.0.30
dhcp-client-0006 IN A 192.168.0.41
dhcp-client-0007 IN A 192.168.0.42
dhcp-client-fff1 IN A 192.168.0.31
dhcp-client-fff2 IN A 192.168.0.32
dhcp-client-fff3 IN A 192.168.0.46
dhcp-client-fff4 IN A 192.168.0.34
pcp000021pcs IN A 192.168.0.43
qipgateway IN A 192.168.0.1
test456 IN A 192.168.0.2
wsp000015wss IN A 192.168.0.38
;***********************************
; Other resource records
;***********************************
1234 232 IN A 1234567
456 333 IN PTR pt12.
456 333 IN NAPTR ma1
456 333 IN MX ma1
456 333 IN PTR pt12.
456 333 IN NAPTR ma1
456 333 IN MX ma1
```

The following table describes the fields on the report.

Table 29-24 Resource Record by zone report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the resource record is located.
Zone Name	Name of the zone that contains the resource records
Include Extension	Whether the extension was included when the report was produced.
RR Type	Type of the Resource Record.
Parent (Name/Address)	Name and IP address of the parent zone where the records reside.
Data	Content of the Resource Record

Infrastructure reports

Overview

Purpose

Infrastructure reports list changes that have occurred during a specified period to different elements of VitalQIP. The following reports are available from the **Infrastructure** section of the Reports hierarchy.

- Administrator Activity
- Administrator Generation Audit
- Administrator Profile Audit
- Administrative Role Audit
- Block Audit
- Domain Controller Generation Audit
- DHCP Server Generation Audit
- DNS Server Generation Audit
- DNS View Audit
- IPv4 Network Audit
- IPv4 Subnet Audit
- IPv4 Subnet Organization Audit
- IPv6 Address Audit
- IPv6 Subnet Audit
- Managed Files Audit
- MyView Audit
- Organization Audit
- Pool Audit
- Rule Audit
- MyView

The Administrator Activity report allows a master administrator to audit the activities of any administrator.

Produce an Administrator Activity Audit report

Purpose

Use this procedure to produce an Administrator Activity report. The Administrator Activity report allows a master administrator to audit the activities of any administrator.

Procedure

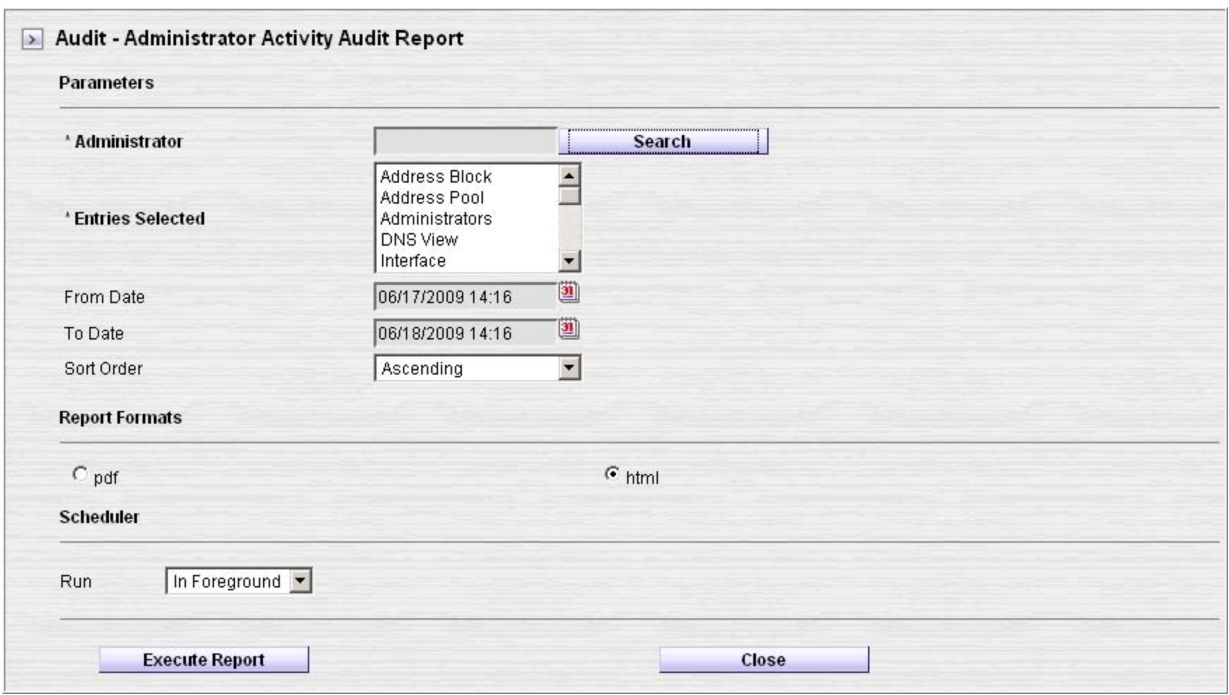
To produce an Administrator Activity report, follow these steps.

1 Click the **Reports** menu.

Result: The Reports hierarchy opens.

2 Expand **Audit** in the **Infrastructure** node, and click **Admin Activity**.

Result: The Administrator Activity Audit Report page opens.



3 Click **Search** and enter search criteria in the Administrator Search window. You can simply click **Search** to produce a **Search Results** list of all administrators in the database.

Note: If you are logged in as a normal administrator, only your administrator name is listed in the **Administrator** field. Proceed to Step 5.

4 Highlight the administrator whose activity you wish to audit and click **Select**.

Note: If you accessed this report from the Administrator properties screen, this field is preset to the value of the currently logged in Administrator.

5 Select the object types you wish to audit from the **Entries Selected** list. You can select multiple object types by holding down the **Ctrl** or **Shift** keys as you click.

6 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

7 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

8 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

9 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

10 Click **Execute Report**.

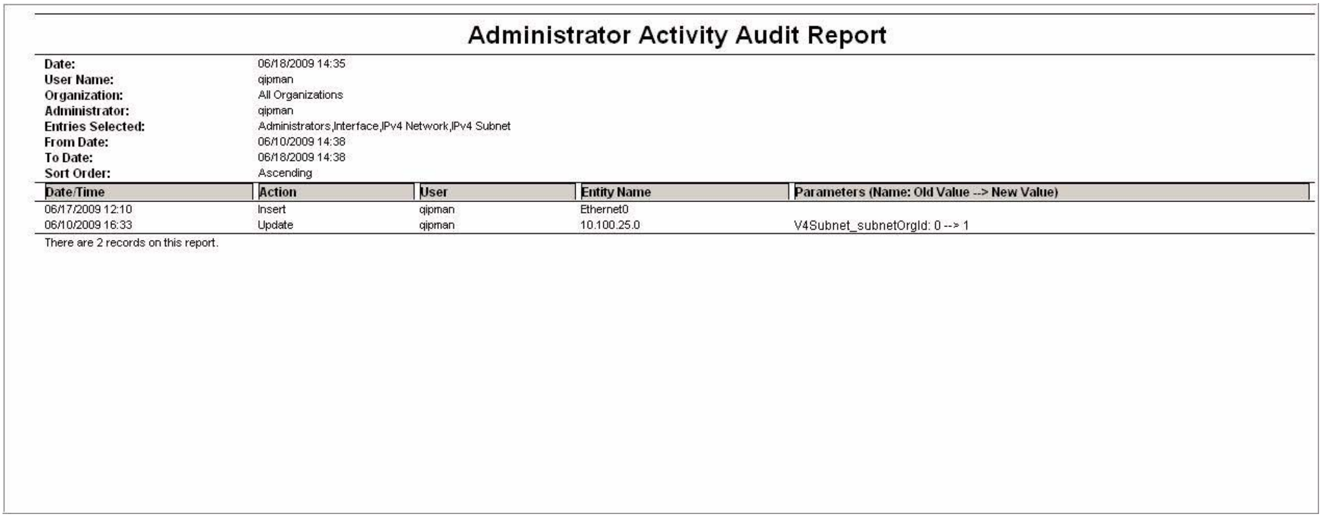
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Administrator Activity report appears as follows.

Figure 29-22 Sample Administrator Activity Audit report



Administrator Activity Audit Report

Date:	06/18/2009 14:35
User Name:	qipman
Organization:	All Organizations
Administrator:	qipman
Entries Selected:	Administrators,Interface,IPv4 Network,IPv4 Subnet
From Date:	06/10/2009 14:38
To Date:	06/18/2009 14:38
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
06/17/2009 12:10	Insert	qipman	Ethernet0	
06/10/2009 16:33	Update	qipman	10.100.25.0	V4Subnet_subnetOrgId: 0 --> 1

There are 2 records on this report.

The following table describes the fields on the report.

Table 29-25 Administrator Activity Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the object is located
Administrator	Administrator that is the subject of this report.
Entries Selected	Indicates which object types were selected for audit.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort Order	Indicates whether data are sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Produce an Administrator Generation Audit report

Purpose

To produce an Administrator Generation Audit report.

Before you begin

- An Administrator Generation Audit report can refer to administrators whose user name has been changed or deleted.
- This report can be executed without entering any parameters.
- You can edit the **Administrator** field in this report to enter a specific Administrator user name, the name of a deleted or renamed Administrator user. The wildcard character is supported.
- The **Admin Name** field in the Administrator Search page cannot be used to search for deleted or renamed Administrators.

Procedure

To produce an Administrator Generation Audit report, follow these steps.

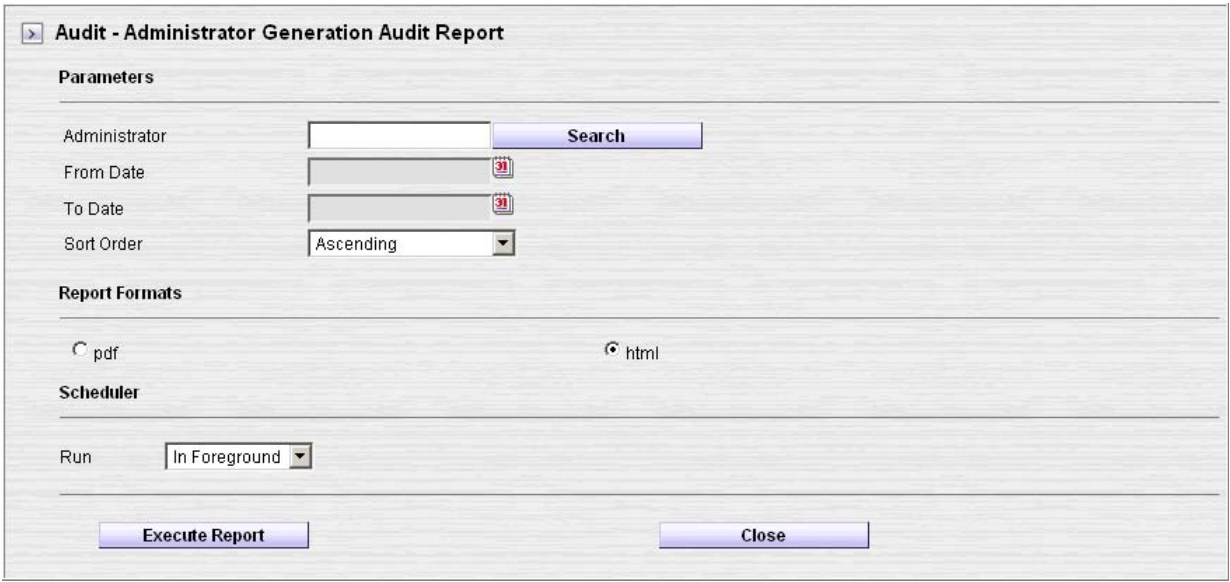
1 Click the **Reports** menu.

Result: The Reports hierarchy opens.

2 Expand **Audit** in the **Infrastructure** node, and click **Admin Generation**.

Result: The Administrator Generation Audit report opens.

Note: This report is also accessible from the Administrator properties screen by clicking **Reports**. The **Administrator** field is preset to the value of the currently logged-in Administrator.



3 Click **Search** and enter search criteria in the Administrator Search window. You can simply click **Search** to produce a **Search Results** list of all administrators in the database.

Note: If you are logged in as a normal administrator, only your administrator name is listed in the **Administrator** field. Proceed to Step 5.

4 Highlight the administrator whose server generation activity you wish to audit and click **Select**.

5 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

6 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

7 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

9 Click **Execute Report**.

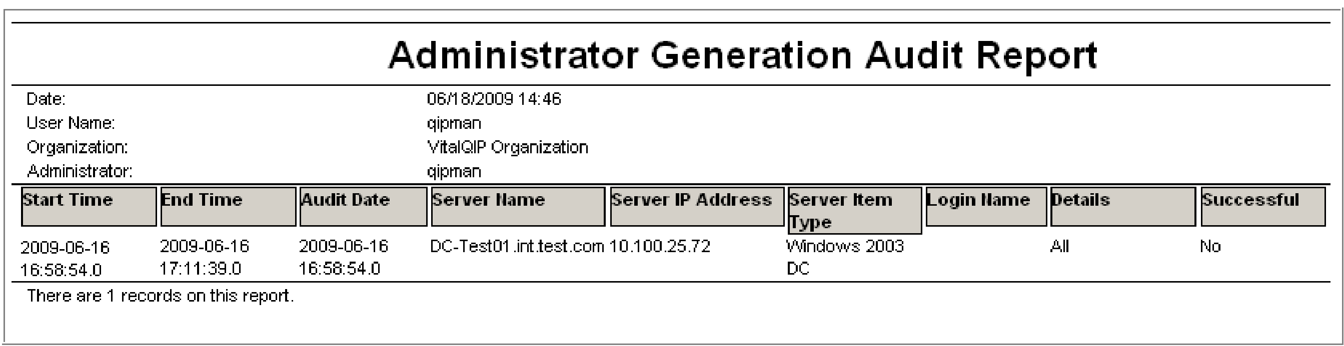
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Administrator Generation Audit report appears as follows.

Figure 29-23 Sample Administrator Generation Audit report



Administrator Generation Audit Report

Date: 06/18/2009 14:46
User Name: qipman
Organization: VitalQIP Organization
Administrator: qipman

Start Time	End Time	Audit Date	Server Name	Server IP Address	Server Item Type	Login Name	Details	Successful
2009-06-16 16:58:54.0	2009-06-16 17:11:39.0	2009-06-16 16:58:54.0	DC-Test01.int.test.com	10.100.25.72	Windows 2003 DC		All	No

There are 1 records on this report.

The following table describes the fields on the report.

Table 29-26 Administrator Generation Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the object is located
Administrator	Administrator that is the subject of this report.
Column headings	
Start Time	Start time of the generation.
End Time	End time of the generation

Field	Description
Audit Date	The date that the generation audit record was created. This date is used by **`qip-clear`** CLI when audit records are deleted on a time basis (with the **`-d`** parameter).
Server Name	The name of the server that the generation was performed against at the time the generation was performed.
Server IP Address	The IP address of the server that the generation was performed against at the time the generation was performed.
Server Item Type	The server type at the time that the generation was performed.
Login Name	The login name of the administrator who started the generation at the time the generation was performed.
Details	Possible values are: DC: Changed or All DHCP: Server DNS: Update | Config and Data - Changed | All | Selected NIS/Local: Server
Successful	Yes or No

Produce an Administrator Profile Audit report

Purpose

Use this procedure to produce an Administrator Profile Audit report. The Administrator Profile Audit report shows changes done with the Administrator Profile. It lists only add/delete/modify activities and basic attributes. It does not list the changes in the managed list or Organizational defaults for the selected administrator.

Procedure

To produce an Administrator Profile Audit report, follow these steps.

1. Click the **Reports** menu.

   Result: The Reports hierarchy opens.

2. Expand **Audit** in the **Infrastructure** node, and click **Admin Profile**.

Result: The Administrator Profile Audit report opens.

Note: This report is also accessible from the Administrator properties screen by clicking **Reports**. The **Administrator** field is preset to the value of the currently logged-in Administrator.

3 Click **Search** and enter search criteria in the Administrator Search window. You can simply click **Search** to produce a **Search Results** list of all administrators in the database.

Note: If you are logged in as a normal administrator, only your administrator name is listed in the **Administrator** field. Proceed to Step 5.

4 Highlight the administrator whose profile you wish to audit and click **Select**.

5 Select start and end dates to define the range of activity you want to view.

6 Select a sort order from the **Sort Order** drop-down menu.

7 Choose when to run the report in the **Scheduler** section. Refer to “Schedule a report” (p. 29-6) for more information.

8 Click **Execute Report**.

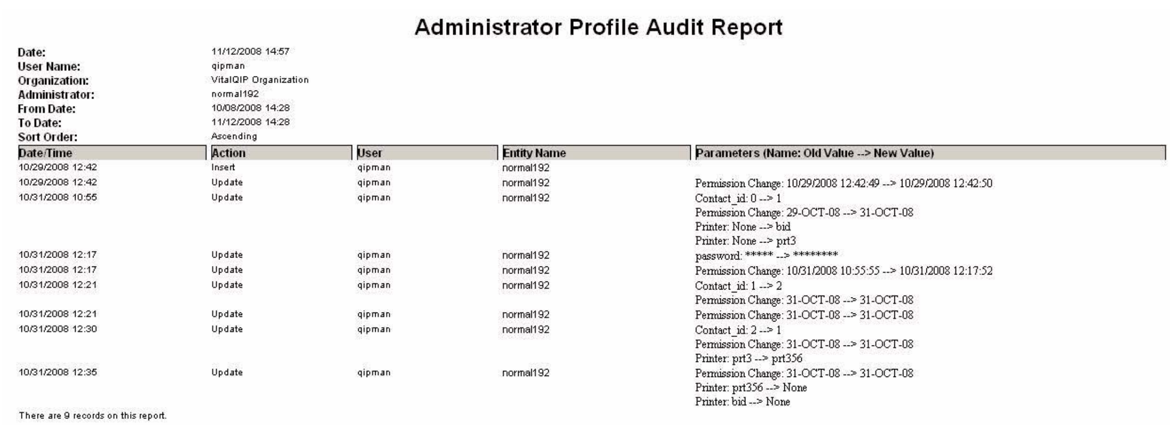
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Adminstrator Profile Audit report appears as follows.

Figure 29-24 Sample Administrator Profile Audit Report



Administrator Profile Audit Report

Date:	11/12/2008 14:57
User Name:	qipman
Organization:	VitalQIP Organization
Administrator:	normal192
From Date:	10/08/2008 14:28
To Date:	11/12/2008 14:28
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
10/29/2008 12:42	Insert	qipman	normal192	
10/29/2008 12:42	Update	qipman	normal192	Permission Change: 10/29/2008 12:42:49 --> 10/29/2008 12:42:50
10/31/2008 10:55	Update	qipman	normal192	Contact_id: 0 --> 1 Permission Change: 29-OCT-08 --> 31-OCT-08 Printer: None --> bid Printer: None --> prt3
10/31/2008 12:17	Update	qipman	normal192	password: ***** --> ********
10/31/2008 12:17	Update	qipman	normal192	Permission Change: 10/31/2008 10:55:55 --> 10/31/2008 12:17:52
10/31/2008 12:21	Update	qipman	normal192	Contact_id: 1 --> 2 Permission Change: 31-OCT-08 --> 31-OCT-08
10/31/2008 12:21	Update	qipman	normal192	Permission Change: 31-OCT-08 --> 31-OCT-08
10/31/2008 12:30	Update	qipman	normal192	Contact_id: 2 --> 1 Permission Change: 31-OCT-08 --> 31-OCT-08 Printer: prt3 --> prt356
10/31/2008 12:35	Update	qipman	normal192	Permission Change: 31-OCT-08 --> 31-OCT-08 Printer: prt356 --> None Printer: bid --> None

There are 9 records on this report.

The following table describes the fields on the report.

Table 29-27 Administrator Profile Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the resource record is located.
From Date	Earliest date for which audit activity appears on the report.
To Date	End date for which audit activity appears on the report.
Administrator	Administrator whose activity is being audited.
Sort Order	Ascending or Descending order by date.
Date/Time	The date and time the action occurred.

Field	Description
Action	Allowable values are as follows: • Add • Delete • Modify
User	User who performed the action.
Entity Name	The type of entity that had a changed parameter value.
Parameters (Name: Old Value --> New Value)	The parameter that changed, and its old and new values. Parameters are as follows: • Password • Printer • Business Unit • Parent Admin • Permission Change

Produce an Administrative Role Audit report

Purpose

Use this procedure to produce an Administrative Role Audit report. The Administrative Role Audit report shows the changes made with Administrative Role. It lists only add/delete/modify activities and basic attributes. It does not list the changes in the Role contents.

Procedure

To produce an Administrative Role Audit report, follow these steps.

1. Click the **Reports** menu.

   Result: The Reports hierarchy opens.

2. Expand **Audit** in the **Infrastructure** node, and click **Admin Role**.

   Result: The Administrative Role Audit report opens.

Note: This report is also accessible from the Administrative Role properties screen by clicking **Reports**. The Administrative Role field defaults to the role previously selected.

3 Select an administrative role from the **Adminstrative Role** drop-down list.

4 Select start and end dates to define the range of activity you want to view.

5 Select a sort order from the **Sort Order** drop-down list.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

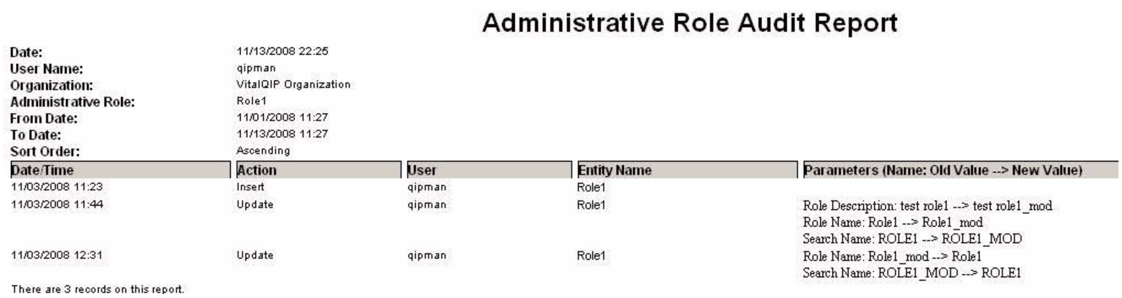
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Adminstrative Role Audit report appears as follows.

Figure 29-25 Sample Administrative Role Audit Report



Administrative Role Audit Report

Date:	11/13/2008 22:25
User Name:	qipman
Organization:	VitalQIP Organization
Administrative Role:	Role1
From Date:	11/01/2008 11:27
To Date:	11/13/2008 11:27
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
11/03/2008 11:23	Insert	qipman	Role1	
11/03/2008 11:44	Update	qipman	Role1	Role Description: test role1 --> test role1_mod Role Name: Role1 --> Role1_mod Search Name: ROLE1 --> ROLE1_MOD
11/03/2008 12:31	Update	qipman	Role1	Role Name: Role1_mod --> Role1 Search Name: ROLE1_MOD --> ROLE1

There are 3 records on this report.

The following table describes the fields on the report.

Table 29-28 Administrative Role Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the resource record is located.
From Date	Earliest date for which audit activity appears on the report.
To Date	End date for which audit activity appears on the report.
Administrative Role	Administrative Role whose activity is being audited.
Sort Order	Ascending or Descending order by date.
Date/Time	The date and time the action occurred.
Action	Allowable values are as follows: • Add • Delete • Modify
User	User who performed the action.
Entity Name	The type of entity that had a changed parameter value.
Parameters (Name: Old Value --> New Value)	The parameter that changed, and its old and new values. Parameters are as follows: • Administrative Role Name • Search Name • Role Description

Produce a Block Audit report

Purpose

Use this procedure to produce Block Audit reports. Instructions are provided for access from the Reports hierarchy or from the Block Properties page.

From the menu or toolbar

To produce a Block Audit report, follow these steps.

1 Click the **Reports** menu.

Result: The Reports hierarchy opens.

2 In the **Infrastructure - Audit** section, click **Block**.

Result: The Block Audit Report page opens.

3 Click **Search**.

Result: The Pool/Block Search Criteria window opens. Refer to "Search for a block" (p. 29-10) for further information.

4 Highlight the block you wish to audit and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected block appears in the **Block Name** field.

---

5 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

---

6 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

---

7 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

---

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

---

9 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

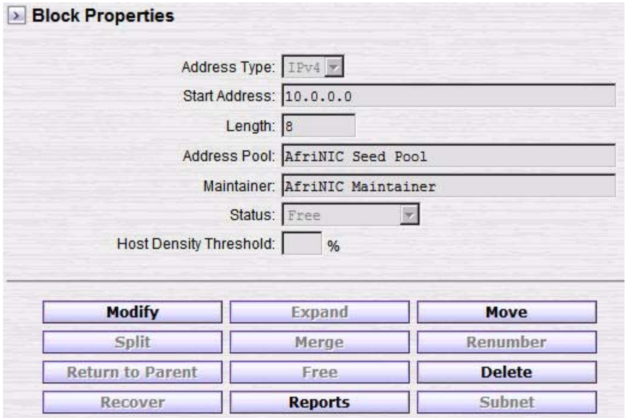
From the Block Properties page

To produce a Block Audit report on a block in the hierarchy, follow these steps.

---

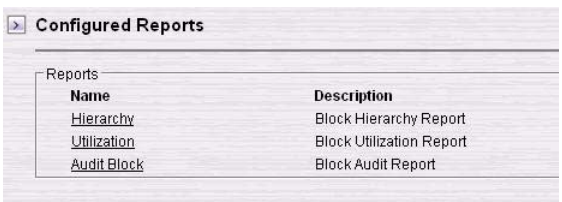
1 Select the block on which you want to report.

Result: The Block Properties page opens.



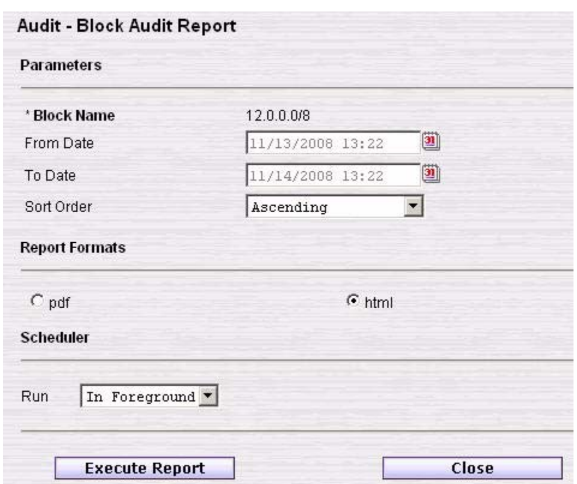
2 Click **Reports**.

Result: The Configured Reports page opens.



3 Click the **Block** link.

Result: The Block Audit Report page opens in the Report Execution window.



4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

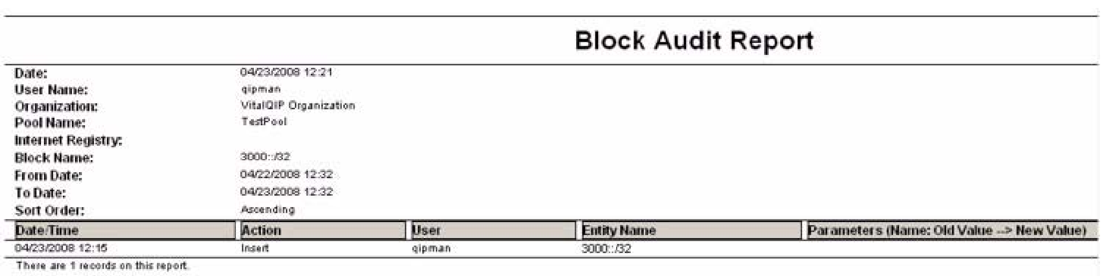
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Block Audit report appears as follows. Fields on this report are similar for all audit reports.

Figure 29-26 Sample Block Audit report



Block Audit Report

Date:	04/23/2008 12:21
User Name:	qipman
Organization:	VitalQIP Organization
Pool Name:	TestPool
Internet Registry:	
Block Name:	3000::/32
From Date:	04/22/2008 12:32
To Date:	04/23/2008 12:32
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
04/23/2008 12:15	Insert	qipman	3000::/32	

There are 1 records on this report.

The following table describes the fields on the report.

Table 29-29 Block Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
Block Name	Item that is the subject of this report.
Internet Registry	Internet registry (ARIN, APNIC or RIPE) to which the element is associated. This field is blank if the element is not associated with an Internet registry. **Note:** This field only displays for block and pool audit reports.
Block Name	Address of the block, followed by the prefix that indicates its length. **Note:** This field only displays for block reports.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Produce a DC Generation Audit report

Purpose

To produce a Domain Controller Generation Audit report.

Before you begin

- A Domain Controller Generation Audit report can refer to administrators whose user name has been changed or deleted.

- This report can be executed without entering any parameters.
- You can edit the **DC Name** field in this report to enter a specific Domain Controller, or the name of a deleted or renamed Domain Controller. The wildcard character is supported.
- The **DC Name** field in the Server Search page cannot be used to search for deleted or renamed Domain Controllers.

Procedure

To produce a Domain Controller Generation Audit report, follow these steps.

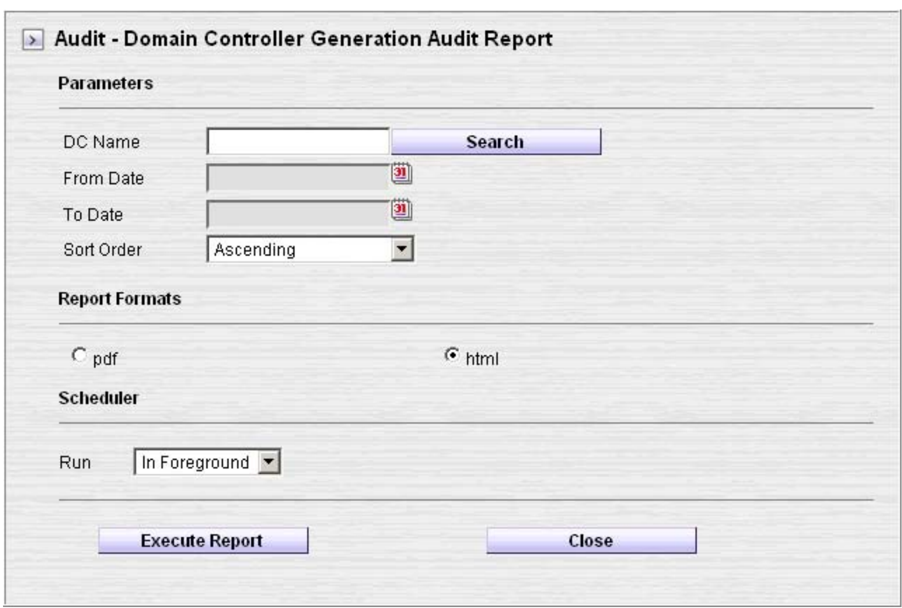
1 Click the **Reports** menu.

Result: The Reports hierarchy opens.

2 Expand **Audit** in the **Infrastructure** node, and click **DC Generation**.

Result: The Domain Controller Generation Audit Report page opens.

Note: This report is also accessible from the Domain Controller Server properties page by clicking **Reports**. The **DC Name** field defaults to the server previously selected.



3 Click **Search** and enter search criteria in the Server Search window. You can simply click **Search** to produce a **Search Results** list of all Domain Controllers in the database.

4 Highlight the server you wish to audit and click **Select**.

5 Select start and end dates to define the range of activity you want to view.

6 Select a sort order from the **Sort Order** drop-down list.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Domain Controller Generation Audit report appears as follows.

Figure 29-27 Sample Domain Controller Generation Audit report

DC Server Generation Audit Report

Date:	06/18/2009 17:30
User Name:	qipman
Organization:	VitalQIP Organization
DC Server Name:	DC-Test01.int.test.com
DC Server IP Address:	10.100.25.72

Start Time	End Time	Audit Date	Login Name	Server Name	Server IP	Server Item Type	Details	Successful
2009-06-16 16:58:54.0	2009-06-16 17:11:39.0	2009-06-16 16:58:54.0	qipman				All	No

There are 1 records on this report.

The following table describes the fields on the report.

Table 29-30 Domain Control Generation Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the server is located
DC Server Name	Name of the server that is the subject of the report.
DC Server IP Address	IP address of the server that is the subject of the report.
Column headings	
Start Time	Start time of the generation.
End Time	End time of the generation
Audit Date	The date that the generation audit record was created. This date is used by **`qip-clear`** CLI when audit records are deleted on a time basis (with the **`-d`** parameter).
Server Name	The name of the server that the generation was performed against at the time the generation was performed.
Server IP	The IP address of the server that the generation was performed against at the time the generation was performed.
Server Item Type	The server type at the time that the generation was performed.
Details	Possible values are: Changed or All
Successful	Yes or No

Produce a DHCP Server Generation report

Purpose

To produce a DHCP Server Generation report.

Before you begin

- A DHCP Generation Audit report can refer to administrators whose user name has been changed or deleted.
- This report can be executed without entering any parameters.

- You can edit the **DHCP Server Name** field in this report to enter a specific DHCP server name, or the name of a deleted or renamed DHCP server. The wildcard character is supported.
- The **Server Name** field in the Server Search page cannot be used to search for deleted or renamed DHCP server.

Procedure

To produce a DHCP Server Generation report, follow these steps.

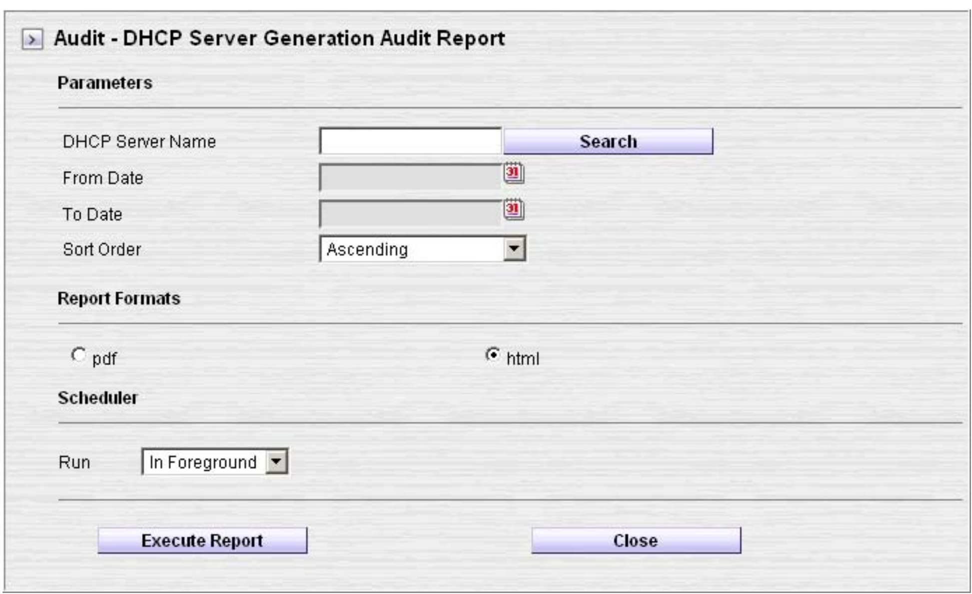
1 Click the **Reports** menu.

Result: The Reports hierarchy opens.

2 Expand **Audit** in the **Infrastructure** node, and click **DHCP Server Generation**.

Result: The DHCP Server Generation Audit Report page opens.

Note: This report is also accessible from the DHCP Server properties page by clicking **Reports**. The **DHCP Server Name** field defaults to the server previously selected.



3 Click **Search** and enter search criteria in the Server Search window. You can simply click **Search** to produce a **Search Results** list of all DHCP servers in the database.

4 Highlight the server you wish to audit and click **Select**.

5 Select start and end dates to define the range of activity you want to view.

6 Select a sort order from the **Sort Order** drop-down list.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The DHCP Server Generation Audit report appears as follows.

Figure 29-28 Sample DHCP Server Generation Audit report

DHCP Server Generation Audit Report

Date:	06/18/2009 17:53
User Name:	qipman
Organization:	VitalQIP Organization
DHCP Server Name:	lablinux501.int.test.com
DHCP Server IP Address:	10.100.25.60
DHCP Server Type:	LUCENT DHCP 5.6

Start Time	End Time	Audit Date	Login Name	Server Name	Server IP	Server Item Type	Details	Successful
2009-06-08 10:26:25.0	2009-06-08 10:38:51.0	2009-06-08 10:26:25.0	qipman				Server	Yes
2009-06-08 11:24:28.0	2009-06-08 11:36:55.0	2009-06-08 11:24:28.0	qipman				Server	Yes
2009-06-08 11:25:14.0	2009-06-08 11:37:40.0	2009-06-08 11:25:14.0	qipman				Server	Yes
2009-06-08 11:27:51.0	2009-06-08 11:40:17.0	2009-06-08 11:27:51.0	qipman				Server	Yes
2009-06-08 13:40:34.0	2009-06-08 13:53:01.0	2009-06-08 13:40:34.0	qipman				Server	Yes
2009-06-08 13:47:09.0	2009-06-08 13:59:36.0	2009-06-08 13:47:09.0	qipman				Server	Yes
2009-06-08 13:51:55.0	2009-06-08 14:04:22.0	2009-06-08 13:51:55.0	qipman				Server	Yes
2009-06-08 14:12:10.0	2009-06-08 14:24:36.0	2009-06-08 14:12:10.0	qipman				Server	Yes
2009-06-09 09:21:41.0	2009-06-09 09:34:10.0	2009-06-09 09:21:41.0	qipman				Server	Yes
2009-06-09 09:22:27.0	2009-06-09 09:34:55.0	2009-06-09 09:22:27.0	qipman				Server	Yes

There are 10 records on this report.

The following table describes the fields on the report.

Table 29-31 DHCP Server Generation Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the server is located
DHCP Server Name	Name of the server that is the subject of the report.
DHCP Server IP Address	IP address of the server that is the subject of the report.
DHCP Server Type	The server type that is the subject of the report.
Column headings	
Start Time	Start time of the generation.
End Time	End time of the generation
Audit Date	The date that the generation audit record was created. This date is used by **`qip-clear`** CLI when audit records are deleted on a time basis (with the **`-d`** parameter).

Field	Description
Login Name	The login name of the administrator who started the generation at the time the generation was performed.
Server Name	The name of the server that the generation was performed against at the time the generation was performed.
Server IP	The IP address of the server that the generation was performed against at the time the generation was performed.
Server Item Type	The server type at the time that the generation was performed.
Details	Possible values are: Changed or All
Successful	Yes or No

Produce a DNS Server Generation report

Purpose

To produce a DNS Server Generation report.

Before you begin

- A DNS Server Generation Audit report can refer to administrators whose user name has been changed or deleted.
- This report can be executed without entering any parameters.
- You can edit the **DNS Server Name** field in this report to enter a specific DNS server name, or the name of a deleted or renamed DNS server. The wildcard character is supported.
- The **Server Name** field in the Server Search page cannot be used to search for deleted or renamed DNS server.

Procedure

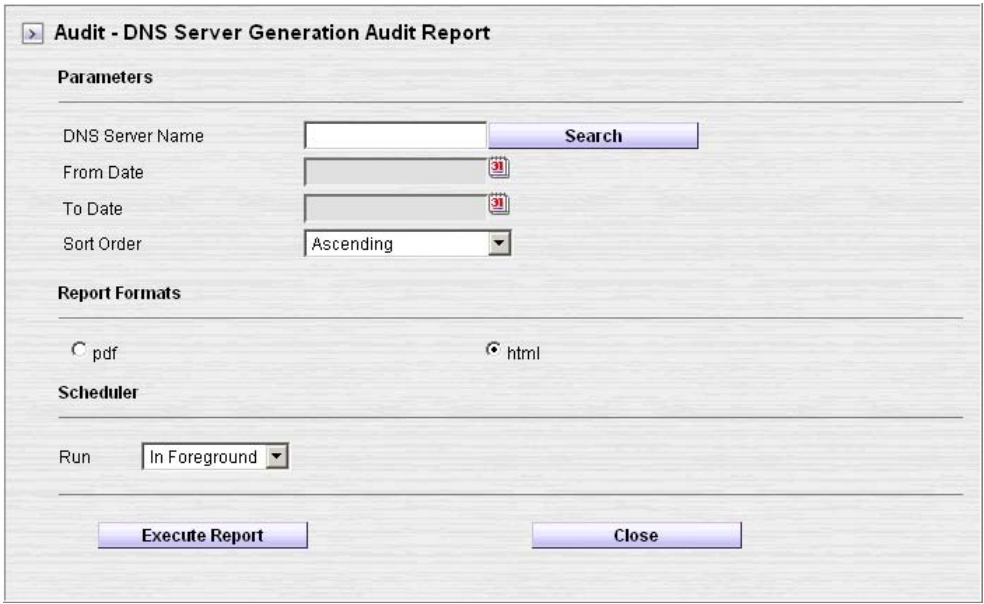
To produce a DNS Server Generation report, follow these steps.

1. Click the **Reports** menu.

   Result: The Reports hierarchy opens.

2 Expand **Audit** in the **Infrastructure** node, and click **DNS Server Generation**.

Result: The DNS Server Generation Audit Report page opens.



3 Click **Search** and enter search criteria in the Server Search window. You can simply click **Search** to produce a **Search Results** list of all DNS servers in the database.

4 Highlight the server you wish to audit and click **Select**.

5 Select start and end dates to define the range of activity you want to view.

6 Select a sort order from the **Sort Order** drop-down list.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The DNS Server Generation Audit report appears as follows.

Figure 29-29 Sample DNS Server Generation Audit report

DNS Server Generation Audit Report

Date:	06/18/2009 18:06
User Name:	qipman
Organization:	VitalQIP Organization
DNS Server Name:	doc-dns2.int.test.com
DNS Server IP Address:	10.100.25.10
DNS Server Type:	LUCENT DNS 4.X

Start Time	End Time	Audit Date	Login Name	Server Name	Server IP	Server Item Type	Details	Successful

No matching records to report.

The following table describes the fields on the report.

Table 29-32 DNS Server Generation Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the server is located
DNS Server Name	Name of the server that is the subject of the report.
DNS Server IP Address	IP address of the server that is the subject of the report.
DNS Server Type	The server type that is the subject of the report.
Column headings	
Start Time	Start time of the generation.
End Time	End time of the generation.

Field	Description
Audit Date	The date that the generation audit record was created. This date is used by **`qip-clear`** CLI when audit records are deleted on a time basis (with the **`-d`** parameter).
Login Name	The login name of the administrator who started the generation at the time the generation was performed.
Server Name	The name of the server that the generation was performed against at the time the generation was performed.
Server IP	The IP address of the server that the generation was performed against at the time the generation was performed.
Server Item Type	The server type at the time that the generation was performed.
Details	Possible values are: Changed or All
Successful	Yes or No

Search for a DNS View

Purpose

Use this procedure to search for a DNS View when you wish to produce a DNS View Audit report.

Before you begin

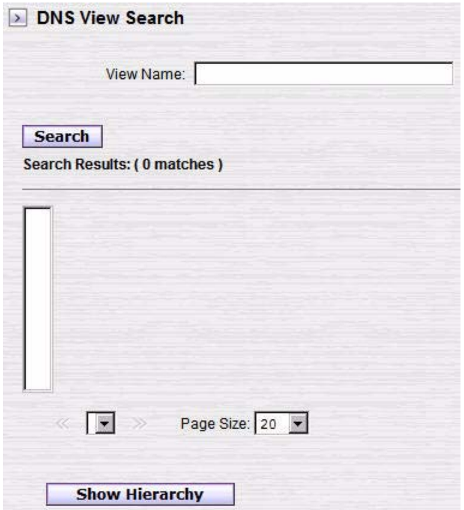
You can use the wildcard character (*) as part of the search string for all searches.

Procedure

To search for a DNS View, follow these steps.

1 Select a DNS View Audit report in the Reports hierarchy and click **Search**.

Result: The DNS View Search page opens.



2 Enter the name of the DNS View for which you are searching in the **View Name** field. This field is case-sensitive. You can enter a partial name followed by an asterisk (*) as a wildcard, or leave the field blank to search all DNS Views.

3 Click **Search**.

Result: The results appear in the **Search Results** list.

END OF STEPS

Produce a DNS View Audit report

Purpose

Use this procedure to produce a DNS View Audit report. Instructions are provided for access from the Reports hierarchy or from the DNS View Properties page.

From the menu or toolbar

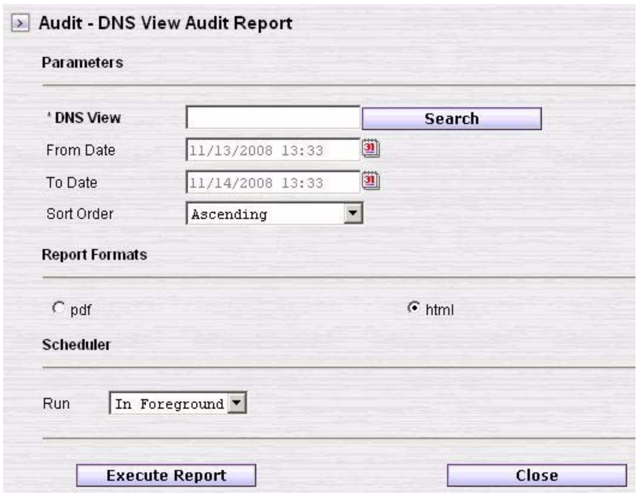
To produce a DNS View Audit report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Infrastructure - Audit** section, click **DNS View**.

Result: The DNS View Audit report opens.



3 Click **Search**.

4 The DNS View Search window opens. Refer to "Search for a DNS View" (p. 29-134) for further information.

5 Highlight the DNS View you wish to audit and click **Select**.

Important! If there are multiple pages of matching objects, use the scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected DNS View appears in the **DNS View** field.

6 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

7 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

8 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

9 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

10 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the DNS View Properties page

To produce a DNS View Audit report on a DNS View in the Zone hierarchy, follow these steps.

1 Select the DNS View on which you want to report.

Result: The DNS View Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **DNS View** link.

Result: The DNS View Audit Report page opens in the Report Execution window.

4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

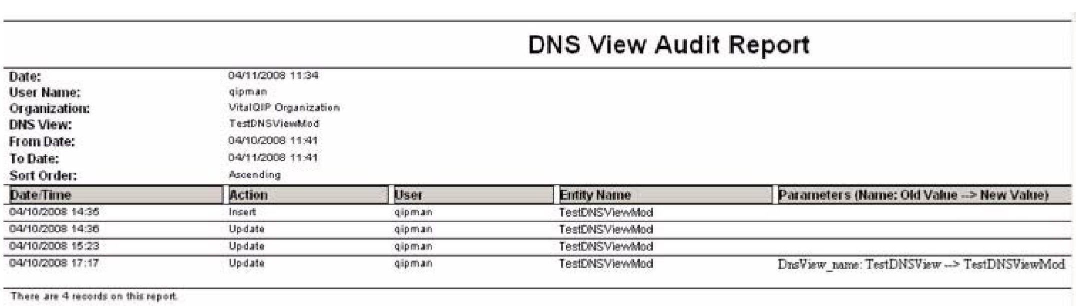
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The DNS View Audit report appears as follows.

Figure 29-30 Sample DNS View Audit report



DNS View Audit Report

Date: 04/11/2008 11:34
User Name: qipman
Organization: VitalQIP Organization
DNS View: TestDNSViewMod
From Date: 04/10/2008 11:41
To Date: 04/11/2008 11:41
Sort Order: Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
04/10/2008 14:35	Insert	qipman	TestDNSViewMod	
04/10/2008 14:36	Update	qipman	TestDNSViewMod	
04/10/2008 15:23	Update	qipman	TestDNSViewMod	
04/10/2008 17:17	Update	qipman	TestDNSViewMod	DnsView_name: TestDNSView --> TestDNSViewMod

There are 4 records on this report.

The following table describes the fields on the report.

Table 29-33 DNS View Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
DNS View	The DNS View that is the subject of this report.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Produce an IPv4 Network Audit report

Purpose

Use this procedure to produce an IPv4 Network Audit report. Instructions are provided for access from the Reports hierarchy or from the Network Properties page.

From the menu or toolbar

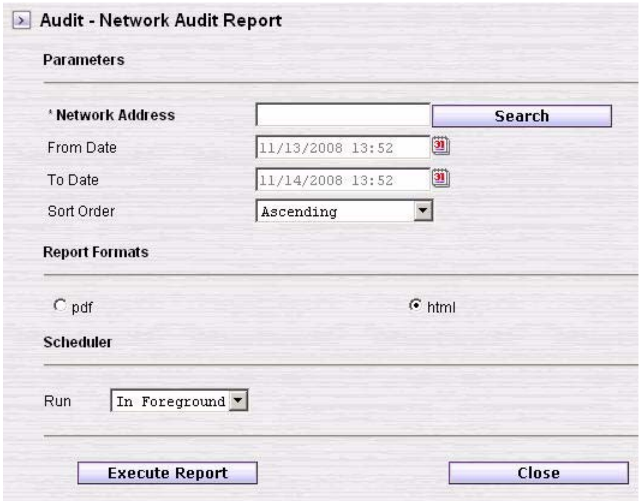
To produce an IPv4 Network Audit report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Infrastructure - Audit** section, click **IPv4 Network**.

Result: The Network Audit report opens.



3 Click **Search**.

4 The IPv4 Search window opens. Refer to "Search for an IPv4 hierarchy item" (p. 29-49) for further information.

5 Highlight the IPv4 network address you wish to audit and click **Select**.

Important! If there are multiple pages of matching objects, use the scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected IPv4 network address appears in the **Network Address** field.

6 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

7 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

8 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

9 Choose when to run the report in the **Scheduler** section. Refer to “Schedule a report” (p. 29-6) for more information.

10 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to “View scheduled jobs” (p. 30-3) for more information.

END OF STEPS

From the Network Properties page

To produce a Network Audit report on an IPv4 network in the IPv4 hierarchy, follow these steps.

1 Select the IPv4 network on which you want to report.

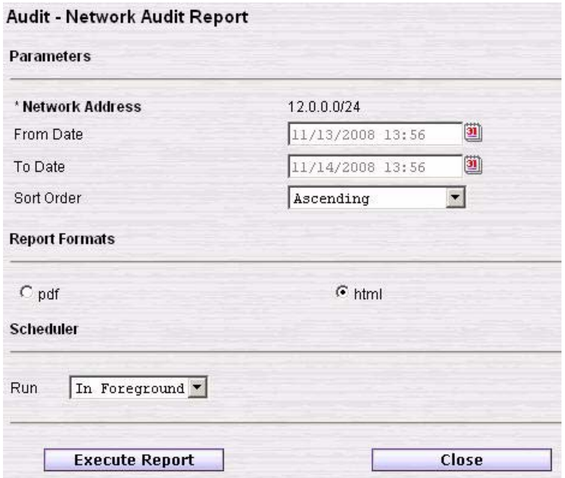
Result: The Network Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Audit IPv4 Network** link.

Result: The Network Audit Report page opens in the Report Execution window.



4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to “Schedule a report” (p. 29-6) for more information.

8 Click **Execute Report**.

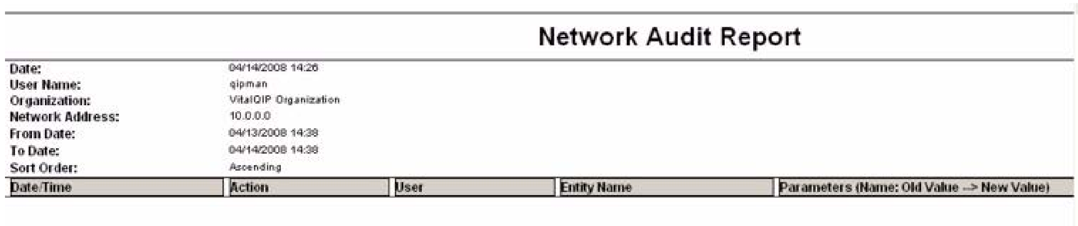
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to “View scheduled jobs” (p. 30-3) for more information.

END OF STEPS

Report format

The Network Audit report appears as follows. Fields on this report are similar for all audit reports.

Figure 29-31 Sample Network Audit report



Network Audit Report

Date:	04/14/2008 14:26
User Name:	qipman
Organization:	VitalQIP Organization
Network Address:	10.0.0.0
From Date:	04/13/2008 14:38
To Date:	04/14/2008 14:38
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)

The following table describes the fields on the report.

Table 29-34 Subnet Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
Network Address	The network that is the subject of this report.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Produce an IPv4 Subnet report

Purpose

Use this procedure to produce an IPv4 Subnet report. Instructions are provided for access from the Reports hierarchy or from the IPv4 Subnet Properties page.

From the menu or toolbar

To produce an IPv4 Subnet report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Infrastructure - Audit** section, click **IPv4 Subnet**.

Result: The Subnet Audit Report page opens.

3 Click **Search**.

Result: The Global Search window opens. Refer to “Search for an IPv4 hierarchy item” (p. 29-49) for further information.

4 Highlight the subnet you wish to audit and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected subnet appears in the **Subnet Address** field.

5 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

6 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

7 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

9 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Subnet Properties page

To produce a Subnet Audit report on a subnet in the IPv4 hierarchy, follow these steps.

1 Select the subnet on which you want to report.

Result: The Subnet Properties page opens.

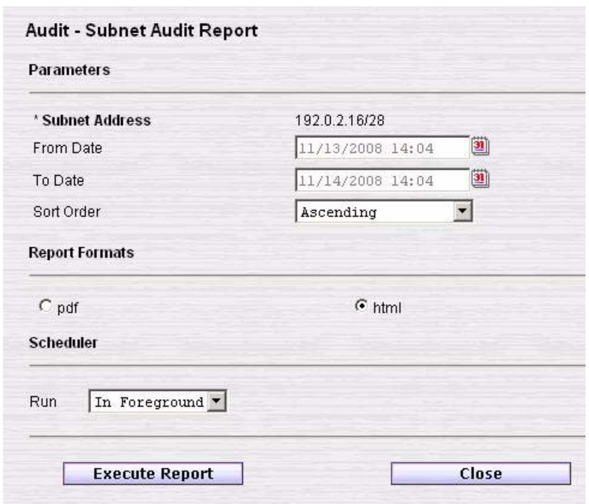
2 Click **Reports**.

Result: The Configured Reports page opens.

---

3 Click the **Audit IPv4 Subnet** link.

Result: The Subnet Audit Report page opens in the Report Execution window.



---

4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

---

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

---

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

---

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

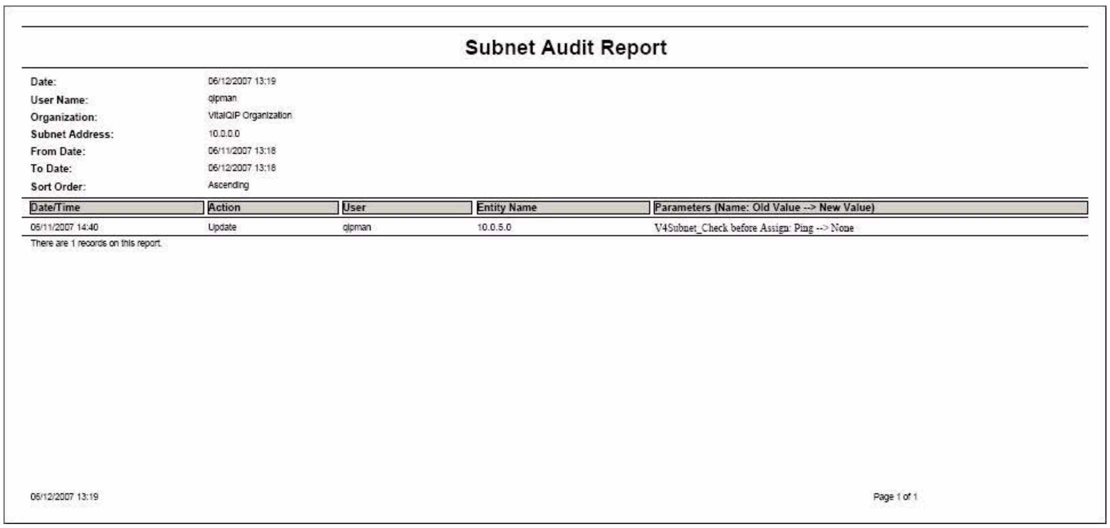
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Subnet Audit report appears as follows. Fields on this report are similar for all audit reports.

Figure 29-32 Sample Subnet Audit report



Subnet Audit Report

Date: 06/12/2007 13:19
User Name: qipman
Organization: VitalQIP Organization
Subnet Address: 10.0.0.0
From Date: 06/11/2007 13:16
To Date: 06/12/2007 13:16
Sort Order: Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
06/11/2007 14:40	Update	qipman	10.0.5.0	V4Subnet_Check before Assign: Ping --> None

There are 1 records on this report.

06/12/2007 13:19 Page 1 of 1

The following table describes the fields on the report.

Table 29-35 Subnet Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
Subnet Address	The subnet that is the subject of this report.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.

Field	Description
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Produce an IPv4 Subnet Organization Audit report

Purpose

Use this procedure to produce an IPv4 Subnet Organization Audit report. Instructions are provided for access from the Reports hierarchy or from the Subnet Organization Properties page.

From the menu or toolbar

To produce an IPv4 Subnet Organization Audit report, follow these steps.

1. Click the **Reports** tab.

   Result: The Reports hierarchy opens.

2. In the **Infrastructure - Audit** section, click **IPv4 Subnet Organization**.

Result: The Subnet Organization Audit Report page opens.

3 Click **Search**.

Result: The IPv4 Search window opens. Refer to "Search for an IPv4 hierarchy item" (p. 29-49) for further information.

4 Highlight the subnet organization you wish to audit and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected subnet appears in the **Subnet Organization** field.

5 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

6 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

7 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

9 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Subnet Organization Properties page

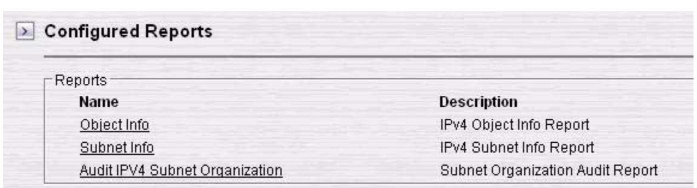
To produce a Subnet Organization Audit report on a subnet in the IPv4 hierarchy, follow these steps.

1 Select the subnet organization on which you want to report.

Result: The Subnet Organization Properties page opens.

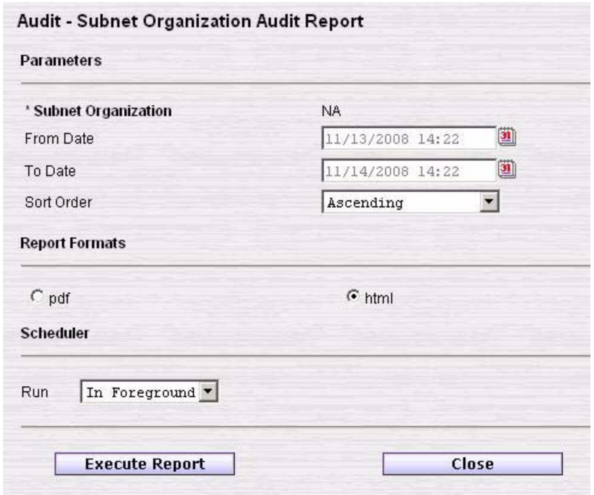
2 Click **Reports**.

Result: The Configured Reports page opens.



3 Click the **Audit IPv4 Subnet Organization** link.

Result: The Subnet Organization Audit Report page opens in the Report Execution window.



4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

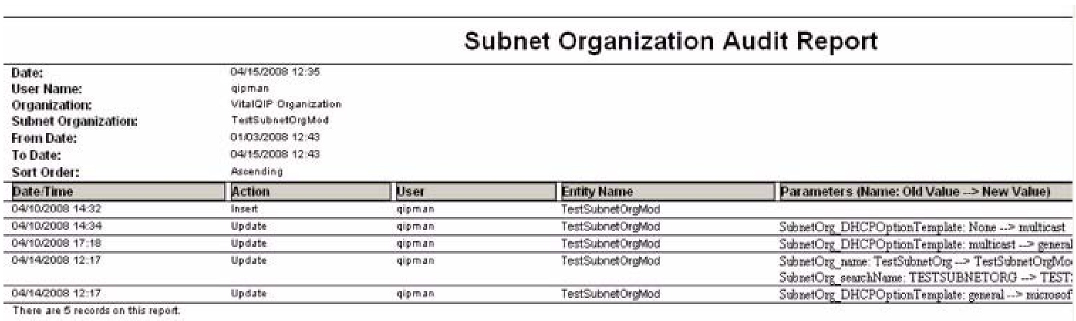
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Subnet Organization Audit report appears as follows. Fields on this report are similar for all audit reports.

Figure 29-33 Sample Subnet Organization Audit report



Subnet Organization Audit Report

Date:	04/15/2008 12:35
User Name:	qipman
Organization:	VitalQIP Organization
Subnet Organization:	TestSubnetOrgMod
From Date:	01/03/2008 12:43
To Date:	04/15/2008 12:43
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
04/10/2008 14:32	Insert	qipman	TestSubnetOrgMod	
04/10/2008 14:34	Update	qipman	TestSubnetOrgMod	SubnetOrg_DHCPOptionTemplate: None --> multicast
04/10/2008 17:18	Update	qipman	TestSubnetOrgMod	SubnetOrg_DHCPOptionTemplate: multicast --> general
04/14/2008 12:17	Update	qipman	TestSubnetOrgMod	SubnetOrg_name: TestSubnetOrg --> TestSubnetOrgMo SubnetOrg_searchName: TESTSUBNETORG --> TEST:
04/14/2008 12:17	Update	qipman	TestSubnetOrgMod	SubnetOrg_DHCPOptionTemplate: general --> microsof

There are 5 records on this report.

The following table describes the fields on the report.

Table 29-36 Subnet Organization Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located.
Subnet Organization	The subnet organization that is the subject of this report.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Produce an IPv6 Address Audit report

Purpose

Use this procedure to produce an IPv6 Address Audit report. Instructions are provided for access from the Reports hierarchy or from the IPv6 or Node hierarchy (or MyView hierarchy if IPv6 seed blocks, subnets, nodes, and address ranges are present).

From the menu or toolbar

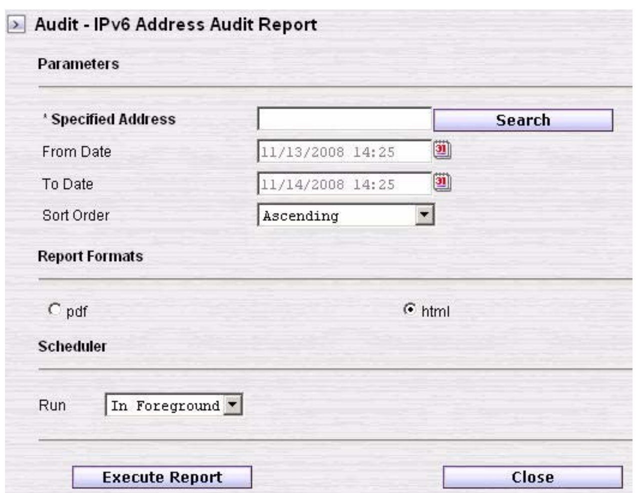
To produce an IPv6 Address Audit report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Infrastructure - Audit** section, click **IPv6 Address**.

Result: The IPv6 Address Audit Report page opens.



3 Click **Search**.

Result: The Subnet Search window opens. Refer to "Search for an IPv6 hierarchy item" (p. 29-67) for further information.

4 Highlight the address you wish to audit and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected address appears in the **Specified Address** field.

---

5 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

---

6 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

---

7 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

---

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

---

9 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Address Range Properties page

To produce an IPv6 Address Audit report on an address in the IPv6 (or MyView) hierarchy, follow these steps.

---

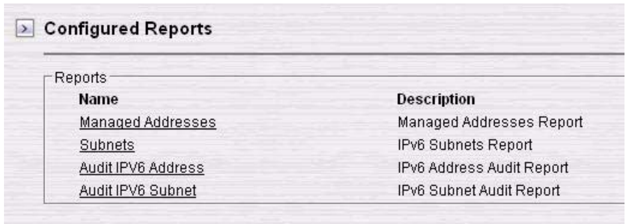
1 Select the IPv6 item (seed block, address range, or subnet) on which you want to report.

Result: The Properties page opens.

---

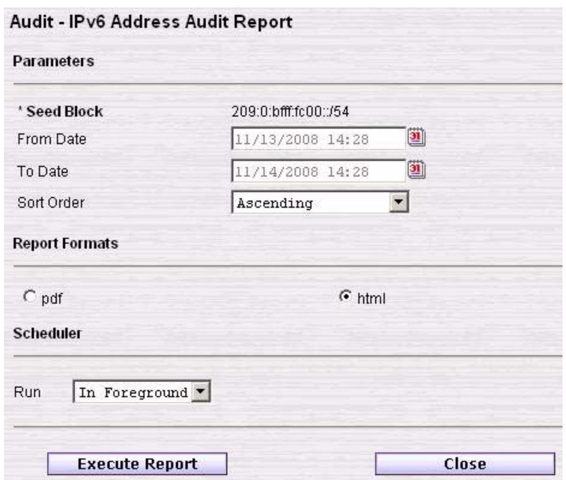
2 Click **Reports**.

Result: The Configured Reports page opens.



3 Click the **Audit IPv6 Address** link.

Result: The IPv6 Address Audit Report page opens in the Report Execution window.



[

4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

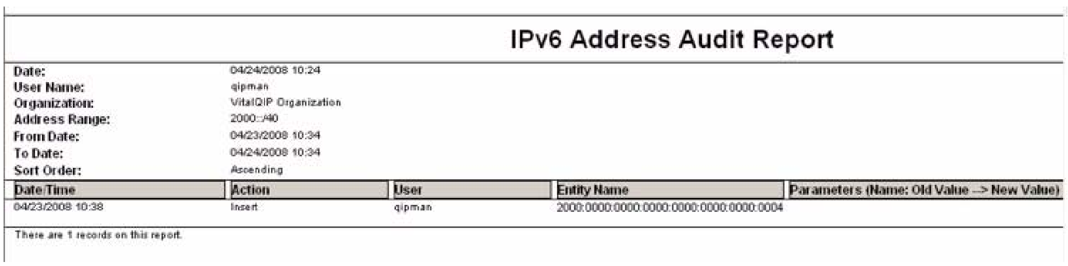
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The IPv6 Address Audit report appears as follows.

Figure 29-34 Sample IPv6 Address Audit report



IPv6 Address Audit Report

Date: 04/24/2008 10:24
User Name: qipman
Organization: VitalQIP Organization
Address Range: 2000::/40
From Date: 04/23/2008 10:34
To Date: 04/24/2008 10:34
Sort Order: Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
04/23/2008 10:38	Insert	qipman	2000:0000:0000:0000:0000:0000:0000:0004	

There are 1 records on this report.

The following table describes the fields on the report.

Table 29-37 IPv6 Address Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
Address Range	The address range that is the subject of this report.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

END OF STEPS

Produce an IPv6 Subnet report

Purpose

Use this procedure to produce an IPv6 Subnet report. Instructions are provided for access from the Reports hierarchy or from the IPv6 hierarchy (or MyView hierarchy if IPv6 seed blocks, subnets, and address ranges are present).

From the menu or toolbar

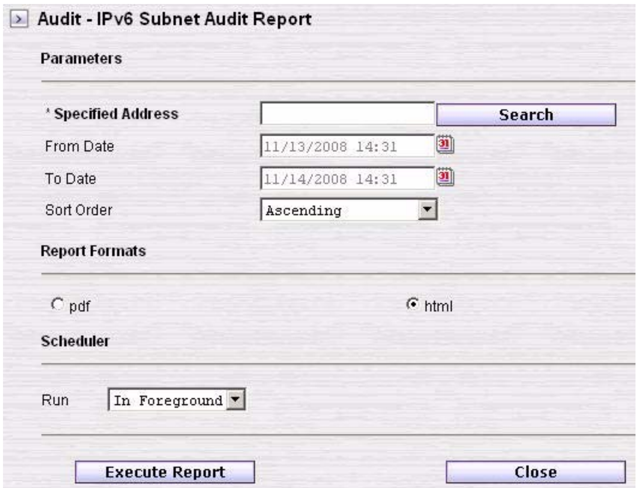
To produce an IPv6 Subnet report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Infrastructure - Audit** section, click **IPv6 Subnet**.

Result: The IPv6 Subnet Audit Report page opens.



3 Click **Search**.

Result: The Subnet Search window opens. Refer to "Search for an IPv6 hierarchy item" (p. 29-67) for further information.

4 Highlight the address you wish to audit and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected address appears in the **Specified Address** field.

5 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

6 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

7 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

9 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Seed Block Properties page

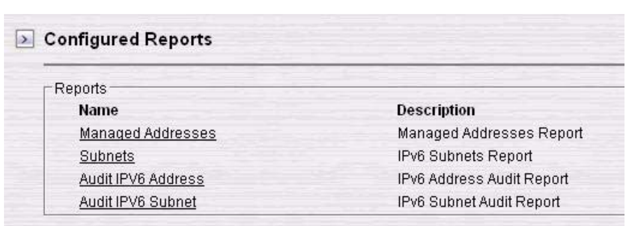
To produce an IPv6 Address Audit report on an address in the IPv6 (or MyView) hierarchy, follow these steps.

1 Select the IPv6 item (seed block, address range, or subnet) on which you want to report.

Result: The Properties page opens.

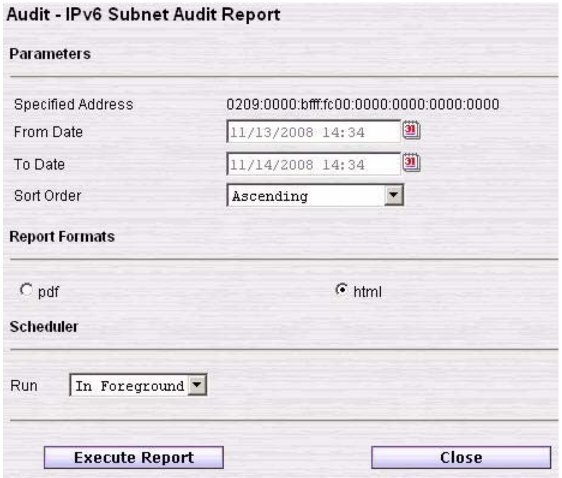
2 Click **Reports**.

Result: The Configured Reports page opens.



3 Click the **Audit IPv6 Subnet** link.

Result: The IPv6 Subnet Audit Report page opens in the Report Execution window.



4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

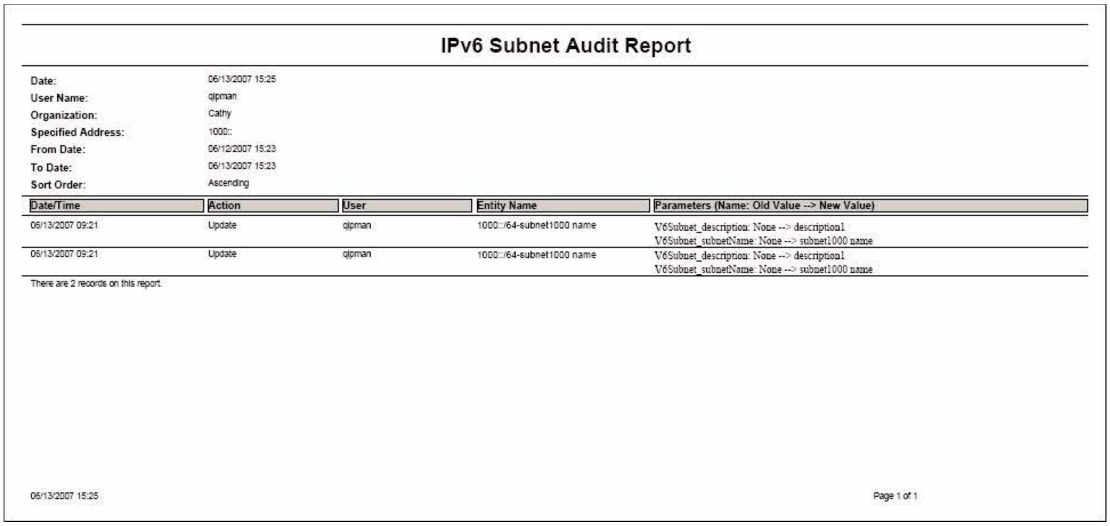
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The IPv6 Subnet Audit report appears as follows.

Figure 29-35 Sample IPv6 Subnet Audit report



IPv6 Subnet Audit Report

Date: 06/13/2007 15:25
User Name: qlpman
Organization: Cathy
Specified Address: 1000::
From Date: 06/12/2007 15:23
To Date: 06/13/2007 15:23
Sort Order: Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
06/13/2007 09:21	Update	qlpman	1000::/64-subnet1000 name	V6Subnet_description: None --> description1 V6Subnet_subnetName: None --> subnet1000 name
06/13/2007 09:21	Update	qlpman	1000::/64-subnet1000 name	V6Subnet_description: None --> description1 V6Subnet_subnetName: None --> subnet1000 name

There are 2 records on this report.

06/13/2007 15:25 Page 1 of 1

The following table describes the fields on the report.

Table 29-38 IPv6 Subnet Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
Specified Address	The subnet address that is the subject of this report.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Search for a managed file

Purpose

Use this procedure to search for a managed file on which you want to produce the managed file audit report.

Procedure

To search for a managed file, follow these steps.

1 Select a Managed File Audit report or a User Defined Attribute and click **Search**.

Result: The Managed File Search window opens.

2 Enter the name of the managed file you are searching in the **File Name** field. This field is case-sensitive. You can enter a partial name followed by an asterisk (*) as a wildcard, or leave the field blank to search all managed files.

3 Click **Search**.

Result: The results appear in the **Search Results** list.

END OF STEPS

Produce the Managed Files Audit report

Purpose

Use this procedure to produce a Managed Files Audit report. Instructions are provided for access from the Reports hierarchy or from the Managed File Properties page.

From the menu or toolbar

To produce a Managed Files Audit report, follow these steps.

---

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

---

2 In the **Infrastructure-Audit** section, click **Managed Files**.

Result: The Managed File Audit Report page opens.

---

3 Click **Search**.

Result: The Managed File Search window opens. Refer to "Search for a managed file" (p. 29-162) for further information.

---

4 Highlight the managed file you wish to audit and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected block appears in the **Managed File** field.

5 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

6 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

7 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

8 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

9 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Managed File Properties page

To produce a Managed Files Audit report on a managed file in the Infrastructure hierarchy, follow these steps.

1 Select the managed file on which you want to report.

Result: The Managed File Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Managed Files** link.

Result: The Managed File Audit Report page opens in the Report Execution window.

4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

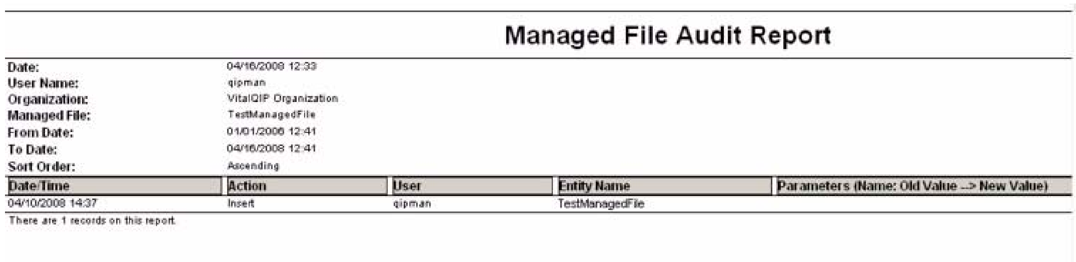
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Managed Files Audit report appears as follows.

Figure 29-36 Sample Managed Files Audit report



Managed File Audit Report

Date:	04/16/2008 12:33
User Name:	qipman
Organization:	VitalQIP Organization
Managed File:	TestManagedFile
From Date:	01/01/2008 12:41
To Date:	04/16/2008 12:41
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
04/10/2008 14:37	Insert	qipman	TestManagedFile	

There are 1 records on this report.

The following table describes the fields on the report.

Table 29-39 Managed Files Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
Managed File	The managed file that is the subject of this report.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.

Field	Description
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Produce the Organization Audit report

Purpose

Use this procedure to produce an Organization Audit report. Instructions are provided for access from the Reports hierarchy or from the Organization Properties page.

From the menu or toolbar

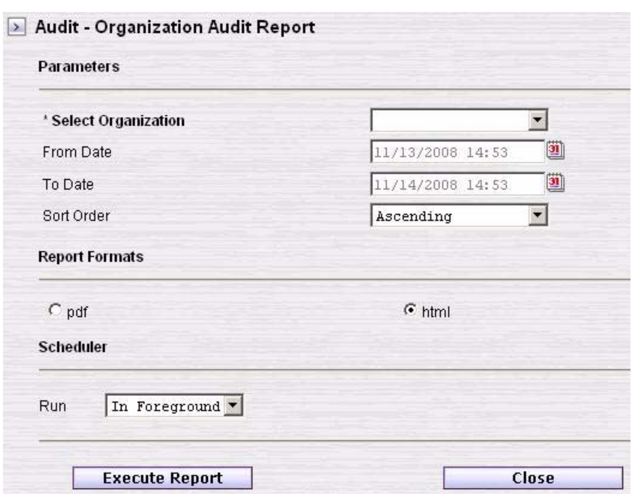
To produce an Organization Audit report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Infrastructure-Audit** section, click **Organization**.

Result: The Organization Audit Report page opens.



3 Select the organization you wish to audit from the **Select Organization** drop-down list.

4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Organization Properties page

To produce an Organization Audit report, follow these steps.

1 In the hierarchy, click the name of the organization for which you want the report.

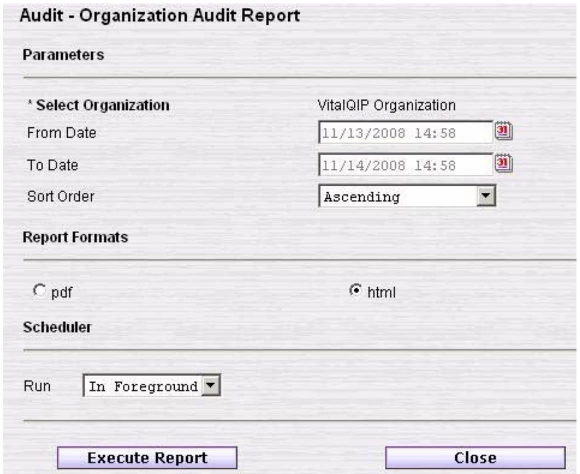
Result: The Organization Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Audit Organization** link.

Result: The Organization Audit Report page opens in the Report Execution window.



4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

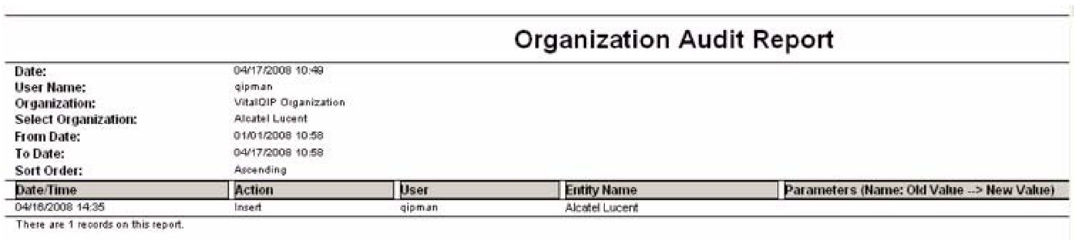
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Organization Audit report appears as follows.

Figure 29-37 Sample Organization Audit report



Organization Audit Report

Date: 04/17/2008 10:49
User Name: qipman
Organization: VitalQIP Organization
Select Organization: Alcatel Lucent
From Date: 01/01/2008 10:58
To Date: 04/17/2008 10:58
Sort Order: Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
04/16/2008 14:35	Insert	qipman	Alcatel Lucent	

There are 1 records on this report.

The following table describes the fields on the report.

Table 29-40 Organization Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
Select Organization	The name of the organization that is the subject of this report.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Produce a Pool Audit report

Purpose

Use this procedure to produce Pool Audit reports. Instructions are provided for access from the Reports hierarchy or from the Pool Properties page.

From the menu or toolbar

To produce a Pool Audit report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Infrastructure - Audit** section, click **Pool**.

Result: The Pool Audit Report page opens.

3 Click **Search**.

Result: The Pool or Block Search Criteria window opens. Refer to "Search for a pool" (p. 29-13) for further information.

4 Highlight the pool you wish to audit and click **Select**.

Note: If there are multiple pages of matching objects, use the list scrolling arrows or the drop-down list to select another page of search results. Change the page size as needed.

Result: The Search window closes and the selected block appears in the **Pool Name** field.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From the Pool Properties page

To produce a Pool Audit report, follow these steps.

1 In the hierarchy, click the name of the pool for which you want the report.

Result: The Pool Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Audit Pool** link.

Result: The Pool Audit Report page opens in the Report Execution window.

4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

6 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

7 Click **Execute Report**.

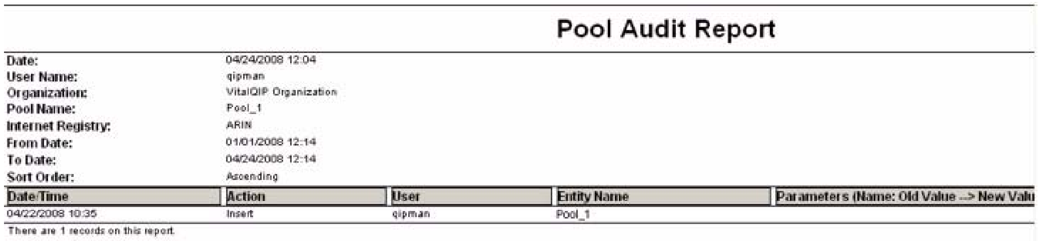
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Pool Audit report appears as follows.

Figure 29-38 Sample Pool Audit report



Pool Audit Report

Date:	04/24/2008 12:04
User Name:	qipman
Organization:	VitalQIP Organization
Pool Name:	Pool_1
Internet Registry:	ARIN
From Date:	01/01/2008 12:14
To Date:	04/24/2008 12:14
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Valu
04/22/2008 10:35	Insert	qipman	Pool_1	

There are 1 records on this report.

The following table describes the fields on the report.

Table 29-41 Pool Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the pool is located
Pool Name	Pool Name that is the subject of this report.
Internet Registry	Internet registry with which this pool is registered. Blank indicates the pool is not assigned to an Internet registry.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort Order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

Produce a Rule Audit report

Purpose

Use this procedure to produce a Rule Audit report. Instructions are provided for access from the **Reports** hierarchy or the **Address Allocation** section.

From the menu or toolbar

To produce a Rule Audit report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Infrastructure - Audit** section, click **Rule**.

Result: The Rule Audit Report page opens.

3 Select a rule from the **Rule Name** drop-down list.

4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to *html* format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

From a Properties page

To produce a Rule Audit report on a rule in the Address Allocation and Infrastructure hierarchy, follow these steps.

1 Select the rule on which you want to report.

Result: The Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Audit Rule** link.

Result: The Rule Audit Report page opens in the Report Execution window.

4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

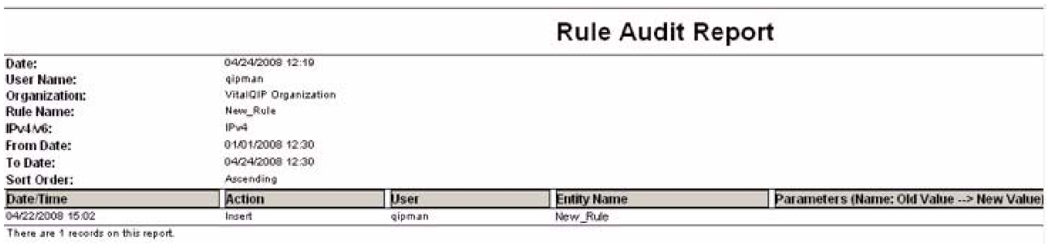
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The Rule Audit report appears as follows.

Figure 29-39 Sample Rule Audit report



Rule Audit Report

Date:	04/24/2008 12:19
User Name:	qipman
Organization:	VitalQIP Organization
Rule Name:	New_Rule
IPv4/v6:	IPv4
From Date:	01/01/2008 12:30
To Date:	04/24/2008 12:30
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
04/22/2008 15:02	Insert	qipman	New_Rule	

There are 1 records on this report.

The following table describes the fields on the report.

Table 29-42 Rule Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
Rule Name	The name of the rule that is the subject of this report.
IPv4/v6	Indicates whether it is an IPv4 or an IPv6 rule
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

END OF STEPS

Produce a MyView Audit report

Purpose

Use this procedure to produce a MyView Audit report. Instructions are provided for access from the Reports hierarchy or from the MyView Properties page.

From the menu or toolbar

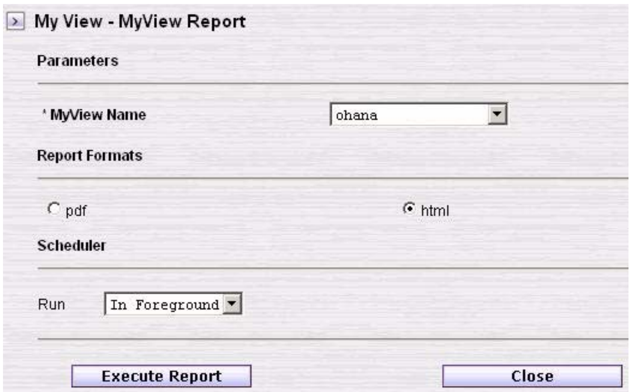
To produce a MyView Audit report, follow these steps.

1 Click the **Reports** tab.

Result: The Reports hierarchy opens.

2 In the **Infrastructure-Audit** section, click **MyView**.

Result: The MyView Audit Report page opens.



3 Select a view from the **MyView Name** drop-down list.

4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to “View scheduled jobs” (p. 30-3) for more information.

END OF STEPS

From the Personal View Properties page

To produce a MyView Audit report on a view in the MyView or MyView Management hierarchy, follow these steps.

1 Select the view on which you want to report.

Result: The Personal View Properties page opens.

2 Click **Reports**.

Result: The Configured Reports page opens.

3 Click the **Audit MyView** link.

Result: The MyView Audit Report page opens in the Report Execution window.

4 The report defaults to a 24-hour date range prior to the time you selected the report. To change either the **From Date** or the **To Date** values, click the Calendar icon and use the widget controls to change time, month, day or year values.

5 The report defaults to data sorted in **Ascending** order. Select **Descending** order if required.

6 The report output defaults to **html** format. If you prefer to view output in a PDF file, select **pdf**.

7 Choose when to run the report in the **Scheduler** section. Refer to "Schedule a report" (p. 29-6) for more information.

8 Click **Execute Report**.

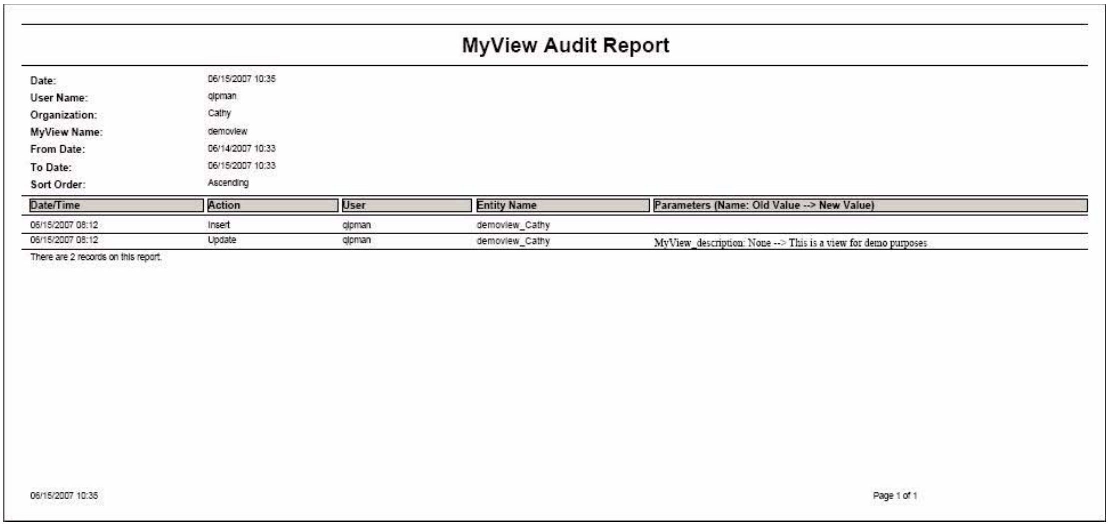
Result: If the job is scheduled in foreground, the report opens. If the job is scheduled in background or at a later time, the Job Scheduler page opens. Refer to "View scheduled jobs" (p. 30-3) for more information.

END OF STEPS

Report format

The MyView Audit report appears as follows.

Figure 29-40 Sample MyView Audit report



MyView Audit Report

Date:	06/15/2007 10:35
User Name:	qlpman
Organization:	Cathy
MyView Name:	demoview
From Date:	06/14/2007 10:33
To Date:	06/15/2007 10:33
Sort Order:	Ascending

Date/Time	Action	User	Entity Name	Parameters (Name: Old Value --> New Value)
06/15/2007 08:12	Insert	qlpman	demoview_Cathy	
06/15/2007 08:12	Update	qlpman	demoview_Cathy	MyView_description: None --> This is a view for demo purposes

There are 2 records on this report.

06/15/2007 10:35 Page 1 of 1

The following table describes the fields on the report.

Table 29-43 MyView Audit report fields

Field	Description
Date	Date and time the report was produced.
User Name	User who produced the report.
Organization	Organization where the item is located
MyView Name	The name of the view that is the subject of this report.
From Date	Starting date for the audit report date range.
To Date	Ending date for the audit report date range.
Sort order	Indicates whether data is sorted in Ascending or Descending order.
Column headings	
Date/Time	Date and time that the action occurred.
Action	Action that triggered the audit entry.
User	User who performed the action.
Entity Name	Component affected by the user.
Parameters (Name: Old Value > New Value)	The specific value change that occurred, showing the previous and revised values.

30 Job scheduler

Overview

Purpose

This chapter describes how to use the Job Scheduler.

Contents

This chapter covers these topics.

Job scheduler

Overview

Purpose

The Job Scheduler feature is designed to avoid the user having to wait an indeterminately long time for a request to complete, and to allow for jobs to be scheduled to run at a later time. All jobs are run as the VitalQIP Administrator who scheduled the job.

Supported areas for scheduling

The Job Scheduler is supported in the following areas of the VitalQIP web client:

Table 30-1 Job Scheduler support

Menu	Function	Reference
IPv4 Address Management	Modify V4 subnets	"Modify subnet profile" (p. 9-43) "Modify multiple subnet properties" (p. 9-57)
	Delete V4 subnets	"Delete multiple subnets" (p. 9-70)
	Modify V4 objects	"Modify multiple object properties" (p. 10-16)
IPv6 Address Management	Add V6 subnets	"Add a subnet" (p. 16-11) "Schedule subnet configuration" (p. 16-13).
	Split V6 subnets	"Split a subnet" (p. 16-18) "Schedule subnet configuration" (p. 16-13)
	Block renumbering	"Renumber a block" (p. 28-29) (Block Allocation) "Renumber a subnet" (p. 16-21) (Pv6 Address Management) "Schedule subnet configuration" (p. 16-13).
DHCP	DHCP push	"Generate DHCP configuration files" (p. 22-4)
	Clone DHCP server	"Clone a DHCP server" (p. 19-9)
DNS	DNS push	"Generate DHCP configuration files" (p. 22-4).
	Clone DNS server	"Clone a DNS server" (p. 13-18)
Zones	Modify zones	"Add/modify a zone" (p. 14-7) "Modify multiple zones" (p. 14-10)
Reports	All reports	Refer to descriptions of each report in Chapter 13 and "Schedule a report" (p. 29-6).

Users have a choice of either running the job immediately (**In Foreground**), or scheduling the job to run in background (**In Background**) or at a later time (**Scheduled At**). In the latter two cases, the user must check back at a later time in the Job Scheduler to verify that the job has completed.

Policy file configuration

Retain records

Scheduled job information is retained in the database, allowing future jobs to be preserved across server restarts. The results of past jobs are also retained to allow the user to see job status information and/or error conditions. The number of days to retain records is set by the **`retentionDays`** policy in the **`Job Scheduler`** section of the *qip.pcy* file.

Concurrent jobs

While multiple jobs can be run concurrently, users should take care not to run many simultaneous resource-intensive jobs. The exact number of supported concurrent jobs can be configured with the **jobThreads** policy in the **`Job Scheduler`** section of the *qip.pcy* file.

View scheduled jobs

Purpose

Use this procedure to check the status of scheduled jobs. You can specify various filter criteria to narrow the list of displayed jobs.

Before you begin

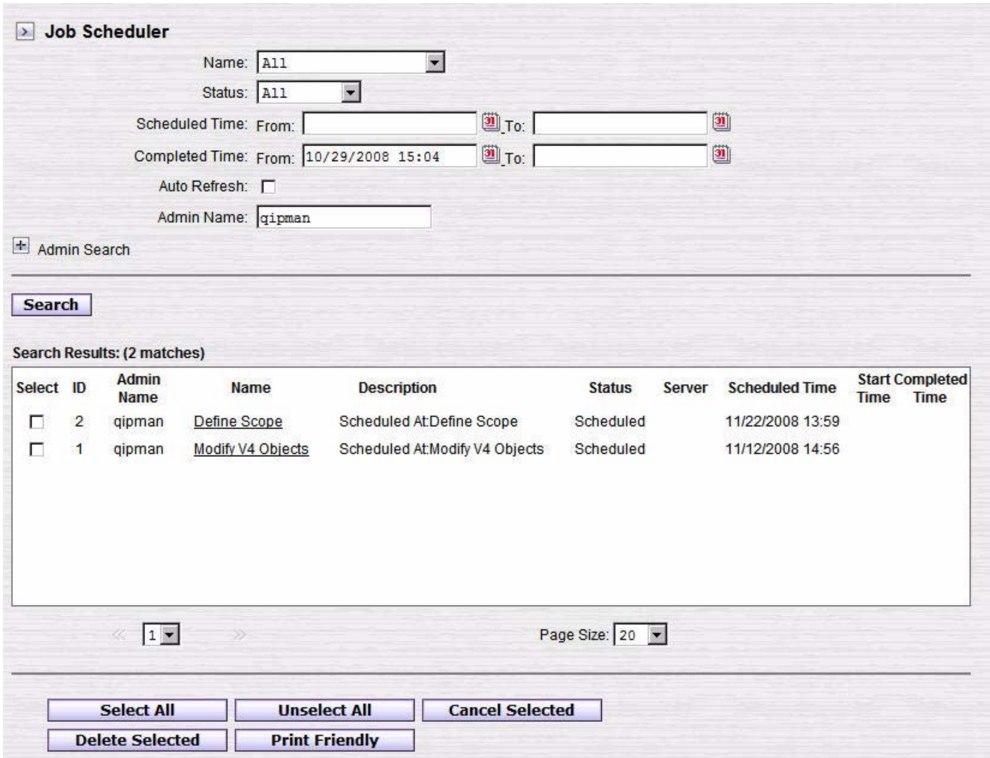
Search results are restricted by the organization the user is logged into.

Procedure

To check scheduled job status, follow these steps.

1 Mouse over **Infrastructure** and click **Job Scheduler**.

Result: The Job Scheduler page opens. The job scheduler defaults to showing all jobs for the current user of all status types over the last two weeks.



Note: If no jobs are currently saved in the VitalQIP database for the current user, a dialog box opens with the message **The search returned no results**. Click **OK** to close it.

2 To refine your job list, refer to the following table as you modify field values.

Table 30-2 Job Scheduler fields

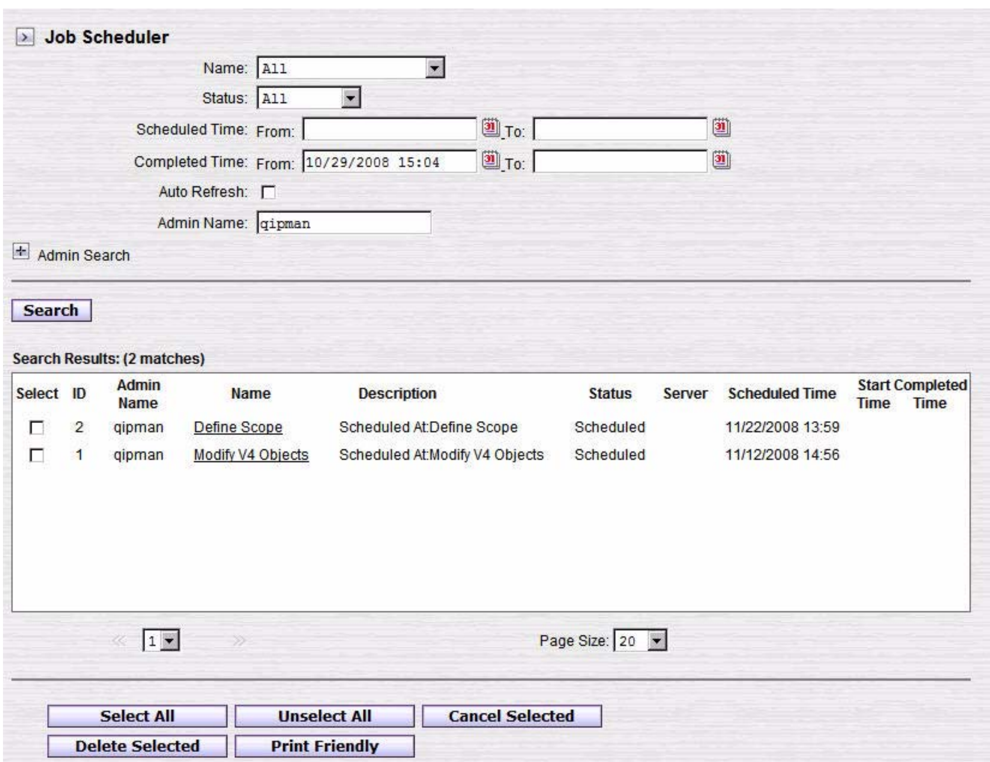
Field	Description
Name	Select a job category from the drop-down list of the following job types: • **All** • **Add V6 Subnets** • **Push DNS** • **Renumber V6 Subnet** • **Split V6 Subnet** • **Run Report** • **Renumber Block** • **Create IPv4 Objects** • **Push DHCP** • **Push DC** • **Change DHCP Logging** • **Modify Scope** • **Define Scope** • **Delete V4 Subnets** • **Modify V4 Subnets** • **Modify V4 Objects** • **Modify Zones** • **Clone Server** The default value is **All**.
Status	Select a status category from the drop-down list of status choices: • **All** • **Running** • **Pending** • **Scheduled** • **Completed** • **Failed** • **Cancelled** The default value is **All**.

Field	Description
Scheduled Time: From	Filters for jobs that were scheduled or were started after the specified time. To specify a date and time, follow these steps. 1. Click the Calendar icon ( ). **Result:** The Calendar widget opens with the current date and time.  2. Choose from the following actions. a. To choose a different time, click in the hour and minute fields and enter a new time in 24-hour format. b. To choose a different month, choose a later month from the month drop-down list. c. To choose a different year, click > to enter a future year or < to return to a prior year. d. To choose a different day, click another day in the month. **Result:** After a different day is clicked, the calendar widget closes and a date and time are displayed.
Scheduled Time: To	Filters for jobs that were scheduled or were started before the specified time. To specify a date and time, click the Calendar icon ( ) and follow the steps above.
Completed Time: From	Filters on jobs that have completed after the specified time, or do not filter if no time specified. Jobs that have not yet completed are not filtered. Defaults to two weeks before the current date. To specify a date and time, click the Calendar icon ( ) and follow the steps above.
Completed Time: To	Specifies a filter for jobs that have completed before the specified date and time. To specify a date and time, click the Calendar icon ( ) and follow the steps above.

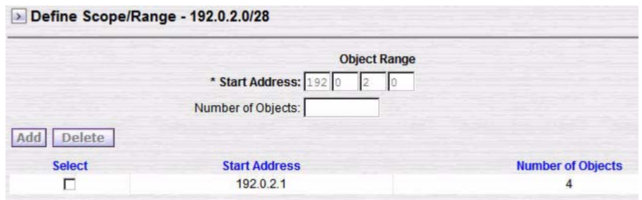
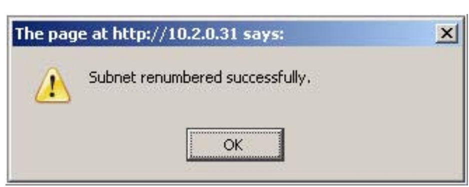
Field	Description
Auto Refresh	Specifies whether the page should refresh automatically. If checked, the list of jobs automatically refreshes every 15 seconds. This is not configurable by the user.
Admin Name	Filters on which user's jobs are displayed. This field is disabled if the user is not a master or organization administrator, since normal administrators may only view their own jobs. The default value is the current user. This field also displays the results of an Admin Search. For more information, refer to "Search for another administrator's jobs" (p. 30-10). • To view all users' jobs, clear this field. • To view a different user's jobs, you may also enter the user ID of the administrator rather than use the Admin Search function.

3 Click **Search**.

Result: If matches exist for your job search criteria, the **Search Results** list is refreshed. If no matches exist, a dialog box opens with the message **The search returned no results**. Click **OK** to close it.



4 Choose from one of the following actions.

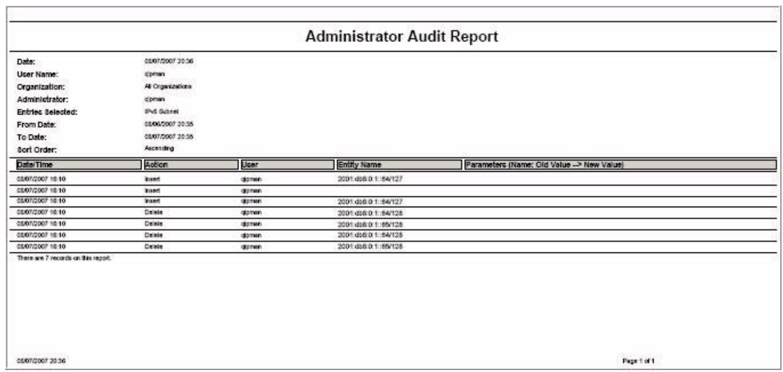
If you want to...	**Then...**
Review the job information	1. Click the link in the Search Results **Name** column. **Result:** A detailed job information page opens. All fields are read-only.  2. Click **OK**. **Result:** The detailed job information page closes and the Job Scheduler page appears.
Review a failed job	1. Click the **Failed** link in the Search Results **Status** column. **Result:** An error page opens.  2. Click **Details**. **Result:** A stack trace of the error opens. 3. Click **OK**. **Result:** The error page closes and the Job Scheduler page appears.
Review a completed subnet action or DNS push	1. Locate the job you wish to review in the **Search Results** list. The **Name** entry should read **Add V6 Subnets**, **Renumber V6 Subnets**, **Split V6 Subnets**, or **Push DNS**. 2. Click the **Completed** link in the **Status** column. **Result:** A dialog box opens.  3. Click **OK**. **Result:** The dialog box closes and the Job Scheduler page appears.

<table>
<tr><th>If you want to...</th><th>Then...</th></tr>
<tr><td>Review details of the a scheduled job</td><td>1. Locate the job you wish to review in the Search Results list.
2. Click the Run Report in the Name entry.

Result: A windows opens that shows the set values for running the report.

3. Click Close to exit the page.</td></tr>
<tr><td>Review a completed report</td><td>1. Locate the job you wish to review in the Search Results list. The Name entry should read Run Report.
2. Click the Completed link in the Status column.

Result: The report opens in another browser window.



3. Review the report. For information on the content of specific reports, refer to the relevant section describing the report in Chapter 29, “Reports”.
4. Close the report window when you have finished working with it.

Result: The Job Scheduler opens.</td></tr>
<tr><td>Cancel scheduled job(s)</td><td>1. Place a check mark in the job(s) you wish to cancel.
2. Click Cancel Selected.

Result: A dialog box opens with the message Job(s) cancelled successfully.

Note: You should only use the Select All button when the Search Results list contains only jobs with a status of Scheduled. Otherwise, an error message opens with the message Could not cancel selected jobs!

3. Click OK.

Result: The Job Scheduler opens.</td></tr>
</table>

If you want to...	Then...
Delete job(s)	1. Place a check mark in the job(s) you wish to delete. You may use the **Select All** button to select every job in the list. Click **Unselect All** to deselect all checked jobs. 2. Click **Delete Selected**. **Result:** A dialog box opens with the message **Job(s) deleted successfully**. 3. Click **OK**. **Result:** The Job Scheduler opens.
Print the list of jobs	1. Click **Print Friendly**. **Result:** The Job Scheduler opens with all jobs displayed in an easily printable format. The view has the same content as the Job Scheduler page except that the information is read-only and is not paginated. A maximum of 1000 rows can be displayed. 2. Print the list. Since there are many columns, you should choose to print in landscape format for best results. 3. Click **OK**. **Result:** The Job Scheduler opens.

5 To close the Job Scheduler page, select another function from the VitalQIP web client menu.

END OF STEPS

Search for another administrator's jobs

Purpose

Use this procedure to search for scheduled jobs belonging to another administrator.

Procedure

To search for another administrator's scheduled jobs, follow these steps.

1 Mouse over **Infrastructure** and click **Job Scheduler**.

Result: The Job Scheduler page opens. If there are no jobs scheduled, a dialog box opens with the message **The search returned no results**. Click **OK** to close it.

2 Enter job scheduler criteria as required in the **Job Scheduler** section. Refer to Table 30-2, "Job Scheduler fields" (p. 30-5) for information on the fields.

3 Expand the **Admin Search** section.

Result: The **Admin Name Filter** field opens.

4 Choose one of the following actions.

If you want to...	Then...
Filter administrator IDs ***manually***	1. Enter your search criteria in the **Admin Name Filter** field. You may use the wildcard character (*) as needed. To clear the **Admin Name Filter**, click **Clear**. 2. Click **Search** (in the **Admin Search** section). **Result:** The results of your search criteria are displayed in the administrator ID list. 3. Select the administrator whose job list you wish to view. **Result:** The administrator ID appears in the **Admin Name** field.
Filter administrator IDs ***automatically***	1. Check the **Auto Complete** check box. **Result:** The **Search** button above the list of administrator IDs is grayed out. 2. Enter your search criteria in the **Admin Name Filter** field. You may use the wildcard character (*) as needed. To clear the **Admin Name Filter**, click **Clear**. **Result:** The results of your search criteria are displayed in the administrator ID list as you enter text. 3. Select the administrator whose job list you wish to view. **Result:** The administrator ID appears in the **Admin Name** field.

5 Click **Search** (above the **Search Results** list).

Result: If matches exist for your job search criteria, the **Search Results** list is populated. If no matches exist, a dialog box opens with the message **The search returned no results**. Click **OK** to close it.

6 For information on other actions you may take, refer to Step 4 in "View scheduled jobs" (p. 30-3).

END OF STEPS

31 Troubleshooting

Overview

Purpose

This chapter contains information you can use to troubleshoot the VitalQIP web client.

Contents

This chapter covers these topics.

Troubleshooting the web client

Application errors

Purpose

This section describes some common application problems and suggested solutions.

Table 31-1 Troubleshooting problems

Problem	Solution
Web GUI does not process commands and does not provide an error message.	Pop-ups may be disabled in your Web browser. Be sure that pop-ups are enabled for VitalQIP, as the application uses this function to provide messages to the user.
Firefox prompts you to “Turn off unresponsive script.”	1. Type **`about:config`** in Firefox’s address bar. 2. Filter down to the value for **`dom.max_script_run_time`**. 3. Change the value to something higher than the default (which is 5) or set it to 0 which allows the script to run for as long as it needs. 4. Further information: **http://kb.mozillazine.org/Dom.max_script_run_time**
Browser cannot display the VitalQIP Web GUI or provides an error message indicating a proxy problem.	If the VitalQIP web server is on your corporate intranet, and you have proxies defined, you may need to adjust the users' proxy exception lists. **Internet Explorer:** 1. Click on **Tools** > **Internet Options** > **Connections** > **LAN Settings** > **Advanced**. 2. List is in the **Exceptions** section. It is labeled "Do not use proxy server for addresses beginning with:". **Firefox:** 1. Click on **Tools** > **Options** > **Connection Setting**. 2. List is labeled **No Proxy For**. 3. If the users launch the web GUI using the fully qualified hostname web address (for example *http://webserver.lucent.com/qip*), ensure either the fully qualified hostname or *.domain is listed as an exception (for example *.lucent.com). 4. If the users launch the web GUI using the IP address web address (for example *http://1.2.3.4/qip*), ensure the specific web server IP address is listed as an exception (for example 1.2.3.4).

Problem	**Solution**
After localization and login,the main tabs do not appear correctly, or the Login screen is missing its splash screen,	Check the localization steps. The required images files are not copied.
After localization, labels for some Web Client objects (for example, field names, page titles, static values in drop-down lists or Hierarchy) have a value of "UNDEFINED".	Check the *GuiCatalog_<country Code>.properties* file, make sure that the tag name for that label has not been altered.
• One web browser cannot display the Web Client, but another on the same machine can. • Web browser cannot display the Web Client using a URL, but can display it using an IP address.	Clear all cookies in the browser that came from VitalQIP.
The web UI cannot be launched on occasion.	This problem occurs when the servlet is unable to find a page that is requested. One scenario where this occurs is when a user who has previously logged in using a language (such as Chinese) reinstalls VitalQIP and deletes the language directory containing the Chinese localized files.To fix the problem, either clear all cookies from the browser, or delete the cookies in the browser that came from the VitalQIP servlet. For example, if you are using Mozilla FireFox, follow these steps. 1. Select **Tools** > **Options**. In the Options dialog box and click the Privacy (padlock) icon. 2. Select the **Cookies** tab 3. Click the **View Cookies** button. A list of cookies organized by originating server opens. 4. Delete the cookies under the fully qualified domain name or IP address of the VitalQIP web server.
"Long Running Script" browser message can occur when expanding networks, subnets, and so on in large datasets.	In most cases, it is recommended to allow the script run until the intended results are displayed. If desired, the message timeout can be altered. Contact technical support for details.

Internet registry email not being sent

Purpose

In some instances, email to the Internet Registries is not being sent, although a success message is seen after completion of the RIR Screen. This typically occurs when allocating a Used IPv4/IPv6 block in a pool associated with one of the internet registries, ARIN, RIPE, APNIC, or AFRInic.

Resolution

Ensure the SMTP server's IP address and port is correctly specified in the *$QIPHOME/web/conf/email.properties* file on the server where the VitalQIP web client is installed. If the SMTP server is having problems or is not configured correctly, the *$QIPHOME/tomcat/logs/catalina.out* file contains messages similar to the following:

```
Mail server connection failed; nested exception is
   javax.mail.MessagingException
: Could not connect to SMTP host: 12.12.12.12, port: 25;
  nested exception is:
        java.net.ConnectException: Connection timed out
```

or

```
Mail server connection failed; nested exception is
   javax.mail.MessagingException
: Could not connect to SMTP host: 10.200.100.140, port: 25;
  nested exception is:
        java.net.ConnectException: Connection refused
```

After correcting the email parameters in the *$QIPHOME/web/conf/email.properties* file, re-start the Tomcat services. Refer to "Start or stop the Tomcat server" (p. 1-5) for information about this procedure.

32 Northbound interface

Overview

Purpose

This chapter contains information on the northbound interface that is used by one or more upstream systems to send address allocation records to VitalQIP.

Contents

This chapter contains the following topics.

VitalQIP northbound interface

Overview

Purpose

The VitalQIP northbound interface (also known as the VitalQIP Web Service) is a SOAP-based web service that enables SOAP clients to access the address allocation, address management, DNS and other infrastructures related functionality provided by VitalQIP. The interface uses the Simple Object Access Protocol (SOAP), which encodes messages using Extensible Markup Language (XML), and uses HTTP and HTTPS for transport. The Web Services Description Language (WSDL) specifies interface operations, their associated messages and message parameters, the schema for the data types required by the messages, port types, and binding information.

Operations available through northbound interface

The following operations are supported by the VitalQIP Web Service Application. An operation can include one or more messages. For the VitalQIP Web Service Application, each operation can have a Request message, a Response message, and a Fault message.

VitalQIP Web Service supports the following objects:

- Access Control Device
- Access Control Subscriber
- Address Management Blocks
- Address Pools
- Address Ranges
- Blocks
- DNS Views (Views, Zones, Servers and Access Control Lists)
- Internet Registries
- IPv4 Subnet (Get and Search only)
- IPv6 Subnet
- Maintainers
- Managed Files
- Nodes
- Rules
- Templates
- User Defined Attributes (UDA)
- User Defined Attribute Groups

For more information on messages and programming a client to use the northbound interface, contact your Lucent sales representative to obtain the *VitalQIP Web Service Specification*. The northbound interface uses a Web Services Description Language (WSDL) document. WSDL is written in Extensible Markup Language (XML) and defines a SOAP interface to VitalQIP. The WSDL document is located at the following URL:

http://<WebServerIPAddress>:<WebServerport>/ws/services/VQIPWebService?wsdl

Using northbound interface

Starting VitalQIP northbound interface

The northbound interface can be started along with the rest of the VitalQIP services by executing the following:

If your operating system is...	Then..
UNIX	1. Go to the $QIPHOME directory. 2. Execute: **`./startTomcat.sh`**
Windows	1. From the Desktop, select **Start** > **Programs** > **Administrative Tools** > **Services**. 2. From Services, right-click **VitalQIP Apache Tomcat 5.5 Server** and select **Start**.

Stopping VitalQIP northbound interface

The northbound interface can be stopped along with the rest of the VitalQIP services. Refer to the following table to choose an action.

If your operating system is...	Then..
UNIX	1. Go to the $QIPHOME directory. 2. Execute: **`./stopTomcat.sh`**
Windows	1. From the Desktop, select **Start** > **Programs** > **Administrative Tools** > **Services**. 2. From Services, right-click **VitalQIP Apache Tomcat 5.5 Server** and select **Stop**.

Checking status of VitalQIP northbound interface

Check the availability of the northbound interface by accessing the following URL:

http://<ServerIPAddress>:<WebServerPort>/ws/services/listServices

where ***<ServerIPAddress>*** and ***<WebServerPort>*** are the IP address and port respectively being used by the VitalQIP Apache Tomcat Web Server. If the Web Service is accessible, **VQIPWebService** appears in the list of services.

Glossary

A

AC
Access Control

ACL
Access Control List

AD
Active Directory

AfriNIC
African Network Information Centre

API
Application Programming Interface

APNIC
Asia Pacific Network Information Centre

ARIN
American Registry for Internet Numbers

ARP
Address Resolution Protocol

ASCII
American Standard Code for Information Interchange

B

BIND
Berkeley Internet Name Domain

C

CIDR
Classless Inter-Domain Routing

CMS
Call Management Server

CNAME
Canonical Name

D

DC
Domain Controller

DHCP
Dynamic Host Configuration Protocol

DLL
Dynamic Link Library

DN
Distinguished Name

DNS
Domain Name System

DOCSIS
Data Over Cable Service Interface Specification

DSS
Domain SAP/RIP Server

E

ENUM
E.164 NUmber Mapping

F

FQDN
Fully Qualified Domain Name

G

GAP
Global Allocation Policy

GSS TSIG
Generic Security Service - Transaction Signature

H

HD
Host Density

HTML
HyperText Markup Language

HTTP
Hypertext Transfer Protocol

I

IANA
Internet Assigned Numbers Authority

ICMP
Internet Control Message Protocol

IEEE
Institute of Electrical and Electronics Engineers

IEN
Internet Experiment Note

IRC
Internet Relay Chat

ISP
Internet Service Provider

K

KDC
Key Distribution Center

L

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

LDIF
LDAP Data Interchange Format

LDRM
Lucent DHCP Rules Manager

M

MAC
Media Access Control

MADCAP
Multicast Address Dynamic Client Allocation Protocol

MTA
Mail Transfer Agent

MTU
Maximum Transmit Unit

MX
Mail Exchanger

N

NAPTR
Name Authority Pointer

NBDD
NetBIOS Datagram Distribution

NDS
Novell Directory Services

NIC
Network Interface Card

NIS
Network Information Service

NNTP
Network News Transport Protocol

NTP
Network Time Protocol

NVT
Network Virtual Terminal

O

OSPF
Open Shortest Path First

P

PDF
Portable Document Format

POP
Post Office Protocol

POSIX
Portable Operating System Interface for Unix

PTR
Pointer

R

RFC
Request For Comment

RIPE
Réseaux IP Européens

RIR
Regional Internet Registry

RNDC
Remote Name Daemon Controller

RR
Resource Record

S

SIP
Session Initiation Protocol

SLP
Service Location Protocol

SNMP
Simple Network Management Protocol

SOA
Start Of Authority

STDA
StreetTalk Directory Assistance

SWIP
Shared WhoIS Project

T

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TGT
Ticket Granting Ticket

TTL
Time To Live

TZ
Time Zone

U

UAP
User Authentication Protocol

UDA
User Defined Attribute

UDF
User Defined Field

UDP
User Datagram Protocol

UI
User Interface

URL
Uniform Resource Locator

V

VLSM
Variable Length Subnet Masking

W

WWW
World Wide Web

Index