VitalQIP® DNS/DHCP & IP Management Software

VitalQIP® (QIP) | Release 7.2

User's Guide

190-409-068R7.2
Issue 3
July 2009

License statement

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

Contents

About this document

Purpose xv

Reason for reissue xv

How to use this information product xvii

Conventions used xviii

Related information xix

Product Training Support xx

Technical support xx

How to order xxi

How to comment xxi

1 Operate the VitalQIP management system

Log into VitalQIP

Log in 1-4

Change administrator password 1-7

Log in as another user or organization 1-9

Exit VitalQIP 1-10

The VitalQIP management system

The VitalQIP toolbars 1-13

User modes in VitalQIP 1-18

VitalQIP infrastructure overview

Navigate the VitalQIP GUI

QIP Hierarchy function 1-25

Use the QIP Hierarchy function 1-26

Use DHCP Server hierarchy 1-28

Use DNS Server hierarchy 1-30

Create User-Defined hierarchy 1-32

Quick View

Use Network Quick View 1-36

Use Subnet Quick View 1-38

Domain folders

Maintenance of folders 1-40

Go to/search function

Find an object 1-43

Find an object by location 1-49

Find an object by contact 1-51

2 DHCP policies and templates

DHCP/Bootp templates

DHCP template classes and options 2-3

Add a new template class 2-5

Add a new option to a DHCP class 2-7

Rename a DHCP template class 2-11

Modify a DHCP template option 2-12

Delete a DHCP template class or option 2-13

DHCP/Bootp template option values

RFC 1497 Vendor Extensions 2-15

IP Layer Parameters per Host 2-19

IP Layer Parameter per Interface 2-21

Link Layer Parameters per Interface 2-24

TCP Parameters 2-25

Application and Service Parameters 2-26

DHCP Extensions 2-33

Novell options 2-37

RFC 2563 options 2-40

SLP Protocol options 2-41

User Authentication Protocol options 2-43

Domain Search option 2-44

PacketCable options 2-45

DHCP/Bootp option templates

Standard templates offered with VitalQIP 2-52

The general template 2-53

The microsoft_clients template 2-54

The Windows multicast template ... 2-55
Create a new DHCP option template ... 2-56
Enter user-defined values ... 2-59
Modify a DHCP option template ... 2-60
Delete a DHCP option template ... 2-61
Copy a DHCP option template ... 2-62

DHCP policy templates

Create a DHCP policy template ... 2-64
DHCP configuration file policies ... 2-67
DHCP server policies ... 2-71
Set PingDelay policy ... 2-89

Client Class

Add a new Client Class ... 2-91
Modify a Client Class ... 2-94
Delete a Client Class ... 2-95
3 Object policies and profiles

Access Control Lists (ACLs)

Create an ACL template ... 3-4
Modify an ACL template ... 3-8
Delete an ACL template ... 3-9

Naming policies

Establish object naming policies ... 3-11
Customize object names ... 3-12
Use a business unit ID to customize object naming policies ... 3-14
Name dynamically allocated objects ... 3-17
User-defined object naming policy user exit ... 3-18

Global policies

Establish global policies ... 3-22

Profiles

Manufacturer Profiles ... 3-42
Add a new manufacturer ... 3-43
Apply a model name to a manufacturer ... 3-45
Change the manufacturer profile ... 3-47

Delete a manufacturer profile 3-48
Manage location profiles 3-49
Manage contact profiles 3-51

User-defined fields

Create a user-defined field 3-54
Modify a user-defined field 3-55
Delete a user-defined field 3-56

Object classes

Create a new object class 3-58
Modify an object class 3-61
Delete an object class 3-62
4 Manage servers

Servers

Add a server 4-4
Modify a server profile 4-8
Delete a server profile 4-9
Enter email addresses 4-10

DHCP and Bootp servers

Lucent DHCP server configuration files 4-11
Client Naming Policy 4-13
VitalQIP interface 4-14
Start and stop the DHCP Service/VitalQIP Update Service 4-16
Bootp server type 4-17
Lucent DHCP 5.4, Lucent DHCP 5.5, and Lucent DHCP 5.6 server types 4-19
Support for DHCP failover server 4-24
Configuration of failover parameters on primary DHCP server 4-26
Configuration of dhcpd.pcy on failover DHCP server 4-30
Windows 2003 DHCP server type 4-33

Global MAC address pools

Define global MAC address pools 4-38

DNS servers

DNS configuration and data files 4-41
WINS gateway support 4-42

Remote DNS servers 4-43
NIS, OS Files, and the domain 4-44
BIND-9 DNS server type 4-45
LUCENT DNS 4.X server type 4-51
Windows 2003 DNS server type 4-56
NIS server type 4-62
LOCAL HOST server type 4-64
Windows 2003 Domain Controller server type 4-66

Non-managed DNS servers

Define a non-managed DNS server 4-69
Establish zone options 4-73
Modify a non-managed server 4-75
Delete a non-managed server 4-76
5 Manage networks

Organizations

Add an organization 5-5
Add values to user-defined fields 5-8
Modify an organization profile 5-9
Delete an organization profile 5-10

Domains

Define internal root zones for internal root servers 5-11
Create domain profile 5-13
Define primary/secondary servers 5-18
Set up Resource Records for the domain 5-21
Set zone options 5-26
Extensions zone options 5-27
BIND 8.X zone options 5-28
BIND 9.X zone options 5-31
LUCENT DNS 3.X zone options 5-35
LUCENT DNS 4.X zone options 5-38
Windows 2003 DNS Zone Options 5-42
Set up user-defined fields for a domain 5-44
Modify a domain profile 5-45

Delete a domain profile 5-46
Change DNS options on multiple zones 5-47
Change multiple zone options 5-49
Change user-defined fields in multiple zones 5-50

Networks and subnets

Create a new network 5-54
Modify a network 5-57
Delete a network 5-58
Create subnets 5-59
Use the Auto. Calculate option 5-62
Use the User Define option 5-64
Split or join subnets 5-65
Assign a primary DNS server to one or more subnets 5-67
Establish network warnings 5-68
Define address ranges for the network 5-69

Reverse zones

Set up a reverse zone 5-72
Split a reverse zone 5-75
Review and modify reverse zone properties 5-77
Review reverse zone information 5-78
Review/define primary and secondary servers 5-80
Reverse zone resource record setup 5-83
Define reverse zone options 5-85
Reverse zone user-defined field setup 5-87

OSPF areas

OSPF explained 5-88
Create an OSPF area 5-90
Manage subnets with an OSPF area 5-93
Manage ranges with an OSPF area 5-94
Establish OSPF area warnings 5-97
Modify an OSPF area 5-99
Delete an OSPF area 5-100

Subnet organizations

Define a subnet organization 5-102
Apply Global Allocation Policies 5-105
Set up a subnet organization warning 5-107
Set up a Windows 2003 site for a subnet organization 5-109
Modify a subnet organization 5-111
Delete a subnet organization 5-112

Applications

Add an application 5-114
Modify an application 5-116
Delete an application 5-117

6 Manage administrators and users

Administrative roles

Create an administrative role 6-4
Modify an administrative role 6-7
Delete an administrative role 6-8
Check administrative role assignments 6-9

Administrators

Create an administrator profile 6-12
Create an administrator access list 6-23
Customize administrator menus 6-30
Modify an administrator profile 6-33
Delete an administrator profile 6-35
Assign an administrative role 6-36

User groups

Add a user group 6-40
Modify a user group 6-43
Delete a user group 6-44

Users and groups

Define VitalQIP users 6-46
Enter location information 6-49
Assign users to groups 6-51
Associate users with subnets 6-52

Associate users with managed ranges 6-53
Assign user-defined fields values 6-55
Modify a user profile 6-56
Delete a user profile 6-57
View user groups 6-58

7 Manage subnets and objects

Manage subnet profiles

Select a subnet 7-4
Change the way subnets are displayed 7-6
Search for a subnet 7-7
Save or print subnet information 7-8
View/modify subnet profile 7-9
Set Windows DNS secure update policies 7-14
Assign location and contact information 7-15
Manage object ranges in subnet 7-16
Assign user-defined fields to subnet 7-18

Object management

Edit object properties 7-23

Manage objects in subnet

Add a static object 7-27
Enter object aliases 7-34
Enter asset information 7-38
Enter general information 7-40
Enter user-defined fields 7-43
Enter users’ information 7-44
Enter resource record information 7-45
Enter router information 7-49
Enter mail server information 7-51
Enter wiring HUB information 7-53
Enter wiring HUB slot and port 7-55
Enter DECNet information 7-57
Enter IPX information 7-58
Enter NetBIOS information 7-59

Enter Manual Bootp information 7-60
Enter Dynamic Configuration information 7-62
Enter Windows DNS secure update policies 7-65
Allocate a dynamic IP address 7-67
Modify a dynamically allocated IP address 7-75
Un-allocate a dynamically allocated object 7-77
Reserve an IP address 7-79
Modify a reserved IP address 7-82
Un-reserve one or more IP addresses 7-83
Subnet Moves 7-84
Move a Subnet 7-85
Move an object 7-87
Schedule an object move 7-89
Schedule an object move and specify the move destination 7-92
Modify a scheduled move 7-94
Cancel a scheduled move 7-96

Reclaim addresses

Schedule a reclaim 7-98
Check status of a scheduled reclaim 7-104
Reclaim addresses manually 7-108
Sample reclaim reports 7-110

8 Network services

Network services overview

Search for text in configuration file 8-4
Copy configuration file 8-5
Print configuration file 8-6
Email configuration file 8-7

DHCP generation

Control debug levels for Lucent DHCP servers 8-10
Generate DHCP configuration files 8-11

DNS generation

Generate DNS configuration and data files 8-19

Bootptab file generation

Generate the Bootptab file 8-25

Local host generation

Generate local host records 8-29

NIS generation

Generate NIS Files 8-33

Windows Domain Controller generation

Generate Windows Domain Controller files 8-37

View active leases

Generate active leases 8-41
Modify active lease reports 8-43
Delete an active lease 8-44

9 Reports

Reports overview

Report types 9-6

Object List Reports

Generate an Objects by Address Range report 9-9
Generate an Objects by Location report 9-11
Generate an Objects by Administrator report 9-13
Generate an Objects by Application report 9-15

Inquire reports

Generate an Inquire report 9-19

Free Subnet report

Generate a Free Subnet report 9-26

DHCP reports

Generate a DHCP report 9-29

Administrator Profile reports

Generate an Administrator Profile report 9-32

Administrative Role reports

Generate an Administrative Role report 9-36

DNS Zone report

Create a DNS Zone report 9-39

Object Audit History report

Create an Object Audit History report 9-42

Administrator Audit History

Create an Administrator Audit History report 9-45

10 Import data

VitalQIP import/export functions

Import with VitalQIP GUI 10-2

Import data for domain, OSPF area, network, subnet, or subnet organization 10-3

Import data for objects 10-6

Import data into a MAC address pool 10-10

A Application default file for Motif client

Application Specific Resources A-2

Sample QIPManage.ad A-5

ip-manage command line options A-16

IN Index

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, UNIX, and Windows platforms. VitalQIP works with directory services and RDBMS configurations.

Reason for reissue

The following table lists the changes to the VitalQIP GUI in release 7.2 that required the *VitalQIP User's Guide* to be reissued.

Table 1 User's Guide changes

Issue	Feature name	Description	Feature impact
3	Lucent DHCP 5.6 server type	VitalQIP now supports Lucent DHCP 5.6 server type.	• "AbusiveClientLockout" (p. 2-71) • "AbusiveClientMonitorPeriod" (p. 2-71) • "AbusiveClientWarningCount" (p. 2-71) • "SupportClientID" (p. 2-86)
3		Added information about minimum leasetime that can be requested for the HonorRequestedLeaseTime policy.	"HonorRequestedLeaseTime" (p. 2-78)

Issue	Feature name	Description	Feature impact
3		Added a note after step 7 in the section “Add a static object”. Fixes VQIP00020537.	“Add a static object” (p. 7-27)
3	Client ID is displayed in the Object profile.	Client ID is a read-only text field. It appears only for the object types **Dynamic DHCP**, **Manual DHCP**, and **Automatic DHCP**.	“Client ID” (p. 7-63)
3		Modified verbiage for the policy name “DNS SOA Serial Number Type”. Fixes VQIP00020532.	“DNS SOA Serial Number Type” (p. 3-31)
3		Modified the description for the DHCP server policy **DefaultUnavailableThreshold**. Fixes VQIP00021879.	“DefaultUnavailableThreshold” (p. 2-76)
3	DNSSEC enabled server	The **DNSSEC enabled server** parameter is added to support DNSSEC on DNS servers.	Table 4-9, “DNS BIND-9 parameters” (p. 4-45) and Table 4-10, “LUCENT DNS 4.X parameters” (p. 4-51)
3	DNSSEC enabled zone	The **DNSSEC enabled server** parameter is added to support DNSSEC on zones.	Table 5-7, “BIND 9.X zone options” (p. 5-31) and Table 5-9, “LUCENT DNS 4.X zone options” (p. 5-38)
3		Added a note in the topic “The Options Menu” of the section “Object Management”. Fixes VQIP00022193.	Note on page 7-22.
3	Removed all occurences of LUCENT DNS 3.X and BIND-8.X DNS server types.		Throughout the book.
2	Lucent DHCP 5.5 Server type	VitalQIP now supports Lucent DHCP 5.5 Server type.	“Lucent DHCP 5.4, Lucent DHCP 5.5, and Lucent DHCP 5.6 server types” (p. 4-19)

Issue	Feature name	Description	Feature impact
2	Server Level Policies	VitalQIP now supports the following additional Server Level Policies: • SupportMultiUserClass • SupportRelayAgentServer Override • UpdatePreclusionDuration • AckRenewForUnusedAddress • DropAllDhcpInformPackets • OfferOnlyApiRequestedAddress • SharedNetworkThreshold Processing • SupportRelayAgentServer Override	"DHCP server policies" (p. 2-71)
2	DHCP 5.5 Server Options	• Broadcast and Multicast Control Service Domain List • Broadcast and Multicast Control Service Address List • Timezone specified as IEEE 1003.1 string text • Timezone specified as TZ Database string text • SIP Server Address List • SIP Server Domain List	"Application and Service Parameters" (p. 2-26)
2	Vendor Class column	The Vendor Class column has been added in the View Active Leases Information window.	Step 5 "Generate active leases" (p. 8-41)
1	Revised ACL template interface	The ACL template interface has been revised.	"Create an ACL template" (p. 3-4)

How to use this information product

This manual is organized as follows:

Chapter 1, "Operate the VitalQIP management system"	This chapter provides information about operating the VitalQIP management system.

Chapter 2, "DHCP policies and templates"	This chapter provides information on setting up DHCP policies and templates.
Chapter 3, "Object policies and profiles"	This chapter covers the establishment of the policies for objects.
Chapter 4, "Manage servers"	This chapter covers the management of servers in VitalQIP.
Chapter 5, "Manage networks"	This chapter covers the management of the networks defined in VitalQIP.
Chapter 6, "Manage administrators and users"	This chapter covers the management of VitalQIP administrators and users.
Chapter 7, "Manage subnets and objects"	This chapter covers the management of subnets and objects.
Chapter 8, "Network services"	This chapter covers the creation of necessary data and configuration files for DHCP and DNS management.
Chapter 9, "Reports"	This chapter covers reports and how to generate them. Sample reports are also included.
Chapter 10, "Import data"	This chapter covers importing and exporting data from VitalQIP using the interface. See the ***VitalQIP Command Line Interface User's Guide*** for information on importing and exporting data using the command line interface.
Appendix A, "Application default file for Motif client"	This chapter describes the *QIPManage.ad* file, the application defaults file for the VitalQIP Motif client.

Conventions used

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

Table 2 Typographical conventions

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**.

Convention	Meaning	Example
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*
italics	Manual and book titles. Directories, paths, file names, and e-mail addresses.	See 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: 190-409-042)

  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: 190-409-043)

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

  This guide discusses and describes how to use the *VitalQIP Command Line Interface*.
- *VitalQIP Web Client User's Guide* (part number: 190-409-079)

  This guide describes how to use the web client 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.

Table 3 Technical support information

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	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 **https://support.lucent.com** or contact your local sales representative.

Region	Address	Contact information
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 order additional VitalQIP manuals online at **https://support.lucent.com**.

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**).

1 Operate the VitalQIP management system

Overview

Purpose

The purpose is to cover the basics for operating the VitalQIP management system.

Contents

The following topics are covered:

Log into VitalQIP	1-3
Log in	1-4
Change administrator password	1-7
Log in as another user or organization	1-9
Exit VitalQIP	1-10
The VitalQIP management system	1-11
The VitalQIP toolbars	1-13
User modes in VitalQIP	1-18
VitalQIP infrastructure overview	1-22
Navigate the VitalQIP GUI	1-25
QIP Hierarchy function	1-25
Use the QIP Hierarchy function	1-26
Use DHCP Server hierarchy	1-28
Use DNS Server hierarchy	1-30
Create User-Defined hierarchy	1-32
Quick View	1-35

Use Network Quick View	1-36
Use Subnet Quick View	1-38
Domain folders	1-40
Maintenance of folders	1-40
Go to/search function	1-42
Find an object	1-43
Find an object by location	1-49
Find an object by contact	1-51

Log into VitalQIP

Whether you are beginning by setting up the VitalQIP Infrastructure or using VitalQIP to manage IP addresses on a more routine basis, you need to log into the VitalQIP system. Before you log into VitalQIP for the first time, you need to find out your user name and password from your VitalQIP Administrator.

At any time, you can log in with another user name from the **File|Login** option of the VitalQIP main menu. Refer to "Log in as another user or organization" (p. 1-9).

Log in with several organizations

Once you have set up two or more organizations in your network infrastructure (refer to "Organizations" (p. 5-4)), your login process contains an Organization window when you log in as a Master administrator or as a Normal administrator with more than one organization in their Managed List.

Select the organization you want to manage from the **Organization** drop-down list and click **Continue**. Once you have defined other organizations, the default organization is the last organization you logged into.

> **Note:** If only one organization has been defined, the **Change Organization** option does not appear on the Login menu. Furthermore, the Organization drop-down list does not appears.

Log in

Purpose

Use this procedure to log into VitalQIP.

Before you begin

- A default Master Administrator user name of “qipman” with a password of “qipman” is established during installation. The “qipman” profile can be modified and even deleted as soon as there is another Master Administrator profile in the VitalQIP database.
- The QIPDATASERVER environment variable is the first entry displayed in the **Database** field. Other database-specific entries are listed beneath it. Setting the QIPDATASERVER value to the most frequently used database allows for less scrolling in search of the appropriate **Database** upon logging in.
- An Administrator Profile can become locked if an administrator fails to type the correct password after the configured number of times. Another administrator must change the password in the Administrator Profile to unlock the Administrator Profile. See “Create an administrator profile” (p. 6-12) for more information.

Procedure

To log into VitalQIP for the first time, follow these steps:

1 To begin the login process:

If you are…	**Then…**

Logging in on a UNIX operating system	• Export your display by executing:
	`DISPLAY=<ipaddr>:0.0`
	`export DISPLAY`
	• Before you run ip-manage, your VitalQIP environment variables need to be sourced. Environment variables and their values are stored in *$QIPHOME/etc/shrc* or *cshrc*. To set your environmental variables, issue the following commands:
	`cd <VitalQIP_directory>/etc`
	`. ./shrc` `OR` **`source cshrc`**
	• Change your directory to *$QIPHOME/usr/bin*.
	• Run:
	`./ip-manage &`
	The VitalQIP login window opens. For more information on **ip-manage**, see “ip-manage command line options” (p. A-16).

Logging in on a Windows operating system	From the Desktop, select **Start | Programs | VitalQIP | VitalQIP**. The VitalQIP login window opens.

2 Select a **Database** from the drop-down list box.

3 Type your **User Name** and press **Tab**.

4 Type your VitalQIP **Password** and press **Enter**.

5 The Password Change screen opens if password expiration is enabled and the password has expired, or the **Require New Admin Password** (located in the VitalQIP web client) is enabled and you are logging in for the first time. Do the following:

a. In the **Old Password** field, enter your old password.

b. In the **New Password** field, enter your new password.

c. In the **Retype New Password** field, enter you new password again.

6 If there is more than one organization, select the organization or click **Continue** to proceed.

The VitalQIP Management System window opens.

Note: If you receive error messages during login, refer to the *Administrator Reference Manual* for troubleshooting information.

END OF STEPS

Change administrator password

Purpose

For security reasons, you should change your password ***immediately*** after logging in for the first time.

Before you begin

- VitalQIP can place restrictions on passwords. These restrictions are configured in the Administrator Security window of the VitalQIP web client. For more information, see the *VitalQIP Web Client User's Guide*. 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 window of the VitalQIP web client. The acceptable complexity settings are:
  - Alpha only
  - Numeric only
  - No limitations
  - Alpha and numeric
- 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 by using the **`qip-crypt`** command. See the *VitalQIP Command Line Interface User's Guide* for information about **`qip-crypt`**.

Procedure

To change your password, follow these steps:

1 Select **Administrator Password** from the **File** menu. The Change Password window opens.

2 Type your old password and press **Enter**.

3 Type the new password you wish to use and press **Enter**. Retype your new password and press **Enter** or click **OK**. A confirmation window opens.

4 Click **OK**. Be sure to make note of your new password.

Note: After an administrator changes a password, it is essential that the administrator log out and log in again with the new password. Failure to do so will result in an error whenever the administrator tries to perform a file generation.

END OF STEPS

Log in as another user or organization

Purpose

Use this procedure to log into VitalQIP as another user or change to another organization without exiting the GUI.

Procedure

To log in as another user:

1 Select **File|Login|Change Server/Administrator**. The Login window opens, and you can log in as a different user.

2 The Password Change screen opens if password expiration is enabled and the password has expired, or the **Require New Admin Password** (located in the VitalQIP web client) is enabled and you are logging in for the first time. Do the following:

a. In the **Old Password** field, enter your old password.

b. In the **New Password** field, enter your new password.

c. In the **Retype New Password** field, enter you new password again.

3 If you have more than one organization, the Organization window opens. Select another organization and click **Continue**.

To log into another organization

To log into a different organization:

1 Select **File|Login|Change Organization**. The Organization window reopens.

2 Select a different organization and click **Continue**.

END OF STEPS

Exit VitalQIP

Purpose

Use this procedure to quit the VitalQIP database.

Procedure

To exit VitalQIP, follow these steps:

1 Select **Exit** from the **File** menu of the VitalQIP Management system main menu. A confirmation dialog box opens.

2 Click **Yes** to confirm that you want to exit.

END OF STEPS

The VitalQIP management system

The following paragraphs describe some shortcuts for use with the VitalQIP Management system.

Cancel a function

VitalQIP allows you to cancel any time-consuming function that displays a “Working” or “Processing” window.

These functions include network, reclaim and certain report functions while they are being processed. To cancel a function, click **Cancel** on the current window.

Enter a date and time

The standard format for entering a date and time is *mm/dd/yyyy hh:mm* (month/day/year hours:minutes - you do have to enter the **/** and : characters). If the date is entered in *mmddyy* format, VitalQIP rejects the date and issues an error message, requesting a four-digit year.

Help

Clicking on the **Help** menu allows you to access context-sensitive help topics via the GUI.

Keyboard commands

To emulate the Windows Explorer interface style more closely, the following Hierarchies and General keyboard commands are supported.

Hierarchies

These keyboard commands only work while you are in the Hierarchies.

- **F5** - refreshes current hierarchy.
- **F6** - tabs to next hierarchy tab (wraparound).
- **Shift-F6** - tabs to previous hierarchy tab (wraparound).
- **Left** and **Right** arrows - expands/contracts tree nodes.
- Alphanumeric keys - searches expanded tree nodes for match. The match text resets to a blank string after .75 seconds of keyboard inactivity. The search starts as soon as a key is entered. Example: typing “123” will find items that start with “1”, “12”, “123” in that order. To reset the search string, simply delay typing for .75 seconds.

General

These Keyboard Commands work wherever you are in the VitalQIP interface.

- **Alt-0** - moves the focus to the **Hierarchy** tab (currently selected tab/highlighted item).

- **Alt-1** - moves the focus to the GoTo/Search dialog.

The VitalQIP toolbars

The VitalQIP Management System main window contains toolbars that can be customized. Toolbars enable you to customize the look and function of your main window to suit your application needs. You can easily customize toolbars by adding and removing buttons, creating your own custom toolbars, hiding or displaying toolbars, and moving toolbars.

When you first log into VitalQIP, all VitalQIP-provided toolbars are displayed in the main window. You can drag and drop the toolbars, dock them to any edge of the window, or leave them as windows anywhere on the desktop. Click your mouse on the double bar (gripper) at the left of the toolbar and drag it to another portion of the window.

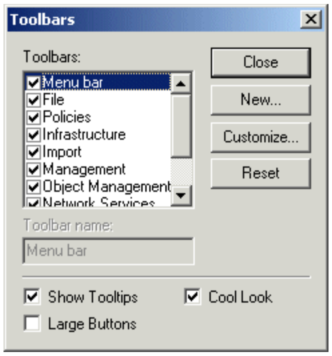
Bringing the toolbar to any edge of the window will dock it into that edge of the window. You can always move it back to the top or bottom. You can also leave the toolbar floating in the window, where it appears with a title bar. If you move or customize toolbars and log out of VitalQIP, the toolbars appear as you left them when you next log in.

> **Note:** Toolbar locations are maintained on the current workstation. Logging into VitalQIP via another workstation will not maintain modified toolbar format and location.

Customize VitalQIP toolbars

You can customize a VitalQIP toolbar merely by dragging and dropping the buttons. Move the button from one toolbar to another by holding down the **Alt** key and then the left mouse button while you drag the button to a specific spot on another toolbar. The button will merge into the toolbar at the selected position. Alternately, dragging a button off a toolbar and releasing the mouse button will remove the button from the toolbar.

To hide, reset, or customize the toolbars, access the **View|Toolbars** function. The Toolbars window opens.



Toolbars:
☑ Menu bar
☑ File
☑ Policies
☑ Infrastructure
☑ Import
☑ Management
☑ Object Management
☑ Network Services

Toolbar name: Menu bar

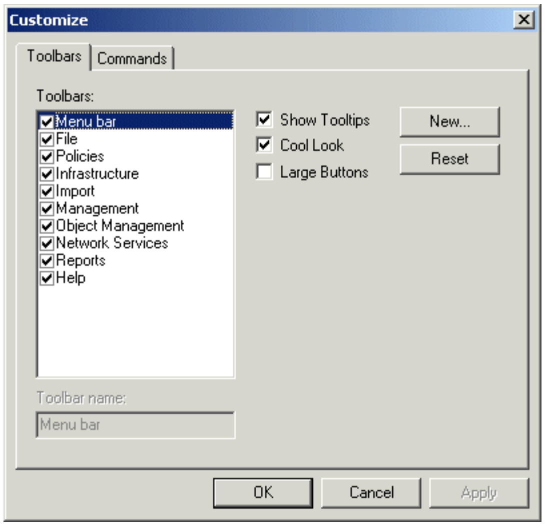
☑ Show Tooltips ☑ Cool Look
□ Large Buttons

Hide a toolbar by highlighting it and deselecting the check box.

To reset a toolbar, highlight the toolbar and click **Reset**. This makes the toolbar appear as the original VitalQIP-provided toolbar. If the toolbar is customized, the customizations are gone.

You can also customize the toolbar within this window. Click **Customize** to view the Customize window.

The **Toolbars** tab displays all available toolbars. You can reset the toolbars to their default buttons, or you can create a new toolbar by clicking **New**.



Toolbars:

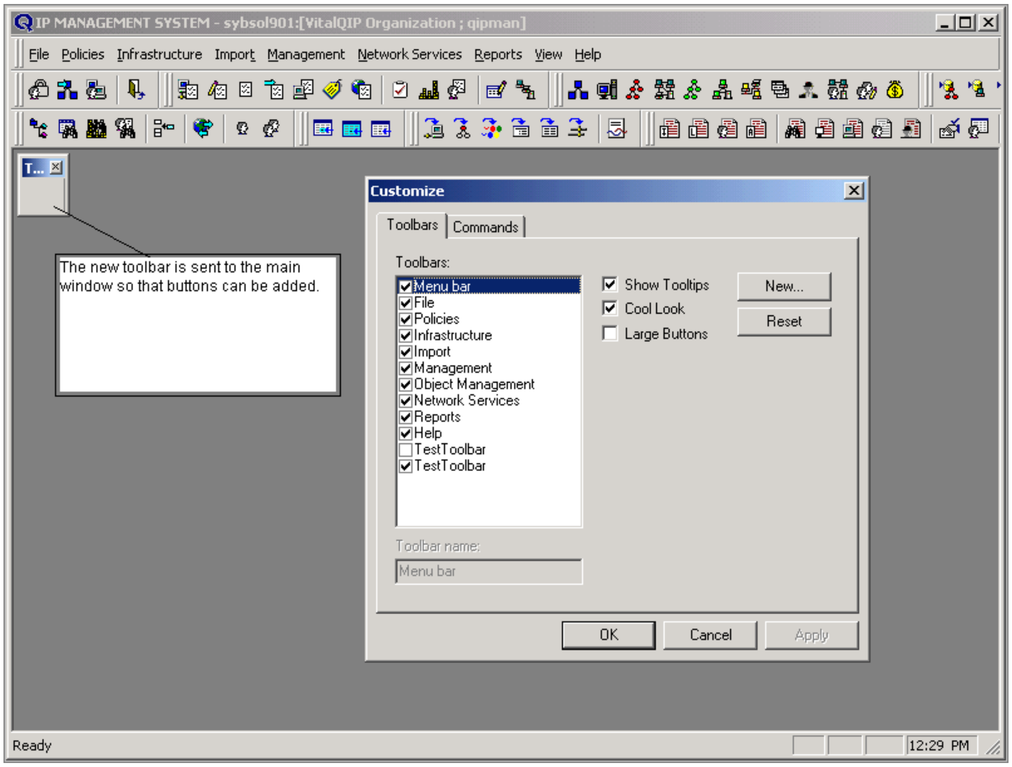
- ☑ Menu bar
- ☑ File
- ☑ Policies
- ☑ Infrastructure
- ☑ Import
- ☑ Management
- ☑ Object Management
- ☑ Network Services
- ☑ Reports
- ☑ Help

☑ Show Tooltips
☑ Cool Look
□ Large Buttons

Toolbar name: Menu bar

Create a new toolbar

The new toolbar “TestToolbar” was created, and automatically displayed on the main VitalQIP window.



The new toolbar is sent to the main window so that buttons can be added.

Toolbars:

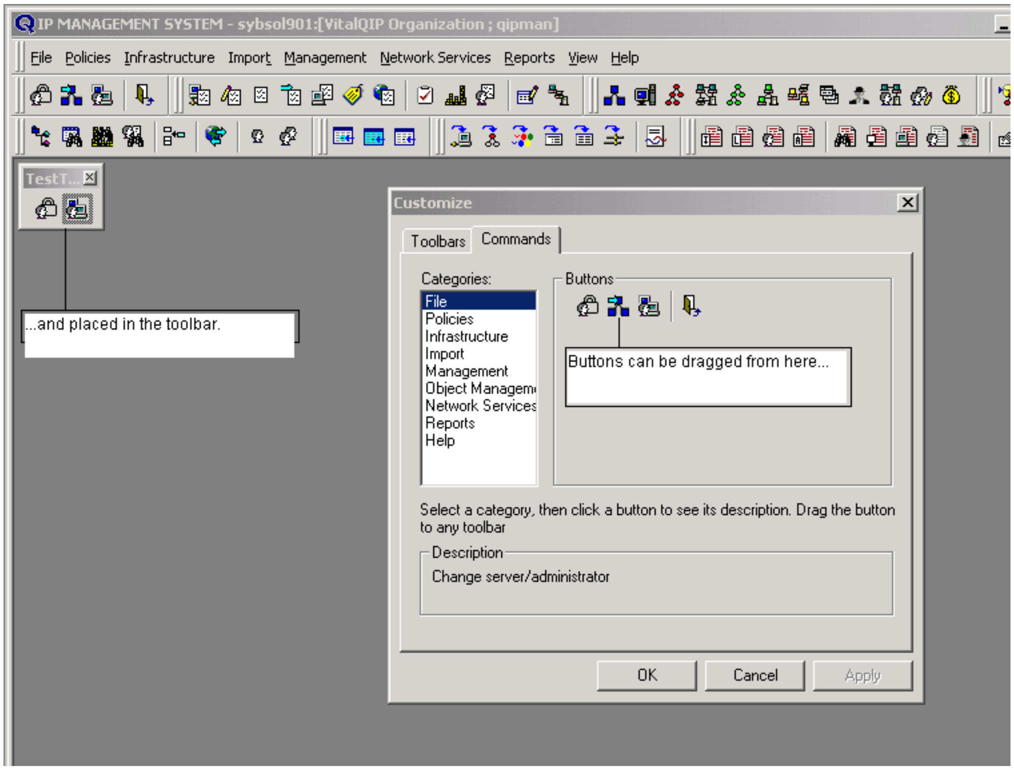
- ☑ Menu bar
- ☑ File
- ☑ Policies
- ☑ Infrastructure
- ☑ Import
- ☑ Management
- ☑ Object Management
- ☑ Network Services
- ☑ Reports
- ☑ Help
- □ TestToolbar
- ☑ TestToolbar

☑ Show Tooltips
☑ Cool Look
□ Large Buttons

Toolbar name: Menu bar

At this point, you can choose to access the **Commands** tab. You can add the buttons you want to use in the new toolbar or drag and drop buttons from other toolbars.

The **Commands** tab displays all the buttons in each of the VitalQIP-provided toolbars. Clicking on a button displays its function at the bottom of the window. You can drag any button from this tab directly to the new toolbar already waiting in the main window.



IP MANAGEMENT SYSTEM - sybsol901:[VitalQIP Organization ; qipman]
File Policies Infrastructure Import Management Network Services Reports View Help
TestT...
Customize
Toolbars
Commands
Buttons
OK
Cancel
Apply

...and placed in the toolbar.

Categories:
File
Policies
Infrastructure
Import
Management
Object Managem
Network Services
Reports
Help

Buttons can be dragged from here...

Select a category, then click a button to see its description. Drag the button to any toolbar

Description
Change server/administrator

You can add as many buttons as you like to the new toolbar. Just click on a new category and select the buttons you need.

Your new toolbar displays in the **Toolbars** tab. If you click on that toolbar, you will notice that you can delete it altogether if you choose. The VitalQIP-provided toolbars cannot be deleted, but they can be reset to their default configuration.

Additional toolbar features

Show Tips - Check this box to display the title of the function when the mouse arrow rests on the button.

Cool Look - Check this box to achieve a flat look rather than a raised button look on the toolbars. Non Cool Look toolbars can be dragged by selecting an area within a button, and moving it to another location before releasing the mouse button.

Large Buttons - Check this box to increase the size of the buttons for easier viewing.

Status bar

The **View|Status Bar** function allows you to hide the status bar at the bottom of the window.

Hierarchy legends

The **View|Hierarchy Legends** function in the **View** menu opens a snapshot window of all the icons used by VitalQIP and what they represent. Use this as a reference tool.

User modes in VitalQIP

There are three types of User Modes in the VitalQIP GUI (Graphical User Interface): Advanced, Standard, and Basic. This allows the complexity of some aspects of the interface to be hidden from users who do not, or should not, use those functions. The levels do not alter the security or permissions of administrators. They are designed as a convenience for the navigation of the GUI.

User modes are established when you set up administrator profiles for each user of the VitalQIP database. When the user logs in after you have set up an administrator profile, the mode tied to that administrator is displayed as checked (✓) in the **View** menu. If the user is assigned the Advanced Mode, all functions available in the Standard and Basic Modes can also be accessed.

If the user is assigned the Standard Mode, all Basic Mode functions can be accessed but additional Advanced Mode functions cannot be.

If Basic Mode is assigned to the user, the administrator cannot access additional functions in the Standard or Advanced Modes. Additionally, the administrator in Basic mode is prevented from entering information into the **Resource Records** and **Mail Servers** tabs of the Object Profile.

Standard mode is the default for any VitalQIP administrator created by the VitalQIP system administrator.

Additionally, you can customize these modes further through the **Customize** tab of the **Infrastructure|Administrator** option.

The availability of menus and functions for each user mode is shown in the following table.

Table 1-1 User Modes

Menu	Function	Modes
File	Administrator Password	Basic, Standard, Advanced
	Login	Basic, Standard, Advanced
	Change Organization	Basic, Standard, Advanced
	Change Server/Administrator	Basic, Standard, Advanced
	Exit	Basic, Standard, Advanced

Menu	Function	Modes
Policies	DHCP/Bootp Templates	Standard, Advanced
	Class/Option Setup	Standard, Advanced
	Option Template	Standard, Advanced
	Policy Template	Standard, Advanced
	ACL Templates	Standard, Advanced
	Client Class	Standard, Advanced
	Naming Policies	Standard, Advanced
	Global Policies	Advanced
	Manufacturer Profiles	Advanced
	Location Profiles	Advanced
	Contact Profiles	Advanced
	User-Defined Fields	Advanced
	Object Classes	Advanced
Infrastructure	Organization	Advanced
	Server	Standard, Advanced
	Domain	Standard, Advanced
	Network/Reverse Zone	Standard, Advanced
	Non-Managed DNS Server	Advanced
	OSPF	Advanced
	Subnet Organization	Standard, Advanced
	Application	Standard, Advanced
	Administrator	Standard, Advanced
	Administrative Role	Advanced
	User Group	Advanced
Import	Domain	Standard, Advanced
	Network	Standard, Advanced
	OSPF	Advanced
	Subnet Organization	Standard, Advanced
	Subnet	Standard, Advanced
	Object	Standard, Advanced
	MAC Address	Standard, Advanced

Menu	Function	Modes
Management	VitalQIP Hierarchy	Basic, Standard, Advanced
	Object Management	Basic, Standard, Advanced
	All Subnets	Basic, Standard, Advanced
	Used Subnets	Basic, Standard, Advanced
	Unused Subnets	Basic, Standard, Advanced
	User Management	Basic, Standard, Advanced
	User Profile	Basic, Standard, Advanced
	User Groups	Basic, Standard, Advanced
	Go To/Search	Basic, Standard, Advanced
	Object	Basic, Standard, Advanced
	Object by Location	Basic, Standard, Advanced
	Object by Contact	Basic, Standard, Advanced
	Reclaim Addresses	Standard, Advanced
	Global MAC Address Pool	Standard, Advanced
Network Services	DHCP Generation*	Basic, Standard, Advanced
	DNS Generation*	Basic, Standard, Advanced
	Windows DC Generation*	Basic, Standard, Advanced
	Bootptab File Generation*	Basic, Standard, Advanced
	Local Host Generation*	Basic, Standard, Advanced
	NIS Generation*	Basic, Standard, Advanced
	View Active Lease*	Basic, Standard, Advanced

Menu	Function	Modes
Reports	Management Reports	Basic, Standard, Advanced
	Object by Address Range	Basic, Standard, Advanced
	Object by Location	Basic, Standard, Advanced
	Object by Administrator	Basic, Standard, Advanced
	Object by Application	Basic, Standard, Advanced
	Inquire	Basic, Standard, Advanced
	Free Subnet	Basic, Standard, Advanced
	DHCP	Basic, Standard, Advanced
	Administrator Profile	Basic, Standard, Advanced
	Administrative Role	Basic, Standard, Advanced
	DNS Zone	Basic, Standard, Advanced
	Object Audit History	Basic, Standard, Advanced
	Administrator Audit History	Basic, Standard, Advanced
View	Hierarchy Legends	Basic, Standard, Advanced
	Basic Mode	Basic, Standard, Advanced
	Standard Mode	Standard, Advanced
	Advanced Mode	Advanced
	Toolbars	Basic, Standard, Advanced
	Toolbar Edit	Basic, Standard, Advanced
	Status Bar (Windows only)	Basic, Standard, Advanced
Help	Contents	Basic, Standard, Advanced
	Technical Support	Basic, Standard, Advanced
	About VitalQIP	Basic, Standard, Advanced

* Administrators must also have the respective service (indicated by an asterisk) in their Managed List to perform generations.

VitalQIP infrastructure overview

You should set up the infrastructure of your VitalQIP system before any production data is entered, and before the software is made available for general use. Unless you are importing an existing infrastructure, you need to give careful consideration to how your firm's networks, domains, reverse zones, and subnets need to be organized. Additionally, you probably want to define additional administrator profiles to the one you are using, so that your colleagues can manage subsets of the overall infrastructure such as specific subnets, subnet organizations, managed ranges, and applications. For that reason, the Infrastructure menu includes the Administrative Role and Administrator functions

The different elements of the VitalQIP infrastructure are discussed in brief below. If you are using VitalQIP to manage nothing but IP addresses, only server and network setup is required. In any situation where you use DNS and/or DHCP, setup of a domain and subnets is also required. The other elements are optional.

Organization

Optional. The Organization function allows you to manage networks based on organization. For example, an organization could be a separate physical location with completely different policies. The "VitalQIP Organization" is provided by default.

Server

Optional. The Server function allows you to define and manage servers that host IP services, such as DHCP and DNS. Servers can be defined as Bootp, DHCP, DNS, Local Host, NIS, or Windows Domain Controller. Additionally, Bootp, DHCP, Local Host, and NIS servers can be defined at the corporate, domain, network, OSPF area, or subnet level. This provides the flexibility to adopt a corporate, regional (for example, network or OSPF area), or individual subnet Bootp and/or DHCP methodology.

Domain

Required. The Domain function allows you to create DNS Domains. These are the basic units of the DNS naming system.

Network/Reverse Zone

Required. The Network/Reverse Zone option allows you to define the IP addressing scheme of your network and reverse zone. You can also assign ranges of addresses to the networks and some basic parameters.

VitalQIP defaults to a simple network and structure, which gives you the ability to subnet those networks and reverse zones. It allows you to identify networks or portions of networks as having address-to-name lookups. Separating the Reverse Zone function from the Domain Profile enables you to assign different parameters and have more flexibility in managing your network.

Non-Managed DNS Server

Optional. This function allows VitalQIP-Managed secondary DNS servers to pull zones from non-managed primary DNS servers. It allows you to specify:

- the name and IP address of a DNS server that is not managed by VitalQIP and contains data that is not in VitalQIP
- the names of the domains (zones) and reverse zones that you want your server to pull from the non-managed server
- the selection of one or more of your servers to be the secondary DNS server for these zones

Zones that are defined with this function should ***not*** be defined as normal VitalQIP domains or reverse zones. To define a secondary server that is in a VitalQIP-managed domain, use the Domains function.

OSPF

Optional. OSPF (Open Shortest Path First) routing area definitions are obtained by applying an OSPF area mask to the network. If OSPF routing areas are used, each subnet group range falls within a specific OSPF area. If OSPF areas are not used, the subnet group ranges are independent of OSPF.

Subnet Organization

Optional. A subnet organization is a group of subnets defined by a name for administrative purposes. Subnet organizations can be used to assign administrators, to specify Windows domain controllers to which the subnet organization is pushed, to group subnets by geographic location, or simply to provide an easy-to-recognize name. A subnet can be associated with only one subnet organization.

Application

Optional. Defining applications allows you to assign an administrator to a range of addresses that cross subnet group boundaries. Reports are available by application, which can provide a unique classification capability.

Administrative Roles

Optional. An Administrative Role is a collection of infrastructure components that can be assigned to an administrator as a part of their Managed List. By using an administrative role to assign common access to administrators, new infrastructure can be added to the role and all administrators associated with that role will have access to the infrastructure.

Administrator

Optional. The Administrator function establishes the access an administrator can have to the various objects in the database and characteristics of the management interface they will use. This is accomplished by defining Warnings, what files they can update and create for servers, and the ability to change subnet names among other things.

User Group

Optional. This function allows you to group users and define them as one, utilizing the same parameters.

Navigate the VitalQIP GUI

Various ways of navigating VitalQIP are discussed in:

- The QIP Hierarchy function is typically your interface for viewing your network infrastructure. See "QIP Hierarchy function" below.
- Context menus also appear when you right-click on objects in the hierarchy tabs, as well as in the Object Management windows. Refer to "Context menu for the QIP Hierarchy" (p. 1-27) and "Context menu for the subnet selection window" (p. 7-5).
- Quick View windows can also be set up as default methods for accessing networks, subnets, and objects. Refer to "Quick View" (p. 1-35).
- Users with networks containing large numbers of domains and subnets can use Domain Folders to group them logically into folders, and thereby access infrastructure components more easily. Refer to "Domain folders" (p. 1-40).
- The more traditional ways of accessing subnets and objects are through the Object Management menu function, and the Go To/Search functions. Refer to "Go to/search function" (p. 1-42) and "Object management" (p. 7-19).

QIP Hierarchy function

The QIP Hierarchy function opens the hierarchy of the Organizations, and beneath them the Domains, Networks, OSPF Areas, Subnet Organizations, and Subnets that have been created within each organization. The QIP Hierarchy essentially provides you with an interface where you can search for and access a specific object within a subnet and then open the Object Management window.

Right-clicking on any of the Hierarchy levels opens a context menu where you can access Object Management and Reclaim functions quickly and easily, as well as add to and delete from the hierarchy. Depending on your selection, certain options on the context menu are enabled or disabled.

If the Administrator has "Network Quick View" or "Subnet Quick View" enabled, double-clicking on a network or subnet in the hierarchy opens the associated Quick View. If you right-click on a cell in the Quick View, a context-sensitive shortcut menu appears.

You can also look at the parameters of any DHCP server or DNS server that has been assigned to you via the **DHCP Servers** and **DNS Servers** tabs.

The User-Defined Hierarchy gives you the ability to create your own hierarchical view (refer to "Create User-Defined hierarchy" (p. 1-32)).

Use the QIP Hierarchy function

Purpose

Use this procedure to use the QIP Hierarchy function.

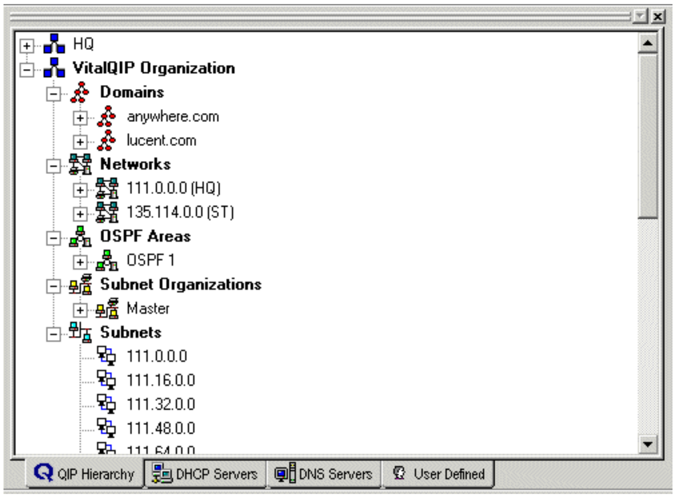
Before you begin

- If you exit with the Hierarchy appearing in the main window, when you log in the next time, the last active tab is opened.
- Only one organization is opened in the QIP Hierarchy unless the administrator has been assigned multiple Organizations. A Master-level administrator can view all organizations, and use the **File|Login|Change Organization** option to access other organizations for modification.
- Only the organization that was selected upon login has the child nodes opened automatically (Domains, Networks, OSPF Areas, and Subnet Organizations).
- Domains appear as a hierarchical tree only if the “Display Domain Folders” option in **Administrator Profile|Customize** is set. For more information on this option, refer to “Administrators” (p. 6-11) and “Domain folders” (p. 1-40).

Procedure

To use the QIP Hierarchy, follow these steps:

1 Select **QIP Hierarchy** from the **Management** menu. The Hierarchy window opens within the main window, opening Organizations and labels (Domains, Networks, and so on) that have been assigned to you.



2 To view networks and subnets in a domain, OSPF area, network or subnet, click on that item.

3 Right-click on the item, and select the option from the context menu and click.

4 You can also double-click on a subnet to view all objects within that subnet via the Object List display.

END OF STEPS

Context menu for the QIP Hierarchy

The right-click options available in the QIP Hierarchy are:

- **Add** - displays the hierarchy selection's Profile Option window. For example, if you have a domain highlighted and you right-click, the Domain Profile Option window opens in Add Mode.
- **Delete** - displays the hierarchy selection's Profile Option window. For example, if you have a domain highlighted and you right-click, the Domain Profile Option window opens in Delete Mode.
- **Object Management** - displays the Object Management: Objects window.
- **Quick View** - displays subnets or objects in a grid-like pattern for quick access. Refer to "Quick View" (p. 1-35) for more information.
- **Reclaim** - opens the Reclaim Objects window (refer to "Reclaim addresses" (p. 7-97)).
- **Reports** - opens the Object List Report: By Address window.
- **Properties** - Selecting this option opens the properties for that selection.This option is also used to change the properties of multiple domains and reverse zones. Refer to "Change multiple zone options" (p. 5-49).
- **Add Folder** - allows you to create a folder if the **Create Infrastructure** and **Display Domain Folders** options in your Administrator Profile are set to True. For more information on the maintenance of folders, refer to "Maintenance of folders" (p. 1-40).
- **Delete Folder** - allows you to delete a folder if the **Create Infrastructure** and **Display Domain Folders** options in your Administrator Profile are set to True.
- **Rename Folder** - allows you to rename a folder if the **Create Infrastructure** and **Display Domain Folders** options in your Administrator Profile are set to True.
- **Reassign** - allows you to reassign domains to folders if the **Create Infrastructure** and **Display Domain Folders** options in your Administrator Profile are set to True.

Use DHCP Server hierarchy

Purpose

This tab at the base of the QIP Hierarchy window allows you to view, configure, and manage all DHCP servers within an organization. The hierarchy displays the DHCP servers, managed networks and the managed ranges within the network.

Before you begin

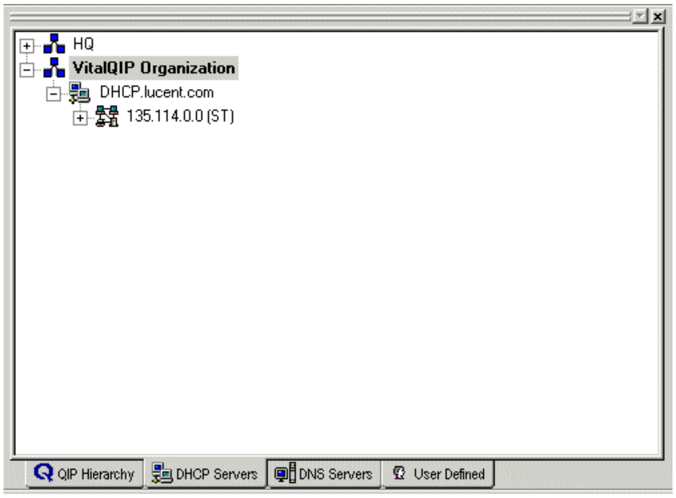
The DHCP Server hierarchy may be empty if the user (login ID) does not have access to DHCP servers.

Procedure

To use the DHCP Server Hierarchy, follow these steps:

1 Select **QIP Hierarchy** from the **Management** menu. A window opens showing the last tab you accessed.

2 If the **DHCP Servers** tab is not shown, click the **DHCP Servers** tab in the Hierarchy window to open the DHCP Servers that have been assigned to your organization.



3 Click a specific **DHCP Server** in the hierarchy. To see the networks this DHCP Server manages, expand the hierarchy. You can then expand it further to see the ranges of dynamic objects this DHCP Server manages.

4 Right-click to see the context menu, which opens the File Generation, Reports, and Properties functions. The functions are disabled or enabled depending on where you are accessing them.

- The **Properties** function displays the Server Profile.
- The **File Generation** function displays the DHCP Generation window.
- The **Reports** function accesses the VitalQIP: DHCP Report window.
- From the network, the **Properties** function displays the Network Profile, and the **Reports** option opens the Object List report window.
- From the subnet, the **Properties** function displays the Subnet Profile. The **Reports** option opens the Object List report window with the current Subnet selected.
- From the managed ranges, the **Properties** function displays the DHCP Server Properties window.

END OF STEPS

Use DNS Server hierarchy

Purpose

The **DNS Servers** tab in the Hierarchy window allows you to view, configure, and manage DNS Servers. The hierarchy display is similar to that of the QIP Hierarchy, but begins with DNS Servers and shows the Domains and Reverse Zones managed by that DNS server.

Before you begin

The DNS Hierarchy may be empty if your user (login) ID does not have access to DNS servers.

Procedure

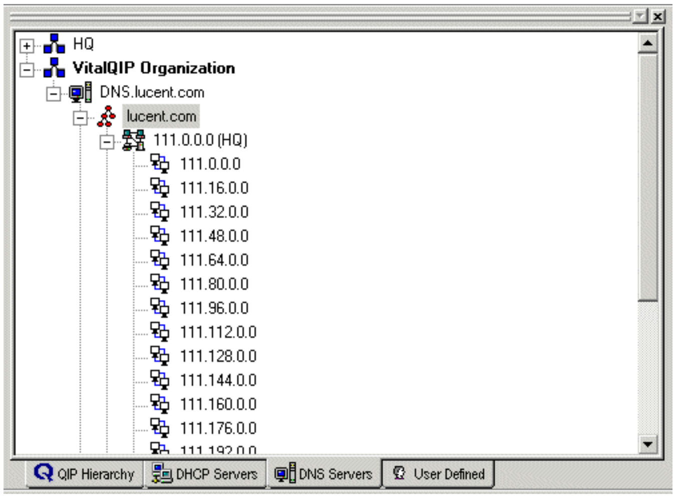
To use the DNS Server Hierarchy, follow these steps:

1 Select the **Hierarchy** option under **Management** in the menu bar. A window opens showing the last tab you accessed.

2 If the **DNS Servers** tab is not shown, click the **DNS Servers** tab to open the DNS Server Hierarchy. The DNS Servers Hierarchy window appears, displaying the secured and unsecured DNS Servers that have been assigned to you.

Note: The “keyed” icon indicates that the DNS Server is secure.

When you expand the DNS Hierarchy, you can access the domains, networks and subnets associated with the DNS Server. From here, you can manage the objects by right-clicking on a subnet and selecting Object Management.



3 If your Administrator Profile allows you to view Network, Subnet, and/or Domain QuickViews, you can double-click on an item to display the QuickView for the Domain. From there you can get to the Subnet QuickView and then double-click on an Object to open the Object Profile.

- The **File Generation** function displays the DNS Generation window, and is only accessible from the DNS Server option right-click menu.
- The **Delete** function displays the Server Profile, the Domain Profile, or the Network Profile, in Delete mode, depending on from where you are accessing the right-click menu.
- The **Object Management** function displays the Object Management window, and is accessible only when you highlight a subnet.
- The **QuickView** function displays the Domain Quick View.
- The **Reclaim** function displays the Reclaim IP Address window.
- The **Reports** function displays the Object List report.
- The **Properties** function displays the Server Profile, Domain Profile, Reverse Zone Profile, Network Profile, or Subnet Profile, depending on where you are accessing the option from in the DNS Hierarchy.

END OF STEPS

Create User-Defined hierarchy

Purpose

Each user can have one User-Defined Hierarchy. This is a convenient function that allows you to set up a smaller, personalized hierarchy view for organizational purposes. You can add labels, domains, networks, OSPF areas, subnets, applications, and servers to your hierarchy.

From these Node Types, you can quickly access the properties of the node, create reports on the nodes, and through the Subnet node, access the Object Management list without having to go through the main window.

Before you begin

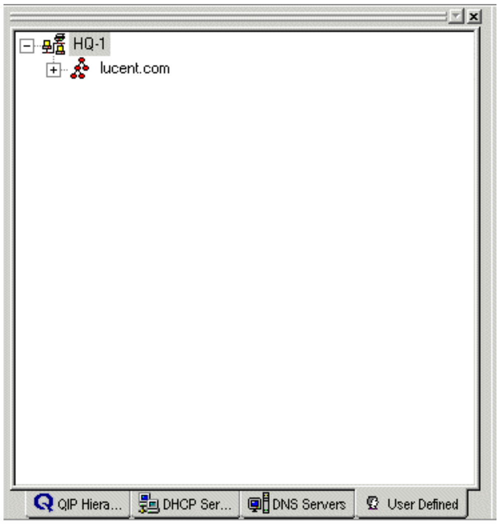
No pre-defined relationship exists between items in the User-Defined Hierarchy; it is for display/organization purposes. For example, you can place networks *under* subnets.

Procedure

When you first install and enter VitalQIP, the User-Defined Hierarchy portion of the QIP Hierarchy is empty until you define it. To create a User-Defined Hierarchy, follow these steps:

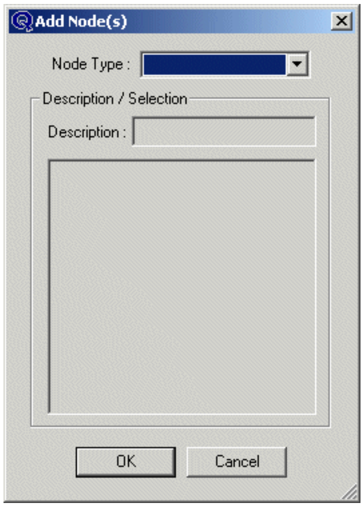
1 Access the **Management|QIP Hierarchy** option in VitalQIP (if no hierarchy is displayed). A window opens showing the last tab you accessed.

2 If the **User Defined** tab is not shown, click on the **User Defined** tab in the QIP Hierarchy. The **User Defined** tab opens.



3 Right-click to see the context menu. There are four options (three options are disabled except the **Node Management** option the first time you populate the **User Defined** tab). You can access the Object Management, Reports, or Properties windows based on the selected node when you access the context menu.

4 To populate the **User Defined** tab, right-click in the hierarchy, and select the **Node Management | Add Root Node** option. A “root” node is parent to a child node and appears above the child (children). The Add Node(s) window opens.



5 From the **Node Type** drop-down list, choose the type of node you want to add to the User-Defined Hierarchy (for example, Domain, Network, and so on). Only when you select “Label” as a **Node Type** does the **Description** field become active, and you can enter text.

The list in the Description/Selection area of the window changes depending on the **Node Type** you selected.

6 Click **OK**. The type you selected is added as a root to your User-Defined Hierarchy node.

7 Once you have added the root, you can add a sibling or child to your hierarchy, in addition to other root nodes. A “child” node appears below the highlighted node, while a “sibling” node appears on the same hierarchical level as the highlighted node.

8 Right-click and select either the **Add Child Node** or the **Add Sibling Node** option from the context menu. Repeat these steps until you have built your desired hierarchy.

END OF STEPS

Quick View

When there are large numbers of subnets and networks, you can use **Quick View** to navigate in the VitalQIP system. If this option was enabled in your **Administrator Profile**, you see the Quick Views by default. Otherwise, the **Quick View** option is accessible from the right-click context menu.

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 hierarchy, and the subnets are displayed in the Quick View window. From the subnet level, you can see the objects. Double-click on an individual square to display the Object Profile for that object, or the Object List if you are selecting a subnet.

Move the mouse over the grid to display the object's address at the top of the window. Up to 256 objects are displayed at a time. If there are more than 256 objects, you can move to subsequent pages by using the arrows or the slider at the bottom of the window.

Use Network Quick View

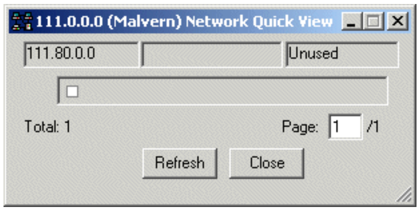
Purpose

The Network Quick View function can be set up as the default by checking the **Network Quick View** check box on the **Customize** tab in the **Administrator Profile**. Otherwise, it is available through the shortcut menu in the QIP Hierarchy when the Networks, Domains, OSPF Areas, or Subnet Organizations are opened. For more information on setting up the Network Quick View as a default, refer to "Customize administrator menus" (p. 6-30).

Procedure

To access the Network Quick View, follow these steps:

1 Expand the **Networks** in the Hierarchy, and double-click on a network. The **Network Quick View** opens.


111.0.0.0 (Malvern) Network Quick View

111.80.0.0 | | Unused

□

Total: 1 Page: 1 /1

2 Right-click on an object to access the following functions from the Quick View display:

- **Object Management** - displays the Object List for that Subnet cell.
- **Quick View** - displays the Subnet Quick View.
- **Reclaim** - displays the Reclaim IP Address window so that you can reclaim addresses in the selected subnet.
- **Move** - displays the Subnet Move window to move the subnet to another network.
- **Delete Scheduled Move** - deletes a subnet from the scheduled move list.
- **Report** - displays the Object List Report: By Address window.
- **Properties** - displays the subnet profile for the selected subnet.
- **Refresh** - refreshes the selected Quick View with the most recent changes.

3 Double-click on a subnet cell to display the **Subnet Quick View**. Right-click on an object to access the following functions from the Quick View display:

- **Add|Static, Dynamic, or Reserved** - enables you to add objects to specified subnets as static, dynamic, or reserved.
- **Delete|Static, Dynamic, or Reserved** - enables you to delete objects from the specified subnet.
- **Modify|Static, Dynamic, or Reserved** - enables you to modify objects in the specified subnet.
- **Move|Schedule** - displays the Object Move Option window enabling you to schedule the specified object for a move.
- **Move|Cancel** - cancels the object move. This is a function and does not display a window.
- **Move|Modify** - displays the Object Move Option window so you can modify the object's move.
- **Properties** - displays the Object Profile for the specified object.
- **Refresh** - refreshes the Quick View with the most recent information.

4 Double-click on an object cell to display the object's Object Profile.

END OF STEPS

Use Subnet Quick View

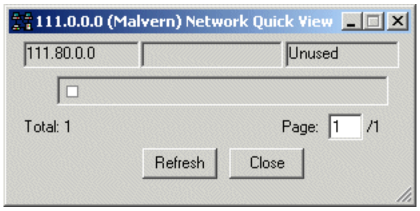
Purpose

The Subnet Quick View function can be set up as the default by checking the **Subnet Quick View** check box on the **Customize** tab in the **Administrator Profile**. If not set up as a default, you can select Quick View on the context menu in the QIP Hierarchy wherever subnets can be displayed. For more information on the Quick View as a default, refer to "Customize administrator menus" (p. 6-30).

Procedure

To access the Subnet Quick View, follow these steps:

1 Double-click on a subnet in the hierarchy. The Subnet Quick View opens. This displays all objects in the subnet as cells.



111.0.0.0 (Malvern) Network Quick View

111.80.0.0 | | Unused

□

Total: 1

Page: 1 /1

2 Right-click on an object to access the following functions from the Quick View display:

- **Add|Static, Dynamic, or Reserved** - enables you to add objects to specified subnets as static, dynamic, or reserved.
- **Delete|Static, Dynamic, or Reserved** - enables you to delete objects from the specified subnet.
- **Modify|Static, Dynamic, or Reserved** - enables you to modify objects in the specified subnet.
- **Move|Schedule** - displays the Object Move Option window enabling you to schedule the specified object for a move.
- **Move|Cancel** - cancels the object move. This is a function and does not display a window.
- **Move|Modify** - displays the Object Move Option window so you can modify the object's move.
- **Properties** - displays the Object Profile for the specified object.
- **Refresh** - refreshes the selected subnet in the Quick View with the most recent information.

3 Double-click on an object cell in the Subnet Quick View to display the Object Profile.

END OF STEPS

Domain folders

In addition to using Quick View windows to help manage large networks, you can also use the Domain Folders function to navigate through networks with large numbers of domains. This function allows large numbers of domains to be grouped into folders for ease of management. This function is set up in the Administrator Profile when you check the **Display Domain Folders** check box in the **Customize** tab. Once it is checked and you enable the function by logging out and back in again with the **Login|Change Server/Administrator** function on the **File** menu, all areas throughout VitalQIP where domains are displayed use the folder/domain schema.

Maintenance of folders

Folder "maintenance" is performed through the context menu that appears when you right-click on a domain or folder in the **QIP Hierarchy**. If the **Display Domain Folders** option in the Administrator Profile is checked, the administrator has the following options available for maintenance through the right-click context menu:

Note: Folder maintenance functions are not available to Administrators designated as "Read-Only" and "Normal" (Basic Mode).

- **Add Folder** - adds a folder to the selection you highlighted. The folder name must be unique among the child folders.

  When adding a new folder, a folder named "New Folder" is created. The folder will then be selected for renaming. If a folder named "New Folder" already exists as a child of a selected folder, the newly created folder will be named "New Folder (x)" (where "x" is an increasing number until a unique folder name can be created). The folder name can then be modified.
- **Delete Folder** - deletes the highlighted folder.

  Note: A folder must be empty before it can be deleted.
- **Rename Folder** - allows you to change the name of a folder.
- **Reassign** - allows you to select a group of domains and reassign (move) them to another folder. The destination folder must already exist. First, select the domains to reassign, then select the **Reassign** option from the context menu. A dialog opens allowing the user to select the destination folder. After the folders are moved, the hierarchy is refreshed.

Specific "rules" regarding the use and management of domain folders are explained, as follows.

Rules for creating and managing folders

Keep the following items in mind when you are creating and managing folders:

- Folders are maintained from within the **QIP Hierarchy** tab's context menu (when you right-click on the option). If the **Display Domain Folders** option in the Administrator Profile is not checked, then the folder maintenance menu items are disabled in the QIP Hierarchy context menu.
- Regardless of whether or not the **Display Domain Folders** option is selected, the root **Domain** node (label) cannot be removed, renamed, or modified by any administrator.
- All administrators can open any folder to view the contents of the folder. Access to the domains within the folders is limited by an administrator's access privilege.
- No administrator privileges are associated directly with individual folders.
- Folders may contain other folders and/or domains.
- Folders and domains are listed in alphabetical order.
- Multiple folders of the same name may exist. However, children of the same parent node ***must*** be uniquely named.
- Folder names are limited to 30 characters and cannot start or end with space characters. All printable characters except the following: \ / : * ? " < > | are allowed.
- A folder cannot be deleted unless it is empty.
- Folders can be renamed.
- Domains can be reassigned to another folder. The destination folder must already exist. Multi-selection of domains within multiple folders are selectable and movable to another folder. The domain's location within the destination folder is based on the alphabetic ordering within the folder. Following reassignment, the domain hierarchy must be refreshed.
- If a domain is not assigned to a folder when created, it is attached to the default folder **Domains**.
- A domain may exist within only one folder.
- Folders can only be created under the default domain folder (domains) or another domain folder. They cannot be created under domains.
- Domain expansion (in tree hierarchies) opens only the top-level folder/domains. You can expand the tree by selecting the desired folder to expand.

Go to/search function

The GoTo/Search function allows you to find an item by its name, address, location, or contact. Three options are available to search for an item:

- **GoTo/Search Object** option provides the convenience of searching for items by name or address.
- **GoTo/Search|Object by Location** option offers the ability to look for objects based on its location.
- **GoTo/Search|Object by Contact** option allows you to look for objects by contact information.

Find an object

Purpose

Use this procedure to find an object.

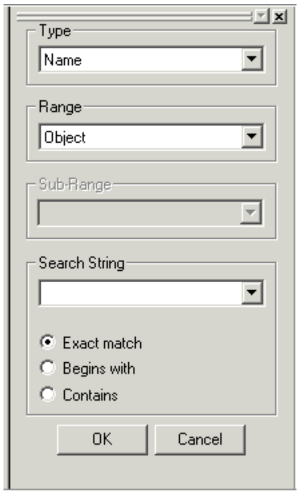
Before you begin

- Double-click on an object in the upper pane of the Results window to bring up the object's properties/profile, if one is available for the object.
- If you search for an organization with a specific User-Defined Field (UDF), *all* organizations with that User-Defined Field are returned, regardless of administrator level. Therefore, an administrator may not be authorized to access a returned organization and will receive a "privilege-denied" message.
- Only a Master administrator or a Normal administrator with an Organization Managed Type set to Read/Write can add, delete, or modify an organization User-Defined Field via the Organization Profile displayed for the UDF selected in the Go To/Search.

Procedure

To find an object using the **GoTo/Search|Objects** option, follow these steps:

1 Select **Management|GoTo/Search|Object** in the menu bar. The Go To window opens in the VitalQIP main window.



Type: Name

Range: Object

Sub-Range:

Search String:

● Exact match

○ Begins with

○ Contains

2 Refer to the following table as you fill in the fields you need to complete for your search.

Table 1-2 Goto/Search fields

Field	Description
Type	In the **Type** field, select whether you are searching for a Name, IP Address, MAC Address, DECNet Address, User Defined Field, or Resource Record. The following table describes the field options.
Range	Select the **Range** you will be searching for (for example, Object, Domain, Network, and so on). This field is not accessible when "MAC Address", or "DECNet Address" is selected from the **Type** drop-down list. Refer to Table 1-3, "Type options" (p. 1-44) for more information. Anything you last searched on will remain in the drop-down list until you log out of VitalQIP.
Resource Record Type	This field is enabled if you selected "Resource Record" from the **Type** drop-down list. Select the type of resource record (such as, CNAME, MX, HINFO, and so on) you are looking for.
Search String	Just below the **Search String** field an example appears of what the string should look like. Enter the IP Address in dotted decimal notation (for example, 198.200.138.217). Enter the MAC addresses with (or without) colon separators. (Refer to the following table for more information.) **Note:** Wildcard characters ***** and **?** can be used as part of the search string. ***** matches 0 or more characters while **?** searches for single characters only. These characters cannot be used when "Address", "MAC Address", or "DECNet Address" is selected in the **Type** field.

Table 1-3 Type options

Type	Range	Sub-range	Search string	Description
Name	All, Domain, Network, OSPF Area, Subnet Organization, Subnet, Object Name, Alias Name, Router Group	N/A	Refer to the description for the **Search String** field.	Searches for all the objects within a specific range based on the **Search String** field. **Note:** For object searches, the fully qualified domain name and hostname can be used. Such search strings must end in a period.

Type	Range	Sub-range	Search string	Description
Address	All, Network, Subnet, Object	N/A	Must be exact in the following format: 000.000.000.000	Searches for all the IP addresses within a specific range based on the entry in the **Search String** field.
MAC Address	Hexadecimal address	N/A	Must be in either 12 or 16 hexadecimal character format. This format is determined by the MAC16 Global Policy being true or false.	Searches for all the MAC addresses based on the entry in the **Search String** field.
DECNet Address	N/A	N/A	Must be the following format: 00,0000	Searches for all the DECNet addresses based on the entry in the **Search String** field.
User Defined Field	All, Organization, Domain, Reverse Zone, Subnet, User, Object	All or the UDFs for the selected Range	Refer to the description for the **Search String** field.	Searches for the specified User Defined Field(s) based on the entry in the **Search String** field, and the selections in the Range and UDF Name fields.

Type	Range	Sub-range	Search string	Description
Resource Record	All, Object, Domain, Reverse Zone	All (all resource record types), A (Host Ipv4), CNAME (Canonical Name), HINFO (Host Information), MX (Mail Exchange), NS (Name Server), PTR (Pointer), TXT (Text), WKS (Well Known Services), AAAA (Host Ipv6), AFSDB (Andrew File System), MB (Mailbox Name), MG (Mail Group), MINFO (Mailbox Information), MR (Mail Rename), ISDN, SRV (Server Resource Record), X25	Refer to the description for the **Search String** field.	Searches for the specified resource records within a specific range based on the **Search String** field.

3 If you selected “Name” or “User-Defined Field” from the **Type** field, the **Search String** options become active. Choose one of the following:

- **Exact match** - a name or User-Defined Field that exactly matches the text you typed.
- **Begins with** - a name or User-Defined Field that begins with the text you typed. For example, you could type “**`Freeh`**” to search for “`Freehold`”.
- **Contains** - a name or User-Defined Field that contains the text you typed somewhere within it. For example, you could type “**`xts`**” to search for names such as “`xts000001xts`”.

4 Click **Search**. When a domain is highlighted, the subnets in that domain are displayed in the lower portion of the window.

5 If you selected “Resource Record” from the **Type** field, the **Search String** radio buttons become active. Choose one of the following:

- **Owner** - search on the Owner (the Object Name or Domain Name) of the Resource Record.
- **Data** - search on the Data contained in the Resource Record.
- **Both** - search on both the Owner and the Data of the Resource Record.

Note: When specifying a Domain Name as part of the search criteria, and Owner or Both is selected, the Domain Name must be fully-qualified. Otherwise, the appropriate records may not be found.

6 Click **Search**. Any **Owner** and/or **Data** field that contains the **Search String** (case insensitive) is returned by the search. The following is displayed, based on your search criteria:

- If you searched on an object, the Go To window displays the objects. Double-clicking on the Object takes you to the Object Profile.
- If the search only turns up one object, the Object Profile is displayed.
- If you searched on a domain, network, OSPF area, or subnet organization, the window displays all subnets belonging to this item in an expanded window.

7 Select a subnet from this window, and double-click. The Object Management window opens.

END OF STEPS

Find an object by location

Purpose

Use this procedure to find an object by its location.

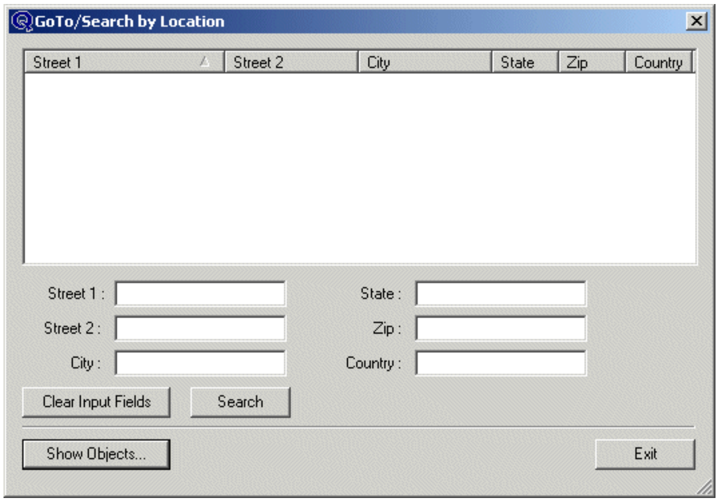
Before you begin

Depending on how the **Location Search** global policy is set, the Go To/Search by Location window defaults to displaying a list of locations (if they exist) upon opening. If the policy is set to True, no list is displayed and you must request that the system perform a search. Refer to Table 3-5, "General policies" (p. 3-29) for more information on setting the **Location Search** policy.

Procedure

To find an object by its location, follow these steps:

1 Select **GoTo/Search|Objects by Location** from the Management menu. The Go To/Search by Location window opens.

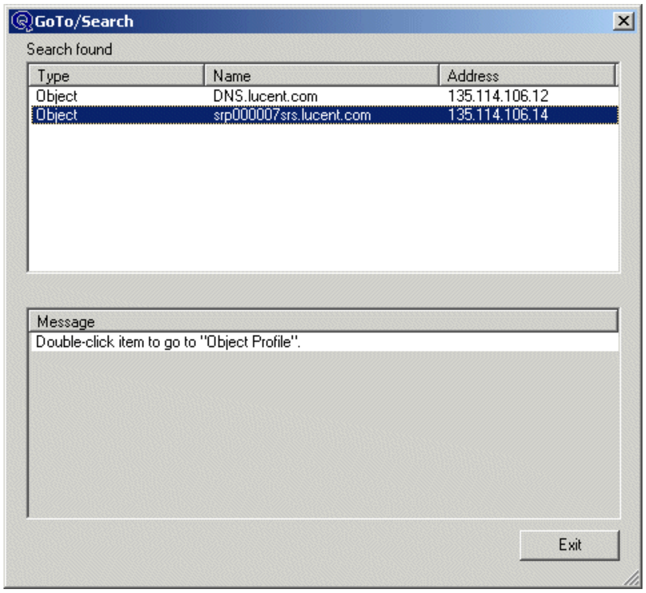


2 Type the Street 1 address, Street 2 address, City, State, Zip, and Country in the appropriate fields. Each of these fields is optional. Wildcards cannot be used in these fields.

3 To clear the fields so you can enter a different location, click **Clear Input Fields**.

4 Once you have entered the information you are searching for in the lower portion of the window, click **Search**. A list displays, matching the search criteria.

5 Select a location from the list, and click **Show Objects**. The Go To/Search window opens. Highlight the object, and a message stating "`Double-click item to go to "Object Profile"` opens in the lower portion of the window.



Type	Name	Address
Object	DNS.lucent.com	135.114.106.12
Object	srp000007srs.lucent.com	135.114.106.14

Message
Double-click item to go to "Object Profile".

6 Double-click on the object to obtain the Object Profile window. Refer to "Find an object" (p. 1-43) for more information on the behavior of this GoTo/Search Results window.

END OF STEPS

Find an object by contact

Purpose

Use this procedure to find an object from its contact information.

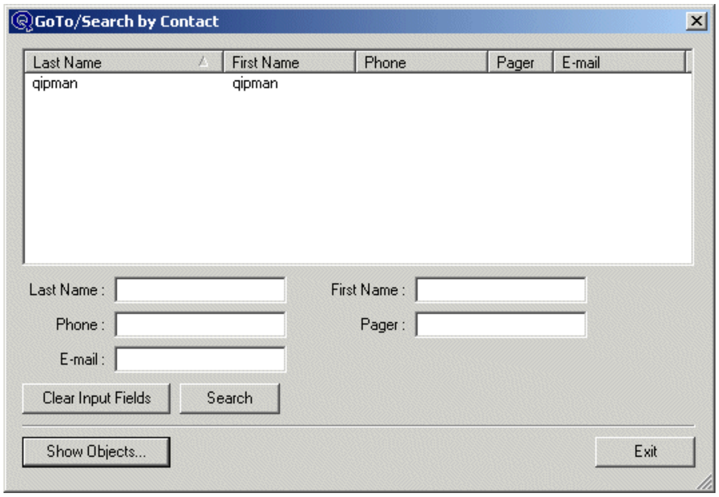
Before you begin

Depending on how the **Contact Search** global policy is set, the Go To/Search by Contact window defaults to displaying a list of locations (if they exist) upon opening. If the policy is set to True, no list is displayed and you must request that the system perform a search. Refer to Table 3-5, “General policies” (p. 3-29) for more information on setting the **Contact Search** policy.

Procedure

To search for an object by contact, follow these steps:

1 Select **Go To/Search|Objects by Contact** from the **Management** the menu. The GoTo/Search by Contact Name window opens.



Last Name	First Name	Phone	Pager	E-mail
qipman	qipman			

Last Name :

First Name :

Phone :

Pager :

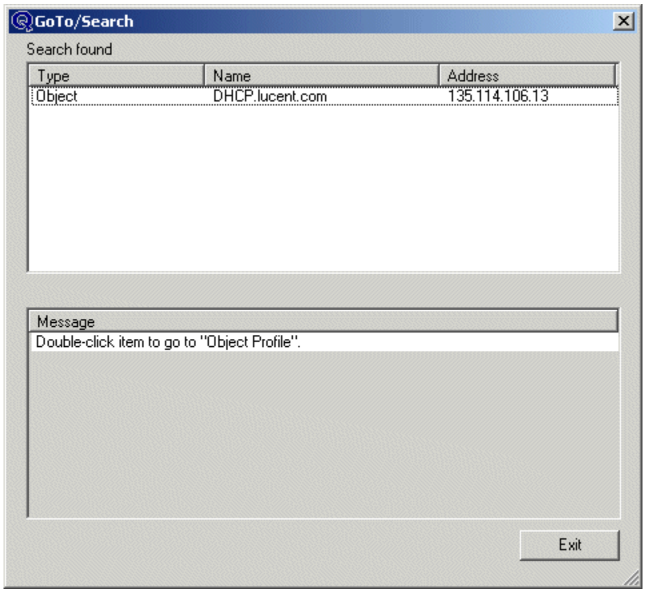
E-mail :

2 Type the last or first name in the appropriate fields. Each of these fields is optional. Searches cannot be performed using the **Phone**, **Pager**, or **E-mail** fields. Wildcards cannot be used in these fields.

3 To clear the fields so you can enter a different contact name, click **Clear Input Fields**.

4 Once you have entered the information you are searching for in the lower portion of the window, click **Search**. A list displays matching the search criteria.

5 To find out which objects an individual is responsible for, select a contact from the list and click **Show Objects**. The GoTo/Search window opens.



Search found

Type	Name	Address
Object	DHCP.lucent.com	135.114.106.13

Message

Double-click item to go to "Object Profile".

6 Highlight the object, and a message stating `Double-click item to go to “Object Profile”` opens in the lower portion of the window. Double-click on the object to obtain the Object Profile window.

END OF STEPS

2 DHCP policies and templates

Overview

Purpose

When planning networks, it is essential to establish standards that should be applied throughout the network for how IP services are expected to function and operate. The purpose is to describe the various functions in VitalQIP that you can use to establish those standards:

- DHCP and Bootp Templates
- Client Class Options

Contents

The following topics are covered:

DHCP/Bootp templates	2-3
DHCP template classes and options	2-3
Add a new template class	2-5
Add a new option to a DHCP class	2-7
Rename a DHCP template class	2-11
Modify a DHCP template option	2-12
Delete a DHCP template class or option	2-13
DHCP/Bootp template option values	2-14
RFC 1497 Vendor Extensions	2-15
IP Layer Parameters per Host	2-19
IP Layer Parameter per Interface	2-21
Link Layer Parameters per Interface	2-24

TCP Parameters	2-25
Application and Service Parameters	2-26
DHCP Extensions	2-33
Novell options	2-37
RFC 2563 options	2-40
SLP Protocol options	2-41
User Authentication Protocol options	2-43
Domain Search option	2-44
PacketCable options	2-45
DHCP/Bootp option templates	2-49
Standard templates offered with VitalQIP	2-52
The general template	2-53
The microsoft_clients template	2-54
The Windows multicast template	2-55
Create a new DHCP option template	2-56
Enter user-defined values	2-59
Modify a DHCP option template	2-60
Delete a DHCP option template	2-61
Copy a DHCP option template	2-62
DHCP policy templates	2-63
Create a DHCP policy template	2-64
DHCP configuration file policies	2-67
DHCP server policies	2-71
Set PingDelay policy	2-89
Client Class	2-90
Add a new Client Class	2-91
Modify a Client Class	2-94
Delete a Client Class	2-95

DHCP/Bootp templates

The **DHCP/Bootp Template** option includes three components:

- **Class/Option Setup** lists the standard DHCP/Bootp RFC Classes and Options supported by VitalQIP (which you may not modify). It also allows you to define your own Classes so you can create site-specific Options.
- **Option Template** is used to define and modify templates for Bootp/DHCP servers, allowing you to define DHCP client options according to specifications contained in the RFCs listed in the following table.

Table 2-1 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
3361	DHCP Option for Session Initiated Protocol (SIP) Servers
3397	DHCP Domain Search option
3442	Classless Static Route Option
3495	DHCP Option for CableLabs Client Configuration
4280	DHCP Options for Broadcast and Multicast Control Servers
4833	DHCP Timezone Option

- **Policy Template** is used to attach DHCP policy templates at the client class, server, subnet, or scope level.

DHCP template classes and options

VitalQIP supplies a set of default DHCP template classes and associated options, based on RFCs listed in the DHCP Request for Comments (RFCs) table. Template classes 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 template classes and options, you can modify and delete your custom classes and options as needed.

Add a new template class

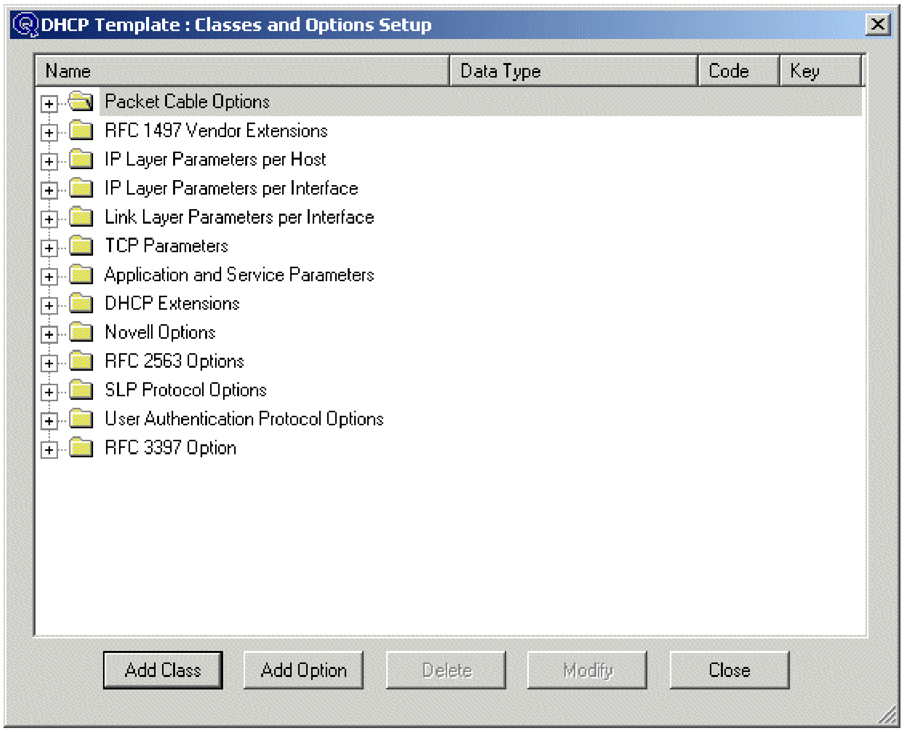
Purpose

Use this procedure to add a new DHCP Template Class.

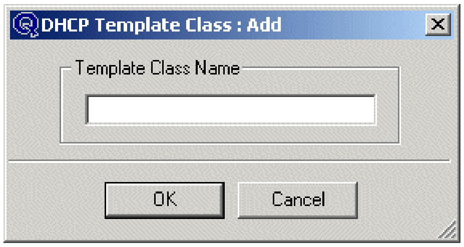
Procedure

To add a new DHCP Template Class, follow these steps:

1 Select **DHCP/Bootp Template|Class/Option Setup** from the **Policies** menu. The DHCP Template Classes and Options Setup window opens.


DHCP Template : Classes and Options Setup
Name
Data Type
Code
Key
Packet Cable 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 Extensions
Novell Options
RFC 2563 Options
SLP Protocol Options
User Authentication Protocol Options
RFC 3397 Option
Add Class
Add Option
Delete
Modify
Close

2 To add a template class, click **Add Class**. The DHCP Template Class:Add window opens.



3 Type the name of the template class you wish to add.

4 Click **OK**. The new template class appears as a folder at the bottom of the **Name** column.

END OF STEPS

Add a new option to a DHCP class

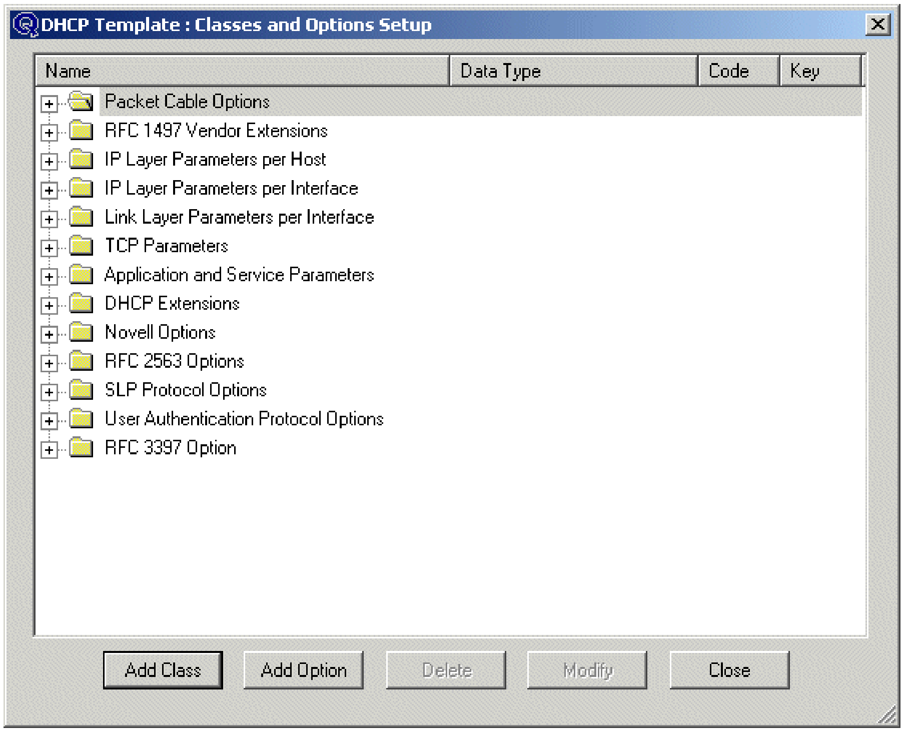
Purpose

Use this procedure to add a new option to a DHCP class.

Procedure

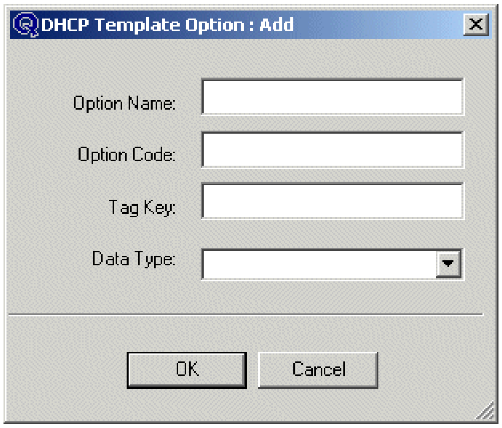
To add a new option, follow these steps:

1 Select **DHCP/Bootp Template|Class/Option Setup** from the **Policies** menu. The DHCP Template: Classes and Options Setup window opens.


DHCP Template : Classes and Options Setup
Name
Data Type
Code
Key
Packet Cable 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 Extensions
Novell Options
RFC 2563 Options
SLP Protocol Options
User Authentication Protocol Options
RFC 3397 Option
Add Class
Add Option
Delete
Modify
Close

2 Select a template class and click **Add Option**.

3 The DHCP Template Option: Add window 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 2-2 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 **OK**. The new option is added to the selected template class.

Note: If you have an option selected when you click **Add Option**, the new option is added under the same class 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 template class

Purpose

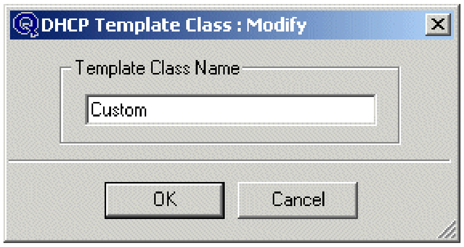
Use this procedure to rename a DHCP template class.

Procedure

To rename a template class, follow these steps:

1 Select **DHCP/Bootp Template|Class/Option Setup** from the **Policies** menu. The DHCP Template: Classes and Options Setup window opens.

2 Select the template class you wish to rename and click **Modify**. The DHCP Template Class: Modify window opens.



Template Class Name: Custom

3 Change the name of the template class and click **OK**. The renamed template class reappears in the DHCP Template: Classes and Options Setup window.

4 Click **Close** to exit the DHCP Template: Classes and Options Setup window.

END OF STEPS

Modify a DHCP template option

Purpose

Use this procedure to modify a DHCP template option.

Procedure

To modify a template option, follow these steps:

1 Select **DHCP/Bootp Template|Class/Option Setup** from the **Policies** menu. The DHCP Template: Classes and Options Setup window opens.

2 Select the template option you wish to change and click **Modify**. The DHCP Template Option: Modify window opens.

3 Make the desired changes to any of the fields and click **OK**. The modified template option reappears in the DHCP Template: Classes and Options Setup window.

4 Click **Close** to exit the DHCP Template: Classes and Options Setup window.

END OF STEPS

Delete a DHCP template class or option

Purpose

Use this procedure to delete a DHCP template class or option.

Before you begin

- You can only delete DHCP template classes/options that have been added; you cannot delete the default classes/options.
- If you delete a class/option, that class/option will be deleted from all templates even if the templates are in use.
- When a class is deleted, all options within that class are also deleted.

Procedure

To delete a template class or option, follow these steps:

1 Select **DHCP/Bootp Template|Class/Option Setup** from the **Policies** menu. The DHCP Template: Classes and Options Setup window opens.

2 Select the template class or option you wish to delete.

3 Click **Delete**. A confirmation dialog box opens.

4 Click **Yes** in response to the confirmation dialog box. The template class or option is removed from the setup window.

END OF STEPS

DHCP/Bootp template option 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 under Class/Option Setup, although your new options must be ones that your DHCP clients can understand. DHCP templates can be created using the existing standard DHCP options and/or your 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 sectionssections explain the options available in each template class. Use these tables as a reference when assigning values to the options in an option template in the **DHCP/Bootp Template|Option Template** function.

> **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**).

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 2-3 Options for RFC 1497 Vendor Extensions

Option name	Option code	Tag key	Data type	Default value	Usage
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.
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.
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.

Option name	Option code	Tag key	Data type	Default value	Usage
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.
Name Server	5	ns	ip_address_list	N/A	Enter the IP address of the IEN-116 name server available to the client.
Domain Name Server	6	ds	static_drop_down_list	Same as in Subnet Profile	List the DNS (STD 13, RFC 1035) name server IP address(es) available to the client. Servers should be listed in order of preference.
Log Server	7	lg	ip_address_list	N/A	Enter the IP address of the MIT-LCS UDP log server available to the client.
Cookie Server	8	cs	ip_address_list	N/A	Enter the IP address of the RFC 865 cookie 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.
Impress Server	10	im	ip_address_list	N/A	Enter the IP address of the Imagen Impress 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.
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.

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.
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.
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).
Swap Server	16	sw	ip address	N/A	Enter the IP address of the client's swap server.
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
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

IP Layer Parameters per Host

The following table describes the RFC 2132 options for IP Layer Parameters per Host.

Table 2-4 Options for IP Layer Parameters per Host

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.
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.
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.
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.

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.
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.

IP Layer Parameter 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 2-5 Options for IP Layer Parameter per Interface

Option name	Option code	Tag key	Data type	Default value	Usage
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.
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.

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.
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.
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.

Option name	Option code	Tag key	Data type	Default value	Usage
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.
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.

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 2-6 Options for Links Layer Parameters per Interface

Option name	Option code	Tag key	Data type	Default value	Usage
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.
ARP Cache Timeout	35	at	numeric	N/A	Enter the time-out in seconds for ARP cache entries, from 0 to 2,147,483,647.
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.

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 2-7 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 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.
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.

Application and Service Parameters

The following table describes the RFC 2132, RFC 3361, RFC 4280, and RFC 4833 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 2-8 Options for Application and Service Parameters

Option name	Option code	Tag key	Data type	Default value	Usage
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 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 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.

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.

Option name	Option code	Tag key	Data type	Default value	Usage
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 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 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: ValueNode type 0x1B-node 0x2P-node 0x4M-node 0x8H-node
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.
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.
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.
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.

Option name	Option code	Tag key	Data type	Default value	Usage
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.
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.
Simple Mail Transport Protocol (SMTP)	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.
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.
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.
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.
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.
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.

Option name	Option code	Tag key	Data type	Default value	Usage
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.
Broadcast and Multicast Control Service Domain List	88	bmdl	name_list	N/A	Lists server names that host the Broadcast and Multicast services that are specified as domain names. **Note:** This parameter is also supported on the Lucent DHCP 5.4 server.
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. **Note:** This parameter is also supported on the Lucent DHCP 5.4 server.
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. **Note:** This parameter is also supported on the Lucent DHCP 5.4 server.
Timezone specified as TZ Database String	101	tzdb	text	255	Specifies a DHCP client's timezone specified as a TZ database string. **Note:** This parameter is also supported on the Lucent DHCP 5.4 server.
SIP Server Address List	120	ssal	ip_address_ list	N/A	Lists the SIP servers specified as IPV4 addresses. **Note:** This parameter is also supported on the Lucent DHCP 5.4 server.
SIP Server Domain List	120	ssdl	text_list	N/A	Lists the SIP servers specified as domain names. **Note:** This parameter is also supported on the Lucent DHCP 5.4 server.

Option name	Option code	Tag key	Data type	Default value	Usage
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.
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.
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.
Scope Life			numeric	N/A	Number of hours before the multicast scope expires.

Note: If you require a sub-option format in the Vendor Specific Information option, the data value must be entered 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). Here is what must be entered in the GUI:

```
[0304c6c88afe210b7375626f7074696f6e3200]
```

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

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

Reads:

`03`	First sub-option, option 3
`04`	Length of 4 octets
`c6c88afe`	IP address 198.200.138.254 in hex
`21`	Second sub-option
`0b`	Length of 11 octets
`7375626f7074696f6e3200`	“suboption2” in hex, null terminated

DHCP Extensions

The following table describes the options for DHCP Extensions.

Table 2-9 Options for DHCP Extensions

Option name	Option code	Tag key	Data type	Default value	Usage
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 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

Option name	Option code	Tag key	Data type	Default value	Usage
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.
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.
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.

Option name	Option code	Tag key	Data type	Default value	Usage
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.
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
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.

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 2-10 RFC 2241 and 2242 Novell options

Option name	Option code	Tag key	Data type	Default value	Usage
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.
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.
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.
AUTO RETRIES			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.
AUTO RETRY_ 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_BROA DCAST			boolean	False	If the value is True, the client ***should*** perform a NetWare Nearest Server Query to find out its nearest NetWare/IP server.

Option name	Option code	Tag key	Data type	Default value	Usage
NWIP Setting			static_drop_down_list	NWP_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		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 2-11 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 2-12 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:
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.
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.

Option/sub-option name	Option code	Tag key	Data type	Default value	Usage
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 2-13 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 2-14 Domain Search option

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**.

PacketCable options

The following table describes the CableLabs Client Configuration 122 sub-options, specified in RFC 3495:

Table 2-15 Sub-options for CableLabs Client Configuration (CCC)

Sub-option name	Data type	Default value	Usage
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 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 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 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 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 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 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.
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.

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 2-16 Sub-options for Site-specific CableLabs Client Configuration (CC)

Sub-option name	Data type	Default value	Usage
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 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.
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.
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 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.
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).

Sub-option name	Data type	Default value	Usage
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.
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.
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.

DHCP/Bootp 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/Bootp 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 DHCP/Bootp Template 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/Bootp option template description

DHCP/Bootp 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 2-17 Locations where DHCP/Bootp option 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 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/Bootp template may define options from the following classes:

- 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
- PacketCable options

Each class has a set of options associated with it, as well as a unique option number. Template options can inherit default values from the VitalQIP infrastructure, or you can assign them static values.

A few things to keep in mind

- A global DHCP 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 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. Manual DHCP and Bootp objects continue to use the object-specified domain name value if it exists.

Standard templates offered with VitalQIP

VitalQIP offers three standard option templates with the product; a **general** template, a **microsoft_clients** template for use with Microsoft Windows clients, and a **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: Modify window.

You can modify the current setting for the **Active Options**, and also extend a template with any option previously added with the DHCP Template Class/Option Setup function, even if the option is not defined in an RFC. For more information on how to create new template classes and options, refer to DHCP template classes and options. For information on how to create your own option template, refer to "Create a new DHCP option template" (p. 2-56).

The general template

Selecting the “general” template in the DHCP Option Template window 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 4th column of the table.

Table 2-18 general template options

Option name	Tag key	Option code	Template class
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 Option Template window 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 4th 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 2-19 microsoft_clients template options

Option name	Tag key	Option code	Template class
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 Option window 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 2-20 Windows multicast template options

Option name	Tag key	Option code	Template class
Scope Life	N/A	N/A	Application and Service Parameters
Multicast TTL	N/A	N/A	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

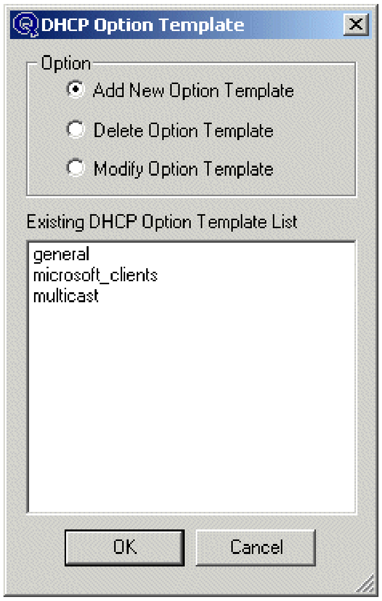
Purpose

Use this procedure to create a new DHCP option template.

Procedure

To create a new option template, follow these steps:

1 Select **DHCP/Bootp Template |Option Template** from the **Policies** menu. The DHCP Option Template window opens.

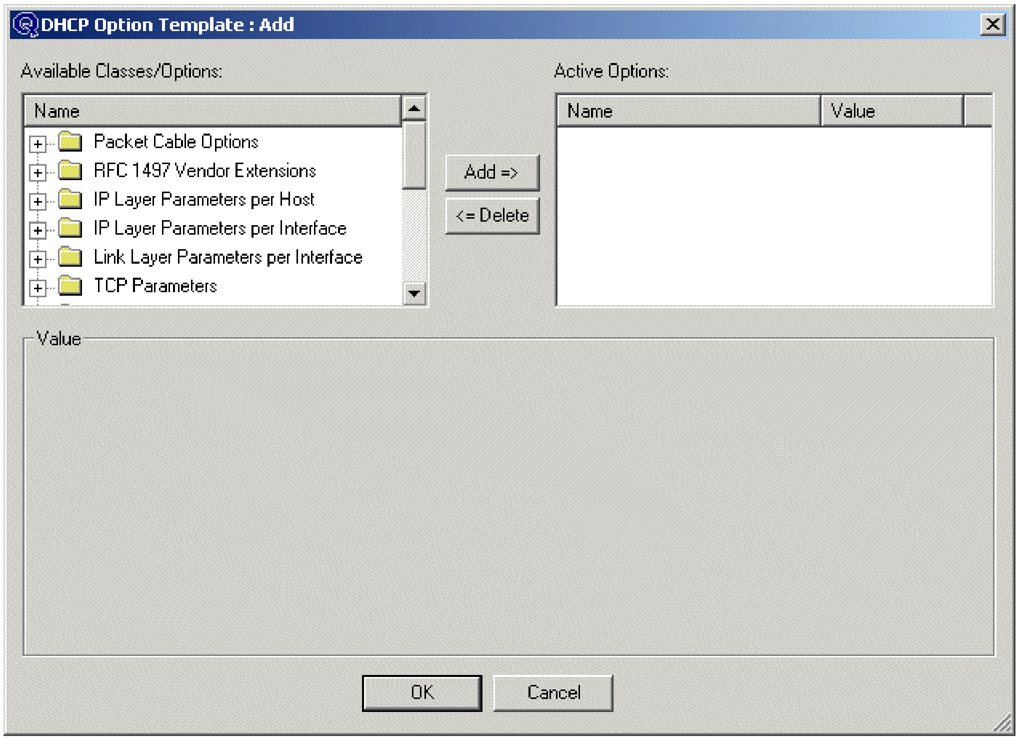

DHCP Option Template

Option
● Add New Option Template
○ Delete Option Template
○ Modify Option Template

Existing DHCP Option Template List

general
microsoft_clients
multicast

2 Click **Add New Option Template** and click **OK**. The DHCP Option Template: Add window opens.


DHCP Option Template : Add
Available Classes/Options:
Name
Packet Cable Options
RFC 1497 Vendor Extensions
IP Layer Parameters per Host
IP Layer Parameters per Interface
Link Layer Parameters per Interface
TCP Parameters
Add =>
<= Delete
Active Options:
Name
Value
Value
OK
Cancel

3 When the DHCP Option Template: Add window opens, the **Available Classes/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.

4 To select options for your DHCP option template, follow one of these steps:

- To select the entire set of options within a class folder, highlight the desired folder and click **Add**. All the options within the class folder appear in the **Active Options** list.
- To select one or only a few options within a folder, click the plus sign to expand the class folder. Use standard Windows selection techniques (click, shift-click, and control-click) to select the desired options. Click **Add** and 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, you need to review the values associated with each and modify them as necessary.

6 To change a value for an option, highlight the option and enter a value in the **Value** field.

Note: Some options have a default value of **Same as in Subnet Profile**, meaning that the value for the option is the same value as defined in the subnet profile. The alternate value is **User Defined**. The procedure for changing the default to a user-defined value is described in "Enter user-defined values" (p. 2-59).

7 When you have finished selecting the options you want in your DHCP option template and have assigned them values, click **OK**. The DHCP Template dialog box appears.

8 Enter a name of up to 64 characters (no spaces) in the **Template Name** field and click **OK**.

END OF STEPS

Enter user-defined values

Purpose

Use this procedure to enter user-defined values.

Procedure

To enter a user-defined value, follow these steps:

1 Select the option in the **Active Options** list. A drop-down list appears in the **Value** list.

2 Select **User Defined** from the **Value** list. A plus sign appears beside the option in the **Active Options** list.

3 To assign a user-defined value, click the plus sign (or double-click the option) to expand it.

4 Highlight **User Defined**. The **Value** field changes so you can enter the value you wish to assign the option.

5 Click **Apply**. (The button label may vary. For example, if you have to add a list of IP Addresses, the button reads **Add**.)

A few things to keep in mind

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 value(s) 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 **Manual Bootp** tab in the Object Profile.

END OF STEPS

Modify a DHCP option template

Purpose

Use this procedure to modify a DHCP option template.

Procedure

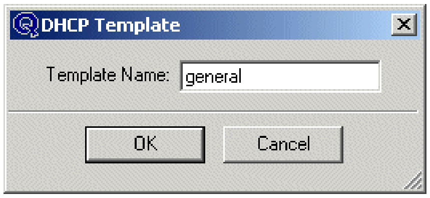
To modify a DHCP option template, follow these steps:

1 In the DHCP Option Template window, select **Modify Option Template**. The DHCP Option Template - Modify window opens.

2 Select the template you wish to modify and click **OK**.

3 Add, delete, or modify options and their values in the template as necessary.

4 Click **OK** to save the changes. The DHCP template dialog box opens.



Template Name: general

5 Click **OK**.

END OF STEPS

Delete a DHCP option template

Purpose

Use this procedure to delete a DHCP option template.

Procedure

To delete a DHCP option template, follow these steps:

1 In the DHCP Option Template window, click **Delete Option Template**. The DHCP Options Template - Delete opens.

2 Select the option template you wish to delete, and then click **OK**. A confirmation dialog box opens.

3 Click **Yes**.

END OF STEPS

Copy a DHCP option template

Purpose

This section describes how to copy a DHCP template.

Procedure

To copy a DHCP option template, follow these steps:

1. In the DHCP Option Template window, select **Modify Option Template**.

2. Select the option template you wish to copy and click **OK**. The DHCP Option Template - Modify window opens.

3. Add, delete, or modify values in the template as necessary.

4. Click **OK** when you are ready to save the template. The DHCP Template dialog box opens.

5. Modify the template name.

6. Click **OK** to save a copy of the original template.

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. Two types of policy templates are available.

1. **DHCP Server Policies** that are set at the server level and define the contents of the *dhcpd.pcy* file.
2. **DHCP Configuration File Policies** that are set at the subnet, client class, or scope level and define the following settings in the *dhcpd.conf* file:
   - DHCP Address Shuffling
   - DHCP lease query message hardware override
   - Subnet Selection Option

Create a DHCP policy template

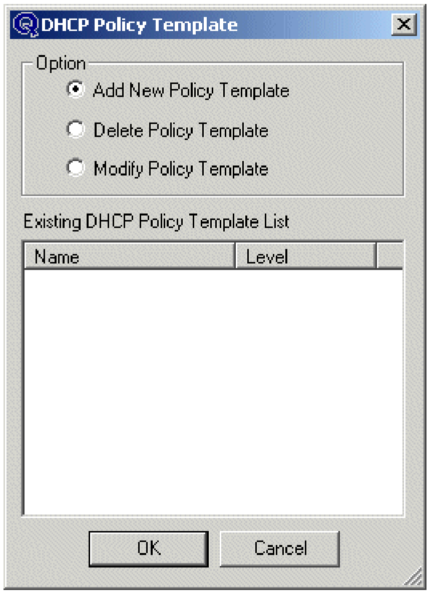
Purpose

Policy templates can be set for four different levels - server, client class, subnet, and scope.

Procedure

To add a new policy template, follow these steps:

1 Select **DHCP/Bootp Template|Policy Template** from the **Policies** menu. The DHCP Policy Template window opens.



Option

● Add New Policy Template

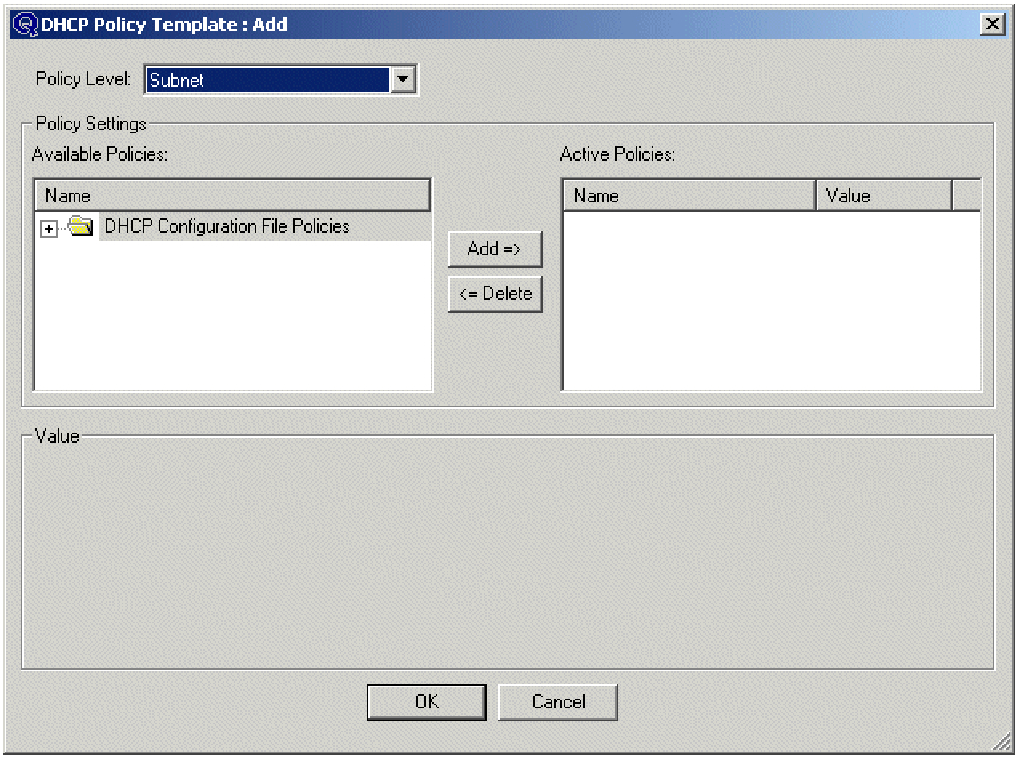
○ Delete Policy Template

○ Modify Policy Template

Existing DHCP Policy Template List

Name	Level

2 Ensure that the **Add New Policy Template** option is selected and click **OK**. The DHCP Policy Template: Add window opens. The Subnet Policy Level is the default, with the DHCP Configuration File Policies folder displayed in the **Available Policies** list.



DHCP Policy Template : Add

Policy Level: Subnet

3 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 Policies** list changes to DHCP Server Policies.

4 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 Policies** list.
- To select one or only a few policies within a Policy folder, click the plus sign to expand the folder. Use standard Windows selection techniques (click, Shift-click, and Control-click) to select the desired option(s). Click **Add** and the option(s) appear in the **Active Policies** list.

5 When the policy appears in the **Active Policies** list, highlight the policy whose default value you wish to change. The **Value** field becomes active and you can select the desired value from the drop-down list (or type a value if the data type is text or numeric).

6 When you have finished making selections and establishing values, click **OK**. The DHCP Template dialog box opens.

7 Enter a unique name for the DHCP template (no spaces allowed) and 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 2-21 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.
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.

Policy name	Values	Default value	Usage
lease-query-hw-type-override	numeric	1	The hardware type (htype) parameter, to be included in the DHCPACK response to the lease query message. Refer to the Internet Assigned Numbers Authority (IANA) list of ARP hardware types in RFC 1700 for a complete list. Since the vast majority of installations are of the Ethernet type, a value of 1 is used by default, if there is no override configured for the subnet. **Note:** This policy is only available at the subnet policy level.
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.
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.
excluded-vendor-classes	text	none	This is a scope level policy that specifies the vendor class values to be excluded from obtaining a lease from the scopes to which this policy is assigned. Trailing wildcards are supported using the asterisk (*).

Policy name	Values	Default value	Usage
excluded-user-classes	text	none	This is a scope level policy that specifies the user class values to be excluded from obtaining a lease from the scopes to which this policy is assigned. Trailing wildcards are supported using the asterisk (*).

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 2-22 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	Integer	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	Integer	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**.
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.

Policy name	Values	Default value	Usage
ExpireAllLeasesOnRestart	True False	True	When set to False, only leases that have expired since the service restarted are deleted. When the option is set to True, all expired leases found in the database are deleted.
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. 2-89) 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.

Policy name	Values	Default value	Usage
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.
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.

Policy name	Values	Default value	Usage
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.
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.

Policy name	Values	Default value	Usage
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
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

This section describes how to set the PingDelay policy.

Procedure

The Lucent DHCP server will need to be configured to perform a ping before assign. To do so, follow these steps:

1 Log into the VitalQIP client.

2 From the **Infrastructure** menu, click **Server**.

3 Select all Lucent DHCP servers which might have been created in previous VitalQIP versions.

4 Click **Modify**.

5 In **Parameter/Values** list, click **+** to expand **Use Server Policy Template** (if it is set False).

6 Click **+** to expand **DHCP Server Policies**.

7 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.

8 Click **OK** to save the change.

9 Perform a DHCP file generation via **Network Services|DHCP Generation** and verify in the *dhcpd.pcy* file that a line with the `PingDelay` policy exists.

END OF STEPS

Client Class

A Client Class allows you to assign DHCP option templates and 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 Client Class are applied to any DHCP client that specifies the matching vendor, user class (refer to Option 60 and Option 77 in RFC 3004, respectively), or device class (refer to RFC 3256).

Options and policies applied to a DHCP client from a 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 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.

Add a new Client Class

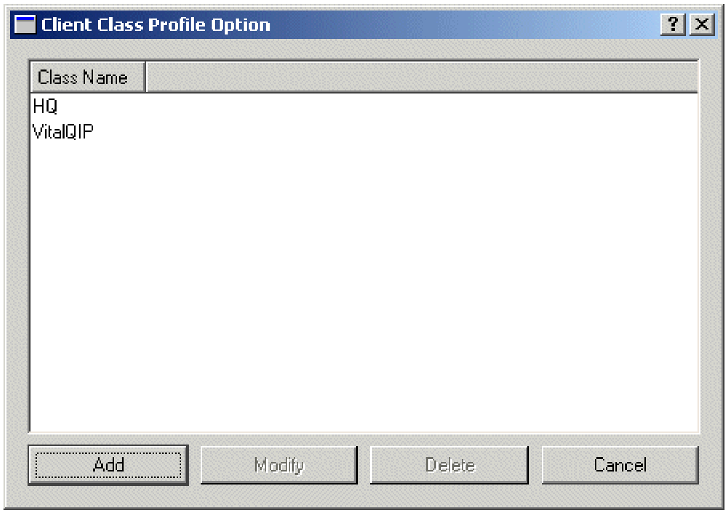
Purpose

This section describes how to add a new Client Class.

Procedure

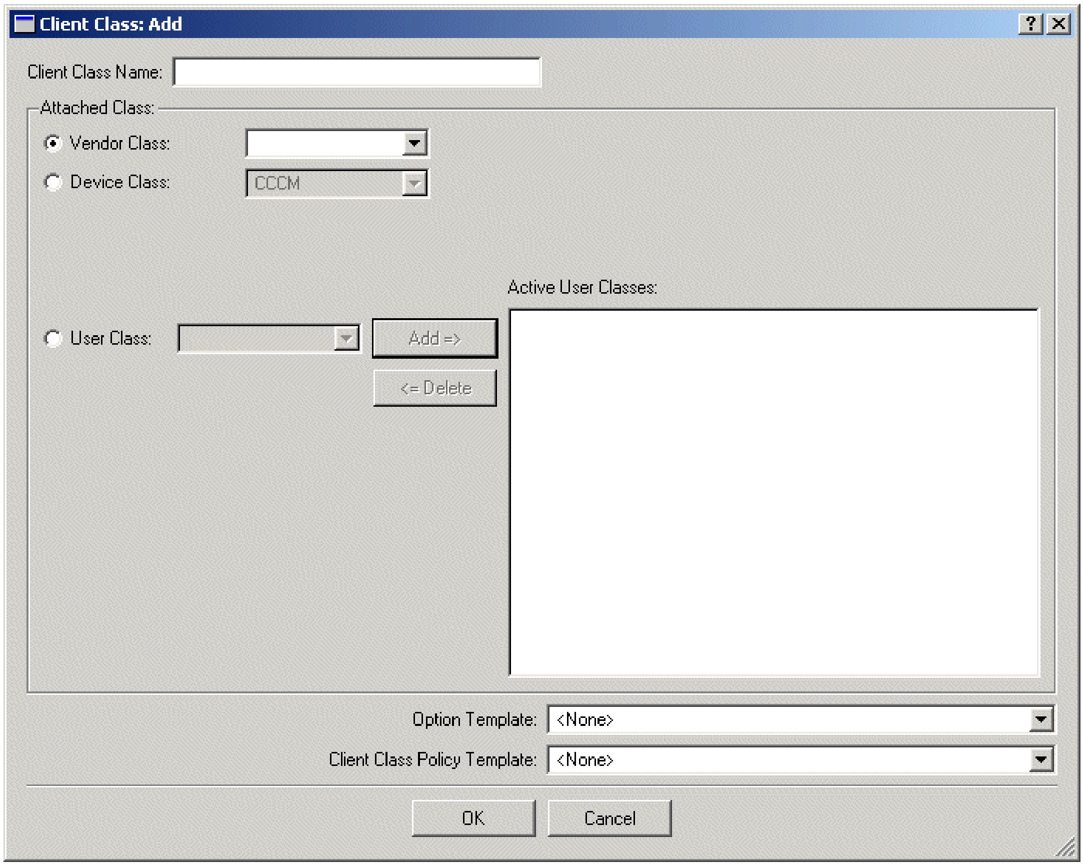
To add a new Client Class, follow these steps:

1 Select **Client Class** from the **Policies** menu. The Client Class Option window opens.



HQ
VitalQIP

2 Check the **Add New Client Class** option and click **OK**. The Client Class: Add window opens.



Client Class: Add

Client Class Name:

Attached Class:

● Vendor Class:

○ Device Class: CCCM

○ User Class:

Active User Classes:

Option Template: <None>

Client Class Policy Template: <None>

3 Enter a name in the **Client Class Name** field.

4 Enter a **Vendor Class**, select a **Device Class**, or one or more **User Classes**. Click **Add** if adding a User Class. Note that you may use a wildcard (*) as the final character for a Vendor Class or User Class.

5 Select a DHCP option template from the Option Template list.

6 Select a client class policy template (if defined) from the **Client Class Policy Template** list and click **OK**.

Note: The selections available in the Client Class Policy Template drop-down list have a ‘Policy Level’ set to ‘Client Class’.

END OF STEPS

Modify a Client Class

Purpose

This section describes how to modify a Client Class.

Procedure

To modify a Client Class, follow these steps:

1 Select **Client Class** from the **Policies** menu. The Client Class Option window opens.

2 Highlight the class you want to change in the **Existing Client Class** list.

3 Click **Modify** and the Client Class: Modify window opens.

4 Make the changes you desire and click **OK** to save.

END OF STEPS

Delete a Client Class

Purpose

This section describes how to delete a Client Class.

Procedure

To delete a Client Class, follow these steps:

1 Select **Client Class** from the **Policies** menu. The Client Class Option window opens.

2 Highlight the class you want to delete in the **Existing Client Class** list.

3 Click **Delete** and the Client Class: Delete window opens.

4 Click **OK** and a Confirmation dialog box opens.

5 Click **OK** to confirm that this client class needs to be deleted.

END OF STEPS

3 Object policies and profiles

Overview

Purpose

When planning networks, it is essential to establish standards that should be applied to objects throughout the network for how object information is treated. The purpose is to describe the various functions in VitalQIP that you can use to establish those standards:

- ACL Templates
- Naming policies
- Global policies
- Profiles
- User-defined fields
- Object Classes

The purpose is also to describe the profiles and user-defined fields you can use to standardize the names not only of manufacturer equipment, but also contact and location information throughout your network. Once the profiles are established, the information can be readily accessed when defining network objects (or even running management reports).

> **Note:** It is also important to establish Administrator profiles with the **Administrator** option on the **Infrastructure** menu. However, they cannot be established until most of the infrastructure is set up.

Contents

The following topics are covered:

Access Control Lists (ACLs)	3-3
Create an ACL template	3-4
Modify an ACL template	3-8

Delete an ACL template	3-9
Naming policies	3-11
Establish object naming policies	3-11
Customize object names	3-12
Use a business unit ID to customize object naming policies	3-14
Name dynamically allocated objects	3-17
User-defined object naming policy user exit	3-18
Global policies	3-21
Establish global policies	3-22
Profiles	3-42
Manufacturer Profiles	3-42
Add a new manufacturer	3-43
Apply a model name to a manufacturer	3-45
Change the manufacturer profile	3-47
Delete a manufacturer profile	3-48
Manage location profiles	3-49
Manage contact profiles	3-51
User-defined fields	3-53
Create a user-defined field	3-54
Modify a user-defined field	3-55
Delete a user-defined field	3-56
Object classes	3-57
Create a new object class	3-58
Modify an object class	3-61
Delete an object class	3-62

Access Control Lists (ACLs)

VitalQIP provides a template mechanism to allow administrators to easily create and maintain Access Control Lists (ACLs). ACLs are written to the *named.conf* file and filter host access to DNS zone option parameters. All administrators who have write access to at least one part of the infrastructure can add, modify, or delete ACLs using the **ACL Template** function on the **Policies** menu.

Note: 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.

Create an ACL template

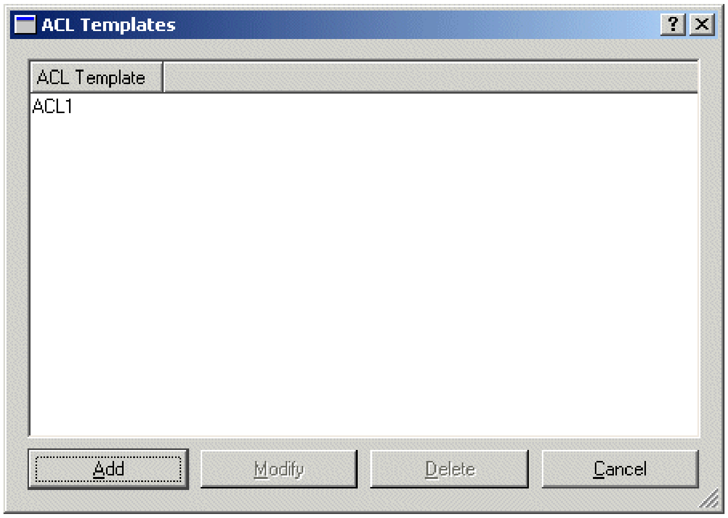
Purpose

Use this procedure to create an ACL template.

Procedure

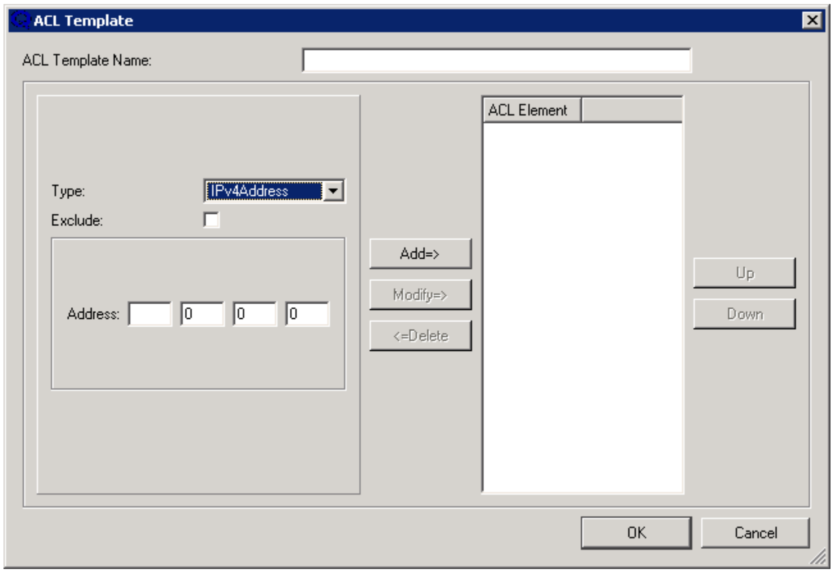
To create an ACL, follow these steps:

1 Select **ACL Templates** from the **Policies** menu. The ACL Templates window opens.



ACL1

Click **Add**. The ACL Template window opens.



Type: IPv4Address

Exclude: □

Address: 0 0 0

2 Enter a **Template Name** of up to 255 alphanumeric characters.

3 Choose one of the following actions.

If you are…	Then…
Adding a IPv4 address ACL element	1. In the **Type** field, select **IPv4 Address**. 2. Check **Exclude** if you wish to prevent the element from being accessed from the Access Control List. 3. In the **Address** field, enter a IPv4 address. 4. Click **Add**. **Result:** The IPv4 address is added to the list.
Adding a IPv4 network ACL element	1. In **Type** field, select **IPv4 Network**. 2. Check **Exclude** if you wish to prevent the element from being accessed from the Access Control List. 3. In the **Address** field, enter a network address. 4. In the **Mask Length** field, enter the length of the network address or use the slider to select a length. 5. Click **Add**. **Result:** The IPv4 network is added to the list.
Adding a IPv6 address ACL element	1. In **Type** field, select **IPv6 Address**. 2. Check **Exclude** if you wish to prevent the element from being accessed from the Access Control List. 3. In the **Address** field, enter a IPv6 address. 4. Click **Add**. **Result:** The IPv6 address is added to the list.
Adding a IPv6 network ACL element	1. In **Type** field, select **IPv6 Network**. 2. Check **Exclude** if you wish to prevent the element from being accessed from the Access Control List. 3. In the **Network** field, enter a network address. 4. In the **Mask Length** field, enter the length of the network address or use the slider to select a length. 5. Click **Add**. **Result:** The IPv6 network is added to the list.

If you are...	Then...
Adding a nested ACL template element	1. In **Type** field, select **ACL Template**. 2. Check **Exclude** if you wish to prevent the element from being accessed from the Access Control List. 3. In the **ACL Template** field, enter an ACL template. The ACL Template is added to the **ACL Template** field. 4. Click **Add**. **Result:** The ACL template is added to the list.
Adding a key ACL element	1. In **Type** field, select **Key**. 2. Check **Exclude** if you wish to prevent the element from being accessed in the DNS View. 3. In the **Key** field, enter a key. 4. Click **Add**. **Result:** The key is added to the list.
Adding other types of ACL elements	1. In **Type** field, select **Other**. 2. Check **Exclude** if you wish to prevent the element from being accessed from the Access Control List. 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.
Modifying 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.
Deleting an ACL element	1. Select an ACL element from the list. 2. Click **Delete**. **Result:** The element is deleted from the list.
Moving 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 in the list – **Down** to moved the element one row down in the list.

4 Click **OK** to save the template. The Add successfully dialog box opens.

5 Click **OK** in response to the Added successfully dialog box.

Once you have saved a template, it is available for selection in the Zone Options and Primary/Secondary Server tabs in the Domain and Reverse Zone profiles.

ACL templates are now accessible to DNS Views and can be referenced in other ACL templates.

END OF STEPS

Modify an ACL template

Purpose

Use this procedure to modify an ACL template.

Procedure

To modify an ACL template, follow these steps:

1 Select **ACL Templates** from the **Policies** menu. The ACL Templates window opens.

2 Highlight the template you wish to modify in the ACL Templates window.

3 Click **Modify**. The ACL Template window opens.

4 Make changes as needed and click **OK** to save.

5 Click **OK** in response to the Modified successfully dialog box.

END OF STEPS

Delete an ACL template

Purpose

Use this procedure to delete an ACL template.

Before you begin

Deleting the last ACL Template associated with a zone option removes that zone option from the server's *named.conf*.

Procedure

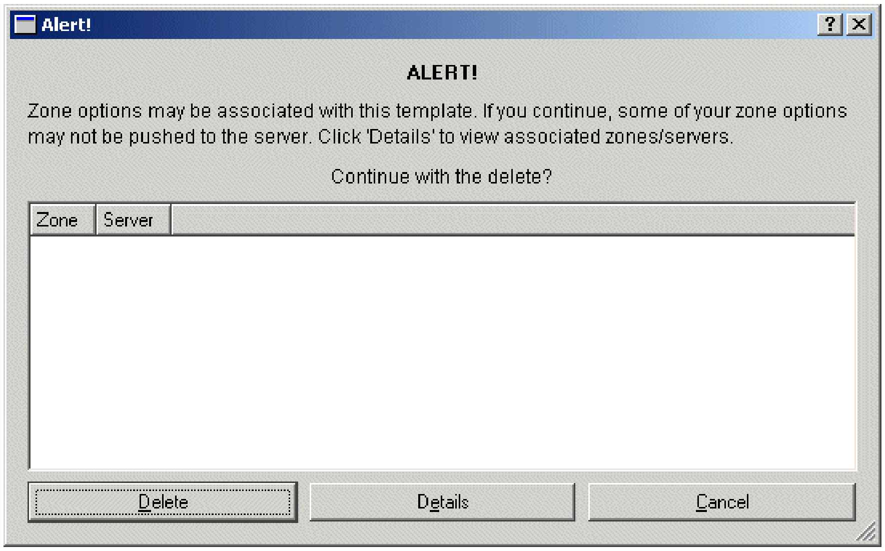
To delete an ACL template, follow these steps:

1 Select **ACL Templates** from the **Policies** menu. The ACL Templates opens.

2 Highlight the template you wish to delete in the ACL Templates window.

3 Click **Delete**. The ACL Template window opens.

4 Click **OK** to delete. If there are any associations with existing servers, zone options, DNS Views, or other ACL templates, the Alert window opens.



ALERT!

Zone options may be associated with this template. If you continue, some of your zone options may not be pushed to the server. Click 'Details' to view associated zones/servers.

Continue with the delete?

5 Click **Details** to check the zones and servers associated with the template.

6 If you are satisfied with the deletion of the ACL template, click **Delete**. The Deleted successfully dialog box opens.

7 Click **OK** in response to the Deleted successfully dialog box.

END OF STEPS

Naming policies

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, one satisfies each request with an instance number automatically incremented. 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 3-1 Sample unique object name policies

Prefix	Instance Length	Suffix	Object Name
pcp	6	pcp	pcp000001pcp
	6	pcp	000001pcp
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 Naming Policies window to any name you choose.

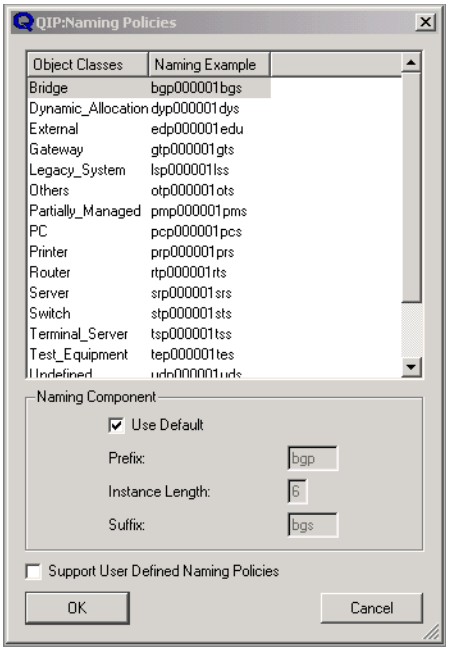
Before you begin

- 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 (described in "Object classes" (p. 3-57)).
- 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. 3-17) for further information.

Procedure

To change object names, follow these steps:

1 Select **Naming Policies** from the **Policies** menu. The Naming Policies window opens.



QIP:Naming Policies

Object Classes	Naming Example
Bridge	bgp000001bgs
Dynamic_Allocation	dyp000001dys
External	edp000001edu
Gateway	gtp000001gts
Legacy_System	lsp000001lss
Others	otp000001ots
Partially_Managed	pmp000001pms
PC	pcp000001pcs
Printer	prp000001prs
Router	rtp000001rts
Server	srp000001srs
Switch	stp000001sts
Terminal_Server	tsp000001tss
Test_Equipment	tep000001tes
Undefined	udp000001uds

Naming Component

☑ Use Default

Prefix: bgp

Instance Length: 6

Suffix: bgs

☐ Support User Defined Naming Policies

2 Select the **Object Class** you wish to customize.

The **Prefix**, **Instance Length**, and **Suffix** fields are displayed in the lower window. If the default global naming policy is being used, the fields are read only and the **Use Default** checkbox is checked.

3 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 for **Prefix**, **Instance Length**, and **Suffix**, as described in the following table. If you click **Use Default** again, the default value for the naming policy appears in the fields, which become read-only again.

Table 3-2 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 8 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.

4 Check the **Support User Defined Naming Policy** 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. 3-18) for detailed information on the fields that are passed with this user exit and how to set it up.

5 Click **OK** to save your changes. A Confirmation prompt opens.

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

END OF STEPS

Use a business unit ID to customize object naming policies

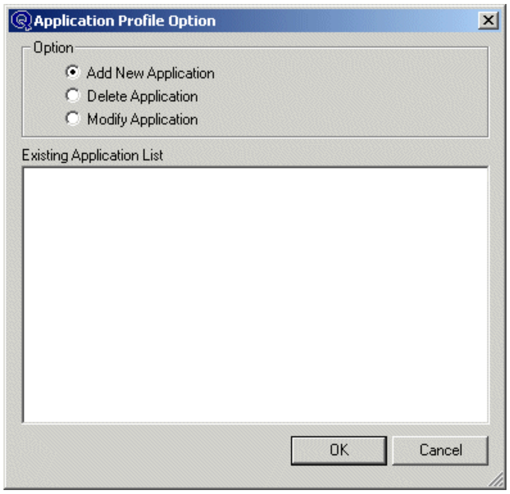
Purpose

Additionally, 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 **Infrastructure** menu.



Application Profile Option

Option

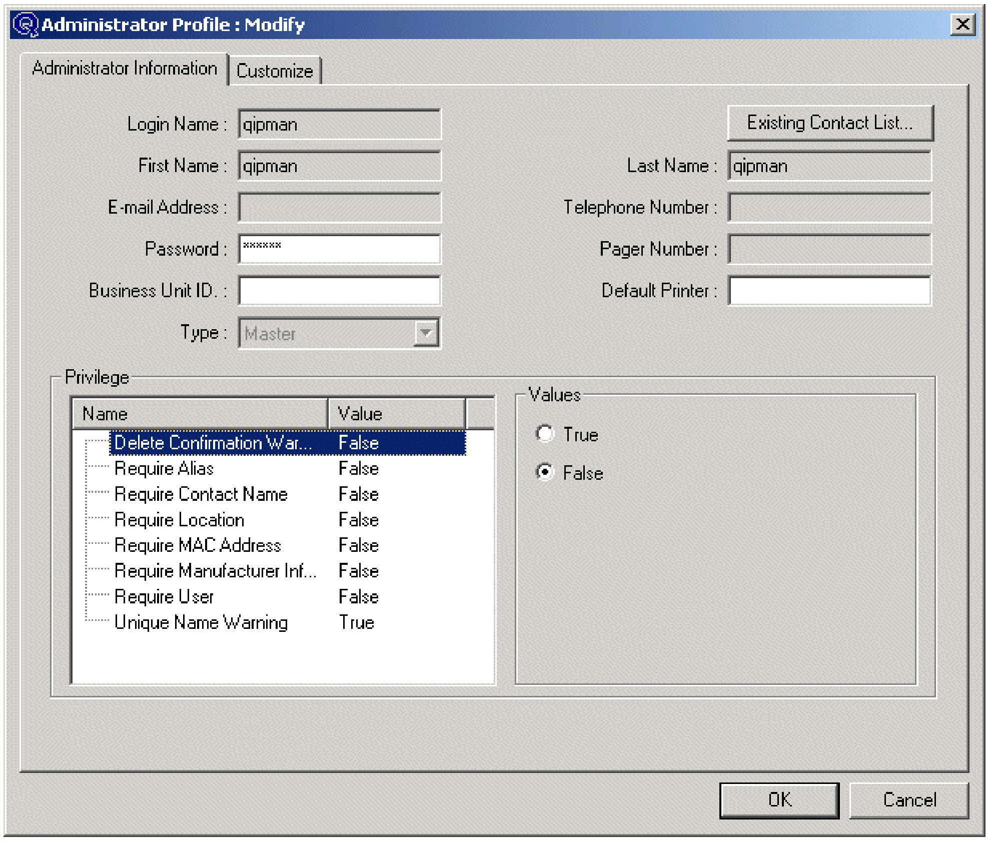
● Add New Application

○ Delete Application

○ Modify Application

Existing Application List

2 Select the administrator profile you wish to modify from the **Existing Administrators** list and click **OK**. The Administrator Profile: Modify window opens.



Administrator Profile : Modify

Administrator Information | Customize

Login Name : qipman

First Name : qipman

E-mail Address :

Password : ******

Business Unit ID. :

Type : Master

Last Name : qipman

Telephone Number :

Pager Number :

Default Printer :

Privilege

Name	Value
Delete Confirmation War...	False
Require Alias	False
Require Contact Name	False
Require Location	False
Require MAC Address	False
Require Manufacturer Inf...	False
Require User	False
Unique Name Warning	True

Values

○ True

● False

3 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”.

4 Click **OK** to save the change to the profile. A confirmation dialog box opens.

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

When the administrator “jsmith” creates objects in the Object Profile, the **Object Name** (as established in the Naming Policies window) will be prefixed with JS. The following table shows the break down of the **Object Name** when a **Business Unit ID** is used.

Table 3-3 Sample object names with business unit ID

Business Unit ID	Prefix	Instance Length	Suffix	Object Name
JS	pcp	6	pcp	JSpcp000001pcp
JS		6	pcp	JS000001pcp
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

- For all object classes ***except*** “Dynamic_Allocation”, if the instance number is set at one or more, either a **Prefix** or **Suffix** (of at least one character) is required. It is not allowed to have an **Instance Length** only.
- 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 Naming Policies window of the **Policies|Naming Policies** option of VitalQIP. See "User-defined fields" (p. 3-53) for more information.

> **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. The **Policies|Global Policies|General|User Exit Name** policy must set to "True" or check the **Support User Defined Naming Policies** check box in **Policies|Naming Policies**.
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 **Policies|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 **Policies|Global Policies|General|Name Validation** global 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.

Global policies

Global policies allow you to establish standardized behavior for the operation of your VitalQIP server. Policies fall under three categories, Dynamic DNS, General, and Reports.

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 for reports. Each policy is explained in a table. You must select a value for each option.

Establish global policies

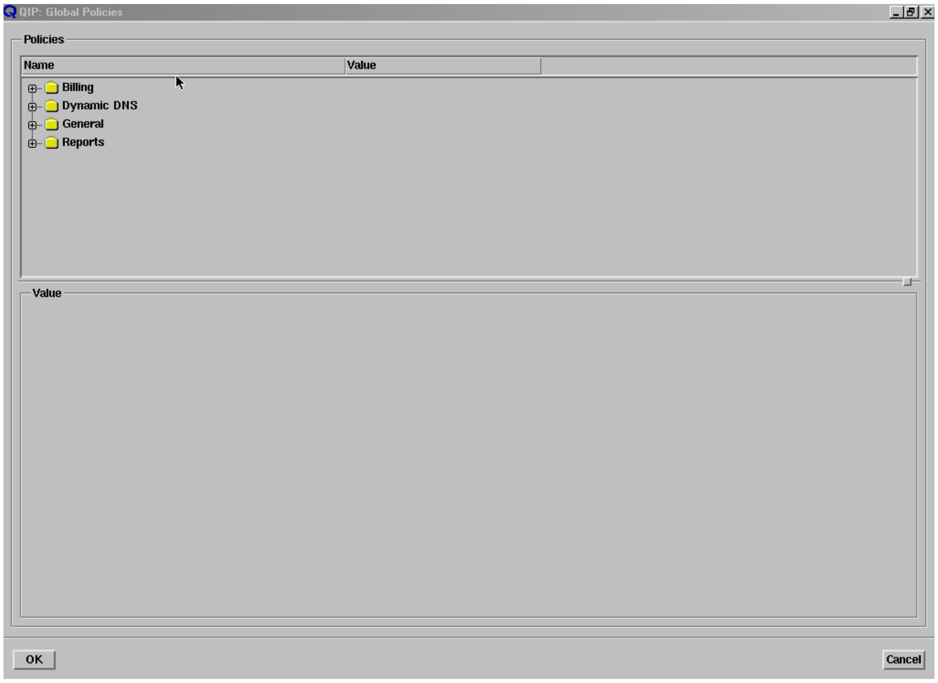
Purpose

Use this procedure to set up global policies.

Procedure

To set up global policies, follow these steps:

1 Select **Global Policies** from the **Policies** menu. The Global Policies window opens.



2 Select the policy **Name** (such as Dynamic DNS or General) you want to modify and expand it to show the available options. The options and default values associated with that policy appear.

3 As you highlight a policy in the listing, the corresponding **Value** options change 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. Clicking **OK** saves the changes and exits the window. Clicking **Cancel** exits without saving any changes.

Table 3-4 Dynamic DNS policies

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

Policy name	Values	Default value	Usage
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|Object Information tab.
Secure DNS Updates			Opens to display the following group of policies, specifically designed to set up Secure DNS.
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.

Policy name	Values	Default value	Usage
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.
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.

Policy name	Values	Default value	Usage
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|Object Information** tab.
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-8.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 3-5 General policies

Policy name	Values	Default value	Usage
Set Default Servers on Subnet	True or False	True	If this policy is set to True, then default servers are assigned. If the policy is set to False, then 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.

Policy name	Values	Default value	Usage
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.
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 a 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.

Policy name	**Values**	**Default value**	**Usage**
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.
DNS SOA Serial Number Type	DATE or NODATE	NODATE	This policy defines the format of the serial number in the DNS files. This option was applicable only 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 9.X servers including LUCENT DNS 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.

Policy name	**Values**	**Default value**	**Usage**
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. Refer to "Set up a Windows 2003 site for a subnet organization" (p. 5-109).
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.
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*.

Policy name	Values	Default value	Usage
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.

Policy name	Values	Default value	Usage
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. Refer to "ClientHostNameProcessing" (p. 2-75) for further information.

Policy name	Values	Default value	Usage
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.
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.)

Policy name	Values	Default value	Usage
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.
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. Updates from the VitalQIP DHCP server to the QIP database via the VitalQIP Update Service for Manual DHCP/Bootp objects will not occur in the VitalQIP 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.

Policy name	Values	Default value	Usage
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.
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. 3-18).

Policy name	Values	Default value	Usage
Validate CNAME Records			This policy determines if VitalQIP validates data to prevent CNAME conflicts. For added or modified CNAME records, these validation checks are driven by the following policies: • Object aliases • Domains • ENUM NAPTRs • IPv4 objects • IPv6 objects • Resource records If any of the above policies is set to True, validation of the respective infrastructure component occurs when a CNAME record is added to VitalQIP. If an IPv4/IPv6 object, VitalQIP domain, Resource record (other than CNAME), or ENUM NAPTR record is added, then validation against CNAMES will occur, if the Validate object aliases policy is set to True. For added or modified records other than CNAME records, validation checks are made against: • Object aliases • CNAME object resource records • CNAME domain resource records • CNAME reverse zone resource records

Policy name	Values	Default value	Usage
			These validation checks help prevent "CNAME and Other data" errors or multiple CNAME errors on the DNS server. Zones with these errors are not loaded or are rejected by the DNS server. If a CNAME conflict occurs during data entry into VitalQIP, an error message is displayed providing information about the collision.
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 3-6 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.

Profiles

The **Manufacturer Profiles** allows you to define the make, model, and tag information for equipment on your network, which you can then associate with objects.

Location Profiles establish location information that can be assigned to the Object Profile, User Profile, and Subnet Profile. You can manage the information on the locations in this window.

Contact Profiles establish contact information that can be assigned to User Groups, Administrators, the Subnet Profile, and the Object Profile.

The **User-Defined Fields** function allows you to define custom fields for Domains, Objects, Organizations, Subnets, Reverse Zones, Users, and Address Allocation.

Manufacturer Profiles

Setting up a list of manufacturers for an object class enables VitalQIP to provide the prefix for the Manufacturer's MAC address automatically when IP addresses are assigned. There is a predefined list of manufacturers for each object class.

Optionally, manufacturers' models have tag names and values associated with them. Tag values are the specific Bootp tags for the manufacturer's equipment.

Add a new manufacturer

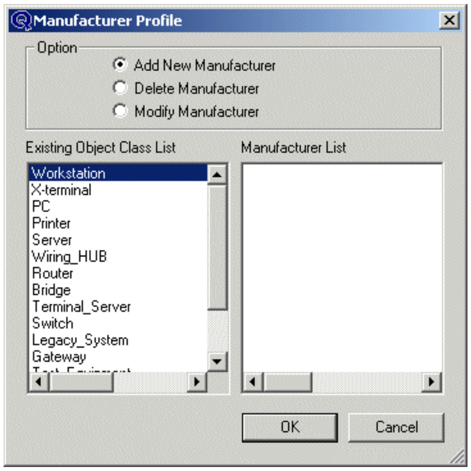
Purpose

Use this procedure to add a new manufacturer.

Procedure

To add a new manufacturer, follow these steps:

1 Select **Manufacturer Profiles** from the **Policies** menu. The Manufacturer Profile window opens.



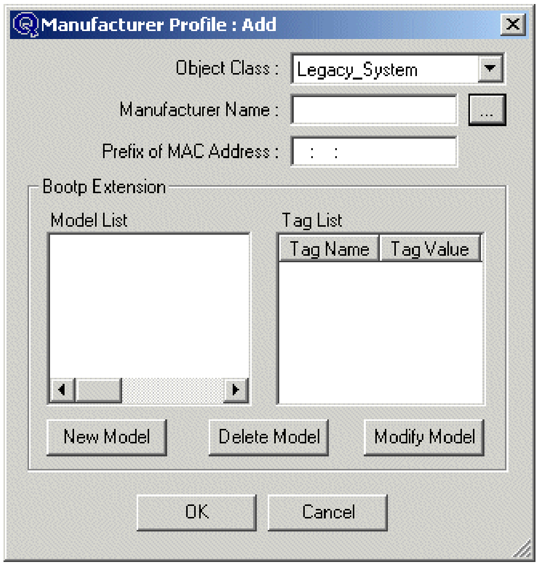
Manufacturer Profile

Option
● Add New Manufacturer
○ Delete Manufacturer
○ Modify Manufacturer

Existing Object Class List:
Workstation
X-terminal
PC
Printer
Server
Wiring_HUB
Router
Bridge
Terminal_Server
Switch
Legacy_System
Gateway
Test_Equipment

Manufacturer List:

2 Since the **Add New Manufacturer** option button is selected by default, click **OK**. The Manufacturer Profile: Add window opens.



Manufacturer Profile : Add

Object Class : Legacy_System

Manufacturer Name :

Prefix of MAC Address : : :

3 Select an object from the **Object Class** list.

4 Enter the **Manufacturer Name** or click **...** to access a listing of default manufacturers and select one from the list.

5 Enter the **Prefix of MAC Address**.

6 Unless you want to add a model name and tag information for Bootp Extension purposes, click **OK**. A confirmation dialog box opens.

7 Click **OK** to save the Manufacture Profile.

END OF STEPS

Apply a model name to a manufacturer

Purpose

Use this procedure to apply a model name to a manufacturer.

Before you begin

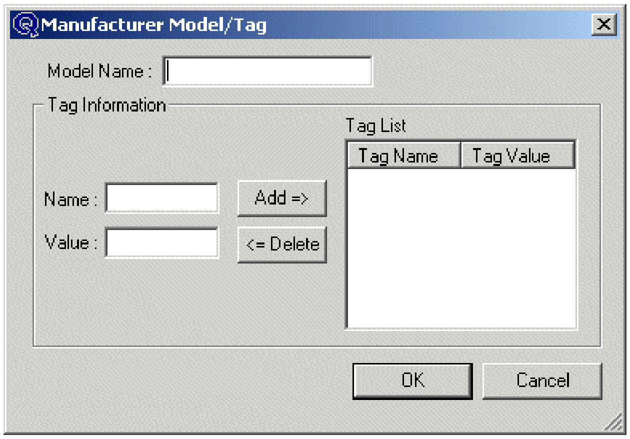
- Tags are the specific Bootp tags for the manufacturer's equipment. There may be a different tag value associated with each model, or the vendor may use one tag for all the equipment it manufactures.
- Tag fields are Bootp parameter identifiers. They are normally two characters long, and generally begin with "T". Their names are selected by the vendor.
- The default **Model Name** is "all" (case insensitive). This means that VitalQIP uses the manufacturer's standard tag value (thereby ignoring the model name). If you specify a model name, however, VitalQIP only uses the tag value for that model (while generating Bootp entries for an object) when selected in the Object Profile window. For example, if the tag field name is "bf", then whenever an object is associated with this manufacturer and model, the default value in the Object Profile window is "bf".

Procedure

To add a model name and tag to a manufacturer profile, follow these steps:

Note: This applies to Bootp Extensions only.

1 If you want to apply a Model Name to a manufacturer, click **New Model** in the Manufacture Profile: Add or Manufacture Profile: Modify window. The Manufacturer Model/Tag window opens.



2 Enter a **Model Name**.

3 Assign a **Name** and **Value** to the model and click **Add**. The tag name and tag value appear in the **Tag List**.

4 Click **OK** and the Bootp Extension information is displayed in the Manufacturer Profile window.

END OF STEPS

Change the manufacturer profile

Purpose

Use this procedure to change a manufacturer profile.

Procedure

To change a manufacturer's name, MAC prefix, or model information, follow these steps:

1 In the Manufacturer Profile window, select the object class from the **Existing Object Class List** and then the associated manufacturer in the **Manufacturer List**.

2 Click **OK**. The Manufacturer Profile: Modify window opens.

3 You can modify the MAC address prefix for an object class, the model/tag settings for a model, and/or the manufacturer name.   You can also delete a model name.

4 When you have finished modifying this manufacturer, click **OK**. A Warning dialog box opens.

5 Click **Yes** to save your changes.

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

END OF STEPS

Delete a manufacturer profile

Purpose

Use this procedure to delete a manufacturer profile.

Procedure

To delete a manufacturer profile, follow these steps:

1 In the Manufacturer Profile window, click **Delete Manufacturer**.

2 Select the object class from the **Existing Object Class List** and then select the manufacturer you want to delete from the **Manufacturer List**.

3 Click **OK** and the Manufacturer Profile: Delete window opens.

4 Verify that you wish to delete the selected manufacturer and click **OK**. A Warning dialog box opens.

5 Click **Yes** to delete the manufacturer.

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

END OF STEPS

Manage location profiles

Purpose

The **Location Profiles** function allows you to provide information on street addresses and/or cities, which can then be associated with Object Profiles, Subnet Profiles, and User Profiles in case you want to record the physical location of these entities.

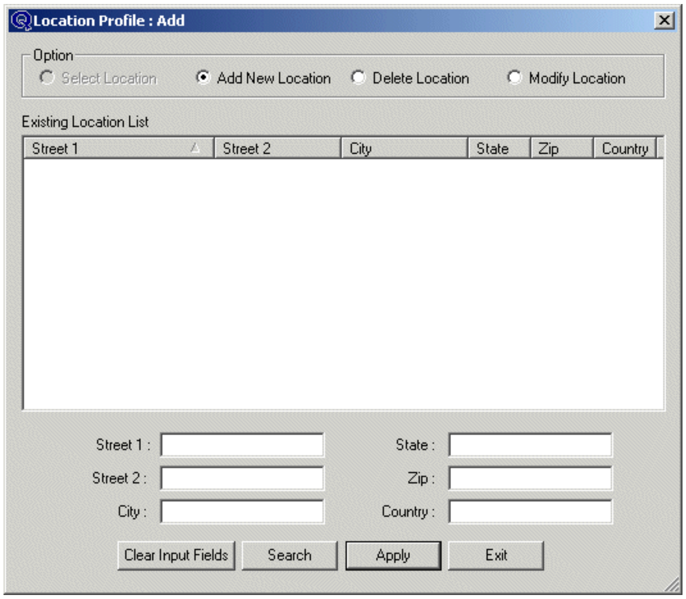
Before you begin

- You can sort the listing by clicking on the columns at the top of the listing.
- **Select Location** is enabled only when you access the Location Profile from other windows, such as the User Profile. It enables you to select from the list and apply the Location Profile information to a user, object, or subnet.
- The **Location Search** policy (page 34) determines whether location data initially appears in the **Existing Location List**. If the policy is set to True, no locations are listed until the search criteria are entered.

Procedure

To establish the Location Profile, follow these steps:

1 Select **Location Profiles** from the **Policies** menu. The Location Profile window opens.



Location Profile : Add

Option: ○ Select Location ● Add New Location ○ Delete Location ○ Modify Location

2 To add a new location, select the **Add New Location** option, and enter new information in the fields at the bottom of the window (if you need to clear the input/search fields first, click **Clear Input Fields**). Click **Apply** to add the new location to the **Existing Location List**.

3 To search for type specific locations, input search information into the input fields in the bottom of the window, and click **Search**. You can search on any or all fields. This type of search is a “begins with” search and does not require a wildcard. In other words, if you input “10” in the Street1 field, every address that begins with “10” will be returned (for example, 10 Valley Stream, 1010 Main Street, and so on). The list opens in the window.

4 To modify a location, highlight the location in the list, click the **Modify Location** option, modify the information in the fields at the bottom of the list, and then click **Apply**.

5 To delete a location, highlight the location in the list, select the **Delete Location** option, and click **Apply**. A confirmation dialog box opens. Click **Yes** if you are sure you want to delete this location. Deleting a location deletes it from any object in the database.

6 Once you have completed adding to, modifying or deleting from the list, click **Exit** to return to the main menu.

END OF STEPS

Manage contact profiles

The **Contact Profiles** function allows you to define information about names, phone numbers, and e-mail addresses of people, so that you can associate User Groups, Administrators, Subnets and Objects with these people if you wish.

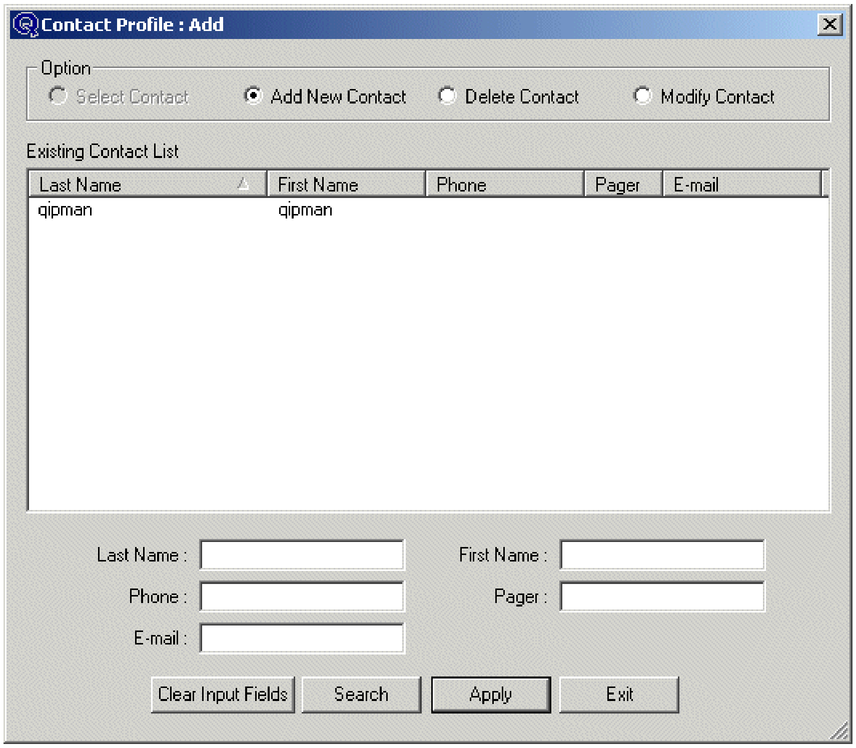
Before you begin

- You can sort the **Existing Contact List** by clicking on a column title.
- **Select Contact** is enabled only when you access the Contact Profile from other windows, such as the User Group Profile. It enables you to select from the list and apply it to a User Group, Administrator Profile, Object Profile, or Subnet Profile.
- The `Contact Search` policy (refer to page 31) determines whether contact data initially appears in the **Existing Contact List** when the window is opened. If the policy is set to True, no contacts are listed until the search criteria are entered.

Procedure

To establish a Contact Profile, follow these steps:

1 Select **Contact Profiles** from the **Policies** menu. The Contact Profile window opens.



Contact Profile : Add

Option

○ Select Contact ● Add New Contact ○ Delete Contact ○ Modify Contact

Existing Contact List

Last Name	First Name	Phone	Pager	E-mail
qipman	qipman			

Last Name :		First Name :	
Phone :		Pager :	
E-mail :			

2 To add a new contact, click **Add New Contact,** and enter new information in the fields at the bottom of the window. Click **Apply** to add the new contact to the **Existing Contacts List**.

> **Note:** You cannot create a contact profile where the first and last names are the same as an existing contact. The last and first names must be unique to ensure administrators cannot modify or delete wrong contact.

3 **Clear Input Fields** clears all the fields at the bottom of the window.

4 To search for specific contacts, type search information into the input fields in the bottom of the window, and click **Search**. You can only search on Last Name and/or First Name. This type of search is a “begins with” search and does not require a wildcard. In other words, if you input “John” in the First Name field, every contact that has the first name “John” will be returned (for example, John Smith, John Brown, and so on). The list opens in the window. Note that the search is case sensitive.

5 To modify a contact, highlight the contact in the list, click **Modify Contact**, and modify the information in the fields at the bottom of the list. Click **Apply** to save your changes.

6 To delete a contact, highlight the contact in the list, select **Delete Contact**, and click **Apply**. A confirmation window opens. Click **Yes** if you are sure that you want to delete this contact. Deleting a contact deletes it wherever it is used in the system (for example, the Object Profile).

7 Once you have completed adding, modifying, or deleting contacts from the list, click **Exit** to return to the main menu.

END OF STEPS

User-defined fields

User-Defined Fields (UDFs) can be established for Users, Subnets, Objects, Organizations, Domains, or Reverse Zones. Additionally, you can add UDFs for use with the web client, where you can perform address management activities. Once they are set up through the **User-Defined Fields** window, they are accessible in the Object Profile, the Subnet Profile, the User Profile, the Organization Profile, the Domain Profile, and the Reverse Zone Profile.

For example, if you wish to track users' Social Security Numbers and Mobile Phone Numbers in the User Profile, you would add those fields in the User-Defined Fields window. When you later open the User Profile, these fields would be accessible under the User-Defined Fields tab to enter data.

All such User-Defined fields may be searched for with the **Management|GoTo/Search** function. Refer to "Go to/search function" (p. 1-42).

A few things to keep in mind

- If you delete a User-Defined Field, all references to that field throughout the database are deleted.
- Only Master-level administrators can create User-Defined Fields for Organizations. If the administrator is not a Master-level administrator, the "Organization" Type will not be shown in the drop-down list.
- Since all organizations have the same User-Defined Fields, all administrators will be adding/modifying/deleting the same list.

Create a user-defined field

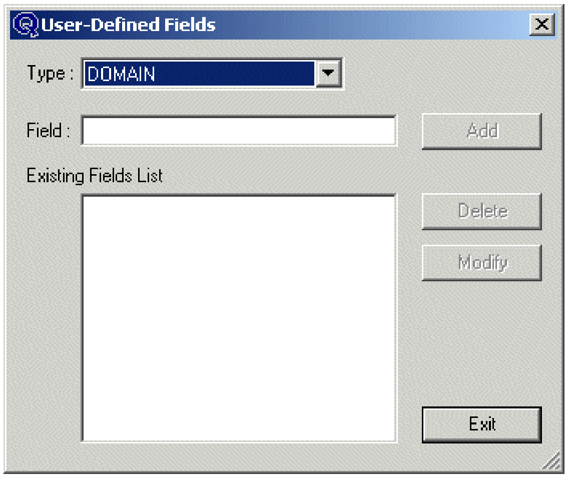
Purpose

Use this procedure to create a user-defined field.

Procedure

To define a user-defined field, follow these steps:

1 Select **User-Defined Fields** from **Policies** menu. The User-Defined Fields window opens.



User-Defined Fields

Type : DOMAIN

Field :

2 Select the field type (such as Domain, Object, Subnet, or User) from the **Type** field.

3 Enter a field name (of up to 30 characters) in the **Field** field.

4 Click **Add**. The new field appears in the **Existing Fields List**.

5 Click **Exit** to close the User-Defined Fields window.

END OF STEPS

Modify a user-defined field

Purpose

Use this procedure to modify a user-defined field.

Procedure

To modify a User-Defined Field, follow these steps:

1 Highlight the field you wish to edit in the **Existing Fields List**.

2 When it appears in the **Field** field, change the text as desired.

3 Click **Modify**. The modified field appears in the **Existing Fields List**.

4 Click **Exit** to close the User-Defined Fields window.

END OF STEPS

Delete a user-defined field

Purpose

Use this procedure to delete a user-defined field.

Procedure

To delete a User-Defined Field, follow these steps:

1 Highlight the field you wish to delete in the **Existing Fields List**.

2 Click **Delete**. A confirmation dialog box opens.

3 Click **Yes**.

4 Click **OK** when VitalQIP confirms that the User-Defined Field is deleted.

END OF STEPS

Object classes

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 then be better able to identify the fields in which they have to enter appropriate information.

The naming policy created in the Object Classes screen will be 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.

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

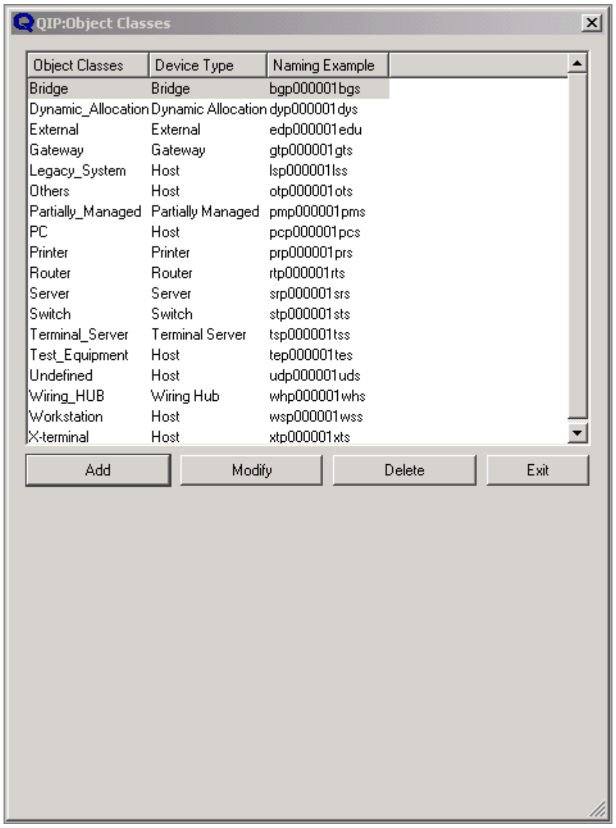
Purpose

Use this procedure to create a new object class.

Procedure

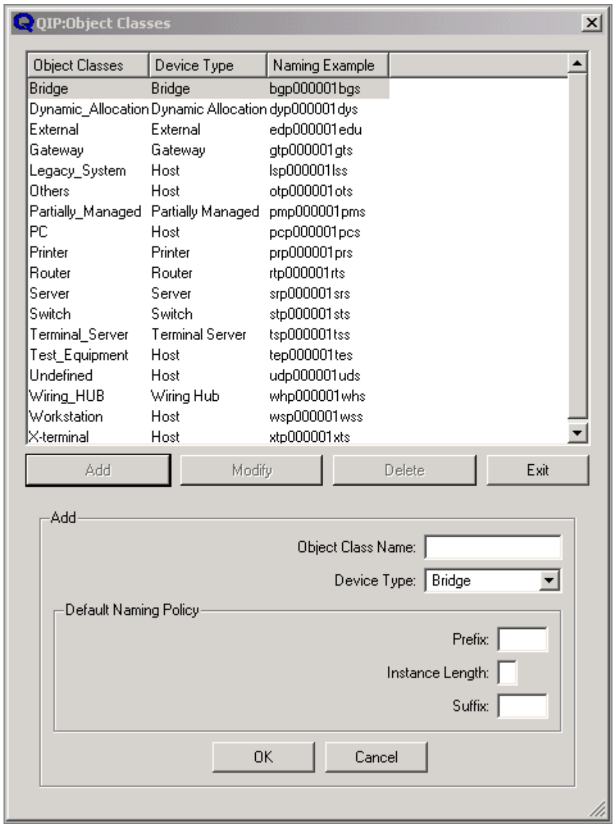
To create an object class, follow these steps:

1 Select **Object Classes** from **Policies** menu. The Object Classes window opens.



Object Classes	Device Type	Naming Example
Bridge	Bridge	bgp000001bgs
Dynamic_Allocation	Dynamic Allocation	dyp000001dys
External	External	edp000001edu
Gateway	Gateway	gtp000001gts
Legacy_System	Host	lsp000001lss
Others	Host	otp000001ots
Partially_Managed	Partially Managed	pmp000001pms
PC	Host	pcp000001pcs
Printer	Printer	prp000001prs
Router	Router	rtp000001rts
Server	Server	srp000001srs
Switch	Switch	stp000001sts
Terminal_Server	Terminal Server	tsp000001tss
Test_Equipment	Host	tep000001tes
Undefined	Host	udp000001uds
Wiring_HUB	Wiring Hub	whp000001whs
Workstation	Host	wsp000001wss
X-terminal	Host	xtp000001xts

2 To add an object class, click **Add**. Add fields appear at the bottom of the window.



Object Classes	Device Type	Naming Example
Bridge	Bridge	bgp000001bgs
Dynamic_Allocation	Dynamic Allocation	dyp000001dys
External	External	edp000001edu
Gateway	Gateway	gtp000001gts
Legacy_System	Host	lsp000001lss
Others	Host	otp000001ots
Partially_Managed	Partially Managed	pmp000001pms
PC	Host	pcp000001pcs
Printer	Printer	prp000001prs
Router	Router	rtp000001rts
Server	Server	srp000001srs
Switch	Switch	stp000001sts
Terminal_Server	Terminal Server	tsp000001tss
Test_Equipment	Host	tep000001tes
Undefined	Host	udp000001uds
Wiring_HUB	Wiring Hub	whp000001whs
Workstation	Host	wsp000001wss
X-terminal	Host	xtp000001xts

Object Class Name:

Device Type: Bridge

Prefix:

Instance Length:

Suffix:

3 Enter an **Object Class Name** of up to 20 characters. Valid characters are alphanumeric, spaces, underscores and dashes.

4 Select a device type from the **Device Type** list:

- Bridge
- Gateway
- Host
- Printer
- Router
- Server
- Switch
- Terminal Server
- Wiring HUB

5 Enter a **Prefix** of 3 alphanumeric characters.

6 Enter an **Instance Length** from 0 to 8 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.

> **Note:** The Instance Length for an object class with a Dynamic Allocation device type cannot be less than 4 characters.

7 Enter a **Suffix** of 3 alphanumeric characters.

8 Click **OK** to save.

END OF STEPS

Modify an object class

Purpose

Use this procedure 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 **Policies** menu. The Object Classes window opens.

2 Select the object class you wish to change and click **Modify**. The fields you can modify appear at the bottom of the Object Classes window.

3 Make the desired changes and click **OK** to save them.

END OF STEPS

Delete an object class

Purpose

Use this procedure 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 **Policies** menu. The Object Classes window opens.

2 Select the object class you wish to delete and click **Delete**. A confirmation prompt appears in the Object Classes window.

3 Click **OK** to delete the object class you no longer want.

END OF STEPS

4 Manage servers

Overview

Purpose

The purpose is to describe how to set up your servers in VitalQIP. It also contains information on how Local Host, Windows Domain Controller, NIS, Bootp, DNS and DHCP servers operate, and the various types of DNS and DHCP servers that are supported by VitalQIP. Information is also provided on managing Global MAC address pools for DHCP servers and non-managed DNS servers.

Contents

The following topics are covered:

Servers	4-3
Add a server	4-4
Modify a server profile	4-8
Delete a server profile	4-9
Enter email addresses	4-10
DHCP and Bootp servers	4-11
Lucent DHCP server configuration files	4-11
Client Naming Policy	4-13
VitalQIP interface	4-14
Start and stop the DHCP Service/VitalQIP Update Service	4-16
Bootp server type	4-17
Lucent DHCP 5.4, Lucent DHCP 5.5, and Lucent DHCP 5.6 server types	4-19
Support for DHCP failover server	4-24

Configuration of failover parameters on primary DHCP server	4-26
Configuration of dhcpd.pcy on failover DHCP server	4-30
Windows 2003 DHCP server type	4-33
Global MAC address pools	4-37
Define global MAC address pools	4-38
DNS servers	4-41
DNS configuration and data files	4-41
WINS gateway support	4-42
Remote DNS servers	4-43
NIS, OS Files, and the domain	4-44
BIND-9 DNS server type	4-45
LUCENT DNS 4.X server type	4-51
Windows 2003 DNS server type	4-56
NIS server type	4-62
LOCAL HOST server type	4-64
Windows 2003 Domain Controller server type	4-66
Non-managed DNS servers	4-68
Define a non-managed DNS server	4-69
Establish zone options	4-73
Modify a non-managed server	4-75
Delete a non-managed server	4-76

Servers

This section describes how to set up your servers in VitalQIP. It also contains information on how Local Host, Windows Domain Controller, NIS, Bootp, DNS and DHCP servers operate, and the various types of DNS and DHCP servers that are supported by VitalQIP.

Servers can be defined as Bootp, DHCP, DNS, NIS, Windows Domain Controller, or Local Host within VitalQIP. You can configure your DNS server first, but you are required to define and configure your domain in the process.

If your network includes Bootp, DHCP, DNS, NIS, Windows Domain Controller, or Local Host 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 Bootp, DHCP, DNS, NIS and/or Local Host data 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. For more detailed information on the File Generation Service, refer to Chapter 8, "Network services".

The VitalQIP Remote Service (**qip-rmtd**) must be loaded and running on the remote BOOTP, DHCP, DNS, NIS or Local Host 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 (**qip-rmisched**) 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 server

Purpose

Use this procedure to add create a server profile.

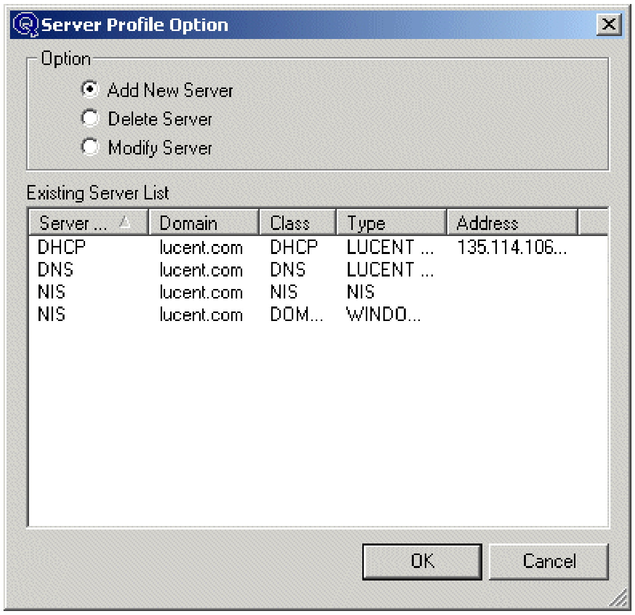
Before you begin

When you select the **Server Class** of BOOTP, DHCP, NIS, or LOCAL_HOST, 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 "Customize administrator menus" (p. 6-30).

Procedure

To set up a server, follow these steps:

1 Select **Server** from the **Infrastructure** menu. The Server Profile Option window opens.



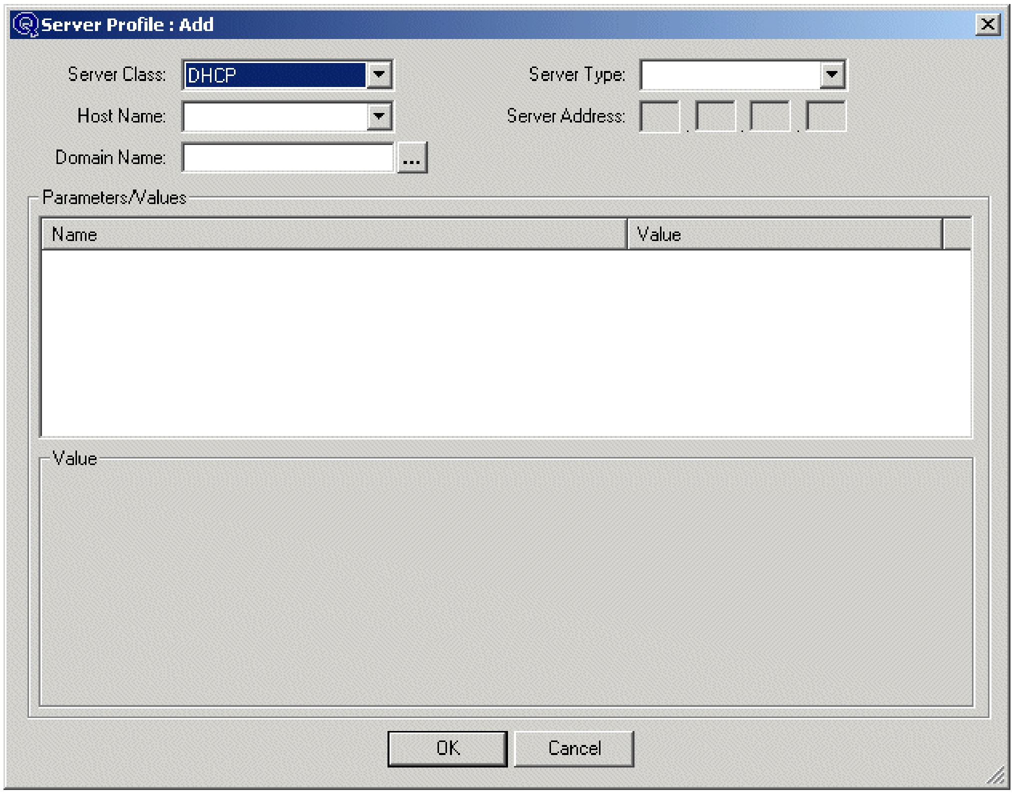
Option

● Add New Server
○ Delete Server
○ Modify Server

Existing Server List

Server ...	Domain	Class	Type	Address
DHCP	lucent.com	DHCP	LUCENT ...	135.114.106...
DNS	lucent.com	DNS	LUCENT ...	
NIS	lucent.com	NIS	NIS	
NIS	lucent.com	DOM...	WINDO...	

2 Click **OK** (since **Add New Server** is the default). The Server Profile: Add window opens.



Server Class: DHCP

3 Select a server class from the **Server Class** drop-down list.

4 Select a server type from the **Server Type** drop-down list in the following table.

Note: There are several server types shown in the Server Type drop-down list that are no longer supported. VitalQIP allows you to import the server types but you cannot manage the servers in VitalQIP. You can change the server type in the Server Profile. The following server types are no longer supported:

- IBM AIX DHCP
- IBM NT DHCP
- MS NT 4.0 DHCP
- BIND 4.9.x DNS
- MICROSOFT-NT4.0

Table 4-1 Server classes and server types

Server class	Server type	Parameter tables
BOOTP	BOOTP	Table 4-2, “Bootp parameters” (p. 4-17)
DHCP	LUCENT DHCP 5.4	Table 4-3, “Lucent server parameters” (p. 4-19)
	LUCENT DHCP 5.5	Table 4-3, “Lucent server parameters” (p. 4-19)
	LUCENT DHCP 5.6	Table 4-3, “Lucent server parameters” (p. 4-19)
	Windows 2003 DHCP	Table 4-6, “Windows 2003 DHCP parameters” (p. 4-33)
DNS	BIND-9.X	Table 4-9, “DNS BIND-9 parameters” (p. 4-45)
	LUCENT DNS 4.X	Table 4-10, “LUCENT DNS 4.X parameters” (p. 4-51)
	Windows 2003 DNS	Table 4-11, “Windows 2003 DNS parameters” (p. 4-56)
NIS	NIS	Table 4-12, “NIS parameters” (p. 4-62)
LOCAL_HOST	LOCAL HOST	Table 4-13, “Local parameters” (p. 4-64)
DOMAIN CONTROLLER	Windows 2003 DC	Table 4-14, “Windows 2003 Domain Controller parameters” (p. 4-66)

5 In the **Host Name** field, either select a server name from the existing host list, or enter a new server host name. You can enter a maximum of 63 alphanumeric characters beginning with an alphanumeric. The host name may include the dash (-) and underscore (_) characters, but cannot contain plus signs (+) or exclamation marks (!).

6 Enter a domain in the **Domain Name** field by clicking on **...** to open the Domain Option: Select window and select a domain from the **Existing Domain List**.

Alternatively, if you have not yet set up a domain:

a. Select the **Add New Domain** option and enter a **Domain Name** and **Zone E-mail Address** in the Domain Profile: Add window.

b. Click **OK** to save the domain profile and answer **Yes** to the “`This domain has not been assigned a DNS Server. Continue?`” warning prompt. (You can add a DNS server at a later time.)

c. Click **OK** at the confirmation prompt and the new domain name appears in the **Domain Name** field in the Server Profile: Add window.

7 Once the Server Type is selected (step 4 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**.

8 Click **OK** and the Server Profile window closes as the profile is saved.

END OF STEPS

Modify a server profile

Purpose

Use this procedure to modify a server profile.

Procedure

To modify an existing server, follow these steps:

1. Select **Server** from the **Infrastructure** menu and when the Server Profile Option window appears, select the **Modify Server** option.

2. Select the server you wish to modify in the **Existing Server List** and click **OK** (or just double-click on the server name). The Server Profile: Modify window opens.

3. Modify it as necessary and click **OK** to save your changes. A warning prompt opens.

4. Click **Yes**. A confirmation dialog box opens.

5. Click **OK**.

END OF STEPS

Delete a server profile

Purpose

Use this procedure to delete a server profile

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.

DNS servers cannot be deleted if they are authoritative for any domain or reverse zone. Such servers are identified as “master” in the *named.conf* file.

Procedure

To delete an existing server, follow these steps:

1 Select **Server** from the **Infrastructure** menu and when the Server Profile Option window appears, select the **Delete Server** option.

2 Select the server you wish to delete in the **Existing Server List** and click **OK** (or just double-click on the server name). The Server Profile: Delete window opens.

3 Click **OK** to delete the server profile. A warning prompt opens.

4 Click **Yes**. A confirmation prompt opens.

5 Click **OK**.

END OF STEPS

Enter email addresses

Purpose

Use this procedure to enter email addresses. The email address in profiles for server, domain, and reverse zone is written to the DNS configuration files and must be entered according to a specific format.

Procedure

To enter an email address, follow these steps:

1 If the email address contains the @ character, the text following the @ character must contain at least one period separating the two domain segments(for example, myname@lucent.com). The text following the @ sign (in this example “lucent.com”) can only use letters a-z (capped or lower case), numbers 0-9 and the dash (-) character. Also, the first and last characters of the text following the @ cannot be a dash.

2 If the email address contains the @ character, the text preceding the @ is not validated, but must be at least one character in length.

3 If the email address does not contain the @ character, the entire field can only use letters a-z (capped or lower case), numbers 0-9 and the dash (-) character. Also, the first and last characters of the text cannot be a dash.

Following these formatting rules allows the email addresses to be processed correctly when you are generating DNS configuration files within VitalQIP.

END OF STEPS

DHCP and Bootp servers

Bootp and DHCP are protocols that automatically assign IP addresses and configure the operating environment of devices represented by objects in VitalQIP. Servers can be defined as Bootp, DHCP, or both, and 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 Bootp and/or DHCP methodology.

VitalQIP supports the Lucent DHCP server on the Windows 2003, Solaris, and Linux platforms. It optionally supports dynamic updates to all authoritative DNS servers. The DHCP service supports specific Bootp and DHCP parameters. Establishment of DHCP servers occurs during the installation of VitalQIP. The configuration files used by the DHCP server are created via **Network Services|DHCP Generation|Server**. These files reside on the 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. Information on setting up server templates is described in "DHCP policy templates" (p. 2-63). 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.

The DNS Server 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: A VitalQIP Command Line Interface 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.

  Note: 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. However, if the user moves the computer and connects to a different subnet, the user gets a new IP address but the same hostname, and the VitalQIP database will see these as duplicate hostnames. 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.

Note: To configure the FIRST_IN/LAST_IN host naming support for Lucent DHCP servers, set , 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

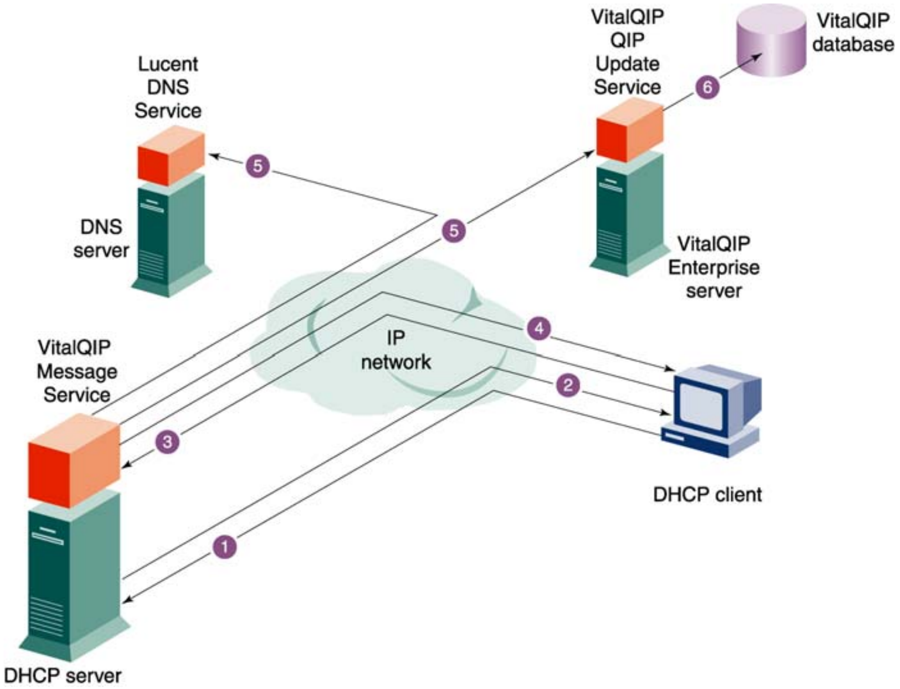
IP Manage and **qip-dhcpgen** (the command line equivalent of the **DHCP Generation** function on the **Network Services** menu) can create the *dhcpd.conf* and *dhcpd.pcy* files, and signal the DHCP server to reread its configuration and policy information. The VitalQIP Remote Service (**qip-rmtd**) 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 4-1 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.

Start and stop the DHCP Service/VitalQIP Update Service

To start the DHCP server and all associated services, refer to the *Administrator Reference Manual*.

> **Note:** The VitalQIP QIP Update Service (**`qip-qipupdated`**) attempts to read a policy file named *qip.pcy*. This file contains debug parameters for the QIP Update Service. This file is created at installation time, but you must update the file to enable debugging on the Update Service. You must modify this file manually if you want to run the QIP Update Service in debug mode. Refer to the *Administrator Reference Manual* for more information on the VitalQIP QIP Update Service.

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 server templates (in the **DHCP/Bootp Template|Policy Template** function on the **Policies** menu - refer to "DHCP server policies" (p. 2-71)) 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)/A-DHCP (Automatic 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 while running **DHCP Generation** on the **Network Services** menu.

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*.

Bootp server type

The following table shows the parameters for the Bootp server type. Items in **bold** in the Options column of the table are defaults.

Table 4-2 Bootp 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 Bootp 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.
Bootptab Filename	Text		The full path and *bootptab* file name. If the path is not included, the file is generated in the *QIP/etc* directory.
Scheduled Automatic Updates	Time Interval or Timeof 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 time).
Bootfile Home Directory	Text		Enter the home directory for the bootfile images, relative to the TFTP Root directory. This is the directory where the boot image file of an object is found.

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 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.
Send Client's Hostname	Boolean	True or **False**	Selecting True causes the client's hostname to be sent in the Bootp reply packet.
TFTP Root Directory	Text		***Required***. Enter the root directory for the server. If you use this, VitalQIP will inform Bootp of this special root directory used by secure TFTP. If you set this field to blank (NULL), the tag “td” will not be generated in the global.qip record in the *bootptab* file.
Vendor Magic Cookie (vm)	Selection	(**Auto**, CMU, RFC1048, RFC1084)	The vendor cookie for this Bootp server.

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 4-3 Lucent server 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		***Required***. Configuration files are created in this directory. On Windows-based systems, this includes the drive letter, (for example, *c:\qip\dhcp*).
DHCP Template	Text	Select From List	Select a DHCP template for this server.

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	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*.

Parameters	**Value type**	**Options**	**Usage**
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. 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	Boolean, Sub-parameters	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 4-4, “Failover parameters for the primary DHCP server” (p. 4-27) 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.

Parameters	Value type	Options	Usage
Support Bootp	Boolean	**True** or False	Select True to have this server support 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).
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. 2-71). When set to True, select a **Server Policy Template** from the list.

Support for DHCP failover server

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. 4-26) 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 operating 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.

A few things to keep in mind

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 10.200.50.0/255.255.255.0 subnet, and primary B server is managing addresses 101-

200 on the same subnet (10.200.50.0/255.255.255.0). 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.
- 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.

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 (as described in Chapter 8, “Network services”). The additions to the *dhcpd.pcy* file to accommodate DHCP failover are discussed in this section.

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.

> **Note:** 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 4-4 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.

Parameter name	**Value type**	**Default value**	**Description**
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.
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.

Parameter name	**Value type**	**Default value**	**Description**
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. Other *dhcpd.pcy* policies are discussed in "DHCP server policies" (p. 2-71).

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:** Please 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 4-5 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.

Parameter name	Value type	Default value	Description
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.
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.

Parameter name	Value type	Default value	Description
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 must exist for each failover server. Each primary server is defined 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
```

Windows 2003 DHCP server 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 4-6 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.

Parameters	Value type	Options	Usage
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 2003 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	Text	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.

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 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.

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 "Registered Clients Only" flag 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 "DHCP server policies" (p. 2-71).

Define global MAC address pools

Purpose

Use this procedure to define global MAC address pools.

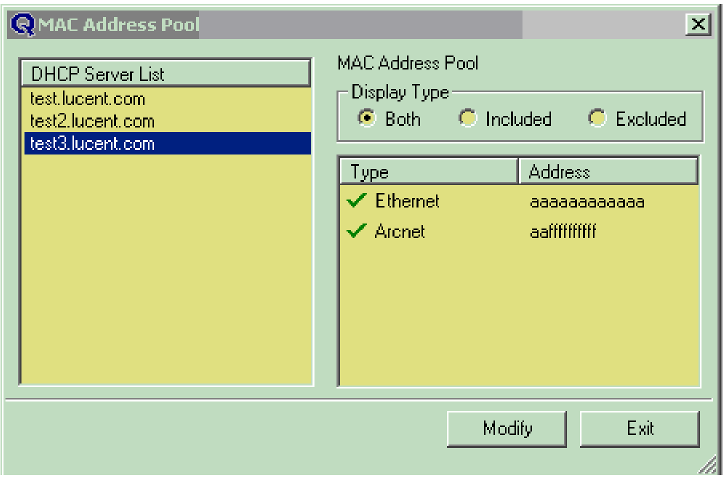
Before you begin

- 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 **Global MAC Address Pool** from the **Management** option of the VitalQIP main menu. The MAC Address Pool window opens.



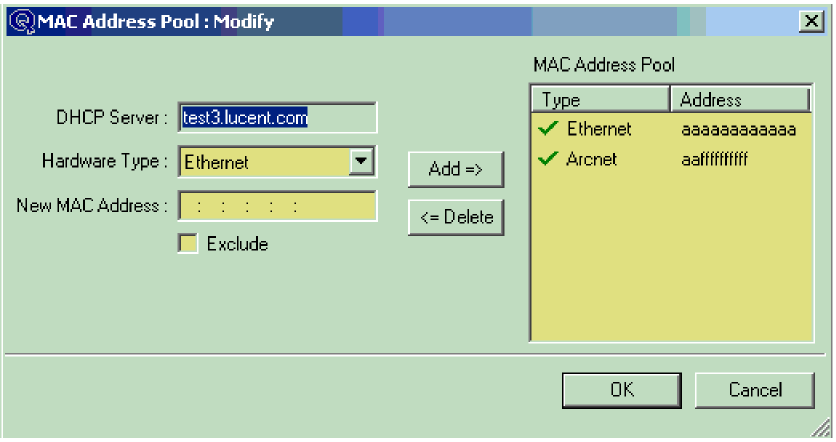
DHCP Server List
test.lucent.com
test2.lucent.com
test3.lucent.com

MAC Address Pool

Display Type: ● Both ○ Included ○ Excluded

Type	Address
✓ Ethernet	aaaaaaaaaaaa
✓ Arcnet	aaffffffffff

2 Select the DHCP server and click **Modify**. The MAC Address Pool: Modify window opens.



MAC Address Pool : Modify

DHCP Server : test3.lucent.com

Hardware Type : Ethernet

New MAC Address : : : : : :

□ Exclude

MAC Address Pool

Type	Address
✓ Ethernet	aaaaaaaaaaaa
✓ Arcnet	aaffffffffff

3 To add a MAC address to a DHCP server, select the hardware type from the **Hardware Type** drop-down list.

4 Enter a MAC address in the **New MAC Address** field.

5 To include a MAC address from the pool, leave the **Exclude** check box unchecked. Otherwise, place a check to exclude the address from the pool.

6 Click **Add** and the MAC address is added to the **MAC Address Pool** list for the selected DHCP server.

7 To unassign a MAC address from the selected DHCP server, select it from the **MAC Address Pool** list and click **Delete**.

8 Click **OK** to save your changes.

9 Click **Exit** to close the MAC Address Pool window.

END OF STEPS

DNS servers

To set up your DNS servers, you establish the name server configuration files with various BIND options. The domain name "**.**" in the configuration files refers to the root domain and, by definition, all DNS servers have access to this "spatial domain".

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. For information on how to do this, refer to "DNS generation" (p. 8-15).

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 Network Services, VitalQIP uses temporary space in the *%QIPHOME%\tmp* directory of the target system. You need to ensure that you have enough *%QIPHOME%\tmp* 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.

WINS gateway support

VitalQIP supports an interface with the Microsoft WINS (Windows Internet Naming Service) within versions of Lucent DNS described in the following table. The purpose of the WINS forwarding is to allow a WINS server to resolve hostnames that DNS cannot resolve, and to allow NetBIOS calls to resolve IP addresses that DNS cannot resolve. This works with either UNIX or Windows DNS servers. Features include:

- Can optionally be turned on and off
- Forwards name requests to WINS server(s)
- Forwards IP address requests to NetBIOS clients
- Can be configured to support multiple WINS servers
- Can optionally cache results within DNS

Table 4-7 WINS forwarding in Lucent DNS

Version	BIND version	Usage
Lucent DNS 3.1	BIND 8.X	WINS forwarding is configured at the domain level, in the **zone block of named.conf** opens on the Domain Profile **Zone Options** tab.
Lucent DNS 4.0	BIND 9.X	*WINS forwarding is not supported.*

Refer to the *Administrator Reference Manual* for the correct syntax and more details of how to implement WINS forwarding in BIND 8.X.

Note: The Lucent DNS version is independent of the version of VitalQIP that you are using. You may replace the *named.exe*, *named*, or *in.named* executable to change the DNS version.

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.

The following table describes the VitalQIP services that must be running on a remote DDNS/DNS server.

Table 4-8 VitalQIP services

Service	What does it do?
VitalQIP Remote Service	Transfers DDNS/DNS files from the VitalQIP Server to Remote Servers.
VitalQIP Domain Name Service	Provides Domain Name Services to the network.
VitalQIP Message Service	Queues messages and forwards them to other services.

NIS, OS Files, and the domain

Network Information Service (NIS) takes the OS files (hosts, netmasks, and ethers), converts them into NIS maps, and provides the ability to distribute these maps to other (primary and/or secondary) NIS servers. The OS files are placed in a user-specified directory through the definition of the NIS server (**Infrastructure|S1erver** option). Each file contains object-specific information for that domain. The following is the format for each file:

/etc/hosts	**(host name**		
IP-Address	Official-Name	Fully-qualified-hostname	hostname Aliases
98.200.153.5	annika	annika.qtek.com	dns_srv nis_srv

etc/netmasks	**(network mask database)**
Network Address	Network Mask
198.200.153.0	255.255.255.0

/etc/ethers	**(Ethernet address to hostname)**
MAC-Address	Official-hostname
00:60:97:ce:f4:40	qaxp02

The network name database (*/etc/networks*) is not supported by VitalQIP because VitalQIP currently does not associate names with the network.

For example, consider the server “server1” managing the following domains:

```
qtek.com
dev.qtek.com
sales.qtek.com
qip.sales.qtek.com
```

VitalQIP creates the following domain-specific directories and OS files:

```
/var/etc/qtek.comhosts, netmasks and ethers
/var/etc/dev.qtek.comhosts, netmasks and ethers
/var/etc/sales.qtek.comhosts, netmasks and ethers
/var/etc/qip.sales.qtek.comhosts, netmasks and ethers
```

Note: The files above are located in */var/etc*, which is not the default location.

VitalQIP does not execute **ypinit**, **ypserv**, or **ypxfrd** for the system. These functions are assigned to the system administrator of the server because there are other maps the administrator has to consider, such as security.

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 4-9 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. **Note:** 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		This is the mail address that appears in the SOA record of a zone file. Refer to “Enter email addresses” (p. 4-10) for formatting requirements.
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.

Parameters	**Value type**	**Options**	**Usage**
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*). **Note:** This parameter defaults to False on existing Bind 9 servers that have been upgraded from previous VitalQIP releases.
DNSSEC enabled server	Boolean	True, False	When the parameter is set to **True** and the userexit configured, a DNS push **Network Services | DNS Generation** function to the DNSSEC enabled server signs the zones of the DNSSEC enabled server using configured keys. All DNSSEC enabled zones, which have the server being pushed to the primary server, are secured with DNSSEC.

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 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. The files are created in a background (batch) mode, then transferred to each server; conf files are generated for all servers. Zone files are generated for primary servers only. For automatic updates of DNS to take effect, an IP address must have been assigned to each domain's primary server. This is achieved through the **Object Management** function. If this parameter is set to None, administrators can manually request VitalQIP to compile 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 **Network Services|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 **Network Services|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 **Network Services|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**	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.

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.

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 4-10 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		This is the mail address that appears in the SOA record of a zone file. Refer to "Enter email addresses" on page 10 for formatting requirements.
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*). **Note:** This parameter defaults to False on existing Lucent DNS 4.X servers that have been upgraded from previous VitalQIP releases.

Parameters	Value type	Options	Usage
DNSSEC enabled server	Boolean	True, False	When the parameter is set to **True** and the userexit configured, a DNS push **Network Services | DNS Generation** function to the DNSSEC enabled server signs the zones of the DNSSEC enabled server using configured keys. All DNSSEC enabled zones, which have the server being pushed to the primary server, are secured with DNSSEC.
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.

Parameters	**Value type**	**Options**	**Usage**
Allow-Secondary-Update	No, Use Server Value, Yes	No, **Use Server Value**, Yes	Indicates whether the secondary server can accept dynamic updates.
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 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. The files are created in a background (batch) mode, then transferred to each server; conf files are generated for all servers. Zone files are generated for primary servers only. For automatic updates of DNS to take effect, an IP address must have been assigned to each domain's primary server. This is achieved through the **Object Management** function. If this parameter is set to None, administrators can manually request VitalQIP to compile 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 **Network Services|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 **Network Services|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 **Network Services|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.

Parameters	Value type	Options	Usage
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.
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**	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.

Windows 2003 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 4-11 Windows 2003 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	This is the mail address that appears in the SOA record of a zone file. Refer to "Enter email addresses" (p. 4-10) for formatting requirements.
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.

Parameters	Value type	Options	Usage
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.
Use server DNS domain as Active Directory domain	Boolean	**True** or False	Determines if the server uses the DNS domain as the Active Server domain. If this parameter is set to False, the following parameter is shown.
Active Directory Domain	Text		The domain used by Active Directory.

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 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. The files are created in a background (batch) mode, then transferred to each server; conf files are generated for all servers. Zone files are generated for primary servers only. For automatic updates of DNS to take effect, an IP address must have been assigned to each domain's primary server. This is achieved through the **Object Management** function. If this parameter is set to None, administrators can manually request VitalQIP to compile 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 *named* file is generated when a **Network Services|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 **Network Services|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.
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.

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 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.
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.

Parameters	Value type	Options	Usage
Server Startup Timeout (seconds)	Seconds	300 seconds	Determines the number of seconds to wait before the server fails a DNS push.

NIS server type

The following table describes the parameters for NIS. Items in **bold** in the Options column of the table are defaults.

Table 4-12 NIS parameters

Parameters	Value type	Options	Usage
Managed Range	Selection	(**Corporation**, Domain, Network, OSPF , Subnet Organizer, Subnet)	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		Location of the NIS data files.
Scheduled Automatic Updates	Boolean, Text	True (Hr. Min.) or **False**	If the Update Interval is set to True, indicate the interval in hours and minutes. The minimum permissible value is one hour.

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 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.

LOCAL HOST server type

The following table describes the parameters for the local host server. Items in **bold** in the Options column of the table are defaults.

Table 4-13 Local parameters

Parameters	Value type	Options	Usage
Managed Range	Selection	(**Corporation**, Domain, Network, OSPF , Subnet Organizer, Subnet)	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		Location of the host files.
Scheduled Automatic Updates	Boolean, Text	True (Hr. Min.) or **False**	If the Update Interval is set to True, indicate the interval in hours and minutes. The minimum permissible value is one hour.

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 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.

Windows 2003 Domain Controller server type

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 2003 Site** tab in the Subnet Organization profile (refer to "Set up a Windows 2003 site for a subnet organization" (p. 5-109)). 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 **Windows 2003 DC Generation** on the **Network Services** menu. Refer to "Generate Windows Domain Controller files" (p. 8-37).

> **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.

The following table describes the Windows 2003 Domain Controller parameters. Items in **bold** in the Options column are defaults.

Table 4-14 Windows 2003 Domain Controller parameters

Parameters	Value type	Options	Usage
LDAP Port	Selection	389	Identifies the LDAP Port.
Active Directory Domain Name	Text		Identifies the active directory domain name.

Parameters	Value type	Options	Usage
User DN	Text		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	Text	“secret”	The password used to connect to Active Directory Domain Name. By default, the password is secret and encrypted in the database.
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).

Non-managed DNS servers

It is important to understand that the Non-Managed DNS Server function is designed to allow DNS servers that are defined by VitalQIP to be secondary DNS servers for primary DNS servers that are not defined in the VitalQIP infrastructure. To define a secondary server that is in a VitalQIP-managed domain (rather than a non VitalQIP-managed domain as explained), use the Domain function on the **Infrastructure** menu.

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.

Do not use the **Non-Managed DNS Server** option under the **Infrastructure** menu to define secondary DNS servers when both the primary and secondary DNS machines are under control of VitalQIP. This is accomplished using the **Primary/Secondary** tab in the Domain or Network/Reverse Zone functions on the **Infrastructure** menu.

Define a non-managed DNS server

Purpose

Use this procedure to set up a Non-Managed DNS Server.

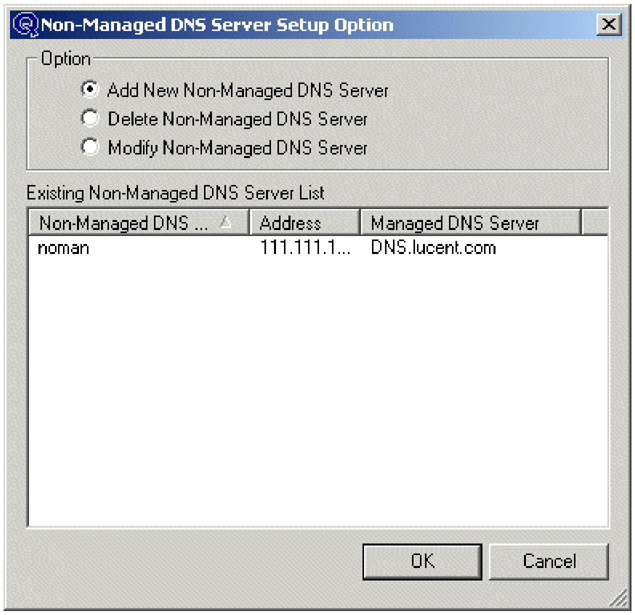
Before you begin

The non-managed server is not updated automatically with the information you define in the Non-Managed DNS Server Setup window. This information consists of the domain(s) and/or the network (in-addr.arpa) zone(s), and it needs to be manually added to the non-managed server's *named.conf* file.

Procedure

To define a non-managed DNS server, follow these steps:

1 Select **Non-Managed DNS Server** from the **Infrastructure** menu. The Non-Managed DNS Server Setup Option window opens.



Non-Managed DNS Server Setup Option

Option

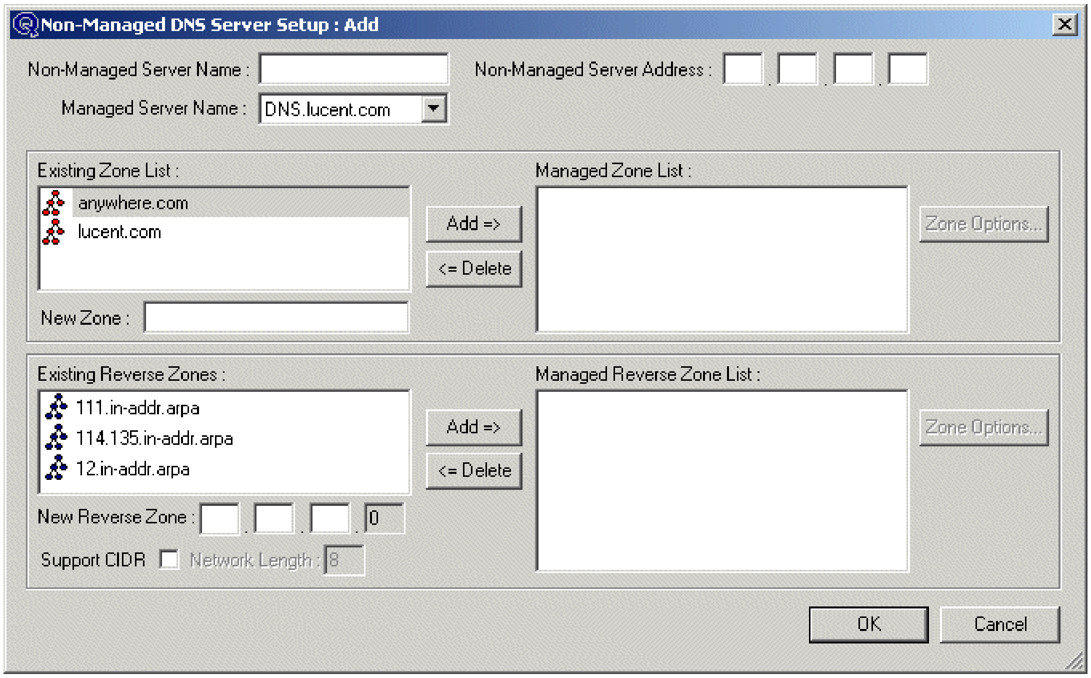
● Add New Non-Managed DNS Server
○ Delete Non-Managed DNS Server
○ Modify Non-Managed DNS Server

Existing Non-Managed DNS Server List

Non-Managed DNS ...	Address	Managed DNS Server
noman	111.111.1...	DNS.lucent.com

2 Select the **Add New Non-Managed DNS Server** option and click **OK**. The Non-Managed DNS Server Setup: Add window opens.

Note: Zones open as a hierarchical tree in the **Existing Zone List**, only if the "Display Domain Folders" option in the Administrator Profile is set.



Managed Server Name : DNS.lucent.com

Existing Zone List :
- anywhere.com
- lucent.com

Existing Reverse Zones :
- 111.in-addr.arpa
- 114.135.in-addr.arpa
- 12.in-addr.arpa

New Reverse Zone : . . . 0

Network Length : 8

3 Fill in the fields with information as necessary, as described in the following table.

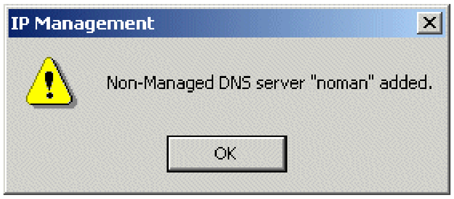
Table 4-15 Non-Managed DNS server setup fields

Field	**Description**
Non-Managed Server Name	Fill in the fully qualified name of the non-managed server.
Non-Managed Server Address	Fill in 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.
Managed Server Name	Select the VitalQIP defined server you wish to have as secondary to zones on this Non-Managed Server. This server must already be established.
Existing Zone List	This box lists the domains (zones) known to VitalQIP. You can assign one or more zones to this non-managed server. Select domain(s) in this list then click **Add**. The domain(s) open in the **Managed Zone List**.

Field	Description
New Zone	This defines a new domain (zone) not in the **Existing Zone List** that you want to be a secondary on the server identified in the **Managed Server Name** field. Type the domain (zone) name in this field and click **Add**. It is added to the **Managed Zones List**, along with your other selections. The **Zone Options** button is enabled when you add a new zone. You can set your zone options using this button.
Managed Zone List	This box lists the domains for which this non-managed server is primary for. To remove a domain (zone) from the **Managed Zone List**, select it and click **Delete**.
Existing Reverse Zones	This box lists the reverse zones (in-addr.arpa zones) known to VitalQIP. You can assign one or more reverse zones to this non-managed server. Select reverse zones in this list, then click **Add**. The reverse zones open in the **Managed Reverse Zones List**.
New Reverse Zone	To define a new reverse zone, type it in this field, then click **Add**. It is added to the **Managed Reverse Zones List** along with your selections from the **Existing Reverse Zones**. The **Zone Options** button is enabled when you add a new reverse zone. You can set your zone options using this button. **Note:** **Support CIDR** is checked, the second and third octets of this field allow you to enter any number you wish. You are no longer restricted based on what you place in the first octet.
Managed Reverse Zone List	This box lists the reversed zones for which this non-managed server is primary. To remove a reverse zone from the **Managed Reverse Zones List**, highlight it, and then click **Delete**.
Support CIDR	The **Support CIDR** box is unchecked by default. If you wish to support CIDR, click the check box. If **Support CIDR** is not checked (off), a network is created on traditional class A, B or C boundaries, with subnets allowed below that boundary. If **Support CIDR** is checked (on), any network can be created.
Network Length	This field is enabled when **Support CIDR** is checked, allowing you to fill in all four octets of the **New Reverse Zone** field.

4 If you added a new zone or new reverse zone and wish to apply zone options, refer to "Establish zone options" following.

5 Click **OK**. A confirmation prompt opens.



Non-Managed DNS server "noman" added.

6 Click **OK**.

END OF STEPS

Establish zone options

Purpose

Use this procedure to establish zone options for a new domain or reverse zone on a non-managed DNS server.

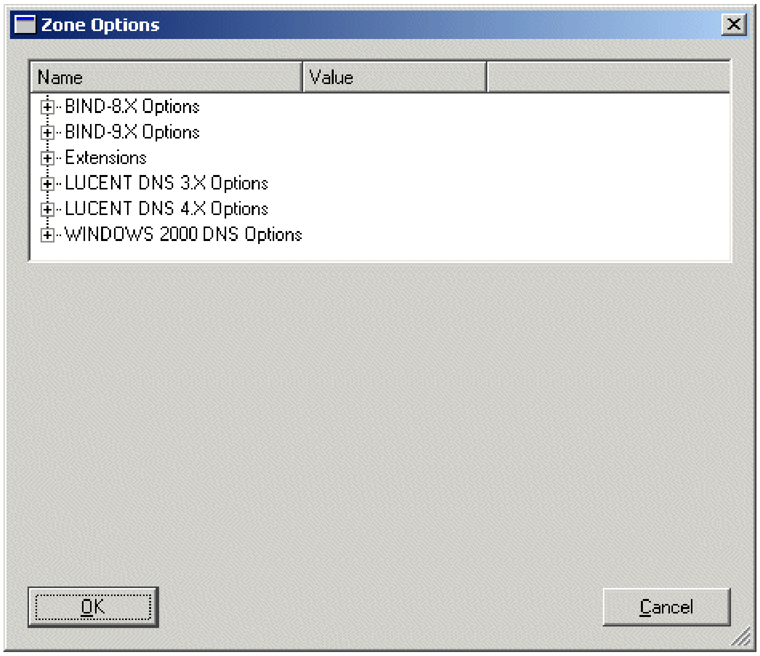
Before you begin

- 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 and cannot be modified.

Procedure

To establish zone options for a new domain or reverse zone on a non-managed DNS server, follow these steps:

1 Highlight the new zone within the **Managed Zone List** and click **Zone Options**. The Zone Options window opens.



2 Expand a zone option, select an option and enter/select a value. See the following table to locate more information about the Zone Options.

Table 4-16 Zone options

Zone options	Values
Extensions	See "Extensions zone options" (p. 5-27).
BIND-8.XOptions	See "BIND 8.X zone options" (p. 5-28).
BIND-9.X Options	See "BIND 9.X zone options" (p. 5-31).
Lucent DNS 4.X Options	See "LUCENT DNS 4.X zone options" (p. 5-38).
Windows 2003 DNS Options	See "Windows 2003 DNS Zone Options" (p. 5-42).

If you select Use List, you may select one or more ACL Templates and click **Add** to add a template to the Values list. To remove an ACL template address from the list, highlight the template and click **Delete**.

3 When you have finished setting up zone options, click **OK** to return to the Non-Managed DNS Server Setup: Add window.

END OF STEPS

Modify a non-managed server

Purpose

Use this procedure to modify a non-managed DNS server.

Procedure

To modify a Non-Managed DNS Server, follow these steps:

1. Select **Non-Managed DNS Server** from the **Infrastructure** menu. The Non-Managed DNS Server Setup Option window opens.

2. Select the **Modify Non-Managed DNS Server** option and highlight the Non-Managed DNS server you wish to modify.

3. Click **OK**. The Non-Managed DNS Server Setup: Modify window opens.

4. Modify the server as necessary and click **OK**. A confirmation prompt opens.

5. Click **Yes**. A confirmation prompt opens.

6. Click **OK**.

END OF STEPS

Delete a non-managed server

Purpose

Use this procedure to delete a non-managed DNS server.

Before you begin

If a non-managed server is deleted while it has zones associated with it, those zones are not removed from its managed counterpart. The zones ***are*** deleted from the managed counterpart in the database, but the push logic does not remove them from the managed DNS server. Therefore, the DNS server continues to serve them until the zones are manually deleted.

Note: It is not valid to create two non-managed servers with the same managed counterpart, delete one of the non-managed servers, and change the IP address of the remaining non-managed server to that of the deleted server. It is also not valid to create a non-managed server with two different managed counterparts, delete one of the non-managed server/managed server combinations and change the managed server's name of the remaining combination to that of the deleted one. Although VitalQIP allows both situations in the user interface, the DNS configuration files may not be cleaned up appropriately and the zones managed by the original non-managed/managed server combination may not be removed from the DNS configuration files.

Procedure

To delete an existing Non-Managed DNS Server, follow these steps:

1. Select **Non-Managed DNS Server** from the **Infrastructure** menu. The Non-Managed DNS Server Setup Option window opens.

2. Select the **Delete Non-Managed DNS Server** option and highlight the Non-Managed DNS Server you wish to delete.

3. Click **OK** and the Non-Managed DNS Server Setup: Delete window opens.

4. Click **OK** to delete it. A Warning prompt opens.

5. Click **Yes**. A confirmation dialog box opens.

6 Click **OK**.

END OF STEPS

5 Manage networks

Overview

Purpose

The purpose is to provide information on the management of the networks defined in VitalQIP. It includes information on organizations, domains, networks, subnets, reverse zones, OSPF areas, subnet organizations, and applications.

Contents

The following topics are covered:

Organizations	5-4
Add an organization	5-5
Add values to user-defined fields	5-8
Modify an organization profile	5-9
Delete an organization profile	5-10
Domains	5-11
Define internal root zones for internal root servers	5-11
Create domain profile	5-13
Define primary/secondary servers	5-18
Set up Resource Records for the domain	5-21
Set zone options	5-26
Extensions zone options	5-27
BIND 8.X zone options	5-28
BIND 9.X zone options	5-31
LUCENT DNS 3.X zone options	5-35

LUCENT DNS 4.X zone options	5-38
Windows 2003 DNS Zone Options	5-42
Set up user-defined fields for a domain	5-44
Modify a domain profile	5-45
Delete a domain profile	5-46
Change DNS options on multiple zones	5-47
Change multiple zone options	5-49
Change user-defined fields in multiple zones	5-50
Networks and subnets	5-51
Create a new network	5-54
Modify a network	5-57
Delete a network	5-58
Create subnets	5-59
Use the Auto. Calculate option	5-62
Use the User Define option	5-64
Split or join subnets	5-65
Assign a primary DNS server to one or more subnets	5-67
Establish network warnings	5-68
Define address ranges for the network	5-69
Reverse zones	5-71
Set up a reverse zone	5-72
Split a reverse zone	5-75
Review and modify reverse zone properties	5-77
Review reverse zone information	5-78
Review/define primary and secondary servers	5-80
Reverse zone resource record setup	5-83
Define reverse zone options	5-85
Reverse zone user-defined field setup	5-87
OSPF areas	5-88
OSPF explained	5-88

Create an OSPF area	5-90
Manage subnets with an OSPF area	5-93
Manage ranges with an OSPF area	5-94
Establish OSPF area warnings	5-97
Modify an OSPF area	5-99
Delete an OSPF area	5-100
Subnet organizations	5-101
Define a subnet organization	5-102
Apply Global Allocation Policies	5-105
Set up a subnet organization warning	5-107
Set up a Windows 2003 site for a subnet organization	5-109
Modify a subnet organization	5-111
Delete a subnet organization	5-112
Applications	5-113
Add an application	5-114
Modify an application	5-116
Delete an application	5-117

Organizations

Setting up Organizations provides multiple VitalQIP management systems with one physical database. 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. This is an optional infrastructure definition, and can be performed later.

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:

- DHCP Templates
- DHCP Options Templates
- DHCP Policy Templates
- Naming Policies
- Manufacture Profile
- User- Define Fields
- Object Class

In this profile you can also establish values for Organization User-Defined fields which you have previously set up in the **User-Defined Fields** function on the **Policies** menu. Refer to “User-defined fields” (p. 3-53) for more information on setting up User-Defined Fields for Organizations.

Add an organization

Purpose

Use this procedure to add a new organization.

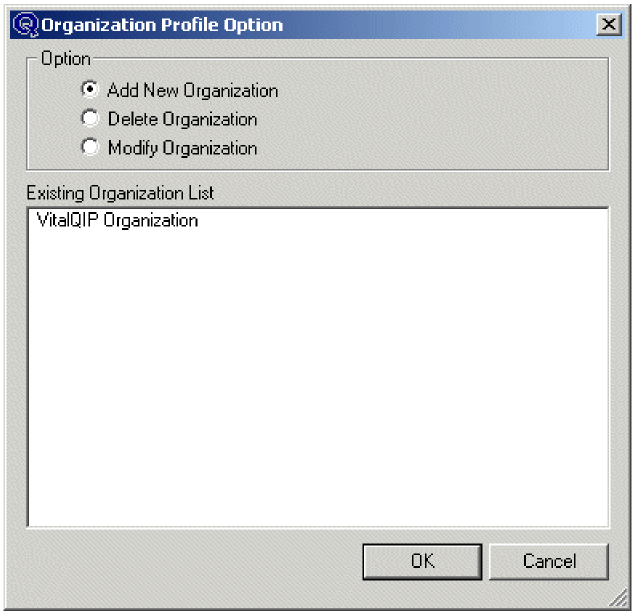
Before you begin

- When more than one organization is defined in the database, a Master administrator always has to select an organization during the login process.
- To manage other organizations, you can select a new organization through the **File|Login|Change Organization**, or use the Hierarchy window to select another organization.
- All administrators view the same list of User-Defined Fields.
- Master administrators and normal administrators with an Organization Managed Type set to Read/Write have access to Organization User-Defined Fields when using the Go To/Search function.

Procedure

To add an organization, follow these steps:

1 Select **Organization** from the **Infrastructure** menu. The Organization Profile Option window opens.



Organization Profile Option

Option

● Add New Organization

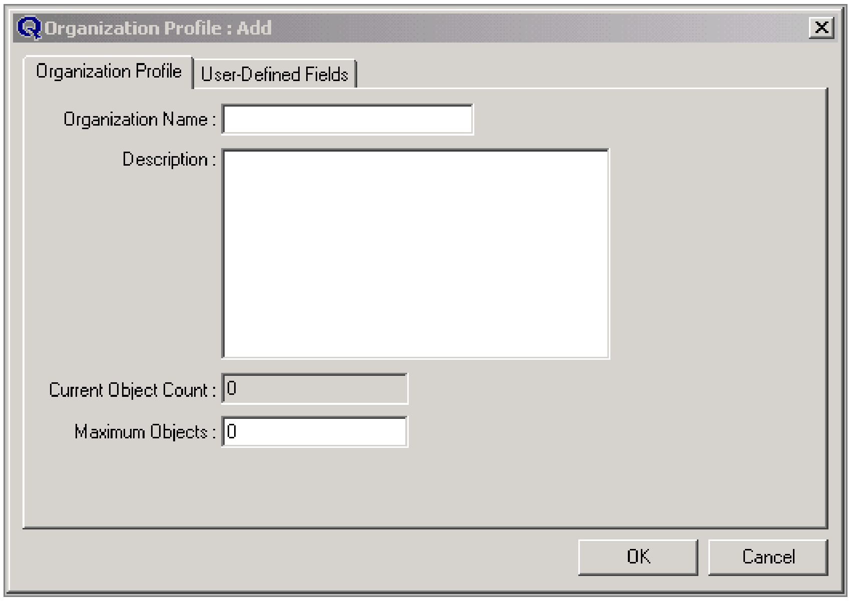
○ Delete Organization

○ Modify Organization

Existing Organization List

VitalQIP Organization

2 Click **OK** (since **Add New Organization** is already selected). The Organization Profile: Add window opens.



Current Object Count : 0

Maximum Objects : 0

3 Enter an **Organization Name** (up to 32 characters are allowed). It must be unique from all other organizations defined in the database.

4 Click in the **Description** field (or press **Tab)** and enter a description if you wish (up to 255 characters are allowed).

5 If you are a Master administrator, you can define the number of objects that can exist for this organization in the **Maximum Objects** field. An entry of zero indicates that there is no limit. If you try to add more objects than the limit displayed in the Maximum Objects field, you will receive an error message.

Note: The objects that are counted are static and dynamic objects. Reserved, planned to use, selected, and unused objects are not counted.

6 If you have previously defined User-Defined Fields for Organizations and wish to enter a value, click the **User-Defined Fields** tab.

7 Select the field for which you want to enter a value.

8 Click **Value** field and enter a value of up to 128 characters.

9 Click **OK** when you are ready to save your Organization Profile. A status dialog box opens.

10 Click **OK** .

END OF STEPS

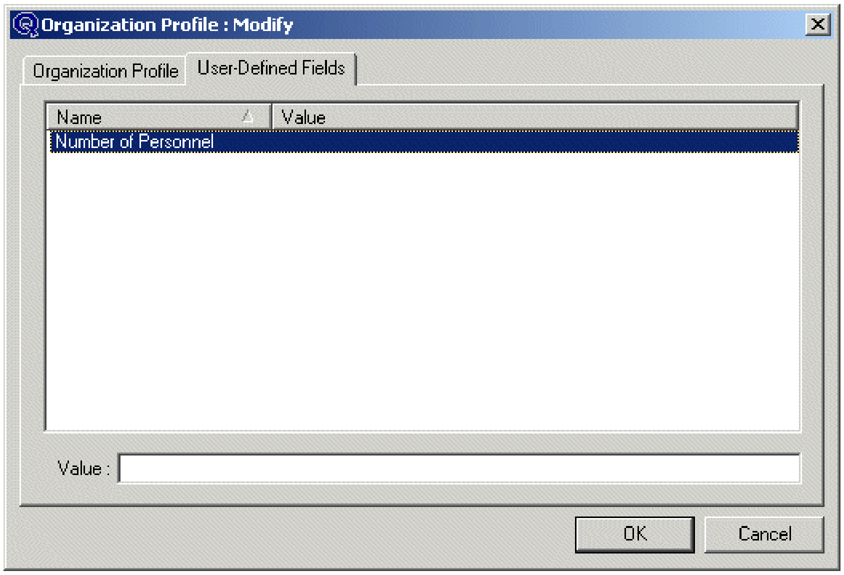
Add values to user-defined fields

Purpose

The **User-Defined Fields** tab allows you to assign values to any fields you have already established with the **User-Defined Fields** function on the **Policies** menu for use in an Organization Profile or use in an Organization Profile. For instance, suppose you have previously created a user-defined field called “Number of Personnel”, you could assign a value (of up to 127 alphanumeric characters) as follows.

Procedure

1 Click the **User-Defined Fields** tab.



Name	Value
Number of Personnel	

Value :

2 Enter a value (of up to 127 alphanumeric characters) and click **OK**.

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

END OF STEPS

Modify an organization profile

Purpose

Use this procedure to modify an organization profile.

Procedure

To modify an existing Organization, follow these steps:

1 Click **Modify Organization** in the Organization Profile Option window.

2 Select the organization you wish to modify in the Existing Organization List and click **OK**, or simply double-click on the organization name. The profile for this organization opens.

3 Modify as necessary, and click **OK** to save your changes. The status dialog box opens.

4 Click **OK**.

END OF STEPS

Delete an organization profile

Purpose

Use this procedure to delete an organization profile.

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 objects.

Procedure

To delete an existing Organization, follow these steps:

1 Click **Delete Organization** in the Organization Profile Option window.

2 Select the organization you wish to delete and click **OK**. The profile for this organization opens.

3 Click **OK** to delete it. The confirmation dialog box opens.

4 Click **Yes**.

Note: Although you cannot delete the “VitalQIP Organization” (the default), you can rename it.

END OF STEPS

Domains

One or more domains for primary and secondary servers under the control of VitalQIP can be defined through the **Domain** function on the **Infrastructure** menu. VitalQIP organizes domains into a logical hierarchy. Under this function, IPv6 reverse zones can be created. (See “VitalQIP support of IPv6 reverse zones” (p. 8-17) for more information about how VitalQIP supports IPv6 reverse zones.)

One or more networks or subnets can be assigned to each domain. A network can belong to multiple domains, but only one is considered the primary (default) domain.

Once the domain names for all primary and secondary servers have been defined, the servers must be assigned IP addresses. This cannot be done until the network infrastructure has been defined and the specific networks containing these servers’ addresses have been created.

If your network contains many domains, you may find it easier to manage them if you set up domain folders (defined in the Administrator Profile function on the **Customize** tab). The domains in the network can be organized within distinctive folders, which make it easier to navigate your network without any impact on performance. Furthermore, administrators can be assigned to the resulting domains (refer to “Customize administrator menus” (p. 6-30)).

Define internal root zones for internal root servers

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 domain hierarchy. All zone options and SOA values are defined in the domain profile for that zone. To create the root zone, you simply need to create a root domain 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 domain. You must click **Yes** to continue.
- Once a root zone is created, you cannot change the name.
- Renaming an existing domain 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 Domain List** in the Domain 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 domain profile for the root zone.

Create domain profile

Purpose

Use this procedure to create a domain profile.

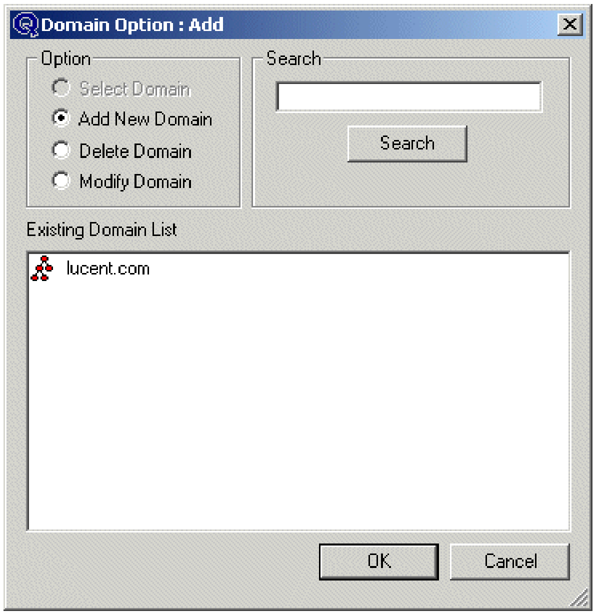
Before you begin

- A domain and an object cannot have the same name.
- If your organization allows Internet name resolution when defining Domains, do not define any of the Internet's root domains. Specifically, do not define the root (dot) "**.**" domain (.com, .edu, .gov, and so on). Doing so would cause any primary domain server to be defined as an Internet Root Server.
- If your organization is completely isolated from the Internet and you wish to configure an Internal Root Server, refer to "Define internal root zones for internal root servers" (p. 5-11).
- VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and the profile cannot be saved while the conflict exists. This feature can be disabled by setting the **Validate CNAMES** sub-policies to False. These polices are under the **Validate CNAME Records** policy. See Table 3-5, "General policies" (p. 3-29) for more information on the policy. When you add or modify a domain, validation checks are made against:
  - Object aliases
  - CNAME object resource records
  - CNAME domain resource records
  - CNAME reverse zone resource records

Procedure

To set up your domains by using the Domain Profile, follow these steps:

1 Select **Domain** from the **Infrastructure** menu. The Domain Profile Option window opens.

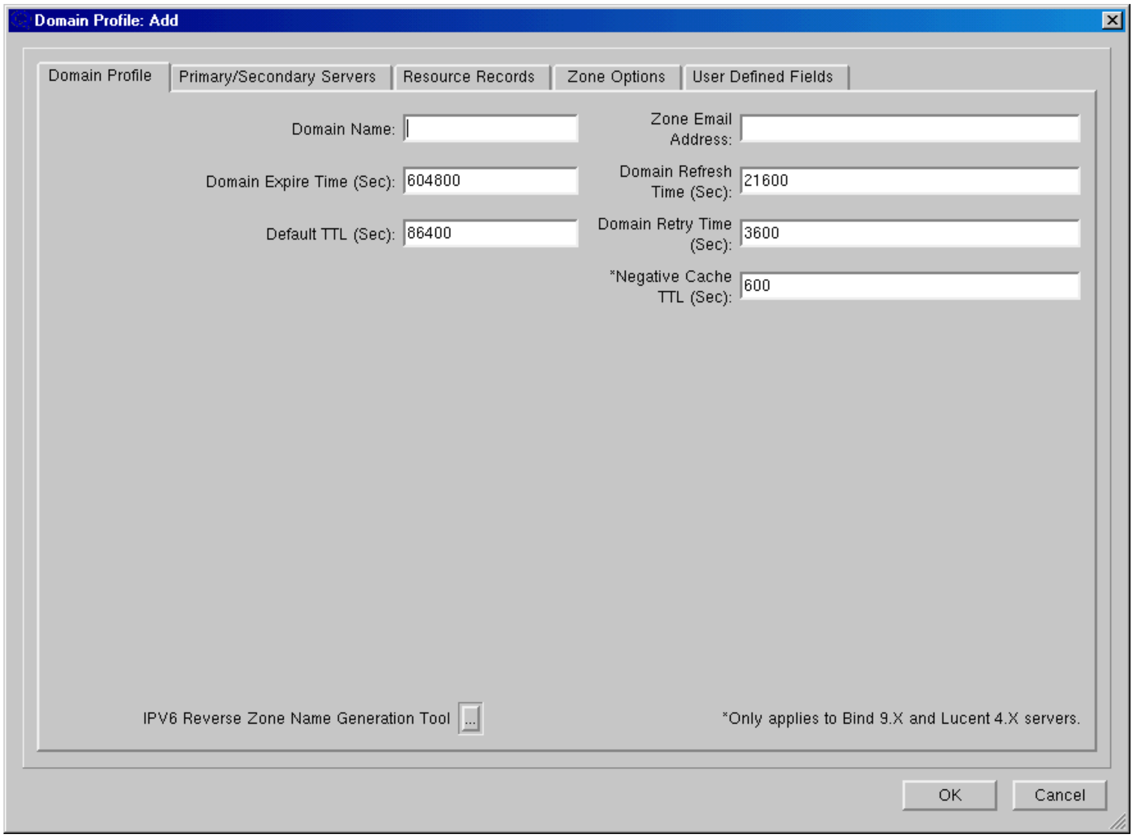


○ Select Domain
● Add New Domain
○ Delete Domain
○ Modify Domain

lucent.com

The display in the **Existing Domain List** in the Domain Option window is based on the administrator’s **Display Domain Folders** setting. This setting is defined in the **Administrator Profile** on the **Customize** tab.

2 Select **Add New Domain** and click **OK**. The Domain Profile: Add window opens.



Domain Name:

Zone Email Address:

Domain Expire Time (Sec): 604800

Domain Refresh Time (Sec): 21600

Default TTL (Sec): 86400

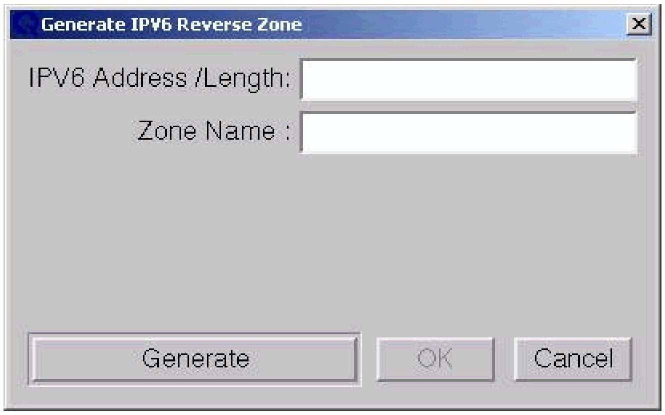
Domain Retry Time (Sec): 3600

*Negative Cache TTL (Sec): 600

*Only applies to Bind 9.X and Lucent 4.X servers.

3 Enter a fully qualified domain name in the **Domain Name** field. If you are adding an IPv6 reverse zone use the **IPv6 Reverse Zone Name Generation Tool** button to add a name. The **IPv6 Reverse Zone Name Generation Tool** button allows IPv6 reverse zones to be created. For more information about how VitalQIP supports IPv6 reverse zones, see "VitalQIP support of IPv6 reverse zones" (p. 8-17). You can create reverse zone options for IPv6 by doing the following:

a. Click **IPv6 Reverse Zone Name Generation Tool**. The IPV6 Reverse Zone Generation screen opens.



b. 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.

c. The address must be validated and converted to a reverse zone address. To do so, click **Generate**. 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.c.e.f.ip6.arpa.

d. To add the reverse zone name to the **Domain Name** field of the **Domain Profile** tab, click **OK**.

4 Enter an email address in the **Zone E-mail Address** field. This is the email address that is put in the SOA records. Any errors posted by DNS are sent to this email address. You must have a value for this field. Refer to "Enter email addresses" (p. 4-10) for formatting requirements.

5 Change the timing defaults for secondary servers as needed (refer to the following table).

The timing values define when the Secondary Servers attempt to refresh their database. Each must be defined, and is measured in seconds. The system defaults are recommended if you are starting out; you can refine them as you gain network management experience.

Table 5-1 Domain profile fields

Field	Description
Domain Expire Time (Sec)	***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).
Domain Refresh Time (Sec)	***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).
Default TTL (Sec)	***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.
Domain Retry Time (Sec)	***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).
Negative Cache TTL (Sec)	***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.

6 When you have finished entering or adjusting the values in the **Domain Profile** tab, you can select other tabs to continue setting up the domain. Refer to the following sections for further details.

7 Click **OK** to save a domain profile.

8 Click **OK** at the confirmation prompt.

END OF STEPS

Define primary/secondary servers

Purpose

The **Primary/Secondary Servers** tab allows you to define the primary domain servers for the domain, and secondary domain servers or “slaves” to the domain. These servers manage the domain you identified in the **Domain Profile**. All existing DNS servers appear in the **Existing DNS Servers List** as you defined them in the **Server Profile**, and you can add them to the **Selected DNS Servers List** as either primary servers or secondary servers.

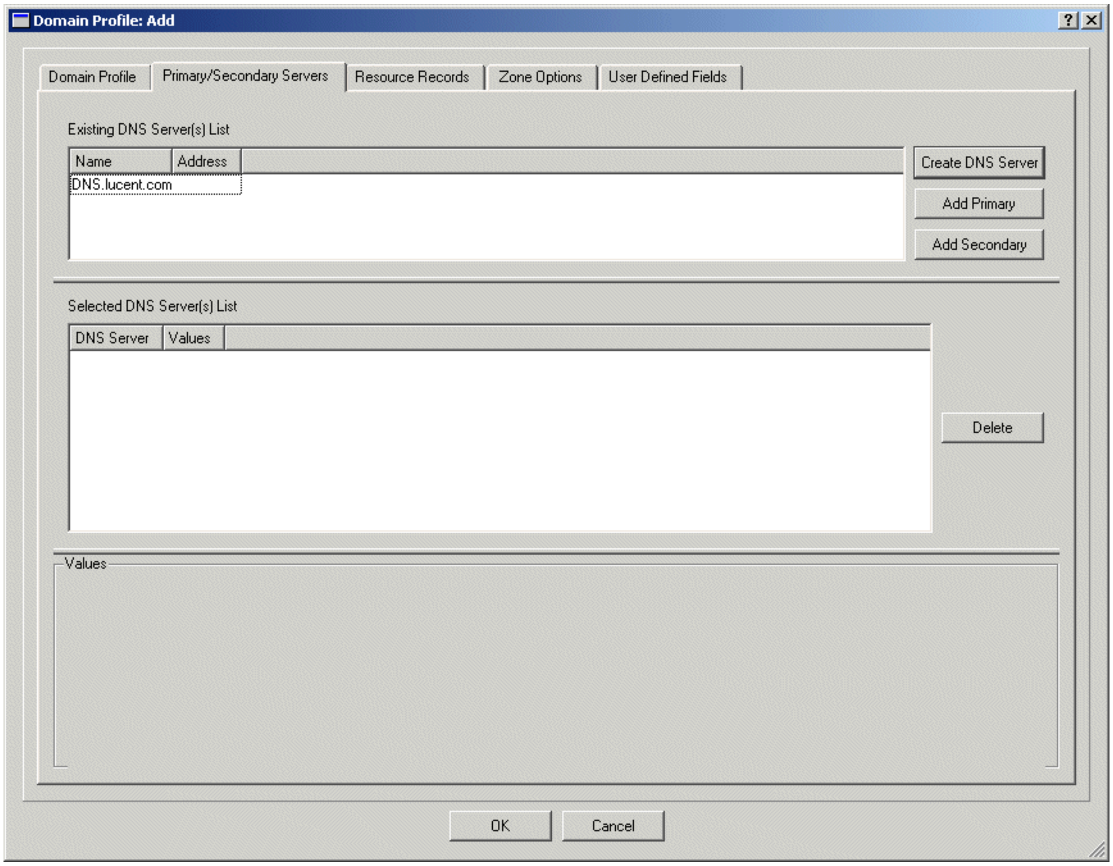
Before you begin

- For VitalQIP, it is a good idea to have at least one primary server defined for all domains, although VitalQIP does allow you to have a domain defined without adding a primary server.
- Although it is possible to have more than one primary server per domain, it is not recommended.
- If you choose to define multiple primary servers for a domain, 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/secondary server, follow these steps:

1 Click the **Primary/Secondary Servers** tab.



DNS.lucent.com

2 To add a primary domain server, select a DNS server from the **Existing DNS Servers List** and click **Add Primary**. The server is added to the **Selected DNS Servers List**, as a primary server managing this domain.

3 After you have added the DNS server to the Selected DNS Servers List, you can change the zone options if desired. Simply click on the server to expand it, and select the **Zone Option**. A field appears in the Values section. You select **User Zone Value** or **Customize**. If you select **Customize**, the zone values appear in the tree and you can change them as desired.

> **Note:** The icon indicates that the server in the **Selected DNS Servers List** is secure for the current zone. If the server has been defined with the **Secure DNS Updates** parameter set to True in the Server Profile, it appears with a key/server icon and you can enable secure DNS updates by setting the **Send Secure Updates** parameter to

True. For more information on setting up secure DNS, refer to the *Administrator Reference Manual*.

4 You have the option of making a DNS sever a stealth server. The reverse zone stealth server options show up only for a newly-defined DNS server associated with either a new or already created reverse zone. The other way to see the stealth server options is to open the reverse zone properties file and save the reverse zone. When you redisplay the reverse zone properties, you see the stealth zone options in place.

When you expand a server in the Selected DNS Servers List, an option called **Stealth Server** is available. By default, the option is set to False. When the value is changed to True, the server's NS records are no longer placed in the zone files on other servers and another sub-option called **Override Server Name in SOA** is enabled.

By default, **Override Server Name in SOA** is set to False. When this sub-option set to True, another option called **Override Server Name** is enabled. Set **Override Server Name** to the host name of the server to appear in the SOA record instead of the stealth server's name.

5 You can add one or more DNS server(s) as secondary servers to manage this domain. They must be hierarchically associated with a primary server. To add secondary DNS servers to this domain, highlight the server(s) you wish to add as secondary servers in the **Existing DNS Servers List** ***and*** highlight the primary server in the **Selected DNS Servers List** to which you wish them to be secondary; then click **Add Secondary**.

6 To delete servers from the **Selected DNS Servers List**, highlight one or more servers in the list and click **Delete**.

7 Clicking **Create DNS Server** displays the Server Profile with “DNS” selected. This allows you to add a new DNS server to the **Existing DNS Servers List**. You can then assign a domain to this DNS Server in the Domain Profile’s **Primary/Secondary Servers** tab.

END OF STEPS

Set up Resource Records for the domain

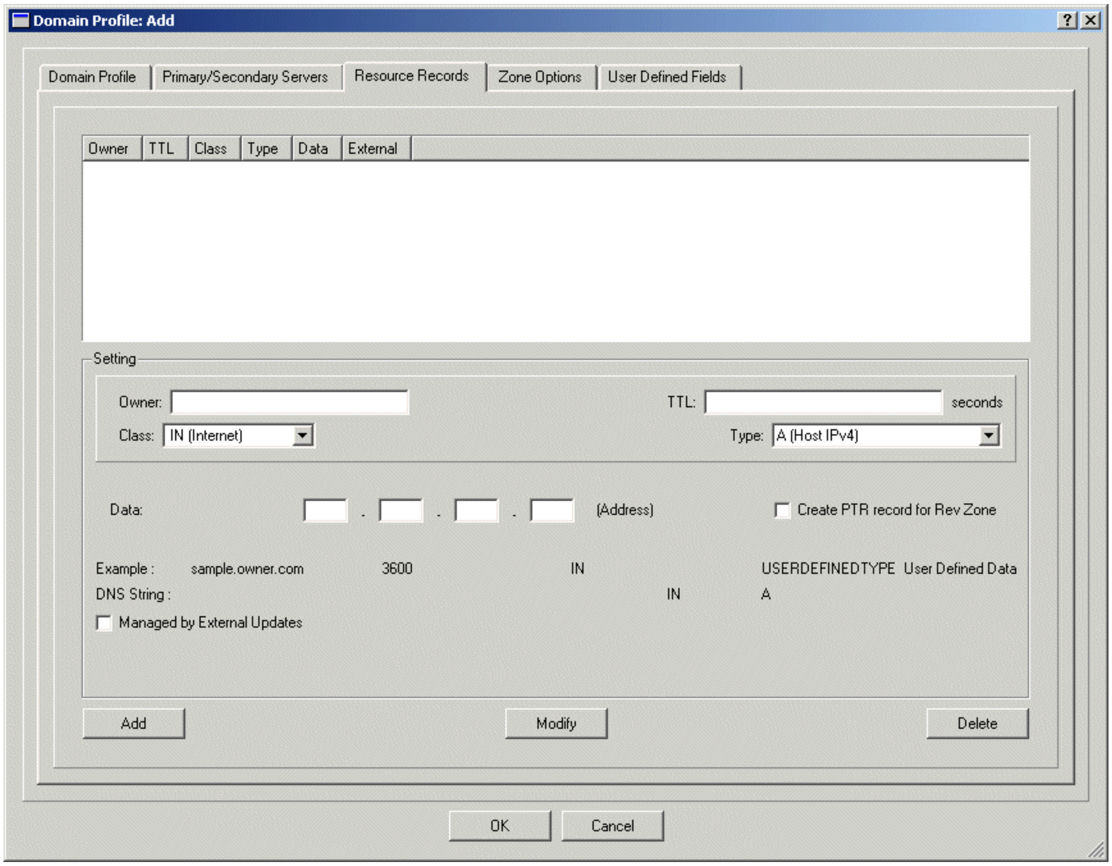
The **Resource Records** tab allows you to create, modify, and delete Resource Records for a domain. This option allows Resource Records for the domain to be written to the configuration file. VitalQIP validates and formats the information on input.

Before you begin

- The **Resource Records** tab is only available if the administrator has the "Create Resource Record" privilege set to True. Refer to "Create an administrator profile" (p. 6-12) for more information.
- VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and the profile cannot be saved while the conflict exists. This feature can be disabled by setting the **Validate CNAMES** sub-policies to False. These polices are under the **Validate CNAME Records** policy. See Table 3-5, "General policies" (p. 3-29) for more information on the policy. When records other than CNAME records are added or modified, validation checks are made against:
  - Object aliases
  - CNAME object resource records
  - CNAME domain resource records
  - CNAME reverse zone resource records

  When CNAME records are added or modified, validation checks are made against:
  - Object aliases
  - Domain names
  - Any Object Profile resource records
  - Any Domain Profile resource records
  - Any Reverse Zone resource records
  - ENUM NAPTR resource records
  - IPv6 node names

– MX records



Owner:

TTL: seconds

Class: IN (Internet)

Type: A (Host IPv4)

Data: . . . (Address)

□ Create PTR record for Rev Zone

Example : sample.owner.com 3600 IN USERDEFINEDTYPE User Defined Data

DNS String : IN A

□ Managed by External Updates

The fields are described in the following table.

Table 5-2 Resource Records tab fields

Field	Description
Owner	Enter whatever name you are using to define the owner for this domain.
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, or enter the class(es) you want to use for this object.
TTL (Time To Live)	The length of time (in seconds) the name server will hold this information. If no TTL is defined, unlimited is implied.

Field	**Description**
Type	Select the **Type** of Resource Record from the listing, or enter your own **Type** in this field. The settings for the different types are described in the Resource Records tab fields table. For additional information on these record types, refer to *DNS and BIND*, by Cricket Liu and Paul Albitz.
Data	The data associated with the specific resource record type. Whenever you select a Resource Record **Type** in the **Setting** section, the **Data** control is updated to allow for the correct formatting of the selected resource record. Refer to the Setting Fields Shown table following.
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. 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, different settings are displayed in the remainder of the **Setting** section, as described in the following table.

Table 5-3 Setting fields

Type field choice	**Data fields displayed**
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)	**CPU** – enter the central processing unit type. **OS** – enter the operating system type. MX (Mail Exchanger)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.

Type field choice	Data fields displayed
MX (Mail Exchanger)	**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.
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 *letc/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)	**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.

Type field choice	Data fields displayed
ISDN	**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)	**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 relative weight for entries with the same priority using any numbers between 0 and 65535. **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.

For A type Resource Records you can have PTR records generated automatically by checking the **Create PTR for Reverse Zone** check box. If selected, PTR resource records are automatically created in the correct reverse zone whenever an A record is being added or modified. However, the reverse zone must exist.

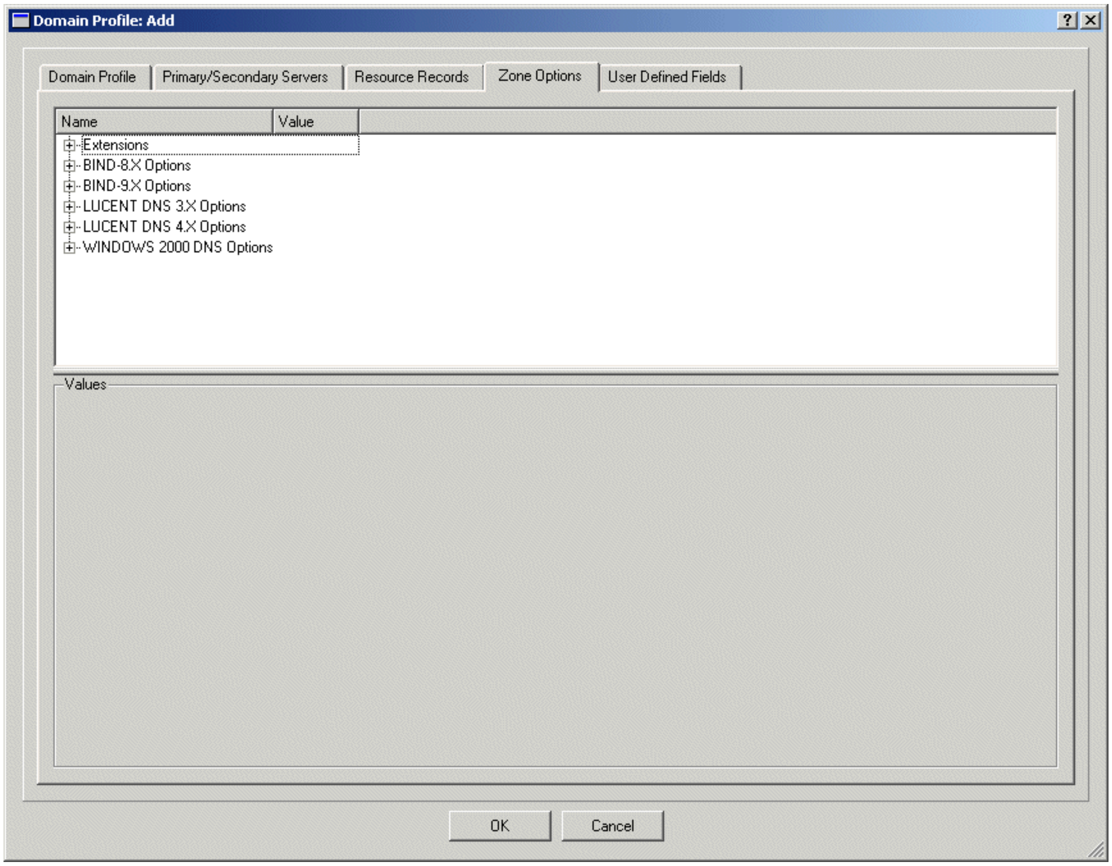
If it does not exist, the error message "`The 'PTR' record cannot be created because the Reverse Zone for <`*`the_IP_address`*`> doesn't exist`" is displayed, and you must uncheck the **Create PTR for Reverse Zone** check box.

Whenever an A record is modified, an additional PTR record is created. You must go to the affected Reverse Zone to delete earlier PTR records. Deleting an A record does not delete the associated PTR record from the reverse zone.

> **Note:** The contents of the **Resource Records** tab are not validated in the same way as the contents in the Object Profile, such as the **Alias** and **Mail** tabs. If erroneous information is entered into the **Resource Records** tab, the erroneous information is entered into the zone and could cause errors with the loading of the zone. For information on proper usage and syntax, see *DNS and BIND* by Paul Albitz & Cricket Liu, published by O'Reilly & Associates.

Set zone options

The **Zone Options** tab allows you to set up your zone options.



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 5-4 Zone options

Zone Options	Values
Extensions	See "Extensions zone options" (p. 5-27).
BIND-8.X Options	See "BIND 8.X zone options" (p. 5-28).
BIND-9.X Options	See "BIND 9.X zone options" (p. 5-31).
Lucent DNS 4.X Options	See "LUCENT DNS 4.X zone options" (p. 5-38).
Windows 2003 DNS Options	See "Windows 2003 DNS Zone Options" (p. 5-42).

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 5-5 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 255,000 characters. 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 255,000 characters. For example:
	`mailhost2IN A198.200.138.234`
	`mailhost1IN MXmailhost2.quadritek.com.`
	`oneilltIN A198.200.138.236`
	`myaliasIN CNAMEoneillt.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 a parameter value is set to **Use Server Value** (USV), the DNS options are not written to the root zone of the server. DNS options only apply to root servers. To use server values for any zone, the server values need to be defined in the server's option block. (The option block for the server is defined by the **Corporate Extension** parameter in the Server Profile.) The **allow-update** option cannot be set in the server's option block since this is only a zone level option. By setting **allow-update** to USV, you are in effect turning off updates. If the options are not defined in the Corporate Extension and the USV flag is set, the default values for the options are used, as follows:

```
allow-transfer none
   allow-update   none
   allow-query    none
   check-names    fail
   notify         no
```

Table 5-6 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 resolver. The **Use List** option value presents two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Access Control Lists (ACLs)" (p. 3-3). **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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Access Control Lists (ACLs)" (p. 3-3). **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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Access Control Lists (ACLs)" (p. 3-3). **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.

BIND 8.X zone option	Value type	Option value	Usage
check-names	Selection	**Warn**, Fail, Ignore, Use Server Value	**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.
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 Value** (USV), the DNS options are not written to the root zone of the server. DNS options only apply to root servers. To use server values for any zone, the server values need to be defined in the server's option block. (The option block for the server is defined by the **Corporate Extension** parameter in the Server Profile.) The **allow-update** option cannot be set in the server's option block since this is only a zone level option. By setting **allow-update** to USV, you are in effect turning off updates. If the options are not defined in the Corporate Extension and the USV flag is set, the default values for the options are used, as follows:

```
allow-transfer none
  allow-update   none
  allow-query    none
  check-names    fail
  notify no
```

Table 5-7 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 via **Network Services | DNS Generation** function.

BIND 9.X zone option	**Value type**	**Option value**	**Usage**
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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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-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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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-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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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.

BIND 9.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 **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.

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 5-8 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 resolver. The **Use List** option value presents two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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 3.X zone option	Value type	Option value	Usage
check-names	Selection	**Warn**, Fail, Ignore, Use Server Value	**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.
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 5-9 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 via **Network Services | DNS Generation** function.
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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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-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 two sub-options: **ACL Template** - allows you to select an ACL template. Refer to "Client Class" (p. 2-90). **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 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.

LUCENT DNS 4.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.

Windows 2003 DNS Zone Options

The following table describes the Windows 2003 zone options. Default values in the Option value column appear in boldface.

Note: Windows 2003 zone options can also be used with a Windows 2003 DNS server.

Table 5-10 Windows 2003 DNS zone options

Windows 2003 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.
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**. Therefore, if you want DDNS to work properly, you must set this option to a value other than **No**.

Windows 2003 DNS zone option	Value type	Option value	Usage
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.

Set up user-defined fields for a domain

You can establish values for User-Defined fields for Domains in the **User-Defined Fields** tab. Information entered in this tab does not get loaded into the Domain Zone file.

The User-Defined fields for Domains must first be defined in the **User-Defined Fields** function on the **Policies** menu.

Modify a domain profile

Purpose

Use this procedure to modify a domain profile.

Procedure

To modify an existing domain, follow these steps:

1 Select **Modify Domain** and select the domain you wish to modify in the **Existing Domain** list (or simply double-click on the domain you wish to modify).

Note: To search for specific domains, enter a domain name in the **Search** field. The matching domains are displayed in the **Existing Domain List** as a list (no folders). You can then select the domain to modify (or delete) from the list. If a domain is added at this time, it will be placed in the default **Domains** folder. Performing a search with no search criteria causes the top-level folder/domain hierarchy to be displayed in the **Existing Domain List**.

2 Click **OK** and the Domain Profile: Modify window opens.

3 Modify the Domain Profile as necessary and click **OK** to save your changes. A confirmation prompt opens.

4 Click **OK**.

END OF STEPS

Delete a domain profile

Purpose

Use this procedure to delete a domain profile.

Before you begin

If you delete a domain, it will disassociate the domain from all objects. It will also remove MX records that reference the domain. Any server that is named with this domain will not be removed (for example, if you delete domain *xxx.com*, the DHCP server named *dhcp1.xxx.com* will not be removed).

Procedure

To delete an existing domain, follow these steps:

1 Select **Delete Domain** and then select the domain you wish to delete from the **Existing Domain** list.

2 Click **OK** and the Domain Profile: Delete window opens.

3 Click **OK** to delete it. A Question dialog box opens.

4 Click **Delete**. A confirmation prompt opens.

5 Click **OK**.

END OF STEPS

Change DNS options on multiple zones

Purpose

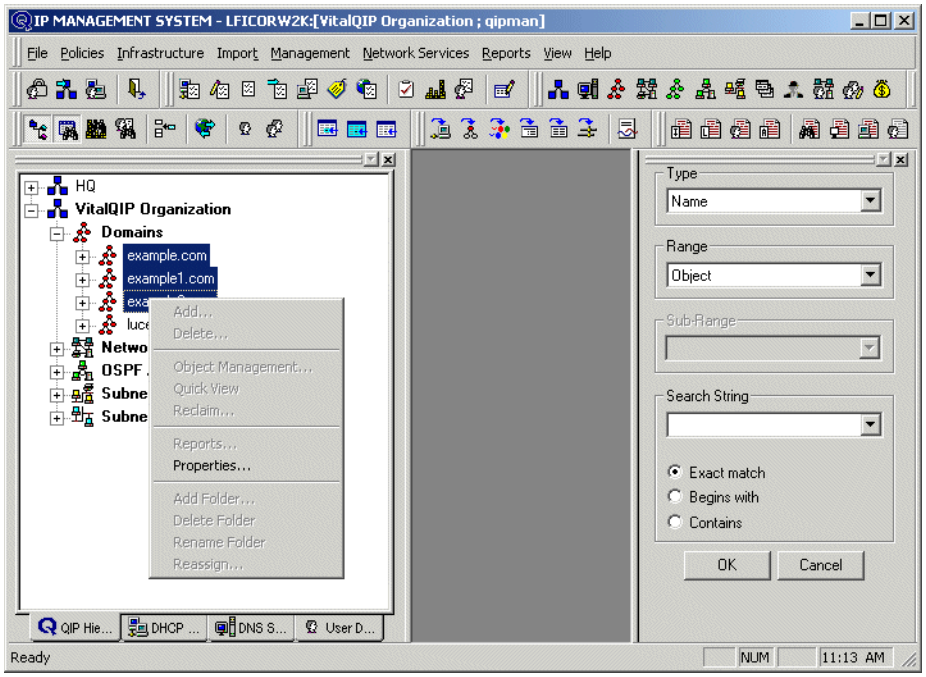
If you have privileges as a Master administrator, or Normal administrator with write permission for all selected zones in the QIP Hierarchy, you can select multiple zones (domains ***or*** reverse zones) and specify a set of DNS options once that will be applied to all those zones without you having to open each domain or reverse zone individually.

> **Note:** After changing DNS options on multiple domains or reverse zones, you can edit individual properties.

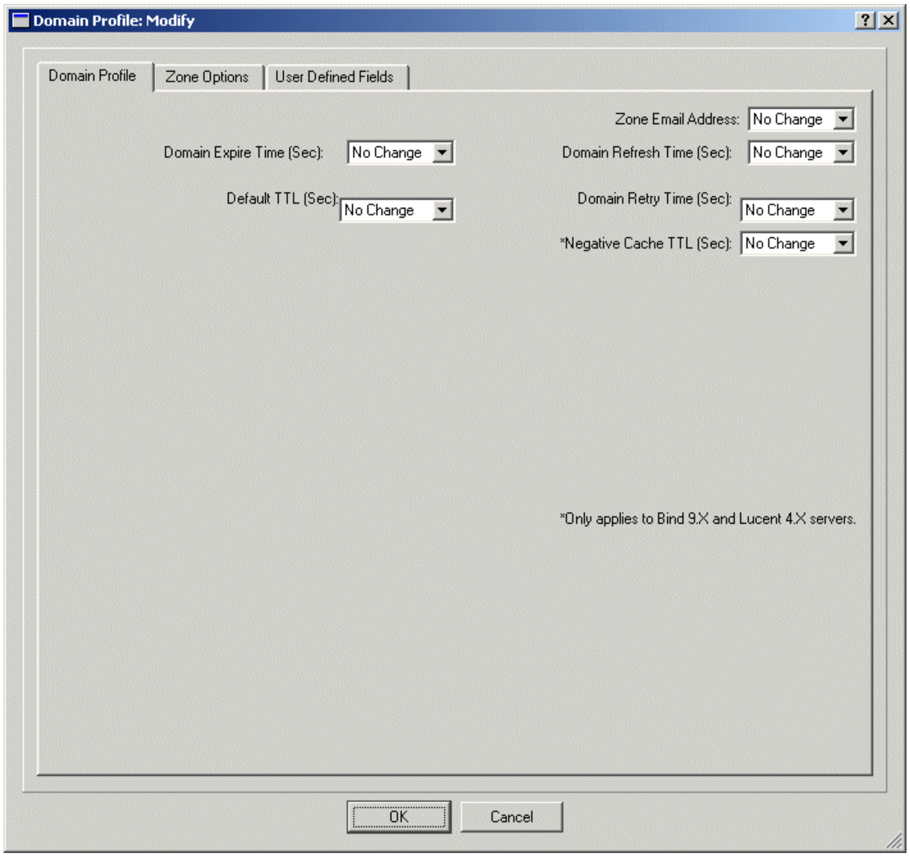
Procedure

To change DNS options on multiple domains or reverse zones, perform the following steps:

1 In the QIP Hierarchy, select the zones for which you have write permission and right-click on the selected zone.



2 Choose **Properties.** The Domain Profile window (Network/opens.



Zone Email Address: No Change

Domain Expire Time (Sec): No Change

Domain Refresh Time (Sec): No Change

Default TTL (Sec): No Change

Domain Retry Time (Sec): No Change

*Negative Cache TTL (Sec): No Change

*Only applies to Bind 9.X and Lucent 4.X servers.

3 You can modify a field by entering a new value. Leave those fields for which you do not wish to make a global change at the **No Change** default.

4 Select other tabs and make changes as needed. Review the following sections for further information on making changes to Zone Options and User-Defined Fields.

5 Click **OK** to save your changes. A Confirmation prompt opens.

6 Click **OK**.

END OF STEPS

Change multiple zone options

Select the **Zone Options** tab to modify option settings for multiple zones.

> **Note:** If you deselect any parent in the Name tree, its children are also automatically deselected.

For a description of the different zone options, refer to:

- "Extensions zone options" (p. 5-27)
- "BIND 8.X zone options" (p. 5-28)
- "BIND 9.X zone options" (p. 5-31)
- "LUCENT DNS 3.X zone options" (p. 5-35)
- "LUCENT DNS 4.X zone options" (p. 5-38)
- "Windows 2003 DNS Zone Options" (p. 5-42)

If you select Use List, you may select one or more ACL Templates and click **Add** to add a template to the Values list. To remove an ACL template address from the list, highlight the template and click **Delete**.

Change user-defined fields in multiple zones

Select the **User Defined Fields** tab to modify user-defined field values over multiple domains and/or reverse zones.

To modify a value, select a user-defined field and enter a new value in the **Value** field.

Networks and subnets

The **Network/Reverse Zone** function on the Infrastructure menu allows you to define a network and assign subnets to it, as well as customize your reverse zone settings. This can be an involved decision regarding subnet masking and the support of CIDR.

Before you begin to define the subnets on your network(s), there are a few concepts to review. Understanding these concepts helps you optimize the way you structure networks and subnets, because they allow you to decrease the amount of traffic on your network and through your routers. These concepts are Subnets, Subnet Masks, Variable Length Subnet Masking, and Classless Inter-Domain Routing (CIDR).

It is important that you have a thorough understanding of your existing network, because the network infrastructure must be input into VitalQIP.

Note: More information on how network types are defined and how variable-length subnet masks are applied can be found in the *Administrator Reference Manual*.

Subnets

A subnet is a portion of a network that shares a common address component. For example, a subnet could be defined as all devices with IP addresses that start with 100.100.100, all part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons. IP network addresses are divided into subnets based on the number in the first octet and a “Subnet Mask”.

Subnet masks

A mask is a filter that selectively includes or excludes certain parts of an address, and is used to determine what subnet an IP address belongs to, or what network a subnet belongs to.

The mask is a configuration parameter used by a TCP/IP end-node and IP router to determine what part of the IP address represents the host. An end-node uses the mask value to determine whether the destination is directly reachable (on the same network) or remote (in which case the packet must be sent to a router since it cannot be sent directly to the destination).

Variable Length Subnet Mask (VLSM)

VLSM, the precursor to CIDR, lifts the restrictions of subnetting by relaying subnet information through routing protocols. This idea leads us directly to CIDR.

Traditionally, the Internet assigned “classes” of addresses: Class A, Class B, and Class C was the most common. Class A addresses are addresses with the first three digits as 1-126, Class B are 128-192, and Class C are 193-223. Each address has two parts: one part to identify a unique network and the second part to identify a unique host in that network. Another way the old Class A, B, and C addresses were identified was by looking at the first 8 bits of the address and converting it to its decimal equivalent.

Classless Inter-Domain Routing (CIDR)

Short for Classless Inter-Domain Routing*,* CIDR is a new scheme that replaces the older system based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses.

CIDR can be a replacement for the old process of assigning Class A, B and C addresses with a generalized network “prefix”. This makes it possible to use bitmask or Variable Length Subnet Mask (VLSM) within the block.

There are two reasons for the use of the CIDR protocol:

1. The current inventory of IP addresses is running out of IP addresses to assign, and a restructuring of IP address assignments (using CIDR) increases efficiency.
2. Global routing tables are at capacity. Using CIDR minimizes the route table entries with hierarchical routing aggregation.

Instead of being limited to network identifiers (or “prefixes”) of 8, 16, or 24 bits, CIDR currently uses prefixes anywhere from 1 to 32 bits. Thus, blocks of addresses can be assigned for networks as small as 2 hosts up to networks with over 2,048 M hosts, allowing for address assignments that much more closely fit an organization's specific needs.

A CIDR address includes the standard 32-bit IP address and information on how many bits are used for the network prefix. For example, in the CIDR address 206.13.01.48/25, the “/25” or 25-bit mask indicates the first 25 bits are used to identify the unique network, leaving the remaining bits to identify the specific host.

Subnetting on your VitalQIP network

In a traditional subnetted network, several restrictions apply, which have been lifted by CIDR. However, if older, non-CIDR routing protocols are in use, these restrictions must still be observed.

> **Note:** Refer to the *Administrator Reference Manual* for information on CIDR, Subnet Masks, and basic Subnetting. You can also refer to RFC 1517, RFC 1518, RFC 1519, RFC 1520, and RFC 1878.

A few things to keep in mind

– A subnet(s) can belong to more than one domain, however, there is only one Default Domain. This is a rule imposed by VitalQIP.

– Domains open as a hierarchical tree in the **Existing Domains List** of the Subnet Calculator: Managed Domains window, only if the **Display Domain Folders** option in the Administrator Profile is set to True. For more information on this option, refer to "Customize administrator menus" (p. 6-30), and "Domain folders" (p. 1-40).

Create a new network

Purpose

Use this procedure to create a new network.

Before you begin

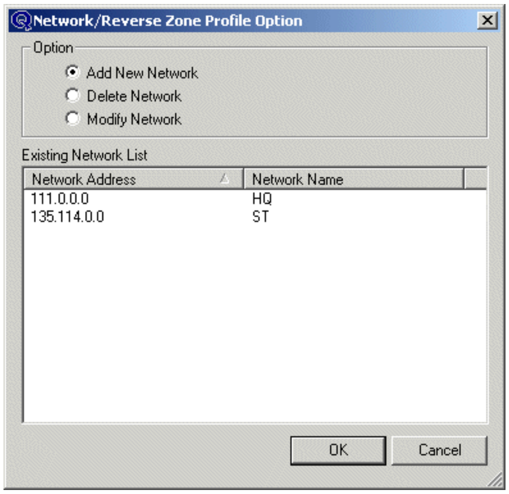
The Network Profile has several tabs: one for the actual Network Profile data, one for establishing **Network Warnings**, and one for establishing **Address Ranges** within the Network. When modifying or deleting a network, the **Reverse Zones** tab is also displayed.

The buttons along the bottom of the window apply to the network itself, whereas the buttons along the side apply to the creation or modification of the subnets within the network. Fill in the information for the Network Profile first and then create the subnets for the network.

Procedure

To create a new network, follow these steps:

1 Select **Network/Reverse Zone** from the **Infrastructure** menu. The Network/Reverse Zone Profile Option window opens.



Network/Reverse Zone Profile Option

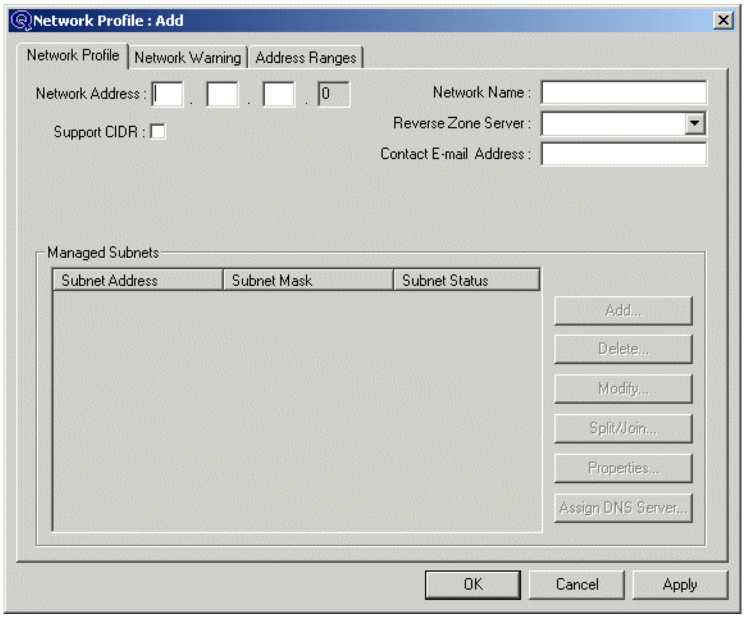
Option

● Add New Network
○ Delete Network
○ Modify Network

Existing Network List

Network Address	Network Name
111.0.0.0	HQ
135.114.0.0	ST

2 Select the **Add New Network** option and click **OK**. The Network Profile: Add window opens.



3 Fill in the fields as described in the following table.

Table 5-11 Network Profile fields

Field	Description
Network Address	This field identifies the network you are building. You can then assign subnets to this network. Enter the **Network Address** you want to define.
Support CIDR	The **Support CIDR** box is unchecked by default. If you wish to support CIDR, click the box. If **Support CIDR** is not checked, a network is created on traditional class A, B or C boundaries with subnets allowed below that boundary. If **Support CIDR** is checked, any network can be created.
Network Name	***Optional***. Assign a name to the network you are setting up. In addition, you can also modify the name of a network in this field. Network names must be unique within your organization.

Field	**Description**
Reverse Zone Server	***Optional***. Assign a **Reverse Zone Server** to this network. You can choose from a list of all DNS servers created through the Server Profile. Assigning a DNS server here identifies the Primary Reverse Zone server for this network.
Contact E-mail Address	This email address appears in the SOA record for the reverse zone. Any errors posted by DNS are sent to this email address. Selecting a Reverse Zone Server automatically displays the associated **Contact E-mail Address** from the server profile. Refer to "Enter email addresses" (p. 4-10) for formatting requirements.

4 Click **Apply**. A Confirmation prompt opens.

5 Click **OK**.

6 The **Managed Subnets** list is enabled and you can add one or more subnets to the network you have just created, as described in "Create subnets" (p. 5-59). Additionally, the Reverse Zone is automatically created and the **Reverse Zone** tab appears in the Network Profile. Refer to "Reverse zones" (p. 5-71) for information on Reverse Zones.

END OF STEPS

Modify a network

Purpose

Use this procedure to modify a network profile.

Procedure

To modify an existing network, follow these steps:

1 Select **Network/Reverse Zone** from the **Infrastructure** menu. The Network/Reverse Zone Profile Option window opens.

2 Select the **Modify Network** option and highlight the network you wish to modify.

3 Click **OK** and the profile for the network opens.

4 Modify it as necessary and click **OK**. A Confirmation prompt opens.

5 Click **OK**. Once a network has been created, its base address cannot be modified regardless of the CIDR setting.

END OF STEPS

Delete a network

Purpose

Use this procedure to delete a network.

Procedure

To delete an existing network, follow these steps:

1. Select **Network/Reverse Zone** from the **Infrastructure** menu. The Network/Reverse Zone Profile Option window opens.

2. Select the **Delete Network** option and highlight the network you wish to delete.

3. Click **OK**. The Network Profile: Delete opens.

4. Click **OK** to delete it. A Question dialog box opens.

   Note: If you delete a network, all objects, subnets, reverse zones, pool, or block attached to the network are also deleted.

5. Click **Yes**. A Confirmation prompt opens.

6. Click **OK**.

END OF STEPS

Create subnets

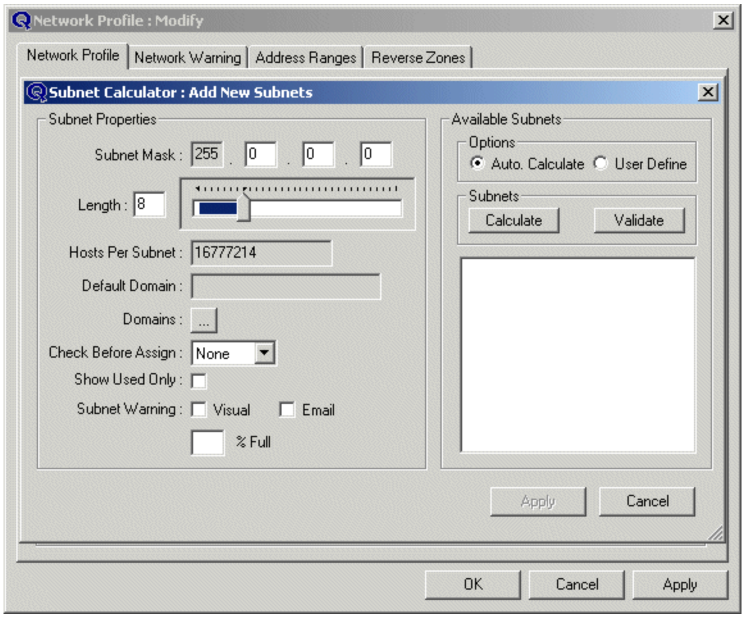
Purpose

Use this procedure to create subnets. You can have VitalQIP calculate subnets automatically with the Auto Calculate option, or define them yourself with the User Define option.

Procedure

To create subnets, follow these steps:

1 After you define a network and the **Managed Subnets** list is enabled, click **Add**. The Subnet Calculator: Add New Subnets window opens.



Subnet Mask : 255 . 0 . 0 . 0

Length : 8

Hosts Per Subnet : 16777214

Default Domain :

Check Before Assign : None

Show Used Only : □

Subnet Warning : □ Visual □ Email

% Full

Options: ● Auto. Calculate ○ User Define

2 To establish subnet properties, use the slider to create your **Subnet Mask**, **Length**, and **Host Per Subnet**. As you move the Subnet Mask slider to the right, the **Subnet Mask**, **Length**, and **Hosts Per Subnet** is shown. You may also enter the subnet length in the **Length** field or **Subnet Mask**; the **Subnet Mask**, **Length**, and **Hosts Per Subnet** is displayed accordingly.

3 Define the remaining subnet properties, as described in the following table.

Table 5-12 Subnet properties fields

Field	Description
Default Domain	The initial default domain in the Subnet Calculator window is empty until you click **...** next to the **Domains** field, and add one through the Managed Domains window. The domain you assign becomes the default domain for this listing of subnets. Other subnets in this network can have a different **Default Domain**. This is not a required field.
Domains	Click **...** to display a listing of available domains you can assign to the subnets. The Subnet Calculator: Managed Domains window opens. Select a domain as follows: 1. Expand the hierarchy, if needed, and select one or more from the list and click **Add**. The selected domains appear in the **Managed Domain List**. They do not display in a hierarchical format. The default domain displays next to the word "default" in the **Managed Domain List**. You can change the default domain in this window by highlighting another domain and clicking **Default**. Likewise, you can delete a domain from the Managed Domain List using **Delete**. 2. When you have selected a domain, click **OK**.
Check Before Assign	Lets you configure VitalQIP to check whether a static IP address is in use before it allows a user to allocate an address that is part of these subnets. ("Allocated" is taken to mean a state other than unused, that is, used, reserved, dynamically allocated, planned, or any form of Bootp or DHCP.) The options are "Ping" or "None". An address can be in use legally (if it was previously allocated) or illegally. VitalQIP performs this check by sending a Ping on static or manual-Bootp objects. If no reply is received to the Ping, the address is free to be assigned. Otherwise, a warning message opens that states the address is currently in use and asks if the user wants to allocate it. The message opens only when adding an object in the VitalQIP client and is not caused by DHCP handing out leases. For dynamic DHCP objects, you can configure the DHCP server to ping addresses before assigning them..
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". However, this can be overridden with the **View** menu in Object Management.

Field	**Description**

Subnet Warning	A warning is posted if the percentage of allocated IP addresses is greater than the percentage defined in this field. “Allocated” is taken to mean a state other than unused, that is, used, reserved, dynamically allocated, planned, or any form of Bootp or DHCP. If **Email** is checked, emails are sent to the email address in the Administrator Profile of all administrators assigned to manage the subnet.
	Note: On Windows platforms, you must enter a valid SMTP Host IP address in the *QSendMail.ini* file located in the system directory (the default value is *localhost*). For example:
	`[SendMail]`
	`SMTP Host=10.100.30.1`
	`IIS header=Yes`
	`Mime Encoding=Yes`
	`Return Path=sample@sample.com`

% Full	When the number of objects put into service for a subnet reaches the threshold defined in this field (from 0% to 99% full), an alarm is issued.

4 You can define your subnets using one of two options - **Auto Calculate** or **User Define**. **Auto Calculate** automatically determines the subnets for the new network, using the subnet mask. **User Define** allows you to define the subnets for the network. Refer to “Use the Auto. Calculate option” (p. 5-62) and “Use the User Define option” (p. 5-64) for information on each option.

5 Click **Apply**. The new subnet(s) opens in the **Managed Subnets** listing of the Network Profile.

END OF STEPS

Use the Auto. Calculate option

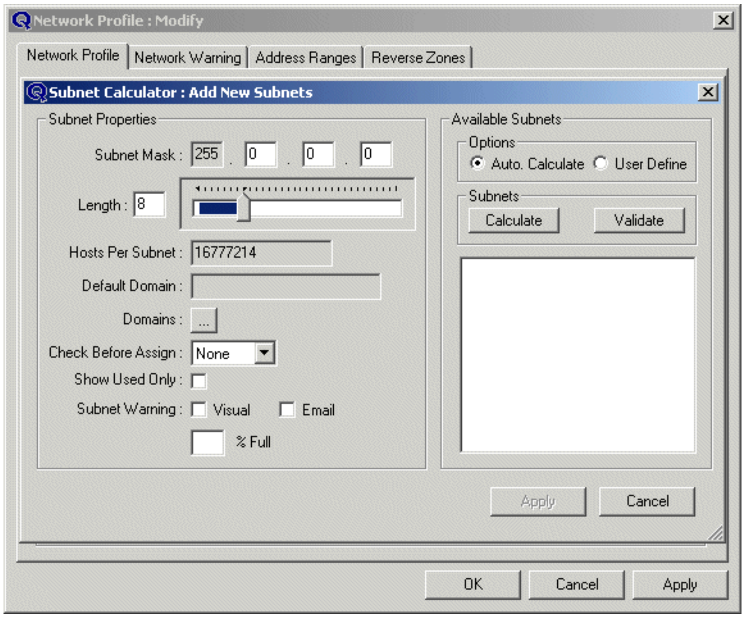
Purpose

Use this procedure to calculate subnets automatically.

Procedure

To calculate subnets automatically, follow these steps:

1 When the Subnet Calculator: Add New Subnets window is displayed, click **Calculate**.



Network Profile : Modify

Subnet Calculator : Add New Subnets

Subnet Properties

Subnet Mask : 255 . 0 . 0 . 0

Length : 8

Hosts Per Subnet : 16777214

Default Domain :

Check Before Assign : None

Show Used Only : □

Subnet Warning : □ Visual □ Email

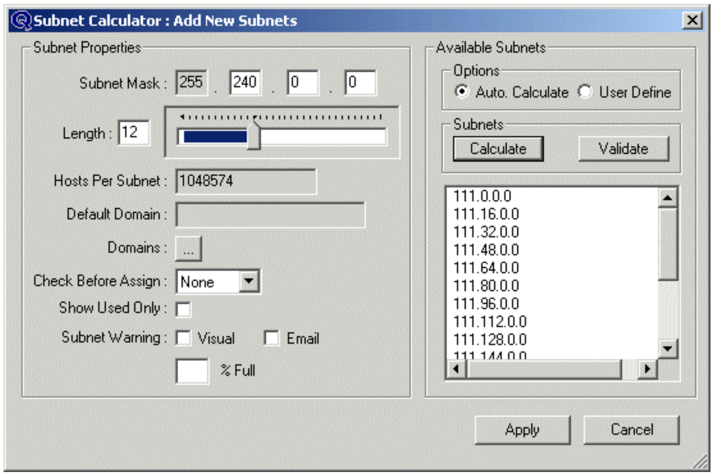
% Full

Available Subnets

Options

● Auto. Calculate ○ User Define

2 A list of all subnets that can be generated based on the **Subnet Mask/Length** appears.



Subnet Mask : 255 . 240 . 0 . 0

Length : 12

Hosts Per Subnet : 1048574

Default Domain :

Check Before Assign : None

Show Used Only : □

Subnet Warning : □ Visual □ Email

% Full

● Auto. Calculate ○ User Define

111.0.0.0
111.16.0.0
111.32.0.0
111.48.0.0
111.64.0.0
111.80.0.0
111.96.0.0
111.112.0.0
111.128.0.0
111.144.0.0

3 Select the subnet(s) you wish to calculate or valid1ate. (Multiple subnets can be selected using **Ctrl** or **Shift** and clicking the subnets.)

4 Click **Validate** to determine if the subnets are in use, or if the current administrator has privileges to create the selected subnets. If specific subnets are in use, the subnets are de-selected from the list.

5 Click **Apply** and the selected subnets are created. A Confirmation prompt opens.

6 Click **OK**. The subnets appear in the **Managed Subnets** list.

Note: Subnet Properties (for example, Default Domain, Check Before Assign, and so on) are applied to the subnets you select in the **Available Subnets** list. You can establish Subnet Properties before or after you calculate the Available Subnets.

END OF STEPS

Use the User Define option

Purpose

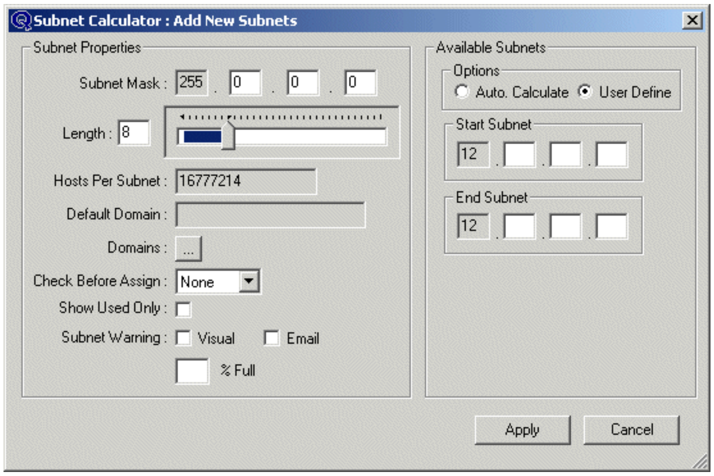
You can use the **User Define** option if you have a large network (Class A or B), and you wish to have more control over the addresses of the subnets to be created.

> **Note:** These addresses cannot be validated (**Validate** is disabled). Thus, if any of the subnets overlap, *no* subnets in the range are created.

Procedure

To calculate subnets manually, follow these steps:

1 When the Subnet Calculator: Add New Subnets window is displayed, click **User Define**. The Subnet Calculator: Add New Subnets window opens.



Subnet Calculator : Add New Subnets

Subnet Properties

Subnet Mask : 255 . 0 . 0 . 0

Length : 8

Hosts Per Subnet : 16777214

Default Domain :

Check Before Assign : None

Show Used Only : □

Subnet Warning : □ Visual □ Email

% Full

Available Subnets

Options: ○ Auto. Calculate ● User Define

Start Subnet: 12 . . .

End Subnet: 12 . . .

2 Enter the **Start Subnet** and **End Subnet**. The Start Subnet is the address of the first subnet to be created. The End Subnet is the address of the last subnet to be created.

3 Click **Apply** and a range of subnets is created based on the Start and End Addresses. A Confirmation prompt opens.

4 Click **OK**. The subnets appear in the **Managed Subnets** list.

END OF STEPS

Split or join subnets

Purpose

The Split/Join function is available on the Network Profile window. You can select a subnet that already exists in your network, and expand it further by splitting it into smaller subnets. Alternatively, you can join (or reduce) the number of subnet addresses on your network and use the space more efficiently. The only time a subnet can be joined is when you specify a subnet mask that applies to the subnets you want to join. For example, if you want to join the 10.1.1.0/24 subnet with the 10.1.2.0/24 subnet, you should specify that the new subnet have a mask of 23 bits; otherwise, the join will not occur. Both the splitting and the joining of subnets on your network are based on the **Subnet Mask** value.

Before you begin

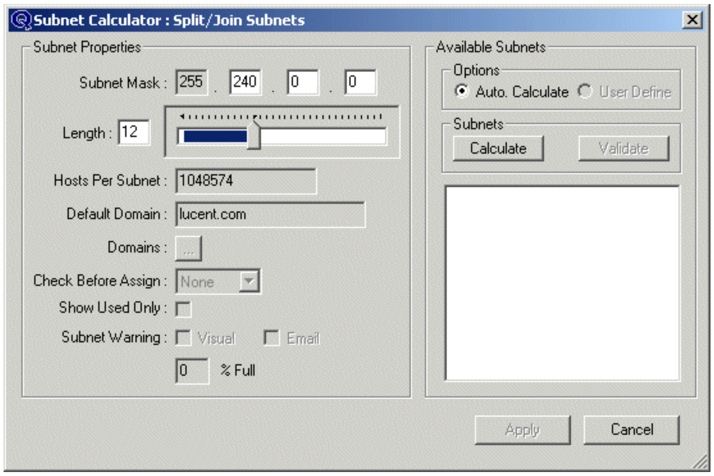
- If you join or split one or more subnets, the default router for the group may change.
- Subnets cannot be joined if two objects in the “destination” subnets have the same MAC address (because duplicate MAC addresses cannot exist in the same subnet).

Procedure

To join or split your subnets, follow these steps:

1 Select one or more addresses in the **Managed Subnets** list of the Network Profile window.

2 Click **Split/Join**. The Subnet Calculator: Split/Join Subnets window opens.



Subnet Calculator : Split/Join Subnets

Subnet Properties

Subnet Mask : 255 . 240 . 0 . 0

Length : 12

Hosts Per Subnet : 1048574

Default Domain : lucent.com

Domains : ...

Check Before Assign : None

Show Used Only : □

Subnet Warning : □ Visual □ Email

0 % Full

Available Subnets

Options

● Auto. Calculate ○ User Define

Subnets

3 Slide the calculator slider to the right to expand.

4 Click **Subnet Calculator**. A new list (based on the **Hosts Per Subnet** value) displays in the **Available Subnets** address list.

5 Highlight the addresses you want to add to the network with **Ctrl** or **Shift**, and click **OK**.

6 These joined or split subnet addresses are now part of your network.

Note: If you selected more than one subnet in the **Managed Subnets** list to split, the values displayed in the **Subnet Properties** section of the **Subnet Calculator: Split/Join Subnets** will not be recognized. You must select each of the new subnets in the **Managed Subnets** list, click **Modify** and re-establish the properties you want to apply to those subnets.

END OF STEPS

Assign a primary DNS server to one or more subnets

Purpose

You can assign a DNS server to one or more subnets in the **Managed Subnets** list. If it is not done here, you can assign a DNS server to subnets one at a time in the Subnet Profile.

Procedure

To assign a DNS server to a subnet, follow these steps:

1 Select one or more Subnet Addresses from the **Managed** list.

2 Click **Assign DNS Servers**. The Assign DNS Server dialog box opens.

3 Select a server from the **Primary DNS Server** drop-down list and click **Apply**.

END OF STEPS

Establish network warnings

The Network Warning tab shows the options for setting network warnings. If the number of objects put into service on this network reaches the threshold defined in this window, a warning is set off. Putting a subnet into service means to define at least one IP Address object within the subnet. The subnet is marked as “Used”.

Use the following calculation for defining warnings:

The number of used addresses ÷ the total number of addresses × 100 = the percentage (%).

“Used” addresses refer to all static, reserved, and (all types of) dynamic addresses. Refer to the following table for a description of the fields.

Table 5-13 Network warning fields

Field	Description

Warning Type	Select **Visual** to have the alarm delivered as a warning dialog box when a network warning threshold is reached.
	Select **Email** to have the alarm delivered as an email message sent to all administrators who manage this network and reverse zone. You can select both warning types.
	Note: On Windows platforms, you must enter a valid SMTP Host IP address in the *QSendMail.ini* file located in the system directory (the default value is *localhost*). For example:
	`[SendMail]`
	`SMTP Host=10.100.30.1`
	`IIS header=Yes`
	`Mime Encoding=Yes`
	`Return Path=sample@sample.com`

Warning Managed Addresses	When the number of addresses put into service for this Network area reaches the threshold defined in this field (from 0% to 99% full), an alarm will be issued.

Define address ranges for the network

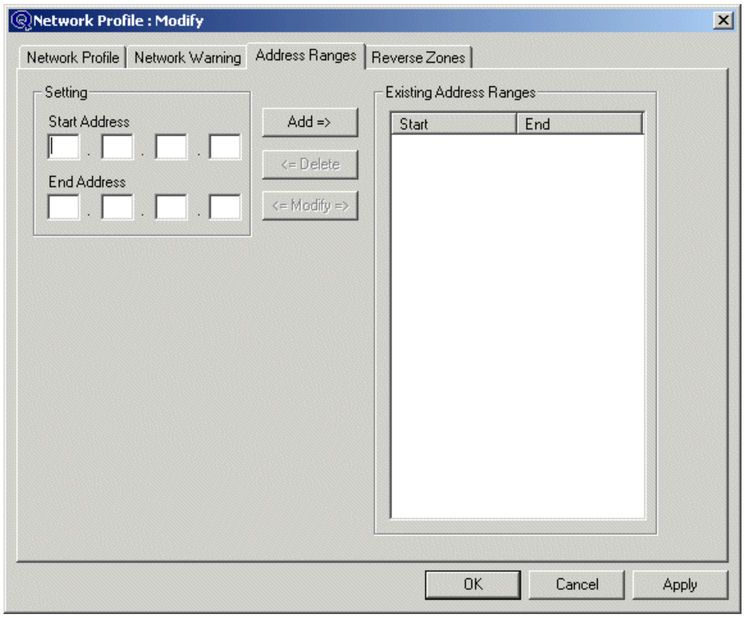
Purpose

The **Address Ranges** tab in the Network Profile allows you to add, delete, and modify address ranges within a specific network. Administrator profiles can be defined that allow administrators to create and manage objects within the assigned address ranges as part of their managed list.

Procedure

To establish address ranges, follow these steps:

1 Select the **Address Ranges** tab.



2 Define a starting subnet address (**Start Address**) and an ending subnet address (**End Address**) for each range.

3 Click **Add**. The established Range displays in the **Existing Address Ranges** list, along with any other established address ranges.

Once you have defined address ranges within the network, you can assign an administrator to manage that address range by adding it to a Managed List. Refer to "Create an administrator access list" (p. 6-23).

END OF STEPS

Reverse zones

Use the Reverse Zone function to establish reverse zones for your network and thereby allow:

- Multiple primaries for reverse zones of the same network
- Greater granularity for creating reverse zones

By default, VitalQIP builds reverse zone files based on the class of the network. The address-to-name lookup is sometimes referred to as reverse mapping. This function is used to override the default and allow a customer to establish a more granular zone creation.

Each network has its own file of one zone for the reverse mapping, regardless of the Class. For IPv4, the reverse network addresses delegate the IN.ADDR.ARPA records of a network. VitalQIP allows you to establish the reverse lookup of address-to-name files with the **Reverse Zone** function.

> **Note:** For IPv6 reverse zones, the Domain Profile is used to create IPv6 reverse zones. For more information, see "Create domain profile" (p. 5-13)

The Reverse Zone Profile is separate from the Domain setup to give you more flexibility. You may want to assign different values for the same parameters in this file than the ones in the name-to-address file. ***This is an optional setup function to give you more flexibility, but also requires a certain level of network administration knowledge to apply effectively.***

> **Note:** Any administrator who has read permissions on the reverse zone(s) associated network can see the zones, and anyone who has write permissions on the network can insert, modify, delete, or view the zones.

Set up a reverse zone

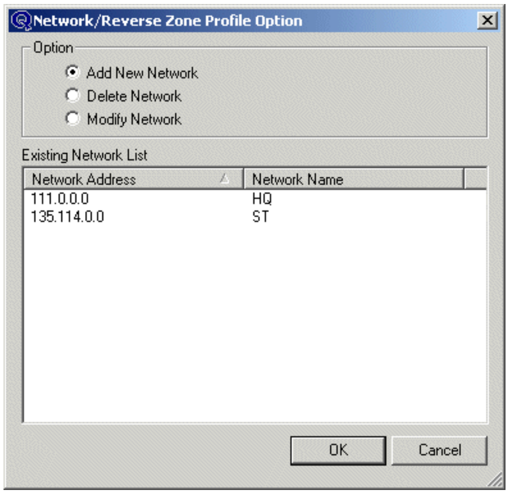
Purpose

Use this procedure to define a reverse zone on a network. This procedure is only for IPv4 reverse zones.

Procedure

To define a reverse zone, follow these steps:

1 Select **Network/Reverse Zone** from the **Infrastructure** menu. The Network/Reverse Zone Profile Option window opens.



Network/Reverse Zone Profile Option

Option

● Add New Network

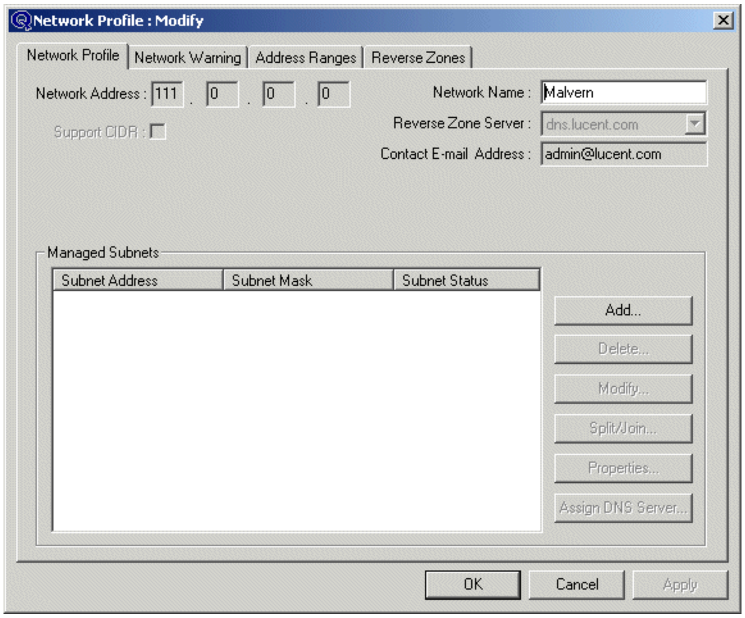
○ Delete Network

○ Modify Network

Existing Network List

Network Address	Network Name
111.0.0.0	HQ
135.114.0.0	ST

2 Select the network where you want to set up Reverse Zones and click **OK**. The Network Profile: Modify window opens.



Network Address : 111 . 0 . 0 . 0

Network Name : Malvern

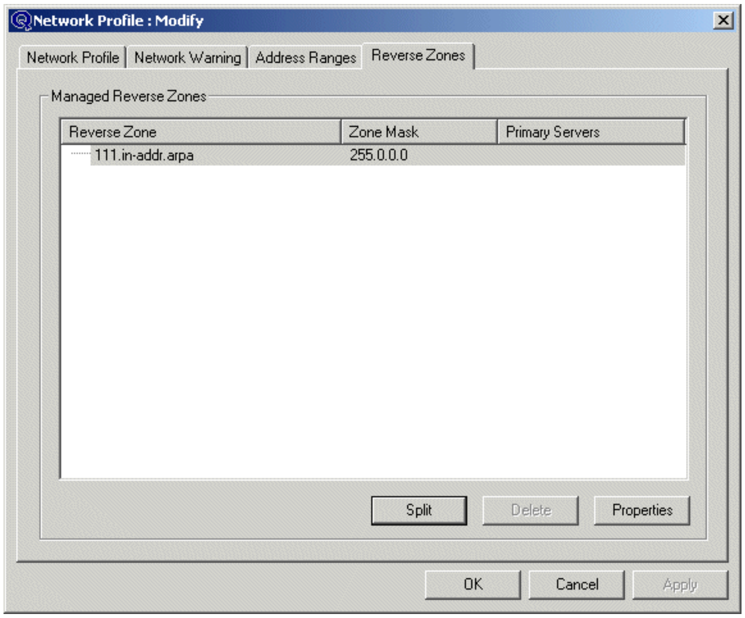
Reverse Zone Server : dns.lucent.com

Contact E-mail Address : admin@lucent.com

Support CIDR : ☐

Subnet Address	Subnet Mask	Subnet Status

3 Click the **Reverse Zone** tab and the reverse zones for that network are displayed.



Reverse Zone	Zone Mask	Primary Servers
111.in-addr.arpa	255.0.0.0	

4 You can now split, delete or view/modify the Reverse Zone Profile information through **Properties** for that Reverse Zone.

END OF STEPS

Split a reverse zone

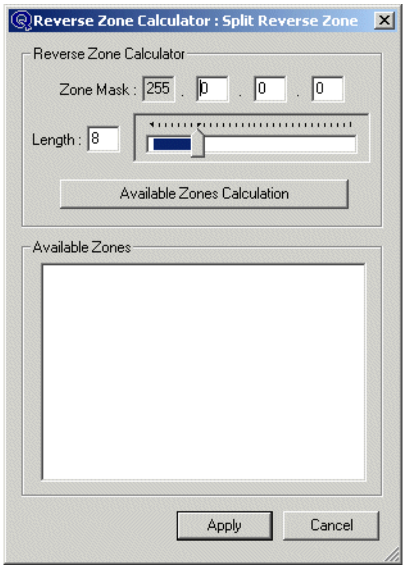
Purpose

Use this procedure to split a reverse zone. This procedure is only for IPv4 reverse zones.

Procedure

To split a reverse zone, follow these steps:

1 Select a Reverse Zone from the **Managed Reverse Zones** list, and click **Split**. The Reverse Zone Calculator : Split Reverse Zone window opens.



Reverse Zone Calculator : Split Reverse Zone
Reverse Zone Calculator
Zone Mask : 255 . 0 . 0 . 0
Length : 8
Available Zones Calculation
Available Zones
Apply
Cancel

2 Specify the **Zone Mask** field value.

The first octet in the **Zone Mask** ***is always*** greyed out. Use the slider to calculate the amount displayed in the **Length** field. As you move the slider, you decrease or increase the number of reverse zones available for this network. The octets change accordingly in the **Zone Mask** field.

3 Click **Available Zones Calculation**. This function calculates the number of reverse zones available to you for this network. The reverse zones open in the **Available Zones** list for this network.

4 Highlight one or more reverse zones in the Available Zone(s) list, and click **Apply**. The addresses you selected now open in the **Managed Reverse Zones** listing in the Reverse Zone Profile window.

You can further expand these zones by highlighting one (or more) of the new zones you created and clicking **Split** again. You can once again use **Available Zones Calculation** and create more reverse zones.

Note: You cannot have a delegated reverse zone for the same server or parent.

END OF STEPS

Review and modify reverse zone properties

Purpose

Use this procedure to review and modify reverse zone settings. This procedure is only for IPv4 reverse zones.

Procedure

To review or modify reverse zone settings, follow these steps:

1 Select the network for the reverse zone you wish to review.

2 Click **Properties**. The Reverse Zone Profile window opens.

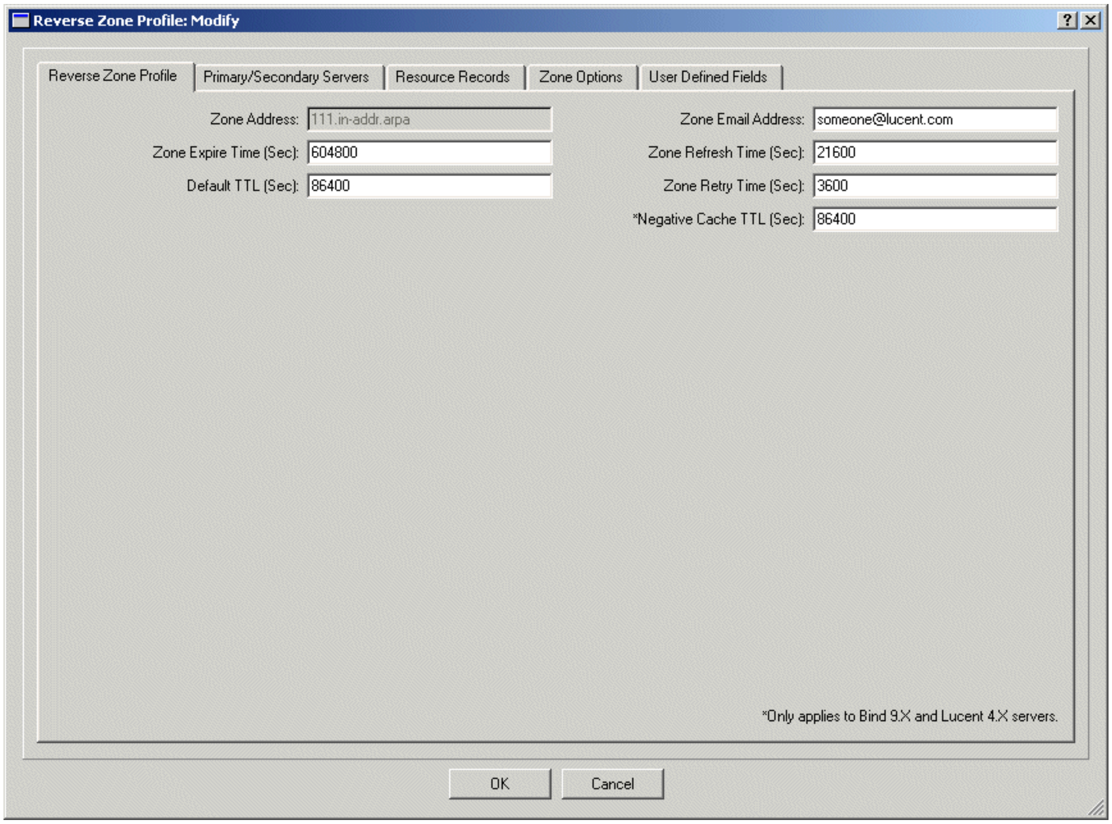
Note: One Reverse Zone exists automatically for each network. The Reverse Zone Profile is closely related to the Domain Profile, and they share similar parameters, only in reverse.

3 To review or modify reverse zone information, review the fields and tabs. The **Reverse Zone** field cannot be modified.

END OF STEPS

Review reverse zone information

The **Reverse Zone Profile** tab contains the zone email address and timing values for an IPv4 reverse zone. The timing values define when the Secondary Servers attempt to refresh their database. Each must be defined, and is measured in seconds. The system defaults normally suffice initially; you can fine-tune them as you gain experience with the network. These timing values are associated with the Primary (authoritative) Server. If the same primary server is defined for multiple domains, the timing values are the same throughout the different domains. If the same host is used as a primary server to multiple domains, it must use a different primary server name for each domain that has different timing values.



Zone Address: 111.in-addr.arpa
Zone Expire Time (Sec): 604800
Default TTL (Sec): 86400
Zone Email Address: someone@lucent.com
Zone Refresh Time (Sec): 21600
Zone Retry Time (Sec): 3600
*Negative Cache TTL (Sec): 86400

*Only applies to Bind 9.X and Lucent 4.X servers.

To establish reverse zone information, refer to the descriptions in the following table.

Table 5-14 Reverse zone information fields

Field	Description
Zone E-mail Address	***Required.*** Any errors posted by DNS are sent to this email address. You must have a value for this field. Refer to "Enter email addresses" (p. 4-10) for formatting requirements.

Field	Description
Zone Expire Time (Sec)	***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).
Zone Refresh Time (Sec)	***Required.*** The refresh time dictates how often the secondary server should verify its data. The default is 21,600 seconds (six hours).
Default TTL (Sec)	***Required.*** The default TTL defines the time interval for other servers to cache all resource records in the database file. The TTL (Time To Live) is supplied with query responses. The default value is 86,400 seconds (one day).
Zone Retry Time (Sec)	***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).
Negative Cache TTL (Sec)	***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.

Review/define primary and secondary servers

Purpose

Select the **Primary/Secondary Servers** tab to review the Primary and Secondary Domain Servers or “slaves” that manage the IPv4 Reverse Zone. These servers would manage the Reverse Zone you identified in the Domain Profile. All existing DNS server(s) appear as you defined them in the Server Profile, and you can add them to the **Selected DNS Server(s) List** as either primary servers or secondary servers.

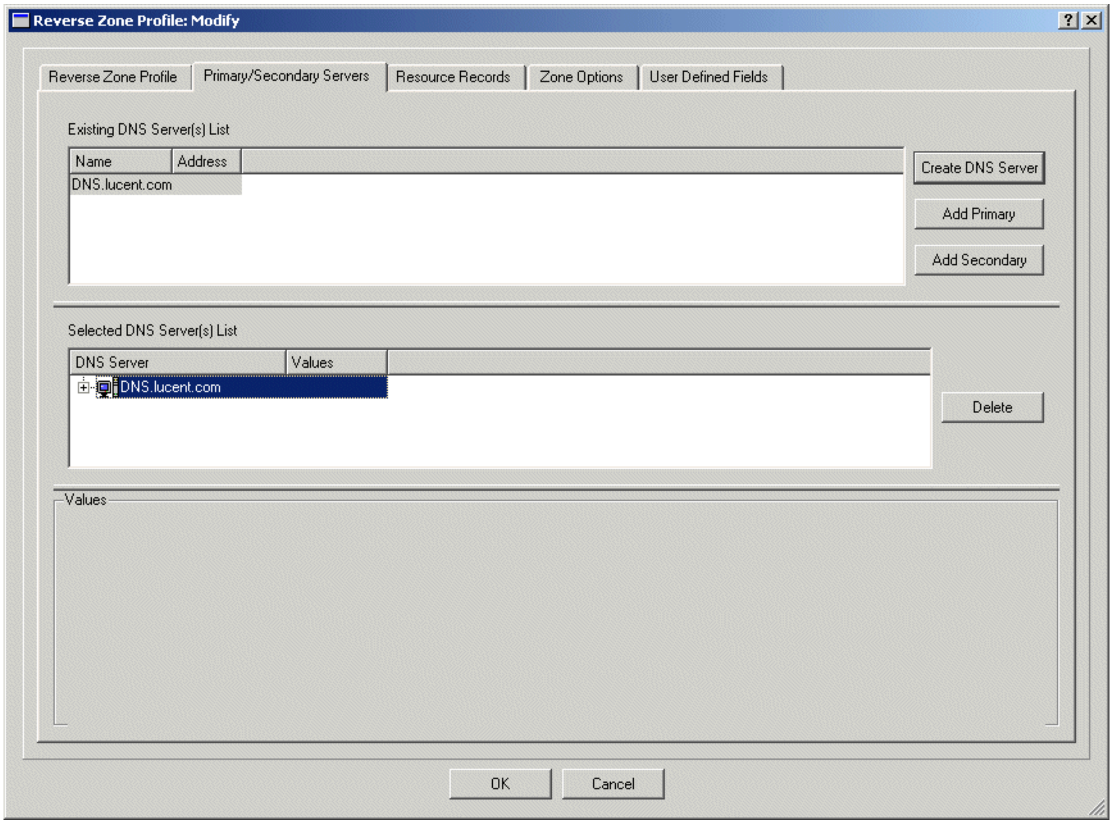
Before you begin

- For VitalQIP, it is a good idea to have at least one Primary Server defined for all Domains, although VitalQIP does allow you to have a domain defined without adding a Primary Server.
- Although it is possible, VitalQIP does not recommend that you have more than one Primary Server per Reverse Zone.
- If you chose to define multiple primary servers for a domain, you can associate the same secondary to multiple primaries; VitalQIP will correctly create the files.

Procedure

To define another primary/secondary server, follow these steps:

1 Select the **Primary/Secondary Servers** tab:



2 Remove the currently assigned primary server from the **Selected DNS Server(s) List**. Select the primary server and click **Delete**.

3 Add a different Primary DNS server to this Reverse Zone. Select a DNS server from the **Existing DNS Server(s) List** and click **Add Primary**. The server is added to the **Selected DNS Server(s) List** as a primary server managing this reverse zone.

4 If desired, you can change the Zone Options. Click on the server to expand it, and select the **Zone Option**. A field appears in the Values section. You select **User Zone Value** or **Customize**.

If you select **Customize**, the zone values appear in the tree. You can change the Zone Option values as desired. Click on the Zone Option to see the values. See the following table for more information about the Zone Options.

Table 5-15 Zone options

Zone options	Values
Extensions	See "Extensions zone options" (p. 5-27).
BIND-8.XOptions	See "BIND 8.X zone options" (p. 5-28).
BIND-9.X Options	See "BIND 9.X zone options" (p. 5-31).
Lucent DNS 3.X Options	See "LUCENT DNS 3.X zone options" (p. 5-35).
Lucent DNS 4.X Options	See "LUCENT DNS 4.X zone options" (p. 5-38).
Windows 2003 DNS Options	See "Windows 2003 DNS Zone Options" (p. 5-42).

The icon indicates that the server in the **Selected DNS Servers List** is secure for the current zone. If the server has been defined with the **Secure DNS Updates** parameter set to True in the Server Profile, it appears with a key/server icon and you can enable secure DNS updates by setting the **Send Secure Updates** parameter to True. For more information on setting up secure DNS, refer to "Secure dynamic updates support" the *Administrator Reference Manual*.

5 You can add one or more DNS server(s) as secondary servers to manage the reverse zone. They must be hierarchically associated with a Primary Server. To add Secondary DNS Servers to the Reverse Zone, highlight the servers you wish to add as secondary servers in the **Existing DNS Server(s) List** *and* highlight the primary server in the **Selected DNS Server(s) List** to which you wish them to be secondary, then click **Add Secondary**.

END OF STEPS

Reverse zone resource record setup

The **Resource Records** tab allows you to create, modify, and delete Resource Records for an IPv4 reverse zone. This option allows resource records for the reverse zone to be written to the configuration file. VitalQIP validates and formats the information on input.

> **Note:** The **Resource Record** tab appears only if the Administrator has the "Create Resource Record" privilege set to True. Refer to "Administrators" (p. 6-11) for further information.

Whenever you select a Resource Record **Type** in the **Setting** section in the lower portion of the window, the **Data** control is updated to allow for the correct formatting of the data associated with the selected type.

Once you input all the required information, click **Add**, and the Resource Record is displayed in the upper portion of the window.

To modify a Resource Record in the listing, select it, click **Modify**, and alter the values in the lower portion accordingly.

Likewise, to delete a Resource Record in the list, select it and click **Delete**.

Whenever an A record is modified in the Domain Profile, an additional PTR record is created in the Reverse Zone if the **Create PTR record for Rev Zone** check box is checked. The earlier PTR records, however, are not deleted from the Reverse Zone and need to be removed. Similarly, when an A record is deleted from the Domain Profile, the associated PTR record is not automatically removed from the Reverse Zone and needs to be removed.

> **Note:** VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and the profile cannot be saved while the conflict exists. This feature can be disabled by setting the **Validate CNAMES** sub-policies to False. These polices are under the **Validate CNAME Records** policy. See "General policies" (p. 3-29) for more information on the policy. When records other than CNAME records are added or modified, validation checks are made against:
>
> - Object aliases
> - CNAME object resource records
> - CNAME domain resource records
> - CNAME reverse zone resource records
>
> When CNAME records are added or modified, validation checks are made against:
>
> - Object aliases
> - Domain names
> - Any Object Profile resource records

- Any Domain Profile resource records
- Any Reverse Zone resource records
- ENUM NAPTR resource records
- IPv6 node names
- MX records

Note: The contents of the **Resource Records** tab are not validated in the same way as the contents in the Object Profile, such as the **Alias** and **Mail** tabs. If erroneous information is entered into the **Resource Records** tab, the erroneous information is entered into the zone and could cause errors with the loading of the zone. For information on proper usage and syntax, see *DNS and BIND* by Paul Albitz & Cricket Liu, published by O'Reilly & Associates.

Define reverse zone options

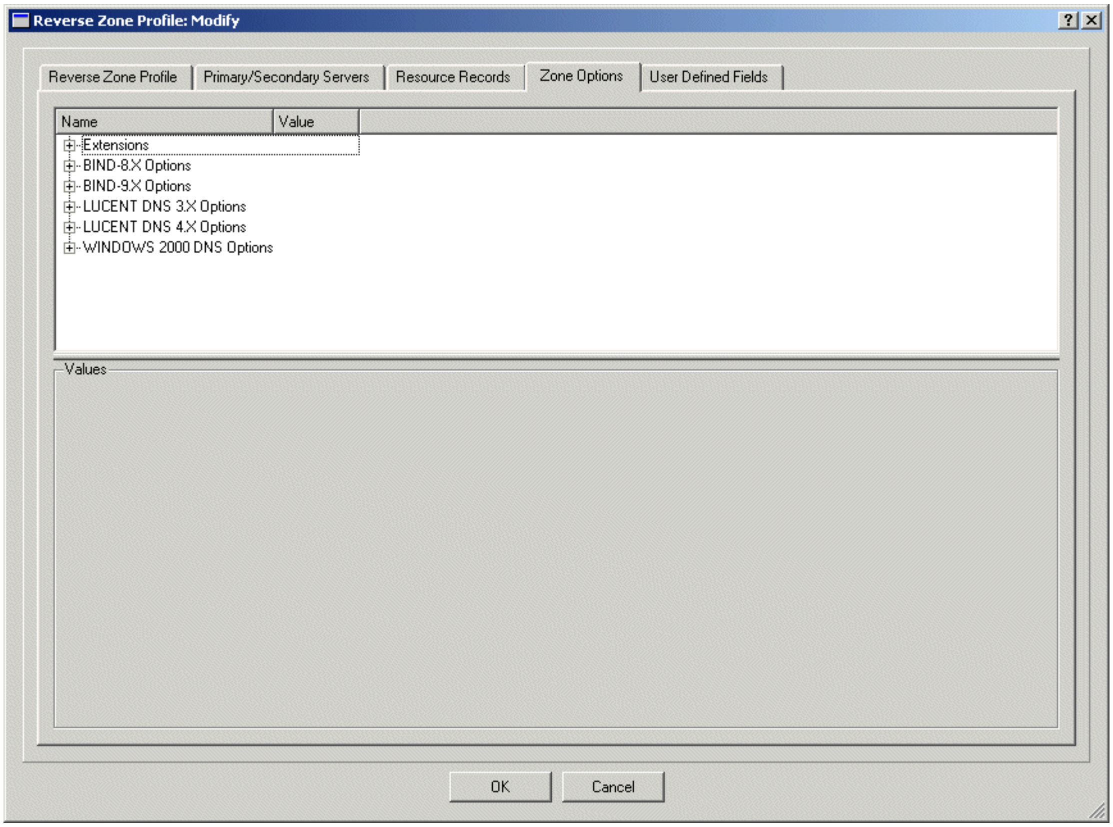
Purpose

Use this procedure to create reverse zone options. This procedure is only for IPv4 reverse zones.

Procedure

To create reverse zone options, follow these steps:

1 Select the Zone Options tab. The **Zone Options** tab opens.



2 Set up the reverse zone options. Refer to the specific tables referenced in the following table for further information.

Table 5-16 Zone options

Zone options	Values
Extensions	See "Extensions zone options" (p. 5-27).
BIND-8.XOptions	See "BIND 8.X zone options" (p. 5-28).
BIND-9.X Options	See "BIND 9.X zone options" (p. 5-31).
Lucent DNS 3.X Options	See "LUCENT DNS 3.X zone options" (p. 5-35).
Lucent DNS 4.X Options	See "LUCENT DNS 4.X zone options" (p. 5-38).
Windows 2003 DNS Options	See "Windows 2003 DNS Zone Options" (p. 5-42).

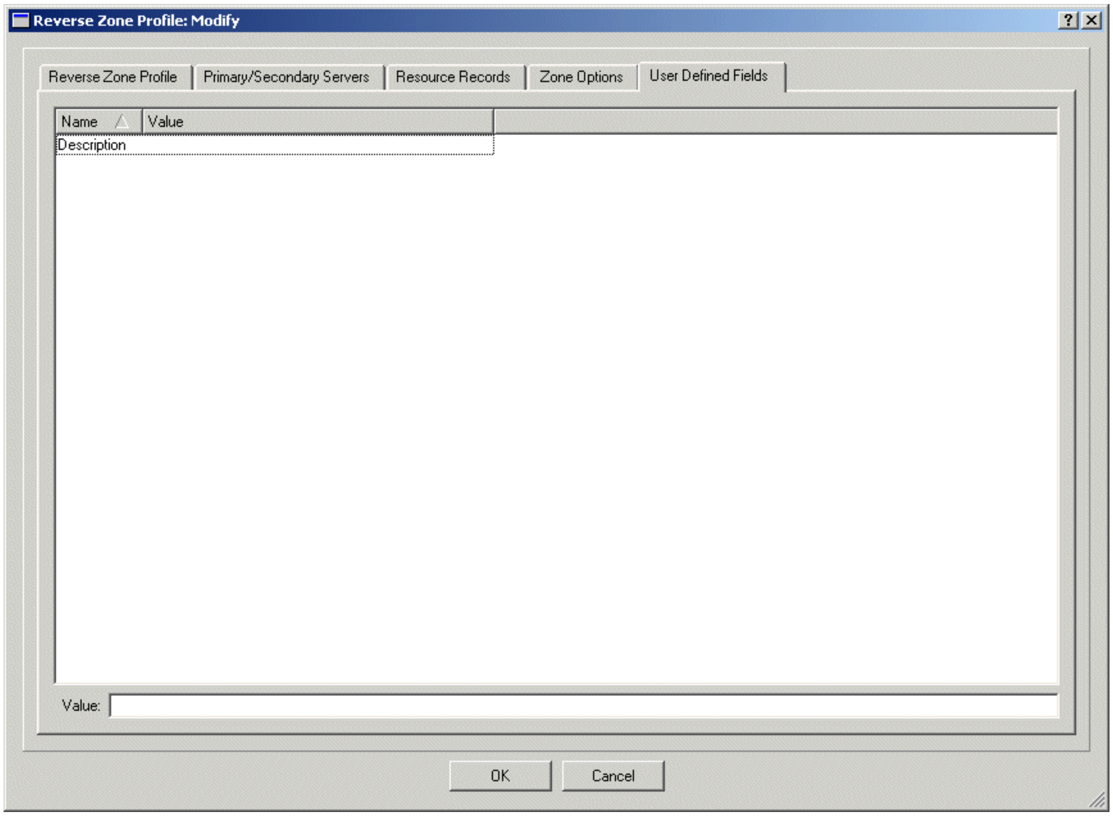
3 If you select **Use List**, you may select one or more ACL Templates and click **Add** to add a template to the Values list. To remove an ACL template address from the list, highlight the template and click **Delete**.

END OF STEPS

Reverse zone user-defined field setup

You can establish values for User-Defined fields for Reverse Zones in the **User-Defined Fields** tab.

> **Note:** The User-Defined Fields for Reverse Zones must first be defined in the **User-Defined Fields** function on the **Policies** menu.



OSPF areas

OSPF (Open Shortest Path First) is a protocol that defines how routers share routing information. Unlike the older Routing Information Protocol (RIP), which transfers entire routing tables, OSPF transfers only routing information that has changed since the previous transfer. As a result, it does not need to transfer as much data, which conserves bandwidth. The advantages of OSPF are:

- It is specifically designed to operate with larger networks
- It fully supports subnetting, including VLSM (Variable Length Subnetting) and non-contiguous subnets
- It uses small “hello” packets to verify link operation without transferring large tables

OSPF is independent of the VitalQIP network/subnet hierarchy. Setting up OSPFs in VitalQIP can help an organization manage the IP subnets and address ranges associated with OSPF areas.

OSPF explained

OSPF enables the flexible configuration of IP subnets. Each route distributed by OSPF has a destination and a mask. Two different subnets of the same IP network number may have different sizes (for example, different masks). This is commonly referred to as variable length subnetting (VLSM). A packet is routed using the best route (for example, longest or most specific match).

OSPF divides its routing domain into areas. Some users simply use OSPF Areas as a grouping mechanism within VitalQIP, and therefore, do not need the OSPF Area backbone, 0.0.0.0. Area 0.0.0.0, the backbone, is required only if you are using OSPF to create routes using VitalQIP and to meet the requirements of OSPF.

Using OSPF divides interior routing into two levels. If traffic must travel between two areas, the packets are first routed to the backbone. This may cause non-optimal routes, since inter-area routing is not performed until the packet reaches the backbone. Once there, it is routed to the destination area, which is then responsible for final delivery. This layering permits addresses to be consolidated by area, reducing the size of the link state addresses. Small networks can operate with a single OSPF area, which must be area 0.0.0.0.

Every subnet must belong to one OSPF area. Each router maintains a list of all the subnets in an area. If subnets are contiguous in an area, the number of entries in the router can be reduced. This is called “route summarization”. The rules for creating contiguous ranges of addresses are strict. A mask must be applied to the subnet to determine the start and ending addresses. This is called the “OSPF area mask”. VitalQIP can help you determine these parameters.

VitalQIP allows you to set up your OSPF areas in different ways. You can assign subnets to the OSPF area, or assign a range of addresses to the OSPF area, or you can do both. There are checks within VitalQIP that prevent you from assigning an address (as part of a range) that is already in another subnet, which could be assigned to another OSPF area.

You can set up your OSPF areas before or after you define your subnets. You cannot, however, assign subnets to your OSPF areas until your subnets are defined.

OSPF areas can be assigned their own administrators. An OSPF area administrator is only allowed to assign, reserve, and move objects in the OSPF area for which the administrator has been assigned.

Create an OSPF area

Purpose

Use this procedure to create an OSPF area. If you are a larger company, you will probably find it more convenient to have OSPF areas manage “ranges” rather than “subnets”.

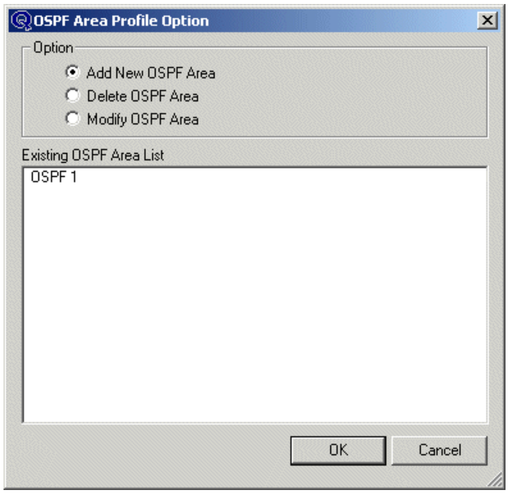
Before you begin

- A subnet cannot belong to more than one OSPF area. OSPF areas do not overlap. Even if you assign ranges to the OSPF area(s), you have essentially negated the subnet(s) from which those addresses came when that subnet has been assigned to an OSPF area.
- The VitalQIP graphical user interface allows you to define the OSPF Area Backbone (0.0.0.0), if you intend to use the OSPF Profile to create OSPF routes.
- A managed range is not required when adding an OSPF Area to VitalQIP.

Procedure

To set up an OSPF area, follow these steps:

1 Select **OSPF** from the **Infrastructure** menu. The OSPF Area Profile Option window opens.



OSPF Area Profile Option

Option

● Add New OSPF Area

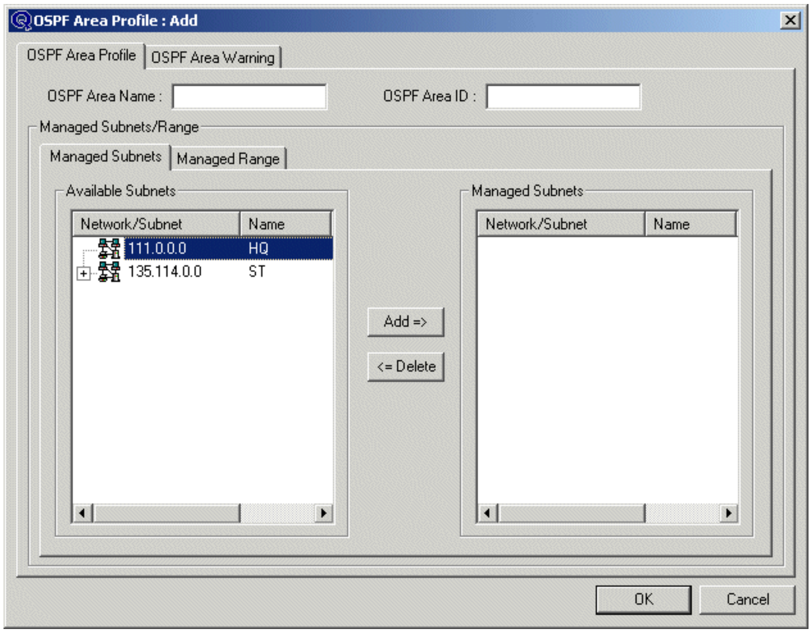
○ Delete OSPF Area

○ Modify OSPF Area

Existing OSPF Area List

OSPF 1

2 Select the **Add New OSPF Area** option and click **OK**. The profile for this OSPF Area Profile: Add window opens.



Available Subnets:

Network/Subnet	Name
111.0.0.0	HQ
135.114.0.0	ST

Managed Subnets:

Network/Subnet	Name

3 Enter the name for the OSPF area in the **OSPF Area Name** field. The name must be unique.

4 Enter a unique number in the **OSPF Area ID** field. Two OSPF Areas in the same organization cannot have the same OSPF Area ID.

5 Use the **Managed Subnets** and **Managed Range** sub-tabs to define the subnets or ranges that will manage the OSPF Area. Refer to “Manage subnets with an OSPF area” (p. 5-93) and “Manage ranges with an OSPF area” (p. 5-94).

6 Set up OSPF Area Warnings if desired (refer to “Establish OSPF area warnings” (p. 5-97)).

7 Click **OK** when you are ready to save the OSPF Area.

8 Click **OK** when the confirmation prompt opens.

END OF STEPS

Manage subnets with an OSPF area

Purpose

Use this procedure to assign the subnets to be managed in an OSPF area.

Procedure

To assign a subnet to an OSPF area, follow these steps:

1 Click the **Managed Subnets** sub-tab and highlight the subnets in the **Available Subnets** list that you want to manage with an OSPF area.

2 Click **Add**. The list of subnets in the **Managed Subnets** list are the subnets your specified OSPF area will manage.

To delete subnets from being managed by this OSPF area, highlight them in the **Managed Subnets** list and click **Delete**.

END OF STEPS

Manage ranges with an OSPF area

Purpose

Use this procedure to manage ranges with an OSPF area. Although it is more complicated to set up an OSPF area to manage ranges, it provides more flexibility and convenience, especially for companies with large networks.

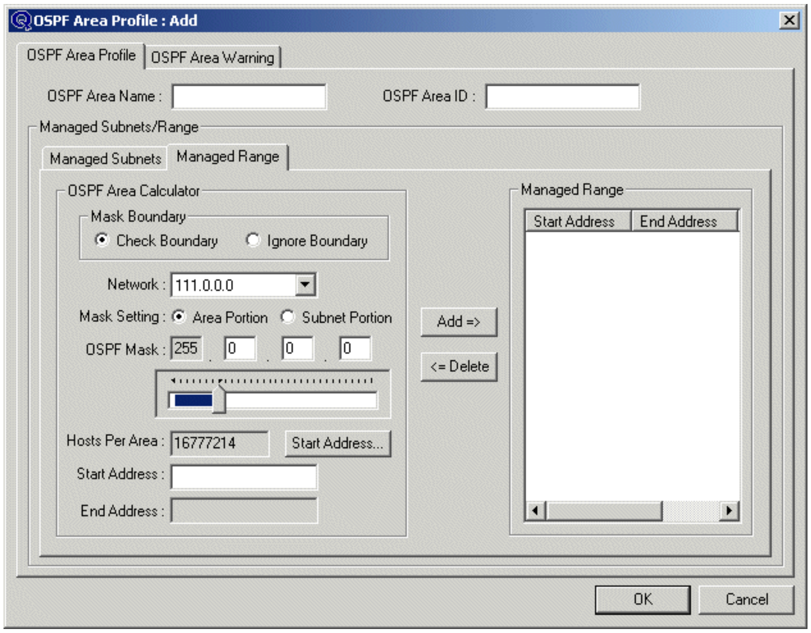
Before you begin

You can only use this option for subnets that have not yet been defined. If you have already defined subnets, use the “Managed Subnets” option.

Procedure

To set up a managed range with an OSPF Area, follow these steps:

1 Click the **Managed Range** sub-tab.



OSPF Area Profile : Add

Mask Boundary: ● Check Boundary ○ Ignore Boundary

Network : 111.0.0.0

Mask Setting : ● Area Portion ○ Subnet Portion

OSPF Mask : 255 . 0 . 0 . 0

Hosts Per Area : 16777214

2 To use the OSPF Area Calculator, refer to the descriptions of the fields in the following table and enter applicable values.

> **Note:** If you select on a range in the **Managed Range** list and click **Delete,** the **OSPF Area Calculator** portion of the window is repopulated. You can now re-use the slider

without filling in the profile again. If you click **OK** in the window, the range is truly deleted and you have to begin again.

Table 5-17 Managed range fields

Field	Description
Mask Boundary	**Mask Boundary** refers to the boundary (start and end) of the addresses that you will calculate (using the slider). The **Check Boundary** option disables the **End Address** field and calculates it for you based on what you put in the **Start Address** field and your **OSPF Mask** setting (using the slider). The **Ignore Boundary** option allows you to enter your own **Start Address** and **End Address**, disabling the ability to create an **OSPF Mask** setting (using the slider). Only the validity of the address is checked.
Network	Select a **Network Address** from the list of available network addresses in the drop-down list.
Mask Setting	This field requires some background regarding the relationship of OSPF areas and routers. IP address “ranges” for OSPF are used for route summaries (or link summaries) in OSPF. The **Mask Setting** in this window can be specified as using either the **Area Portion** (high-order bits) or the **Subnet Portion** (low-order bits), thus 255.255.255.0 and 0.0.0.255 would mean the same thing. Network Administrators may have entered the addresses in different routers with different formats (either high or low order). Select either **Area Portion** or **Subnet Portion** in this field.
OSPF Mask	***Required***. The mask indicates the number of areas that can be used for that network number. You can use the scroll bar following this field to scroll through the available OSPF area masks. For example, the network mask can be written as 255.255.128.0 or as 0.0.127.255. Both produce the same result.
Hosts Per Area	This field is automatically filled in with the maximum number of hosts possible in this OSPF area, given the selected mask.
Start Address	***Required***. Enter a Start Address as follows: 1. Click **Start Address...** to open the Start Address Selection window. 2. Select the Start Address for the OSPF area and click **OK**. The Start Address you selected appears in the **Start Address** field. 3. Click **Add** and the range appears in the **Managed Range** list. VitalQIP expands the network into OSPF areas based on the OSPF network mask.

Field	Description
End Address	***Required***. The end address automatically defaults to the last address in the area defined. It ***cannot*** be overwritten if the “Check Boundary” option is selected.

Establish OSPF area warnings

Purpose

Use this procedure to define the threshold at which a warning is issued. If the number of objects put into service on this OSPF area reaches the threshold defined in this window, a warning is set off.

Before you begin

Use the following calculation for defining warnings:

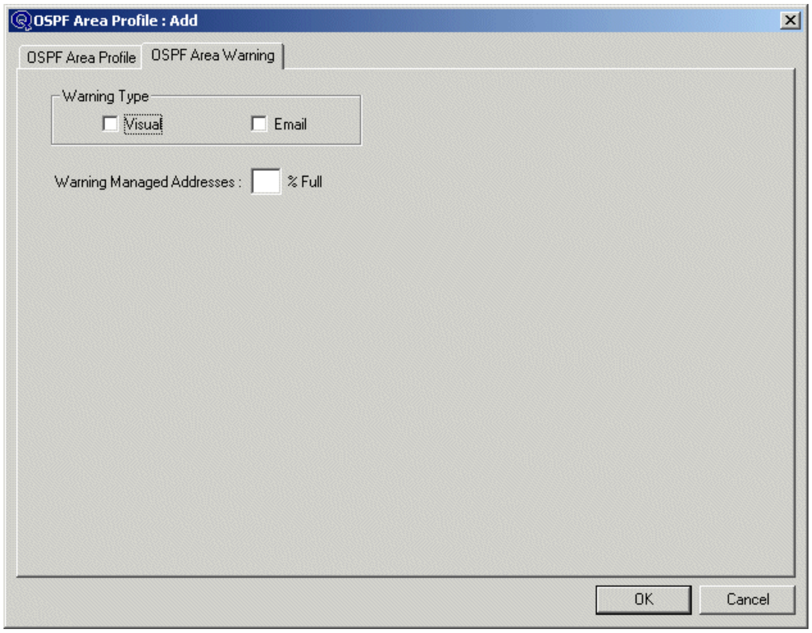
`Number of` *`used addresses`* `÷ Total number of addresses × 100 = Percentage (%)`

`Used addresses` refer to all static, reserved and (all types of) dynamic addresses.

Procedure

To set up OSPF area warnings, follow these steps:

1 Click the **OSPF Area Warnings** tab.



2 Set the OSPF Area warning fields described in the following table.

Table 5-18 OSPF area warning fields

Field	Description

Warning Type	Check **Visual** to have the alarm delivered as a visual warning to the screen when an OSPF Area warning threshold is reached.
	Check **Email** to have the alarm delivered as email sent to all OSPF administrators. You can select both warning types. If **Email** is checked, emails are sent to the email address in the Administrator Profile of all administrators assigned to manage the OSPF area.
	Note: On Windows platforms, you must enter a valid SMTP Host IP address in the *QSendMail.ini* file located in the system directory (the default value is *localhost*). For example:
	`[SendMail]`
	`SMTP Host=10.100.30.1`
	`IIS header=Yes`
	`Mime Encoding=Yes`
	`Return Path=sample@sample.com`

Warning Managed Addresses	When the number of addresses put into service for this OSPF area reaches the threshold defined in this field (from 0% to 99% full), an alarm is issued.

Modify an OSPF area

Purpose

Use this procedure to modify an existing OSPF area.

Procedure

To modify an existing OSPF Area, follow these steps:

1. Select **OSPF** from the **Infrastructure** menu. The OSPF Area Profile Option window opens.

2. Select the **Modify OSPF Area** option and highlight the OSPF area you wish to modify.

3. Click **OK** and the profile for the OSPF area you selected opens.

4. Modify it as necessary and click **OK**. A confirmation prompt opens.

5. Click **OK** in response to the confirmation prompt.

END OF STEPS

Delete an OSPF area

Purpose

Use this procedure to delete an OSPF area.

Before you begin

If you delete an OSPF area, all references to the OSPF area in the Subnet Organization are removed. No objects, subnets, or networks are deleted.

Procedure

To delete an existing OSPF area, follow these steps:

1 Select **OSPF** from the **Infrastructure** menu. The OSPF Area Profile Option window opens.

2 Select the **Delete OSPF Area** option and highlight the OSPF area you wish to delete.

3 Click **OK**. The OSPF Area Profile: Delete opens.

4 Click **OK** to delete the profile. A Warning prompt opens.

5 Click **Yes**.

6 Click **OK**.

END OF STEPS

Subnet organizations

The Subnet Organizations function provides a method for grouping one or more subnets based on geography or organization.

A single subnet cannot belong to more than one organization, nor does it have to belong to any 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 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.

Global Allocation Policy

You can use GAP (Global Allocation Policy) to apply rules regarding the assignment of addresses to objects to more than one subnet in a subnet organization.

For example, a Global Allocation Policy (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.

For information on setting up Global Allocation Policies, refer to "Apply Global Allocation Policies" (p. 5-105).

Windows 2003 Domain Controller Sites

You can use subnet organizations to define Windows Domain Controller Sites. Refer to "Set up a Windows 2003 site for a subnet organization" (p. 5-109).

Define a subnet organization

Purpose

Use this procedure to create a subnet organization.

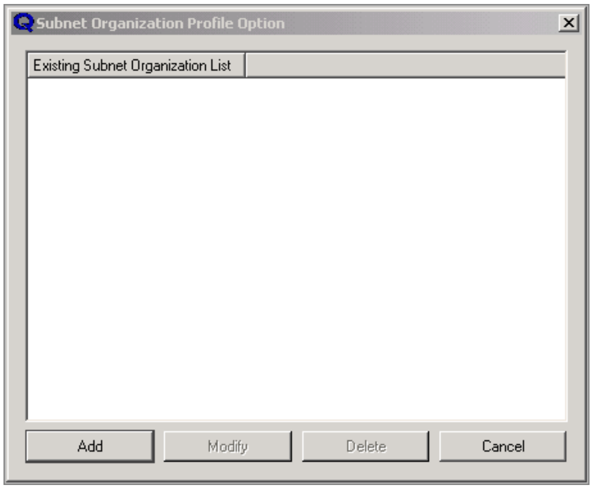
Before you begin

You can only choose from the **Available Subnets** list. If you want to expand or contract portions of the subnet(s), you must go back to the **Network Profile** function.

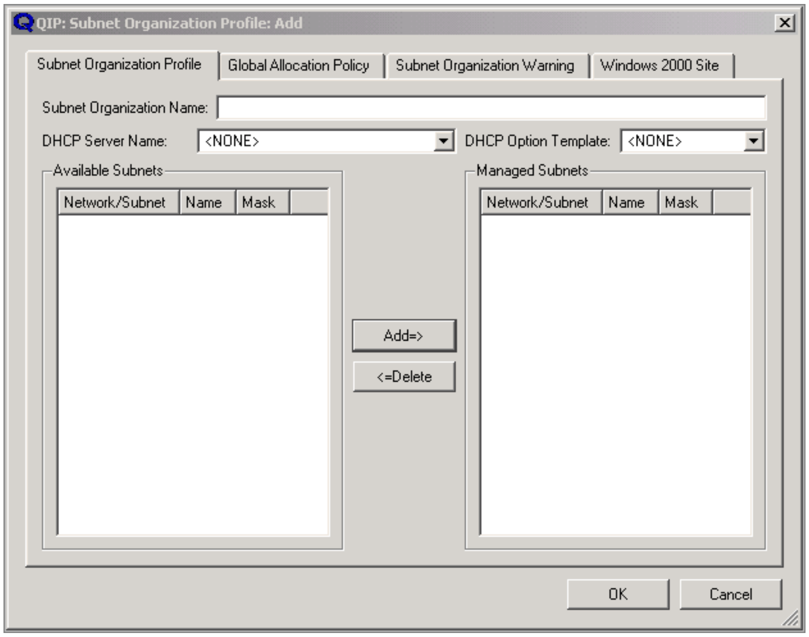
Procedure

To define a subnet organization, follow these steps:

1 Select **Subnet Organization** from the **Infrastructure** menu. The Subnet Organization Profile Option window opens.


Subnet Organization Profile Option
Existing Subnet Organization List
Add
Modify
Delete
Cancel

2 To add a new subnet organization, click **Add**. The Subnet Organization Profile: Add window opens.



3 Enter the **Subnet Organization Name** with which you would like to associate the subnets. It must be unique and cannot exceed 32 characters.

4 ***Optional***. If you wish to associate a specific DHCP server with the subnet organization, so that during the push process all objects in the managed subnets that have **Same as in Subnet Profile** selected in the subnet profile and **Same as in SubnetOrg Profile** selected in the object profile will take on the same DHCP server settings, select a DHCP server from the **DHCP Server Name** drop-down list.

5 ***Optional***. If you wish to associate a specific DHCP Option Template with the subnet organization, so that during the push process all objects in the managed subnets that have **Same as in Subnet Profile** selected in the subnet option template and **Same as in SubnetOrg Profile** selected in the object option template will take on the same DHCP Option Template settings, select an option template from the **DHCP Option Template** drop-down list.

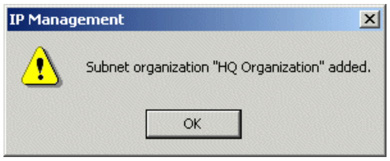
6 In the **Available Subnets** list, select the network or subnet (expand the network to list the subnet) you want to include in the subnet organization and click **Add**.

Note: If you select a network from the tree in the **Available Subnets** listing and click **Add**, all subnets in the Network are added to the **Managed Subnets** list, with the name of the network at the top of the tree. If you expand the tree and select only one subnet, it is added to the **Managed Subnets** list as a network, with only that subnet (with the same name) under it.

7 Repeat as necessary until all the subnets you wish to include are displayed in the **Managed Subnets** list. (Use **Delete** to remove any subnet incorrectly added.)

8 To refine your subnet organization profile, select another tab.

9 Click **OK**. A confirmation prompt opens.



Subnet organization "HQ Organization" added.

10 Click **OK**.

END OF STEPS

Apply Global Allocation Policies

Purpose

The Global Allocation Policy (GAP) function allows you to assign a particular object type to a particular address on each subnet in the subnet organization.

For 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. Therefore, if the 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
```

(The first and last address of each subnet is reserved for network and broadcast.)

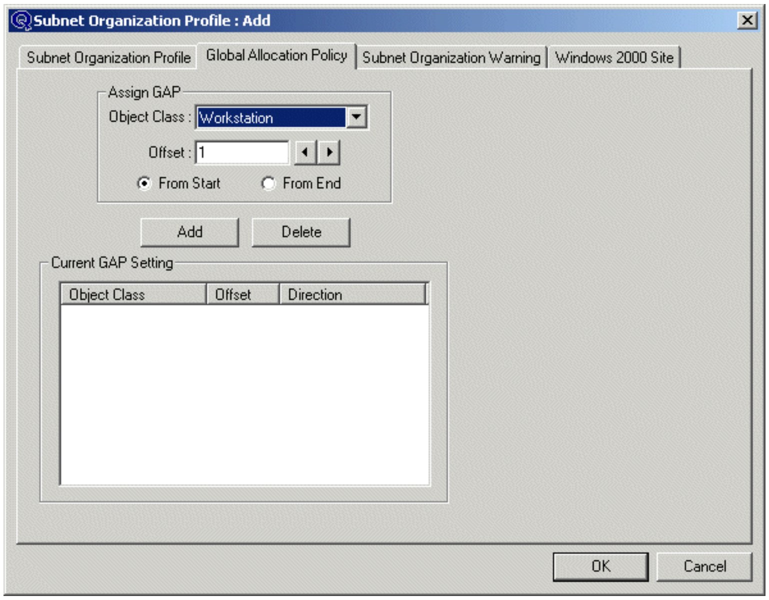
Before you begin

- 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 or deleted), all GAP objects become ***real*** objects within the Subnet (for example, the object status changes from Used (GAP) to Used). If you need to restore the subnet to the initial state with all original GAP entries set as they were when the subnet was defined, you must delete ***all*** objects within the subnet, close the subnet and then re-open it.
- A subnet must belong to a subnet organization to have a GAP assigned.
- If a subnet in an organization is too small for the GAP, the address index is not used.
- 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 Select the **Global Allocation Policy** tab.



Object Class : Workstation

Offset : 1

● From Start ○ From End

2 Select an object class from the **Object Class** drop-down list.

3 Select an **Offset** number. An **Offset** number determines the address within a range of addresses this type of object receives when it is added to the subnet organization.

4 Choose either the **From Start** or **From End** option. This determines the position as being from the start of the address range or from the end of the address range.

5 Click **Add**. To remove an object class from the **Current GAP Setting** list, select it and click **Delete**.

END OF STEPS

Set up a subnet organization warning

Purpose

Warnings can be posted for subnet organizations. A warning is posted if the percentage of allocated IP addresses is greater than the number defined on the warnings window. The total used addresses are divided by the “Allocated” addresses. “Allocated” means a state other than unused: used, reserved, dynamically allocated, planned, or any form of Bootp or DHCP.

Use the following calculation for defining warnings:

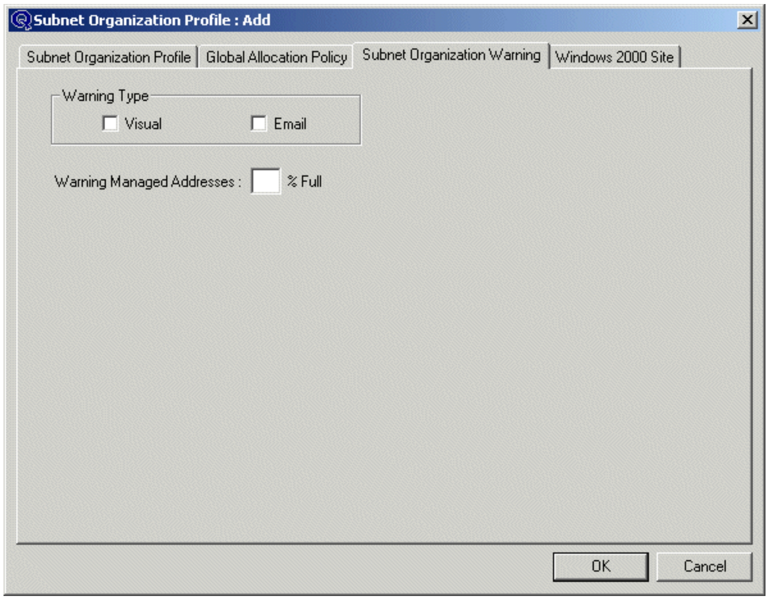
```
(Number of used addresses / Total number of addresses) x 100 =
   Percentage (%)
```

Used addresses refer to all static, reserved and (all types of) dynamic addresses.

Procedure

To set up a subnet organization warning, follow these steps:

1 Select the **Subnet Organization Warning** tab.


Subnet Organization Profile : Add
Subnet Organization Profile
Global Allocation Policy
Subnet Organization Warning
Windows 2000 Site
Warning Type
□ Visual
□ Email
Warning Managed Addresses :
% Full
OK
Cancel

2 Determine your **Warning Type**. Check **Visual** to have the alarm delivered as a visual message to the screen when a network warning threshold is reached. Check **Email** to have the alarm delivered as email sent to the subnet group administrator. You can select both warning types.

If **Email** is checked, emails are sent to the email address in the Administrator Profile of all administrators assigned to manage the subnet organization.

> **Note:** On Windows platforms, you must enter a valid SMTP Host IP address in the *QSendMail.ini* file located in the system directory (the default value is *localhost*). For example:

```
[SendMail]

SMTP Host=10.100.30.1

IIS header=Yes

Mime Encoding=Yes

Return Path=sample@sample.com
```

3 Enter a percentage (from 0 to 99) in the **Warning Managed Addresses** field. When the number of objects put into service for a subnet organization reaches the threshold, an alarm is issued.

END OF STEPS

Set up a Windows 2003 site for a subnet organization

Purpose

Use this procedure to set up a Windows 2003 site.

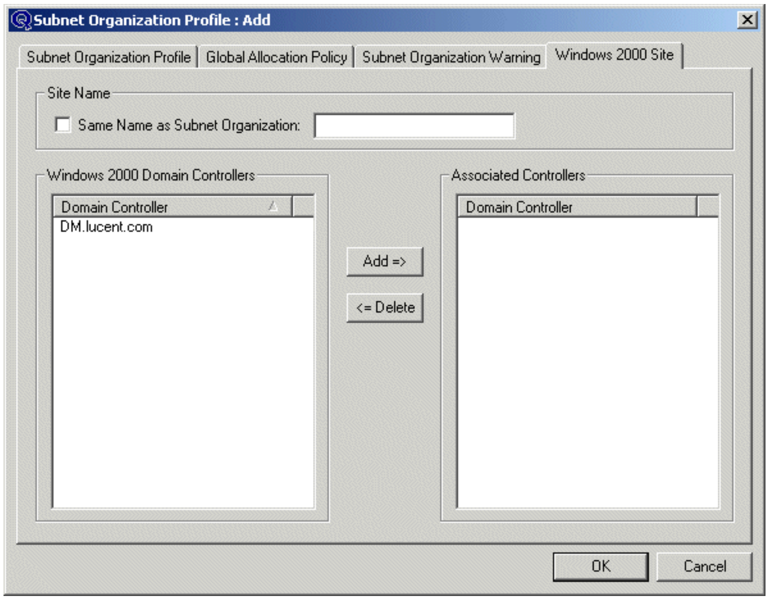
Before you begin

- To set up VitalQIP so that it can manage a Windows 2003 site, you need to establish a server as a Windows 2003 Domain Controller (refer to "Windows 2003 Domain Controller server type" (p. 4-66)). Once defined, it can be associated with the Windows 2003 Site in the **Windows 2003 Site** tab in the Subnet Organization profile.
- Define the global policy **Delete Sites/Subnets from Active Directory** (refer to Table 3-5, "General policies" (p. 3-29)). If set to True, it allows you to delete information from Active Directory whenever a subnet and/or subnet organization is deleted from VitalQIP. This 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 as well.

Procedure

To set up a Windows 2003 Site to be managed by VitalQIP, follow these steps:

1 Select the **Windows 2003 Site** tab.


Subnet Organization Profile : Add
Subnet Organization Profile
Global Allocation Policy
Subnet Organization Warning
Windows 2000 Site
Site Name
□ Same Name as Subnet Organization:
Windows 2000 Domain Controllers
Domain Controller
DM.lucent.com
Add =>
<= Delete
Associated Controllers
Domain Controller
OK
Cancel

2 Enter a **Site Name** for the site. This field is restricted to the characters a-z, A-Z, 0-9, and - . Blanks, periods, and names that consist of only numbers are not allowed. Active Directory is case insensitive, so you cannot create two site names that differ only in case.

3 Check the **Same Name as Subnet Organization** checkbox if the site has the same name as the subnet organization. If that name contains illegal characters, an error is generated and the subnet organization cannot be saved.

4 Choose one or more servers from the **Windows 2003 Domain Controllers** list and click **Add**.

To remove a controller from the **Associated Controllers** list, select it and click **Delete**. A message appears requesting that you confirm whether you wish to remove the site and associated subnets from Active Directory on that domain controller. Click **Yes** to remove it.

END OF STEPS

Modify a subnet organization

Purpose

Use this procedure to modify a subnet organization.

Before you begin

If at least one of the managed subnets has a DHCP Server Name and/or DHCP Option Template value set to **Same as in SubnetOrg Profile**, you cannot change a DHCP Server Name and/or DHCP Option Template to <NONE>.

Similarly, you cannot remove a subnet from a subnet organization if it has a DHCP Server Name and/or DHCP Option Template value set to **Same as in SubnetOrg Profile** and at least one dynamic object that has the same DHCP server and/or DHCP template set to **Same as in Subnet Profile**.

The Global Allocation Policy tab is disabled if an address template is associated with the Subnet Organization. You can associate an address template with a subnet organization using the VitalQIP web client.

Procedure

To modify an existing subnet organization, follow these steps:

1. Select **Subnet Organization** from the **Infrastructure** menu. The Subnet Organization Profile Option window opens.

2. Select the subnet organization you wish to modify from the **Existing Subnet Organization List** and click **Modify**. The Subnet Organization Profile: Modify window opens.

3. Modify as necessary and click **OK** to save your changes. A confirmation prompt opens.

4. Click **OK**.

END OF STEPS

Delete a subnet organization

Purpose

Use this procedure to delete a subnet organization.

Before you begin

- If a Subnet Organization is deleted, all references to the organization are removed. No objects, subnets, or networks are deleted, however.
- If a subnet is split or joined, it is automatically removed from the subnet organization.
- You cannot delete a subnet organization that has managed subnets in which the DHCP Server Name and/or DHCP Option Template value are set to **Same as in SubnetOrg Profile**.

Procedure

To delete an existing subnet organization, follow these steps.

1. Select **Subnet Organization** from the **Infrastructure** menu. The Subnet Organization Profile Option window opens.
2. Select the subnet organization you wish to delete from the **Existing Subnet Organization List**.
3. Click **Delete**. The Subnet Organization Profile: Delete window opens.
4. Click **OK** to delete the selected subnet organization. A Warning prompt opens.
5. Click **Delete**. A confirmation prompt opens.
6. Click **OK**.

END OF STEPS

Applications

Applications can be used to differentiate between departments, divisions, or any function that requires separate reporting. For example, applications can be used to assign special deployments to specific administrators. Another example is to reserve a range of addresses for application servers and allow certain server administrators access to only these ranges.

An application can be defined with any alphanumeric name, such as “accounting”. Any individual hostname or IP address can be assigned to an application. Reports can be generated by application. Normal subnet administrators can make application assignments. The application name is added by individual IP address.

Add an application

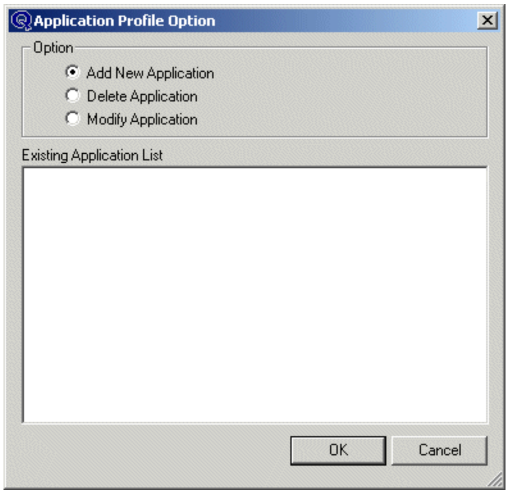
Purpose

Use this procedure to create an application.

Procedure

To add an application, follow these steps:

1 Select **Application** from the **Infrastructure** menu. The Application Profile Option window opens.



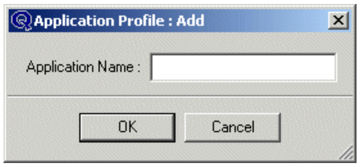
Application Profile Option

Option

● Add New Application
○ Delete Application
○ Modify Application

Existing Application List

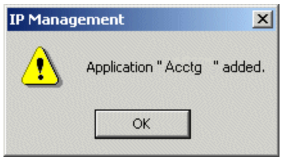
2 Select the **Add New Application** option and click **OK**. The Application Profile: Add window opens.



Application Profile : Add

Application Name :

3 Type the name for the application and click **OK**. A confirmation prompt opens.



Application "Acctg " added.

4 Click **OK**.

END OF STEPS

Modify an application

Purpose

Use this procedure to modify an application.

Procedure

To modify an application, follow these steps:

1 Select **Application** from the **Infrastructure** menu. The Application Profile Option window opens.

2 Select the **Modify Application** option.

3 Select the application you wish to rename and click **OK**. The Application Profile: Modify window opens.

4 Type the new name for the application and click **OK**. A Warning prompt opens.

5 Click **Yes**. A confirmation prompt opens.

6 Click **OK**.

END OF STEPS

Delete an application

Purpose

Use this procedure to delete an application.

Procedure

To delete an existing application, follow these steps:

1 Select **Application** from the **Infrastructure** menu. The Application Profile Option window opens.

2 Select the **Delete Application** option.

3 Select the application you wish to delete and click **OK**. The Application Profile: Delete window opens.

4 Click **OK**. If you have any objects assigned to the application, a warning appears, informing you that deleting an application can also remove all objects associated with the application.

5 If you answer **Yes**, all objects are removed along with the application. If you answer **No**, the application ID is set to NULL (blank) for any object that belonged to the deleted application. A confirmation prompt opens.

6 Click **OK**.

END OF STEPS

6 Manage administrators and users

Overview

Purpose

The purpose is to describe how to set up and manage VitalQIP administrators and users. It contain information on administrator roles, administrators, user groups, and users.

Contents

The following topics are covered:

Administrative roles	6-3
Create an administrative role	6-4
Modify an administrative role	6-7
Delete an administrative role	6-8
Check administrative role assignments	6-9
Administrators	6-11
Create an administrator profile	6-12
Create an administrator access list	6-23
Customize administrator menus	6-30
Modify an administrator profile	6-33
Delete an administrator profile	6-35
Assign an administrative role	6-36
User groups	6-39
Add a user group	6-40
Modify a user group	6-43
Delete a user group	6-44

Users and groups	6-45
Define VitalQIP users	6-46
Enter location information	6-49
Assign users to groups	6-51
Associate users with subnets	6-52
Associate users with managed ranges	6-53
Assign user-defined fields values	6-55
Modify a user profile	6-56
Delete a user profile	6-57
View user groups	6-58

Administrative roles

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.

Create an administrative role

Purpose

Use this procedure to create an administrative role.

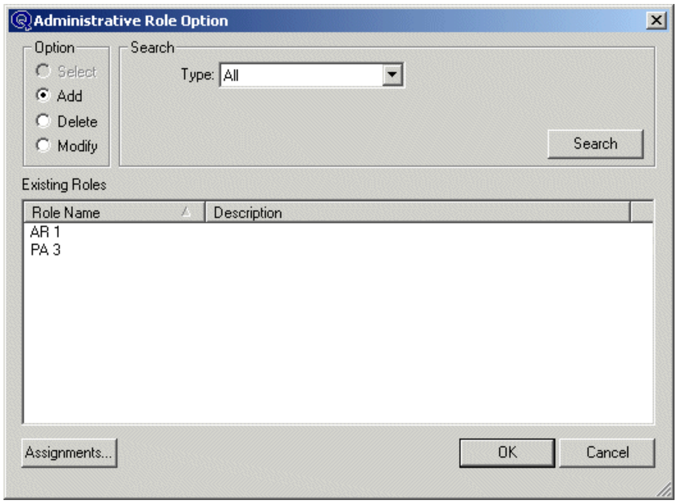
Before you begin

Only “Master” and “Organization” administrators can create administrative roles and the function is only available when the ‘Advanced’ GUI mode is assigned to the profiles for those administrator types.

Procedure

To create an administrative role, follow these steps:

1 Select **Administrative Role** from the **Infrastructure** menu. The Administrative Role Option window opens.



Administrative Role Option

Option: ○ Select ● Add ○ Delete ○ Modify

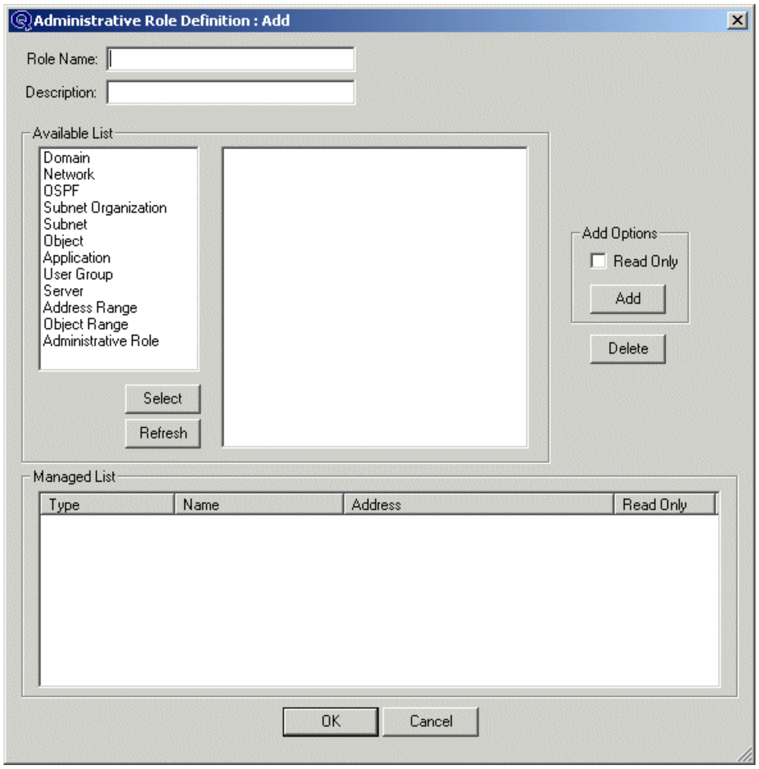
Search — Type: All

Existing Roles

Role Name	Description
AR 1	
PA 3	

2 Select **Add**.

3 Click **OK**. The Administrative Role Definition: Add window opens.



4 In the **Role Name** field, enter a unique name of up to 32 characters.

5 In the **Description** field, enter a description of up to 255 characters that clarifies the contents or purpose of the role.

6 Select the first component that you wish to add to the **Managed List** from the **Available List** and click **Select**.

7 The **Available List** box displays all infrastructure components to which you have access. If you wish to update the list, click **Refresh**. Use **Ctrl** and **Shift** to select whatever components you wish to add to the **Managed List**.

If you select **Administrative Role** from the **Available List** drop-down list you can copy and append the contents of one or more existing administrative roles to the **Managed List**. If there is a duplicate definition, a warning appears and you must choose one of the following:

Yes	Overwrite the current definition.
Yes (All)	Overwrite all duplicate definitions.
No	Retain the current definition.
No (All)	Retain all duplicate definitions in the **Managed List**.

8 Decide if you wish to restrict the selected components to be “Read Only” by selecting the **Read Only** box. Read access indicates the administrator can only ***view*** these segments of the infrastructure. The **Managed List** displays “True” for Read Only and “False” if the administrator has Write access.

> **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**.

> **Note:** If the same infrastructure component is contained within an assigned administrative role and the **Managed List**, and one definition is set to “Read Only” and the other is set to “Write”, the definition with “Write” capability prevails.

9 Click **Add** to add selected components to the **Managed List**. To remove a component you added in error, highlight it and click **Delete**.

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

11 Click **OK** to save the administrative role. A confirmation prompt opens.

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 laboriously updating each profile, you need only update a role and the updated role becomes visible for an administrator on his or her 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 has access to it.

Procedure

To modify an existing administrative role, follow these steps:

1 Select **Administrative Role** from the **Infrastructure** menu. The Administrative Role Option window opens.

2 Select the role you wish to modify from the **Existing Roles** list and click **OK**. The Administrative Role Definition: Modify window opens.

Note: If you need to display roles of a specific type, select an infrastructure type from the **Type** drop-down list and enter search specifications. Click **Search** to refresh the **Existing Roles** list so that it displays roles that match your search specifications.

3 Make the changes you need and when completed, click **OK**. A warning prompt opens.

4 Click **Yes**. A confirmation prompt opens.

5 Click **OK**.

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 **Administrative Role** from the **Infrastructure** menu. The Administrative Role Option window opens.

2. Select the **Delete** option and highlight the role you wish to delete in the **Existing Roles** list. Click **OK** and the Administrative Role Definition: Delete window opens.

3. Verify that the role is the one you want to delete and click **OK**. A warning prompt opens.

4. Click **Yes**. A confirmation prompt opens.

5. Click **OK**.

END OF STEPS

Check administrative role assignments

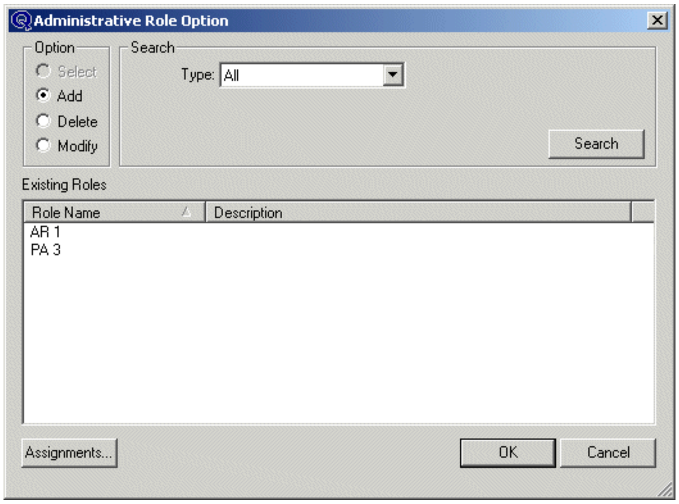
Purpose

Use this procedure to check assignments to administrative roles.

Procedure

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

1 Select **Administrative Role** from the **Infrastructure** menu. The Administrative Role Option window opens.



Administrative Role Option

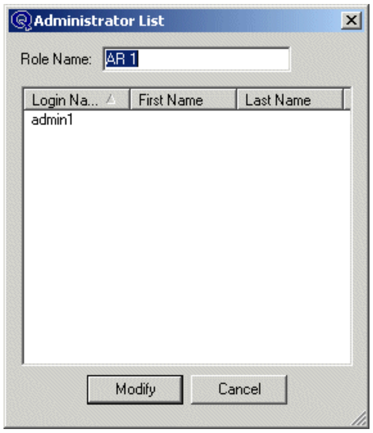
Option
○ Select
● Add
○ Delete
○ Modify

Search
Type: All

Existing Roles

Role Name	Description
AR 1	
PA 3	

2 Highlight the role you wish to check and click **Assignments**. The Administrator List window opens.

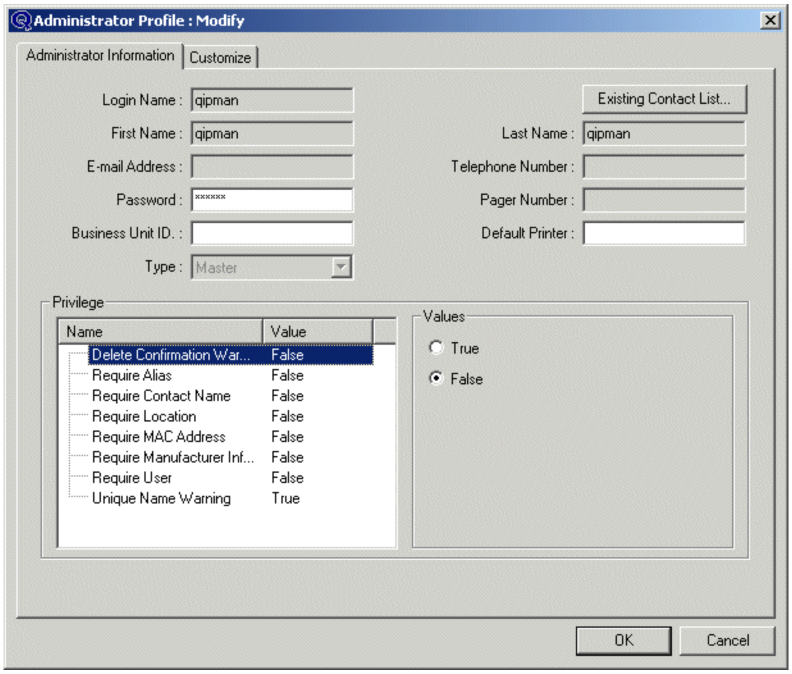


Administrator List

Role Name: AR 1

Login Na...	First Name	Last Name
admin1		

3 If you are a “Master” administrator and wish to modify an Administrator Profile in the list, select the **Login Name** and click **Modify**. The Administrator Profile: Modify window opens.



Login Name :	qipman		
First Name :	qipman	Last Name :	qipman
E-mail Address :		Telephone Number :	
Password :	******	Pager Number :	
Business Unit ID. :		Default Printer :	
Type :	Master		

Privilege

Name	Value
Delete Confirmation War...	False
Require Alias	False
Require Contact Name	False
Require Location	False
Require MAC Address	False
Require Manufacturer Inf...	False
Require User	False
Unique Name Warning	True

Values

○ True

● False

4 Make changes as needed and click **OK**. A confirmation prompt opens.

5 Click **OK**.

END OF STEPS

Administrators

You use the Administrator Profile to define the administrative policies, privileges, and roles of those individual(s) who are expected to manage the network or portions of the network, and to define what impact they have on their assigned portions.

Administrator information

In the **Administrator Information** tab, you define the different types of administrator and assign privileges to each administrator profile. The two types are Normal administrator and Master administrator.

Access information

In the **Access Information** tab, you define the components of the network for which the administrator is authoritative. The privileges you establish in the **Administrator Information** tab apply to ***all*** the selections you make in the **Access Information** tab. If you are setting up similar profiles for several administrators, you should consider defining an administrative role and assigning it to each profile. That way, if there are infrastructure changes to the network components assigned to the role, you need only update the administrative role and save yourself the trouble of having to update each administrator profile to reflect the modified infrastructure. For information on setting up administrative roles, refer to “Administrative roles” (p. 6-3).

Customization

In the **Customize** tab, you specify the menus that the administrator whose profile you are creating can access. You can also define how the Hierarchy appears when it is expanded by setting the Domain Folder and Quick View options.

Create an administrator profile

Purpose

Use this procedure to create a new administrator profile.

Before you begin

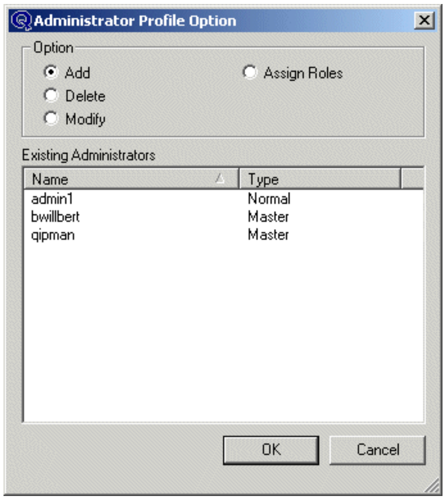
- Each Administrator name or ID must be unique. Delegated administrators can create other administrators.
- If you log in as a new administrator, you only see the domains, OSPF areas, subnets, subnet groups, networks, applications, objects, user groups, servers, address ranges, and object ranges assigned to you by the administrator who defined/created your Administrator Profile.
- If you see <LOCKED> in the title bar of the **Administrator Information** tab in the administrator profile, it means that the administrator being referenced has failed to successfully login the maximum number of attempts permitted, and the account is disabled. In order for the locked out administrator to login, another administrator with administrator profile privileges must change the password of the locked out administrator. The LOCKED status will be removed from the administrator profile. For more information on administrator security, see the *VitalQIP Web Client User's Guide*.
- 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 by using the **`qip-crypt`** command. See the *VitalQIP Command Line Interface User's Guide* for information about **`qip-crypt`**.
- VitalQIP can place restrictions on password. These restrictions are configured in the Administrator Security window of the VitalQIP web client. For more information, see the *VitalQIP Web Client User's Guide*. 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 window of the VitalQIP web client. The acceptable complexity settings are:
  - – Alpha only
  - – Numeric only
  - – No limitations
  - – Alpha and numeric

Procedure

To create an administrator profile, follow these steps:

1 Select **Administrator** from the **Infrastructure** menu. The Administrator Profile Option window opens.



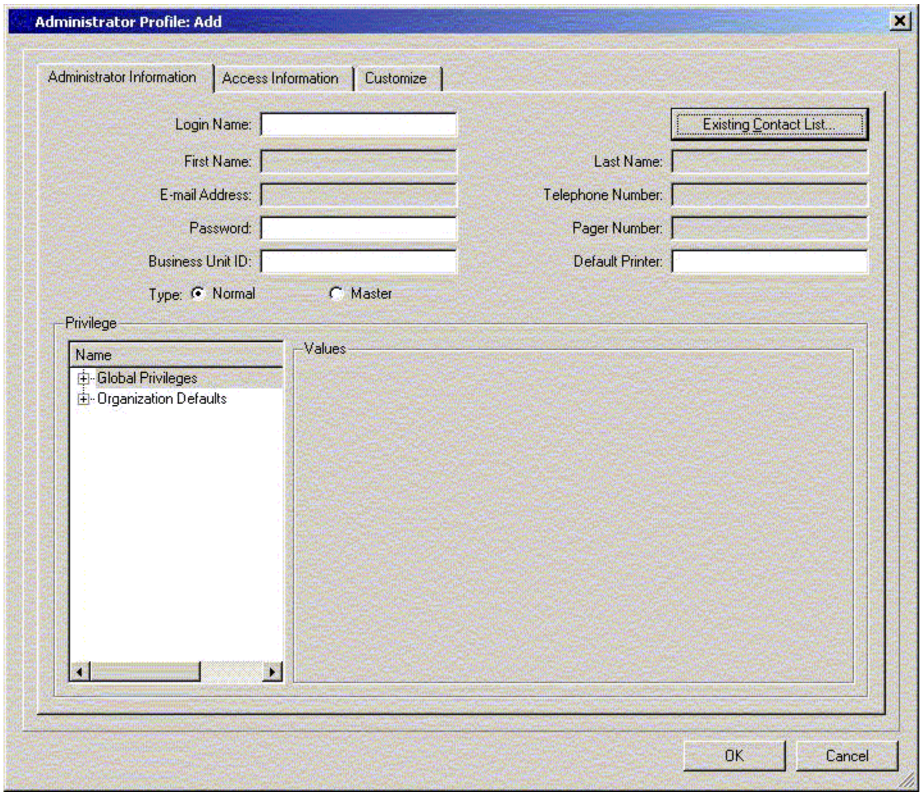
Option

● Add ○ Assign Roles
○ Delete
○ Modify

Existing Administrators

Name	Type
admin1	Normal
bwillbert	Master
qipman	Master

2 Check that the **Add** option is selected and click **OK**. The Administrator Profile: Add opens.



3 ***Required***. Enter the system identification name of the Administrator Profile in the **Login Name** field. This could be initials or the first letter of the first name and the last name with no spaces, or whatever you wish to define.

4 Click **Existing Contact List** to access the current list of contacts. Select a contact from the **Existing Contact List** (or create a new contact profile) and click **Apply**. The **First Name**, **Last Name**, **Email Address**, **Telephone Number**, and **Pager Number** fields display information if it is available.

5 ***Required***. Enter the password the administrator wil 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 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 Profile type and can modify the Privilege list in the **Administrator Information** tab and add to or modify the **Access Information** tab. A user with a “Normal” Administrator Profile can add other “Normal” Administrator Profiles and assign them privileges, Administrative Roles and access rights.
- A “Master” Administrator has access to all organizations and so has no **Access Information** tab. It also can add, modify, and delete Administrative Roles. Only “Master” Administrators can create, modify, or delete “Master” Administrators.

9 Select the privileges you wish to assign to the Administrator Profile 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:	
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.

Name	Value
Allow Password Expiration	The default value is True. When this privilege is set to True, the password of the administrator uses the settings in the Administrator Security screen, located in the VitalQIP Web Client, to determine if the password expires. If the settings in the Administrator Security screen are set to force the password to expire, the password of the administrator expires. When this privilege is set to False, the password of the administrator never expires regardless of what is set in the Administrator Security screen.
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.

Name	Value
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.
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 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**
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 address allocation are displayed.
Add Nodes	The default is True. This privilege allows an administrator to add nodes in the VitalQIP web client.
Manage Nodes	The default is True. This privilege allows an administrator to add, modify, and delete nodes in the VitalQIP web client.
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.
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**
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 hide all other tabs in the VitalQIP web client.
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.
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.

Name	Value
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.
Restrict CNAME	The default value is False, and this option only applies to “Normal” administrators. This privilege, if set to True, prohibits an administrator from entering CNAME and MX records, which do not belong to the subnet’s assigned domain(s). If set to False, an administrator can enter CNAME and MX records, which do not belong to the administrator’s assigned domains without error.

Name	Value
Restrict Subnet	The default value is False, and this option applies only to "Normal" administrators. This privilege, if set to True, 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 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.

10 When you have selected the privileges you wish to assign to the Administrator Profile, you can proceed to setting up the **Access Information** (if defining a "Normal" administrator) and **Customize** tabs. Refer to "Create an administrator access list" (p. 6-23) and "Customize administrator menus" (p. 6-30).

END OF STEPS

Create an administrator access list

Purpose

The **Access Information** tab allows you to set up access rights to one or more organizations for each administrator. You can assign roles you have previously set up with the Administrative Roles function, as well as assign items to be managed for each organization, such as networks, domains, servers, and so on. You can only add an access list for “normal” administrators. Master administrators do not have access lists associated with them.

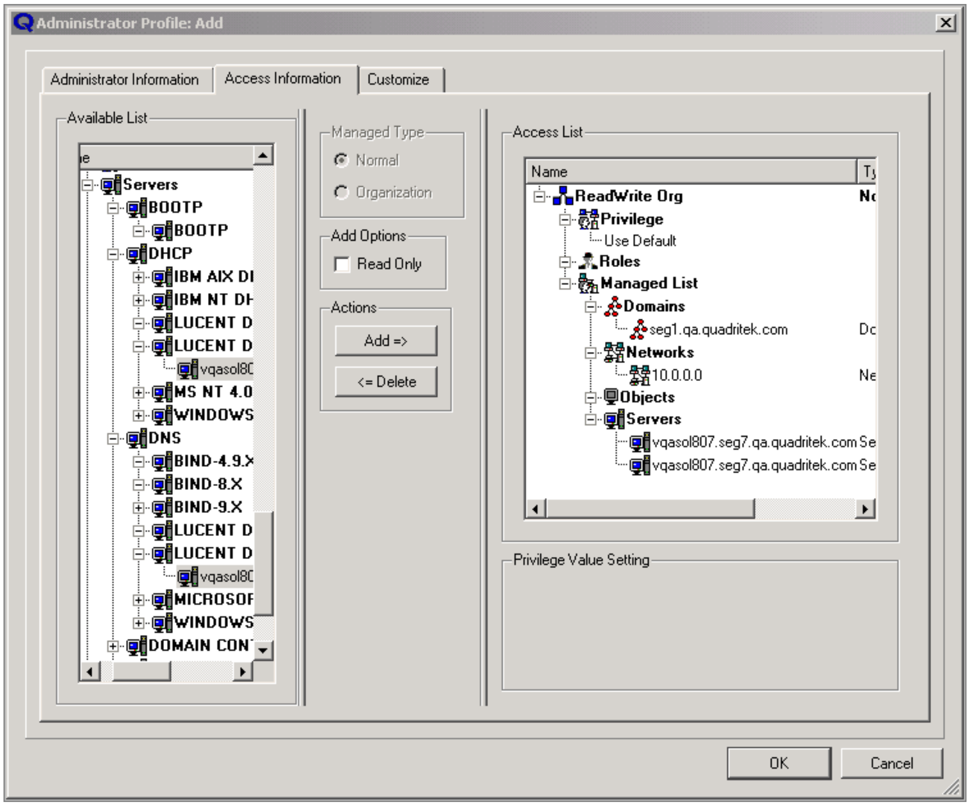
Before you begin

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

Procedure

To create an Access List, follow these steps:

1 In the Administrator Profile, select the **Access Information** tab.



The Available List hierarchy displays all information components to which you have access, such as organizations, domains, networks, subnets, and so on. Only one organization can be expanded at a time, however.

2 Select an organization in the **Available List**.

3 Set up the administrator type on an organizational level. Select either of the following Managed Types:

- **Normal** - allows you to set up custom privileges, assign roles, and set up a managed list for the organization. This is the default Managed Type.
- **Organization** - allows you to give an administrator access to the entire organization. There are no administrative roles nor a managed list, although privileges can be customized.

4 If the selected Managed Type is Organization, you may choose to give an administrator read-only access to that organization by checking the **Read Only** check box.

5 Click Add to add the organization to the Access List.

If the Managed Type is set to **Normal**, the selected organization appears in the Access List with three items: **Privilege**, **Roles**, and **Managed List**.

If the Managed Type is set to **Organization**, the selected organization appears in the Access List with one item: **Privilege**.

If the Managed Type is set to **Organization** with an access type of **Read Only**, the organization appears in the Access List with Read Only Access only.

6 ***For Normal administrators only.*** If the Managed Type is **Normal**, you can change the Privilege setting from the default settings in the Administrator Information window. To change settings, highlight **Use Default** and click **False** in the Privilege Value Setting box. Expand **Use Default** and modify settings as needed. Refer to Table 6-1, "Privilege parameters" (p. 6-15) for further information on each privilege.

7 If the Managed Type is **Normal**, you can assign one or more administrative roles. Expand **Roles** and double-click the roles you want to assign. A check appears beside the roles that have been assigned.

8 If the Managed Type is **Normal**, you can add specific components of the network that are not already defined in an assigned role to the **Managed List**.

Select the components from the **Available List**.

> **Note:** The Available List box displays all infrastructure components to which you have access. Use **Ctrl** and **Shift** if you want to select multiple components to add to the Managed List.

9 Decide if you wish to restrict the selected components to be "Read Only" by selecting the **Read Only** box. Read access indicates the administrator can only view these segments of the infrastructure. For further information on read/write access rights, refer to Table 6-2, "Administrator read/write access" (p. 6-26).

> **Note:** You must make this decision before you click the **Add** button. If you later change your mind, 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.

Click **Add** when you have completed your selections.

10 Repeat steps 2 through 9 as needed to add other organizations to the Access List. You can change Managed Types for each organization you add to the Access List.

11 If you wish to customize menu selections for the current administrative profile, proceed to the **Customize** tab. Otherwise, click **OK** to save the Administrator Profile.

END OF STEPS

Read/write access in the Managed List

Read access is established when you check the **Read Only** box. Read access indicates the administrator can only ***view*** these segments of the infrastructure. The Access column in the Access List displays either "Read/Write" or "Read Only". **Read Only** can be applied to each item in the Managed List.

> **Note:** The display shown when "Domain" is selected from the **Available List** is based on the Administrative users "Display Domain Folders" option in this profile.

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

Table 6-2 Administrator read/write access

Access To▶ **Managed List Types▼**	**Domains**	**Networks**	**OSPF Area**	**Subnets**	**Objects**	**User Groups**	**Subnet Orgs**	**Servers**	**Applications**	**Address Ranges**	**Comments**
Domains	R/ W	----	----	R/ W	R/ W	----	----	----	----	----	
Networks	----	R/ W	----	R/ W	R/ W	----	----	----	----	----	
OSPF Areas	----	----	R/ W	R/ W	R/ W	----	----	----	----	----	
Subnets	----	----	----	R/ W	R/ W	----	----	----	----	----	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.

Access To▶ **Managed List Types▼**	**Domains**	**Networks**	**OSPF Area**	**Subnets**	**Objects**	**User Groups**	**Subnet Orgs**	**Servers**	**Applications**	**Address Ranges**	**Comments**
Objects	----	----	----	----	R/W	----	----	----	----	----	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 get a privilege denied.
User Groups	----	----	----	----	----	R/W	----	----	----	----	Can also create users.
Subnet Organizations	----	----	----	R/W	R/W	----	R/W	----	----	----	
Servers	----	----	----	----	----	----	----	R/W	----	----	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.

Access To▶ Managed List Types▼	Domains	Networks	OSPF Area	Subnets	Objects	User Groups	Subnet Orgs	Servers	Applications	Address Ranges	Comments
Applications	----	----	----	R	R/W	----	----	----	R/W	----	Can create/modify objects in the subnet or object if the subnet has this application defined.
Address Ranges	----	R	----	R/W	R/W	----	----	----	----	----	You cannot change the properties of the network, but you can add subnets to the network.
Object Ranges	----	----	----	R	R/W	----	----	----	----	----	

Customize administrator menus

Purpose

The **Highest Level GUI Mode** privilege in the **Administrator Information** tab of the Administrator Profile allows you to assign a “mode” to an administrator. In addition, you can further customize the menu items presented to the administrator by enabling or disabling *specific* menu options.

For example, an “Advanced Mode” administrator can access the **DHCP/Bootp Template** function in the **Policies** tab. Through the **Customize** tab this function can be disabled while all the other functions in the Policies menu can be left enabled.

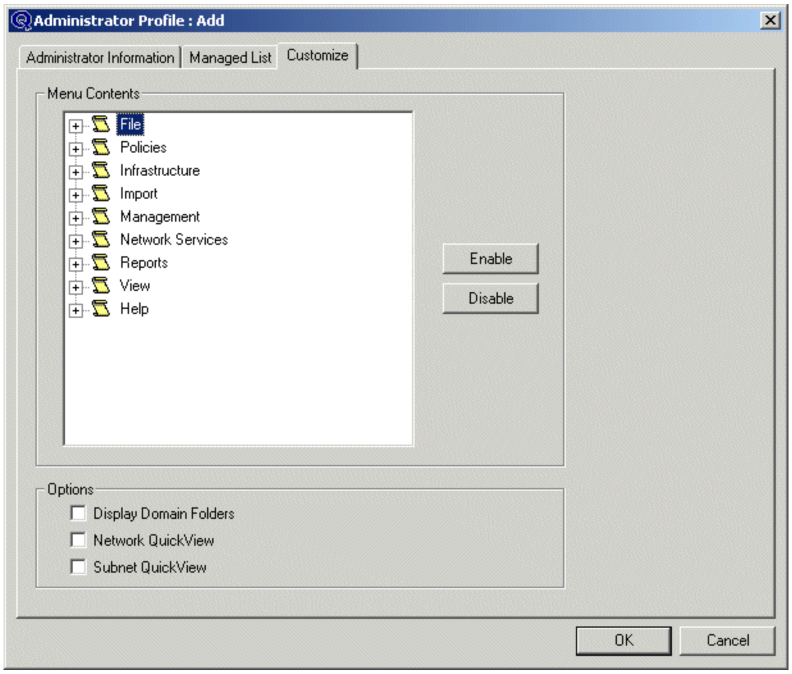
Before you begin

Any changes made to menus for administrators affect the administrator’s options in the VitalQIP web client interface, as well as the VitalQIP interface. For example, if an administrator is not given access to DHCP/Bootp Templates in the VitalQIP interface, that administrator does not have access to that option in the VitalQIP web client interface either.

Procedure

To customize menu items, follow these steps:

1 Expand the menu you wish to customize. A checkmark appears next to each menu item that is enabled.



2 To disable an option in a menu, uncheck the item.

You can also specify three additional options for the administrator you are profiling. All these options default to unchecked (false). They are:

- **Display Domain Folders** - Check this box to allow this administrator to display and select domains grouped into folders. This allows for a logical grouping when large numbers of domains are managed. The QIP Hierarchy, as well as domain selection windows, will display the domain folders. The root folder is always be the existing Domain node (label) in the hierarchies and domain selection windows. If the box is left unchecked, all domains belong to the default root folder in the QIP Hierarchy. Domain selection windows display available domains in a list. Refer to "Rules for creating and managing folders" (p. 1-41) for rules on creating and maintaining folders.
- **Network QuickView** - If this box is checked, subnets default to displaying in QuickView format in the hierarchy. If you double-click (or click the expand sign) on a network in the Network, a domain, an OSPF area, or a subnet organization in the hierarchy, it displays the subnets in QuickView format rather than the Subnet Selection window. This option is useful if you have to manage large numbers of subnets. For more information on this feature, refer to "Use Network Quick View" (p. 1-36).

- **Subnet QuickView** - If this box is checked, objects default to displaying in QuickView format when you double-click on a subnet in the hierarchy. This option is useful if you have to manage large numbers of objects. For more information on this feature, refer to "Use Subnet Quick View" (p. 1-38).

END OF STEPS

Modify an administrator profile

Purpose

Use this procedure to modify an administrator profile.

Before you begin

- If you see <LOCKED> in the title bar of the **Administrator Information** tab in the administrator profile, it means that the administrator being referenced has failed to successfully login the maximum number of attempts permitted, and the account is disabled. In order for the locked out administrator to login, another administrator with administrator profile privileges must change the password of the locked out administrator. The LOCKED status will be removed from the administrator profile. For more information on administrator security, see the *VitalQIP Web Client User's Guide*.
- VitalQIP can place restrictions on password. These restrictions are configured in the Administrator Security window of the VitalQIP web client. For more information, see the *VitalQIP Web Client User's Guide*. Restrictions can be set for:
  - Length of password
  - 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 window of the VitalQIP web client. The acceptable complexity settings are:
  - Alpha only
  - Numeric only
  - No limitations
  - Alpha and numeric

Procedure

To modify an administrator profile, follow these steps:

1 Select **Administrator** from the **Infrastructure** menu. The Administrator Profile Option window opens.

2 Select the **Modify** option if you wish to change privileges, or managed list settings. Select **Assign Role** if you only wish to assign (or modify a previously assigned) an administrative role.

3 Select the Administrator Profile you wish to modify and click **OK**. The Administrator Profile: Modify window opens.

4 Make changes as needed and click **OK**. A confirmation prompt opens.

5 Click **OK**.

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 **Infrastructure** menu. The Administrator Profile Option window opens.

2 Select the **Delete** option.

3 Select the Administrator Profile you wish to delete and click **OK**. The Administrator Profile: Delete window opens.

4 Verify that the Administrator information belongs to the profile you wish to delete and click **OK**. A warning confirmation opens.

5 Click **Yes**. A confirmation prompt opens.

6 Click **OK**.

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” administrator profiles. You can assign more than one role to an administrator profile. Furthermore, you can select more than one administrator to which to assign the same role.

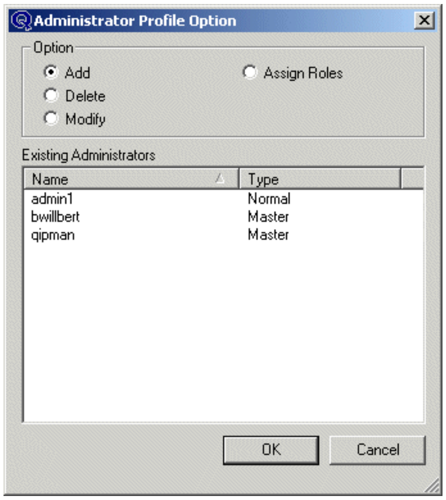
Before you begin

- If you are a “Master” or “Organization” administrator, you can also modify or define new roles to the administrator profiles you have selected, if you so desire (refer to “Create an administrative role” (p. 6-4) 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.
- If the selected administrators do not currently manage the organization that contains the roles, they will automatically be assigned that organization to manage, in order for them to have the privilege (access rights) of being assigned the role. They will now manage that organization as a Normal Managed Organization with Read/Write access. Besides the access to that organization that the role provides, they will also have whatever access for that organization that is defined in the Global Privileges and Organization Defaults for that administrator in their Administrator Profile.

Procedure

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

1 Select **Administrator** from the **Infrastructure** menu. The Administrator Profile Option window opens.


Administrator Profile Option

Option

● Add
○ Delete
○ Modify
○ Assign Roles

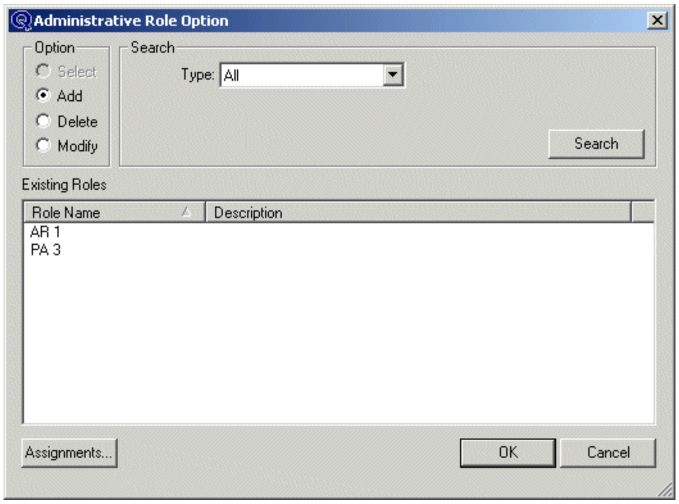
Existing Administrators

Name	Type
admin1	Normal
bwillbert	Master
qipman	Master

2 Select the **Assign Roles** option.

3 Select the Administrator Profile to which you wish to assign an administrative role and click **OK**. The Administrative Role Option window opens.

Note: You can use standard multi-select keys (**Shift** and **Ctrl**) to select several "Normal" administrator profiles at once. If you select a master administrator type in error, it is automatically deselected after you click **OK**.


Administrative Role Option

Option

○ Select
● Add
○ Delete
○ Modify

Search

Type: All

Existing Roles

Role Name	Description
AR 1	
PA 3	

4 Select the roles you wish to assign to the selected Administrator Profiles from the **Existing Roles** list and click **OK**. A confirmation prompt opens.

> **Note:** If you need to display roles of a specific type, select an infrastructure type from the **Type** drop-down list and enter search specifications as needed. Click **Search** to refresh the **Existing Roles** list so that it displays roles that match your search specifications.

5 Click **OK** in response to the confirmation prompt that appears after each role is assigned.

END OF STEPS

User groups

The **User Group Profile** allows you to set up generic User Groups to manage the network, instead of individual names. This is not the same grouping as the contacts and administrators, although they can be part of this grouping. This is used to manage the *network* users and allows you to organize a group of users into one category.

You can define logical groupings of individuals in any way your infrastructure requires. For instance, you can define groups by physical location, or type of users: all users in the United Kingdom could be in one group, and all users in the Netherlands could be in another. Alternatively, all users who perform administrative functions could be in one group, all executives in another group, all helpdesk personnel in another.

> **Note:** Since a user profile cannot be created without there being a user group to which to assign it, you need to create at least one empty user group. Once a single user group is defined, user profiles can be created and automatically added to that group. If you want more control over which user group a user profile belongs to, create the user groups you need first and then you are forced to choose which group to assign to a user profile before it can be saved. Refer to "Assign users to groups" (p. 6-51) for details on how to set up the User Profile.

Add a user group

Purpose

Use this procedure to create a user group.

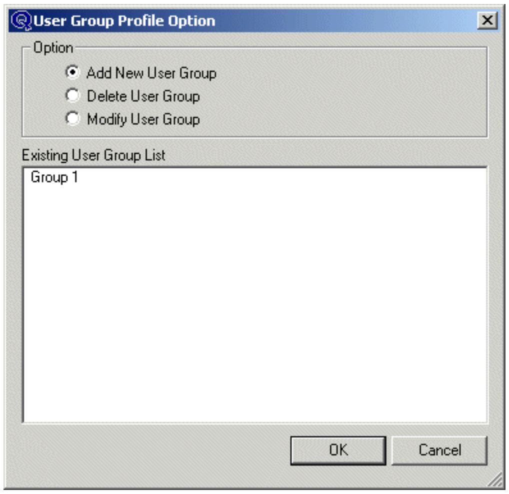
Before you begin

You cannot have groups within groups. In other words, hierarchy among user groups is not allowed.

Procedure

To add a user group, follow these steps:

1 Select **User Group** from the **Infrastructure** menu. The User Group Profile Option window opens.



User Group Profile Option

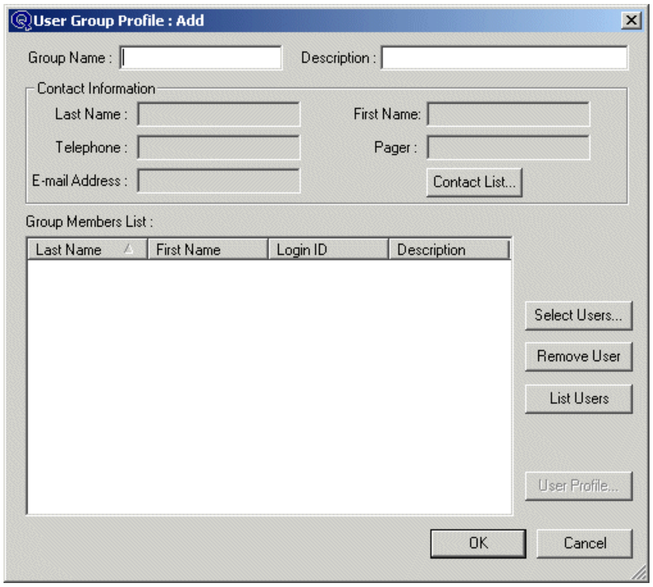
Option

● Add New User Group
○ Delete User Group
○ Modify User Group

Existing User Group List

Group 1

2 Select the **Add New User Group** option and click **OK**. The User Group Profile: Add window opens.



3 Enter a new user group name (of up to 32 characters) in the **Group Name** field.

4 Add a description of the user group (of up to 30 characters) in the **Description** field.

5 Assign a contact to this User Group by clicking **Contact List** and selecting a contact from the list. (The available contacts are entered in the **Contact Profile** function on the **Policies** menu.) The person you select is the owner/administrator of the User Group.

6 To create an empty user group, click **OK**. A confirmation prompt opens.

7 Click **OK**. Repeat these steps to create other user groups as needed. Now that you have one or more empty user groups, you can create a user profile at this time.

8 To add (previously defined) users to a group, click **Select User**. The User Profile Option window opens.

Note: The **Existing User List** in the User Profile can be sorted by clicking on the column headings.

– To create a list of all users, click **Search**. At the “Search will return ALL users. Continue?” prompt, click **Yes**.

– Alternatively, if you know the **Login Name** or the **Login ID** of the user(s) you wish to add, select the appropriate option and enter the name or ID (or even a partial name or ID) in the **Search** field, and click **Search**. Select one or more users and click **OK**.

9 Click **OK** when you have completed using the **User Group Profile**.

END OF STEPS

Modify a user group

Purpose

Use this procedure to modify a user group.

Procedure

To modify a user group, follow these steps:

1 Select **User Group** from the **Infrastructure** menu. The User Group Profile Option window opens.

2 Select the User Group you wish to modify and click **OK**. The User Group Profile: Modify opens.

3 Click **List Users** and the current users of the User Group are displayed in the **Group Members List**.

4 Modify as necessary. You can modify user profiles, add other user profiles, or remove user profiles from the group.

- To add other user profiles to the group, click **Select User** and select one or more profiles from the User Profile Option window.
- To modify the user through the User Profile, click **User Profile** and the User Profile Option window opens. Once you have updated the user profile and clicked **OK** to save it, the **Group Members List** is updated.
- To delete one or more users from the User Group, highlight the user(s) and click **Remove User**. At the `Are you sure you want to remove the selected users?` prompt, click **Yes**.

5 Click **OK**. A confirmation prompt opens.

6 Click **OK**.

END OF STEPS

Delete a user group

Purpose

Use this procedure to delete a user group.

Before you begin

If a User Group is deleted, all user profiles that are associated ***only*** with this User Group and no other are also deleted. A warning with the total number of user profiles affected is displayed first. If you wish to preserve any of those user profiles, click **Cancel** and remove the user profiles from the list first.

Procedure

To delete a user group, follow these steps:

1 Select **User Group** from the **Infrastructure** menu. The User Group Profile Option window opens.

2 Select the **Delete** option and select the User Group you wish to delete.

3 Click **OK**. The User Group Profile: Delete opens.

4 Click **OK**. A warning prompt opens.

5 Click **Yes**. A confirmation prompt opens.

6 Click **OK**.

END OF STEPS

Users and groups

The User Management function gives you the ability to establish and manage users that are using your network(s) and place those users into specific groups.

There are two options under User Management: **User Profile** and **User Groups**. The User Profile is where you set up the individual users. Accessing User Groups displays a list of already established User Groups and the users that belong to the Group. User Groups are initially established in the **User Group** function on the **Infrastructure** menu.

Note: You must create at least one user group before you can create a user profile.

For example, if a user has one or more workstations or laptops, you can assign the MAC address of these systems to this user. When the DHCP server gives out a lease, the relationship between the IP Address and the user is automatically established, enabling you to keep track of what user is using what object. You can assign MAC addresses, IP addresses, and hostnames to a User Profile in the **Managed Range(s)** tab. These addresses and names belong to this User Profile until you delete them.

Setting up users through the **User Profile** allows you to define users and their corresponding attributes including names and subnets, as well as location information and user group information. Additionally, you can define user-defined information for this user (for example, birthday, spouse’s name, beeper number, and so on).

Define VitalQIP users

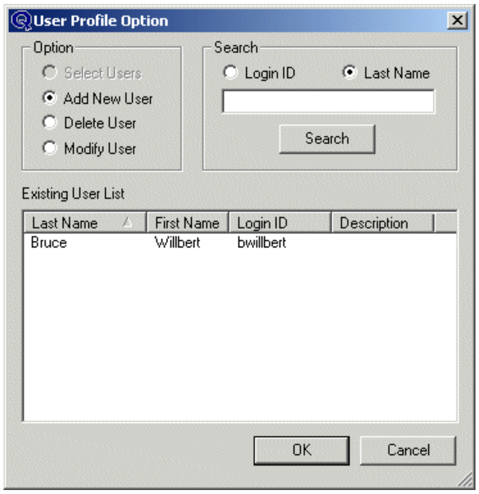
Purpose

Use this procedure to create profiles for VitalQIP users.

Procedure

To define VitalQIP Users, follow these steps:

1 Select **User Management|User Profile** from the **Management** menu. The User Profile Option window opens.



User Profile Option

Option

○ Select Users
● Add New User
○ Delete User
○ Modify User

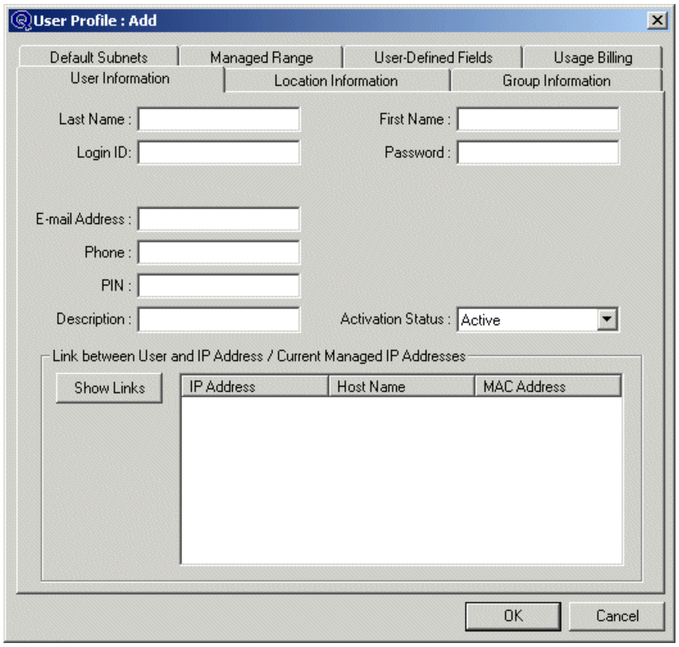
Search

○ Login ID ● Last Name

Existing User List

Last Name	First Name	Login ID	Description
Bruce	Willbert	bwillbert	

2 To add a new user, verify that **Add New User** is checked, and click **OK**. The User Profile: Add window opens.



3 Fill in the fields as described in the following table.

Table 6-3 User Profile fields

Fields	Description
Last Name	Enter the **Last Name** of the user in this field (for example, Smith).
First Name	Enter the user's **First Name** in this field (for example, Jane).
Login ID	Enter the user's **Login ID** (for example, jsmith). When a user wants to use your network, they would be assigned a Login ID through this window. This login must be unique for each user.
Password	Enter the user's **Password**. The **Password Masking** global policy determines whether the password displays or is masked in this field.

Fields	**Description**
Password Mask	Click this box if you do not want to toggle the password field between asterisks and the actual password. If the **Password Masking** global policy is set to ALWAYS_ON, you cannot turn masking off. If the **Password Masking** global policy is set to OFF or ON, it will be enabled and you can individually restrict (or not) a user's password to display as asterisks. For more information on the **Password Masking** global policy, refer to Table 3-5, “General policies” (p. 3-29).
E-mail Address	Enter the user's **E-mail Address** in this field.
Phone	Enter the user's telephone number in this field.
PIN	Enter a personal identification number for this user. This field can be up to 30 characters. This field is used by add-on VitalQIP applications.
Description	This is a free form text field. You can enter up to 30 characters.
Activation Status	You can identify whether or not this user is Active, Inactive or Pending (activation on the network).

4 Click **Show Links** to display all of the MAC Addresses, Host Names and /or IP Addresses that you are currently using. You must be linked to these at the moment you click the button. To see all objects assigned to the user, or to assign new objects or delete objects, refer to the **Managed Range** tab.

5 Enter information in the other User Profile tabs as necessary. Refer to the following sections for more information.

6 Click **OK**. A confirmation prompt opens.

7 Click **OK**.

END OF STEPS

Enter location information

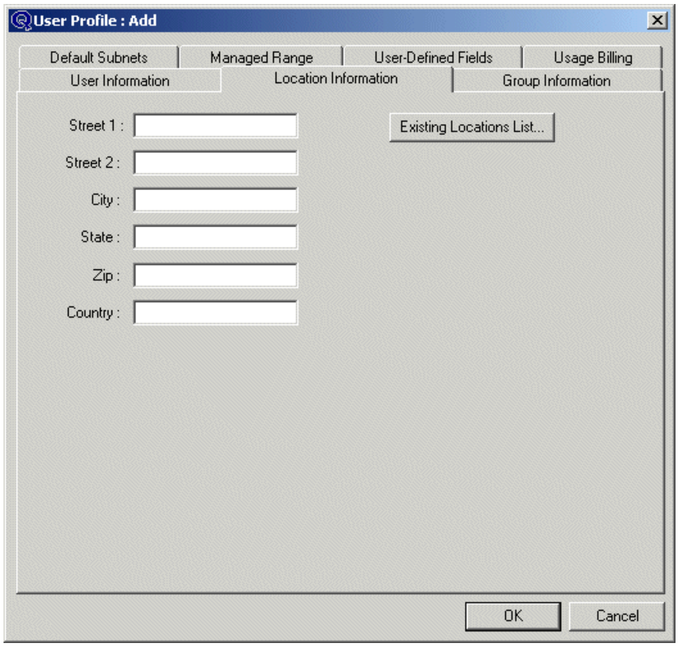
Purpose

Use this procedure to add a location to the User Profile.

Procedure

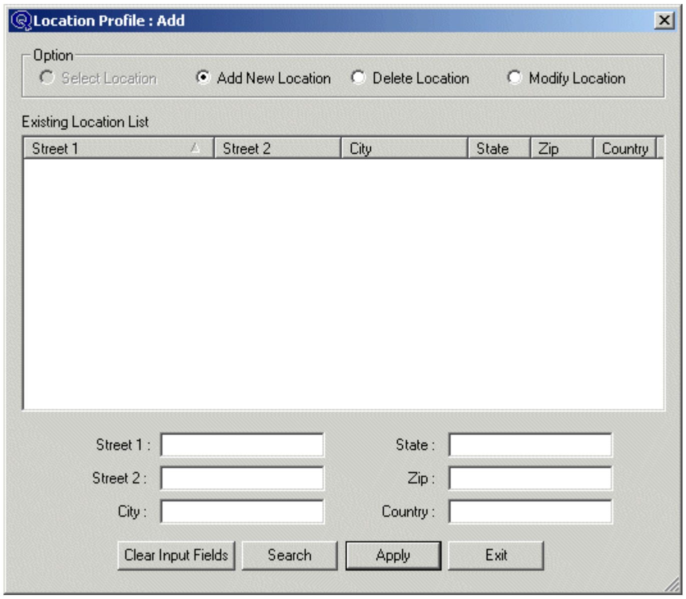
To add a location to the User Profile, follow these steps:

1 Select the **Location Information** tab.



There are two methods available to add location information to a User Profile. Either enter location information into the fields directly, or click **Existing Locations List** and select from a pre-defined list of locations.

If you click **Existing Locations List**, the Location Profile opens with a list of locations that have already been defined in the **Location Profiles** function on the **Policies** menu.



Location Profile : Add

Option: ○ Select Location ● Add New Location ○ Delete Location ○ Modify Location

2 Highlight the location you want to apply to a user, and click **Select**. The selected location appears in the **Location Information** tab.

END OF STEPS

Assign users to groups

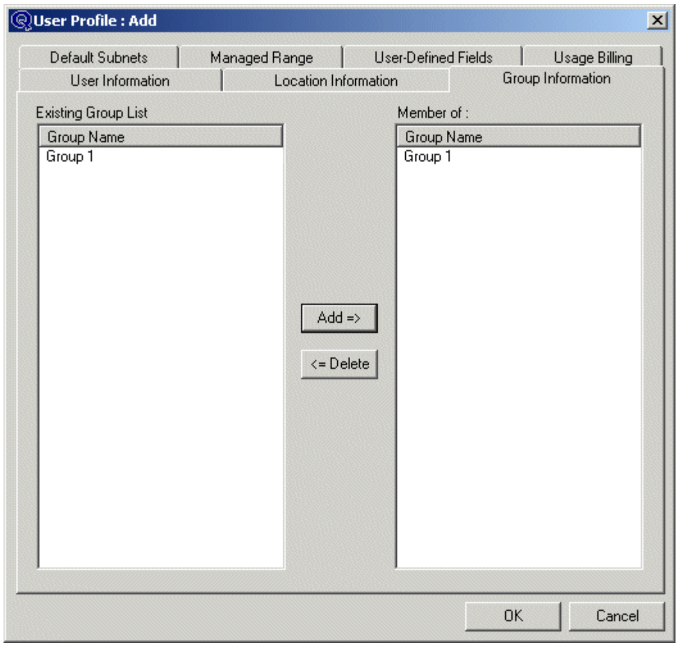
Purpose

Use this procedure to add one or more users to a group.

Procedure

To add one or more users to a group, follow these steps:

1 Select the Group information tab assigns a user to one or more groups, select the **Group Information** tab.



2 Select a group from the **Existing Group List** and click **Add**. This assigns the user as a **Member of** the group.

You can unassign a user from a group by selecting the group in the **Member of** and clicking **Delete**.

> **Note:** If there is only one group defined within the system, the user is automatically added to this group.

END OF STEPS

Associate users with subnets

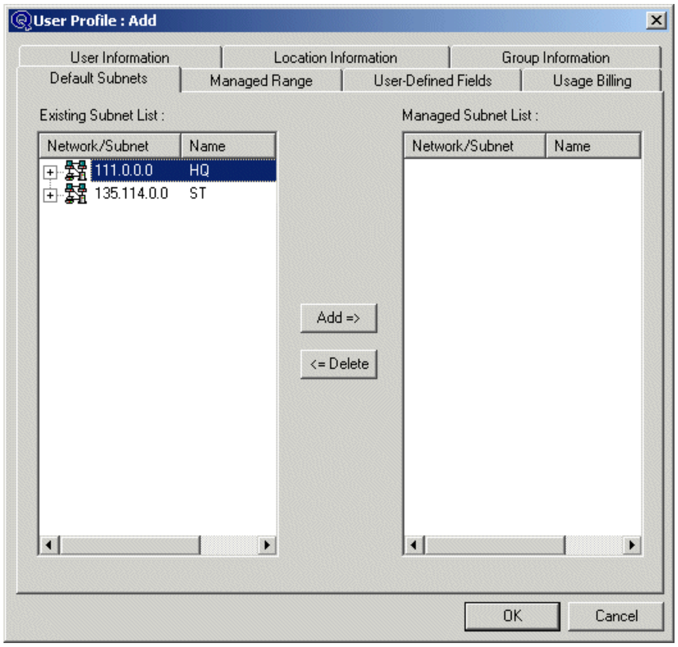
Purpose

Use this procedure to associate a user with one or more specific subnets.

Procedure

To associate a user with one or more specific subnets, follow these steps:

1 Select the **Default Subnets** tab.



2 Open the hierarchical tree in the **Existing Subnet List** and add the selected subnets to the **Managed Subnet List**.

To delete a user's managed subnets, select the subnet in the **Managed Subnet List** and click **Delete**.

END OF STEPS

Associate users with managed ranges

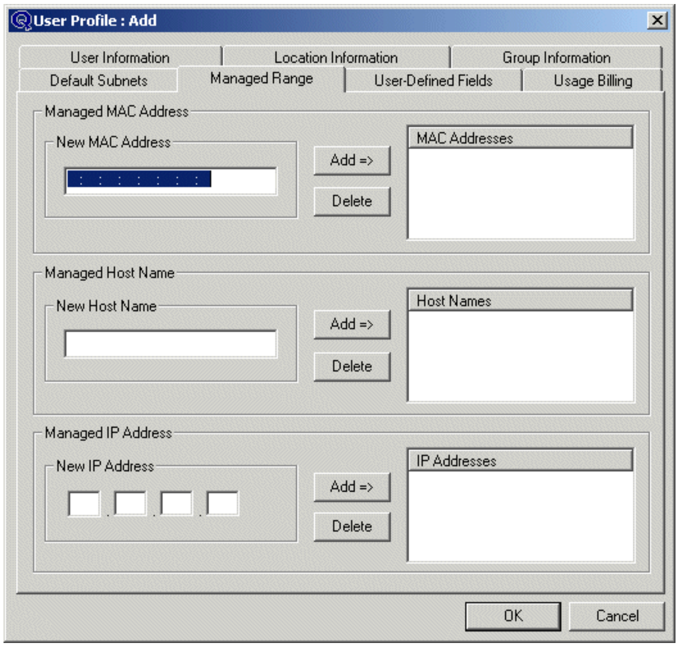
Purpose

Use this procedure to define the MAC addresses, hostnames and/or IP addresses with which a user is associated.

Procedure

To associate a user with a managed range, follow these steps:

1 Select the **Managed Range** tab.



The information entered in this tab is used to establish a link between a user and the IP address space. For example, if you define a managed MAC address, when **Show Links** is selected in the User Information window, any object that has this MAC address is displayed.

2 Type the MAC address, IP address or hostname in the appropriate field and click **Add**.

Likewise, to delete an address or name, highlight it in the listing and click **Delete**.

When you access the object through Object Management, the **User Tab** of the Object Profile will show the users linked to the object.

END OF STEPS

Assign user-defined fields values

Purpose

Use this procedure to assign user-defined field values to User Profile UDFs.

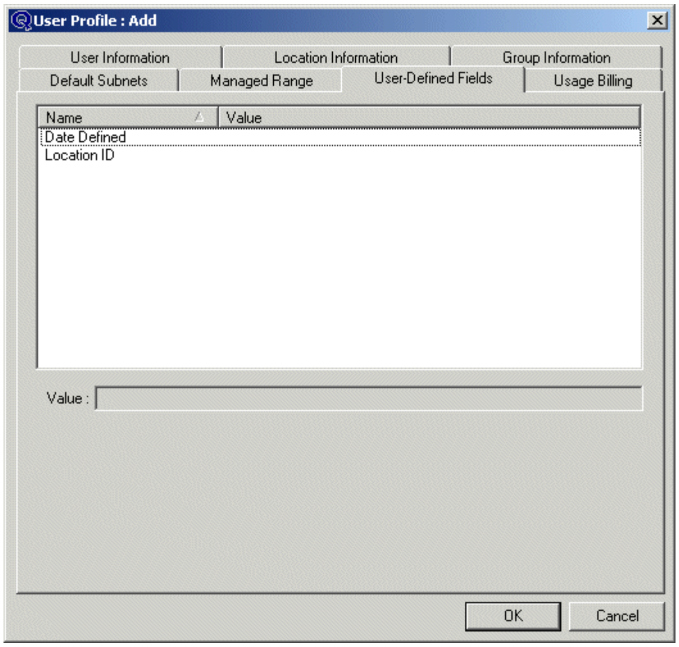
Before you begin

The actual field names for User-Defined Fields are established in the **User-Defined Fields** function on the **Policies** menu.

Procedure

To assign user-defined field values to User Profile UDFs, follow these steps:

1 Select the **User-Defined Fields** tab.



Use the User-Defined Field tab to define information for a user that is not standard to VitalQIP. For example, you may want to keep track of a user's beeper number, birthday, or social security number.

2 Highlight the User-Defined Field name, and enter a value for the name in the **Value** field.

END OF STEPS

Modify a user profile

Purpose

Use this procedure to modify a user profile.

Procedure

To modify an existing user profile, follow these steps:

1 Select **User Management|User Profile** from the **Management** menu. The User Profile Option window opens.

2 To find user profiles that match specific search criteria, choose between the **Login ID** or **Last Name** options.

3 Enter a string in the **Search** field and click **Search**. To return a list of all users, leave the **Search** field blank. Answer **Yes** at the prompt.

4 Select the **Modify** option and select the user profile you wish to modify from the **Existing User List**.

5 Click **OK**. The User Profile: Modify opens.

6 Modify as necessary and click **OK**. A confirmation prompt opens.

7 Click **OK**.

END OF STEPS

Delete a user profile

Purpose

Use this procedure to delete a user profile.

Procedure

To delete an existing user profile, follow these steps:

1 Select **User Management|User Profile** from the **Management** menu. The User Profile Option window opens.

2 To find user profiles that match specific search criteria, choose between the **Login ID** or **Last Name** options.

3 Enter a string in the **Search** field and click **Search**. To return a list of all users, leave the **Search** field blank. Answer **Yes** at the prompt.

4 Select the **Delete** option and select the user profile you wish to delete from the **Existing User List**.

5 Click **OK**. The User Profile: Delete opens.

6 Click **OK**. A warning prompt opens.

7 Click **Yes**. A confirmation prompt opens.

8 Click **OK**.

END OF STEPS

View user groups

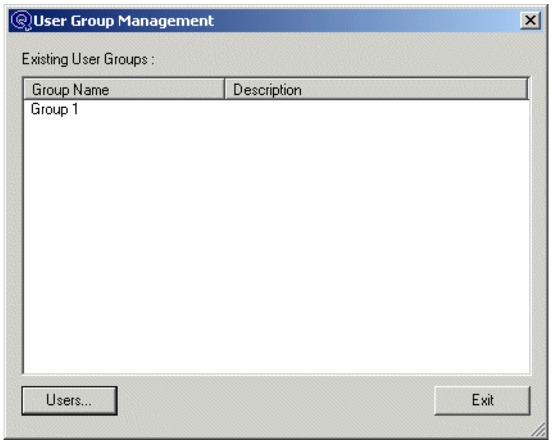
Purpose

This option displays a list of user groups, and within the group, a list of users. You can access a user's individual profile from the list of users.

Procedure

To view the User Groups, follow these steps:

1 Select **User Management|User Groups** from the **Management** menu. The User Group Management window opens.

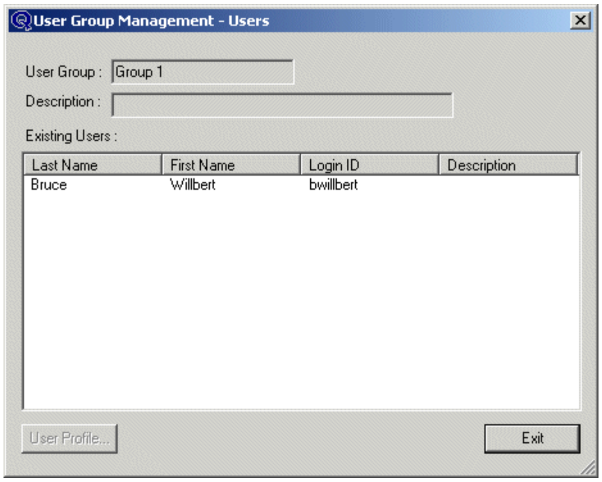


User Group Management

Existing User Groups :

Group Name	Description
Group 1	

2 Highlight a User Group and click **Users**, or double-click on a User Group. The User Group Management - Users window opens, listing the users associated with this user group.



User Group : Group 1

Description :

Existing Users :

Last Name	First Name	Login ID	Description
Bruce	Willbert	bwillbert	

3 To access a User Profile, highlight a user and click **User Profile**. The User Profile Modify window opens.

4 You view or modify the User Profile as needed. Click **OK** when you are finished. A confirmation prompt opens.

5 Click **OK**. The User Group Management - Users window reopens. You can view or modify other User Profiles as needed.

6 When you are finished, click **Exit** to close the User Group Management - Users window. The User Group Management window reopens.

7 You can view other User Groups or click **Exit** to close the window.

END OF STEPS

7 Manage subnets and objects

Overview

Purpose

The purpose is to describe how to subnets and manage objects. It also describes how to reclaim IP addresses.

Contents

The following topics are covered:

Manage subnet profiles	7-3
Select a subnet	7-4
Change the way subnets are displayed	7-6
Search for a subnet	7-7
Save or print subnet information	7-8
Set Windows DNS secure update policies	7-14
Assign location and contact information	7-15
Manage object ranges in subnet	7-16
Assign user-defined fields to subnet	7-18
Object management	7-19
Edit object properties	7-23
Manage objects in subnet	7-26
Add a static object	7-27
Enter object aliases	7-34
Enter asset information	7-38
Enter general information	7-40

Enter resource record information	7-45
Enter router information	7-49
Enter mail server information	7-51
Enter wiring HUB information	7-53
Enter wiring HUB slot and port	7-55
Enter DECNet information	7-57
Enter IPX information	7-58
Enter NetBIOS information	7-59
Enter Manual Bootp information	7-60
Enter Dynamic Configuration information	7-62
Enter Windows DNS secure update policies	7-65
Allocate a dynamic IP address	7-67
Modify a dynamically allocated IP address	7-75
Reserve an IP address	7-79
Modify a reserved IP address	7-82
Un-reserve one or more IP addresses	7-83
Move a Subnet	7-85
Schedule an object move	7-89
Schedule an object move and specify the move destination	7-92
Modify a scheduled move	7-94
Reclaim addresses	7-97
Schedule a reclaim	7-98
Check status of a scheduled reclaim	7-104
Reclaim addresses manually	7-108

Manage subnet profiles

Subnets are managed through the **Object Management** function on the **Management** menu. Once the subnets are displayed, you can access a subnet profile, as well as select a subnet so you can manage an object profile through the subnet to which it belongs.

You may find it useful to define parameters at the subnet level instead of at the IP object level because it allows you to create a uniform set of parameters for all objects on the same subnet. Many objects on the same subnet have the same parameters: the same default gateway, DNS domain name, subnet masks, and so on.

VitalQIP displays only the networks, domains, OSPF areas, subnet organizations, subnets, and IP addresses that have been assigned to you. Managing large numbers of subnets can be handled in a variety of ways. You can use Organizations and Subnet Organizations to group subnets into smaller entities. Both these functions are available on the **Infrastructure** menu.

You can also set up Subnet Administrators to manage certain portions of your network. This is part of the **Administrator Profile|Managed List** function.

In addition to these groupings of subnets, you can use the Network and Subnet QuickViews in the VitalQIP hierarchy windows to display subnets quickly and access the objects in them. (For information on setting up QuickView, refer to "Quick View" (p. 1-35) and to "Customize administrator menus" (p. 6-30).) You should implement all these options if you have large numbers of subnets in your network, so you can improve performance and make your administration activities easier.

Select a subnet

Purpose

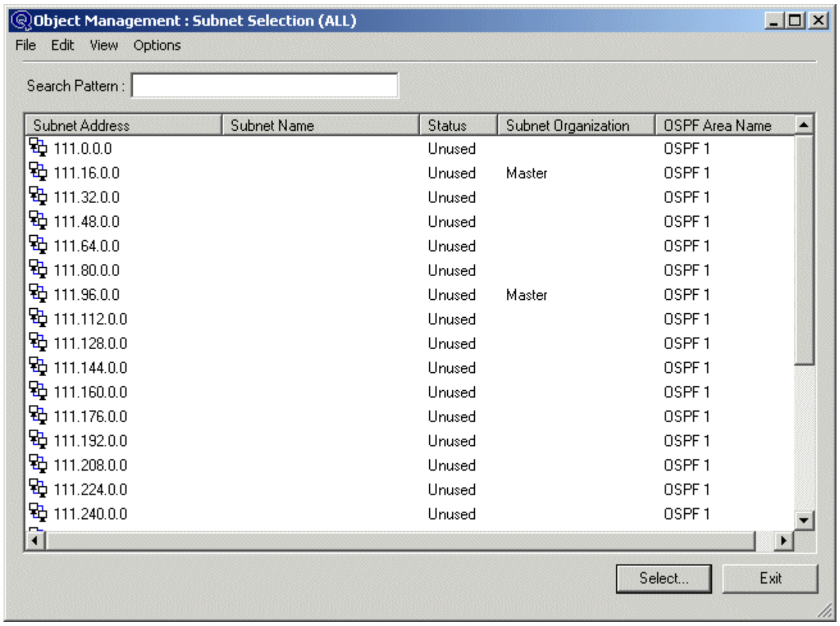
Use this procedure to select subnets.

Procedure

To work with a subnet, follow these steps:

1 Select **Object Management** from the **Management** menu.

2 Select from the **All Subnets**, **Used Subnets**, or **Unused Subnets** submenus. The Object Management: Subnet Selection window opens.



Subnet Address	Subnet Name	Status	Subnet Organization	OSPF Area Name
111.0.0.0		Unused		OSPF 1
111.16.0.0		Unused	Master	OSPF 1
111.32.0.0		Unused		OSPF 1
111.48.0.0		Unused		OSPF 1
111.64.0.0		Unused		OSPF 1
111.80.0.0		Unused		OSPF 1
111.96.0.0		Unused	Master	OSPF 1
111.112.0.0		Unused		OSPF 1
111.128.0.0		Unused		OSPF 1
111.144.0.0		Unused		OSPF 1
111.160.0.0		Unused		OSPF 1
111.176.0.0		Unused		OSPF 1
111.192.0.0		Unused		OSPF 1
111.208.0.0		Unused		OSPF 1
111.224.0.0		Unused		OSPF 1
111.240.0.0		Unused		OSPF 1

If the window defaults to displaying a network address list, expand the tree by clicking on the plus sign beside a network to view the subnets within it. To change the display to a different default and save your preference, refer to "Change the way subnets are displayed" (p. 7-6).

You can view five different columns in this window: Address, Name, Status, Subnet Organization, and OSPF Area. The possible status settings are described in the following table.

Table 7-1 Subnet status

Status	**Results**
Used	Some or all of the IP addresses in this subnet have been assigned.
Unused	None of the IP addresses in this subnet have been assigned.
Planned Use	Addresses are scheduled to be moved into this subnet.
Scheduled Move	This subnet and all the addresses in this subnet are scheduled to be moved to another subnet.

Should you wish to remove a column from the display, select **Display Columns** from the **View** menu and uncheck a column name to remove it. To save the column display you have chosen, select **Save Display** from the **Display Columns** submenu. The next time you enter the Subnet Selection, it is displayed with the columns you saved.

END OF STEPS

Context menu for the subnet selection window

Once you have expanded the network, subnet organization, or OSPF area to display the subnets under it, a context menu is available when you right-click on a subnet. The following options are available.

- **Update Subnet Name** - displays the Modify Subnet Name window so you can change the name of the selected subnet.
- **Reclaim** - opens the Reclaim IP Addresses so you can reclaim addresses. Refer to "Reclaim addresses" (p. 7-97) for more information.
- **Move Subnet** - displays the Subnet Move window enabling you to move the subnet from one network to another. This is only enabled when the Subnet is used (contains objects).
- **Delete Scheduled Move** - allows you to delete the scheduled move of a subnet. This is a function and does not display a window. This function is only enabled when the subnet is scheduled to move.
- **Quick View** - displays subnets or objects in a grid-like pattern for quick access. Refer to "Quick View" (p. 1-35) for more information.
- **Reports** - displays the Object List Report: By Address window.
- **Properties -** displays the Subnet Profile for that selection.

Change the way subnets are displayed

Purpose

Use this procedure to change the default appearance of subnets in the Subnet Selection window.

Procedure

To change the way subnets are displayed, follow these steps:

1 Select **View|View by** to change the display method of the listing in the window. The listing can be displayed by Subnet, Network, Subnet Organization or OSPF Area.

2 Select **Save on Exit** if you want to see the same display each time you access the Object Management: Subnet Selection window.

3 To change the width of a column, click the edge of a column heading and pull it to the right or left.

END OF STEPS

Search for a subnet

Purpose

The search is a single selection search and searches only visibly expanded subnets and labels. The application searches from where you are currently highlighted down the hierarchy. The Subnet Address, Subnet Name, Status and Subnet Organization, and OSPF Area name in the Subnet Selection window are searched if the columns are displayed. If a column is hidden, it is not searched. The search is case-sensitive.

Procedure

To search for a subnet, follow these steps:

1 Type the text in the **Search Pattern** field, then press **Enter**.

2 Press **Enter** again to find the next instance of the text.

The search will loop around to the selected item.

END OF STEPS

Save or print subnet information

Purpose

Use this procedure to save and print subnet information.

Before you begin

- Only subnets that were previously expanded (since the window was last entered) are saved.
- If a “Subnet” is selected in **View|View by** as the sort order, all subnets will print.

Procedure

To save or print a list of subnets, follow these steps:

1 To save a text file of the subnet list, select **File|Save As**.

A Save to File window opens.

2 Select a file and click **Save**.

3 To print a subnet list, select **File|Print**.

The subnet information prints to the designated local printer.

END OF STEPS

View/modify subnet profile

The **Subnet Profile** function allows you to define the default 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. (The DHCP/Bootp templates and Policy Templates are described in Chapter 2, “DHCP policies and templates”.) This is a very practical function because clients on the same subnet generally do have the same subnet default gateway, DNS domain name and subnet masks, among other things.

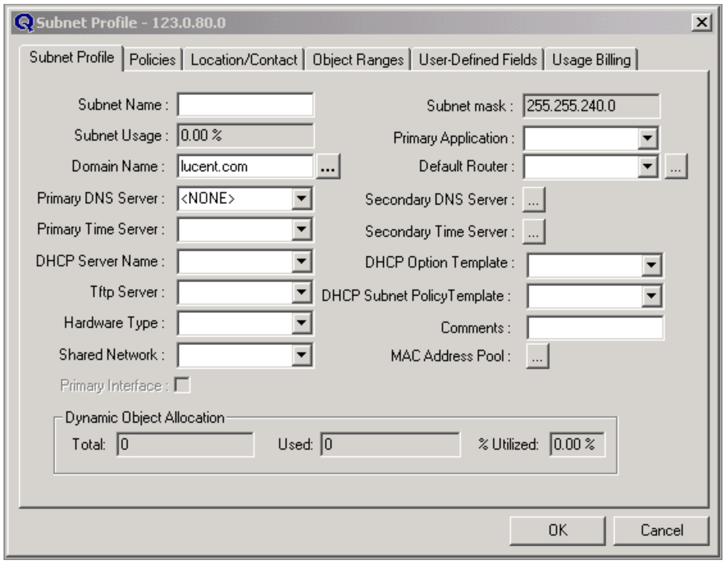
Before you begin

- You can define and revise the subnet profile in either the Object Management: Subnet Selection window or the Object Management window (with the **Subnet Profile** function on the **Edit** menu).

Procedure

To modify or view a Subnet Profile in the Object Management: Subnet Selection window, follow these steps:

1 Highlight a subnet and select **Subnet Profile** from the **Edit** menu (or select **Properties** from the context menu). The Subnet Profile window opens.



Subnet Usage : 0.00 %
Subnet mask : 255.255.240.0
Domain Name : lucent.com
Primary DNS Server : <NONE>
Total: 0
Used: 0
% Utilized: 0.00 %

2 Fill in fields as needed in the **Subnet Profile** tab. For more information on a field, refer to the following table.

Table 7-2 Subnet profile fields

Field	**Description**
Subnet Name	Enter the name (up to 32 characters) for this subnet. This field can be blank (null).
Subnet Mask	The subnet mask for this subnet displays in this field from the Subnet Selection window.
Subnet Usage	This value indicates the percentage of the IP addresses for this subnet that are currently in use.
Domain Name	Either enter a fully qualified, known domain name, or click **...** to display the Domain Option: Select window. If the "Create Infrastructure|Dynamic Domain Creation" privilege in the **Administrator Profile** is set to True, you may either select an existing domain or create a new one. If a new domain is created, it may also be set as the default domain for this subnet.
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 Object Profile, **Router** tab or within a DHCP Template. **Note:** The **Always Append Router** policy automatically adds router objects to the default routers list if set to True. Refer to Table 3-5, "General policies" (p. 3-29). 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. Click **...** to display the Default Router List window. Select a router and click **OK**. To add a router to the Default Router list, click **Add**. To delete a router, click **Delete**.
Primary DNS Server	Assign the primary DNS server for the objects within the subnet by selecting a DNS server from the drop-down list.
Secondary DNS Server	Assign the secondary 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, then click OK. To add a server to the list of DNS servers, click **Add**. To delete a server, click **Delete**.

Field	Description
Primary Time Server	Assign the primary Time server of the domain for the subnet. By default, this is the primary DNS server. Select a server from the drop-down list.
Secondary Time Server	Assign the secondary Time server for the objects within the subnet. Click **...** to display a list of servers that can be assigned. Select a server and click **OK**. To add a server to this list, click **Add**. To delete a server, click **Delete**.
DHCP Server Name	Select the DHCP server assigned to the subnet (if any) from the drop-down list. 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	Assign a DHCP template to the subnet from the drop-down list. The DHCP 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 Template at the subnet level is optional. If no DHCP template is assigned to the subnet, either the template associated with the DHCP server or with an object is used. 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.
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.
DHCP Subnet Policy Template	If you want to assign a previously defined subnet policy template to the current subnet, select one from the drop-down list. Refer to "DHCP policy templates" (p. 2-63).
Comments	Add any comments you wish to add about the subnet.
Hardware Type	Select the hardware type for the objects within the subnet: Ethernet, IEEE802, Token Ring, Pronet, Chaos, Arcnet, or AX.25.

Field	Description
MAC Address Pool	This function is only used when the "RegisteredClientsOnly" policy is set to True in the *dhcpd.pcy* file (refer to "DHCP server policies" (p. 2-71) for more information). Click **...** next to the **MAC Address Pool** field, and the MAC Address Pool:Modify window opens. Follow these steps: 1. Select a **Hardware Type**. 2. Enter a **New MAC Address**. 3. Click **Add** to add the new MAC address to the **MAC Address Pool** for this subnet. You can unassign a MAC address by selecting it from the list and clicking **Delete**. You can use the "*" wildcard character to represent all or part of a MAC address. It must, however, be the last character entered. **Note:** Duplicate MAC addresses are not allowed in the same subnet, even if the **Allow Duplicate MAC Addresses** global policy (described in Table 3-5, "General policies" (p. 3-29)) 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 entering a network name in the field. 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.

3 Select other tabs to complete the definition of the subnet profile. Refer to following sections for information on each tab.

4 Click **OK** to save the subnet profile.

END OF STEPS

Set Windows DNS secure update policies

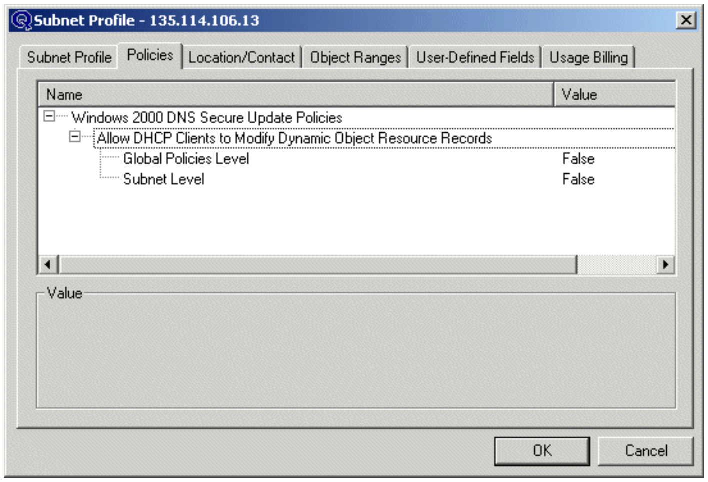
Purpose

You can set the Windows DNS secure zone updates policies at a subnet level (refer to the *Administrator Reference Manual*).

Procedure

To set secure DNS update policies, follow these steps:

1 Click the **Policies** tab. The **Policy** tab opens.



Name	Value
Windows 2000 DNS Secure Update Policies	
Allow DHCP Clients to Modify Dynamic Object Resource Records	
Global Policies Level	False
Subnet Level	False

2 To establish secure zone update policies, refer to the following table.

Table 7-3 Policies in the Policies tab

Policy	Values	Default	Description
Global Policies Level	True or False	False	This policy is read only and shows the Global Policy setting for the secure dynamic updates.
Subnet Level	False, Same as Global Values, True	False	Determines if the secure dynamic updates are set at the subnet level.

END OF STEPS

Assign location and contact information

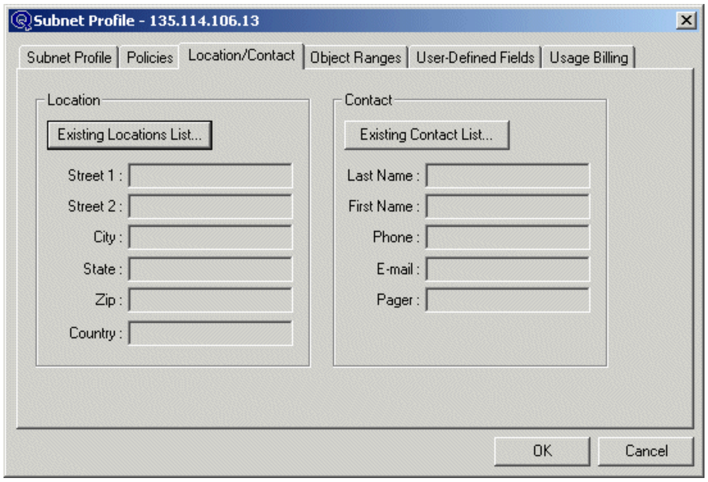
Purpose

Use this procedure to assign location and/or contact information for the subnet profile.

Procedure

To enter location and/or contact information for the subnet profile, follow these steps:

1 Select the **Location/Contact** tab.



2 Enter a new location for the objects in this subnet or click **Existing Locations List** and select a location from a list of current locations. When an object is added within this subnet, it is assigned to this location by default, unless it is overridden within the Object Profile of the object.

3 Enter a new contact for this subnet or click **Existing Contact List** and select a contact from a list of current contacts. When an object is added to this subnet, it is assigned to this contact by default, unless it is overridden within the Object Profile of the object.

> **Note:** To clear a location or contact from these fields, click **Existing Locations List** or **Existing Contact List** to open the Profile window. Select **Clear Input Fields** and click **Apply**.

END OF STEPS

Manage object ranges in subnet

Purpose

The **Object Ranges** tab allows the administrator to add, delete, or modify ranges of addresses within the subnet.

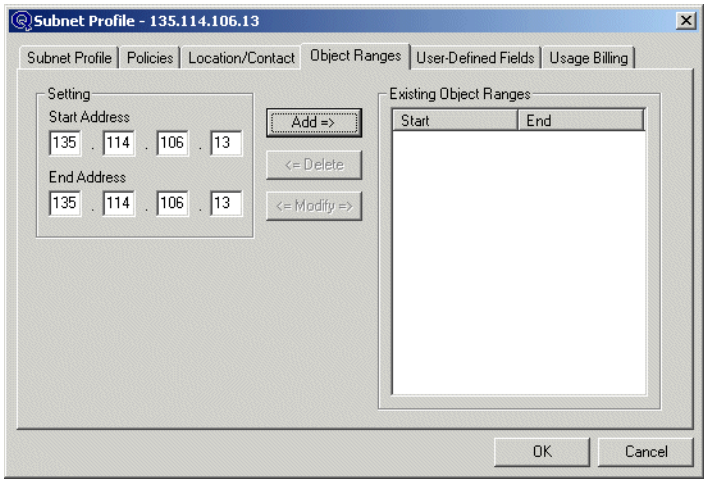
Before you begin

- Objects do not have to exist prior to the times 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 split and join, 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 define an object range, follow these steps:

1 Select the **Object Ranges** tab. The **Object Ranges** tab open.



Subnet Profile - 135.114.106.13

Setting

Start Address: 135 . 114 . 106 . 13

End Address: 135 . 114 . 106 . 13

2 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 when this tab is displayed.

3 Click **Add** and the range appears in the **Existing Object Ranges** list.

4 Repeat steps 3 and 4 as necessary. To delete an object range, highlight the appropriate object range in the **Existing Object Ranges** list, and click **Delete**. 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**.

END OF STEPS

Assign user-defined fields to subnet

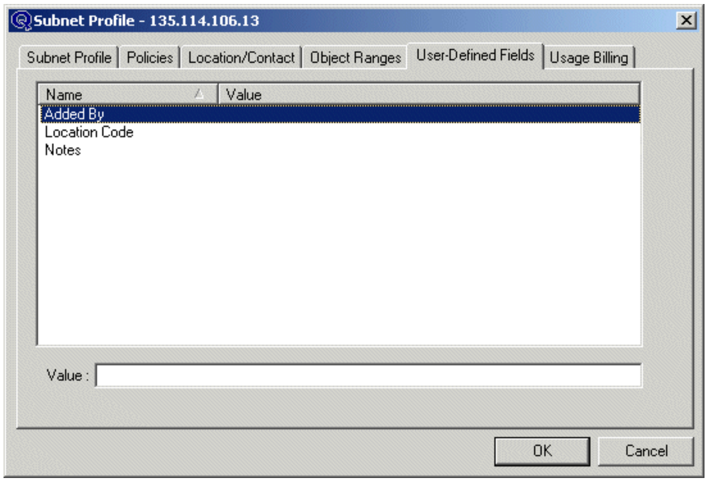
Purpose

In the **User-Defined Fields** tab, you can 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.

Procedure

To add a value for a user-defined field, follow these steps:

1 Select the **User-Defined Fields** tab. The **User Defined Fields** tab opens.



2 Highlight the field for which you wish to provide a value.

3 Enter a value in the **Value** field.

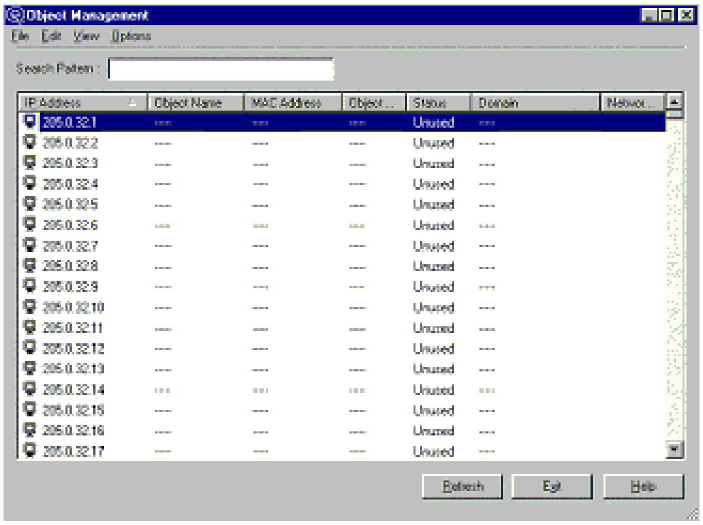
4 Repeat steps 2 and 3 as necessary. To edit or delete a value, highlight a field and use standard edit keys to modify or delete text.

END OF STEPS

Object management

After you select a subnet in the Object Management: Subnet Selection window, the Object Management: Objects window opens. It displays all objects within a specified subnet.

Figure 7-1 Object management objects



IP Address	Object Name	MAC Address	Object...	Status	Domain	Networ...
205.0.32.1	----	----	----	Unused	----	
205.0.32.2	----	----	----	Unused	----	
205.0.32.3	----	----	----	Unused	----	
205.0.32.4	----	----	----	Unused	----	
205.0.32.5	----	----	----	Unused	----	
205.0.32.6	----	----	----	Unused	----	
205.0.32.7	----	----	----	Unused	----	
205.0.32.8	----	----	----	Unused	----	
205.0.32.9	----	----	----	Unused	----	
205.0.32.10	----	----	----	Unused	----	
205.0.32.11	----	----	----	Unused	----	
205.0.32.12	----	----	----	Unused	----	
205.0.32.13	----	----	----	Unused	----	
205.0.32.14	----	----	----	Unused	----	
205.0.32.15	----	----	----	Unused	----	
205.0.32.16	----	----	----	Unused	----	
205.0.32.17	----	----	----	Unused	----	

The Object Management window shows available IP addresses and objects that have already been assigned IP addresses within a subnet (assuming you originally selected **All Subnets** or **Used Subnets** from the **Object Management** menu). The status of each address is also displayed, and if an object is configured, additional columns contain data, such as object name, object class, and so on.

The **Status** column in the Object Management window has a number of values. Also, notice that a colored icon, representing the configuration status of the object/IP address, appears next to each IP address (the same color indicators are also used in Subnet Quick View windows). The status indicators are described in the following table.

Table 7-4 Configuration status indicators

Color	Configuration status
White	Unused
Grey	Static
Blue	Manual Bootp
Yellow	Automatic Bootp
Dark Green	Automatic DHCP
Green	Dynamic DHCP

Color	Configuration status
Red	Manual DHCP

In the Object Management window, you can add one or more static, dynamic or reserved objects. When adding a static object, you are defining the object right away through the Object Profile. When you dynamically allocate an object, you assign the address right away without having to fill out the entire Object Profile (you can fill out the remainder of the information at a later time). When you reserve an object, you are holding the IP address(es) for use by object(s) or subnet(s) at another date. Each option displays a different type of window.

There are several ways to proceed in the Object Management: Objects window. You can double-click on an object to open the Object Profile in either Add or Modify mode, or you can highlight an object and select a function from the **Edit** menu. (Alternatively, you can right-click on one or more objects and select from the context menu.) You can add, modify, delete, schedule moves for objects, ping objects, produce an audit report, review object properties, and refresh. You can also modify the Object and Subnet properties for objects through the **Edit** menu, or by right-clicking and selecting from the context menu. All menus and their options are described, as follows.

The File menu

The **File** menu allows you to Save, Print or Mail an Object List report for this subnet. Click **Exit** to close the window.

The Edit menu

The **Edit** menu lets you add, modify, delete or move static, dynamic, and reserved objects. These menu selections take you to specific windows, so you can perform the following functions.

- When adding a static object (**Edit|Add|Static Object**), the Object Profile window opens. For detailed information, refer to “Manage objects in subnet” (p. 7-26).
- If you are adding a dynamic object (**Edit|Add|Dynamic Object**), the Dynamic Allocation: Add window opens. For detailed information, refer to “Allocate a dynamic IP address” (p. 7-67).
- The **Edit|Add|Reserved Object** option displays the Reserve Allocation: Add window. For detailed information, refer to “Reserve an IP address” (p. 7-79).
- The **Move** function allows you to Schedule, Cancel, and Modify object moves to other subnets. For information on moving objects, refer to “Move an object” (p. 7-87).
- The **Subnet Profile** function allows you to make changes to the Object(s) Subnet through the Subnet Profile. For more information on editing the Subnet Profile, refer to “Manage subnet profiles” (p. 7-3).

- The **Object Properties** function allows you to apply changes to one or more previously defined objects at the same time For more information, refer to "Edit object properties" (p. 7-23).
- The **Subnet Move** function allows you to move all the objects within this subnet to another subnet. For more information, refer to "Subnet Moves" (p. 7-84).

The View Menu

You can change the view in the Object Management window to all objects, only unused objects, or used objects, through the **View** option in the menu. When you select Used Objects, you can filter even more specifically to view all, static, dynamic, reserved Manual Bootp, Automatic Bootp, Manual DHCP, Automatic DHCP or Dynamic DHCP objects.

If you want to view all dynamic objects in a subnet that are managed by DHCP servers, click on **View|DHCP Server Properties**. From there, you can see the specifics on objects that are managed by DHCP servers by double clicking on the specific DHCP server with a particular DHCP scope defined.

If you want to view all objects that are scheduled to move in a selected subnet, select **Scheduled Move Objects** on the **View** menu. From there, you can see the specifics of objects, which are scheduled to be moved by double clicking on the specific object.

You can select certain data to be displayed by accessing **Display Columns** from the **View** menu. The columns that are checked in the **Display Columns** list are displayed in the Object management window. You can select Address, Name, MAC Address, Object Class, Status, Domain, Description and Network Status columns. Selecting **Save on Exit** saves your display choices for subsequent logins.

Finally, you can select **Refresh** and refresh the display to determine if any changes have occurred.

The Options Menu

The **Ping All** and **Ping Selected** options ping one or more addresses and retrieve the Network Status for those addresses. Once you leave the Object Management window, however, those Network Status messages disappear.

- **Ping All** - pings all addresses listed in the window. Once pinged, the **Network Status** displays in the Object Management window.
- **Ping Selected** - allows you to select the objects/IP addresses to ping. Once pinged, the **Network Status** displays in the Object Management window.

Note: Windows users need to be logged in with sufficient local administrative rights to execute ping commands. A ping response “Unreachable” or “No Reply” might be displayed, if the user is logged in to Windows with an account that does not have local administrator rights. This is due to security restrictions imposed by Microsoft Corporation.

Object management window Context menu

To display the Context menu, you must select an object in the Object Management window, and right-click.

Note: Depending on the object’s properties, you will see one or more of these options enabled (thus the term “context menu”).

- **Add** - adds a Static, Dynamic, or Reserved object to the subnet (only applicable on “Unused” IP addresses).
- **Delete** - deletes a Static, Dynamic, or Reserved object from the subnet (only applicable on “Used” IP addresses).
- **Modify** - modifies a Static, Dynamic, or Reserved object in the subnet (only applicable on “Used” IP addresses).
- **Move** - allows you to schedule, cancel, or modify a move for “Used” objects (with the exception of dynamic used objects).
- **Ping** - allows you to select one or more objects/IP addresses to ping. Once pinged, the **Network Status** displays in the Object Management window.
- **Audit Report** - displays the Object Audit History report. Refer to “Create an Object Audit History report” (p. 9-42) for more information.

Edit object properties

Purpose

The **Object Properties** function allows you to apply changes to one or more previously defined objects at the same time. This is a condensed version of the Object Profile.

Before you begin

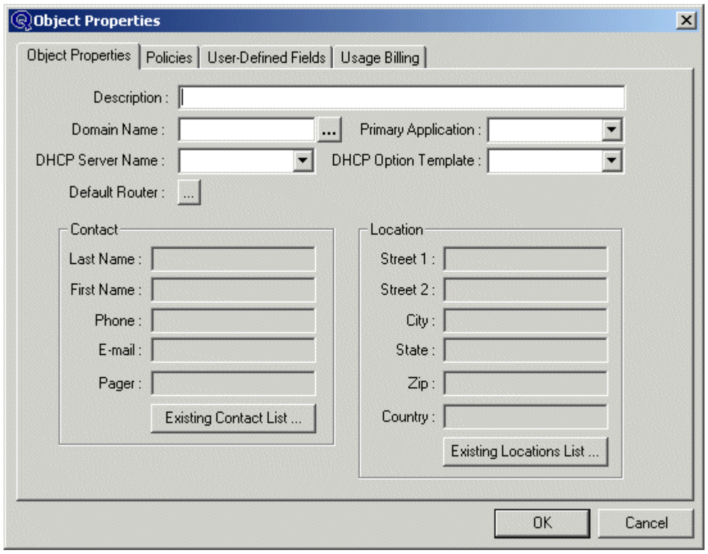
Changes made to the fields here are applied to the selected objects. If no value is entered in the data field, the object retains its original value. For detailed information on the fields in this window, refer to "Manage objects in subnet" (p. 7-26).

Procedure

To edit object properties, follow these steps:

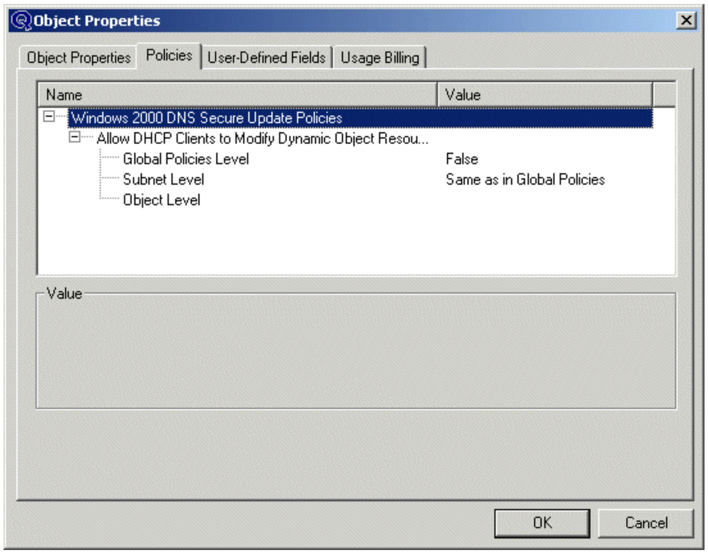
1 Select one or more ***previously defined*** objects in a subnet.

2 Select the **Edit|Object Properties** option. The Object Properties window opens.



3 Add or modify the **Description**, **Domain Name**, **Primary Application**, **DHCP Server Name**, **DHCP Template**, **Default Router** fields and add contacts and locations to this object.

4 The **Policies** tab allows you to set the Windows secure dynamic DNS update policy at the object level. Click the **Policies** tab if you wish to set or modify this policy.

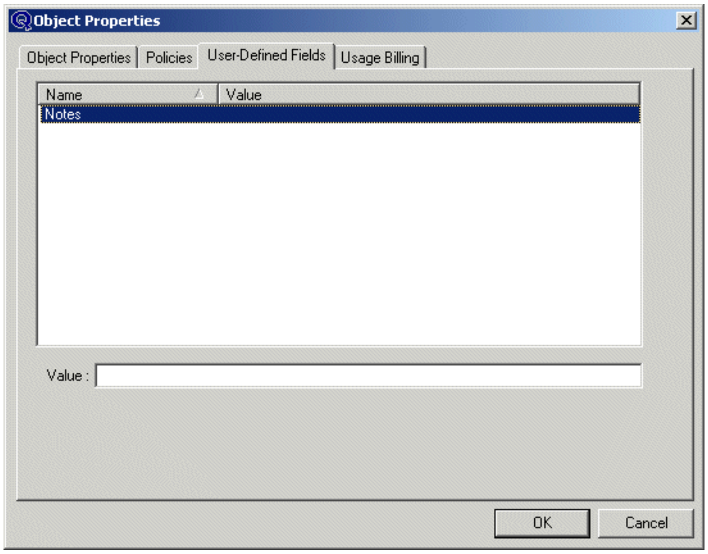


Name	Value
Windows 2000 DNS Secure Update Policies	
Allow DHCP Clients to Modify Dynamic Object Resou...	
Global Policies Level	False
Subnet Level	Same as in Global Policies
Object Level	

5 Select **Object Level** for the **Allow DHCP Clients to Modify Dynamic Object Resource Records** policy. Select one of the following values:

- **False** - disables secure zones with Windows DNS at the object level
- **Same As in Subnet Profile** - uses the Global Policy value to manage secure zones with Windows DNS
- **True** - enables secure zones with Windows DNS at the object level

6 The **User-Defined Fields** tab allows you to add values to already established User-Defined Fields for this object. Click the **User-Defined Fields** tab if you wish to add values to the user-defined fields.



Name	Value
Notes	

Value :

7 Enter the values in the user-defined fields.

END OF STEPS

Manage objects in subnet

In addition to allowing you to manage subnets, **Object Management** allows you to define and manage objects within a subnet. You assign an IP address to an object and fill in an **Object Profile** that provides detailed information on the object. An object can be a workstation, server, printer, router, or any other type of network entity.

Add a static object

Purpose

When you select **Add|Static** from the **Edit** menu or simply double-click on an unused object, the Object Profile appears. At this point, you can add or modify the fields in the Object Profile.

Cancel cancels any work on the object(s).

> **Note:** Do not click **OK** until you are finished filling in fields in *all* tabs of the Object Profile.

> **Note:** To check the number of objects covered by your license, select **Help | About** VitalQIP. To determine how many objects already exist, execute the following commands:

- Sybase:

```
isql -U qipadmin -P password
1>select count(*) from obj_prof
2>go
```

- Oracle:

```
sqlplus qipadmin/password@ORASID
sql>select count(*) from obj_prof
```

If you are already 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.

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.)
- If you select more than one IP address/object to work on from the Object Management window, click **Skip** to skip over one object at a time in the series of objects that you selected. In addition, when you select a series of objects to work on, the context menu available to you offers all options based on the objects and their status.
- You cannot add or modify an object if its MAC address is already defined in another object in the same subnet.
- Do not add more objects to a network than your license allows. Doing so will lock you out of the VitalQIP application.

- VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and the profile cannot be saved while the conflict exists. This feature can be disabled by setting the **Validate CNAMES** sub-policies to False. These polices are under the **Validate CNAME Records** policy. See Table 3-5, "General policies" (p. 3-29) for more information on the policy. When you add or modify an object, validation checks are made against:
  - Object aliases
  - CNAME object resource records
  - CNAME domain resource records
  - CNAME reverse zone resource records
- 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, select **Help | About VitalQIP**. To determine how many objects already exist, execute the following commands:
  - For Sybase:

    ```
    isql -U qipman -P password
    1>select count(*) form obj_prof
    2>go
    ```
  - For Oracle:

    ```
    sqlplus qipman/password@ORASID
    sql>select count(*) form obj_prof
    ```

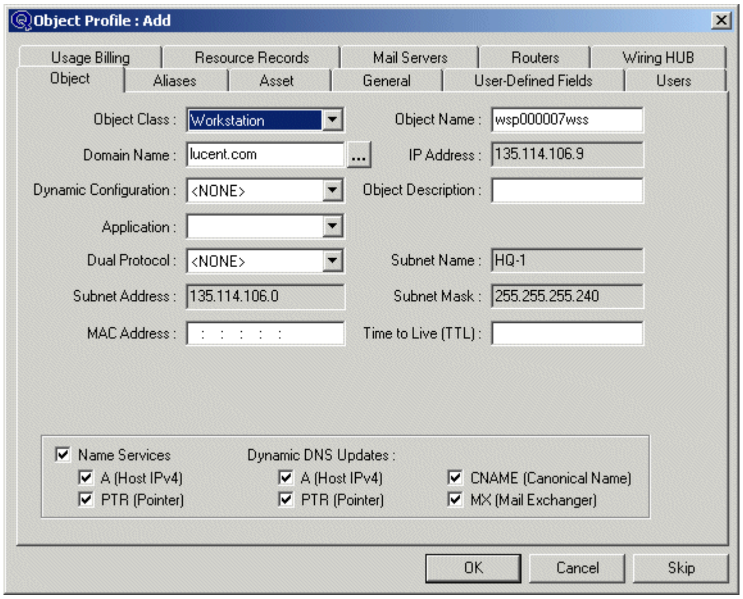
Procedure

To add a static object, follow these steps:

1 Select a subnet from the Object Management: Subnet Selection window.

2 Click **Select** (or double-click on a subnet IP address). The Object Management window (shown in Figure 7-1, "Object management objects" (p. 7-19)) opens.

3 Highlight an IP address or range of IP addresses and press **Enter** (or double-click on an IP address or range of IP addresses to access the Object Profile: Add window.



Object Class :	Workstation	Object Name :	wsp000007wss
Domain Name :	lucent.com	IP Address :	135.114.106.9
Dynamic Configuration :	<NONE>	Object Description :	
Application :			
Dual Protocol :	<NONE>	Subnet Name :	HQ-1
Subnet Address :	135.114.106.0	Subnet Mask :	255.255.255.240
MAC Address :	: : : : :	Time to Live (TTL) :	

☑ Name Services
☑ A (Host IPv4)
☑ PTR (Pointer)

Dynamic DNS Updates :
☑ A (Host IPv4)
☑ PTR (Pointer)
☑ CNAME (Canonical Name)
☑ MX (Mail Exchanger)

4 In the **Object** tab, enter appropriate information as needed. Be sure to select “None” as the value in the **Dynamic Configuration** field. Refer to the following table for a description of each field.

Table 7-5 Object tab fields

Field	Description
Object Class	***Required***. Select an object class from the drop-down list. Depending on the object class you select, different tabs appear because different information is required for each object. **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, etc.) 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 unknown devices. **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 2003 administrators. **Note:** For more information on External and Partially_Managed objects, refer to the *Administrator Reference Manual*.

Field	**Description**
Object Name	***Required***. This field is filled in automatically if your VitalQIP system uses Object Naming Policies as discussed in "Naming policies" (p. 3-11). 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 or a router group, however. 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	Either enter a fully qualified, known domain name, or click **...** to open the Domain Option:Select window. If the administrator is a Master, Organization, or Read-Only Organization; or is a Normal administrator with the "Dynamic Domain Creation" privilege set to True, then you may either select an existing domain, or create a new one. For more information on this option, refer to "Administrators" (p. 6-11), and "Domain folders" (p. 1-40).
IP Address	***Required***. Enter the IP Address associated with the object. This field is filled in automatically. You can enter a different IP address, but it must be unused.
Dynamic Configuration	Select a configuration method for the object: • **None** 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. • **Manual Bootp** allocates the address using the Bootp protocol where the MAC address is defined. The choice of this option adds the **Manual Bootp** tab to the window. • **Automatic Bootp** allocates the address using the Bootp protocol where the MAC address is not known. The choice of this option adds the **Dynamic Configuration** tab to the window. • **Automatic DHCP** allocates the address using the DHCP protocol, from a DHCP template with an infinite lease. The choice of this option adds the **Dynamic Configuration** tab to the window. • **Dynamic DHCP** defines the address using the DHCP protocol, from a DHCP template for a specific lease time. The choice of this option adds the **Dynamic Configuration** tab to the window. • **Manual DHCP** allocates this address using the DHCP protocol where the MAC address is defined. The choice of this option adds the **Dynamic Configuration** tab to the window.
Object Description	Type a description for the object. This field is alphanumeric and allows a maximum of 32 characters. Hyphens and underscores are allowed.

Field	**Description**
Primary Application	Select the primary application associated with this object. For a list of existing applications, click the down arrow next to the field, and select one.
Time Server/Tftp Server	If the object is selected to be a "Server", you can distinguish this server as a Time and/or TFTP server by checking these fields. Selecting the **Time\Tftp Server** checkbox, does not configure the server as a Time or TFTP server. You are responsible for installing and cofiguring the Time or TFTP server as directed by the vendor.
Dual Protocol	Select **None**, **DECNet**, **IPX**, or **NetBIOS**. The selection of any of these options other than **None**, introduces a new tab to the window. If you select **DECNet** as an option in this field, you must fill out the **DECNet** tab. If you selected **NetBIOS**, you must fill out the **NetBIOS** tab. If you selected **IPX**, you must fill out the **IPX** tab.
Subnet Name	This field displays the subnet name.
Subnet Address	The **Subnet Address** field is filled in automatically and cannot be modified.
Subnet Mask	The **Subnet Mask** field is filled in automatically and cannot be modified.
MAC Address	Enter a MAC address here. The same value displays in the **MAC Address** field in the **Asset** tab of the Object Profile. The length of this field is 12 or 16 characters and is determined by the **Allow 16 Character MAC Address** global policy. **Note:** Duplicate MAC addresses are not allowed in the same subnet, even if the **Allow Duplicate MAC Address** global policy is set to True (described in Table 3-5, "General policies" (p. 3-29)). If you attempt to add or modify the object and its MAC address is being used by another object in the same subnet, you receive an error message.
Time to Live (TTL)	The amount of time (in seconds) this information lives on the DNS server.
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. A router group cannot have the same name as an object, alias, or domain in the same zone. **Note:** Router groups can also be used to configure multi-homed objects within VitalQIP, but the objects must be defined as routers.

Field	**Description**
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 overwritten 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.
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 overwritten by the **Dynamic DNS Updates** check boxes that you select here.

5 When you have updated the information in the **Object** tab, proceed to other tabs and add data as needed. Refer to the following sections for information on each tab.

6 Click **OK**. A confirmation prompt opens.

7 Click **OK**. The Object Management appears with the object you added highlighted and displaying a status of “Static”.

Note: When you create a static object and enter the object name as **null**, the object gets created without any errors. However, when you do a DNS generation, the object is displayed as an A record without the name **null**. This creates problems for DNS resolution. Enter the A record for **null** on the Resource Records tab of either the Domain Profile or the IP Object Profile. The word **null** entered as the owner for an A record will not be modified the same way as an object hostname.

END OF STEPS

Enter object aliases

The **Aliases** tab allows you to identify one or more aliases for an object.

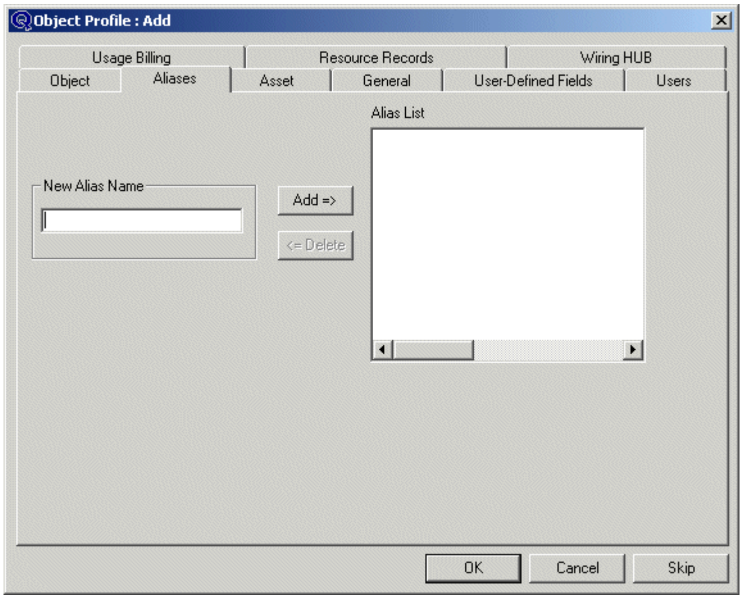
Before you begin

- 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 the profile cannot be saved while the conflict exists. This feature can be disabled by setting the **Validate CNAMES** sub-policies to False. These polices are under the **Validate CNAME Records** policy. See Table 3-5, "General policies" (p. 3-29) for more information on the policy. When you add or modify CNAME records, validation checks are made against:
  - Object aliases
  - 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
- Aliases associated with a Manual DHCP object are not dynamically updated in DNS when a Manual DHCP object changes its name during a DHCP lease renew. To fix this problem, a DNS push is required. Another DNS solution is to define an "A" record in the **Resource Record** tab that maps to the IP address of the Manual DHCP object.

Procedure

To complete the **Aliases** tab, follow these steps:

1 Click the **Aliases** tab.



2 Enter an alias (of up to 63 alphanumeric characters) in the **New Alias Name** field. Hyphens and underscores are allowed.

3 Click **Add**. The alias appears in the **Aliases List**. If you added an alias in error, you can remove it by selecting it and clicking **Delete**.

END OF STEPS

Alias example

The following examples illustrate how VitalQIP processes alias names. The object “myhostname” has been added in the domain “quadritek.com”. The alias names have been added to the **Aliases** tab in the Object Profile. Use the following legend to help read the examples.

Domain	Status
quadritek.com	Managed in VitalQIP
qa.quadritek.com	Managed in VitalQIP
test.com	Managed in VitalQIP
noqip.com	***Not*** managed in VitalQIP

Table 7-6 Example 1: Pushed to “quadritek.com” zone file (db.quadritek.com)

Alias Name	`www`
Written to	`www.quadritek.com.  IN  CNAME`
Explanation	The alias entered is not fully qualified (VitalQIP interprets aliases ending with a period as fully qualified names); VitalQIP therefore assumes the
Alias Name	`www3.quadritek.com`
Written to	`www3.quadritek.com.  IN  CNAME`
Explanation	The alias entered is not fully qualified, but the zone *quadritek.com* ***does*** exist. VitalQIP therefore assumes that the alias belongs under the
Alias Name	`www4.quadritek.com.`
Written to	`www4.quadritek.com.  IN  CNAME`
Explanation	The alias entered ***is*** fully qualified (note trailing period in entered alias name) and the *quadritek.com* zone ***does*** exist; VitalQIP therefore writes
Alias Name	`www5.test.com`
Written to	`www5.test.com.quadritek.com.  IN  CNAME`
Explanation	The alias entered is ***not*** fully qualified and, even though the *test.com* zone ***does*** exist within VitalQIP, VitalQIP still writes the alias Resource Record
Alias Name	`www7.noqip.com`
Written to	`www7.noqip.com.quadritek.com.  IN  CNAME`
Explanation	The alias entered is ***not*** fully qualified and the zone *noqip.com* does not exist within VitalQIP; VitalQIP writes the alias Resource Record to the

Table 7-7 Example 2: Pushed to “test.com” zone file (db.test.com)

Alias Name	`www6.test.com.`
Written to DNS	`www6.test.com.   IN   CNAME`
Explanation	The alias entered ***is*** fully qualified *and* the test.com domain ***does*** exist within VitalQIP; VitalQIP therefore writes the alias Resource Record to

Table 7-8 Example 3: Pushed to “qa.quadritek.com” zone file (db.qa.quadritek.com)

Alias Name	`www1.qa`
Written to DNS	`www1.qa.quadritek.com.  IN  CNAME`
Explanation	The alias entered is not fully qualified, but the *qa.quadritek.com* zone ***does*** exist; VitalQIP therefore places the above alias Resource Record in
Alias Name	`www2.qa.`
Written to DNS	
Explanation	Not pushed out at all because the domain *qa* does not exist within
Alias Name	`www8.noqip.com.`
Written to DNS	
Explanation	Not pushed out at all because the domain *noqip.com.* does not exist

Enter asset information

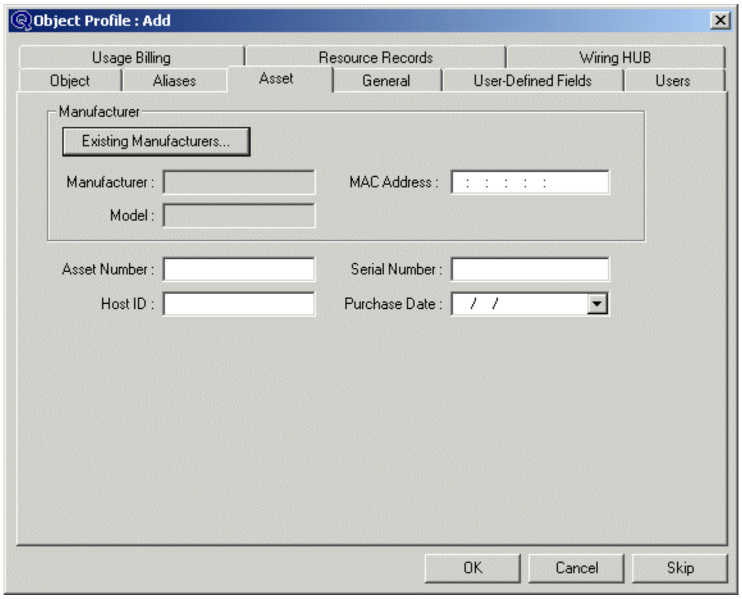
Purpose

You can establish **Asset** information in this window. Asset information is generally referred to as additional hardware/object information you want to keep track of.

Procedure

To enter asset information, follow these steps:

1 Select the **Asset** tab.



2 Fill in the fields described in the following table.

Table 7-9 Asset tab fields

Field	Description
Manufacturer	Click **Existing Manufacturer(s) List** and the Manufacturer's List window opens. Select a manufacturer from the list. If there are Models associated with the manufacturers, they will list in this window as well (only if you selected from the **Existing Manufacturer(s) List**). If you selected a manufacturer, and there are models associated with that particular manufacturer, they appear in the window, as well.
MAC Address	Type the **MAC Address** for this object. If you selected a manufacturer from the listing, this field will be filled in automatically with the prefix for the manufacturer's default MAC address. The remaining octets need to be completed. If the manufacturer's prefix is zeroes (0), you are not required to complete the remaining octets and the MAC address is assumed to be blank. This field is required if an object is tagged as Bootp. This field is a hexadecimal integer (uses 0-9 and A-F only) and is a maximum of 12 or 16 digits. The length is determined by the **Allow 16 Character MAC Address** global policy. Otherwise, enter a MAC Address for the manufacturer. **Note:** Duplicate MAC addresses are not allowed in the same subnet. If you attempt to modify or add an object and its MAC address is being used by another object in the same subnet, you will receive an error message.
Model	If you selected a manufacturer, and there are models associated with a particular manufacturer, they are displayed here.
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	Type 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.
Date of Purchase	Enter the date this asset was purchased.

END OF STEPS

Enter general information

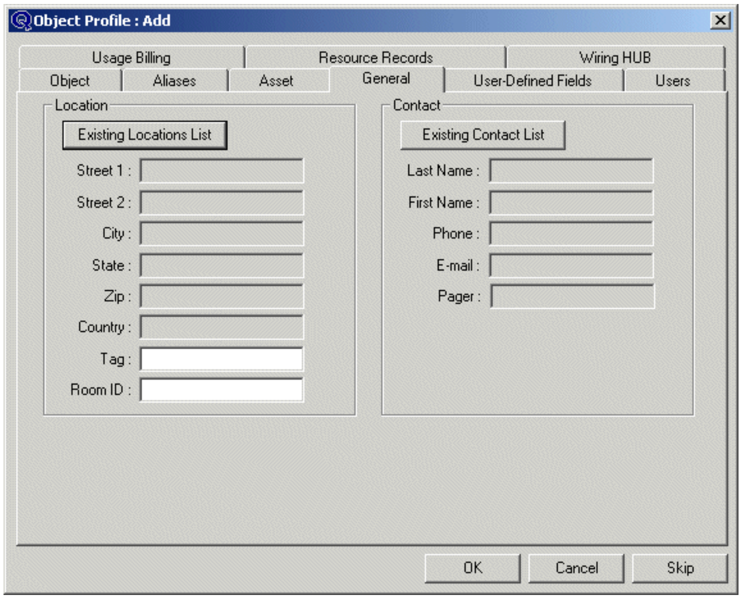
Purpose

The **General** tab allows you to select the **General** information for an object, such as Location and Contact information for the object. The Location and Contact information is defaulted from the Subnet Profile when a new object is added, unless you specify a location and contact for the object here.

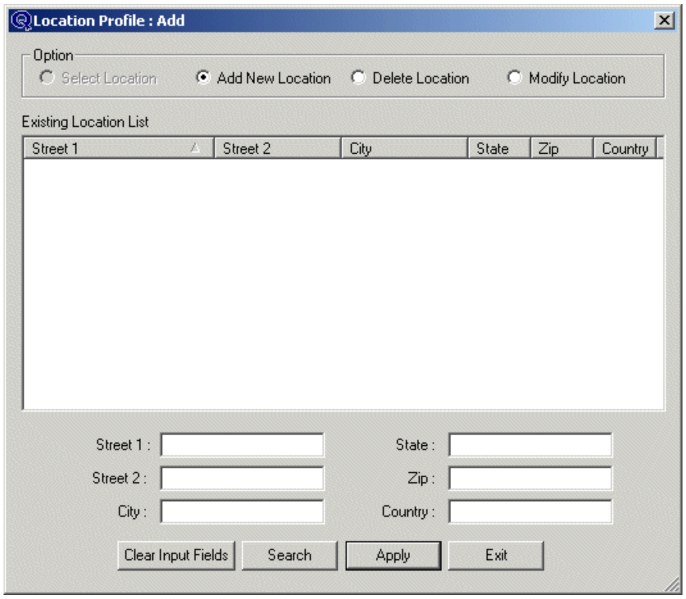
Procedure

To enter general information about an object, follow these steps:

1 Click the **General** tab.



2 If you require a list of current locations available to you, click **Existing Locations List**. The Location Profile window opens.



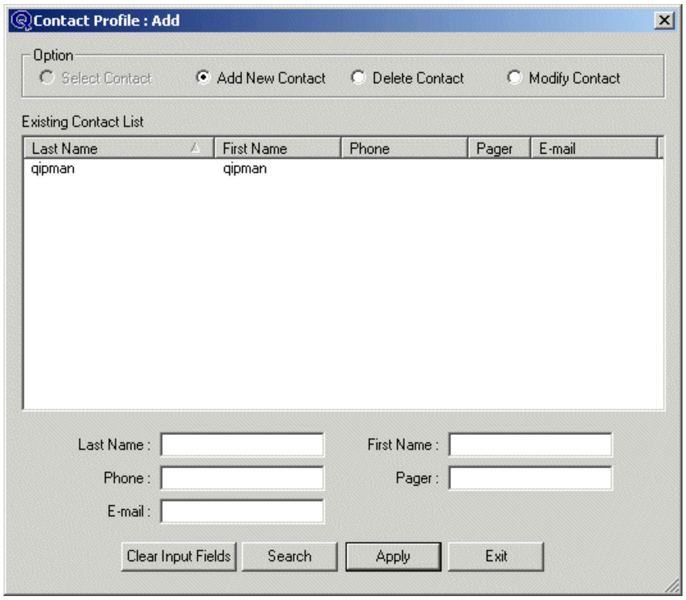
This window is identical to the window that displays if you select the **Location Profile** option under **Policies**. **Select Location** should already be selected.

3 Highlight the location you wish to apply to an object and click **Apply**. The **Object Profile|General** tab displays the information you selected.

You can also add, delete, and modify locations (refer to "Manage location profiles" (p. 3-49) for further information).

4 Enter a Manufacturer **Tag** and a **Room ID** for an object if required.

5 If you would like to see a list of current contact information, click **Existing Contact List**, and a list displays in the Contact Profile window. It works identically to the Location Profile.



Last Name	First Name	Phone	Pager	E-mail
qipman	qipman			

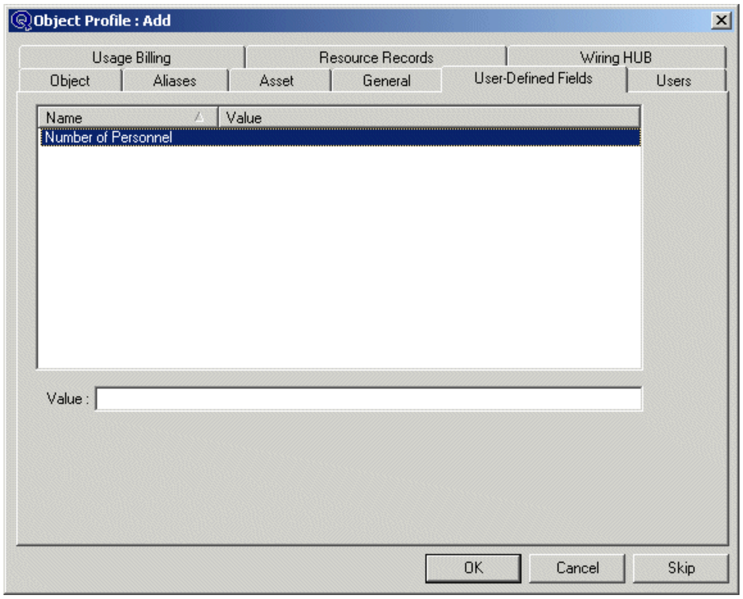
6 Highlight the contact you wish to apply to an object and click **Apply**. The **Object Profile|General** tab displays the information you selected.

You can also add, delete, and modify contact information (refer to "Manage contact profiles" (p. 3-51) for further information).

END OF STEPS

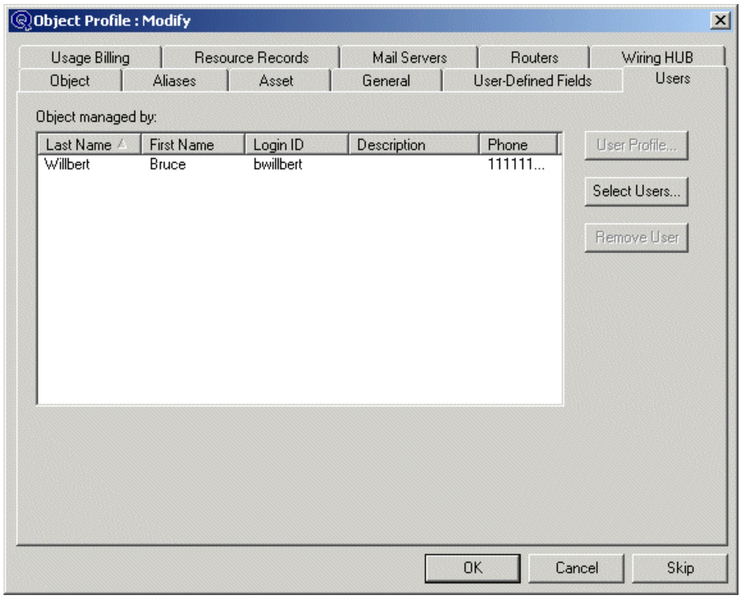
Enter user-defined fields

User-Defined Fields for objects (as well as subnets, users, domains, reverse zones, and organizations) are established in the **Policies|User-Defined Fields** option of the interface. The **User-Defined Fields** tab of the Object Profile window displays those fields and allows you to enter values against them, in relation to objects. For instance, if you want to associate an Internal Tracking Number with an object, highlight that User-Defined field and enter a value.



Enter users' information

Users associated with an object are listed in the **Users** tab. Sort on any of the fields in the title bar by clicking on it.



Object managed by:

Last Name	First Name	Login ID	Description	Phone
Willbert	Bruce	bwillbert		111111...

You can view the User's profile if you select a user from the list and click **User Profile**. You can also modify information on the user through this function. Alternatively, you can assign users to an object by clicking **Select Users**. This button will only be enabled if the Administrator Profile privilege "Allow User Selection" is set to True. If the privilege "Require User" is set to True, at least one user must be assigned to an object. Refer to "Administrators" (p. 6-11) for more information. Users can be associated with objects in the **User Management|User Profile** function on the **Management** menu.

To remove a user from an Object Profile, select the user and click **Remove User**. The user is not removed from the entire system, just from the Object Profile.

Enter resource record information

Purpose

The **Resource Records** tab allows you to create and modify Resource Records for a domain if your Administrator Profile has the "Create Resource Records" privilege selected. This function allows resource records for the domain to be written to the DNS configuration files. VitalQIP validates and formats the information on input.

Before you begin

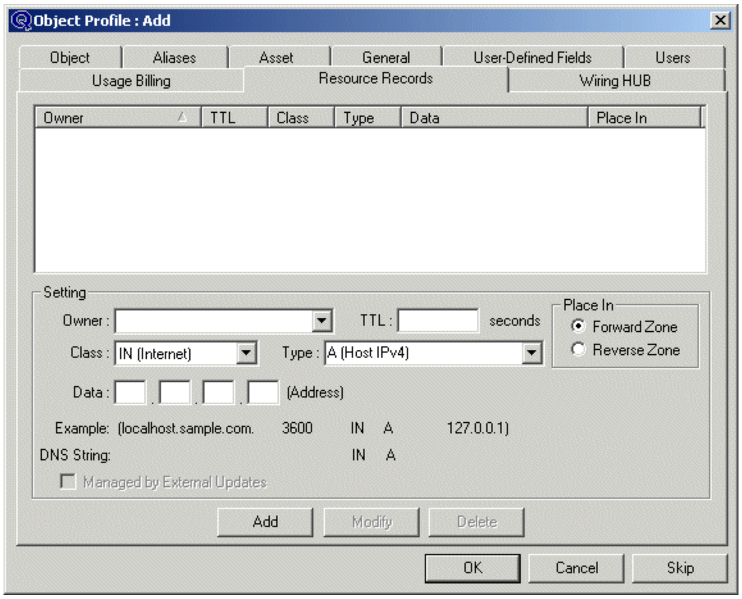
- VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and the profile cannot be saved while the conflict exists. This feature can be disabled by setting the **Validate CNAMES** sub-policies to False. These polices are under the **Validate CNAME Records** policy. See Table 3-5, "General policies" (p. 3-29) for more information on the policy. When you add or modify records other than CNAME records, validation checks are made against:
  - Object aliases
  - CNAME object resource records
  - CNAME domain resource records
  - CNAME reverse zone resource records

  When you add or modify CNAME records, 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
- If the Administrator's "Create Resource Records" privilege is disabled (False), the **Resource Records** tab is not displayed for Domains, Reverse Zones, or Objects.

Procedure

To enter resource record data for an object, follow these steps:

1 Select the **Resource Records** tab.



Owner :

TTL : seconds

Class : IN (Internet)

Type : A (Host IPv4)

Place In: ● Forward Zone ○ Reverse Zone

Data : . . . (Address)

Example: (localhost.sample.com. 3600 IN A 127.0.0.1)

DNS String: IN A

□ Managed by External Updates

2 Fill in the fields described in the following table.

Table 7-10 Resource Records tab fields

Field	Description
Owner	Select from the default **Owner** options supplied, or enter whatever you are using to define the Owner for this object. Defaults are HOST_NAME or FULL_NAME. The HOST_NAME is the value you entered in the **Object Name** field in the **Object** tab for this object. The FULL_NAME is the value you entered in the **Object Name** field plus the value in the **Domain Name** field (this is a fully qualified Domain Name).
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, or enter the class(es) you want to use for this object.
TTL (Time To Live)	The length of time (in seconds) the name server will hold this information. If no TTL is defined, unlimited is implied.

Field	Description
Type	Select the **Type** of Resource Record from the listing, or enter your own **Type** in this field. For additional information on these record types, refer to *DNS and BIND*, by Cricket Liu and Paul Albitz. **Note:** If you select **WKS**, the **Protocol** field is usually UDP or TCP, although it can be any entries in */etc/protocols*. The **Service** field consists of a service list below port number 256 for the */etc/services* files. If you select **SRV**, the **Priority**, **Weight**, and **Port** fields are unsigned 16-bit numbers (between 0 and 65535). The **Target** field is a domain name.
Data	The data associated with the specific resource record type. Whenever you select a Resource Record **Type** in the **Setting** section, the **Data** control is updated to allow for the correct formatting of the selected resource record. Based on the Resource Record Type you select, different settings appear in the Data and Example area of the **Setting** section. For information on these settings, refer to Table 5-3, "Setting fields" (p. 5-23).
Place In (Forward Zone/Reverse Zone)	Select where you want to place the resource records after they are generated; in the Forward Zone or the Reverse Zone.
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 VitalQIP QIP Update Service. 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*.

3 Once you input all the required information, click **Add**, and the Resource Record is displayed in the upper portion of the window.

4 To modify a Resource Record in the listing, select it, alter the values in the lower portion accordingly, and click **Modify**.

5 To delete a Resource Record in the listing, select it and click **Delete**.

END OF STEPS

Enter router information

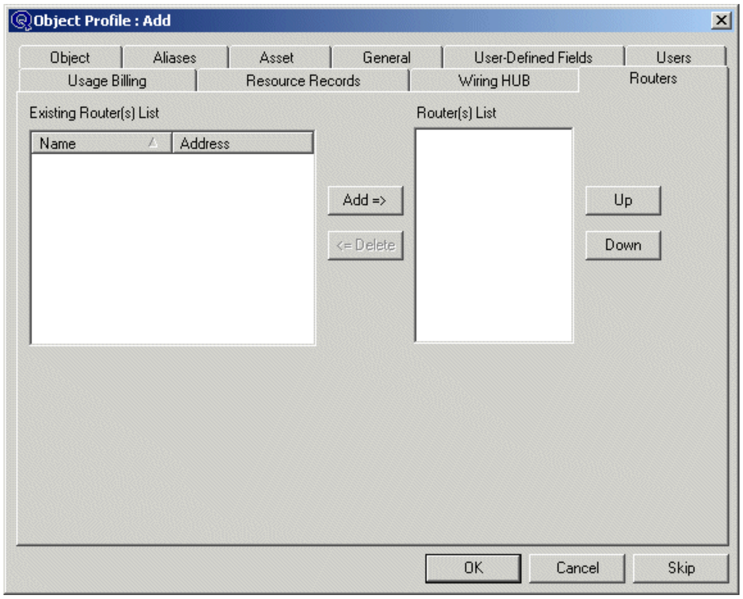
Purpose

Use this procedure to assign one or more routers to an object.

Procedure

To assign a router to an object, follow these steps:

1 Select the **Routers** tab.



2 Select a router associated with an object from the **Existing Router(s) List**.

3 Click **Add** to place it in the current **Router(s) List**.

4 If there is more than a single router in the **Router(s) List** and you wish to specify which router has precedence over another, select an assigned router and click **Up** to move it higher on the list and **Down** to move it lower.

5 To remove a router from the assigned list, highlight a router and click **Delete**.

END OF STEPS

Enter mail server information

Purpose

You can define the object that is designated to forward mail to another defined mail host by using the **Mail Servers** tab. The function creates an MX record.

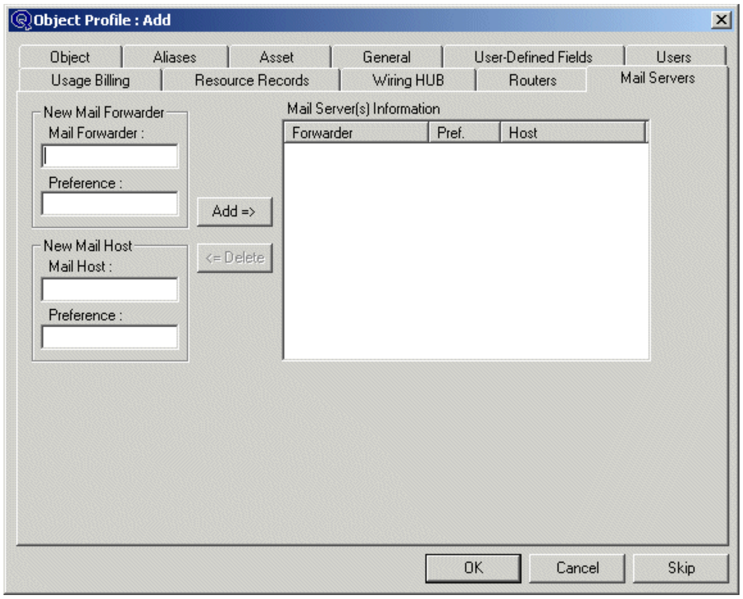
Before you begin

- VitalQIP validates data to prevent CNAME conflicts in the same organization by default. If a CNAME conflict occurs, an error message displays, and the profile cannot be saved while the conflict exists. This feature can be disabled by setting the **Validate CNAMES** sub-policies to False. These polices are under the **Validate CNAME Records** policy. See Table 3-5, "General policies" (p. 3-29) for more information on the policy. When you add or modify a mail server, validation checks are made against:
  - Object aliases
  - CNAME object resource records
  - CNAME domain resource records
  - CNAME reverse zone resource records

Procedure

To complete the **Mail Servers** tab, follow these steps:

1 Select the **Mail Servers** tab.



2 You can either add to or delete mail server information for the current object.

3 Fill in the fields described in the following table.

Table 7-11 Mail Servers tab fields

Field	Description
New Mail Forwarder	To add a mail forwarder, enter the object or domain name of the **Mail Forwarder** in this field. Establishing this name will allow mail to be forwarded on to its final destination.
New Mail Forwarder 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. You can assign the "best" mail exchanger with a preference value "0".
New 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.
New Mail Host 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. You can assign the "best" mail exchanger with a preference value of "0".

END OF STEPS

Enter wiring HUB information

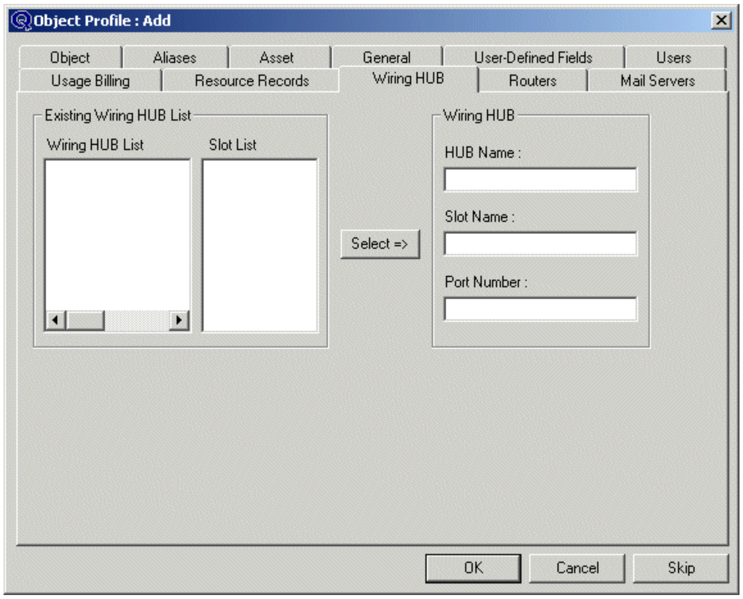
Purpose

The **Wiring HUB** tab allows you to identify the Wiring HUB associated with this object.

Procedure

To complete the **Wiring HUB** tab, follow these steps:

1 Select the **Wiring HUB** tab. A list of existing Wiring HUBs appears, along with the associated slots.



2 Select a Wiring HUB from the **Wiring Hub List**.

3 Select a Slot name from the **Slot List** you wish to associate with this object.

4 Click **Select** to associate it with the object.

5 The next available port on this slot is automatically assigned, and the port number appears in the **Port Number** field. You can also enter a known Port Number in this field without selecting from the list.

END OF STEPS

Enter wiring HUB slot and port

Purpose

Use this procedure to add wiring HUB slot and port information to an object.

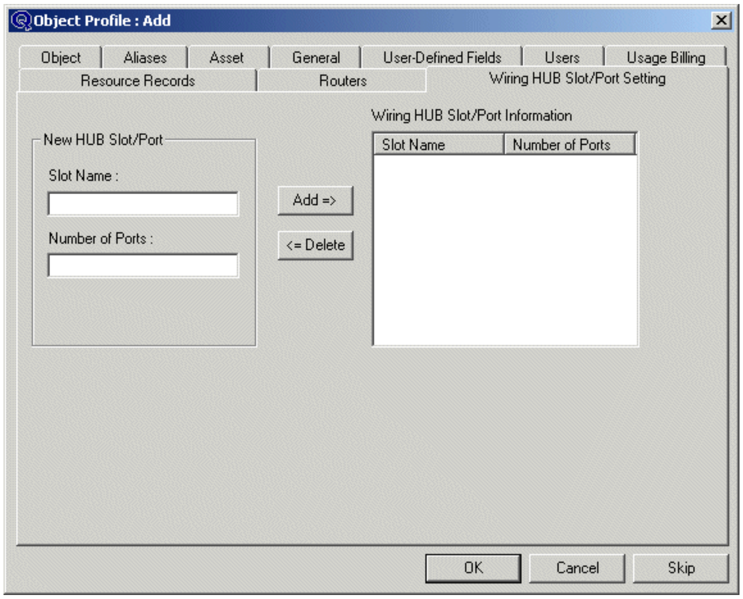
Before you begin

The **Wiring HUB Slot/Port** tab appears only when “Wiring HUB” is selected in the **Object Class** field on the Object Profile.

Procedure

To add wiring HUB information for an object, follow these steps:

1 Select the **Wiring HUB Slot/Port Setting** tab.



2 Enter a slot name in the **Slot Name** field.

3 Enter the number of port slots in the **Number of Ports** field.

4 Click **Add** to enter the slot name/port information in the **Wiring HUB Slot/Port Information** list.

5 To delete a slot name from an existing list of **Wiring HUB Slot/Port Information**, select the slot name and click **Delete**.

END OF STEPS

Enter DECNet information

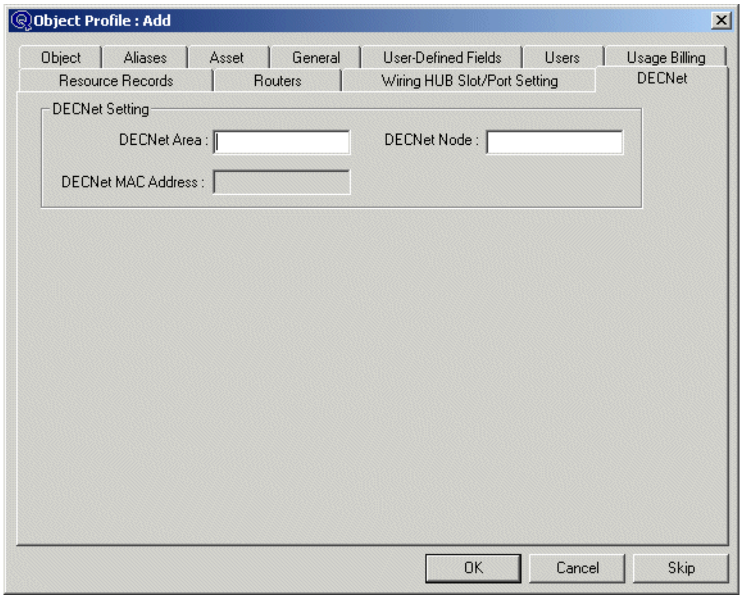
Purpose

The **DECNet** tab is only available if you chose “DECNet” as your value in the **Dual Protocol** field of the **Object** tab.

Procedure

To complete the **DECNet** tab, follow these steps:

1 Select the **DECNet** tab.



2 Fill in the fields described in the following table.

Table 7-12 DECNet tab fields

Field	Description
DECNet Area	Type the **DECNet Area**. This value can be between 1 and 63.
DECNet Node	Type the **DECNet Node**. This value can be between 1 and 1023.
DECNet MAC Address	The **DECNet MAC Address** field is filled in automatically once the first two fields are filled in, and it cannot be changed.

END OF STEPS

Enter IPX information

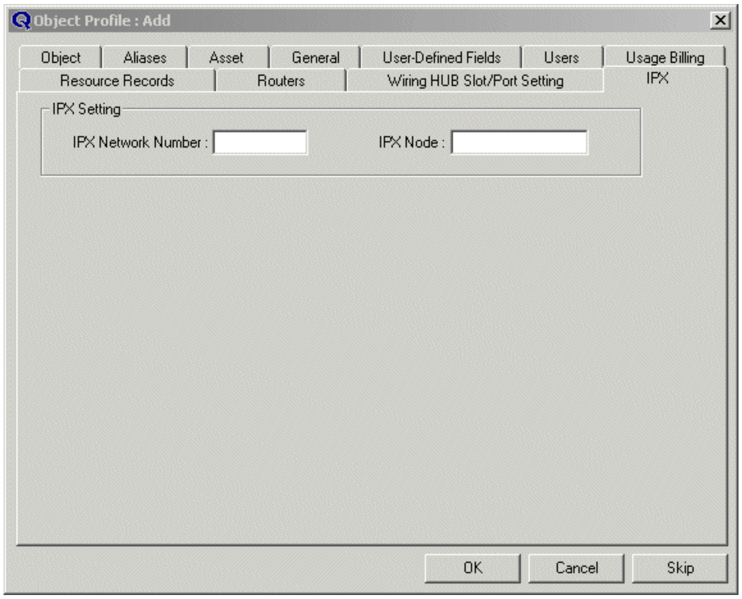
Purpose

The **IPX** tab is only available if you chose “IPX” as your value in the **Dual Protocol** field on the **Object** tab. These two fields together form a unique station address, which is presumed to be unique in the world. Net and node numbers are represented in ASCII in either block or dashed notation as: ‘0101a040,00001b498765’ . Leading zeros need not be present.

Procedure

To complete the **IPX** tab, follow these steps:

1 Select the **IPX** tab.



2 Fill in the fields described in the following table.

Table 7-13 IPX tab fields

Field	Description
IPX Network Number	The **IPX Network Number** is an administrative domain and typically names a single ethernet or token ring segment.
IPX Node	The **IPX Node** number is a station’s physical address.

Enter NetBIOS information

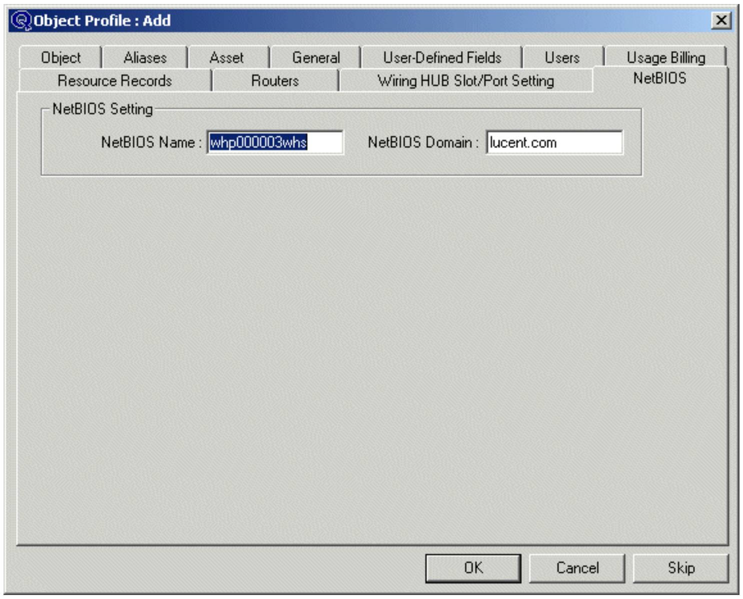
Purpose

The **NetBIOS** tab is only available if you chose “NetBIOS” as your value in the **Dual Protocol** field on the **Object** tab.

Procedure

To complete the **NetBIOS** tab, follow these steps:

1 Select the **NetBIOS** tab.



NetBIOS Name : whp000003whs

NetBIOS Domain : lucent.com

2 Fill in the fields described in the following table.

Table 7-14 NetBIOS tab fields

Field	Description
NetBIOS Name	Enter the **NetBIOS Name** associated with the NetBIOS of this object. The default is the same as the object name.
NetBIOS Domain	Enter the **NetBIOS Domain** associated with the NetBIOS of this object. The default is the same as the domain name for this object.

Enter Manual Bootp information

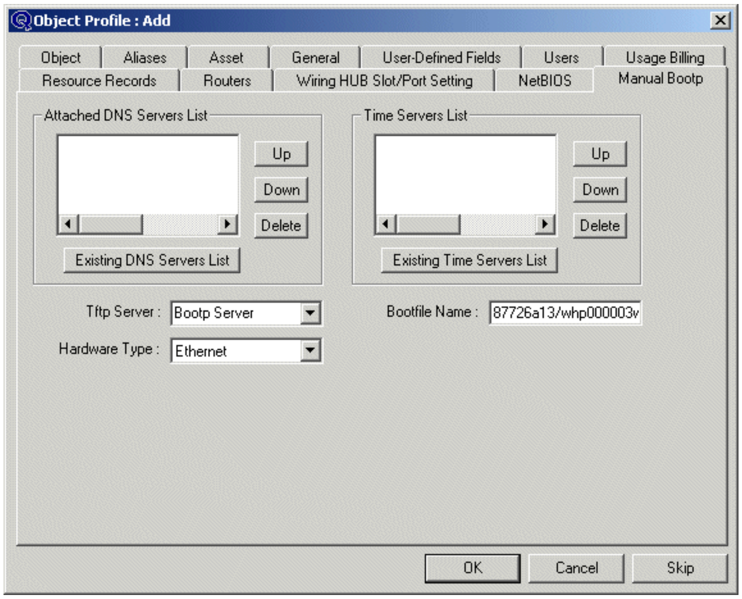
Purpose

The **Manual Bootp** tab is only available if you selected “Manual Bootp” as the value for the **Dynamic Configuration** field of the **Object** tab.

Procedure

To complete the **Manual Bootp** tab, follow these steps:

1 Click the **Manual Bootp** tab.



Tftp Server : Bootp Server

Hardware Type : Ethernet

Bootfile Name : 87726a13/whp000003v

2 Select the DDNS/DNS servers associated with this object. If none are displayed, click **Existing DNS Servers List** and select servers from the Server List window. Use **Up** and **Down** to order the DDNS/DNS servers.

3 Click **OK** to close the Server List window. The selected servers appear in the **Attached DNS Servers List**.

4 Select the Time servers associated with this object. If none are displayed, click **Existing Time Servers List**. Use **Up** and **Down** to order the DDNS/DNS servers.

5 Click **OK** to close the Server List window. The selected server(s) appear in the **Time Servers List**.

6 By default, the **Tftp Server** is the same as the Bootp server. If you wish to select a different TFTP server, click the down arrow next to the field and select a server.

7 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.

8 Select the **Hardware Type** for the object from the drop-down list.

END OF STEPS

Enter Dynamic Configuration information

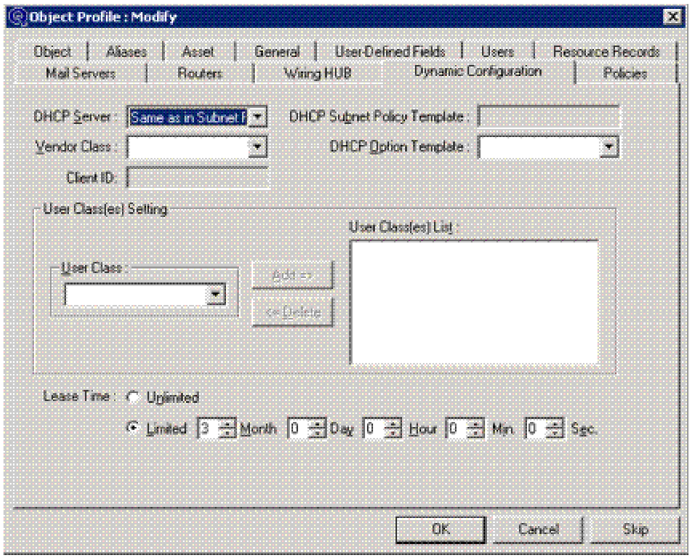
Purpose

The **Dynamic Configuration** tab is only available if you selected **Automatic Bootp, Manual DHCP**, **Automatic DHCP** or **Dynamic DHCP** from the **Dynamic Configuration** field on the **Object** tab. You can use this tab to assign DHCP settings to the object.

Procedure

To complete the **Dynamic Configuration** tab, follow these steps:

1 Select the **Dynamic Configuration** tab.



DHCP Server : Same as in Subnet I

Lease Time : ○ Unlimited ● Limited 3 Month 0 Day 0 Hour 0 Min. 0 Sec.

2 Fill in the fields described in the following table.

Table 7-15 Dynamic Configuration fields

Field	Description
DHCP Server	Assign a **DHCP Server** to this object. View the list of available DHCP servers by clicking the down arrow next to the field. The field defaults to the DHCP Server defined in the Subnet Profile. Select **Same as in subnet profile** if the object is in a subnet managed by a subnet organization and you wish to use settings associated with a DHCP server previously assigned to that subnet organization.
Vendor Class	Select a **Vendor Class** from the drop-down list. For more information on Vendor Class, refer to "DHCP/Bootp templates" (p. 2-3). **Note:** If you selected **Manual DHCP** as the Dynamic Configuration in the Object Profile, the **Vendor Class** field will be disabled.
Client ID	This field is displayed only if the dynamic configuration is **Dynamic DHCP**, **Manual DHCP**, or **Automatic DHCP**. It will not appear when the dynamic object is being added. This field will appear only when a dynamic object is being viewed, modified, or deleted. This field is a hexadecimal encoded string.
User Class	***This field is for Lucent DHCP only***. The **User Class** allows you to define specific categories of users options; for example, assigning a **User Class** for mobile computing that would specify a shorter lease time. Select a User Class from the **User Class** drop-down list and click **Add** to add the User Class to the User Classes list. User Classes can be deleted from the User Classes list. **Note:** If you selected **Manual DHCP** as the Dynamic Configuration in the Object Profile, the **User Class** field will be disabled.
DHCP Subnet Policy Template	This policy is set in the Subnet Profile. This field is filled in automatically and cannot be modified.

Field	Description
DHCP Option Template	Assign a **DHCP Option Template** to this object. View the list of available DHCP option templates by clicking the down arrow next to the field. Select **Same as subnet** if the object is in a subnet managed by a subnet organization and you wish to use settings associated with a DHCP Option Template previously assigned to that subnet organization.
DHCP Scope Policy Template	Assign a DHCP Scope Policy Template. View the list of available DHCP Scope Policy Templates by clicking the down arrow next to the field. Refer to "DHCP policy templates" (p. 2-63) for more information on setting up scope policy templates.
IBM Class Option Template	***This field applies to IBM DHCP only***. Class templates apply to a particular vendor class within a subnet. They should be used instead of assigning a template to a set of objects within a subnet. Click on the arrow next to the field to view a list of Class Option Templates. You can select from this list. **Note:** If you selected **Manual DHCP** as the Dynamic Configuration in the Object Profile, the **Class Option Templates** field will be disabled.
Lease Time	***This field is for Dynamic DHCP only, all others are 'Unlimited'***. If you wish the lease time to be limited, click **Limited**, then select a time interval in months, days, hours, minutes, and/or seconds. The default lease time is 3 months. If a lease time is defined in the DHCP Template (Option 51), the lease time defined in the template overwrites the value defined here. **Note:** This field only displays the default lease time and not the actual lease time. The actual lease time can be viewed in the DHCP template or using **Network Services | View Active Leases**.

END OF STEPS

Enter Windows DNS secure update policies

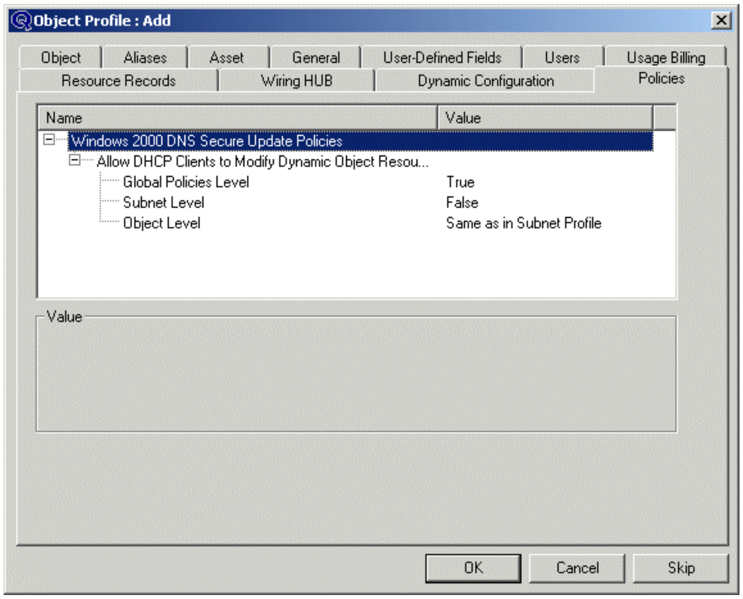
Purpose

The **Policies** tab appears when **Dynamic Configuration** is set to **Automatic Bootp**, **Manual DHCP**, **Automatic DHCP** or **Dynamic DHCP** on the **Object** tab. If you are using a secure zone with Windows DNS, you can define whether a Dynamic DHCP object uses secure zones at the object level.

Procedure

To set Windows DNS secure update policies, follow these steps:

1 Click the **Policies** tab.



Name	Value
Windows 2000 DNS Secure Update Policies	
Allow DHCP Clients to Modify Dynamic Object Resou...	
Global Policies Level	True
Subnet Level	False
Object Level	Same as in Subnet Profile

2 Select **Object Level** for the **Allow DHCP Clients to Modify Dynamic Object Resource Records** policy.

3 Select one of the following values:

- **False** - disables secure zones with Windows DNS at the object level
- **Same As in Subnet Profile** - uses the Global Policy value to manage secure zones with Windows DNS
- **True** - enables secure zones with Windows DNS at the object level

4 Click **OK** when you are ready to save the profile.

END OF STEPS

Allocate a dynamic IP address

Purpose

Dynamic allocation allows you to assign one or more addresses designated for use with DHCP/Bootp (otherwise known as dynamic objects) and lets you fill in information (through the Object Profile) about the objects later, through the **Add|Dynamic** option. You also have the ability to modify or un-allocate dynamic addresses, and modify the parameter settings for objects.

The following dynamic allocation configuration methods are available:

- **Dynamic/Static (none)** allocates addresses to be defined at a later time as DHCP or Bootp addresses. This type is used as a placeholder for dynamic-type objects that have not been defined yet.
- **Manual Bootp** defines addresses as using the Bootp protocol where the MAC address is defined.
- **Automatic Bootp** defines addresses as using the Bootp protocol where the individual MAC addresses are not known.
- **Manual DHCP** defines addresses as using the DHCP protocol where the MAC address is defined.
- **Automatic DHCP** defines addresses as using the DHCP protocol, using a DHCP template and having an infinite lease.
- **Dynamic DHCP** defines addresses as using the DHCP protocol, using a DHCP template for a specific lease time.

Before you begin

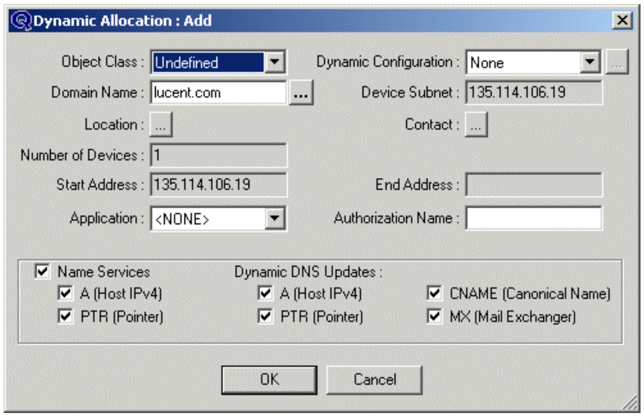
- If objects are selected before selecting the **Edit|Add|Dynamic** menu option, the **Number of Devices**, **Start Address** and **End Address** fields are filled in automatically and cannot be edited. Otherwise, these fields are blank by default and values must be entered by the user.
- If you try to add more objects than the maximum number established for your organization, you will receive an error message and the objects cannot be added. See "Add an organization" (p. 5-5) for more information.

Procedure

To allocate one or more dynamic IP addresses, follow these steps:

1 Highlight one or more objects with the status of "Unused" in the Object Management window.

2 Select **Add | Dynamic** from the **Edit** menu, or right-click on the addresses/objects and select **Add**. The Dynamic Allocation: Add window opens.



Dynamic Allocation : Add

Object Class : Undefined

Dynamic Configuration : None

Domain Name : lucent.com

Device Subnet : 135.114.106.19

Location : ...

Contact : ...

Number of Devices : 1

Start Address : 135.114.106.19

End Address :

Application : <NONE>

Authorization Name :

☑ Name Services

☑ A (Host IPv4)

☑ PTR (Pointer)

Dynamic DNS Updates :

☑ A (Host IPv4)

☑ PTR (Pointer)

☑ CNAME (Canonical Name)

☑ MX (Mail Exchanger)

3 Fill in the Dynamic Allocation: Add window as desired, referring to the following table for information on the fields.

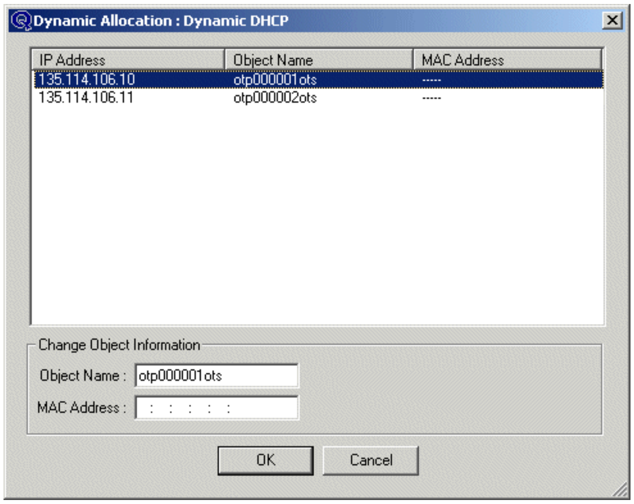
Table 7-16 Dynamic Allocation fields

Field	**Description**
Object Class	If you wish to assign an object class (Workstation, Router, and so on) to the addresses, select the class.
Dynamic Configuration	Select a dynamic allocation method for this object: **None**, **Manual Bootp**, **Automatic Bootp**, **Manual DHCP**, **Automatic DHCP**, or **Dynamic DHCP**. Based on your selection here, when you click **...** next to the **Dynamic Configuration** field, one of two different windows appears so that you can supply the Dynamic Object with the appropriate information. For further information on configuring Manual Bootp values, refer to "Manual Bootp setup" (p. 7-71). For further information on configuring the other dynamic allocation methods, refer to "Automatic Bootp and DHCP configuration" (p. 7-72).
Domain Name	Either enter a full qualified, known domain name, or click **...** to display the Domain Option: Select window. If the **Display Domain Folders** option in the Administrator Profile is set, this field is a browse-edit function. You can select or type in the domain. If not, domains display in list format. For more information on this option, refer to "Administrators" (p. 6-11) and "Domain folders" (p. 1-40).
Device Subnet	This field reflects the subnet in which the IP address is located.

Field	**Description**
Location	Click this button to display the Location Profile. By default, VitalQIP assigns the location defined in the Subnet Profile. You can select a different location by clicking **...** for a list of locations. Select a location from the list and click **Apply**. You can also add, delete, and modify locations.
Contact	Click this button to display the Contact Profile. By default, VitalQIP assigns the contact defined in the Subnet Profile. You can select a different contact by clicking **...** for a list of contacts. Select a contact from the list and click **Apply**. You can also add, delete, and modify contacts.
Number of Devices	If you highlighted one or more addresses (as opposed to selecting the **Edit|Add|Dynamic** option from the Object Management window without highlighting addresses), this field shows the number of addresses you selected. If you did not select IP addresses, fill in the number of IP addresses you wish to reserve. If you specify the number of devices, VitalQIP picks the "first" available address and allocates the number of objects you specified.
Start Address/End Address	If you do not specify a Number of Devices, you can enter the address range manually by specifying a **Start Address** and **End Address**. If you specify a **Start Address**, you ***must*** specify **End Address**; therefore, the number of devices is not required. If you selected a range of addresses in the Object Management window prior to selecting **Edit|Add|Dynamic**, these fields are calculated for you.
Application	Specify the name of the application you wish to assign to the IP address or addresses. The application field is used to associate 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.
Authorization Name	The person who authorized the dynamic allocation of the addresses.
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 (**Dynamic DNS Mask** and **Static DNS Mask**), but can be overwritten by the **Name Services** options you select here. When a push occurs (**Network Services** function), whatever values are checked will be written to the server.

Field	Description
Dynamic DNS Updates	Select the 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 (**Dynamic DNS Mask** and **Static DNS Mask**), but they can be overwritten by the **Dynamic DNS Updates** options that you select here.

4 When you have finished filling in the Dynamic Allocation window, click **OK**. A new window appears, listing the IP addresses that will be dynamically allocated.



Dynamic Allocation : Dynamic DHCP

IP Address	Object Name	MAC Address
135.114.106.10	otp000001ots	-----
135.114.106.11	otp000002ots	-----

Change Object Information

Object Name : otp000001ots

MAC Address : : : : : :

5 If desired, you can modify the object names.

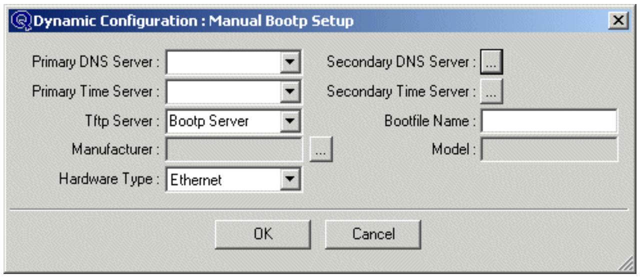
6 For any M-Bootp and M-DHCP objects, you must supply a MAC Address. Refer to the Table 7-5, “Object tab fields” (p. 7-30) for more information on the MAC Address field. If you added any M-Bootp objects, and you entered a Bootfile Name in the Manual Bootp Setup window, that value will be the default for all objects in the list. You can also assign a unique Bootfile Name to a specific object. Select the IP address you wish to edit, and add the new name in **Bootfile Name** field at the bottom of the window.

7 Click **OK**. A confirmation window opens.

8 Click **OK**. The Object Management window reappears, showing the new status of the addresses you dynamically assigned.

Manual Bootp setup

If you selected **Manual Bootp** in the Dynamic Allocation: Add window and clicked **...** next to the **Dynamic Configuration** field, the Dynamic Configuration: Manual Bootp Setup window opens.



Dynamic Configuration : Manual Bootp Setup

Primary DNS Server :

Secondary DNS Server :

Primary Time Server :

Secondary Time Server :

Tftp Server : Bootp Server

Bootfile Name :

Manufacturer :

Model :

Hardware Type : Ethernet

9 Assign Manual Bootp settings to the objects, as described in the following table.

Table 7-17 Manual Bootp setup fields

Field	Description
Primary DNS Server	To select the primary DNS server, select one from the drop-down list.
Secondary DNS Server	If you wish to select a Secondary DNS server, select one from the drop-down list.
Primary Time Server	To select the Primary Time server, select one from the drop-down list.
Secondary Time Server	If you wish to select a Secondary Time server, select one from the drop-down list.
Tftp Server	By default, the TFTP server is the same as the Bootp server. If you wish to select a different TFTP server, select one from the drop-down list.
Bootfile Name	Enter the Bootfile path and file name to indicate the configuration file used to “boot” this device. If you are creating multiple objects, this Bootfile name will be applied to all objects. **Note:** The data required to generate unique bootfile names (for example, Object name) is not available until the Dynamic Allocation confirmation window is displayed. Here you can modify the object name, assign the MAC address and create unique Bootfile Names.

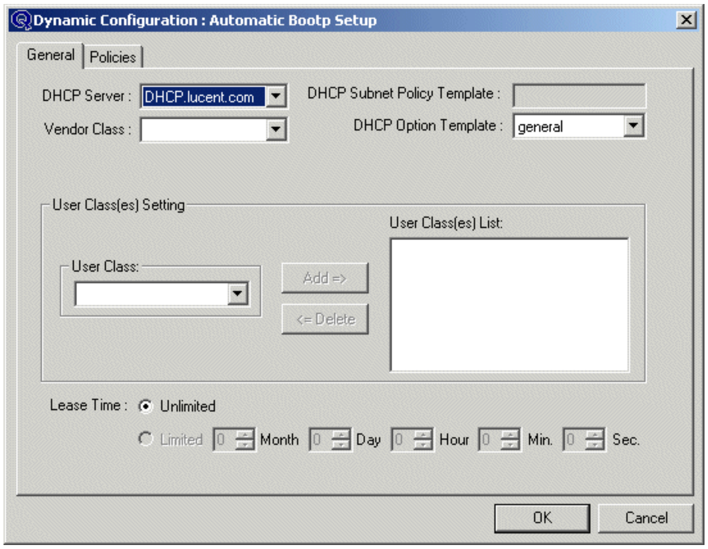
Field	Description
Manufacturer	You can select the manufacturer for this object by clicking **...**. The **Manufacturer List** appears. Select a manufacturer; all models assigned to the manufacturer are displayed in the **Model List**. Select a model from the list and click **OK**. The manufacturer and model display in the Manual Bootp Setup window.
Model	The manufacturer's model for this object.
Hardware Type	Select the hardware type that corresponds to this object: Ethernet, IEEE802, Token Ring, Pronet, Chaos, Arcnet, or AX.25.

10 Click **OK** and you see the Dynamic Allocation: Add window once again.

11 Continue entering information in the window (refer to Table 7-16, "Dynamic Allocation fields" (p. 7-68) as needed).

Automatic Bootp and DHCP configuration

If you selected **Automatic Bootp**, **Automatic DHCP**, **Dynamic DHCP**, or **Manual DHCP**, click **...** next to the **Dynamic Configuration** field. The Dynamic Configuration: Automatic Bootp Setup window opens.



Dynamic Configuration : Automatic Bootp Setup

DHCP Server : DHCP.lucent.com

DHCP Subnet Policy Template :

Vendor Class :

DHCP Option Template : general

Lease Time : ● Unlimited ○ Limited 0 Month 0 Day 0 Hour 0 Min. 0 Sec.

12 Assign DHCP settings to the objects, as described in the following table.

Table 7-18 Automatic Bootp and DHCP setup fields

Field	Description
DHCP Server	To select the DHCP server, click on the down arrow to the right of the field for a list of servers and select a server. Select **Same as in Subnet Profile** if you wish to use the DHCP server defined in the Subnet Profile. The **DHCP Scope Policy Template** field appears as soon as a DHCP server is selected.
Vendor Class	Select a **Vendor Class** from the drop-down list to optionally identify the vendor type and configuration of a DHCP client. The **Vendor Class Identifier** (option 60 of RFC2132) is established in the **DHCP/Bootp Template** options of the **Policies** menu. For example, you may have the **Vendor Class Identifier** configured for the MCFT NT 5.0 (Microsoft NT 5.0 DHCP), and have this template, in turn, attached to a range of addresses. If you assign this object the Vendor class MCFT NT 5.0, when the object tries to get a lease, it will be given an address in the range with the DHCP template attached, which has this **Vendor Class Identifier**. If there is no address available in this subnet, the client is given the first available address outside the subnet. However, if you have the **ForcedVendorClass** policy turned on in the DHCP policy file, the client will be forced to accept only an address from the range that has that template attached, or it will not be given an address. Refer to "DHCP server policies" (p. 2-71) for more information on the **ForceClass** policy.
User Class	***This field is for Lucent DHCP only***. The **User Class** allows you to define specific categories of users options; for example, assigning a **User Class** for mobile computing that would specify a shorter lease time. Select a User Class from the **User Class** drop-down list and click **Add** to add the User Class to the User Classes list. User Classes can also be deleted from the User Classes list.
IBM Class Option Template	***IBM DHCP only***. Class templates apply to a particular vendor class within a subnet. They should be used instead of assigning a template to a set of objects within a subnet. Click the down arrow button to view a list of class templates and select one.
DHCP Subnet Policy Template	This policy is set in the Subnet Profile. This field is filled in automatically and cannot be modified.
DHCP Option Template	If you wish to change the DHCP Option template, select a template from the drop-down list. Select **Same as in Subnet Profile** if you wish to use the template assigned to the DHCP server in the Subnet Profile.

Field	**Description**
DHCP Scope Policy Template	Assign a DHCP Scope Policy Template. View the list of available DHCP Scope Policy Templates by clicking the down arrow next to the field. Refer to "DHCP policy templates" (p. 2-63) for more information on setting up scope policy templates.
Lease Time	***This field is for Dynamic DHCP only, all others are 'Unlimited'***. If you wish the lease time to be limited, click **Limited**, then select a time interval in months, days, hours, minutes, and/or seconds. The default lease time is 3 months. If a lease time is defined in the DHCP Template (Option 51), the lease time defined in the template overwrites the value defined here. **Note:** This field only displays the default lease time and not the actual lease time. The actual lease time can be viewed in the DHCP template or using **Network Services | View Active Leases**.

13 If you wish to set secure Windows dynamic DNS at the object level click the **Policies** tab. (Refer to "Enter Windows DNS secure update policies" (p. 7-65) for more information.)

14 Click **OK** and you see the Dynamic Allocation: Add window once again.

15 Continue entering information in the window (refer to Table 7-16, "Dynamic Allocation fields" (p. 7-68) as needed).

END OF STEPS

Modify a dynamically allocated IP address

Purpose

This function is used to fill in all or part of the Object Profile for a dynamically allocated object. This does not change the state of the object, except that objects that were defined as “Dynamic” (for example, dynamic configuration without using Bootp or DHCP) are changed to “Used”.

Procedure

To modify a dynamically allocated IP address, follow these steps:

1 Highlight the IP addresses/objects in the Object Management window.

2 Select **Edit|Modify|Dynamic** (or right-click and select the **Modify|Dynamic** option). The Object Profile: Modify window opens.

3 If necessary, change the object class (which may cause the object name to change, as well), and fill in the rest of the Object Profile window as desired.

4 Click **OK**. A warning prompt opens.

5 Click **Yes**. A confirmation prompt opens.

6 Click **OK**.

7 If you selected more than one IP address, the Object Profile window opens again, for the next address. Repeat steps 4 to 7 to change the Object Profile for this IP address. If you ***do not*** wish to assign an object to an address, click **Skip**.

8 When you finish modifying or skipping all the IP addresses you selected, a confirmation window opens. Click **OK**.

9 The Object Management window reopens. The addresses you modified now have the state “Used”.

END OF STEPS

Un-allocate a dynamically allocated object

Purpose

Use this procedure to un-allocate a dynamically allocated object and change its state from “Dynamic” back to “Unused”.

Before you begin

- If an object has one or more aliases assigned to it, you must remove the alias(es) before you can un-allocate it. For instructions, refer to “Modify a dynamically allocated IP address” (p. 7-75).
- If you have the administrator privilege “Delete Confirmation Warning” set to True, steps 3 through 8 below apply. If “Delete Confirmation Warning” is set to False, however, you see a confirmation dialog box only (that is, no Object Profile with a **Skip** button). If you click **Yes**, all selected objects are deleted without confirmation.

Procedure

To un-allocate a dynamically allocated object, follow these steps:

1 Highlight the IP addresses/objects in the Object Management window.

2 Select **Edit|Delete|Dynamic** (or right-click and select the **Delete|Dynamic** option). The Object Profile: Delete window opens.

3 View the Object Profile window to verify that you wish to delete this object. If you selected more than one object to delete, the Object Profile window opens again, for the next object. Repeat steps 3 to 4 to delete the Object Profile for this object.

4 Click **OK** to delete this object or if you ***do not*** wish to delete this object, click **Skip**. If you click **OK**, a warning window opens.

5 Click **Yes**. A confirmation prompt opens.

6 Click **OK**.

7 When you finish deleting or skipping all the objects you selected, a confirmation window opens. Click **OK**.

8 The Object Management window reopens. The objects you unallocated now display as “Unused”.

END OF STEPS

Reserve an IP address

Purpose

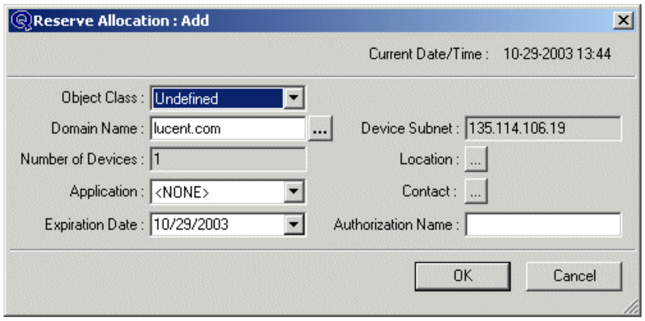
You can reserve IP addresses for use on or before a particular date. This is done through the **Add | Reserved** function in the Object Management List. The status must be “Unused”.

Procedure

To reserve an IP address, follow these steps:

1 Highlight one or more “Unused” addresses in the Object Management window.

2 Select **Edit | Add | Reserved** (or right-click and select the **Add | Reserved** function). The Reserve Allocation: Add window opens.



Current Date/Time : 10-29-2003 13:44

Object Class : Undefined
Domain Name : lucent.com
Number of Devices : 1
Application : <NONE>
Expiration Date : 10/29/2003
Device Subnet : 135.114.106.19
Location : ...
Contact : ...
Authorization Name :

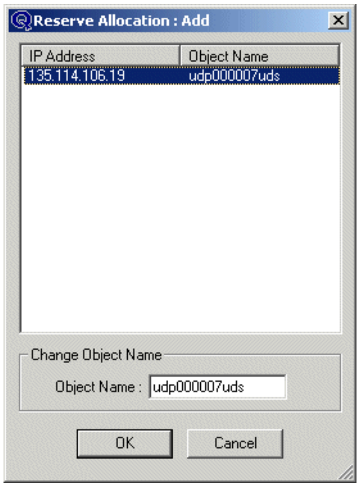
3 Fill in the Reserve Allocation window as desired, referring to the following table for information on the fields.

Table 7-19 Reserve allocation fields

Field	Description
Object Class	If you wish to assign an object class (Workstation, Router, and so on) to the address(es) you are reserving, click the down arrow and select the class.
Domain Name	Either enter a full qualified, known domain name, or click **...** to display the Domain Option: Select window. If the **Display Domain Folders** option in the Administrator Profile is set, this field is a browse-edit function. You can select or type in the domain. If not, domains display in list format. For more information on this option, refer to “Administrators” (p. 6-11) and “Domain folders” (p. 1-40).
Device Subnet	This field reflects the subnet in which the IP address is located.

Field	**Description**
Number of Devices	If you highlighted one or more addresses (as opposed to selecting the **Edit|Add|Reserved** option from the Object Management window without highlighting addresses), this field shows the number of addresses you selected. ***If you did not select IP addresses***, fill in the number of IP addresses you wish to reserve. If you specify the number of devices, VitalQIP picks the "first" available address and allocates the number of objects you specified.
Location	Click this button to display the Location Profile. By default, VitalQIP assigns the location defined in the Subnet Profile. You can select a different location by clicking **...** for a list of locations. Select a location from the list, then click **Apply**. You can also add, modify, or delete a location from this window.
Contact	Click this button to display the Contact Profile. By default, VitalQIP assigns the contact defined in the Subnet Profile. You can select a different contact by clicking **...** for a list of contacts. Select a contact from the list, then click **Apply**. You can also add, modify, or delete a contact from this window.
Application	The name of the application with which you wish to associate the reserved the IP address(es).
Expiration Date	The date on which the address(es) will no longer be reserved. Use the format *mm/dd/yyyy*. **Note:** VitalQIP checks at midnight of each day and releases all reserved addresses specified to be released on this Expiration Date. For example, if the **Expiration Date** is defined as 11/11/2001, at midnight on 11/10/2001, the addresses will be released.
Authorization Name	The person who authorized the reservation of the IP address(es).

4 When you finish filling in the Reserve window, click **OK**. The Reserve Allocation: Add window opens, listing the IP address(es) that will be reserved.



IP Address	Object Name
135.114.106.19	udp000007uds

Change Object Name

Object Name : udp000007uds

5 If desired, you can change an object name by selecting it, then modifying the name.

6 Click **OK**. A confirmation prompt opens.

7 Click **OK**. The Object Management window reopens, showing the status of these addresses as “Reserved”.

END OF STEPS

Modify a reserved IP address

Purpose

This function allows you to fill in the Object Profile for a reserved IP address. The status of the address changes from **Reserved** to **Static**.

Procedure

To modify a reserved IP address, follow these steps:

1 Highlight one or more addresses in the Object Management window.

2 Select **Edit|Modify|Reserved**. The Object Profile: Modify window opens.

3 If necessary, change the object name to one that indicates the object type.

4 Fill in or modify the rest of the Object Profile window, as desired.

5 When you finish modifying the Object Profile window, click **OK**. A confirmation window opens.

6 Click **OK** to confirm that you want to make the change. A window opens, indicating that the Object Profile has been changed. The status of the object is now “Static”.

7 If you selected more than one IP address, the Object Profile opens again with the next object’s information. Repeat steps 4-7. (If you ***do not*** wish to define an object for an address, click **Skip** or **Next**.)

END OF STEPS

Un-reserve one or more IP addresses

Purpose

Un-reserve an IP address when you wish to change its state from “Reserved” back to “Unused”.

Procedure

To un-reserve an IP address, follow these steps:

1 Highlight one or more addresses in the Object Management window.

2 Select **Edit|Delete|Reserved**. The Object Profile: Delete window opens.

> **Note:** The Object Profile may not appear, based on the “Delete Confirmation Warning” setting for that Administrator. This value is determined in the Administrator Profile.

3 View the Object Profile window to verify that you wish to un-reserve this object.

4 Click **OK**. or if you ***do not*** wish to un-reserve this object, click **Skip**. If you selected more than one object to delete, the Object Profile window opens again, for the next object. Repeat steps 4 to 7 to delete the Object Profile for this object. Otherwise, a warning prompt opens.

5 Click **Yes**. A confirmation prompt opens.

6 A window opens, indicating that this IP address has been unreserved. Click **OK**. The Object Management window reopens, showing these addresses as having their original status.

END OF STEPS

Subnet Moves

You can move all objects within a subnet to another subnet, either immediately or at a pre-scheduled date. You can also reschedule a scheduled move or delete a scheduled move.

There are some objects that cannot be moved. If you attempt to move an entire subnet and there are immovable objects within that subnet, they will remain behind. Those objects that are allowed to be moved are transferred to the new subnet address. Additionally, when you "move" an object, certain information in the Object Profile is also moved, while other information is handled differently.

What cannot be moved

Some subnet components cannot be moved:

- A-DHCP, A-BOOTP, D-DHCP objects.
- Domain Name, if the Domain Name is valid in the destination subnet. If not, the default domain name in the destination subnet profile will be used.
- M-BOOTP objects: (Only) Time server, TFTP server, DNS Server and Hardware Type does ***not*** move - The information in the destination Subnet Profile will be used.
- All Contact and Location information.
- Reserved objects.

Ping destination address

The pinging of a destination address during an object or subnet move is also affected.

- During an Object Move with a User-Defined destination address, a manual or static destination address will be pinged if the Subnet of the destination address has the **Check Before Assign** option turned on.
- During an Object Move with an auto-assigned address, no pinging of the destination address occurs.
- During an Object Move with a User-Defined destination address, the destination address will be pinged if the Subnet of the destination address has the **Check Before Assign** option turned on. (Access the Network Profile, and click **Modify** to **Modify the Subnet Properties**.) Whether the move is scheduled or not, the ping occurs immediately.

Move a Subnet

Purpose

Use this procedure to move a subnet.

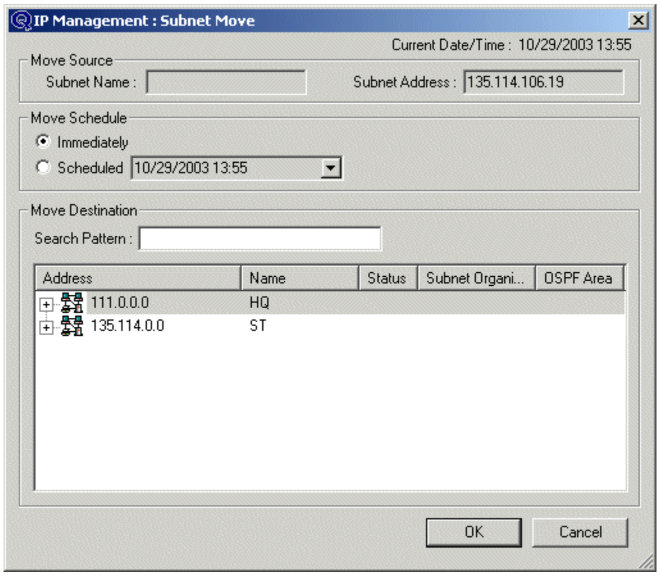
Before you begin

- In a scheduled move, the clients local time is converted to the VitalQIP enterprise server time, and stored in the database. The VitalQIP Schedule Service (**`qipd`**) checks the current enterprise server date/time on a timed interval, and then compares this date/time with the objects that are scheduled to move.
- If the destination Subnet is unable to accommodate the number of addresses being moved into it, the Subnet Move will fail and an error message is displayed.
- Moves cannot be scheduled for more than a year in advance.
- If the VitalQIP enterprise server and the client objects to be moved reside in different time zones, then the scheduled move should be based on the ***Client's local time***, not on the enterprise server's local time.
- When a subnet is scheduled to move and the destination does not have enough free space for the objects to be moved into, VitalQIP moves as many objects from the source to the destination subnet as possible (filling the destination subnet) and leaves the unmovable objects in the source subnet. That is, it performs a partial subnet move.

Procedure

To move a subnet, follow these subnets:

1 Access the **Edit|Subnet Move** option from the Object Management Objects, or from the **Network Quick View** right-click context menu, select **Move**. The IP Management: Subnet Move window displays with the **Subnet Name** and/or the **Subnet Address** provided.



IP Management : Subnet Move

Current Date/Time : 10/29/2003 13:55

Move Source

Subnet Name :

Subnet Address : 135.114.106.19

Move Schedule

● Immediately

○ Scheduled 10/29/2003 13:55

Move Destination

Search Pattern :

Address	Name	Status	Subnet Organi...	OSPF Area
111.0.0.0	HQ			
135.114.0.0	ST			

2 Select whether you want this subnet move to be done **Immediately** or **Scheduled**. If you select **Scheduled**, select a date and time from the drop down calendar.

3 Establish your **Move Destination**. You can search on a specific Subnet by typing in the **Search Pattern** field. The Subnet Address, Subnet Name, Status, Subnet Organization and OSPF Area can be searched. It will search as you type. For example, if you want to move this subnet to the Malvern subnet, type “Malvern” in the **Search Pattern** field and all subnets with the name Malvern display. If you typed only “M”, all subnets that begin with M will display, and so on.

4 Once you have selected the **Subnet Move Destination**, click **OK**. A Subnet Move: Result window opens the objects within the subnet that were moved.

5 You can email, print or save this report to a file. Click **Exit**.

END OF STEPS

Move an object

There are two different ways to perform a move; you can:

- Have VitalQIP provide a list of possible move destinations (**Auto Assign Destination**).
- Specify the move destination yourself (**User Specify Destination**).

Before you begin

- In a scheduled move, the client's local time is converted to the VitalQIP enterprise server time, and stored in the database. The VitalQIP Schedule Service (**`qipd`**) checks the current VitalQIP server date/time on a timed interval, and compares this date/time with the objects that are scheduled to move.
- If the VitalQIP enterprise server and the client objects to be moved reside in different time zones, the scheduled move should be based on the ***Client's local time***, not on the enterprise server's local time.
- The message opens only when adding an object in the VitalQIP client and is not caused by DNSP handing out leases.
- When a group of objects is selected to move from a large subnet to a smaller subnet (in an immediate move), and there is not enough space in the destination for all the objects selected, a report dialog is generated listing all the addresses that were not able to be moved (indicating they were skipped).
- If you schedule a subnet move, and objects are added to the subnet before the move takes place, they will also be moved.
- You cannot move "Unused" objects.
- Ensure the Administrator performing the move has "Write" privileges to both the Object Range ***and the Subnet to which the object is being moved***.
- If moving objects from one subnet to another, objects that have the same MAC address as objects in the subnet will not be moved.
- When an M-DHCP object is moved out of the managed range of its current DHCP server, the default DHCP server in the destination subnet is entered in the **DHCP Server** field of the Object Profile's **Dynamic Configuration** tab.
- You must schedule object moves at least one hour before the move. If a sufficient number of objects are selected and scheduled to be moved within five minutes of the current time, an error message will display that the current time is within 5 minutes of the scheduled move time and processing will stop. The report generated will show the list of objects that were scheduled, and the list of objects that could not be moved. You can then re-select the object (s) to move and select a new move date and time.

- When a user modifies an object, which is scheduled to be moved, VitalQIP will delete the scheduled move from the VitalQIP database. If you want the object to be moved, the object move must be rescheduled.
- Objects cannot be moved in certain situations. They are as follows:
  - Dynamic objects, including those that are only placeholders, that is, with a dynamic allocation setting but a configuration set to None.
  - A-DHCP, A-BOOTP, and D-DHCP objects.
  - Domain Name, if the Domain Name is valid in the destination subnet. If not, the default domain name in the destination subnet profile will be used.
  - M-BOOTP objects: Only Time server, TFTP server, DNS Server and Hardware Type do not move. The information in the destination Subnet Profile will be used.
  - All Contact and Location information.
  - Reserved objects.

Schedule an object move

Purpose

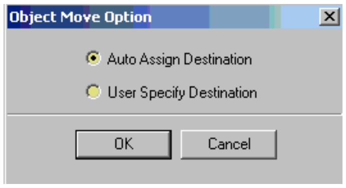
Use this procedure to move objects and have VitalQIP automatically provide a list of possible destinations.

Procedure

To schedule an object move, follow these steps:

1 The Object Management window lists all the IP addresses whose state is Static, Used (GAP), Reserved, Dynamic, M-Bootp, or M-DHCP. Highlight the Static, Used (GAP), Dynamic, M-Bootp, or M-DHCP objects that you want to move. (You cannot move Reserved objects.)

2 Select **Edit|Move|Schedule**, or you can select **Move|Schedule** through the right-click context menu of the **Subnet Quick View** that opens the subnets' objects. The Object Move Option window opens.

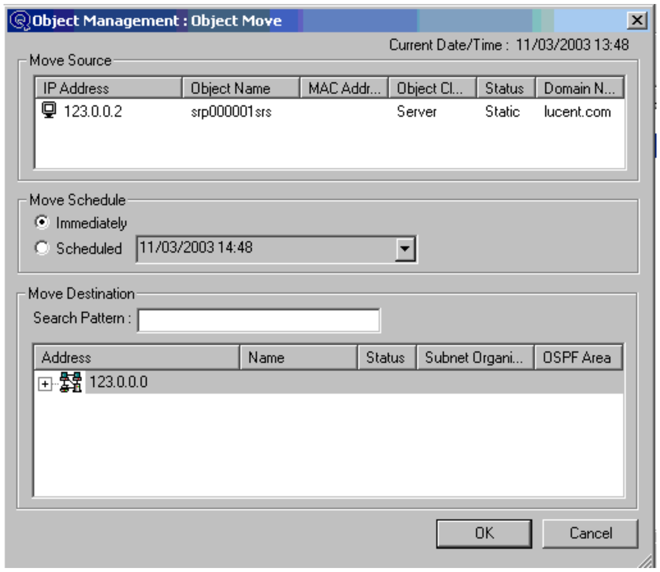


Object Move Option

● Auto Assign Destination

○ User Specify Destination

3 Click **Auto Assign Destination** and click **OK**. The Object Management: Object Move window opens.



Object Management : Object Move

Current Date/Time : 11/03/2003 13:48

Move Source

IP Address	Object Name	MAC Addr...	Object Cl...	Status	Domain N...
123.0.0.2	srp000001srs		Server	Static	lucent.com

Move Schedule

● Immediately

○ Scheduled 11/03/2003 14:48

Move Destination

Search Pattern :

Address	Name	Status	Subnet Organi...	OSPF Area
123.0.0.0				

4 The object(s) you selected - ***that are allowed to be moved*** - appear in the **Move Source** list. The possible destination subnets for the move appear at the bottom of the window.

5 You may wish to change the display of these subnets. To change the sort order to be ascending or descending, click the arrow in the currently sorted (where the sort arrow appears) list heading, or change the sort key by clicking any column heading.

6 Establish your **Move Destination**. You can search on a specific Subnet by typing in the **Search Pattern** field. The Subnet Address, Subnet Name, Status, Subnet Organization and OSPF Area can be searched on. It will search as you type. For example, if you want to move an object in the **Move Source List** to the Malvern subnet, type “Malvern” in the **Search Pattern** field and all subnets with the name Malvern will display. If you typed only “M”, all subnets that begin with M will display, and so on.

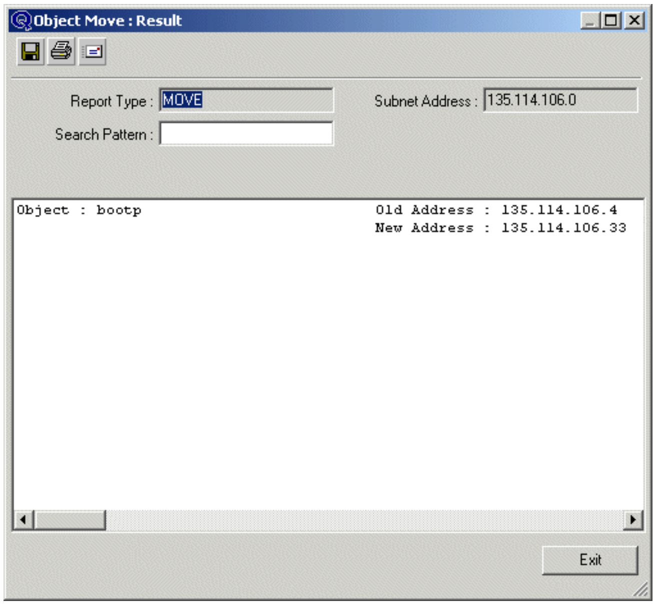
7 Alternatively, to select the Move destination, click on a subnet listed in the lower half of the window, or type the address in the **Move Destination** field.

8 If you wish to schedule the move for a future date, click **Scheduled** and select the date/time for the move from the calendar. This is called a Scheduled Move (SM).

9 If you do not specify a time, the move will take place at 12:00:01 AM on the date specified.

10 Click **OK**. A warning prompt opens.

11 Click **Yes**. The Object Management: Result window opens.



Report Type : MOVE

Subnet Address : 135.114.106.0

Search Pattern :

```
Object : bootp                              Old Address : 135.114.106.4
                                            New Address : 135.114.106.33
```

12 You can save, print, or email the report as desired. Click exit to close the window. The Object Management window reopens. Any addresses you assigned for a scheduled move now have the status “Static(SM) or “Reserved(SM)” or “Dynamic (SM)”.

END OF STEPS

Schedule an object move and specify the move destination

Purpose

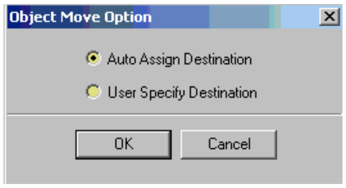
Use this procedure to schedule a move and specify the destination yourself.

Procedure

To schedule an Object Move and specify the move destination, follow these steps:

1 Highlight one or more addresses in the Object Management window.

2 Select **Edit | Move | Schedule**. The Object Move Option window opens.

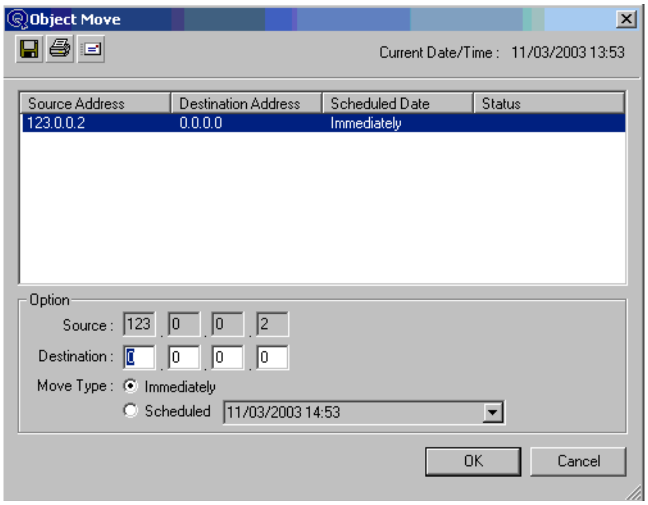


Object Move Option

● Auto Assign Destination

○ User Specify Destination

3 Select **User Specify Destination**, then click **OK**. The Object Move window opens.



Object Move

Current Date/Time : 11/03/2003 13:53

Source Address	Destination Address	Scheduled Date	Status
123.0.0.2	0.0.0.0	Immediately	

Option

Source : 123 . 0 . 0 . 2

Destination : 0 . 0 . 0 . 0

Move Type : ● Immediately

○ Scheduled 11/03/2003 14:53

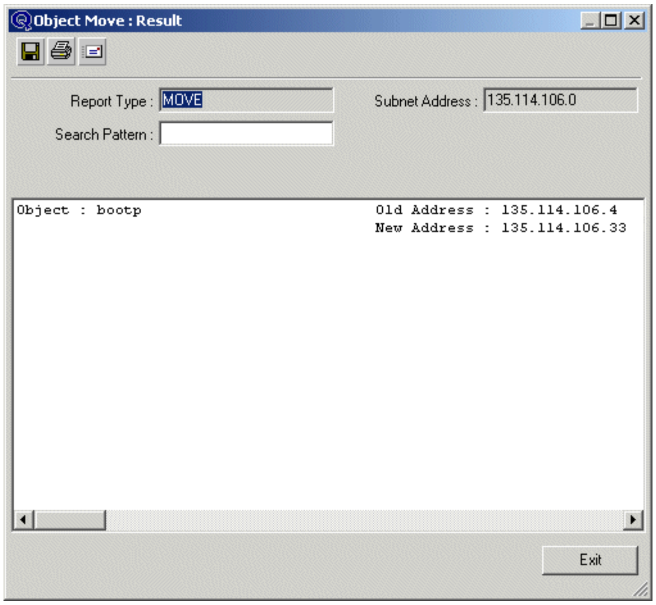
4 The objects you selected - ***that are allowed to be moved*** - to move are listed.

5 Fill in the destination subnet you wish to move the objects.

6 If you wish to schedule the move for a future date, click **Scheduled** and select the date/time for the move. This is called a **Scheduled Move (SM)**.

7 If you do not specify a time, the move will take place at 12:00:01 AM on the date specified.

8 Click **OK**. The Object Move: Results windows opens.



Report Type : MOVE
Subnet Address : 135.114.106.0
Search Pattern :

```
Object : bootp                          Old Address : 135.114.106.4
                                        New Address : 135.114.106.33
```

9 Click **Exit** to close the window. The Object Management window reopens. Any addresses you assigned for a planned move now have the state “Static(SM) or “Reserved(SM)” or “Dynamic (SM)”.

END OF STEPS

Modify a scheduled move

You can modify the date and time and/or the destination of a scheduled move (addresses for which the state is “Static(SM)” or “Reserved(SM)” or “Dynamic(SM)”).

Procedure

To modify a scheduled move, follow these steps:

1 Highlight one or more addresses whose scheduled move(s) you want to change in the Object Management window.

2 Select **Edit|Move|Modify**. The Object Move Option window opens.

3 Click **Auto Assign Destination** to have VitalQIP provide a list of move destinations, or **User Specify Destination** if you already know the destination. Click **OK**.

If you selected **Auto Assign Destination**, the Object Management: Object Move window opens.

If you selected **User Specify Destination**, the Object Move windows opens.

4 If you selected **Auto Assign Destination**:

a. The object - ***that is allowed to be moved*** - appears in the **Move Source** list. The possible destination subnets for the move appear at the bottom of the window.

b. You may wish to change the display of these subnets. To change the sort order to be ascending or descending, click the arrow in the currently sorted (where the sort arrow appears) list heading, or change the sort key by clicking any column heading.

c. Establish your **Move Destination**. You can search on a specific Subnet by typing in the **Search Pattern** field. The Subnet Address, Subnet Name, Status, Subnet Organization and OSPF Area can be searched on. It will search as you type. For example, if you want to move an object in the **Move Source List** to the Malvern subnet, type “Malvern” in the **Search Pattern** field and all subnets with the name Malvern will display. If you typed only “M”, all subnets that begin with M will display, and so on.

d. Alternatively, to select the Move destination, click on a subnet listed in the lower half of the window, or type the address in the **Move Destination** field.

e. If you wish to schedule the move for a future date, click **Scheduled** and select the date/time for the move from the calendar. This is called a Scheduled Move (SM). If you do not specify a time, the move will take place at 12:00:01 AM on the date specified.

f. Click **OK**. A warning prompt opens.

g. Click **Yes**. The Object Management: Result window opens.

h. You can save, print, or email the report as desired. Click **Exit** to close the window. The Object Management window reopens. Any addresses you assigned for a scheduled move now have the status “Static(SM) or “Reserved(SM)” or “Dynamic (SM)”.The Objects you selected to move - ***that are allowed to be moved*** - display in the **Move Source List**.

5 If you selected **User Specify Location**:

a. The objects you selected - *that are allowed to be moved* - to move are listed.

b. Fill in the destination subnet you wish to move the objects.

c. If you wish to schedule the move for a future date, click **Scheduled** and select the date/time for the move. This is called a **Scheduled Move (SM)**. If you do not specify a time, the move will take place at 12:00:01 AM on the date specified.

d. Click **OK**. The Object Move: Results windows opens.

e. Click **Exit** to close the window. The Object Management window reopens. Any addresses you assigned for a planned move now have the state “Static(SM) or “Reserved(SM)” or “Dynamic (SM)”.

END OF STEPS

Cancel a scheduled move

Purpose

Use this procedure to cancel a scheduled object move. The object's status changes from "Static(SM)", "Reserved(SM)", or "Dynamic(SM)" to "Unused".

Note: "SM" denotes "Scheduled Move".

Procedure

To cancel a scheduled move, follow these steps:

1. Highlight one or more addresses in the Object Management window.
2. Right-click, and select **Edit|Move|Schedule**. A warning prompt opens.
3. Click **Yes**. A confirmation prompt opens.
4. Click **OK**. The Object Management window reopens. The objects whose scheduled moves you deleted now have the status "Unused".

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 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 3-5, "General policies" (p. 3-29).

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 actually 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 reclaimed only if the Status is "Static" or "Reserved" or "Dynamic" and if it has a Network Status of "In DNS; Unreachable" or "Not in DNS; Unreachable". The ping must indicate that the address is not specified as "not allowed to reclaim".

If the object does not respond to the ping, the Database Status of the address is marked as "Unused". To re-use the address, access the address through Object Management.

Schedule a reclaim

Purpose

Use this procedure to schedule a reclaim of IP addresses.

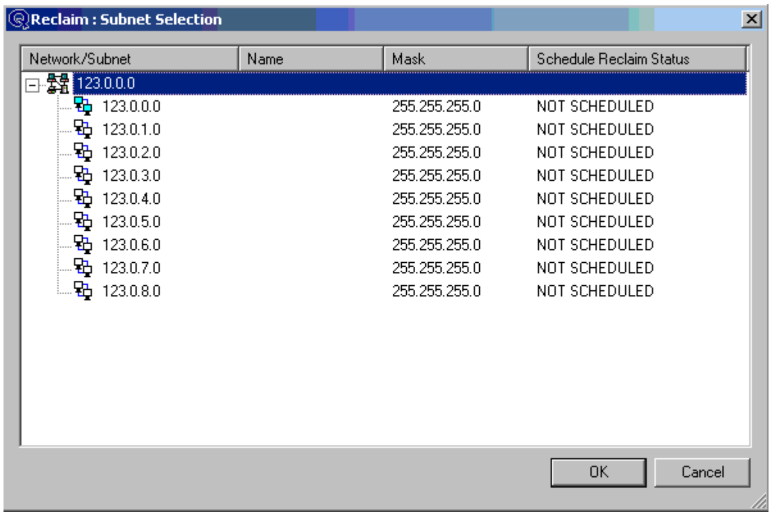
Before you begin

- 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 select the reclaim type ‘Reclaim Only’, a warning dialog box opens indicating that no reclaim audit history will be retained. If you are sure that is what you want, click **Yes**. Otherwise, click **No** and choose a different **Reclaim Type** parameter.
- 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 Select **Reclaim Addresses** from the **Management** menu. The Reclaim: Subnet Selection window opens.

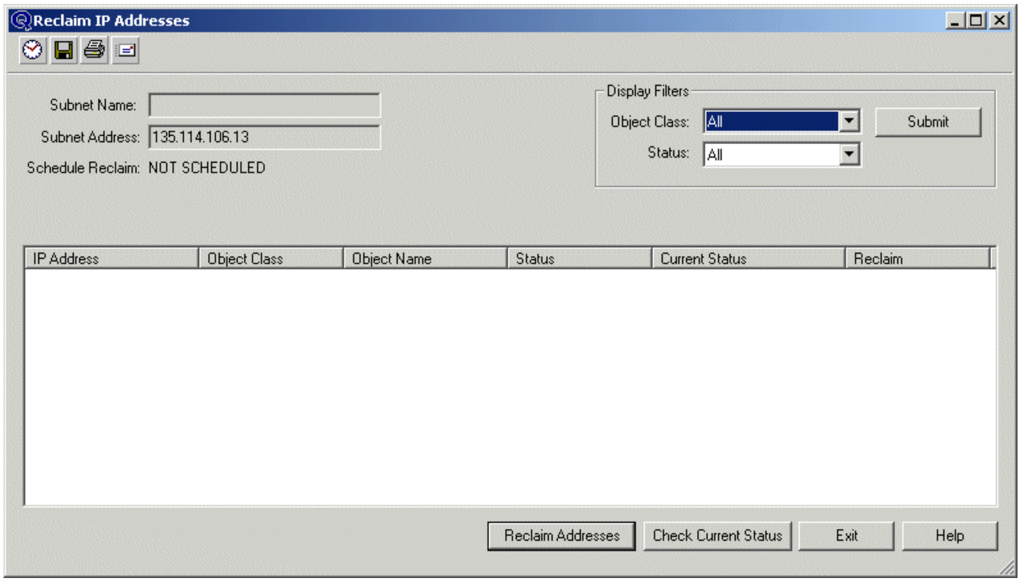


Network/Subnet	Name	Mask	Schedule Reclaim Status
123.0.0.0			
123.0.0.0		255.255.255.0	NOT SCHEDULED
123.0.1.0		255.255.255.0	NOT SCHEDULED
123.0.2.0		255.255.255.0	NOT SCHEDULED
123.0.3.0		255.255.255.0	NOT SCHEDULED
123.0.4.0		255.255.255.0	NOT SCHEDULED
123.0.5.0		255.255.255.0	NOT SCHEDULED
123.0.6.0		255.255.255.0	NOT SCHEDULED
123.0.7.0		255.255.255.0	NOT SCHEDULED
123.0.8.0		255.255.255.0	NOT SCHEDULED

2 Expand the network and review the **Schedule Reclaim Status** column. It can display the following values:

- **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.

3 Highlight a subnet you wish to schedule for a reclaim and click **OK** (or double-click on a subnet). The Reclaim IP Addresses window opens.



Subnet Name:
Subnet Address: 135.114.106.13
Schedule Reclaim: NOT SCHEDULED

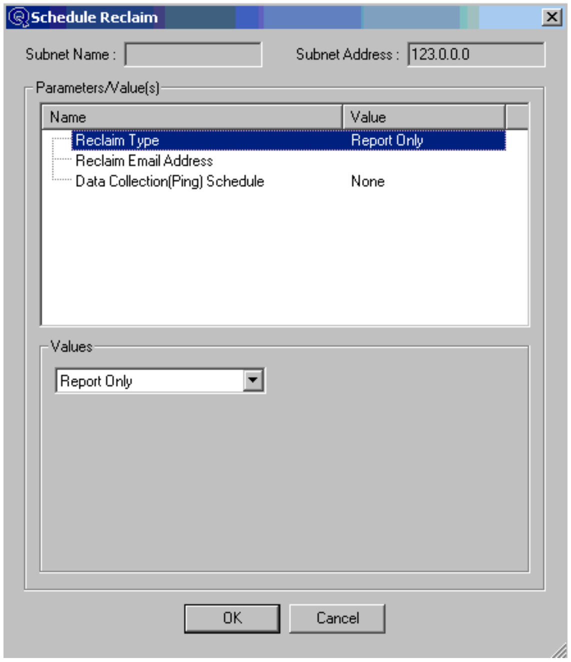
Object Class: All
Status: All

IP Address	Object Class	Object Name	Status	Current Status	Reclaim

4 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 **Status** drop-down list. Possible values are All, Reclaimable, Static, Reserved, Dynamic (None), Unused, and Others.

5 Click **Submit** and IP addresses appear in the reclaim list. Those addresses that appear with a large green check mark can be reclaimed.

6 To schedule a reclaim, click the Clock icon. The Schedule Reclaim window opens.



Subnet Name :

Subnet Address : 123.0.0.0

Name	Value
Reclaim Type	Report Only
Reclaim Email Address	
Data Collection(Ping) Schedule	None

Values: Report Only

7 Select parameters for scheduling the reclaim, as described in the following table.

Table 7-20 Schedule reclaim parameters

Parameter	Default value	Usage
Reclaim Type	Report Only	If the **Allow Automatic Reclaim** global policy is set to True, you can select "Report Only", "Reclaim Only", and "Report and Reclaim". Refer to Table 3-5, "General policies" (p. 3-29) for further information on the **Allow Automatic Reclaim** global policy. If the policy is set to False, "Report Only" is the only available **Reclaim Type**. Reports are generated at the time(s) or interval(s) specified by the **Data Collection (Ping) Schedule** parameter and stored in the *%QIPHOME\Report* directory where they are stored with a date and time stamp in the filename to aid identification. If you select "Report and Reclaim" or "Reclaim Only", you are effectively choosing Automatic Reclaim, and addresses are reclaimed once the schedule is completed. You can, of course, check the status of such reclaims while they are in progress and abort the reclaim if you discover that addresses you have designated to be reclaimed are in fact in use legally.
Reclaim E-mail Address		***Required***. 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 for pinging the objects whose addresses have been selected for reclaiming. 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.

8 Click **OK** when you have finished setting up the schedule parameters. A confirmation prompt opens.

9 Click **OK**.

10 Click **Exit** to close the Reclaim IP Addresses window.

END OF STEPS

Check status of a scheduled reclaim

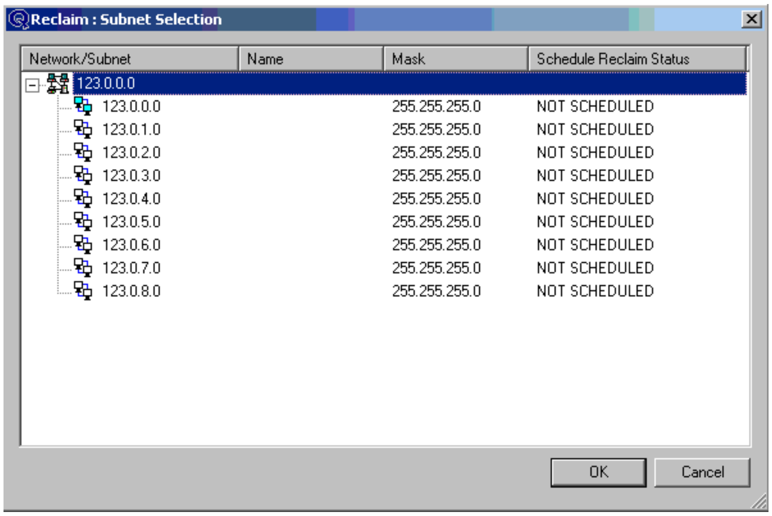
Purpose

Once a scheduled reclaim has started, you may want to check its progress.

Procedure

To check on a reclaim, follow these steps:

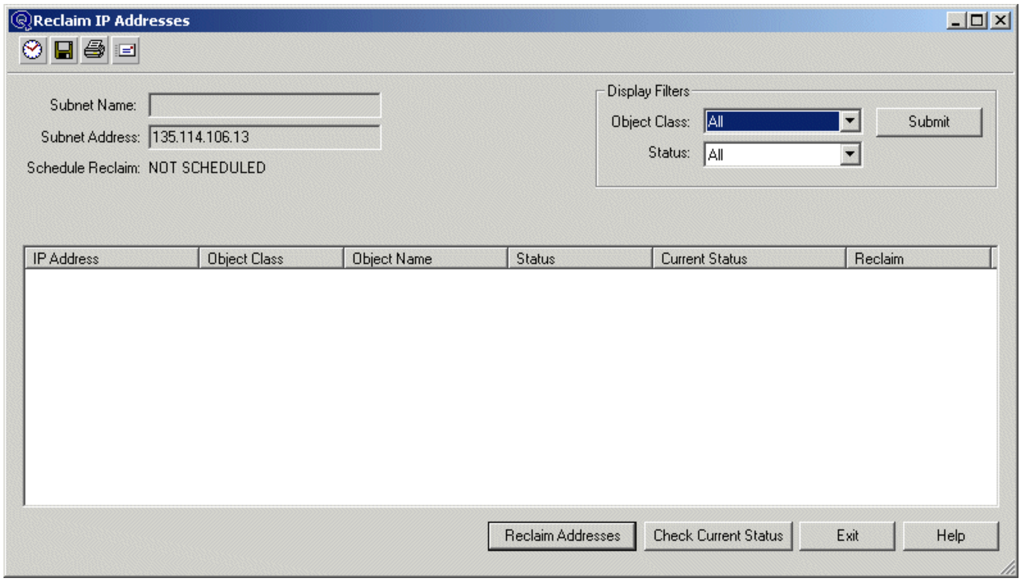
1 Select **Reclaim Addresses** from the **Management** menu. The Reclaim: Subnet Selection window opens.



Network/Subnet	Name	Mask	Schedule Reclaim Status
123.0.0.0			
123.0.0.0		255.255.255.0	NOT SCHEDULED
123.0.1.0		255.255.255.0	NOT SCHEDULED
123.0.2.0		255.255.255.0	NOT SCHEDULED
123.0.3.0		255.255.255.0	NOT SCHEDULED
123.0.4.0		255.255.255.0	NOT SCHEDULED
123.0.5.0		255.255.255.0	NOT SCHEDULED
123.0.6.0		255.255.255.0	NOT SCHEDULED
123.0.7.0		255.255.255.0	NOT SCHEDULED
123.0.8.0		255.255.255.0	NOT SCHEDULED

2 Expand the network and review the **Schedule Reclaim Status** column.

3 Highlight the subnet you want to check (it displays IN PROGRESS in the **Schedule Reclaim Status** column) and click **OK**. The Reclaim IP Addresses window opens.



Subnet Address: 135.114.106.13

Schedule Reclaim: NOT SCHEDULED

Object Class: All

Status: All

4 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 **Status** drop-down list. Possible values are All, Reclaimable, Static, Reserved, Dynamic (None), Unused, and Others.

5 Click **Submit** and IP addresses appear in the reclaim list.

6 The values in the columns are explained in the following table.

Table 7-21 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.

Column	Description
# 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
Reclaim	Shows whether the address is reclaimable. The available values are: **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.

7 If you wish to check the status manually at this time, select one or more objects and click **Check Current Status**. The `Do you want the results to be collected and reflected in the database?` prompt opens.

8 Click **Yes** and the results are displayed in the window as well as being stored with the scheduled objects in the database. If you click **No**, the result is not stored with the scheduled objects. The **#Try**, **#In DNS**, **#Reachable** and **Last Reachable** columns are updated, if applicable.

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 address(es) you want to reclaim (the **Reclaim** column should read "Allowed") and click **Reclaim Address**.

> **Result:** The `Selected addresses will be reclaimed as unused addresses. Are you sure?` prompt opens.

10 Click **Yes** to continue and the addresses are reclaimed. Additionally, 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.

11 Click **Exit** to close the Reclaim IP Addresses window.

END OF STEPS

Reclaim addresses manually

Purpose

If you do not have the **Allow Automatic Reclaim** global policy set to True, you will need to complete a reclaim manually after a scheduled reclaim has completed.

Procedure

To complete the Reclaim process, follow these steps:

1 Select **Reclaim Addresses** from the **Management** menu. The Reclaim: Subnet Selection window opens.

2 Expand the network and review the **Schedule Reclaim Status** column.

3 Highlight the subnet you want to check (it displays COMPLETED in the **Schedule Reclaim Status** column) and click **OK**. The Reclaim IP Addresses window opens.

4 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 **Status** drop-down list. Possible values are All, Reclaimable, Static, Reserved, Dynamic (None), Unused, and Others.

5 Click **Submit** and IP addresses appear in the reclaim list.

6 Select the addresses you wish to reclaim appear in the reclaim list.

7 Click **Reclaim Addresses**. The warning prompt opens.

8 Click **Yes** and the reclaim continues through each address selected. When completed, the **Reclaim** column reads “Done”.

9 Click **Exit** to exit the Reclaim IP Addresses window.

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 17:30Start 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 17:30Start 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 17:30Start Date:  02/18/2002 23:19
Collection Frequency: Collect: Every Day At (17:30 ) Total: 2 Days
SUBNET: 188.184.0.32
```

8 Network services

Overview

Purpose

The purpose is to describe the VitalQIP network services functions, which are used to configure, view, and update the policy, data, and configuration files for services like DNS and DHCP.

Contents

The following topics are covered:

Network services overview	8-3
Search for text in configuration file	8-4
Copy configuration file	8-5
Print configuration file	8-6
Email configuration file	8-7
DHCP generation	8-9
Control debug levels for Lucent DHCP servers	8-10
Generate DHCP configuration files	8-11
DNS generation	8-15
Generate DNS configuration and data files	8-19
Bootptab file generation	8-24
Generate the Bootptab file	8-25
Local host generation	8-28
Generate local host records	8-29
NIS generation	8-32

Generate NIS Files	8-33
Windows Domain Controller generation	8-36
Generate Windows Domain Controller files	8-37
View active leases	8-40
Generate active leases	8-41
Modify active lease reports	8-43
Delete an active lease	8-44

Network services overview

The **Network Services** function allows you to configure, view, and update the policy, data and configuration files of Network Services, such as DNS and DHCP. Data and configuration files define the behavior of DNS and DHCP servers through the transmission, or "push" of data to the servers when a Network Services function is performed. The information that is transmitted is determined by both the setup of the Infrastructure and the subnet information. All Infrastructure must be set up prior to using the Network Services (NS) functions. Minimally, you should have defined the Domain and Network, defined and configured the Bootp, DHCP, and DNS servers, and modified the 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 DNS and DHCP with VitalQIP. The VitalQIP Network Services 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
- NIS services
- Windows Domain Controller
- Local host services
- Viewing Active leases for a DHCP server or a specific subnet of a DHCP server

All Network Services functions can be searched, copied, printed, or emailed once they have been generated to your computer screen. The one exception is the View Active Leases option since that option is for viewing only.

Search for text in configuration file

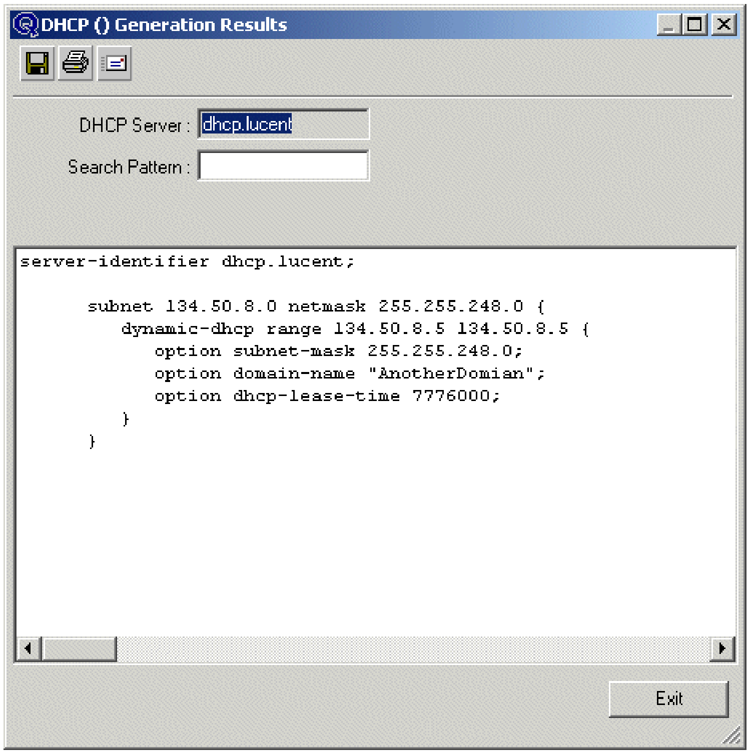
Purpose

After you generate files, a Results windows opens. You can search for a text string in the configuration file.

Procedure

To search for text in a configuration file, follow these steps:

1 After the configuration file window opens (an example follows), type the string in the **Search Pattern** field.



DHCP Server : dhcp.lucent

Search Pattern :

```
server-identifier dhcp.lucent;

     subnet 134.50.8.0 netmask 255.255.248.0 {
        dynamic-dhcp range 134.50.8.5 134.50.8.5 {
           option subnet-mask 255.255.248.0;
           option domain-name "AnotherDomian";
           option dhcp-lease-time 7776000;
        }
     }
```

2 Press **Enter**.

3 To find the same string again, press **Enter** again.

END OF STEPS

Copy configuration file

Purpose

Use this procedure to save a configuration file.

Procedure

To save a configuration file, follow these steps:

1 In the configuration file window, click the **Disk** icon at the top left of the window. The Save to File window opens.

2 If you wish to output the file in Comma Separated Values (CSV) format, click **CSV Format**. In CSV format, each output line value is separated by a comma, except for the last value, which is terminated by a new line. Here is a sample of CSV output:

```
Domain=qtek.com
Network=198.200.153.0
object name=a1, subnetmask=255.255.255.0, defaultroute=198.200.153.1
object name=a2, subnetmask=255.255.255.0, defaultroute=198.200.153.1
```

3 Enter a file name and click **OK**.

END OF STEPS

Print configuration file

Purpose

Use this procedure to print a configuration file.

Procedure

To print a configuration file, follow these steps:

1 In the configuration file window, click the **Printer** icon.

2 Enter a printer name.

3 Click **OK**.

END OF STEPS

Email configuration file

Purpose

Use this procedure to email a configuration file.

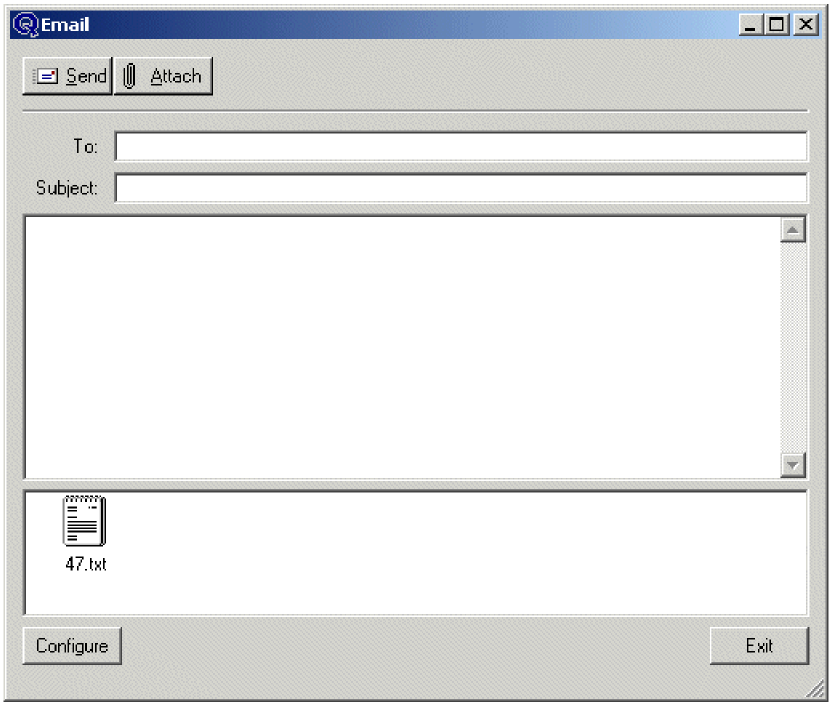
Before you begin

This program does not keep track of sent mail.

Procedure

To use email, follow these steps:

1 Click the **Email** icon in the configuration window. VitalQIP searches for mail information in the registry. If it is found, the Email dialog is displayed and you can send an email.



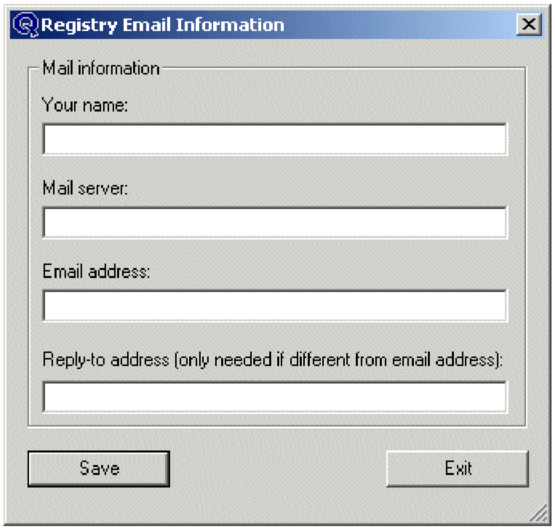
2 To email information to a user, enter at least one email address in the **To:** field. To email information or send messages to multiple recipient's, separate addresses with a comma or semicolon.

3 To add an attachment, click **Attach**. You can send multiple attachments. To delete attachments, click on the attachment(s) and press **Delete**.

4 Click **Send** when you have completed the email.

If mail information is not found, the Registry Email Information window is displayed automatically

Note: You can also change mail information at any time. Click **Configure** in the Email window and the Registry Email Information window is displayed.



Registry Email Information
Mail information
Your name:
Mail server:
Email address:
Reply-to address (only needed if different from email address):
Save
Exit

5 Enter a user name, mail server, email address, and reply-to address. The reply-to address is only needed if it is different from the email address.

6 Click **Save** to save the data to the registry.

7 To exit the configuration file window, click **Exit**.

End of Steps

DHCP generation

Network Services|DHCP Generation option generates 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 **Network Services|DHCP Generation Server** is performed, the DHCP configuration files are generated, based on your Server Type described in the following table.

Table 8-1 Generated DHCP configuration files

Server Type	Files
Lucent DHCP	*dhcpd.conf*, *dhcpd.pcy*, *x.ddns.conf* (Refer to the note below), and *dhcp.db*
IBM for AIX	*dhcpsd.cnf*
Bootp	*bootptab*
Microsoft 2003	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.

A few things to keep in mind

- "Additional Policies" established in the Server Profile for the DHCP servers do not appear when you select **Network Services|DHCP Generation** and request **Screen** as the Destination option.
- M-BOOTP objects are pushed to the DHCP servers, based on the value of the "Managed Range" parameter in the **Infrastructure|Server** function. If you select "Network" as your Managed Range, when a DHCP push occurs, M-BOOTP objects that are available on that network are pushed to the selected server.
- 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), or DNS 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, 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 re initialize 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

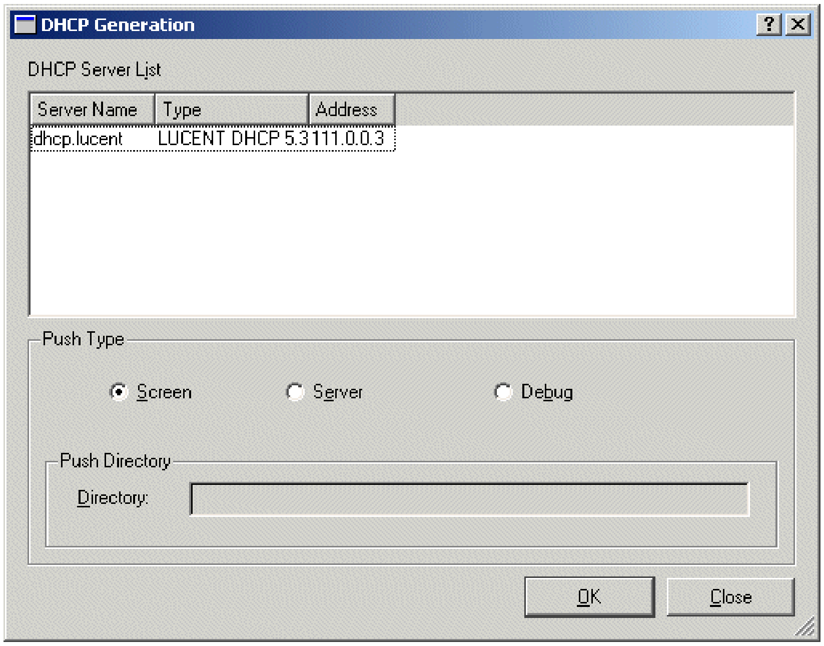
Purpose

Use this procedure to generate DHCP configuration files.

Procedure

To generate DHCP configuration files, follow these steps:

1 Select **DHCP Generation** from the **Network Services** menu. The DHCP Generation window opens.



Server Name	Type	Address
dhcp.lucent	LUCENT DHCP 5.3	111.0.0.3

● Screen ○ Server ○ Debug

Directory:

2 Choose a Destination option. To view the DHCP files on your computer screen, select **Screen**. To send them to a DHCP server, select **Server**. If you select **Server**, the **Directory** field becomes active and you can change the directory (originally specified in the Server Profile).

For Lucent DHCP 5.4 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**. A Debug section is activated. You can select one of the following:

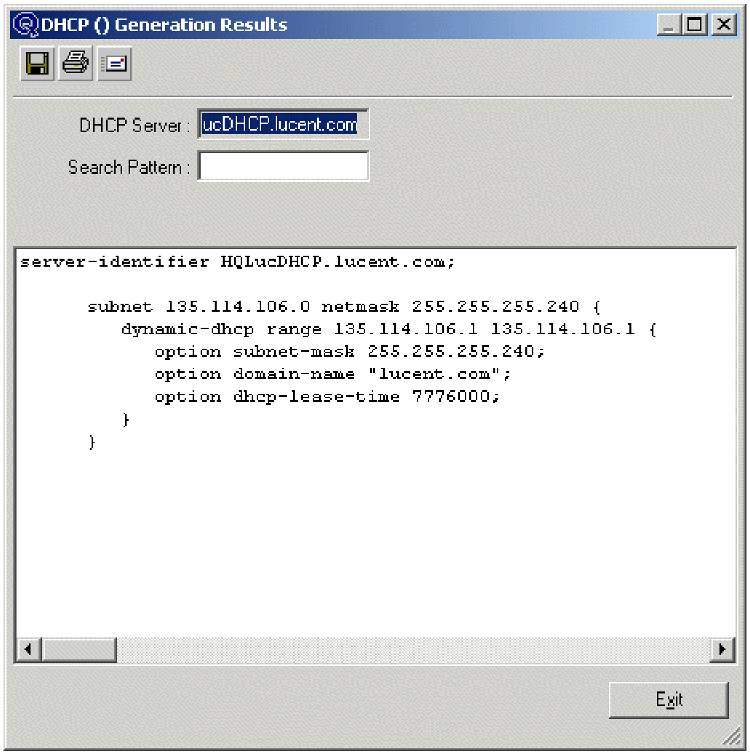
- **Change Debug Level** - changes the debug level. Select from one of the following values:

- – **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.

- **Clear Debug Log** - clears the debug log.
- **Stop Debug Log** - stops debugging.

3 Select a DHCP server from the **DHCP Server List** and click **OK**.

4 If you selected **Screen**, the DHCP files for this DHCP server appear in the DHCP Generation Results window. If desired, you can search, copy, print, or email them. Click **Exit** to close the window.



DHCP Server : ucDHCP.lucent.com

Search Pattern :

```
server-identifier HQLucDHCP.lucent.com;

      subnet 135.114.106.0 netmask 255.255.255.240 {
         dynamic-dhcp range 135.114.106.1 135.114.106.1 {
            option subnet-mask 255.255.255.240;
            option domain-name "lucent.com";
            option dhcp-lease-time 7776000;
         }
      }
```

5 If you selected **Server**, the DHCP files are exported to the specified directory on the server.

6 Click **Close** to exit the window.

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 with the **Network Services|DHCP Generation** function. 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.

Note: 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`**.

DNS generation

Each DNS Server contains Resource Records (RRs), which provide the data that make the DNS system work. The **Network Services|DNS Generation** function creates those records and other records required by DNS.

For BIND 8.X and 9.X, DNS generation can determine the maximum serial number for the zones being generated across all primary DNS servers for the zones defined in VitalQIP. This functionality is dependent upon **DNS Serial Number Query Type on Generation server** parameter.

The process can determine 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. On Lucent DNS 4.X servers, the **Selected Zones Only** option allows you to select specific zones in the DNS Server List.

A few things to keep in mind

- When you perform a **Network Services|DNS Generation** with the Type "Configuration & Data" and Destination "Local", the files described in the following table are created on the GUI client.
- When two pushes to the same DNS server occur simultaneously, one of those pushes is locked out in order to prevent the configuration files from being corrupted. An error message is displayed to this effect.

The **Configuration & Data** files are created and updated. The following table describes the files included for the DNS server(s):

Table 8-2 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 the Infrastructure|Server option is added to the beginning of this file.
boot (Microsoft only)	In Windows, 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 RRs for the domain. The domain extension goes to the bottom of this file.
db.reverse zone	Generates all RRs for the reverse zone.

VitalQIP support of BIND

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 resource record information established in the Domain Profile.

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.

Directory options

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. For more information on BIND parameter settings, refer to Table 4-9, “DNS BIND-9 parameters” (p. 4-45).

Corporate extensions

For Windows 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;
};
  .
  .
  .
```

VitalQIP support of IPv6 reverse zones

VitalQIP recognizes IPv6 reverse zones and generates PTR records for them based on the IPv6 address management data entered through the VitalQIP web client. The push recognizes any zone that ends in “ip6.arpa” as a IPv6 reverse zone. It then does the following:

- The zone section of the *named.conf* file is created identically to existing managed zones
- The *db* file for the zone is created with SOA and NS records generated identically to existing zones

The PTR information in the *db* file for the zone is generated by querying for any IPv6 addresses that fall into that zone (and not into delegated sub zones) and then retrieving the names for those addresses and creating the associated PTR as long as the `Publish PTR` field is checked for that entry.

Generate DNS configuration and data files

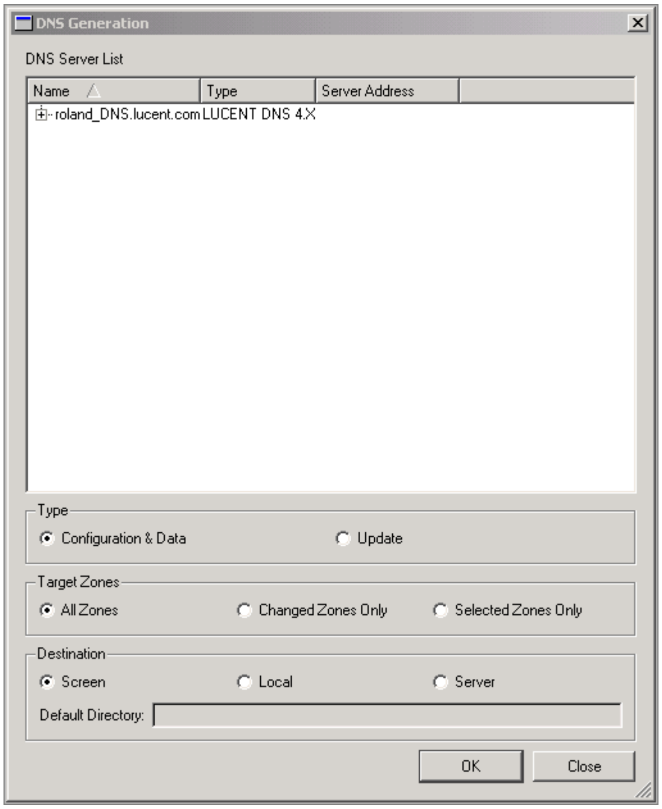
Purpose

Use this procedure to generate and view or push DNS Configuration and Data files on a local server, or on a Remote DNS Server.

Procedure

To generate and push DNS Configuration and Data files on a local server, or on a Remote DNS Server, follow these steps:

1 Select **DNS Generation** from the **Network Services** menu. The DNS Generation window opens.



DNS Generation

DNS Server List

Name	Type	Server Address
⊞ roland_DNS.lucent.com	LUCENT DNS 4.X	

Type: ● Configuration & Data ○ Update

Target Zones: ● All Zones ○ Changed Zones Only ○ Selected Zones Only

Destination: ● Screen ○ Local ○ Server

Default Directory:

2 Select the server you wish to update. Expand the server list as needed.

3 Select one of the following:

- **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 DNS server, the above options are not displayed. Instead, you can select one of the following:

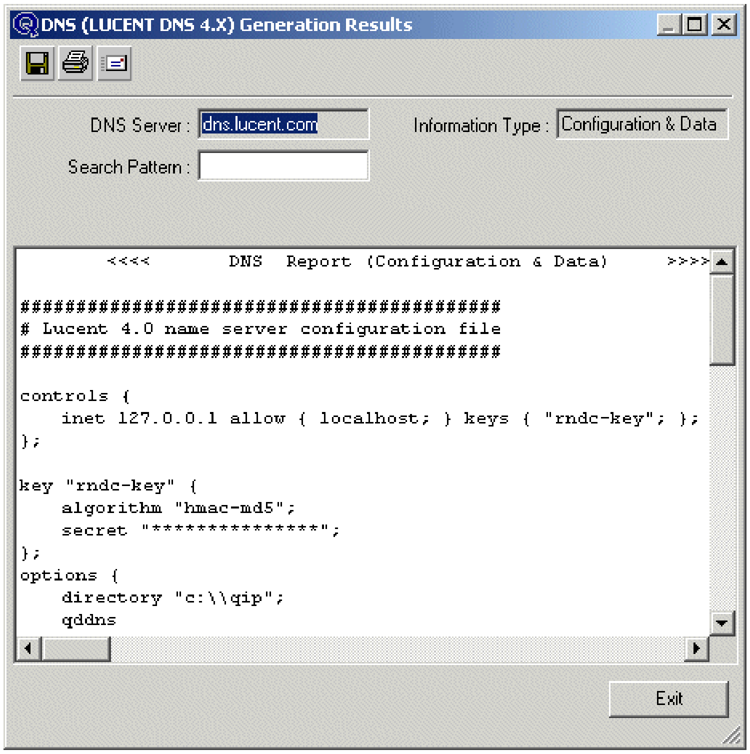
- **All Records** - generates the Windows DNS configuration and data files, including incrementing the SOA serial number and reloading the server.
- **Changed Records Only** - generates files for only changed records. You must perform at least one full push (All records/All zones) before you can perform 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.

4 In the **Target Zone** box, select one of the following:

- **All Zones** - updates all zones.
- **Changed Zones Only** - updates only those zones that have changed since the last push.
- ***Lucent DNS 4.X servers only***. **Selected Zones Only** - updates only the zones you have selected in the DNS Server List.

5 Select one of the following destinations:

– **Screen** - the DNS configuration files for the selected DNS server appear in the DNS Generation Results window. If desired, you can search, copy, print, or email the file. Click **Exit** to close the window.



DNS Server : dns.lucent.com
Information Type : Configuration & Data
Search Pattern :

```
       <<<<        DNS  Report (Configuration & Data)      >>>>

###########################################
# Lucent 4.0 name server configuration file
###########################################

controls {
    inet 127.0.0.1 allow { localhost; } keys { "rndc-key"; };
};

key "rndc-key" {
    algorithm "hmac-md5";
    secret "****************";
};
options {
    directory "c:\\qip";
    qddns
```

– **Server** - the generated files are sent to a DNS server (local or remote).

– **Local** - files are created on your administrative client system.

6 Click **OK**. The files are displayed on your screen or generated to the directory specified.

7 Click **Close** to exit this window.

END OF STEPS

DNS 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 user exits that allow you to manipulate the DNS configuration file after the file has been created with the **Network Services|DNS Generation** function. The DNS user exits can be executed during a **Network Services|DNS Generation** update to the server or on a configuration and data push. The user exits are defined in the following table.

Table 8-3 DNS user exits

Push type	User exit name	Usage
Update	qipdnsuserexit	Run on client during a local push or on remote during a server push ***after*** files are generated but before DNS is restarted.
	qippredns userexit	Run on client during a local push or on remote during a server push ***before*** files are generated. It can be used to call the **`qip-syncexternal`** CLI to get external DNS updates before the push.
	qipdnsuserexitfgs	Run on File Generation Service during a server push ***after*** files are generated and before they are sent to the remote server.
	qippredns userexitfgs	Run on File Generation Service during a server push ***before*** files are generated. It can be used to call the **`qip-syncexternal`** CLI to get external DNS updates before the push.
Configuration & Data	qipdnscnfuserexit	Run on client during a local push or on remote during a server push ***after*** files are generated but before DNS is restarted.
	qippre dnscnfuserexit	Run on client during a local push or on remote during a server push ***before*** files are generated. It can be used to call the **`qip-syncexternal`** CLI to get external DNS updates before the push.
	qipdnscnfuserexitfgs	Run on File Generation Service during a server push ***after*** files are generated and before they are sent to the remote server.
	qippre dnscnfuserexitfgs	Run on File Generation Service during a server push ***before*** files are generated. It can be used to call the **`qip-syncexternal`** CLI to get external DNS updates before the push.

The DNS user exits are located in the *%QIPHOME%\userexits* directory. The user exits can be run on the client during a local push, on the remote during a server push, or on the File Generation Service. The user exit is run if it exists and has the five parameters listed below. The user exit can be any executable routine.

Note: Use full path names within user exit routines. Otherwise, output files are directed to *%QIPHOME%*.

Synopsis

```
Update type: %QIPHOME%\userexits\qipdnsuserexit or qipprednsuserexit
   (.bat,.exe,.cmd, pl) [server_name] [server_IP] [current_push_directory]
   [remote_push_directory] [SERVER or LOCAL]
Configuration & Data type: %QIPHOME%\userexits\qipdnscnfuserexit or
   qipprednscnfuserexit (.bat,.exe,.cmd) [server_name] [server_IP]
   [current_push_directory] [remote_push_directory] [SERVER or LOCAL]
```

Parameters

The following parameters are passed to the user exits:

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.

Bootptab file generation

Network Services|Bootptab File Generation|Server generates the Bootptab file. This file maintains the clients' MAC addresses and Bootp Object Records containing the IP address, subnet mask, default router, and DNS server for servers that are tagged as Bootp servers.

Generate the Bootptab file

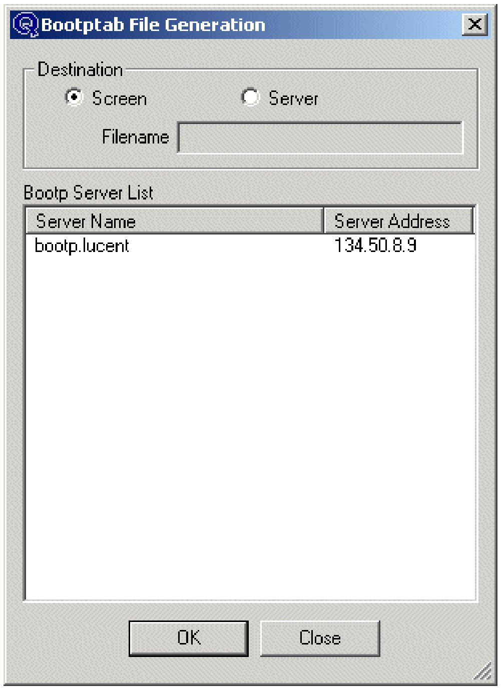
Purpose

Use this procedure to generate a Bootptab file.

Procedure

To generate the Bootptab file, follow these steps:

1 Select **Bootptab File Generation** from the **Network Services** menu. The Bootp File Generation window opens.



Bootptab File Generation

Destination

● Screen ○ Server

Filename

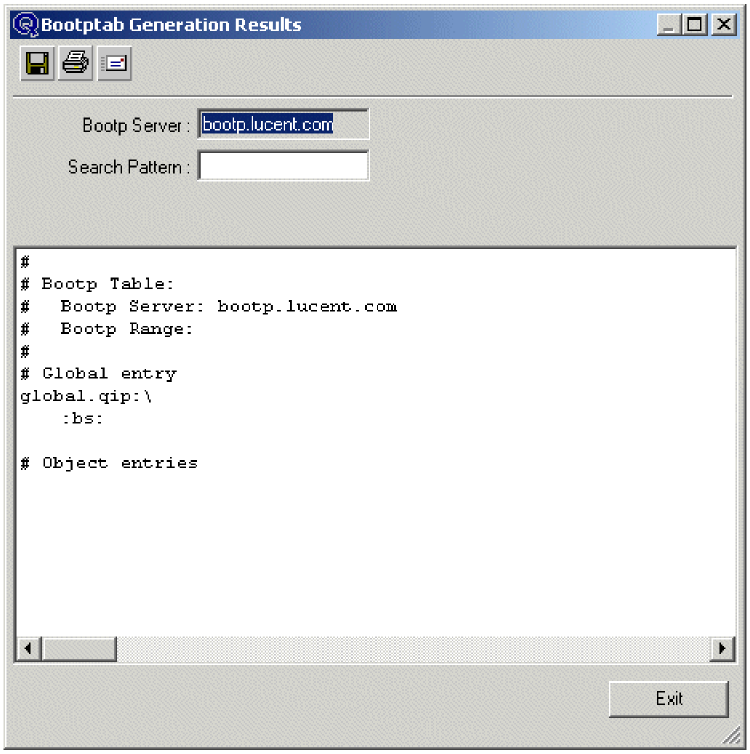
Bootp Server List

Server Name	Server Address
bootp.lucent	134.50.8.9

2 Choose a Destination option. Select **Screen** to display the Bootptab file on your computer screen, or **Server** to send the Bootptab file to a server. If you select **Server**, the **Filename** field becomes active and you can change the Bootptab filename (originally specified in the Server Profile).

3 Select the Bootp server from the **Bootp Server List** and click **OK**.

4 If you selected **Screen**, the Bootp object records for this Bootp server appear in the Bootptab Generation Results window. If desired, you can search, copy, print, or email the Bootptab file. Click **Exit** to close the window.



Bootp Server : bootp.lucent.com

Search Pattern :

```
#
# Bootp Table:
#   Bootp Server: bootp.lucent.com
#   Bootp Range:
#
# Global entry
global.qip:\
    :bs:

# Object entries
```

5 If you selected **Server,** the Bootptab file is created in the Bootfile home directory on the server.

6 Click **Cancel** to exit this window.

END OF STEPS

Bootp 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 (**`qipbootpuserexit`**) that allows you to manipulate the Bootptab configuration file after it has been created with the **Network Services|Bootptab File Generation** function. 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\qipbootpuserexit(.bat, .exe, .cmd, .pl)
   [server_name] [server_IP] [current_push_directory]
   [remote_push_directory] [SERVER or LOCAL]
```

Parameters

The following parameters are passed to **qipbootpuserexit**:

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 temporary directory of the File Generation Service. **Note:** The directory may be set to NONE if the directory is not available.
remote_push_directory	The same directory as the *current_push_directory* but on the Remote Service. **Note:** The directory may be set to NONE if the directory is not available.
Server or **Local**	Specifies the type of push.

Note: 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 **qipbootpuserexitfgs**.

Local host generation

If you use Local Host files as part of your naming service, VitalQIP can update those with the **Network Services|Local Host Generation** option. This option creates files, hosts for all domains, networks, OSPF Areas, Subnet Organizations, Subnets or Corporations.

Generating a **Network Services|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

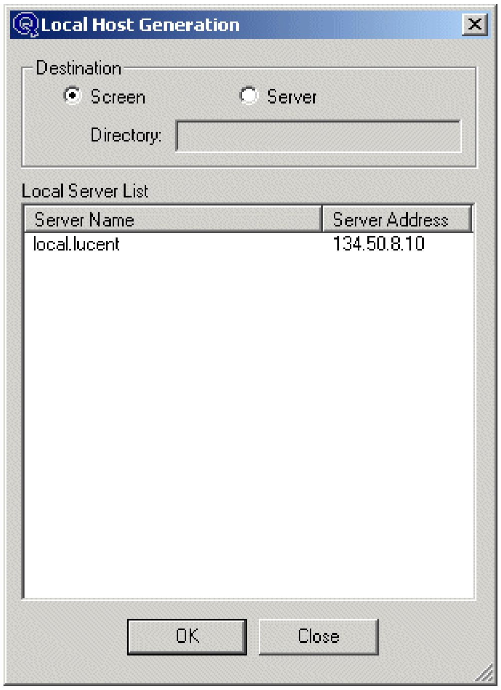
Purpose

Use this procedure to generate local host records.

Procedure

To generate local host records, follow these steps:

1 Select **Local Host Generation** from the **Network Services** menu. The Local Host Generation window opens.



Local Host Generation

Destination

● Screen ○ Server

Directory:

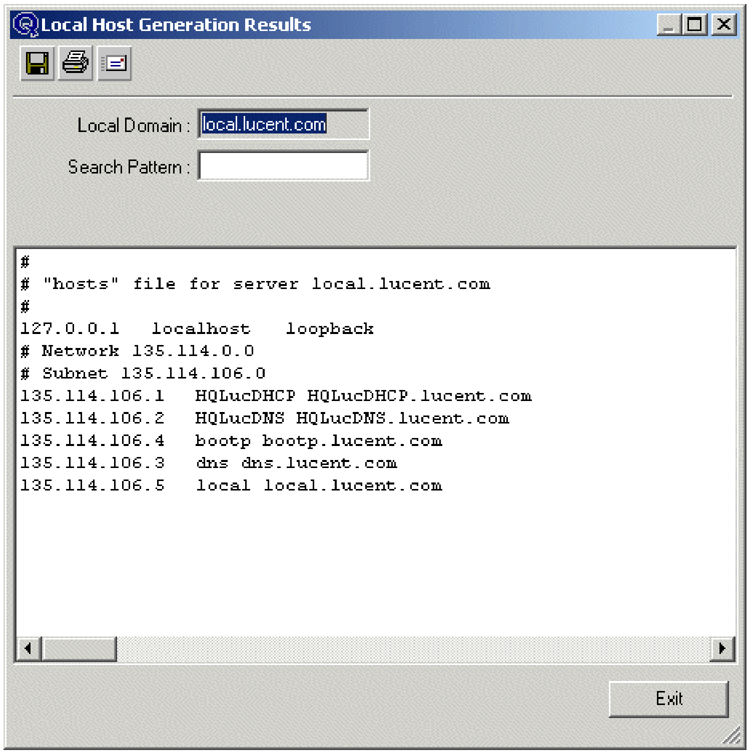
Local Server List

Server Name	Server Address
local.lucent	134.50.8.10

2 Choose a Destination option. Select **Screen** to send the host records to your computer screen, or **Server** to send them to a server. If you select **Server**, the **Directory** field becomes active and you can change the directory (originally specified in the Server Profile).

3 Select the local server from the **Local Domain List** and click **OK**.

4 If you selected **Screen**, the host records for all the domains appear in the Local Host Generation Results window. If desired, you can search, copy, print, or email them. Click **Exit** to close the window.



Local Domain : local.lucent.com

Search Pattern :

```
#
# "hosts" file for server local.lucent.com
#
127.0.0.1   localhost   loopback
# Network 135.114.0.0
# Subnet 135.114.106.0
135.114.106.1   HQLucDHCP HQLucDHCP.lucent.com
135.114.106.2   HQLucDNS HQLucDNS.lucent.com
135.114.106.4   bootp bootp.lucent.com
135.114.106.3   dns dns.lucent.com
135.114.106.5   local local.lucent.com
```

5 If you selected **Server**, the host records are exported to the specified directory on the server.

6 Click **Close** to exit this window.

END OF STEPS

Local host 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 (`qiplocaluserexit`), giving you the ability to manipulate the Local Host configuration file after its creation, using the **Network Services|Local Host Generation** function. The user exit is run if it exists and has the five parameters listed below.

Note: Use full path names within user exit routines. Otherwise, output files are directed to *%QIPHOME%*.

Synopsis

```
%QIPHOME%\userexits\qiplocaluserexit(.bat, .exe, .cmd, .pl)
   [server_name] [server_IP] [current_push_directory]
   [remote_push_directory] [SERVER or LOCAL]
```

Parameters

The following parameters are passed to **`qiplocaluserexit`**:

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 temporary directory of the File Generation Service. **Note:** The directory may be set to NONE if the directory is not available.
remote_push_directory	The same directory as the *current_push_directory* but on the Remote Service. **Note:** The directory may be set to NONE if the directory is not available.
`Server` or **`Local`**	Specifies the type of push.

Note: 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 **`qiplocaluserexitfgs`**.

NIS generation

If you use NIS as part of your naming service, VitalQIP can update those files with the NIS Generation functions. NIS Generation creates files, hosts, netmasks and ethers for all domains, networks, OSPF Areas, Subnet Organizations, Subnets or Corporations. Performing an 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

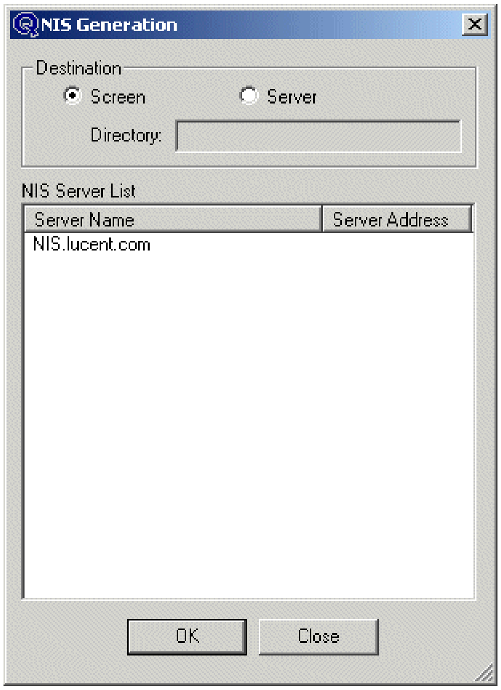
Purpose

Use this procedure to generate NIS files.

Procedure

To generate NIS files, follow these steps:

1 Select **NIS Generation** from the **Network Services** menu. The NIS Generation window opens.



Destination

● Screen ○ Server

Directory:

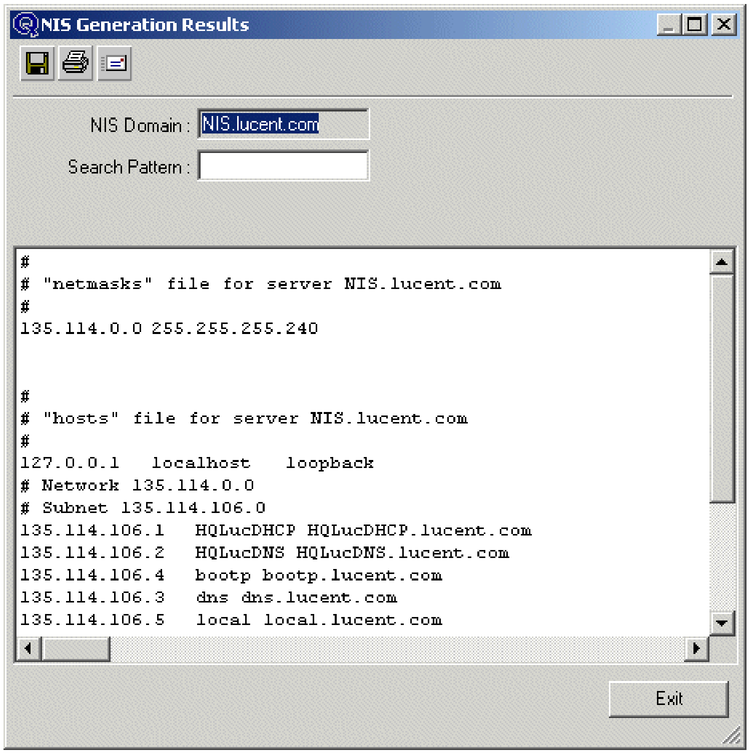
NIS Server List

Server Name	Server Address
NIS.lucent.com	

2 Choose a Destination option. Select **Screen** to send the NIS records to your computer screen, or **Server** to send them to a server. If you select **Server**, the **Directory** field becomes active and you can change the directory, if necessary.

3 Select the NIS server from the list and click **OK**.

4 If you selected **Screen**, the NIS records for all domains appear in the NIS Generation Results window. If desired, you can search, copy, print, or email them. Click **Exit** to close the window.



NIS Domain : NIS.lucent.com

Search Pattern :

```
#
# "netmasks" file for server NIS.lucent.com
#
135.114.0.0 255.255.255.240



#
# "hosts" file for server NIS.lucent.com
#
127.0.0.1   localhost   loopback
# Network 135.114.0.0
# Subnet 135.114.106.0
135.114.106.1   HQLucDHCP HQLucDHCP.lucent.com
135.114.106.2   HQLucDNS HQLucDNS.lucent.com
135.114.106.4   bootp bootp.lucent.com
135.114.106.3   dns dns.lucent.com
135.114.106.5   local local.lucent.com
```

5 If you selected **Server**, the NIS records are exported to the specified directory on the server.

6 Click **Close** to exit this window.

END OF STEPS

NIS user exit

VitalQIP provides a user exit (**`qipnisuserexit`**), giving you the ability to manipulate the Local Host configuration file after its creation with the NIS Generation function. The user exit is run if it exists and has the five parameters listed below.

> **Note:** Use full path names within user exit routines. Otherwise, output files are directed to *%QIPHOME%*.

Synopsis

```
%QIPHOME%\userexits\qipnisuserexit(.bat,.exe,.cmd) [server_name]
   [server_IP] [current_push_directory] [remote_push_directory]
   [SERVER or LOCAL]
```

Parameters

The following parameters are passed to **`qipnisuserexit`**:

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 temporary directory of the File Generation Service. **Note:** The directory may be set to NONE if the directory is not available.
remote_push_directory	The same directory as the *current_push_directory* but on the Remote Service. **Note:** The directory may be set to NONE if the directory is not available.
`Server` or **`Local`**	Specifies the type of push.

Note: 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 **`qipnisuserexitfgs`**.

Windows Domain Controller generation

The Windows DC Generation function generates the information on subnets and subnet organizations that Windows stores in its Active Directory. Once you have selected a Domain Controller, all sites and subnets associated with it are created in the Windows Active Directory.

Generate Windows Domain Controller files

Purpose

Use this procedure to generate Windows Domain Controller files.

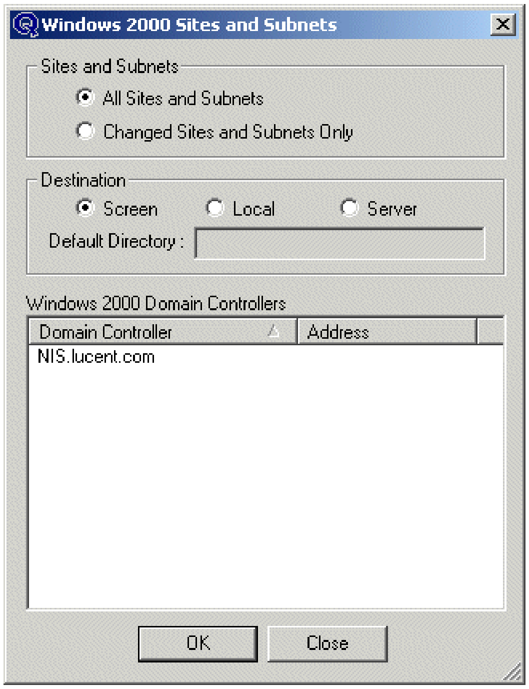
Before you begin

- LDIF files may be imported into Active Directory using Microsoft's LDIFDE tool.
- The Remote service is not required on the Domain Controller to perform a Domain Controller Generation.

Procedure

To generate Windows Domain Controller files, follow these steps:

1 Select **Windows 2000 DC Generation** from the **Network Services** menu. The Windows 2000 Sites and Subnets window opens.



Windows 2000 Sites and Subnets

Sites and Subnets
- ● All Sites and Subnets
- ○ Changed Sites and Subnets Only

Destination
- ● Screen ○ Local ○ Server

Default Directory :

Windows 2000 Domain Controllers

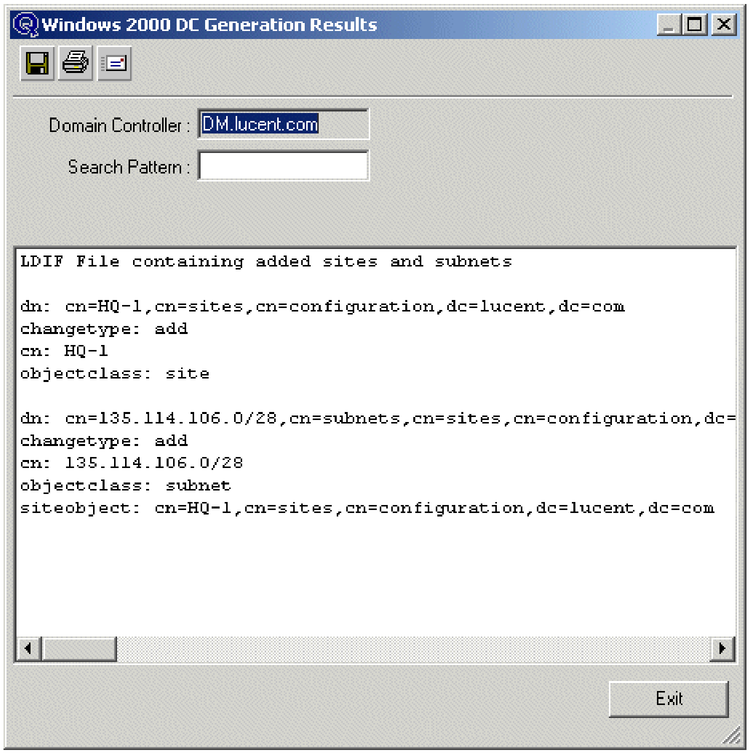
Domain Controller	Address
NIS.lucent.com	

2 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.

3 Choose a **Destination** option. Select **Screen** to send the site and subnet records to your computer screen in LDAP Data Interchange Format (LDIF), **Local** to send them to an LDIF file (the **Directory** field becomes active and you must specify a directory), or **Server** to send them to a server.

4 Highlight the **Windows 2000 Domain Controller** to which you wish to push and click **OK**.

5 If you selected **Screen**, the site and subnet records appear in the Windows 2000 DC Generation Results window.



Domain Controller : DM.lucent.com

Search Pattern :

```
LDIF File containing added sites and subnets

dn: cn=HQ-1,cn=sites,cn=configuration,dc=lucent,dc=com
changetype: add
cn: HQ-1
objectclass: site

dn: cn=135.114.106.0/28,cn=subnets,cn=sites,cn=configuration,dc=
changetype: add
cn: 135.114.106.0/28
objectclass: subnet
siteobject: cn=HQ-1,cn=sites,cn=configuration,dc=lucent,dc=com
```

If desired, you can search, copy, print, or email the results. Click **Exit** to close the window.

6 If you selected **Local**, the site and subnet records are exported to the specified directory on the local server.

7 If you selected **Server**, the site and subnet records are exported to the specified Windows Domain Controller.

8 Click **Close** to exit this window.

END OF STEPS

View active leases

The View Active Leases function generates a report about the leases for all subnets or a specific subnet of a DHCP server. This information is retrieved from the DHCP server.

Only the DHCP servers that have been assigned to you are displayed, enabling you to view leases that this DHCP server is managing. This includes “read only” and “writable” servers.

> **Note:** Lease Information is retrieved directly from the DHCP server’s lease database, not the VitalQIP database.

Generate active leases

Purpose

Use this procedure to view active leases.

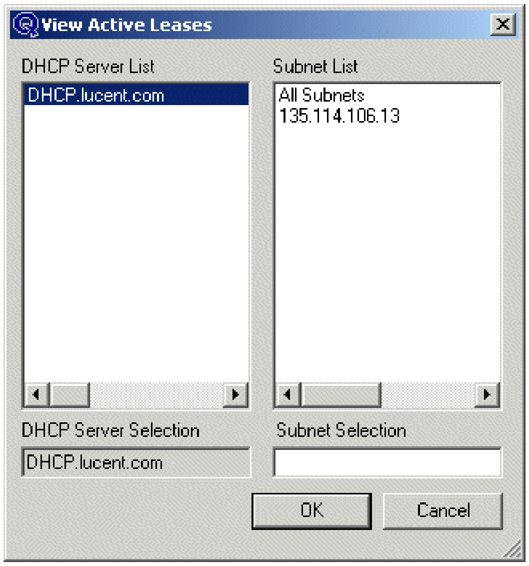
Before you begin

The VitalQIP Active Lease Service (**`qip-netd`**) must be running on the same server where the DHCP server is running to provide Active Lease information.

Procedure

To view active leases, follow these steps:

1 Select **View Active Leases** from the **Network Services** menu. The View Active Leases window opens.



DHCP Server List: DHCP.lucent.com

Subnet List: All Subnets, 135.114.106.13

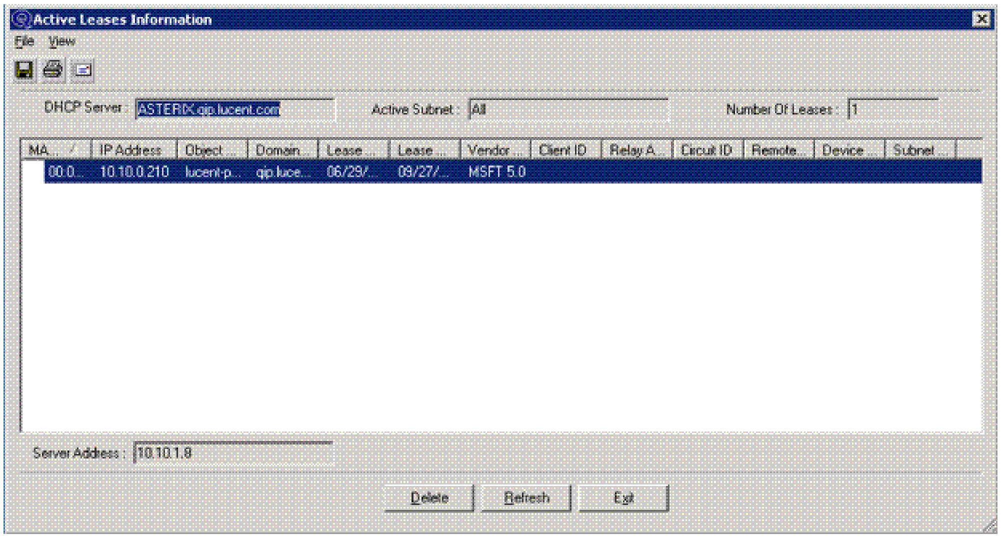
DHCP Server Selection: DHCP.lucent.com

Subnet Selection:

2 Select a DHCP server from the **DHCP Server List**. A list of subnets for this server may appear.

3 In the Subnet List window, select either a specific subnet or "All Subnets".

4 Click **OK**. An Active Leases Information report opens.



DHCP Server : ASTERIX.qip.lucent.com

Active Subnet : All

Number Of Leases : 1

MA...	IP Address	Object ...	Domain...	Lease ...	Lease ...	Vendor ...	Client ID	Relay A...	Circuit ID	Remote...	Device ...	Subnet ...
00:0...	10.10.0.210	lucent-p...	qip.luce...	06/29/...	09/27/...	MSFT 5.0						

Server Address : 10.10.1.8

The items listed in the Active Leases Information window 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.

5 Click the **Vendor Class** column to sort the vendor classes in alphabetical order.

6 Click **OK**.

End of Steps

Modify active lease reports

Purpose

VitalQIP now displays Relay Agent Information (Option 82), as provided by the DHCP Message Service.

Procedure

To modify what is displayed in the Active Lease reports, follow these steps.

1 To control which columns are displayed, select **View Columns** from the **View** menu. The default is to display all columns, but you may deselect columns as desired.

2 To display expired leases, in addition to active leases, select **View|Display Type** and check **Expired**. If the Active Lease is expired, an “X” icon appears next to that address in the display.

3 To display unparsed Option 82 data (if more options have been added to Option 82 before a VitalQIP release handles them), check **Display Columns|Relay Agent Information Option|Option**.

END OF STEPS

Delete an active lease

Purpose

Use this procedure to delete an active lease.

Procedure

To delete an Active Lease, follow these steps:

1 Select the lease from the listing. You can select multiple active leases for deletion.

2 Press **Delete**.

END OF STEPS

9 Reports

Overview

Purpose

The purpose is to describe the various management and operational reports you can run.

Contents

The following topics are covered:

Reports overview	9-3
Report types	9-6
Object List Reports	9-8
Generate an Objects by Address Range report	9-9
Generate an Objects by Location report	9-11
Generate an Objects by Administrator report	9-13
Generate an Objects by Application report	9-15
Inquire reports	9-18
Generate an Inquire report	9-19
Free Subnet report	9-25
Generate a Free Subnet report	9-26
DHCP reports	9-28
Generate a DHCP report	9-29
Administrator Profile reports	9-31
Generate an Administrator Profile report	9-32
Administrative Role reports	9-35

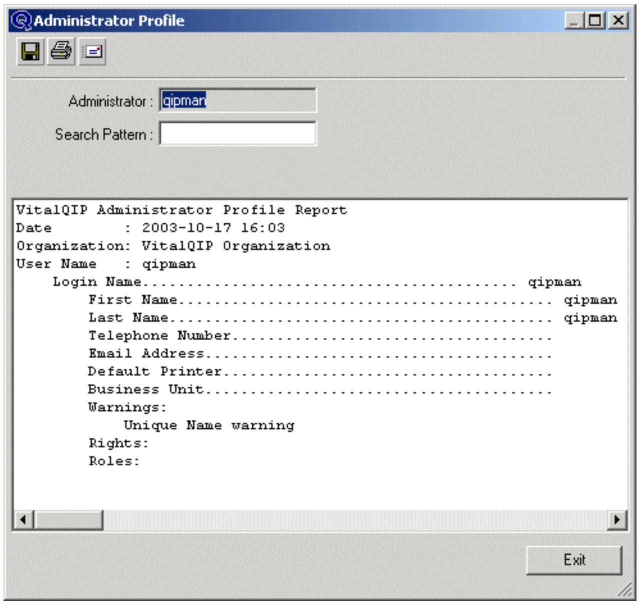
Generate an Administrative Role report	9-36
DNS Zone report	9-38
Create a DNS Zone report	9-39
Object Audit History report	9-41
Create an Object Audit History report	9-42
Administrator Audit History	9-44
Create an Administrator Audit History report	9-45

Reports overview

The Reports function allows you to obtain management and operational reports containing concise and pertinent information for certain aspects of the database. All reports can be generated in either Text or Comma Separated Values (CSV) format, and viewed immediately on the screen or saved to a file. If you request the report to be saved to a file, the Save as File window opens. You can identify where you want the report to be located and assign a filename for the report. The information can be sorted as required.

> **Note:** The **Object Name Length** global policy determines how many of characters of the Object Name are printed on a report. The default is 96. This can be changed in the **Global Policies** function on the **Policies** menu.

The following illustration displays the results of a requested report in **Text** format displayed on the **Screen**.



Administrator : qipman

Search Pattern :

```
VitalQIP Administrator Profile Report
Date        : 2003-10-17 16:03
Organization: VitalQIP Organization
User Name   : qipman
    Login Name........................................ qipman
        First Name........................................ qipman
        Last Name......................................... qipman
        Telephone Number.................................
        Email Address.....................................
        Default Printer...................................
        Business Unit.....................................
        Warnings:
            Unique Name warning
        Rights:
        Roles:
```

Once the report has been generated to the screen, you can search through the report, copy it to a file, print it or email it.

Search for a text string in a report

To search for a text string in a report, follow these steps:

1. Type the string in the **Search Pattern** field.
2. Press **Enter**.
3. To find the same string again, press **Enter** again.

Save a report to a file

To save the report to a file, follow these steps:

1. Click the **Disk** icon at the top left of the window. The Save to File window opens.
2. If you wish to output the file in Comma Separated Values (CSV) format, click **CSV Format**. In CSV format, each output line value is separated by a comma, except for the last value, which is terminated by a new line. Here is a sample of CSV output:

```
Domain=qtek.com4
Network=198.200.153.0
object name=a1, subnetmask=255.255.255.0, defaultroute=198.200.153.1
object name=a2, subnetmask=255.255.255.0, defaultroute=198.200.153.1
```

3. Fill in a file name and click **OK**.

Print a report

To print a report, follow these steps:

1. Click the **Printer** icon.
2. Fill in a printer name.
3. Click **Print**.

Email a report

When you access the **Email** icon from the report screen to email a report, VitalQIP searches for mail information in the registry. If it is found, the Email dialog box is displayed and the user can send email.

To email information to a user, follow these steps:

1. Enter at least one email address into the **To:** field. To have multiple recipients receive the report message, separate addresses with a comma or semi-colon.
2. To add an attachment, click **Attach**. You can send multiple attachments. To delete attachments, click on the attachment and press **Delete**.
3. Click **Send** when you have completed the email.

If mail information is not found, the Registry Email Information window is displayed, letting you know so that you can enter the following mail information fields, **Your name**, **Mail server**, **Email address**, and **Reply-to address**. The reply-to address is only needed if it is different from the email address. Save the data to the registry by clicking **Save**.

You can change mail information at anytime by clicking **Configure** in the Email window. Clicking this button accesses the Registry Email Information window.

Note: This program does not keep track of sent mail.

Exit the report window

To exit the Report window, click **Close**.

Report types

There are two types of reports that can be obtained via the VitalQIP interface; Management reports and Audit Histories.

Management reports

The following table describes the available management report types.

Table 9-1 Management report types

Report type	Description
Objects by Address Range	Report of all IP Addresses and their Object Classes in a Domain, Network, OSPF Area, Subnet Organization, or Subnet. This report displays by Network and Subnet.
Objects by Location	Report of all objects in a location.
Objects by Administrator	Report of all objects created by a specified administrator.
Objects by Application	Report of all objects belonging to a certain application.
Inquire	An inquiry report for a domain, OSPF area, subnet organization, subnet, object, IP address, MAC address, DECNet area and address, resource record, or UDF.
Free Subnet	Report of all free subnets available in a network.
DHCP	Report of DHCP server profile information and DHCP/Bootp objects managed by the server.
Administrator Profile	Report of a specified Administrator's profile information.
Administrative Role	Report of a specified Administrative Role information.
DNS Zone	Report of all the Resource Records for a specific zone.

Audit histories

The following table describes the audit history report types.

Table 9-2 Audit history report types

Report type	Description
Object Audit History	Report of the history of a specified object during a specified period.

Report type	Description
Administrator Audit History	Report of the history of a specified administrator during a specified period.

Object List Reports

Object List reports include:

- **Objects by Address Range** - provides a list of objects in a specific range (Domain, OSPF Area, Subnet Organization, Network, and Subnet)
- **Objects by Location** - provides a list of objects with selected location information
- **Objects by Administrator** - provides a list of objects added, modified, or deleted by the selected administrator
- **Objects by Application** - provides a list of objects associated with a particular application

All Object List reports are formatted the same with the exception of the identification of their managed range.

Generate an Objects by Address Range report

Purpose

The VitalQIP Object List reports show data by network (ascending by IP address), and then subnet (ascending by IP address). If a subnet has no objects that meet the selected criteria, the subnet information will not display. If no objects within a network are found, the network title will not display.

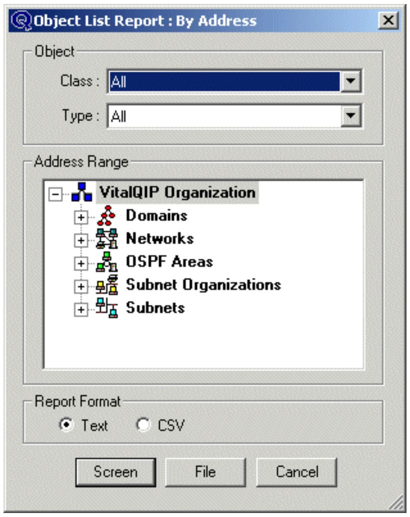
Before you begin

- Domains appear as a hierarchical tree in the **Address Range** of the Object List Report:Address Range window, only if the “Display Domain Folders” option in the **Administrator Profile|Customize** is set.
- If the “Address Range” option is Domain, the Primary Server Names appears immediately following the Domain Name in the report.
- “Object Types” are All, Static, Dynamic (None), Reserved, Dynamic (All), Dynamic-DHCP, Manual-DHCP, Automatic-DHCP, Manual-Bootp, Automatic-Bootp, and Scheduled Move.

Procedure

To generate an Object by Address Range report, follow these steps:

1 Select **Management Reports|Objects by Address** from the **Reports** menu. The Object List Report: By Address window opens.



Object List Report : By Address

Object

Class : All

Type : All

Address Range

Report Format

● Text ○ CSV

2 Select the object **Class**.

3 Select the object **Type**.

4 Select an **Address Range** on which you wish to report.

5 Select a **Report Format**.

6 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Generate an Objects by Location report

Purpose

Use this procedure to generate an Objects by Location report.

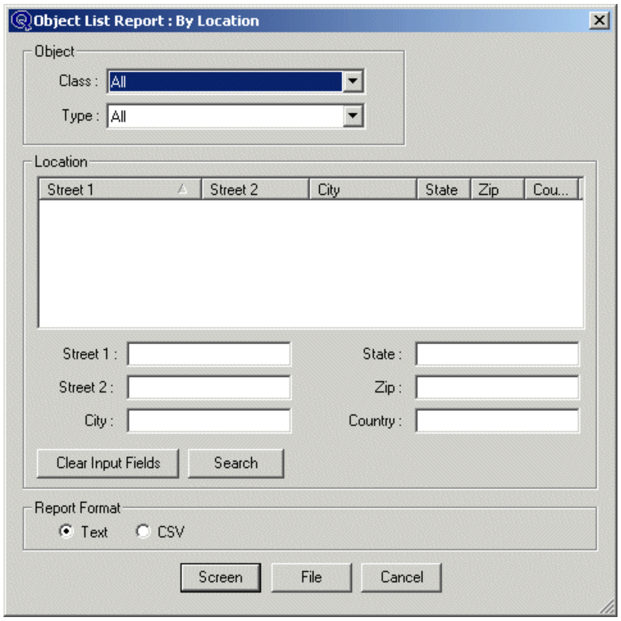
Before you begin

- The location address prints immediately following the Location Name in the report.
- "Object Types" are All, Static, Dynamic (None), Reserved, Dynamic (All), Dynamic-DHCP, Manual-DHCP, Automatic-DHCP, Manual-Bootp, Automatic-Bootp, and Scheduled Move.

Procedure

To generate an Objects by Location report, follow these steps:

1 Select **Management Reports|Objects by Location** from the **Reports** menu. The Object List Report: By Location window opens.



Object List Report : By Location

Object

Class : All

Type : All

Report Format

● Text ○ CSV

2 Select the object **Class**.

3 Select the object **Type**.

4 From the **Location** list, highlight the location for which you want a report. To search for specific locations, input search information into the input fields, and click **Search**. You can search on any or all fields. This type of search is a “begins with” search and does not require a wildcard. In other words, if you input “10” in the **Street 1** field, every address that begins with “10” will be returned (for example, 10 Valley Stream, 1010 Main Street, and so on). The list will display in the window.

5 **Clear Input Fields** enables you to change the search criteria. Click this button to clear all the search fields, or simply change the fields that differ for the next search.

6 Select a **Report Format**.

7 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Generate an Objects by Administrator report

Purpose

Use this procedure to generate an Objects by Administrator report.

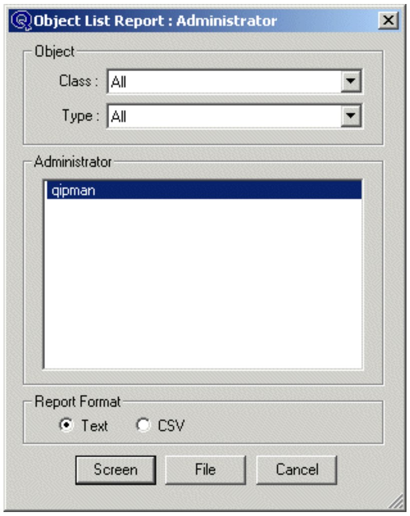
Before you begin

“Object Types” are All, Static, Dynamic (None), Reserved, Dynamic (All), Dynamic-DHCP, Manual-DHCP, Automatic-DHCP, Manual-Bootp, Automatic-Bootp, and Scheduled Move.

Procedure

To generate an Objects by Administrator report, follow these steps:

1 Select **Management Reports|Objects by Administrator** from the **Reports** menu. The Object List Report: Administrator window opens.



Class : All

Type : All

qipman

● Text ○ CSV

2 Select the object **Class**.

3 Select the object **Type**.

4 Select an **Administrator** from the listing by highlighting it.

5 Select a **Report Format**.

6 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Generate an Objects by Application report

Purpose

Use this procedure to generate an Objects by Application report.

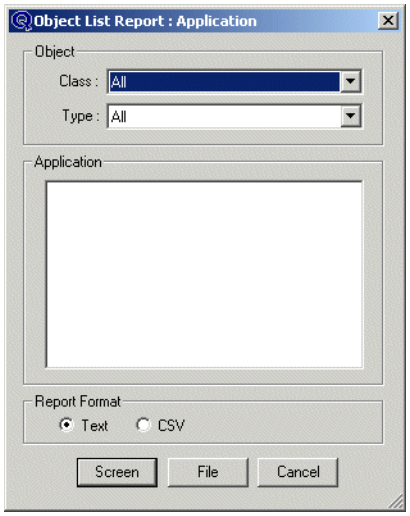
Before you begin

“Object Types” are All, Static, Dynamic (None), Reserved, Dynamic (All), Dynamic-DHCP, Manual-DHCP, Automatic-DHCP, Manual-Bootp, Automatic-Bootp, and Scheduled Move.

Procedure

To generate an Objects by Application report, follow these steps:

1 Select **Management Reports|Objects by Application** from the **Reports** menu. The Object List Report: Application window opens.



Class : All

Type : All

● Text ○ CSV

2 Select the object **Class**.

3 Select the object **Type**.

4 Select an **Application** from the listing by highlighting it.

5 Select a **Report Format**.

6 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Sample Object List report

The following is a sample Object List report:

```
VitalQIP Object List Report

Date         : 1998-06-20 12:39
Organization : VitalQIP Organization
User Name    : qipman
Range        : Corporation
Object Class : ALL
Object Type  : Static


 Network Address: 150.1.0.0 net_150.1.0.0
  Subnet: 150.1.0.0             Name: SN150.1.0.0
   IP Address  Object Name                  Obj Class     Def. Router
   Aliases
   -------------------------------------------------------------------------
   ----------
   150.1.0.1   hub-data-center.usa.world.com    Workstation    None
   150.1.0.2   dc-england.usa.world.com         Router         None
   150.1.0.3   wpenn.usa.world.com              Workstation    None

  Subnet: 150.38.20.0           Name: SN150.1.0.0
   IP Address  Object Name                  Obj Class     Def. Router
   Aliases
   -------------------------------------------------------------------------
   ----------
  150.38.20.1  hub-data-center.usa.world.com Workstation   198.200.138.15
   b.quadritek

   c.quadritek

   d.quadritek
   150.30.20.2   dc-england.usa.world.com       Router         None
```

```
Network Address: 198.200.138.32 net_198.200.138.32
  Subnet: 198.200.138.32        Name: SN198.200.138.32
   IP Address      Object Name                 Obj Class     Def. Router
   Aliases
   ------------------------------------------------------------------------
   ----------
   198.200.138.33   router3333.yourco.com         PC             None
   198.200.138.34   pcp000062pcs.yourco.com       PC             198.200.138.15
   198.200.138.35   dns1.yourco.com               Workstation    None
```

Inquire reports

The Inquire report provides detail about specific criteria. Two types of reports are generated, a listing report and a detailed object report. A listing report will be generated automatically unless only a single object is returned. If a single object is returned from the query, then a detailed object report will be displayed. The body of the report shows data by type (ascending by type description), and then by IP address (ascending by IP).

For a single object in the Detailed Object report, the following items are listed (if defined):

<table>
<tr><td>Object Name</td><td>TTL Time</td><td>Hub</td></tr>
<tr><td>Domain</td><td>Email</td><td>DECNet Area/Address</td></tr>
<tr><td>Subnet</td><td>Pager</td><td>NetBIOS Address</td></tr>
<tr><td>Subnet Name</td><td>Aliases</td><td>Bootfile</td></tr>
<tr><td>MAC Address</td><td>MX Hosts</td><td>Router Group</td></tr>
<tr><td>Room</td><td>DNS Servers</td><td>Dynamic Pushes [A|PTR|CNAME|MX records</td></tr>
<tr><td>Manufacturer</td><td>Routers</td><td>Time|TFTP Server Type</td></tr>
<tr><td>Serial Number</td><td>IP Address</td><td>DHCP Template</td></tr>
<tr><td>Host ID</td><td>Class</td><td>Client Class</td></tr>
<tr><td>Description</td><td>Subnet Mask</td><td>Contact</td></tr>
<tr><td>Slot</td><td>Application</td><td>Phone</td></tr>
<tr><td>IPX Address</td><td>Expiration</td><td>Location</td></tr>
<tr><td>FTP Server</td><td>Tag</td><td>Forwarders</td></tr>
<tr><td>Hardware Type</td><td>Model Type</td><td>Hub Slots</td></tr>
<tr><td>Name Services</td><td>Asset Number</td><td>Time Servers</td></tr>
<tr><td>DHCP Server</td><td>Purchase Date</td><td>User-Defined Fields</td></tr>
<tr><td>Lease Time</td><td></td><td></td></tr>
</table>

Generate an Inquire report

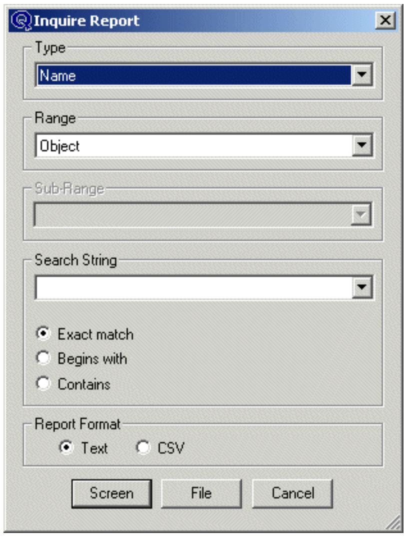
Purpose

Use this procedure to generate an Inquire report.

Procedure

To generate an Inquire report, follow these steps:

1 Select **Management Reports|Inquire** from the **Reports** menu. The Inquire Report window opens.



Type: Name

Range: Object

Sub-Range:

Search String:

● Exact match
○ Begins with
○ Contains

Report Format: ● Text ○ CSV

2 Fill in the following fields:

Type

In the **Type** field, select whether you are searching for a Name, IP Address, MAC Address, DECNet Address, User Defined Field, or Resource Record field. The following table describes the **Type** field options.

Table 9-3 Type field options

Type	Range	Sub-Range	Search String	Description
Name	All Domain Network OSPF Area Subnet Organization Subnet Object Alias Name Router Group	N/A	Refer to the description for the **Search String** field.	This will search for all the objects within a specific range based on the **Search String** field.
Address	All Network Subnet Object	N/A	Must be exact in the following format: 000.000.000.000	This will search for all the IP addresses within a specific range based on the entry in the **Search String** field.
MAC Address	N/A	N/A	Must be in either 12 or 16 character format. This format is determined by the **Allow 16 Character MAC Address** global policy.	This will search for all the MAC addresses based on the entry in the **Search String** field.
DECNet Address	N/A	N/A	Must be the following format: 00,0000	This will search for all the DECNet addresses based on the entry in the **Search String** field.

Type	Range	Sub-Range	Search String	Description
User Defined Field	All Organization Domain Reverse Zone Subnet User Object	All or the UDFs for the selected Range	Refer to the description for the **Search String** field.	This will search for the specified User Defined Field(s) based on the entry in the **Search String** field, and the selections in the **Range** and **UDF Field Name** fields.

Type	**Range**	**Sub-Range**	**Search String**	**Description**
Resource Record	All Object Domain Reverse Zone	All (all resource record types) A (Host Ipv4) CNAME (Canonical Name) HINFO (Host Information) MX (Mail Exchange) NS (Name Server) PTR (Pointer) TXT (Text) WKS (Well Known Services) AAAA (Host Ipv6) AFSDB (Andrew File System) MB (Mailbox Name) MG (Mail Group) MINFO (Mailbox Information) MR (Mail Rename) ISDN SRV (Server Resource Record) X25	Refer to the description for the **Search String** field.	This will search for the specified resource records (entered by the **Resource Record** tab on the reverse zone, domain, or object), based on the **Search String** field.

Range

Select the **Range** you will be searching (for example, Object, Domain, Network, and so on). This field is not accessible when “MAC Address”, or “DECNet Address” is selected from the **Type** drop-down list.

Resource Record Type

This field is enabled if you selected "Resource Record" from the **Type** drop-down list. Select type of resource record (such as, CNAME, MX, HINFO, and so on) you are looking for.

Search String

Just below the **Search String** field, an example appears of what the string should look like. Enter the IP Address in dotted decimal notation (for example, 198.200.138.217). Type the MAC addresses with (or without) colon separators (for example, 00:0A:0B:11:33:22).

> **Note:** The wildcard character * can be used as part of the search string. * matches 1 or more characters. These characters cannot be used when "Address", "MAC Address", or "DECNet Address" is selected in the **Type** field. Also, the VitalQIP web client interface does not recognize this wildcard character.

3 If you selected "Name", "User Defined Field", or "Resource Record" from the **Type** field, the **Search String** radio buttons become active. Choose one of the radio buttons.

- **Exact match** - a name, User-Defined Field, or resource record that exactly matches the text you typed.
- **Begins with** - a name, User-Defined Field, or resource record that begins with the text you typed. Example: You could type "Freeh" to search for "Freehold".
- **Contains** - a name, User-Defined Field, or resource record that contains the text you typed somewhere within it. Example: You could type "xts" to search for names, such as "xts000001xts".

4 Select a **Report Format**.

5 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Sample Inquire report

The following samples are of a compressed and detailed Inquire report.

Sample 1 - Object Listing report

The following is a sample Object Listing report.

```
VitalQIP Inquiry Report
```

```
Date: 1998-06-20 12:39
Organization: VitalQIP Organization
User Name: qipman

TypeAddressName
------------------------------------------------------------
Domain Name---yourcompany.com
Domain Name---us.yourcompany.com
OSPF Area---Yourcompany Backbone
Alias Name198.200.138.23
Object Name198.200.138.1
```

Sample 2 - Detailed Object report

The following sample is a detailed object report. Only one object is displayed, and only the fields defined for that object are displayed. The report is the same for each object.

```
VitalQIP Inquiry Report
Date : 1998-06-20 12:39
Organization: VitalQIP Organization
User Name : qipman

Object Detail Information
  Object Name.......................... miked-nt
  IP-Address...........................198.200.138.213
  Mac Address..........................112233445566
  Object Type..........................static
  Domain Name..........................yourcompany.com
  Network..............................198.200.138.0
  Subnet Address.......................198.200.138.0
  Subnet Mask..........................255.255.255.0
  Subnet Name..........................Yourcompany Yourcity
  Name Services........................Y (A and PTR records)
  Dynamic Pushes.......................A,PTR,CNAME,MX
  TTL Time.............................Unlimited
  Object Class.........................Server
  Dual Protocol........................None
  DNS Server...........................miked-nt.yourcompany.com
       ...............................john.yourcompany.com
  Router(s)............................198.200.138.18
```

Free Subnet report

The VitalQIP Free Subnet report shows undefined address space where a subnet can be created. If a network has no subnets that meet the selected criteria, the subnet information will not display. If no subnets within a network are found, the network title will not display.

Generate a Free Subnet report

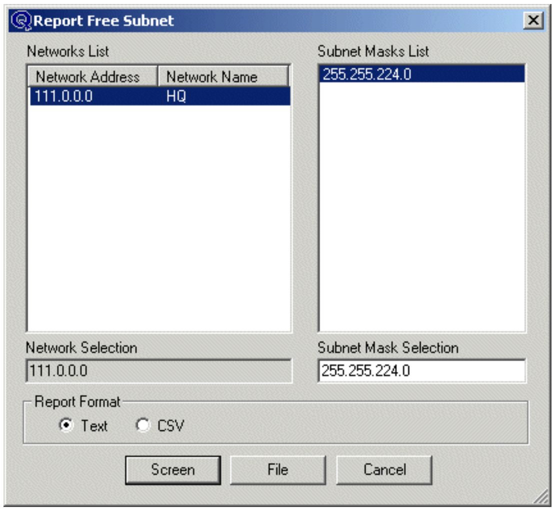
Purpose

A Free Subnet report will retrieve all free subnets in a specified network given the specified Subnet.

Procedure

To generate a Free Subnet report, follow these steps:

1 Select **Management Reports|Free Subnet** from the **Reports** menu. The Report Free Subnet window opens.



Networks List

Network Address	Network Name
111.0.0.0	HQ

Subnet Masks List: 255.255.224.0

Network Selection: 111.0.0.0

Subnet Mask Selection: 255.255.224.0

Report Format: ● Text ○ CSV

2 Select a network from the **Network List**. The Subnet Masks in that network appear in the **Subnet Masks List**.

3 Select a subnet mask from the **Subnet Masks List**, and it displays in the **Subnet Mask Selection** field. You can, alternatively, enter a mask in the **Subnet Mask Selection** field.

4 Select a **Report Format**.

5 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Sample Free Subnet Report

The following is a sample Free Subnet report:

```
VitalQIP Free Subnet Report
Date        : 1999-02-25 15:07
Organization: VitalQIP Organization
User Name   : qipman
    198.200.122.0
    198.200.122.64
    198.200.122.128
    198.200.122.192
```

DHCP reports

The DHCP report provides a report on DHCP information for a particular DHCP server within the system. You can create either a compressed or an expanded report. If there are manual DHCP objects assigned to a DHCP server, the MAC address will display in this report.

In the Expanded and Compressed DHCP reports, for each range within a subnet, the following information appears:

Start and End Address

Template Names

Dynamic Type

MAC Address

Lease Time

For Manual Bootp objects, the end address is blank.

For Non-Manual Bootp ranges, the MAC address appears as “---,” and the Lease Time is either “UNLIMITED” or “x Days x Hours x Minutes x Seconds”.

Generate a DHCP report

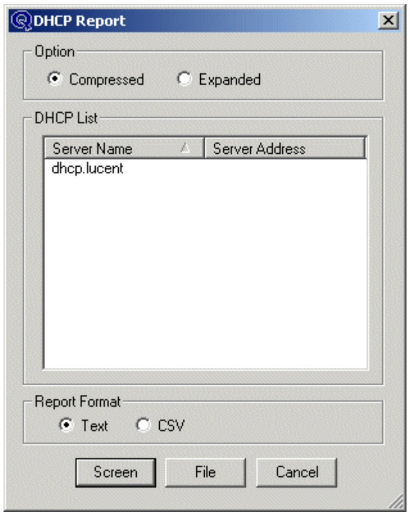
Purpose

A DHCP report will retrieve all DHCP parameters configured for a selected DHCP server and its managed objects, and list the information in an expanded or compressed format.

Procedure

To generate a DHCP report, follow these step:

1 Select **Management Reports|DHCP** from the **Reports** menu. The DHCP Report window opens.



DHCP Report

Option: ● Compressed ○ Expanded

DHCP List

Server Name	Server Address
dhcp.lucent	

Report Format: ● Text ○ CSV

2 Select a DHCP server from the **DHCP Server List**.

3 Select whether you want a **Compressed** (only the DHCP server name opens) or an **Expanded** format. The **Expanded** format will include the Lucent DHCP server's configuration parameters.

4 Select a **Report Format**.

5 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Sample DHCP report

The following samples are of an expanded DHCP report and compressed DHCP report.

Sample 1 - Expanded DHCP report

The following is an expanded DHCP report:

```
VitalQIP DHCP Report
Date        : 2009-06-09 01:59
Organization: VitalQIP Organization
User Name   : qipman
DHCP Server : qlnx2vm2.qa.lucent.com
Report Type : Expanded

Server Name........................................ qlnx2vm2.qa.lucent.com
Managed Range...................................... Corporation
Default Directory.................................. c:\qip
DHCP Template...................................... general
Accept Client Names................................ True
Additional Policies................................ line1
Registered Clients Only............................ False
Remote Server Proxy................................
    Description........................................ Test
Scheduled Automatic Updates........................ None
Support Bootp...................................... True

MAC Pool:
```

Sample 2 - Compressed DHCP report

The following is a sample DHCP report:

```
VitalQIP DHCP Report
Date        : 2009-06-09 01:59
Organization: VitalQIP Organization
User Name   : qipman
DHCP Server : qlnx2vm2.qa.lucent.com
Report Type : Compressed
Server Name........................................ qlnx2vm2.qa.lucent.com
MAC Pool:
```

Administrator Profile reports

The Administrator Profile report provides profile information for the specified administrator.

If defined, Warnings will display as one or more of the following:

```
Unique Name Warning
MAC Address Warning
Alias Warning
Location Warning
General Object Warning
Contact Name Warning
User Name Warning
Delete Confirmation
```

If defined, Privileges will display as one or more of the following:

```
Create New Administrators
Create Infrastructure
Create DNS Resource Records
```

If defined, Rights will display a listing of each thing the administrator has access to:

```
Domain quadritek.com
Network 198.200.138.0
Application my_app
```

If defined, Roles displays a listing of Administrative Roles the administrator has been assigned.

Generate an Administrator Profile report

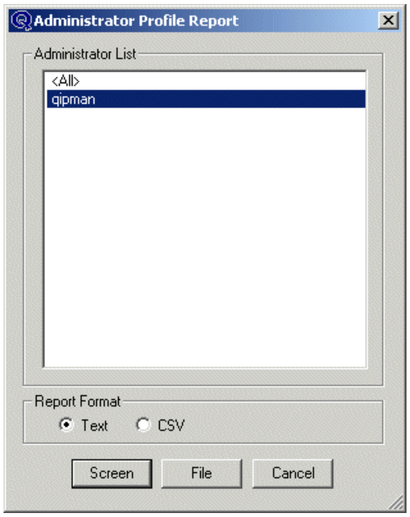
Purpose

The Administrator Profile report displays all the values for the fields supplied through the Administrator Profile function.

Procedure

To generate an Administrator Profile report, follow these steps:

1 Select **Management Reports|Administrator Profile** from the **Reports** menu. The Administrator Profile Report window opens.



2 Select an Administrator from the **Administrator List**.

3 Select a **Report Format**.

4 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Sample Administrator Profile report

The following is a sample Administrator Profile report:

```
VitalQIP Administrator Profile Report
```

```
Date        : 2008-10-21 13:05
Organization: VitalQIP Organization
User Name   : qipman
    Login Name.......................................... qipman
    First Name.......................................... qipman
    Last Name........................................... qipman
    Telephone Number....................................
    Email Address.......................................
    Default Printer.....................................
    Business Unit.......................................
    Default System Privileges
    Allow Password Expiration........................... True
    Delete Confirmation................................. False
    Require Alias....................................... False
    Require Contact Name................................ False
    Require Location.................................... False
    Require MAC Address................................. False
    Require Manufacturer Information.................... False
    Require User........................................ False
    Unique Name Warning................................. False
    Access list
        Organization: Demo 1................................ Organization
            Read Only........................................... False
                Use Default......................................... False
                   Access Node Management.............................. False
                   Access V6 Address Management....................... False
                    Highest Level GUI Mode..............................
   Advanced Mode
Create Infrastructure............................... True
                            Dynamic Domain
   Creation............................ True
                       Create Resource Records.............................
   True
                   Access Address Allocation........................... False
                   Allow User Selection................................ False
                   Delete Confirmation Warning......................... False
                   Display MyView Tab Only............................. False
                   Require Alias....................................... False
                   Require Contact Name................................ False
                   Require Location.................................... False
                   Require MAC Address................................. False
                   Require Manufacturer Information.................... False
                   Restrict CNAME...................................... False
                   Restrict Subnet..................................... False
                    Unique Name Warning................................ True
        Organization: VitalQIP Organization................ Organization
            Read Only........................................... False
            Privileges
                Use Default......................................... False
                   Access Node Management............................. False
                   Access V6 Address Management....................... False
                    Highest Level GUI Mode..............................
   Advanced Mode
Create Infrastructure............................... True
                            Dynamic Domain
   Creation............................ True
                       Create Resource Records.............................
   True
                   Access Address Allocation.......................... False
                   Allow User Selection............................... False
                   Delete Confirmation Warning........................ False
                   Display MyView Tab Only............................ False
                   Require Alias...................................... False
                   Require Contact Name............................... False
                   Require Location................................... False
                   Require MAC Address................................ False
                   Require Manufacturer Information................... False
                   Restrict CNAME..................................... False
                   Restrict Subnet.................................... False
                    Unique Name Warning................................ True
```

Administrative Role reports

The Administrative Role report provides information for the specified role.

Generate an Administrative Role report

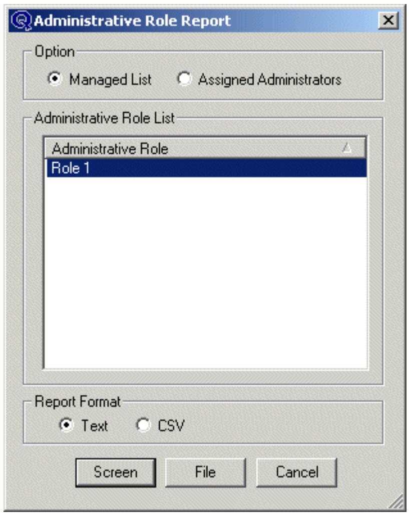
Purpose

The Administrative Role report displays all of the infrastructure data assigned to the role through the Administrative Role function.

Procedure

To generate and Administrative Role report, follow these steps:

1 Select **Management Reports|Administrative Role** from the **Reports** menu. The Administrative Role Report window opens.



2 Select the **Managed List** option or the **Assigned Administrators** option.

3 Select an Administrative Role from the **Administrative Role** list.

4 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Sample Administrative Role Report

The following is a sample report:

```
VitalQIP Role Managed List Report
```

```
Date        : 2004-01-28 14:17
Organization: VitalQIP Organization
User Name   : qipman
Role:  Admin Role A
Domain,lucent.com
Domain,example.com
Domain,example1.com
Domain,example2.com
Network,135.114.0.0,HQ
Subnet Organization,HQ-1
Server - DHCP,135.114.106.1,HQLucDHCP.lucent.com
Server - DNS,135.114.106.2,HQLucDNS.lucent.com
Server - DNS,135.114.106.3,dns.lucent.com
Server - BOOTP,135.114.106.4,bootp.lucent.com
Server - LOCAL_HOST,135.114.106.5,local.lucent.com
Server - NIS,0.0.0.0,NIS.lucent.com
Server - DOMAIN CONTROLLER,135.114.106.6,DM.lucent.com
```

DNS Zone report

The DNS Zone report displays all of the Resource Records for a specified zone. The format of the report is identical to a BIND-compliant DNS zone file.

Create a DNS Zone report

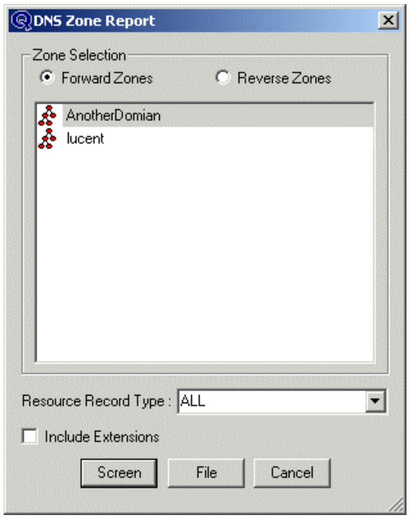
Purpose

Use this procedure to create a DNS Zone report.

Procedure

To create a DNS Zone report, follow these steps:

1 Select **Management Reports|DNS Zone** from the **Reports** menu. The DNS Zone Report window opens.



DNS Zone Report

Zone Selection

● Forward Zones ○ Reverse Zones

AnotherDomian
lucent

Resource Record Type : ALL

□ Include Extensions

2 Select whether you want this report for the **Forward Zones** or the **Reverse Zones**.

3 Select the Domain you want to see the DNS zones for.

4 Select the **Resource Record Type** (All, A, PTR, CNAME, and so on), and decide whether to **Include Extensions** for this zone.

> **Note:** If the Zone Extensions are included in the report, ALL extensions are displayed and no formatting of the extensions is performed.

5 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Sample DNS Zone report

A sample DNS Zone report to the screen follows:

```
;*************
; A records
;*************
localIN  A 135.114.106.5
dns  IN  A 135.114.106.3
bootpIN  A 135.114.106.4
HQLucDNSINA 135.114.106.2
HQLucDHCPINA135.114.106.1
DM   IN  A 135.114.106.6
```

Object Audit History report

The Object Audit History report displays the history of a specified object.

Once a subnet is deleted, the Audit report can continue to be produced. If the subnet information for the Audit report cannot be found in the subnet table, then the report will look to the subnet audit table for the subnet information. If the subnet information cannot be found in the subnet audit table, then the subnet IP address displayed on the report will be 0.0.0.0 and the subnet mask will be 255.0.0.0.

The Object Audit History report does not show changes in DHCP lease information, such as MAC address changes, for DHCP objects. An additional Add-on product, Audit Manager, should be purchased to acquire this functionality.

Create an Object Audit History report

Purpose

Use the Object Audit History to retrieve the history of an object for a certain period.

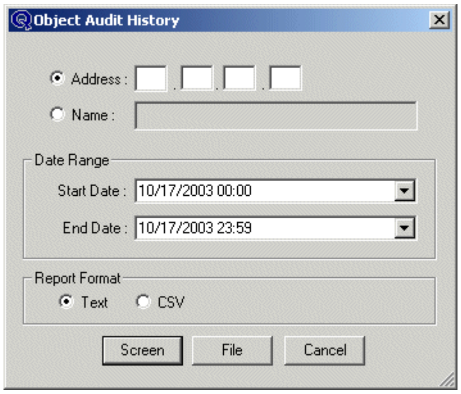
Before you begin

- When “SM” appears in a report, it indicates that the object has a scheduled move.
- Any objects added by an administrator whose profile is later deleted are identified as “Unknown Administrator”.

Procedure

To generate an Object Audit History report, follow these steps:

1 Select **Object Audit History** from the **Reports** menu. The Object Audit History window opens.



● Address : □ . □ . □ . □

○ Name : □

Date Range

Start Date : 10/17/2003 00:00

End Date : 10/17/2003 23:59

Report Format

● Text ○ CSV

2 Type the **Name** or the **IP Address** of the object for which you want to obtain an audit history report.

Note: After an object has been deleted, only use the **IP Address** option to retrieve audit history for that object.

3 Select a **Start Date** and **End Date** for the period of time you want to view. The start date must be earlier than the end date, or else an empty report is generated.

Note: The dates are in *mm/dd/yyyy hh:mm* format. The default start time is 00:00. The default end time is 23:59.

4 Select a **Report Format** (**Text** or **CSV**).

5 Click **Screen** to bring the report to the screen, or click **File** to save the report to a file.

END OF STEPS

Sample Object Audit History Report

The following is a sample Object Audit History report:

```
VitalQIP Object Audit Report
Date        : 2002-01-02 10:32
Organization: VitalQIP Organization
User Name   : qipman

ADDED                     12/28/2001 11:02:00 qipman

Object Name.................... santaserver
IP Address..................... 198.102.15.10
Domain......................... northpole.com
Class.......................... Server
Subnet Address................. 198.102.15.0
Subnet Mask.................... 255.255.255.224
Subnet Name....................
Name services.................. Y (A and PTR records)
Dynamic pushes................. A, PTR, CNAME, MX
TTL time....................... Unlimited
```

Administrator Audit History

The Administrator Audit History report displays the history of an administrator.

Once a subnet is deleted, the Audit report can continue to be produced. If the subnet information for the Audit Report cannot be found in the subnet table, then the report will look in the subnet audit table for the subnet information. If the subnet information cannot be found in the subnet audit table, then the subnet IP address displayed on the report will be 0.0.0.0 and the subnet mask will be 255.0.0.0.

Create an Administrator Audit History report

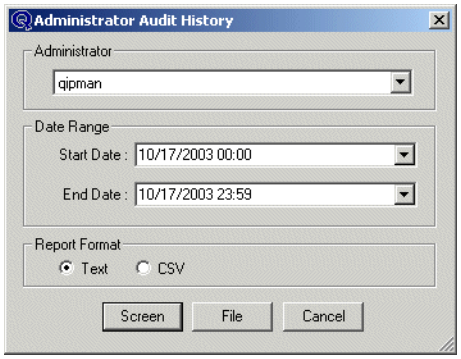
Purpose

The Administrator Audit History retrieves the history of object management activities performed by the selected administrator for a certain period.

Procedure

To generate an Administrator Audit History report, follow these steps:

1 Select **Administrator Audit History** from the **Reports** menu. The Administrator Audit History window opens.



Administrator: qipman

Date Range
Start Date : 10/17/2003 00:00
End Date : 10/17/2003 23:59

Report Format: ● Text ○ CSV

2 Type the **Administrator** name or select an administrator from the drop-down list for which you want to obtain an audit history report.

3 Select a **Start Date** and **End Date** for the period of time for which you want the history of an administrator. The start date must be earlier than the end date, or else an empty report is generated.

> **Note:** Dates are in *mm/dd/yyyy hh:mm* format. The default start time is 00:00. The default end time is 23:59.

4 Select a **Report Format** (**Text** or **CSV**).

5 Click **Screen** to bring the report to the screen or **File** to save the report to a file.

END OF STEPS

Sample Administrator Audit History Report

The following is a sample Administrator Audit History report:

```
VitalQIP Administrator Audit Report
Date        : 2002-01-02 11:20
Organization: VitalQIP Organization
User Name   : qipman

ADDED                12/28/2001 11:02:00 qipman

Object Name.................... santaserver
IP Address..................... 198.102.15.10
Domain......................... northpole.com
Class.......................... Server
Subnet Address................. 198.102.15.0
Subnet Mask.................... 255.255.255.224
Subnet Name....................
Name services.................. Y (A and PTR records)
Dynamic pushes................. A, PTR, CNAME, MX
TTL time....................... Unlimited

ADDED                12/07/2001 14:32:00 qipman

Object Name.................... kyu
IP Address..................... 198.200.138.5
Domain......................... qtek.com
Class.......................... Server
Subnet Address................. 198.200.138.0
Subnet Mask.................... 255.255.255.192
Subnet Name....................
Name services.................. Y (A and PTR records)
Dynamic pushes................. A, PTR, CNAME, MX
TTL time....................... Unlimited
```

10 Import data

Overview

Purpose

The purpose is to describe the use of the VitalQIP Graphical User Interface to import data.

Contents

The following topics are covered:

VitalQIP import/export functions	10-2
Import with VitalQIP GUI	10-2
Import data for domain, OSPF area, network, subnet, or subnet organization	10-3
Import data for objects	10-6
Import data into a MAC address pool	10-10

VitalQIP import/export functions

VitalQIP has various types of import and export capabilities. You can import and export whole VitalQIP databases with the **`qip-import`** and **`qip-export`** Command Line Interface (CLI) commands. You can import certain files and data using the VitalQIP graphical user interface or using the CLI. You can also export DNS and Bootptab file information. All of this information can be found in the *VitalQIP Command Line Interface User's Guide*.

> **Note:** It is recommended that you test the format of the files you intend to import with just a few records before you attempt to import large numbers of objects.

It is also recommended that you follow a logical order when you import data into your database.

1. DNS Servers (**`enterdnssvr`**)
2. Domains (**`enterdomain`**)
3. Networks (**`enternetwork`**)
4. Subnets (**`entersubnet`**)
5. Simple Objects (**`entersimpleobj`**)

During the import, it is recommended that you redirect error messages to a file to trap the potential error messages generated by the VitalQIP, Sybase and/or Oracle database servers. For example, when you run **`enterdomain`** to import domain information, run

```
enterdomain -i datafile.dat -e err.dat
```

Import with VitalQIP GUI

The Import function allows you to import data into VitalQIP from an existing database. You can import data for domains, OSPF areas**,** networks, subnets, subnet organizations, objects, or MAC address pools.

The data for a required higher-level item must exist before you can import the data for lower-level items. For example, before you can import subnet data, the domain data for these subnets must already exist as well as the OSPF area data and/or network data, if used.

> **Note:** All data lines must end in a carriage return, or they are not imported. This includes the final line in an import data file.

Before and after you import a large file, you should backup VitalQIP's database for recovery purposes, using **`qip-export`**. It is also advisable to test the format of the import files with just a few records before attempting an import of many objects.

Import data for domain, OSPF area, network, subnet, or subnet organization

Purpose

Use the following procedure to import data for a domain, OSPF area, network, subnet, or subnet organization.

Before you begin

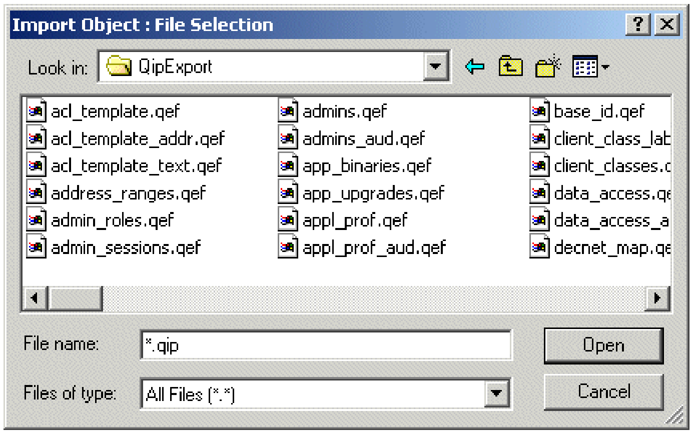
For information on import file formats, refer to the File Format Example for the **enterdomain**, **enterospf**, **entersubnet**, **entersubnetorg**, or **enternetwork** CLI commands in the *VitalQIP Command Line Interface User's Guide*.

Procedure

To import data for a domain, OSPF area, network, subnet, or subnet organization, follow these steps:

1 Select one of the following from the **Import** menu and the File Selection window opens:

- **Domain**
- **Network**
- **OSPF**
- **Subnet**
- **Subnet Organization**



Import Object : File Selection

Look in: QipExport

acl_template.qef
acl_template_addr.qef
acl_template_text.qef
address_ranges.qef
admin_roles.qef
admin_sessions.qef
admins.qef
admins_aud.qef
app_binaries.qef
app_upgrades.qef
appl_prof.qef
appl_prof_aud.qef
base_id.qef
client_class_lab
client_classes.c
data_access.qe
data_access_a
decnet_map.qe

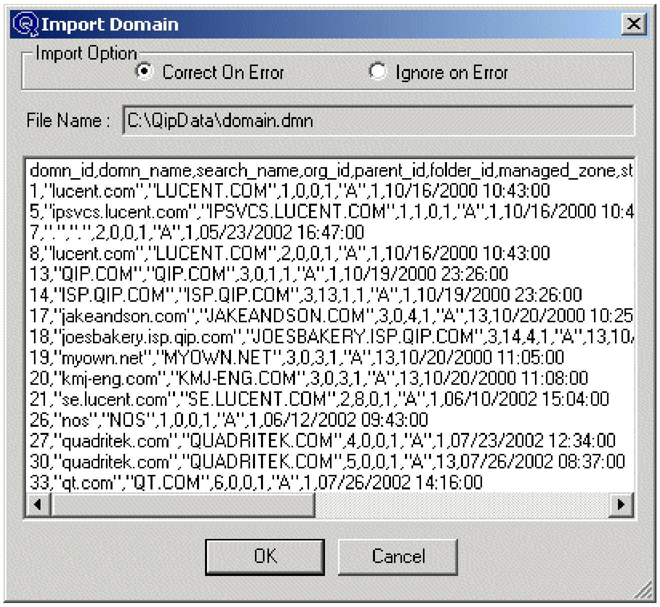
File name: *.qip

Files of type: All Files (*.*)

2 Select the drive, directory, and file you wish to import. You can import the following file types:

- *Domain - .dmn*
- *Network - .net*
- *OSPF - .osp*
- *Subnet - .sub*
- *Subnet Organization - .org*

3 Click **OK**. The Import window opens. It shows the contents of the file you specified.



Import Option: ● Correct On Error ○ Ignore on Error

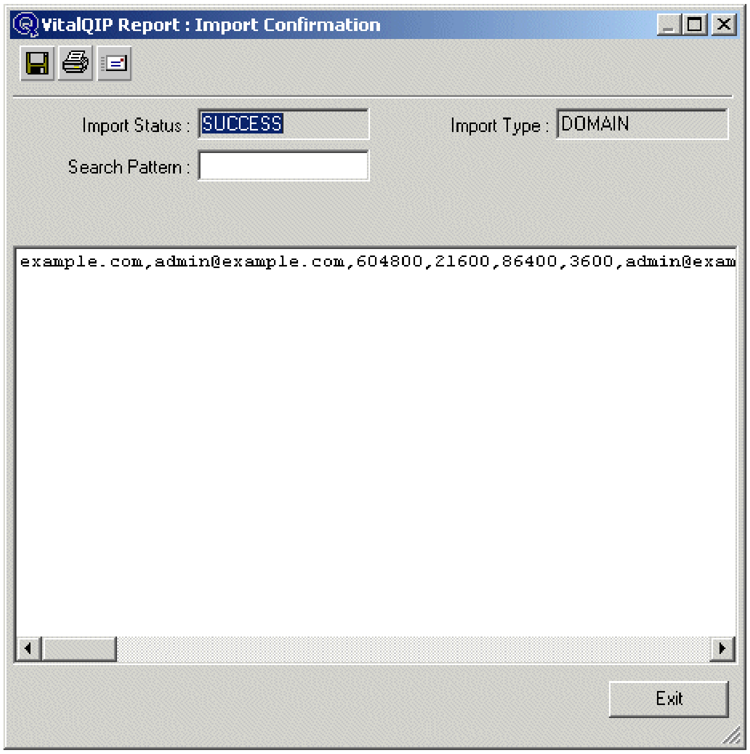
File Name : C:\QipData\domain.dmn

```
domn_id,domn_name,search_name,org_id,parent_id,folder_id,managed_zone,st
1,"lucent.com","LUCENT.COM",1,0,0,1,"A",1,10/16/2000 10:43:00
5,"ipsvcs.lucent.com","IPSVCS.LUCENT.COM",1,1,0,1,"A",1,10/16/2000 10:4
7,".",".",2,0,0,1,"A",1,05/23/2002 16:47:00
8,"lucent.com","LUCENT.COM",2,0,0,1,"A",1,10/16/2000 10:43:00
13,"QIP.COM","QIP.COM",3,0,1,1,"A",1,10/19/2000 23:26:00
14,"ISP.QIP.COM","ISP.QIP.COM",3,13,1,1,"A",1,10/19/2000 23:26:00
17,"jakeandson.com","JAKEANDSON.COM",3,0,4,1,"A",13,10/20/2000 10:25
18,"joesbakery.isp.qip.com","JOESBAKERY.ISP.QIP.COM",3,14,4,1,"A",13,10/
19,"myown.net","MYOWN.NET",3,0,3,1,"A",13,10/20/2000 11:05:00
20,"kmj-eng.com","KMJ-ENG.COM",3,0,3,1,"A",13,10/20/2000 11:08:00
21,"se.lucent.com","SE.LUCENT.COM",2,8,0,1,"A",1,06/10/2002 15:04:00
26,"nos","NOS",1,0,0,1,"A",1,06/12/2002 09:43:00
27,"quadritek.com","QUADRITEK.COM",4,0,0,1,"A",1,07/23/2002 12:34:00
30,"quadritek.com","QUADRITEK.COM",5,0,0,1,"A",13,07/26/2002 08:37:00
33,"qt.com","QT.COM",6,0,0,1,"A",1,07/26/2002 14:16:00
```

4 Select **Correct on Error** or **Ignore on Error**:

- **Correct on Error**: If an error is encountered in the input file, the import will be suspended to allow you to correct the error, and then continue the import.
- **Ignore on Error**: If an error is encountered in the input file, the error will be logged for you to review at the end of the import.

5 Click **OK** to start the import. The Import Result window opens.



Import Status : SUCCESS

Import Type : DOMAIN

```
example.com,admin@example.com,604800,21600,86400,3600,admin@exam
```

6 In the Import Result window, you can do the following in it:

- To search for a text string in the report, type the string in the **Search Pattern** field, then press **Enter**. To find the same string again, press **Enter** again.
- To copy the report to a directory, click **Disk** at the top left of the window. Select the drive and directory, and click **OK**.
- To print the report, click **Printer**. Select the desired printer and click **OK**.
- To email the report, click **E-mail**. Fill in the Email address you wish to send the report to and click **OK**.

Note: Back up VitalQIP's database immediately after importing a large file. Refer to the *Administrator Reference Manual*.

END OF STEPS

Import data for objects

Purpose

Use this procedure to import data for objects.

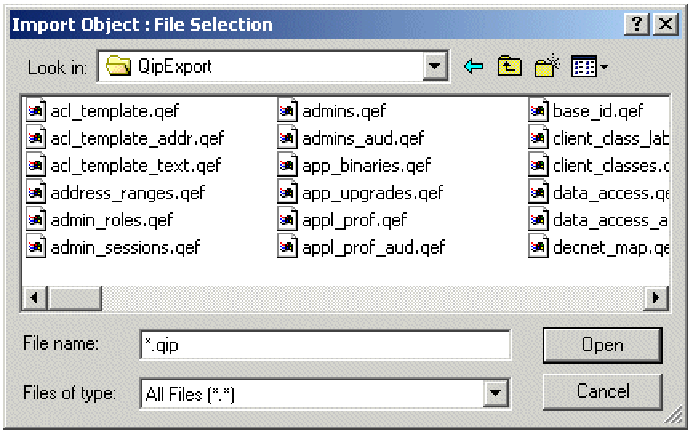
Before you begin

For information on import file formats, refer to the proper file format table for the **`entersimpleobj`**, **`enterdnsobj`**, or **`enterlocalobj`** CLI commands in the *VitalQIP Command Line Interface User's Guide*.

Procedure

To import data for objects, follow these steps:

1 Click **Import** on the VitalQIP main menu, and select **Object** from the **Import** menu. The File Selection window opens.



Look in: QipExport

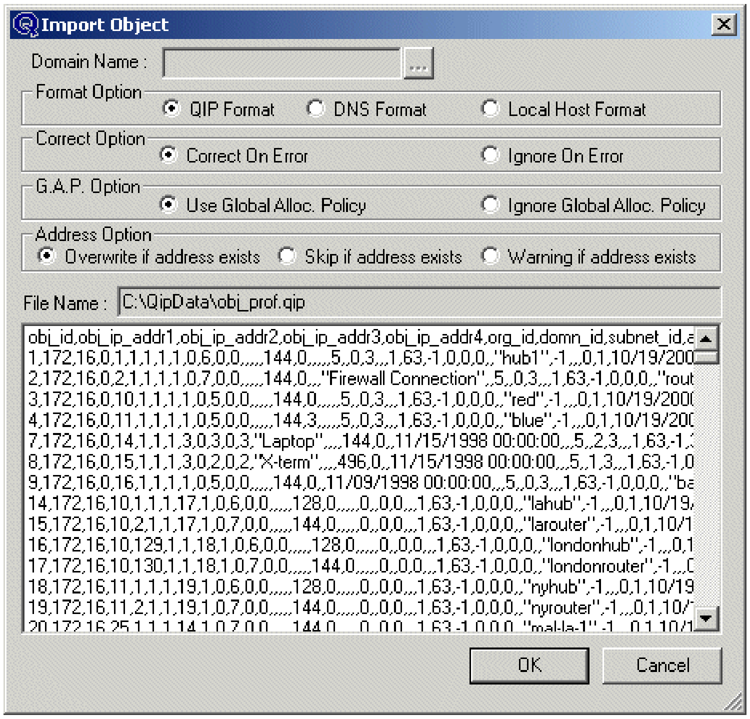
File name: *.qip

Files of type: All Files (*.*)

2 Select the drive, directory and file you wish to import. You can import the following file types:

- *QIP format - .qip*
- *DNS format - .dns*
- *Localhost - .hst*

3 Click **OK**. The Import Object window opens.



Domain Name :

Format Option: ● QIP Format ○ DNS Format ○ Local Host Format

Correct Option: ● Correct On Error ○ Ignore On Error

G.A.P. Option: ● Use Global Alloc. Policy ○ Ignore Global Alloc. Policy

Address Option: ● Overwrite if address exists ○ Skip if address exists ○ Warning if address exists

File Name : C:\QipData\obj_prof.qip

```
obj_id,obj_ip_addr1,obj_ip_addr2,obj_ip_addr3,obj_ip_addr4,org_id,domn_id,subnet_id,a
1,172,16,0,1,1,1,1,1,0,6,0,0,,,,,144,0,,,,,5,,0,3,,,1,63,-1,0,0,0,,"hub1",-1,,,0,1,10/19/200
2,172,16,0,2,1,1,1,1,0,7,0,0,,,,,144,0,,,"Firewall Connection",,5,,0,3,,,1,63,-1,0,0,0,,"rout
3,172,16,0,10,1,1,1,1,0,5,0,0,,,,,144,0,,,,,5,,0,3,,,1,63,-1,0,0,0,,"red",-1,,,0,1,10/19/200
4,172,16,0,11,1,1,1,1,0,5,0,0,,,,,144,3,,,,,5,,0,3,,,1,63,-1,0,0,0,,"blue",-1,,,0,1,10/19/20
7,172,16,0,14,1,1,1,3,0,3,0,3,"Laptop",,,,144,0,,11/15/1998 00:00:00,,,5,,2,3,,,1,63,-1,
8,172,16,0,15,1,1,1,3,0,2,0,2,"X-term",,,,496,0,,11/15/1998 00:00:00,,,5,,1,3,,,1,63,-1,0
9,172,16,0,16,1,1,1,1,0,5,0,0,,,,,144,0,,11/09/1998 00:00:00,,,5,,0,3,,,1,63,-1,0,0,0,,"ba
14,172,16,10,1,1,1,17,1,0,6,0,0,,,,,128,0,,,,,0,,0,0,,,1,63,-1,0,0,0,,"lahub",-1,,,0,1,10/19
15,172,16,10,2,1,1,17,1,0,7,0,0,,,,,144,0,,,,,0,,0,0,,,1,63,-1,0,0,0,,"larouter",-1,,,0,1,10/1
16,172,16,10,129,1,1,18,1,0,6,0,0,,,,,128,0,,,,,0,,0,0,,,1,63,-1,0,0,0,,"londonhub",-1,,,0,1
17,172,16,10,130,1,1,18,1,0,7,0,0,,,,,144,0,,,,,0,,0,0,,,1,63,-1,0,0,0,,"londonrouter",-1,,,0
18,172,16,11,1,1,1,19,1,0,6,0,0,,,,,128,0,,,,,0,,0,0,,,1,63,-1,0,0,0,,"nyhub",-1,,,0,1,10/19
19,172,16,11,2,1,1,19,1,0,7,0,0,,,,,144,0,,,,,0,,0,0,,,1,63,-1,0,0,0,,"nyrouter",-1,,,0,1,10/
20,172,16,25,1,1,1,14,1,0,7,0,0,,,,,144,0,,,,,0,,0,0,,,1,63,-1,0,0,0,,"mal-la-1",-1,,,0,1,10/1
```

4 Select the file format you are importing into VitalQIP: **QIP Format** *(.qip)*, **DNS Format** *(.dns)*, or **Local Host Format** *(.hst)*.

Note: Objects are added with an "Undefined" Object Class.

5 If you selected VitalQIP Format:

a. Select **Correct on Error** or **Ignore on Error**:

Correct on Error: If an error is encountered in the input file, the import will be suspended to allow you to correct the error, and then continue the import.

Ignore on Error: If an error is encountered in the input file, the error will be logged for you to review at the end of the import.

b. If you want to use any global allocation policy that is in effect, click **Use Global Alloc. Policy**. If you want to ignore any global allocation policy, click **Ignore Global Alloc. Policy**.

c. Select the **Address Option** you want to take if an IP address already exists: overwrite the existing address, skip it, or display a warning message.

6 If you selected **DNS Format**:

a. Select from the drop down list the **Domain Name** this data is for. Either enter a fully qualified, known domain name, or click **...** to display the Domain Option: Select window. If the **Display Domain Folders** option in **Administrator Profile|Customize** is set, this field is a browse-edit function. You can select or type in the domain. If not, domains display in list format. For more information on this option, refer to "Administrators" (p. 6-11) and "Domain folders" (p. 1-40).

b. Select **Correct on Error** or **Ignore on Error**:

Correct on Error: If an error is encountered in the input file, the import will be suspended to allow you to correct the error, and then continue the import.

Ignore on Error: If an error is encountered in the input file, the error will be logged for you to review at the end of the import.

c. Select the **Address Option** you want to take if an IP address already exists: overwrite the existing address, skip it, or display a warning message.

d. Back up the VitalQIP database immediately after importing a large file.

7 If you selected **Local Host Format**:

a. Select from the drop-down list the **Domain Name** this data is for. Either enter a fully qualified, known domain name, or click **...** to display the Domain Option:Select window. If the **Display Domain Folders** option in **Administrator Profile|Customize** is set, this field is a browse-edit function. You can select or type in the domain. If not, domains display in list format.

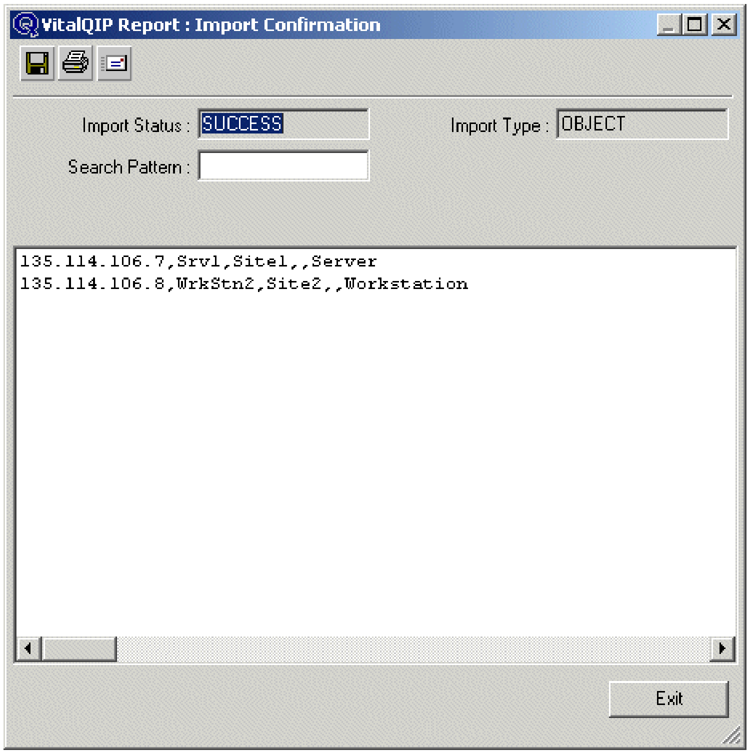
b. Select **Correct on Error** or **Ignore on Error**:

Correct on Error: If an error is encountered in the input file, the import will be suspended to allow you to correct the error, and then continue the import.

Ignore on Error: If an error is encountered in the input file, the error will be logged for you to review at the end of the import.

c. Select the **Address Option** you want to take if an IP address already exists: overwrite the existing address, skip it, or display a warning message.

8 Click **OK** the Import Result windows opens.



Import Status : SUCCESS

Import Type : OBJECT

Search Pattern :

```
135.114.106.7,Srv1,Site1,,Server
135.114.106.8,WrkStn2,Site2,,Workstation
```

9 In the Import Result window, you can do the following:

- To search for a text string in the report, type the string in the **Search Pattern** field, then press **Enter**. To find the same string again, press **Enter** again.
- To copy the report to a directory, click **Disk** at the top left of the window. Select the drive and directory, then click **OK**.
- To print the report, click **Printer**. Select the desired printer, then click **OK**.
- To send the report as an Email message, click **Mailbox**. Fill in the Email address you wish to send the report to, then click **OK**.

Note: Backup VitalQIP's database immediately after importing a large file. Refer to the *Administrator Reference Manual.*

END OF STEPS

Import data into a MAC address pool

Purpose

You may import data into a MAC address pool that manages by a particular DHCP server or belongs to a particular subnet with the GUI.

The import format for MAC Pool addresses is 12 or 16 hexadecimal characters. Colons may be used to separate each pair of hexadecimal characters (for example, 11:22:33:44:55:66), but are not required. Wildcards are supported at the end of a MAC Address (for example, a1b23d*).

Before you begin

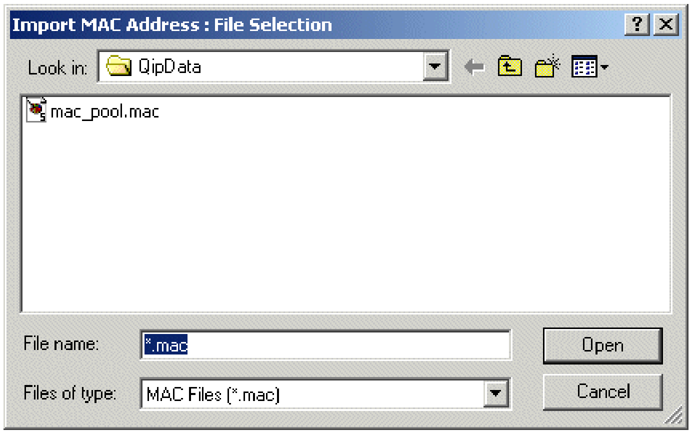
- If you need to import the excluded MAC Pool addresses, add “exclude” at the end of the import string; for example:

  ```
  11:22:33:44:55:66: exclude
  123123123123 exclude
  ```
- The number of digits used depends upon whether the **Allow 16 Character MAC Address** global policy value is set to True (16) or False (12).
- The **Hardware Type** is prepended as the first two characters after the import.

Procedure

To import data into a MAC address pool, follow these steps:

1 Click **Import o**n the VitalQIP main menu, and select **MAC Address Pool** from the **Import** menu. The File Selection window opens.

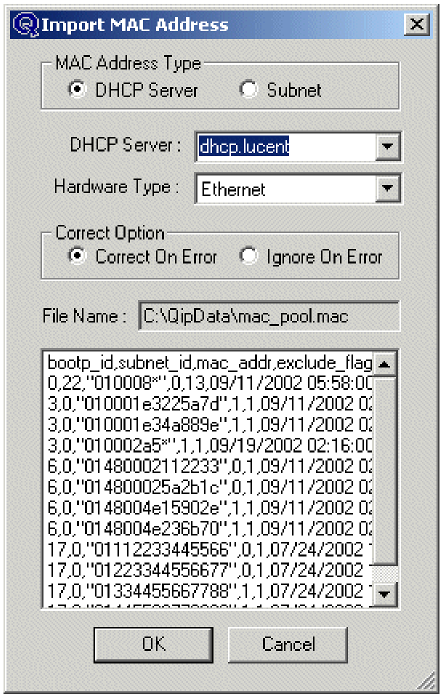


File name: *.mac

Files of type: MAC Files (*.mac)

2 Select the drive, directory and file that you wish to import.

3 Click **OK**. The Import MAC Address window opens.



Import MAC Address

MAC Address Type: ● DHCP Server ○ Subnet

DHCP Server : dhcp.lucent

Hardware Type : Ethernet

Correct Option: ● Correct On Error ○ Ignore On Error

File Name : C:\QipData\mac_pool.mac

```
bootp_id,subnet_id,mac_addr,exclude_flag
0,22,"010008*",0,13,09/11/2002 05:58:0
3,0,"010001e3225a7d",1,1,09/11/2002 0
3,0,"010001e34a889e",1,1,09/11/2002 0
3,0,"010002a5*",1,1,09/19/2002 02:16:0
6,0,"01480002112233",0,1,09/11/2002 0
6,0,"014800025a2b1c",0,1,09/11/2002 0
6,0,"0148004e15902e",1,1,09/11/2002 0
6,0,"0148004e236b70",1,1,09/11/2002 0
17,0,"01112233445566",0,1,07/24/2002
17,0,"01223344556677",0,1,07/24/2002
17,0,"01334455667788",1,1,07/24/2002
```

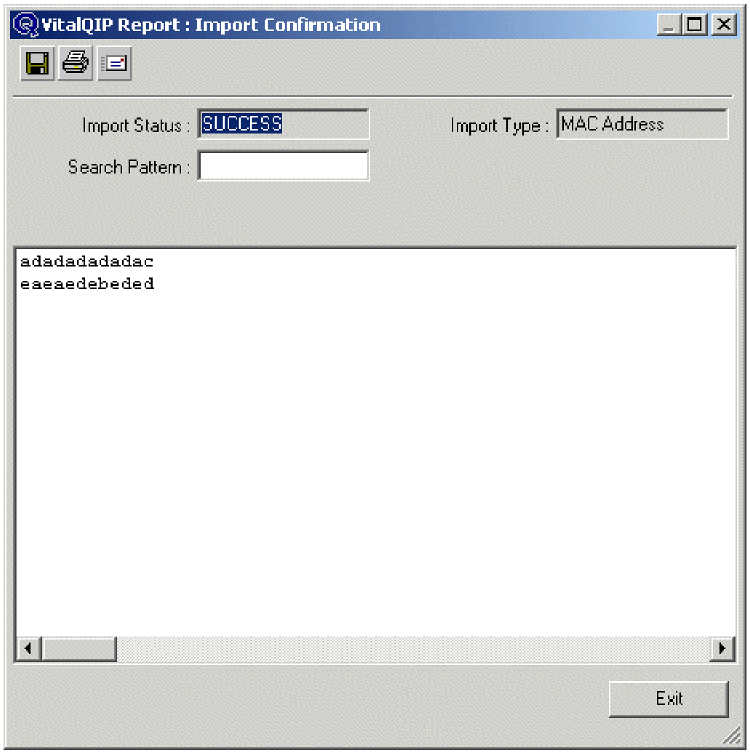
4 Select **DHCP Server** or **Subnet**.

5 Select a DHCP server or subnet from the drop down list.

6 Select **Correct on Error** or **Ignore on Error**:

- **Correct on Error**: If an error is encountered in the input file, the import will be suspended to allow you to correct the error, and then continue the import.
- **Ignore on Error**: If an error is encountered in the input file, the error will be logged for you to review at the end of the import.

7 Click **OK** to start the import.



Import Status : SUCCESS

Import Type : MAC Address

Search Pattern :

```
adadadadadac
eaeaedebeded
```

8 When the Import Result window opens, you can do the following in it:

- To search for a text string in the report, type the string in the **Search Pattern** field and press **Enter**. To find the same string again, press **Enter** again.
- To copy the report to a directory, click **Disk** at the top left of the window. Select the drive and directory and click **OK**.
- To print the report, click **Printer**. Select the desired printer and click **OK**.
- To send the report as an Email message, click **Mailbox**. Fill in the Email address you wish to send the report to and click **OK**.

Note: Backup the VitalQIP database immediately after you import a large file. Refer the *Administrator Reference Manual*.

END OF STEPS

A Application default file for Motif client

Overview

Purpose

The VitalQIP Motif Client default file, *QIPManage.ad*, is provided with VitalQIP. This file is the application default file for the VitalQIP client on UNIX. The application defaults file defines the default resources that control the appearance and behavior of VitalQIP, such as fonts, colors, and window sizes. Most resources are standard resources available for all X/Motif applications. However, there are some VitalQIP application-specific resources, which are discussed in this appendix.

Contents

The following topics are covered:

Application Specific Resources	A-2
Sample QIPManage.ad	A-5
ip-manage command line options	A-16

Application Specific Resources

The VitalQIP Motif client can function without an app-defaults file. However, if you want to make modifications to resources that affect all instances of VitalQIP on a given system, you need to copy *QIPManage.ad* to your systems app-defaults directory and remove the ".ad" filename extension. The location of the app-defaults directory is typically */usr/lib/X11/app-defaults*. Consult your operating system documentation for verification.

After you have copied the file to the proper location, you can edit it to suit your needs. Individual users can also incorporate VitalQIP Motif client resources in their own .*Xdefaults* files or local app-defaults directory to provide per user customization of the application. Please consult the X11(1) man page, or your system's X11 documentation, for instructions on how to do this.

The VitalQIP client on UNIX provides custom resources beyond the standard X/Motif resources that effect the application's behavior. The following table describes each resource.

Table A-1 Description of resources

Resource	Description
QIPManage.confirmExit:True	Determines whether VitalQIP requests confirmation when trying to exit the application. Set it to "True" to indicate confirmation, or set to "False" for no confirmation. The default value is "True".
QIPManage.dataServer: SERVERNAME	Indicates the default server selected in the login screen. The default value is the value of the **QIPDATASERVER** environment variable.
QIPManage.debug:False	Indicates whether to enable debugging. The default is "False".
QIPManage.debugFile: /pathname/of/debug/log/file	Indicates the filename of the debug log if debugging is on. The default value is *$QIPHOME/QIPManage.log*. Environment variable references are not supported in value.

Resource	Description
QIPManage.debugLevel:All	Indicates the level of debugging. The value is a space-separated list of flag words signifying what messages should be logged during debugging. Refer to the *Administrator Reference Manual* for more information on debugging levels. The default value is “All”.
QIPManage.defaultOrganization:ORGNAME	Indicates the default organization selection for master administrators. The default value is the value of the **QIPDEFAULTORG** environment variable.
QIPManage.prefFile:/user/home/path/.qiprc	Indicates the pathname of the user’s local preference file. The default is *$HOME/.qiprc*. Environment variable references are not supported for this value.
QIPManage.helpDir:/full/path/to/help/directory	Indicates the location of online help files. The default is *$QIPHOME/help*. Environment variable references are not supported for this value.
QIPManage.helpExe:/full/path/to/ip-help	Indicates the pathname of the online help executable. The default is *$QIPHOME/usr/bin/ip-help*. Environment variable references are not supported for this value.
QIPManage.helpTocFile:helpcontents1.htm	Indicates the online help table of contents file relative to helpDir. The default is “helpcontents1.htm”.
QIPManage.printCommand:lpr	Indicates the print command for your system. The default is “lpr” for Solaris. The command listed should be able to take data from standard input or as a filename argument.
QIPManage.printerOption:-P	Indicates the option for **printCommand** for specifying the destination printer. The default is **-P** for Solaris.

Resource	Description
QIPManage.multiQuickView:True	Indicates whether a new Subnet Quick View window is created each time it is invoked for a subnet. If this flag is “False”, only one Subnet Quick View window exists at any time. The window is reset when activated for a different subnet. Single window mode is useful when doing subnet browsing. The default is “True”: popup a new window for each subnet.
QIPManage.quickViewRows:16 QIPManage.quickViewColumns:16	Indicates the number of rows and columns for the Subnet Quick View window. The default value is “16” for each resource.
QIPManage.quickViewColWidth:20	Indicates the width, in pixels, of each cell in the Subnet Quick View window. The default is “16”.
QIPManage.quickViewShowLabels:False	Indicates whether text labels are shown for objects in Subnet Quick View grid along with the colors. The default is “False”: do not show the labels.
QIPManage.sendmailExe:/usr/lib/sendmail -t	Specifies the “Sendmail” mail command. To avoid PATH problems, the value should be a full pathname. The command given must be able to take an RFC 822 compliant message as standard input and determine who the Recipients are by the To: and Cc: fields of the message. The default value is “**`/usr/lib/sendmail -t`**”.
QIPManage.toolTipsEnabled:True	Flag if tool tips are enabled. The default is “True”.

Sample QIPManage.ad

As a reference, the following is a sample *QIPManage.ad* file; refer to the *QIPManage.ad* installed with VitalQIP for the latest contents. Lines starting with an explanation point (!) are comments. For detailed information on the syntax of X11 resource files, consult your system's X11 documentation.

```
! #######################################################################
!# QIPManage.ad -- app-defaults file for VitalQIP 6.0
!#
!# Copyright (C) 1993 - 2001, Lucent Technologies Inc.
!#
!#######################################################################
!#######################################################################
!# To use this file, copy it to the app-defaults directory of your
!# system and remove the ".ad" extension.
!# For individual settings, resource can be included in individual
!# .Xdefaults files or app-defaults directory.
!#######################################################################
!#######################################################################
!#Application Specific Resources
!#######################################################################
!#Note: Some application resource have command-line option
!#equivalents.  If a command-line option is specified, it will
!#always take precedence.
!#######################################################################
!QIPManage.confirmExit:True
!#Should VitalQIP ask for confirmation when application exit activated.
!#Default is True.

!QIPManage.dataServer:  SERVERNAME
!#Default server selection in the login screen.  The default
!#value is the value of the QIPDATASERVER environment variable.

!QIPManage.debug:False
!#Should debugging be enabled.  The default is False.

!QIPManage.debugFile:/pathname/of/debug/log/file
!#Filename of debug log if debugging is on.  The default value
!#is "$HOME/QIPManage.log"
!#(note, variable references are not supported in value).

!QIPManage.debugLevel:All
!#The level of debugging.  The value is a space separated list
!#of flag words signifing what messages should be logged during
```

```
!#debugging.  See Chapter 2 of the Administrator Reference Manual for
!#more information on debugging levels.
!#The default value is "All".

!QIPManage.defaultOrganization:ORGNAME
!#Default organization selection for master administrators.
!#The default value is the value of the QIPDEFAULTORG
!#environment variable.

!QIPManage.helpDir:/full/path/to/help
!# Directory contain online help.  Default is "$QIPHOME/help"
!#(note, variable references are not supported in value).

!QIPManage.helpExe:/full/path/to/ip-help
!# Directory contain online help.
!#Default is "$QIPHOME/usr/bin/ip-help"
!#(note, variable references are not supported in value).

!QIPManage.helpTocFile:helpcontents1.htm
!#Help file containing the table of contents.  Interpreted
!#relative to helpDir.
!#Default is "helpcontents1.htm".

!QIPManage.prefFile:/user/home/path/.qiprc
!# Pathname to user's preference file.  Default is "$HOME/.qiprc"
!#(note, variable references are not supported in value).

!QIPManage.printCommand: lpr
!#Print command.  Default is "lpr" for Sun and "lp" for HPUX and AIX.
!#Command listed should be able to take data from standard input or
!#as a filename argument.

!QIPManage.printerOption:-P
!#Print command options for specifying destination printer.  Default
!#is "-P" for Sun and "-d" for HPUX and AIX.

!QIPManage.multiQuickView:True
!#Flag if a new Quick View window is created each time it is
!#in invoked.  If the flag is False, only one Quick View window
!#will exist for each data type at any time, and it will be reset
!#when activated for a different item of the same type. Single
!#window mode is useful when doing browsing. The default is to
!#popup a new window.

!QIPManage.quickViewRows:16
```

```
!QIPManage.quickViewColumns:16
!#Size of the Quick View grid.

!QIPManage.quickViewColWidth:20
!#Width of each column (in pixels).  Note, height of each row
!#is controled by the fontList setting of the grid.

!QIPManage.quickViewShowLabels:False
!#Flag is text labels are shown in cells.  The default is to
!#not show labels.

!QIPManage.sendmailExe:  /usr/lib/sendmail -t
!#Sendmail mail command.  The value should be a full pathname to
!#avoid PATH problems.  Command given must be able to take an
!#RFC822 compliant message as standard input and determine
!#receipients by the To: and Cc: fields of the message.
!#The default value is "/usr/lib/sendmail -t".

!QIPManage.toolTipsEnabled:True
!#Flag if tool tips are enabled.  Default is True.
!#####################################################################
!#General Appearance Resources
!#####################################################################
QIPManage*fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*background: #BFBFBF
QIPManage*foreground: #000000

QIPManage*XmText.background: #FDF5E6
QIPManage*XmTextField.background: #FDF5E6
QIPManage*XmText.fontList: \
    -adobe-courier-medium-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*XmTextField.fontList: \
    -adobe-courier-medium-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*XmToggleButton.selectColor: #FFFF00
QIPManage*XmToggleButtonGadget.selectColor: #FFFF00

!#####################################################################
!#Window/widget Specific Resources
!#####################################################################

!#Login screen
QIPManage*qip-login*XmText.background: #BFBFBF
QIPManage*qip-login*XmTextField.background: #BFBFBF
QIPManage*qip-login*XmComboBox.background: #BFBFBF
```

```
QIPManage*qip-login*fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1

!#Organization Profile
QIPManage*organization_profile*organization_form.width: 400
QIPManage*organization_profile*organization_form.height: 300

!#Object Search Form
QIPManage*QXObjSearchForm*searchHelpLabel.fontList: 6x9

!#Results (text) Window
QIPManage*QXResultsDialog*text.columns: 72
QIPManage*QXResultsDialog*text.rows: 12

!#Free Subnet Window
QIPManage*QXFreeSubnetDialog*messageBox.width: 520
QIPManage*QXFreeSubnetDialog*messageBox.height: 370
QIPManage*QXFreeSubnetDialog*networkSelTextF.background: #BFBFBF
QIPManage*QXFreeSubnetDialog*networkSelTextF.fontList: \
    -adobe-courier-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXFreeSubnetDialog*XmLGrid*background: #BFBFBF

!#Object List Report Window
QIPManage*QXReportObjListDialog*XmLGrid.background: #BFBFBF
QIPManage*QXReportObjListDialog*messageBox.width: 450
QIPManage*QXReportObjListDialog*messageBox.height: 500

!#User-defined Hierarchy Add Node Window
QIPManage*QXUDNodeAddDialog*messageBox.width: 350
QIPManage*QXUDNodeAddDialog*messageBox.height: 450
QIPManage*QXUDNodeAddDialog*XmLGrid.selectionPolicy: SELECT_MULTIPLE_ROW
QIPManage*QXUDNodeAddDialog*XmLGrid.background: #BFBFBF
QIPManage*QXUDNodeAddDialog*XmLGrid.visibleItemCount: 8
QIPManage*QXUDNodeAddDialog*XmList.selectionPolicy: EXTENDED_SELECT
QIPManage*QXUDNodeAddDialog*curNodeTextF.background: #BFBFBF
QIPManage*QXUDNodeAddDialog*XmTextField.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1

!#Object Management Subnet Selection Window
QIPManage*QXObjManSubnetsDialog.messageBox.width: 600
QIPManage*QXObjManSubnetsDialog.messageBox.height: 425
QIPManage*QXObjManSubnetsDialog*statusLabel.fontList: \
    -adobe-helvetica-medium-r-normal--10-*-*-*-*-*-iso8859-1

!#Object Management Object List Window
```

```
QIPManage*QXObjManObjsDialog.messageBox.width: 600
QIPManage*QXObjManObjsDialog.messageBox.height: 425
QIPManage*QXObjManObjsDialog*statusLabel.fontList: \
    -adobe-helvetica-medium-r-normal--10-*-*-*-*-*-iso8859-1

!#object Management Windows
QIPManage*DynAllocAddShell.XmMessageBox.width: 240
QIPManage*DynAllocAddShell.XmMessageBox.height: 300

!#Quick View
QIPManage*QXQuickViewDialog.XmMessageBox.fontList: \
    -adobe-helvetica-bold-r-normal--10-*-*-*-*-*-iso8859-1
QIPManage*QXQuickViewDialog.XmMessageBox.XmForm.XmLGrid.fontList: \
    -adobe-helvetica-medium-r-normal--8-*-*-*-*-*-iso8859-1
QIPManage*QXQuickViewDialog.XmMessageBox.XmForm.titleLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXQuickViewDialog.XmMessageBox.XmForm.XmFrame*fontList: \
    -adobe-helvetica-bold-r-normal--10-*-*-*-*-*-iso8859-1
QIPManage*QXQuickViewDialog.XmMessageBox.XmForm.XmTextField.fontList: \
    -adobe-helvetica-bold-r-normal--10-*-*-*-*-*-iso8859-1
QIPManage*QXQuickViewDialog.XmMessageBox.XmForm.addrTF.columns: 13
QIPManage*QXQuickViewDialog.XmMessageBox.XmForm.statusTF.columns: 12
QIPManage*QXQuickViewDialog.XmMessageBox.XmForm.XmTextField.background:
   #BFBFBF

!#Ping/reclaim Progress Window(s)
QIPManage*pingProgress.width: 350
QIPManage*pingProgress.height: 20
QIPManage*reclaimProgress.width: 350
QIPManage*reclaimProgress.height: 20

!#Reclaim Windows
QIPManage*QXReclaimSubnetSelDialog.messageBox.width: 500
QIPManage*QXReclaimSubnetSelDialog.messageBox.height: 400
QIPManage*QXReclaimObjsDialog.messageBox.width: 715
QIPManage*QXReclaimObjsDialog.messageBox.height: 400
QIPManage*QXReclaimSchedDialog.messageBox2.width: 500
QIPManage*QXReclaimSchedDialog.messageBox2.height: 500

!#Goto/Search By ... Window
QIPManage*QXGotoByDialog.messageBox.width: 450
QIPManage*QXGotoByDialog.messageBox.height: 380

!#Goto/Search Results Window
QIPManage*QXGotoResultsDialog.messageBox.width: 500
```

```
QIPManage*QXGotoResultsDialog.messageBox.height: 460
QIPManage*QXGotoResultsDialog*quickLstGrid.height: 200

!#Network Services File Generation Windows
QIPManage*QXDHCPGenDialog.messageBox.width: 340
QIPManage*QXDHCPGenDialog.messageBox.height: 370
QIPManage*QXDnsGenPriDialog.messageBox.width: 340
QIPManage*QXDnsGenPriDialog.messageBox.height: 420
QIPManage*QXBootpGenDialog.messageBox.width: 340
QIPManage*QXBootpGenDialog.messageBox.height: 370
QIPManage*QXNisGenDialog.messageBox.width: 340
QIPManage*QXNisGenDialog.messageBox.height: 370

!#View Active Leases Subnet Selection Window
QIPManage*QXViewActiveSubnetSelDialog.messageBox.XmForm*XmTextField.backgrou
   nd: \
     #BFBFBF

!#View Active Leases Window
QIPManage*QXViewActiveDialog*messageBox.width: 600
QIPManage*QXViewActiveDialog*messageBox.height: 475
QIPManage*QXViewActiveDialog*messageBox.XmForm*XmTextField.background:
   #BFBFBF
QIPManage*QXViewActiveDialog*messageBox*srvNameTF.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXViewActiveDialog*messageBox*subnetTF.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXViewActiveDialog*messageBox*leaseGrid.leaseFontList: \
    -adobe-courier-medium-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXViewActiveDialog*statusLabel.fontList: \
    -adobe-helvetica-medium-r-normal--10-*-*-*-*-*-iso8859-1

!#Toolbar Edit Window
QIPManage*QXToolbarEditDialog.messageBox.width: 600
QIPManage*QXToolbarEditDialog.messageBox.height: 375

!#Infrastructure Item Selection Window
QIPManage*domainp_option.messageBox.width: 395
QIPManage*domainp_option.messageBox.height: 300

!#Network Profile Windows
QIPManage*NetworkProShell.messageBox.width: 770
QIPManage*NetworkProShell.messageBox.height: 500

!#OSPF Profile Windows
```

```
QIPManage*OSPFProShell.ospf_message_box.width: 722
QIPManage*OSPFProShell.ospf_message_box.height: 600

QIPManage*subnetprogress.width: 350
QIPManage*subnetprogress.height: 20

!# Zone Option Windows
QIPManage*ZoneOptionShell.XmMessageBox.width: 700
QIPManage*ZoneOptionShell.XmMessageBox.height: 400

!# Subnet Profile Windows
QIPManage*SubnetDNSShell.XmMessageBox.width: 440
QIPManage*SubnetDNSShell.XmMessageBox.height: 250
QIPManage*SubnetTservShell.XmMessageBox.width: 440
QIPManage*SubnetTservShell.XmMessageBox.height: 250

!# Hierarchy Legend Window
QIPManage*QXHierLegendDialog*XmRowColumn*XmLabel.fontList: \
    -adobe-helvetica-medium-r-normal--12-*-*-*-*-*-iso8859-1

!# Technical Support Dialog
QIPManage*QXTechSupportDialog*appLabel.fontList: \
    -adobe-helvetica-bold-r-normal--14-*-*-*-*-*-iso8859-1
QIPManage*QXTechSupportDialog*XmFrame*XmLabel.fontList: \
    -adobe-helvetica-medium-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXTechSupportDialog*XmFrame*usLocLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXTechSupportDialog*XmFrame*euroLocLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXTechSupportDialog*XmFrame*wwwLocLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1

!# About Dialog
QIPManage*QXAboutDialog*XmLabel.fontList: \
    -adobe-helvetica-medium-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXAboutDialog*appLabel.fontList: \
    -adobe-helvetica-bold-r-normal--14-*-*-*-*-*-iso8859-1
QIPManage*QXAboutDialog*copyLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXAboutDialog*numActObjsValLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXAboutDialog*licMaxObjsValLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXAboutDialog*entSrvDateValLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
```

```
QIPManage*QXAboutDialog*licExpDateValLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXAboutDialog*licNumValLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXAboutDialog*serNumValLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXAboutDialog*entSrvIDValLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1
QIPManage*QXAboutDialog*unameValLabel.fontList: \
    -adobe-helvetica-bold-r-normal--12-*-*-*-*-*-iso8859-1

!#Subnet Move Window
QIPManage*ObjSubnetMoveShell*ObjSubnetMoveMbox.width: 580
QIPManage*ObjSubnetMoveShell*ObjSubnetMoveMbox.height: 450
QIPManage*ObjSubnetMoveShell*XmForm.resizePolicy: RESIZE_NONE
QIPManage*ObjSubnetMoveShell*XmLGrid.verticalSizePolicy: CONSTANT
QIPManage*ObjSubnetMoveShell*XmLGrid.horizontalSizePolicy: CONSTANT

!#Object Move Window
QIPManage*ObjManMoveShell.XmMessageBox.width: 500
QIPManage*ObjManMoveShell.XmMessageBox.height: 570
QIPManage*ObjectMoveShell.XmMessageBox.width: 385
QIPManage*ObjectMoveShell.XmMessageBox.height: 430

!#Naming Policies Window
QIPManage*NamingPolicyShell.NamingPolicyMbox.width: 405
QIPManage*NamingPolicyShell.NamingPolicyMbox.height: 340

!#Manufacture Policies Windows
QIPManage*man_prof_bootp.XmMessageBox.width: 580
QIPManage*man_prof_bootp.XmMessageBox.height: 395
QIPManage*Man_mod_tag.XmMessageBox.width: 575
QIPManage*Man_mod_tag.XmMessageBox.height: 300
QIPManage*manuf_pro.XmMessageBox.width: 415
QIPManage*manuf_pro.XmMessageBox.height: 275

!#Domain Profile windows
QIPManage*DomainProShell.XmMessageBox.width: 720
QIPManage*DomainProShell.XmMessageBox.height: 460

!#Reverse Zone windows
QIPManage*ReverseZonePro.XmMessageBox.width: 630
QIPManage*ReverseZonePro.XmMessageBox.height: 370
QIPManage*RzoneProShell.XmMessageBox.width: 700
QIPManage*RzoneProShell.XmMessageBox.height: 400
```

```
QIPManage*Calc_zone.XmMessageBox.width: 450
QIPManage*Calc_zone.XmMessageBox.height: 460
QIPManage*rzonep_option.XmMessageBox.width: 415
QIPManage*rzonep_option.XmMessageBox.height: 260

!# Subnet Organization window
QIPManage*subnetp_shell.XmMessageBox.width: 530
QIPManage*subnetp_shell.XmMessageBox.height: 370

!# User Groups window
QIPManage*UserGrpProShell.XmMessageBox.width: 640
QIPManage*UserGrpProShell.XmMessageBox.height: 460

!# DHCP Template windows
QIPManage*DhcpTempShell.XmMessageBox.width: 750
QIPManage*DhcpTempShell.XmMessageBox.height: 580
QIPManage*DhcpParamListShell.XmMessageBox.width: 500
QIPManage*DhcpParamListShell.XmMessageBox.height: 250
QIPManage*DhcpTClassShell.XmMessageBox.width: 300
QIPManage*DhcpTClassShell.XmMessageBox.height: 250

!# Import windows
QIPManage*ImportDomainShell.XmMessageBox.width: 600
QIPManage*ImportDomainShell.XmMessageBox.height: 575
QIPManage*ImportObjectShell.XmMessageBox.width: 600
QIPManage*ImportObjectShell.XmMessageBox.height: 575
QIPManage*ImportMACShell.XmMessageBox.width: 600
QIPManage*ImportMACShell.XmMessageBox.height: 575
QIPManage*importprogress.width: 400
QIPManage*importprogress.height: 20

!# MAC Pool windows
QIPManage*MacpoolShell.XmMessageBox.width: 450
QIPManage*MacpoolShell.XmMessageBox.height: 300
QIPManage*MacpoolModShell.XmMessageBox.width: 480
QIPManage*MacpoolModShell.XmMessageBox.height: 270

!# Domain Folder Selection dialogs
QIPManage*DomainFolderSelectShell.XmMessageBox.width: 260
QIPManage*DomainFolderSelectShell.XmMessageBox.height: 300

!# Error dialogs
QIPManage*error_popup*background: #BFBFBF
QIPManage*error_popup*foreground: #000000
QIPManage*warning_popup*background: #BFBFBF
```

```
QIPManage*warning_popup*foreground: #000000
QIPManage*information_popup*background: #BFBFBF
QIPManage*information_popup*foreground: #000000

!#Tooltip Resources
QIPManage*tooltip*background: #FDF5E6
QIPManage*tooltip*fontList: \
    -adobe-helvetica-medium-r-normal--10-*-*-*-*-*-iso8859-1

!#DB object List
QIPManage*nameIdList.visibleItemCount: 8

!#Date Input
QIPManage*dateInput.hintLabel.fontList: 6x9

!#######################################################################
!#Help Window
!#######################################################################
QIPManage*QXHelpWindow.geometry: 550x575-100+100

QIPManage*XmHTML.fontFamily:  adobe-helvetica-normal-*
QIPManage*XmHTML.fontFamilyFixed: adobe-courier-normal-*
QIPManage*XmHTML.anchorButtons:   False
QIPManage*XmHTML.maxImageColors:   64
QIPManage*XmHTML.imageRGBConversion:  QUICK
!#######################################################################
!#Text Widget Translations
!#######################################################################
!#Define text widget translation to give Unix/emacs like editing
!#capabilities.
QIPManage*XmTextField.translations:  #override \
                !Ctrl<Key>a:    beginning-of-line() \n\
                !Ctrl<Key>b:    backward-character() \n\
                !Ctrl<Key>d:    delete-next-character() \n\
                !Ctrl<Key>e:    end-of-line() \n\
                !Ctrl<Key>f:    forward-character() \n\
                !Ctrl<Key>h:    delete-previous-character() \n\
                !Ctrl<Key>k:    delete-to-end-of-line() \n\
                !Ctrl<Key>u:    select-all()delete-selection()\n\
                !Ctrl<Key>w:    delete-previous-word() \n\
                !Meta<Key>b:    backward-word() \n\
                !Meta<Key>d:    delete-next-word() \n\
                !Meta<Key>f:    forward-word() \n\
                !Meta<Key>h:    delete-previous-word()
QIPManage*XmText.translations:       #override \
!Ctrl<Key>a:    beginning-of-line() \n\
!Ctrl<Key>b:    backward-character() \n\
!Ctrl<Key>d:    delete-next-character() \n\
!Ctrl<Key>e:    end-of-line() \n\
!Ctrl<Key>f:    forward-character() \n\
!Ctrl<Key>h:    delete-previous-character() \n\
!Ctrl<Key>k:    kill-to-end-of-line() \n\
!Ctrl<Key>l:    redraw-display() \n\
!Ctrl<Key>r:    redraw-display() \n\
!Ctrl<Key>u:    beginning-of-line()kill-to-end-of-line()\n\
!Ctrl<Key>v:    next-page() \n\
!Ctrl<Key>w:    delete-previous-word() \n\
!Ctrl<Key>y:    unkill() \n\
!Meta<Key>b:    backward-word() \n\
!Meta<Key>d:    kill-next-word() \n\
!Meta<Key>f:    forward-word() \n\
!Meta<Key>h:    kill-previous-word() \n\
!Meta<Key>v:    previous-page()
```

ip-manage command line options

describes the command line options available (along with the standard X11 Toolkit options) when you run **ip-manage**, the VitalQIP interface.

> **Note:** You must run **ip-manage** with the command shell's **$DISPLAY** variable set, as shown in this example:

```
DISPLAY=<ipaddr>:0.0
export DISPLAY
```

Table A-2 Options for ip-manage

Option	Description
-d or **--debug**	Turn on debugging.
-h or **--help**	Print this message.
-l or **--debug-level** <*level_list*>	Debugging level.
-f or **--debug-file** <*filename*>	Debug log filename.
-s or **--server** <*server*>	Name of enterprise server.
-v or **--version**	Print version information.
-q or **--login-serve**	Name of login server.

Index

71955
MT1 Map1st
Control debug levels for Lucent DHCP servers, 8-10

A
A (Host IPv4) type field, 5-23
AAAA (Host IPv6) type field, 5-24
AbusiveClientLockout server policy, 2-71
AbusiveClientMonitorPeriod server policy, 2-71
AbusiveClientWarningCount server policy, 2-71
Accept Client Names, 4-13
Accept Client Names parameter, 4-20, 4-35
Access Control Enabled server policy, 2-72
Access Control List, 3-3
Access Control server policy, 2-72
access list
create, 6-23
Access Node Management privilege, 6-19
Access V6 Address Management privilege, 6-18
AckLDRMCallout, 2-77
AckRenewForUnusedAddress server policy, 2-73
ACL template
create, 3-4
delete, 3-9
modify, 3-8
ACL Templates
select, 4-74, 5-49, 5-86
ACL. See Access Control List
Activation Status field, 6-48
Active Directory, 4-66
Active Directory Domain Name parameter, 4-66
Active Directory Domain parameter, 4-57
Active Directory Server parameter, 4-34
Active Lease information location, 4-14
Active Leases
delete, 8-44
modify report, 8-43
view Relay Agent Information, 8-43
view report, 8-40
active leases
generate, 8-41
ActiveLeaseExpiration server policy, 2-73
Add Child Node
User-Defined Hierarchy, 1-34
Add Folder function, 1-40
Add Root Node
User-Defined Hierarchy, 1-34
Add Sibling Node
User-Defined Hierarchy, 1-34
add values
User-Defined Fields, 5-8
Additional Policies parameter, 4-20, 4-35
Additional Policies policy, 4-11
address
reclaim, 7-97
Address Ranges
define in network, 5-69
Address Ranges tab, 5-69
address reclaim
manual, 7-108
scheduling, 7-98
Address Resolution Protocol, 2-24
address-to-name lookup, 5-71
administrative role
check assignments, 6-9
create, 6-4
delete, 6-8
modify, 6-7
overview, 6-3
Administrative Role report
generate, 9-36
Administrative Role report type, 9-6
administrator
access list, 6-23
assign role, 6-36
assign to address range, 5-70
Network Quick View, 6-31
reverse zone permissions, 5-71
Administrator Audit History report
generate, 9-45
Administrator Audit History report type, 9-7
administrator menus
customize, 6-30

administrator privileges, 6-15

Administrator Profile, 4-70
- Customize tab, 1-36

administrator profile
- Access Information tab, 6-24
- create, 6-13
- Customize tab, 6-30
- delete, 6-35
- modify, 6-33
- overview, 6-11
- privilege parameters, 6-15

Administrator Profile report
- generate, 9-32

Administrator Profile report type, 9-6

Advanced Mode, 1-18

AFSDB (Andrew File System Data Base) type field, 5-24

aging zone option, 5-42

alias
- Inquire report, 9-20
- object alias, 7-34
- Object Name Length policy, 3-41
- search for object, 1-44
- un-allocate dynamically allocated object, 7-77

All Subnets are Local, 2-21

Allocate Blocks privilege, 6-16

allocated IP address
- subnet organization warning, 5-107

Allow 16 Character MAC Address global policy, 7-32

Allow 16 Character MAC Address policy, 3-29

Allow Automatic Reclaim global policy, 7-97

Allow Automatic Reclaim policy, 3-29

Allow DHCP Clients to Modify Dynamic Object Resource Records policy, 3-29, 7-65

Allow Dotted Hostnames policy, 3-30

Allow Duplicate MAC Address global policy, 7-32

Allow Duplicate MAC Addresses policy, 3-30

Allow Recursion parameter, 4-49, 4-55

Allow User Selection parameter, 6-19

Allow User Selection privilege, 7-44

allow-notify zone option, 5-32, 5-38

allow-query zone option, 5-28, 5-32, 5-35, 5-39

Allow-Secondary-Update parameter, 4-53

allow-transfer zone option, 5-29, 5-33, 5-36, 5-39, 5-42

allow-update zone option, 5-29, 5-33, 5-36, 5-40, 5-42

also notify zone option, 5-30, 5-34, 5-37, 5-40

Always Append Router policy, 3-30

application
- add, 5-114
- delete, 5-117
- modify, 5-116
- overview, 5-113

Application and Service Parameters, 2-26

Application field, 7-80
- dynamic objects, 7-69

Application Specific Resources, A-2

ARP Cache Timeout, 2-24

ARP. See Address Resolution Protocol

Asset Number asset field, 7-39

Asset tab, 7-38

assign administrative role, 6-36

Attached DNS Server(s) List, 7-60

audit history report types, 9-6

Authorization Name field, 7-80
- dynamic objects, 7-69

Auto Configuration of Ipv4 Clients, 2-40

Automatic Bootp, 7-31

Automatic Bootp configuration, 7-67, 7-72

Automatic Bootp Setup fields, 7-73

Automatic DHCP, 7-31

Automatic DHCP configuration, 7-67, 7-72

Automatic DHCP Setup fields, 7-73

Autorelease keyword, 2-88

AUTORETRIES option, 2-38

AUTORETRY_SECS options, 2-38

B

Basic Mode, 1-18

BIND 8.X zone options, 5-28

BIND 9.X zone options, 5-31

BIND configuration file, 8-16

BIND options, 4-41

BIND-9 DNS Server Type, 4-45

boolean data type, 2-8

Boot File Size, 2-17

Boot Method parameter, 4-56

Bootfile Home Directory parameter, 4-17

Bootfile Name, 7-61
- Manual Bootp field, 7-71

Bootfile Name option, 2-36

Bootfile server policy, 2-74

Bootp, 2-45

Bootp Extension, 3-45

Bootp keyword, 2-88

Bootp parameter identifier, 3-45

Bootp server, 4-1, 4-3

Bootp server setup, 4-11

Bootp server type, 4-17

Bootp tag, 3-42

Bootp user exit
- File Generation Service, 8-27
- qipbootpuserexit, 8-26

BootpRequestLDRMCallout, 2-77

Bootptab file
- generate, 8-25

Bootptab File Generation, 8-24

Bootptab Filename parameter, 4-17

bracketed IP address notation, 2-46

Broadcast Address, 2-21

Business Unit ID
- sample object names, 3-16

Business Unit ID field, 3-15

C

calculation
- network warnings, 5-68

Call Management Server, 2-48

canceling functions, 1-11

Change Debug Level, 8-11

change password, 1-7

Change Records B-tree Key Size policy, 3-31

Changed Zones Only option, 8-15

check assignments
- administrative role, 6-9

Check Before Assign field, 5-60

check-names zone option, 5-30, 5-37

CheckTransactionID server policy, 2-74

ciaddr field, 2-88

CIDR, 5-51

CIDR. See Classless Inter-Domain Routing

Class A address, 5-51

Class B address, 5-51

Class C address, 5-51

Class field, 5-22

Class object resource record field, 7-46

Classless Inter-Domain Routing
- address, 5-52
- overview, 5-52

Classless Static Route option, 2-23

Clear Debug Log, 8-12

CLI
- qip-tombstonepurge, 3-26

client
- NDS, 2-37

Client Class, 2-90
- create, 2-91
- delete, 2-95
- modify, 2-94

Client Class parameter, 4-21

Client Identifier option, 2-35

Client Naming Policy, 4-13

ClientHostNameProcessing policy, 2-75, 4-16

CMS FQDN, 2-48

CMS. See Call Management Server

CNAME (Canonical Name) type field, 5-23

Code 255, 2-27

Comma Separated Values format, 9-4

Comments subnet field, 7-11

CompressedLog server policy, 2-75

Configuration & Data generation type, 8-15

configuration file
- copy, 8-5
- email, 8-7
- print, 8-6

configuration files, 4-3, 8-3
- ddns.conf, 4-12
- DHCP server, 4-11
- dhcpd.conf, 4-12
- dhcpd.pcy, 4-12
- DNS, 8-15
- Lucent DHCP Server, 4-11
- VitalQIP creation process, 4-14

contact
- add, 3-52
- delete, 3-52
- modify, 3-52
- profile, 3-51
- search, 3-52
- subnet profile, 7-15

Contact E-mail Address field, 5-56

Contact field, 7-80
- dynamic objects, 7-69

contact information
- subnet profile, 7-15

Contact Search policy, 3-31

contacts
- Go To/Search, 1-42

Cookie Server, 2-16

Coordinated Universal Time, 2-15

Corporate Extension parameter, 4-48, 4-54, 5-28, 5-31

Create "boot" parameter, 4-58

Create "db.127.0.0" parameter, 4-47, 4-53, 4-58

Create "db.cache"/"db.root" parameter, 4-48, 4-53, 4-59

Create "named.conf" parameter, 4-47, 4-53

Create “rndc.conf” parameter, 4-46, 4-51

Create Infrastructure privilege, 6-20

create new toolbar, 1-15

create object class, 3-58

Create Out-of-Zone Glue Records parameter, 4-48, 4-54, 4-59

Create PTR for Reverse Zone check box, 5-25

Create Resource Record privilege, 5-21, 5-83

Create Resource Records parameter, 6-20

Create Resource Records privilege, 6-20, 7-45

Create/Update Administrator parameter, 6-15

Credential Failure, 3-24

CtlReqRetryMax parameter, 4-27

customize toolbar, 1-13

customizing Administrator menus, 6-30

D

Data Collection (Ping) Schedule parameter, 7-102

Data field, 5-23

Data object resource record field, 7-47

Data Type field, 2-8

date and time format, 1-11

Date of Purchase asset field, 7-39

db.cache file extension parameter, 4-48, 4-54, 4-59

DDNS Retry policy, 3-23

DDNS Timeout policy, 3-24

Debug Information parameter, 4-21

debug mode, 4-16

Debug parameter, 4-21

DebugFile parameter, 4-21

Decline keyword, 2-88

DECNet, 7-32, 7-57

DECNet Area field, 7-57

DECNet MAC Address field, 7-57

DECNet Node field, 7-57

DECNet Tab
- fields, 7-57

DECNet tab, 7-57

Default Directory parameter, 4-19, 4-45, 4-51, 4-56, 4-62, 4-64

Default Domain field, 5-60

Default Finger Server, 2-29

Default Internet Relay Chat (IRC) Server, 2-29

Default IP Time-to-Live, 2-20

Default Router subnet field, 7-10

Default TTL field, 5-17, 5-79

Default World Wide Web (WWW) Server, 2-29

DefaultClass server policy, 2-72

DefaultDescentThreshold server policy, 2-75

DefaultLease server policy, 2-76

DefaultUnavailableThreshold server policy, xvi, 2-76

define
- administrative role, 6-4
- DNS server, 4-41
- objects within subnet, 7-26
- server profile, 4-3, 4-4

delete
- administrative role, 6-8
- administrator profile, 6-35
- user group, 6-44

Delete Confirmation Warning parameter, 6-20

Delete Confirmation Warning privilege, 6-20

Delete Folder function, 1-40

Delete keyword, 2-88

Delete Lease policy, 3-32

delete object class, 3-62

Delete Sites/Subnets from Active Directory policy, 3-32, 4-66

Description field, 6-48

Detailed Object Report, 9-24

Device Class, 2-90

Device Subnet field, 7-79
- dynamic objects, 7-68

DHCP, 2-45
- standard templates, 2-52

DHCP configuration file
- generate, 8-9, 8-11

DHCP Configuration File Policies, 2-63, 2-67

DHCP configuration files
- filenames, 8-9

DHCP Extensions options, 2-33

DHCP failover server
- limitations, 4-24
- overview, 4-24

DHCP Generation option, 8-9

DHCP lease, 2-49

DHCP Option 51, 2-49

DHCP Option Template
- Bootptab file support, 2-14
- copy, 2-62
- create, 2-56

delete, 2-61

general, 2-52

microsoft_clients, 2-52

modify, 2-60

multicast, 2-52

pre-defined, 2-14

DHCP Option template
description, 2-49

DHCP option template
enter user-defined values, 2-59

DHCP Option Template field, 7-64, 7-73

DHCP Option Template subnet field, 7-11

DHCP Options
values, 2-14

DHCP Policy Template
create, 2-64

DHCP Policy Templates, 2-63

DHCP push, 8-3

DHCP report
generate, 9-29

DHCP report type, 9-6

DHCP Scope Policy Template field, 7-64, 7-74

DHCP server, 4-1, 4-3
configuration files, 4-11

push logic, 2-59

start, 4-16

stop, 4-16

DHCP Server field, 7-63, 7-73

DHCP Server Hierarchy, 1-28

DHCP Server Name subnet field, 7-11

DHCP Server Policies, 2-63, 2-71

DHCP Server Policies parameter, 4-23

DHCP Server Properties
view, 7-21

DHCP server setup, 4-11

DHCP Subnet Policy Template field, 7-63, 7-73

DHCP Subnet Policy Template subnet field, 7-11

DHCP Template Class
add, 2-5

add new option, 2-7

rename, 2-11

DHCP template class
delete, 2-13

DHCP Template Classes and Options, 2-3
customize classes, 2-4

default, 2-3

DHCP Template Option
delete, 2-13

modify, 2-12

DHCP Template parameter, 4-19, 4-34

DHCP user exit
File Generation Service, 8-14

qipdhcpuserexit, 8-13

qipdhcpuserexitfgs, 8-13

DHCP/Bootp Option Template, 2-45

DHCP/Bootp Template
Class/Option Setup, 2-3

Option Template, 2-3

Policy Template, 2-3

dhcpac.conf, 2-72

dhcpd.pcy file, 2-71

dhcpd.pcy policy file, 4-16

DHCPINFORM messages, 2-76

DHCPRelease message, 4-24

different time zones
subnet move, 7-85

Directory Agent Address, 2-41

Directory Agent Address Sub-Option, 2-41

Directory Agents, 2-41

Disable DNS communication parameter, 4-49, 4-55, 4-60

Disable Recursion parameter, 4-59

DiscoverLDRMCallout, 2-77

Display Columns, 7-21

Display Domain Folders checkbox, 6-31

Display Domain Folders option, 4-4, 4-70, 5-53

Distinguished Name of the User, 4-67

DNS configuration file
generate, 8-19

DNS Configuration Files
Generating, 8-15

DNS Generation, 8-19

DNS push, 8-3

DNS Resource Records, 4-41

DNS resource records
generate, 8-15

DNS Serial Number Query parameter, 4-55, 4-60

DNS Serial Number Query Type parameter, 4-50

DNS server, 4-1, 4-3
define, 4-41

DNS Server Hierarchy
DNS Servers tab, 1-30

keyed icon, 1-31

DNS SOA Serial Number Type policy, xvi, 3-31

DNS Update Service, 4-13

DNS user exit
qipdnscnfuserexit, 8-22

qipprednsuserexit, 8-22

DNS Zone report
generate, 9-39

DNS Zone report type, 9-6

dnscmd, 8-15, 8-16

dnscmd utility, 5-43

DNSUpdateObject message route, 3-28

domain
- create profile, 5-13
- define Primary/Secondary Servers, 5-18
- delete, 5-46
- folders, 5-11
- hierarchical tree, 5-53
- modify profile, 5-45
- overview, 5-11
- profile fields, 5-17
- Resource Records, 5-21
- user-defined fields, 5-44
- Zone Options tab, 5-26

Domain Expire Time field, 5-17

Domain Folders, 1-40

Domain Name field, 7-79
- dynamic objects, 7-68

Domain Name object field, 7-31

Domain Name option, 2-17, 2-53, 2-54

Domain Name Server option, 2-16, 2-53, 2-54

Domain Name subnet field, 7-10

Domain Refresh Time field, 5-17

Domain Retry Time field, 5-17

Domain Search Option, 2-44

domains
- change DNS options on multiple, 5-47
- import data, 10-3

Domains field, 5-60

DropAllDhcpInformPackets server policy, 2-76

DropZeroMacAddressPackets server policy, 2-76

Dual Protocol object field, 7-32

dynamic adress allocation, 7-67

dynamic allocation configuration methods, 7-67

Dynamic Allocation fields, 7-68

Dynamic Configuration
- Manual Bootp tab, 7-60

dynamic configuration, 7-31

Dynamic Configuration field, 7-68

Dynamic Configuration object field, 7-31

Dynamic Configuration tab, 7-31, 7-62
- fields, 7-63

Dynamic DHCP, 7-31

Dynamic DHCP configuration, 7-67

Dynamic DNS Mask, 7-33

Dynamic DNS Mask policy, 3-24

Dynamic DNS Policy, 3-23

Dynamic DNS Updates field
- dynamic objects, 7-70

Dynamic DNS Updates object field, 7-33

Dynamic Object Allocation subnet field, 7-12

Dynamic/Static configuration, 7-67

dynamically allocated IP address
- modify, 7-75

dynamically allocated object
- un-allocating, 7-77

dynamically allocated objects
- naming, 3-17

E

email address
- rules for entering, 4-10

E-mail Address field, 6-48

Email address for local and reverse zones parameter, 4-45, 4-51, 4-56

email addresses
- format rules, 4-10

Enable LDRM Interface server parameter, 2-76

enable-subnet-selection-option policy, 2-68

End Address field, 5-69, 5-96

entering dates and times, 1-11

environment variable
- $QIP_DO_KINIT, 3-25
- $QIP_KEYTAB_PATH, 3-25
- $QIP_PRINCIPAL_NAME, 3-25
- $QIPMESSAGESERVICE, 3-28
- IP_USE_DNS_UPDATE_SVC, 3-28
- QIPDATASERVER, 1-4

Ethernet Encapsulation, 2-24

excluded-user-classes policy, 2-70

excluded-vendor-classes policy, 2-69

Existing Address Ranges list, 5-69

Existing DNS Servers List, 7-60

Existing Reverse Zones field, 4-71

Existing Routers list, 7-49

Existing Zone List field, 4-70

exit VitalQIP, 1-10

Expiration Date field, 7-80

Expiration keyword, 2-88

ExpireAllLeasesOnRestart server policy, 2-73, 2-78

Explicitly Create Blocks privilege, 6-17

Extensions Path, 2-18

F

Failover DHCP Server, 4-30

failover DHCP server
- configure, 4-30

failover parameters
- primary DHCP server, 4-27
- Secondary DHCP Server, 4-30

Failover Server Type parameter, 4-22

Failover/Secondary parameter, 4-22

FGS See File Generation Service

file format
- Network Information Service, 4-44

File Generation Service, 4-3

File|Administrator Password
- Changing, 1-7

File|Exit, 1-10

First Name field, 6-47

FirstIn-LastIn global policy, 4-13

FirstIn-LastIn policy, 3-32

Folder maintenance functions, 1-40

Folder management
- rules, 1-41

ForceClass server policy, 2-78

ForcedVendorClass policy, 7-73

format
- email address, 4-10

Free Blocks privilege, 6-17

Free Subnet report
- generate, 9-26

Free Subnet report type, 9-6

G

GAP, 5-101

Gap Direction policy, 3-33

GAP. See Global Allocation Policy

General tab, 7-40

general Template, 2-53

general Template Options, 2-53

Generate DNS Records for Dynamic Clients policy, 3-33

Generate Simple Unique Name, 3-34

generated DHCP configuration files, 8-9

Generating
- DNS Configuration and Data Files, 8-15
- DNS Resource Records, 8-15

Global Allocation Policy, 5-101, 5-105
- overview, 5-105

global MAC address pool
- modify, 4-37, 4-38

Global MAC Address Pools, 7-112

Global Policies, 3-21

global policies
- create, 3-22
- dynamic DNS, 3-23
- report policy, 3-41

Global Policies Level policy, 7-14

Go To/Search
- by contact option, 1-51
- by location option, 1-49

Grant keyword, 2-88

group
- assign user, 6-51

Group Name object field, 7-32

GSS TSIG secure dynamic DNS update, 3-24

GSSAPI Immediate Retries policy, 3-24

GSSAPI Retry Delay policy, 3-24

H

Hardware Type, 7-61
- Manual Bootp field, 7-72

Hardware Type subnet field, 7-11

hide toolbar, 1-13

Hierarchy, 1-25, 5-11

Hierarchy tabs, 1-11

Highest Level GUI Mode privilege, 6-20

HINFO (Host Information) type field, 5-23

HonorRequestedLeaseTime server policy, 2-78

HonorUnqualifiedBootfile server policy, 2-78

Host ID asset field, 7-39

Host Name option, 2-16

Hosts Per Area field, 5-95

http port, 2-43

https port, 2-43

I

IBM Class Option Template field, 7-64, 7-73

ICMP. See Internet Control Message Protocol

ICMP_REPLY, 2-82

import data
- domains, 10-3
- MAC Address Pools, 10-10
- networks, 10-3
- objects, 10-6
- OSPF areas, 10-3
- subnet organizations, 10-3
- subnets, 10-3

Import External Updates zone option, 5-35, 5-38

Import Result window, 10-5

importing data, 10-2
- error messages, 10-2

using VitalQIP, 10-2

Impress Server, 2-16

IN.ADDR.ARPA records, 5-71

infrastructure
set up, 1-22

InfrastructurelAdministrator Profile, 3-14

init-reboot-address-shuffle policy, 2-67

InitRebootAddressShuffle server policy, 2-79

Inquire report
generate, 9-19

Inquire report type, 9-6

Instance Length field, 3-11, 3-13

Interface MTU, 2-21

internal namespace, 5-11

Internet Control Message Protocol, 2-22

IP Address
dynamic allocation, 7-67

IP address
modify object profile, 7-75
reclaim, 7-97
reserve, 7-79
unallocate dynamic address, 7-77

IP Address Lease Time option, 2-33

IP address notation
bracketed, 2-46

IP Address object field, 7-31

IP Forwarding Enable/Disable, 2-19

IP Layer Parameters per Host options, 2-19

IP Layer Parameters per Interface options, 2-21

ip_address data type, 2-8

ip_address_list data type, 2-8

ip_address_mask_list data type, 2-9

ip_address_pair_list data type, 2-9

ip_mask data type, 2-9

ip_mask_ip_list data type, 2-9

ip-manage Command, A-16

IPv6 Defaults policy, 3-23

IPv6 Reverse Zone Name Generation Tool button, 5-15

IPX, 7-32

IPX Network Number field, 7-58

IPX Node field, 7-58

IPX tab
fields, 7-58

ISDN type field, 5-25

IssueDropUnknownClientTrap server policy, 2-79

K

KDC. See Kerberos Key Distribution Center

Kerberos Key Distribution Center, 2-46, 2-47

Kerberos Keytab Path policy, 3-25

Kerberos Realm, 2-47

key/server icon, 5-19

keyboard commands, 1-11

L

Last Name field, 6-47

LDAP Port parameter, 4-66

LDRM, 2-76

lease parameters, 2-49

Lease Time field, 7-64, 7-74

LeaseExpirationSleepTime policy, 2-79

lease-query-hw-type-override policy, 2-68

LeaveBootpParametersInOptions, 2-79

LevelCritical, 8-12

LevelDebug, 8-12

LevelError, 8-12

LevelInfo, 8-12

LevelWarning, 8-12

Link Layer Parameters per Interface options, 2-24

Local Host Generation, 8-28

local host records
generate, 8-29

LOCAL HOST server type
server type
LOCAL HOST, 4-64

Local Host user exit
File Generation Service, 8-31

Local Servers, 4-1, 4-3, 4-64

location
add, 3-50
delete, 3-50
modify, 3-50
search, 3-50
subnet profile, 7-15

Location field, 7-80
dynamic objects, 7-69

location information
User Profile, 6-50

location profile, 3-49

Location Search policy, 3-34, 3-49

Location/Contact tab
subnet profile, 7-15

locations
Go To/Search, 1-42

log in, 1-4

Log Server, 2-16

Logging In
with several organizations, 1-3

logging in, 1-4

login
- change password, 1-7
- default master administrator, 1-4
- default organization, 1-3
- different organization, 1-9
- different user, 1-9
- Organization window, 1-3
- qipman, 1-4

Login ID field, 6-47

LogLeaseGrantAndRenew server policy, 2-79

LPR Server, 2-16

Lucent DHCP
- server policies, 4-11

Lucent DHCP 5.4 server type, 4-19

Lucent DHCP Rules Manager, 2-76

Lucent DHCP Server
- configure, 4-11

Lucent DHCP server
- Client Names, 4-13

Lucent DHCP Servers
- debug level, 8-10

LUCENT DNS 3.X zone options, 5-35

LUCENT DNS 4.X server type, 4-51

LUCENT DNS 4.X zone options, 5-38

M

MAC address
- duplicate, 5-65

MAC Address asset field, 7-39

MAC Address object field, 7-32

MAC Address Pool subnet field, 7-12

MAC Address Pools
- import data, 10-10

MAC address pools, 4-26

MacWarningsToEventLog server policy, 2-79

MADCAP. See Multicast Address Dynamic Client Application Protocol

Mail Server tab
- Object Profile, 7-51

Mail Servers tab
- fields, 7-52

Maintain Blocks privilege, 6-16

Maintain Pools privilege, 6-18

Maintain Seed Pool privilege, 6-18

manage object ranges, 7-16

manage ranges
- OSPF area, 5-94

Managed by External Updates checkbox, 5-23, 7-47

Managed by External Updates object resource record field, 7-47

Managed List, 5-70, 6-24
- read/write access, 6-26

Managed Range parameter, 4-17, 4-19, 4-33, 4-62, 4-64

Managed Reverse Zone List field, 4-71

Managed Reverse Zones list, 5-75

Managed Server Name field, 4-70

Managed Zone List field, 4-71

Management
- global MAC address pool, 4-38

management report types, 9-6

management reports, 9-3

Management|Go To/Search, 1-43

Mandatory Sub-Option, 2-41, 2-42

Manual Bootp, 7-31

Manual Bootp configuration, 7-67

Manual Bootp Configuration setup, 7-71

Manual Bootp field, 7-71

Manual Bootp setup, 7-71

Manual Bootp setup fields, 7-71

Manual Bootp tab, 7-31, 7-60

Manual DHCP, 7-31

Manual DHCP configuration, 7-67

Manufacturer
- Manual Bootp field, 7-72

manufacturer
- add, 3-43
- apply model name, 3-45
- delete profile, 3-48
- edit name, 3-47
- profiles, 3-42

Manufacturer asset field, 7-39

Mask Boundary field, 5-95

Mask Setting field, 5-95

Mask Supplier, 2-22

Master Administrator, 6-15

Match CIDR Netmask On Reverse Zone policy, 3-35

MaxDebugFileSize parameter, 4-21

Maximum Datagram Reassembly Size, 2-19

Maximum Objects field, 5-6

MaxOutgoingDhcpMessageSize server policy, 2-80

MaxPendingSeconds server policy, 2-80

MaxUnavailableTime server policy, 2-80

MB (Mailbox Name) type field, 5-24

M-Bootp, 7-71

M-Bootp object
  push logic, 2-59

MCFT NT 5.0, 7-73

Merit Dump File, 2-17

Message Service, 4-13

MG (Mail Group) type field, 5-24

Microsoft Default Router Metric Base, 2-31

Microsoft Disable NetBios, 2-31

Microsoft NT 5.0 DHCP, 7-73

Microsoft Release DHCP Lease on Shutdown, 2-31

Microsoft WINS gateway support, 4-42

microsoft_clients Template, 2-54

microsoft_clients Template Options, 2-54

MINFO (Mailbox Information) type field, 5-24

Mobile IP Home Agent, 2-29

Model
  Manual Bootp field, 7-72

Model asset field, 7-39

modify
  administrative role, 6-7
  administrator profile, 6-33
  global MAC address pool, 4-38
  organization, 5-9
  server profile, 4-8
  user group, 6-43

modify object class, 3-61

Move Blocks privilege, 6-17

MR (Mail Rename) type field, 5-24

MSFT 5.0, 2-78

Multicast Address Dynamic Client Application Protocol, 2-55

multicast Template, 2-55

multicast Template Options
  Template Options
    multicast, 2-55

Multicast TTL, 2-31, 2-55

multi-lined_text data type, 2-9

multiple domains
  change DNS options, 5-47
  change user-defined field values, 5-50

multiple reverse zones
  change DNS options, 5-47
  change user-defined field values, 5-50

multiple zones
  change option settings, 5-49

MX (Mail Exchanger) type field, 5-24

N

NackDhcpRequestsForDuplicates server policy, 2-80

NakUnknownClients server policy, 2-80

Name Server, 2-16

Name Services field
  dynamic objects, 7-69

Name Services object field, 7-33

Name Validation policy, 3-36

named.conf, 4-51
  non-managed DNS server, 4-69

Naming Component fields, 3-13

Naming Policies. See Object Name Policies

NBDD. See NetBIOS datagram distribution server

NBNS. See NetBIOS name server

NDS Context, 2-38

NDS Servers, 2-37

NDS Tree Name, 2-38

NDS. See Novell Directory Services

NEAREST_NWIP_SERVER option, 2-38

Negative Cache TTL field, 5-17, 5-79

NetBIOS, 7-32

NetBIOS calls, 4-42

NetBIOS datagram distribution server, 2-28

NetBIOS Domain field, 7-59

NetBIOS Name field, 7-59

NetBIOS name server, 2-28

NetBIOS over TCP/ IP Name Server, 2-54

NetBIOS over TCP/IP Datagram Distribution Server, 2-28

NetBIOS over TCP/IP Name Server, 2-28

NetBIOS over TCP/IP Node Type, 2-28, 2-54

NetBIOS over TCP/IP Scope, 2-28, 2-54

NetBIOS tab, 7-59
  fields, 7-59

NetSh DHCP format, 4-35

Netware/IP Domain Name option, 2-37

Netware/IP Information option, 2-37

Network
  creating, 5-54

network
  create, 5-54
  define address ranges, 5-69
  delete, 5-58
  modify profile, 5-57

Network Address field, 5-55

Network field, 5-95

Network Information Servers, 2-26

Network Information Service, 2-26, 4-44
file format, 4-44

Network Information Service Domain, 2-26

Network Information Service+ Domain, 2-28

Network Information Service+ Servers, 2-29

Network Length field, 4-71

Network Name field, 5-55

Network News Transport Protocol server, 2-29

network objects
naming, 3-11

network profile
add new, 5-54

network profile fields, 5-55

Network Quick View, 6-31
checkbox, 6-31
set up as default, 1-36

Network Quick View function, 1-36

Network Services
overview, 8-3

Network Time Protocol Servers, 2-26

Network Virtual Terminal, 2-17, 2-37

Network Warning
formula for, 5-68

Network Warning fields, 5-68

Network Warning tab, 5-68

networks
import data, 10-3

New Mail Forwarder field, 7-52

New Mail Forwarder Preference field, 7-52

New Mail Host field, 7-52

New Mail Host Preference field, 7-52

New Reverse Zone field, 4-71

New Zone field, 4-71

NIS file
generate, 8-33

NIS Record generation, 8-32

NIS server, 4-1, 4-3

NIS server type, 4-37

NIS user exit
File Generation Service, 8-35
qipnisuserexit, 8-34

NIS, OS Files and the Domain, 4-44

NIS. See Network Information Service

NNTP. See Network News Transport Protocol

Node Management option
User-Defined Hierarchy, 1-33

Node Type
User-Defined Hierarchy, 1-34

Node Types, 1-32

noncontiguous subnet organizations, 5-101

Non-Local Source Routing Enable/Disable, 2-19

Non-Managed DNS Server
create, 4-69

non-managed DNS server
define, 4-69
delete, 4-76
modify, 4-75
named.conf file, 4-69
not updated automatically, 4-69
overview, 4-68
secondary, 4-43
setup fields, 4-70

Non-Managed Server Address field, 4-70

Non-Managed Server Name field, 4-70

no-refresh-interval zone option, 5-43

Normal Administrator, 6-15

notify zone option, 5-30, 5-34, 5-37, 5-40, 5-43

Novell Directory Services, 2-37

Novell Options, 2-37

NS (Name Server) type field, 5-24

NSQ_BROADCAST option, 2-38

Number of Devices field, 7-80
dynamic objects, 7-69

numeric data type, 2-9

numeric_list data type, 2-9

numeric_signed data type, 2-9

NVT. See Network Virtual Terminal

NWIP Setting option, 2-39

NWIP_1_1, 2-39

NWIP_DOES_NOT_EXIST, 2-39

NWIP_EXIST_BUT_TOO_BIG, 2-39

NWIP_EXIST_IN_OPTIONS_AREA, 2-39

O

object
contact information, 7-40
location information, 7-40
schedule a move, 7-89
schedule a move and destination, 7-92
Users tab, 7-44

object alias, 7-34

Object Audit History report
generate, 9-42

Object Audit History report type, 9-6

Object by Address Range report

- generate, 9-9
- Object Class, 3-17
  - manufacturer MAC address, 3-42
- object class
  - create, 3-58
  - delete, 3-62
  - modify, 3-61
- Object Class field, 7-68, 7-79
- Object Class object field, 7-30
- object classes, 3-57
- Object Description object field, 7-31
- Object List report, 9-8
- object management
  - asset information, 7-38
  - automatic bootp setup, 7-72
  - automatic DHCP setup, 7-72
  - cancel scheduled move, 7-96
  - Context menu, 7-22
  - DECNet setup, 7-57
  - define subnet objects, 7-26
  - dynamic object setup, 7-62, 7-68
  - Edit menu, 7-20
  - File menu, 7-20
  - function description, 7-19
  - General tab, 7-40
  - IPX network setup, 7-58
  - mail forwarding, 7-51
  - manual bootp object setup, 7-71
  - manual Bootp setup, 7-60
  - modify reserved address, 7-82
  - modify scheduled move, 7-94
  - move subnet, 7-84
  - NetBIOS setup, 7-59
  - object profile, 7-26
  - Options menu, 7-21
  - policy setup for dynamic object, 7-65
  - Remove User, 7-44
  - reserve IP address, 7-79
  - resourcerecords, 7-45
  - router selection, 7-49
  - schedule an object move, 7-89
  - schedule object move and destination, 7-92
  - subnet selection, 7-4
  - un-reserve reserved address, 7-83
  - User-Defined Fields, 7-43
  - View menu, 7-21
  - wiring hub, 7-53
- object move
  - Auto Assign Destination, 7-87
  - User Specify Destination, 7-87
- Object Move Option window
  - User Specify Destination, 7-92
- Object Name Length global policy, 9-3
- Object Name Length policy, 3-41
- Object Name object field, 7-31
- Object Name Policies
  - Business Unit ID, 3-14
  - create, 3-11
  - dynamically allocated objects, 3-17
  - sample, 3-11
- Object Names
  - customize, 3-12
- Object Profile, 7-27
  - Automatic Bootp configuration, 7-72
  - Automatic DHCP configuration, 7-72
  - DECNET tab, 7-57
  - dynamic allocation setup, 7-68
  - Dynamic Configuration tab, 7-62
  - IPX tab, 7-58
  - Mail Servers tab, 7-51
  - Manual Bootp configuration, 7-71
  - Manual Bootp tab, 7-60
  - modify dynamic object, 7-75
  - modify reserved address, 7-82
  - NetBIOS tab, 7-59
  - Policies tab, 7-65
  - reserve IP address, 7-79
  - Resource Records tab, 7-45
  - Resource Records tab fields, 7-46
  - Routers tab, 7-49
  - un-reserve reserved address, 7-83
  - User-Defined Fields tab, 7-43
  - Wiring HUB Slot/Port tab, 7-55
  - Wiring HUB tab, 7-53
- object profile
  - Aliases tab, 7-34
- object properties
  - edit, 7-21, 7-23
  - User-Defined Fields tab, 7-25
- Object Range tab, 7-16
- Object tab fields, 7-29
- objects
  - Go To/Search, 1-42
  - import data

objects, 10-6

Objects by Address Range report type, 9-6

Objects by Administrator report
generate, 9-13

Objects by Administrator report type, 9-6

Objects by Application report
generate, 9-15

Objects by Application report type, 9-6

Objects by Location report
generate, 9-11

Objects by Location report type, 9-6

OfferOnlyApiRequestedAddress server policy, 2-81

Open Shortest Path First, 5-88

Option 1, 2-84

Option 118, 2-87

Option 119, 2-86

Option 121, 2-86

Option 122, 2-86

Option 43, 2-34

Option 51, 2-84

Option 54, 2-84

Option 55, 2-84

Option 60, 2-90, 7-73

Option 66, 2-79

Option 67, 2-79

Option 77, 2-90

Option 81, 2-81

Option 82, 8-43

option 82, 2-87

Option Code field, 2-8

Option Name field, 2-8

Option Overload option, 2-33

Option81Support server policy, 2-81

organization
add, 5-5
delete, 5-10
modify, 5-9
overview, 5-4
User-Defined Fields, 5-8

OSPF, 5-88
overview, 5-88

OSPF area, 5-88
define, 5-90
delete, 5-100
manage ranges, 5-94
managed range fields, 5-95
managing subnets, 5-93
modify, 5-99

OSPF area mask, 5-88

OSPF area warning fields
Warning Managed Addresses, 5-98
Warning Type, 5-98

OSPF areas
import data, 10-3

OSPF Mask field, 5-95

Owner, 7-46

Owner field, 5-22

Owner object resource record field, 7-46

P

PacketReceiptLDRMCallout, 2-77

PadBootpReply server policy, 2-82

parameters
Bootp, 4-17
DNS BIND-9, 4-45
Local, 4-64
LUCENT DNS 4.X, 4-51
NIS, 4-62
Windows 2000 Domain Controller, 4-66
Windows 2003 DHCP, 4-33
Windows 2003 DNS, 4-56

Partially_Managed, 7-30

Password, 1-3

password data type, 2-9

Password field, 6-47

Password Mask field, 6-48

Password Masking policy, 3-37

Password parameter, 4-67

Path MTU Aging Timeout, 2-20

Path MTU Plateau Table, 2-20

Percent Full field, 5-61

Perform Mask Discovery, 2-22

Perform Router Discovery, 2-22

Perform_Kinit policy, 3-25

Phone field, 6-48

PIN field, 6-48

Ping
All option, 7-21
Selected option, 7-21

Ping Attempts policy, 3-37

ping before assign, 2-89

Ping Retry Delay policy, 3-38

Ping Timeout policy, 3-38

PingAttempts server policy, 2-82

PingBeforeManualBootp server policy, 2-82

PingBeforeManualDhcp server policy, 2-82

PingDelay server policy, 2-82

PingRetention server policy, 2-82

PingSendDelay server policy, 2-82

Place In (Forward Zone/Reverse Zone) object resource record field, 7-47

Planned Use
subnet status, 7-5

policies

global, 3-21

Policies tab, 7-14, 7-65

Policies|Contact Profile, 3-51

Policies|Global Policies, 3-22

Policy Filter, 2-19

Poll Delay parameter, 4-28

PollRetryMax parameter, 4-30

Post Office Protocol Server, 2-29

Postfix of zone db file option, 5-27

PREFERRED_DSS option, 2-39

Prefix Corporate Extension parameter, 4-59

Prefix field, 3-13

Prefix of zone db file option, 5-27

Primary Application object field, 7-32

primary DHCP server
    failover parameters, 4-27

Primary DNS Server
    assign to subnet, 5-67
    Manual Bootp field, 7-71

Primary DNS Server subnet field, 7-10

primary domain server
    add, 5-19

Primary Interface subnet field, 7-12

Primary Time Server
    Manual Bootp field, 7-71

Primary Time Server subnet field, 7-11

Primary/Secondary Servers
    Reverse Zone, 5-80

Primary/Secondary Servers tab, 5-80

PRIMARY_DSS option, 2-39

Principal Name policy, 3-25

privileges
    administrator, 6-15

Protect MDHCP/Bootp Objects policy, 3-38

Provisioning Timer, 2-48

Proxy Kerberos Principal Name parameter, 4-57

Proxy Kerberos Principal Password parameter, 4-57

PTR (Pointer) type field, 5-24

Publish AAAA Records policy, 3-23

Publish PTR Records policy, 3-23

push logic
    Lucent DHCP server, 8-9

Q

qapi, 4-3

Qdhcplib_AC.pcy, 2-72

QIP Hierarchy
    context menu, 1-27

QIP Hierarchy function, 1-25

QIP Update Service
    debug parameters, 4-16

qip.pcy policy file, 4-16

QIPDATASERVER environment variable, 1-4

qip-dhcpgen, 4-14

qip-dhcpgen command, 4-12

qipdhcpuserexit user exit, 8-13

qipdhcpuserexitfgs user exit, 8-14

qip-dnsupdated, 4-11

qip-export CLI, 10-2

qip-genddsnconfs command, 4-49, 4-55, 4-60

QIPHOME/QIPManage.log resource, A-2

qip-import CLI, 10-2

QIPManage.ad, A-1

QIPManage.ad, A-5

QIPManage.confirmExit
    True resource, A-2

QIPManage.dataServer
    SERVERNAME resource, A-2

QIPManage.debug
    Falseresource, A-2

QIPManage.debugFile
    /pathname/of/debug/log/file resource, A-2

QIPManage.debugLevel
    All resource, A-3

QIPManage.defaultOrganization
    ORGNAME resource, A-3

QIPManage.helpDir
    /full/path/to/help/directory resource, A-3

QIPManage.helpExe
    /full/path/to/ip-help resource, A-3

QIPManage.helpTocFile
    helpcontents1.htm resource, A-3

QIPManage.multiQuickView
    True resource, A-4

QIPManage.prefFile
    /user/home/path/.qiprc resource, A-3

QIPManage.printCommand
    lpr resource, A-3

QIPManage.printerOption
    -P resource, A-3

QIPManage.quickViewColumns
    16 resource, A-4

QIPManage.quickViewColWidt h
    20 resource, A-4

QIPManage.quickViewRows
    16 resource, A-4

QIPManage.quickViewShowLab els
    False resource, A-4

QIPManage.sendmailExe

/usr/lib/sendmail -t resource, A-4

QIPManage.toolTipsEnabled True resource, A-4

qip-msgd, 4-13, 4-16

qip-netd, 4-14

qip-qipupdated, 4-13, 4-14, 4-16

qip-rmisched, 4-3, 8-22

qip-rmtd, 4-3, 4-14, 8-22

qip-syncexternal CL, 8-22

qip-tombstonepurge CLI, 3-26

Quick View, 1-35

function descriptions, 1-38

QuickView for the Domain, 1-31

R

Range search field, 1-44

Reassign function, 1-40

Rebinding (T2) Time, 2-34

ReceiveTimeout server policy, 2-72

Reclaim, 7-97

reclaim

manual method, 7-108

scheduling, 7-98

Reclaim E-mail Address parameter, 7-102

Reclaim Reports

samples, 7-110

Reclaim Type parameter, 7-102

refresh-interval zone option, 5-43

RegisteredClientsOnly server policy, 2-83

Relay Agent Information, 8-43

Relay Agent Option, 2-87

Release keyword, 2-88

Remote DNS Servers, 4-43

remote server, 4-3

Remote Server Proxy parameter, 4-18, 4-22, 4-36, 4-48, 4-54, 4-60, 4-63, 4-65

Remote Server Proxy policy, 3-39

Rename Folder function, 1-40

Renew keyword, 2-88

renew-address-shuffle policy, 2-67

RenewAddressShuffle server policy, 2-83

RenewAddressShuffleMaxCount server policy, 2-84

renew-address-shuffle-max-renews policy, 2-67

Renewal (T1) Time, 2-34

Renumber Blocks privilege, 6-18

Report Policy, 3-41

report type

, 9-6

Administrative Role, 9-6

Administrator Audit History, 9-7

Administrator Profile, 9-6

DHCP, 9-6

DNS Zone, 9-6

Free Subnet, 9-6

Inquire, 9-6

Object Audit History, 9-6

Objects by Address Range, 9-6

Objects by Administrator, 9-6

Objects by Application, 9-6

Objects by Location, 9-6

Reports

Free Subnet report, 9-25

Objects by Address Range, 9-8

Objects by Administrator, 9-8

Objects by Application, 9-8

Objects by Location, 9-8

reports

Administrative Role, 9-35

Administrator Audit, 9-44

Administrator Profile, 9-31

CSV Format, 9-4

DHCP report, 9-28

DNS Zone, 9-38

email, 9-4

Inquire, 9-18

Object Audit History, 9-41

print, 9-4

save to file, 9-3

searching for text, 9-3

RequestLDRMCallout, 2-77

Require Alias parameter, 6-20

Require Alias privilege, 6-20

Require Contact Name parameter, 6-21

Require Contact Name privilege, 6-21

Require Location parameter, 6-21

Require Location privilege, 6-21

Require MAC Address parameter, 6-21

Require MAC Address privilege, 6-21

Require Manufacturer Information privilege, 6-21

Require User parameter, 6-19

Require User privilege, 6-19, 7-44

Reserve Allocation fields, 7-79

reserved IP address

modify, 7-82

un-reserve, 7-83

reset toolbar, 1-14

Resource, 7-45

Resource Location Server, 2-16

Resource Record

managed by external updates, 5-23, 7-47

Resource Record Type search field, 1-44

Resource Records
domain, 5-21

resource records
objects, 7-45

Resource Records tab fields, 5-22

Restrict CNAME parameter, 6-21

Restrict CNAME privilege, 6-21

Restrict Subnet privilege, 6-22

reverse mapping, 5-71

reverse zone
add secondary DNS server, 5-82
administrator permissions, 5-71
change DNS options on mulitiple, 5-47
create IPv6 reverse zone, 5-15
define, 5-71, 5-72
information fields, 5-78
IPv6, 5-11
modify, 5-77
multiple primaries, 5-71
Primary/Secondary Servers, 5-80
properties, 5-74
resource records, 5-83
review, 5-77
split, 5-75
user-defined fields, 5-87
zone options, 5-85

Reverse Zone Calculator, 5-75

Reverse Zone Profile, 5-71

Reverse Zone Server field, 5-56

Reverse Zone tab, 5-73

Reverse Zones, 4-71

Review, 5-80

RFC 1001, 2-28

RFC 1035, 2-16

RFC 1042, 2-24

RFC 1179, 2-16

RFC 1191, 2-20

RFC 1256, 2-22

RFC 1497, 2-15

RFC 1517, 5-52

RFC 1518, 5-52

RFC 1519, 5-52

RFC 1520, 5-52

RFC 2132 Options, 2-19

RFC 2241, 2-37

RFC 2242, 2-37

RFC 2308, 5-17

RFC 2563, 2-40

RFC 2610, 2-41

RFC 3004, 2-90

RFC 3256, 2-90

RFC 3397, 2-44

RFC 3495, 2-45

RFC 821, 2-46

RFC 865, 2-16

RFC 868, 2-26

RFC 887, 2-16

RFC 893, 2-24

RFC 894, 2-24

RFC 950, 2-15

RFC2132, 7-73

RIP, 5-88

rndc commands, 8-15

RNDC Key parameter, 4-45, 4-51

RNDC Path parameter, 4-45, 4-51

root domain
define, 5-11

Root Path, 2-17

root server flag, 5-11

root zone, 5-11
create, 5-11

Round Robin parameter, 4-59

route summarization, 5-88

Router option, 2-15, 2-53, 2-54

Router Solicitation Address, 2-22

Router(s) List, 7-49

Routing Information Protocol, 5-88

routing tables, 5-88

RR Set Ordering parameter, 4-52

Rule Level privilege, 6-17

Rule Override privilege, 6-18

rules for managing folders, 1-41

S

Same as in Subnet Profile, 5-103

Same as in subnet profile, 7-63

Same as in SubnetOrg Profile, 5-103, 5-111, 7-11

Same as Subnet Profile, 2-14

sample Administrative Role report, 9-36

sample Administrator Audit History report, 9-46

sample Administrator Profile report, 9-32

sample compressed DHCP report, 9-30

sample DNS Zone report, 9-40

sample expanded DHCP report, 9-30

Sample Free Subnet Report, 9-27

Sample Inquire Report, 9-23

sample Object Audit History report, 9-43

Sample Object List Report, 9-16

Save on Exit, 7-21

Scavenging Interval parameter, 4-59

Schedule Reclaim, 7-97

Schedule Reclaim parameters, 7-102

Scheduled Automatic Updates parameter, 4-17, 4-23, 4-34, 4-47, 4-53, 4-58, 4-62, 4-64, 4-67

Scheduled Move
- subnet status, 7-5

scheduled move
- cancel, 7-96
- modify, 7-94

Scheduled Move Objects, 7-21

scheduled reclaim
- check status, 7-104

scope, 2-49

Scope configuration, 2-41

Scope Life, 2-55

Scope Life option, 2-31

Scope List Sub-Option, 2-42

Search String search field, 1-44

SearchDynamicFirst policy, 4-16

SearchDynamicFirst server policy, 2-84

Secondary Addressing, 7-12

Secondary DHCP Server
- failover parameters, 4-30

Secondary DNS Server
- Manual Bootp field, 7-71

Secondary DNS Server subnet field, 7-10

secondary domain server
- add, 5-20

secondary server
- NS record, 4-43

Secondary Time Server
- Manual Bootp field, 7-71

Secondary Time Server subnet field, 7-11

SecondaryIpAddr option, 4-26

secure DNS
- enable updates, 5-82
- key/server icon, 5-82

secure DNS updates
- enable, 5-19

Secure DNS Updates parameter, 4-52, 4-56, 5-19, 5-82

Secure DNS Updates policy, 3-24

Selected DNS Server(s) List, 5-80

Selected Zones Only option, 8-15

Send Client's Hostname parameter, 4-18

Send Secure Updates parameter, 5-19, 5-82

SendRequestedParamsOnly server policy, 2-84

SendServerIdLast server policy, 2-84

Serial Number asset field, 7-39

server
- add, 4-4
- define, 4-3
- delete profile, 4-9
- modify profile, 4-8

server class, 4-6

server policy template, 4-11

server profile
- delete, 4-9

server type, 4-6
- BIND-9 DNS, 4-45
- Bootp, 4-17
- Lucent DHCP 5.4, 4-19
- LUCENT DNS 4.X, 4-51
- NIS, 4-37
- Windows 2000 Domain Controller, 4-66
- Windows 2003 DHCP, 4-33
- Windows 2003 DNS, 4-56

Servers, 4-4

Service Location Protocol, 2-41

ShareAutoBootpAndDynDhcp policy, 4-16

ShareAutoBootpAndDynDhcp server policy, 2-85

Shared Network subnet field, 7-12

SharedNetworkThresholdProcessing server policy, 2-85

Show Used Only field, 5-60

Simple Mail Transport Protocol option, 2-29

SLP Agents, 2-41

SLP Directory Agent, 2-41

SLP Protocol Options, 2-41

SLP Service Scope, 2-42

SLP. See Service Location Protocol

SMTP. See Simple Mail Transport Protocol

SOA, 8-15

SOA. See Start of Authority

SP Primary DHCP Server Address, 2-47

SP Primary DNS Server Address, 2-47

SP Secondary DHCP Server Address, 2-47

SP Secondary DNS Server Address, 2-47

SP SNMP Entity Address, 2-47

Split erge Blocks privilege, 6-18

Splitting Subnets, 5-65

SRV (Server Resource Record) type field, 5-25

Standalone/Primary parameter, 4-22, 4-26

Standard Mode, 1-18

Start Address field, 5-69, 5-95

Start Address/End Address field
- dynamic objects, 7-69

Start of Authority options, 4-41

Static DDNS Update policy, 3-26

Static DNS Mask, 7-33

static object
- add, 7-27

Static Route option, 2-23

STDA. See StreetTalk Directory Assistance server

stealth server, 5-20

Stop Debug Log, 8-12

StreetTalk Directory Assistance Server, 2-30

StreetTalk Server, 2-29

Strong Kerberos Principal Name parameter, 4-57

Strong Kerberos Principal Password parameter, 4-57

subnet
- assign primart DNS server, 5-67
- associate user, 6-52
- calculate automatically, 5-62
- change display, 7-6
- create, 5-54, 5-59
- join, 5-65
- mask, 5-51
- overview, 5-51
- split, 5-65
- User Define option, 5-64

Subnet Address object field, 7-32

Subnet Calculator, 5-65

Subnet Level policy, 7-14

subnet list
- print, 7-8
- save as text file, 7-8

Subnet Mask object field, 7-32

Subnet Mask option, 2-15, 2-53, 2-54

Subnet Mask subnet field, 7-10

Subnet Move, 7-85

subnet move, 7-84
- limitations, 7-84

Subnet Multiple Application Access policy, 3-39

Subnet Name object field, 7-32

Subnet Name subnet field, 7-10

Subnet Organization
- DHCP Option Template, 5-103
- DHCP Server Name, 5-103

subnet organization
- define, 5-102
- delete, 5-112
- Global Allocation Policy, 5-105
- modify, 5-111
- Windows 2000 site setup, 5-109

subnet organization warning
- formula for, 5-107

subnet organizations
- import data, 10-3

Subnet Profile
- fields, 7-10
- modify, 7-9
- view, 7-9

subnet profile
- Location/Contact tab, 7-15
- manage, 7-3
- Object Ranges tab, 7-16
- User-Defined Fields tab, 7-18

subnet properties fields, 5-60

Subnet Quick View, 6-32
- access, 1-38
- display, 1-36
- function descriptions, 1-36

Subnet Quick View checkbox, 6-32

Subnet Quick View function, 1-38

subnet search, 7-7

subnet selection, 7-4

Subnet Selection Window
- context menu, 7-5

Subnet Selection window
- Configuration Status Indicators, 7-19
- overview, 7-19

Subnet Usage subnet field, 7-10

Subnet Warning field, 5-61

Subnets
- creating, 5-54
- Joining, 5-65
- Splitting, 5-65

subnets
- import data, 10-3

subnet-unavailable-descent-threshold policy, 2-69

subnet-unavailable-threshold policy, 2-69

Suffix Corporate Extension parameter, 4-59

Suffix field, 3-13

Support Bootp parameter, 4-23

Support CIDR field, 4-71, 5-55

Support User Defined Naming Policy checkbox, 3-13

Support VLSM in NIS Generation policy, 3-39

SupportAutoRelease server policy, 2-85

SupportBootpAutoRelease server policy, 2-86

SupportClientID policy, 2-86

SupportEncodingLongOptions server policy, 2-86

SupportMultiUserClass server policy, 2-86

SupportRelayAgentDeviceClass server policy, 2-87

SupportRelayAgentOption server policy, 2-87

SupportRelayAgentServerOverride server policy, 2-87

SupportSubnetSelection server policy, 2-87

Swap Server option, 2-17

SyncBindingBufSize parameter, 4-28, 4-30

SyncBindings parameter, 4-30

SyncBindRetryMax parameter, 4-28, 4-31

SyncFailCritical parameter, 4-31

SyncReqRetryMax parameter, 4-31

T

Tag Key field, 2-8

TCP Default TTL, 2-25

TCP Keepalive Garbage, 2-25

TCP Keepalive Interval, 2-25

TCP Parameters, 2-25

Template Options
- general, 2-53
- microsoft_clients, 2-54

text data type, 2-9

text string
- search, 8-4

text_list data type, 2-9

TFTP Root Directory parameter, 4-18

TFTP Server Name option, 2-35

Tftp Server subnet field, 7-11

TFTP. See Trivial File Transfer Protocol

TGT. See Ticket Granting Ticket

ThresholdMonitorSleepTime server policy, 2-87

Ticket Granting Ticket, 2-46, 2-48

Time Offset, 2-15

Time Server, 2-16

Time Server(s) List, 7-61

Time Server/Tftp Server object field, 7-32

Time To Live field, 5-22

Time to Live object field, 7-32

time_interval data type, 2-10

time_of_day_list data type, 2-10

Tombstone Max Life policy, 3-26

Tombstone Purge Schedule policy, 3-27

toolbar
- Commands tab, 1-15
- Cool Look, 1-16
- create, 1-15
- customize, 1-13
- hide, 1-13
- Large Buttons, 1-16
- reset, 1-14
- Show Tips, 1-16

Trailer Encapsulation, 2-24

tree
- NDS, 2-37

Trivial File Transfer Protoco, 2-18

Trivial File Transfer Protocol, 2-35

TSP AP-REQ/AP-REP Backoff and Retry, 2-45

TSP AS-REQ/AS-REP Backoff and Retry, 2-45

TSP Kerberos Realm Name, 2-46

TSP Primary DHCP Server Address, 2-45

TSP Provisioning Server Address, 2-45

TSP Provisioning Timer, 2-46

TSP Secondary DHCP Server Address, 2-45

TSP Ticket Granting Server Utilization, 2-46

TTL object resource record field, 7-46

TXT (Text) type field, 5-24

Type field, 5-23

Type object resource record field, 7-47

Type Options search field, 1-44

Type search field, 1-44

U

UAP. See User Authentication Protocol

UDF. See User-Defined Field

UDP port number, 2-46

Uniform Resource Locators, 2-43

Unique Name Warning parameter, 6-22

Unique Name Warning privilege, 6-22

Unused
- subnet status, 7-5

unused objects
- move, 7-87

Update generation type, 8-15

Update QIP Operations server policy, 2-88

Update Secondaries policy, 3-27

URLs. See Uniform Resource Locators

Use DNS Update Service policy, 3-28

Use Domain as Realm parameter, 4-52

Use Failover Server parameter, 4-28

Use GSS Interop Flags Default parameter, 4-52

Use GSS Max Contexts Default parameter, 4-52

Use LDRMCallout policy, 2-76

Use server DNS domain as Active Directory domain parameter, 4-57

Use Server Policy Template parameter, 4-23

Use Server Value option value, 5-28

Use Ticket-Granting Ticket, 2-48

Used
- subnet status, 7-5

UseLDRMCallout server policy, 2-77

User Authentication Protocol, 2-43

User Authentication Protocol Options, 2-43

User Class, 2-90

User Class field, 7-63, 7-73

User DN parameter, 4-67

user exit
- qipbootpuserexit, 8-27, 8-31
- qipnisuserexit, 8-35
- User-Defined Object Naming Policy, 3-18

user group
- define, 6-40
- delete, 6-44
- delete user profile, 6-44
- modify, 6-43
- overview, 6-39

User Groups, 6-45
- view, 6-58

User Management, 7-97

User Management function, 6-45

User Modes, 1-18

user name, 1-3

User Name Exit policy, 3-39

User Profile, 6-45
- assign user to group, 6-51
- associate user with managed range, 6-53
- associate user with subnet, 6-52
- delete, 6-57
- Managed Range tab, 6-53
- modify, 6-56
- select location, 6-50
- User-Defined Fields, 6-55

User Profile fields, 6-47

User-Defined Field, 3-53
- add, 3-54
- delete, 3-53, 3-56
- modify, 3-55
- organization, 3-53
- search, 3-53

User-Defined Fields, 7-18

user-defined fields
- change values in multiple domains, 5-50
- domain, 5-44
- object management, 7-43
- reverse zone, 5-87
- User Profile, 6-55

User-Defined Fields tab
- add values, 5-8

User-Defined Hierarchy, 1-25
- create, 1-32

User-Defined Object Naming Policy User Exit, 3-18

V

Validate Domain on Move policy, 3-41

Variable Length Subnet Mask, 5-51
- definition, 5-51

variable length subnetting, 5-88

Vendor Class, 2-90

Vendor Class field, 7-63, 7-73

Vendor Class Identifier, 7-73

Vendor Extensions, 2-15

Vendor Magic Cookie parameter, 4-18

Vendor Specific Information, 2-34
- sub-option format, 2-31

Vendor Specific Information option, 2-27

view DHCP Server Properties, 7-21

View Hierarchy Legends function, 1-17

View menu
- DHCP Server Properties, 7-21
- Display Columns, 7-5, 7-21
- Save Display, 7-5
- Scheduled Move Objects, 7-21

view Scheduled Move Objects, 7-21

View Status Bar function, 1-16

View Toolbars function, 1-13

VitalQIP
- exit, 1-10
- login, 1-4
- toolbars, 1-13
- using the system, 1-11

VitalQIP DHCP Active Lease Service, 4-14

VitalQIP DNS Update Service, 3-28

VitalQIP Domain Name Service, 4-43

VitalQIP Message Service, 3-28, 4-16, 4-43

VitalQIP QIP Update Service, 4-13, 4-14, 4-16, 5-23, 7-47

VitalQIP Remote Service, 4-3, 4-14, 4-43, 8-22

VitalQIP RMI QAPI Service, 4-3

VitalQIP RMI Scheduler Service, 4-3, 4-12, 8-22

VitalQIP Services, 4-43

VitalQIP Update Service, 4-16

VitalQIP Users
- define, 6-46

VLSM, 5-88

VLSM. See Variable Length Subnet Mask

W

WaitCtlRetSecs parameter, 4-29

WaitPollRplSecs parameter, 4-31

WaitSyncBindAckSecs parameter, 4-29, 4-31

WaitSyncBindUpdateSecs parameter, 4-29, 4-32

WaitSyncStartSecs parameter, 4-32

Warning Managed Addresses field, 5-68

Warning Type field, 5-68

wildcard character, 7-12

Windows 2000 Site tab, 5-109

Windows 2003
- Active Directory, 4-66
- site setup, 5-109

Windows 2003 Active Directory, 8-36

Windows 2003 DHCP server type, 4-33

Windows 2003 DNS Secure Update Policies, 3-28

Windows 2003 DNS secure zone updates policies, 7-14

Windows 2003 DNS server, 5-42

Windows 2003 DNS server type, 4-56

Windows 2003 DNS zone options, 5-42

Windows 2003 Domain Controller, 4-1, 4-3
- generate files, 8-37
- parameters, 4-66
- server type, 4-66

Windows 2003 Domain Controller server type, 4-66

Windows 2003 Site tab, 4-66

Windows Internet Naming Service, 4-42

Windows Internet Naming System, 2-54

WINS Gateway, 4-42

WINS server, 2-28

WINS. See Windows Internet Naming Service

WINSOCK2, 2-74

wiring hub
- associate with object, 7-53

Wiring HUB Slot/Port, 7-55

Wiring HUB tab, 7-53

WKS (Well-Known Services) type field, 5-24

Write New Infrastructure to Managed List privilege, 6-18

X

X Window System Display Manager, 2-28

X Window System Font Server, 2-28

X25 type field, 5-25

Z

ZeroCiAddr server policy, 2-88

zone block of named.conf zone option, 5-30, 5-34, 5-37, 5-41

Zone E-mail Address field, 5-78

Zone Expire Time field, 5-79

Zone Mask field, 5-75

Zone Options, 5-19, 5-81

zone options
- BIND 8.X, 5-28
- BIND 9.X, 5-31
- change multiple zone settings, 5-49
- Extensions, 5-27
- LUCENT DNS 3.X, 5-35
- LUCENT DNS 4.X, 5-38
- set up, 5-26
- Windows 2003 DNS, 5-42

zone options zone option, 5-43

Zone Refresh Time field, 5-79

Zone Retry Time field, 5-79