Dell OpenManage Network Manager

User Guide

Notes, and Cautions

A NOTE indicates important information that helps you make better use of your computer or software.

A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

Information in this document is subject to change without notice.
© 2011 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL logo, PowerConnect™, OpenManage™, EqualLogic™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core™ and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™, and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® is a registered trademark and SUSE ™ is a trademark of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter®, and vSphere® are registered trademarks or trademarks of VMWare, Inc. in the United States or other countries.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

May 18, 2011 Rev. A00

Contents

Important Information

This application can give you automated, consolidated configuration and control of network resources.

Consult this product's Release Notes for information about additional changes not covered in the user guide.

This Guide

This guide outlines the features of an entire suite of applications, some of which are optional.

What's New in This Version

This is an update to a previous major release with the following features. Consult the product release notes for more specifics. This release adds enhancements and bug fixes.

Platform

- Microsoft® Vista and Server® 2008 support
- Windows® 7 (business and better) support.

You may manage a heterogeneous network with this application. If you have Dell and Cisco equipment drivers installed, for example, you can manage Dell equipment supported by that driver, *and* Cisco equipment. Consult your sales representative about what applications and drivers are available, and what equipment they support.

NOTE:

The appearance of some pages in the following guide may be different than your product, depending on the products and device drivers you have installed.

Updating Your License

If you have a limited license — for example Dell™ OpenManage™ Network Manager by default limits discovery to ten devices — then your application does not function outside those licensed limits. You can purchase additional capabilities, and can update your license for *OpenManage Network Manager* by putting the updated license file in a convenient directory. Then use the

Settings -> *Permissions* -> *Register License* menu item to open a file browser. Locate the license file, and click the *Register License* button. Your updated license should be visible in *Settings* -> *Permissions* -> *View Licenses*.

NOTE:

If you update your installation from a previous one where you upgraded license, you must also re-register those licenses.

You must restart application server or wait up to 15 minutes before a license modification takes effect. OpenManage Network Manager comes with a 10-device license that lets you manage and monitor up to 10 Dell Powerconnect switches. You can purchase additional licenses through your sales representative. If you try to discover more than 10 devices, a message appears in Discovery that says you have exceeded your license, and only the first 10 devices discovered appear in Resources. To manage a device not in Resources, you must remove a device, then discover only the device you want to add.

A Note About Performance

These applications are designed to help you manage your network with alacrity. Unfortunately, the devices they manage or the networks that communicate with those devices are not always as fast as this software. If discovery takes a long time (it can), often network and device latency is the culprit. You can also optimize installations to be faster, and limit device queries with filters, but device and network latency limit how quickly your system can respond.

NOTE:

If you use management systems other than this one, you must perform a device level resync before performing configuration actions. Best practice is to use a single management tool whenever possible.

1

Hardware, Operating Systems and Ports Used

System Basics

System requirements vary depending on how you use it. You should base the minimum configuration of any system on expected peak load. Typically a configuration running all elements of a system on a single server spends 95% of its time idle and 5% of its time trying to keep pace with the resource demands. If you expect your system to perform an operation that could run create, modify or delete rules on tens or hundreds of thousands of business objects, your real system needs may be much higher.

Recommended Operating System Versions

Disable firewall products during initial installation and testing. The following are recommended operating system versions:

- Microsoft Windows®—This application supports most Windows operating systems from Windows XP forward, with their latest service packs. The supported operating systems are: Windows 2003 (Standard, Enterprise and Web), Windows XP (Pro) SP3 or later, Windows Vista (Business or Ultimate), Windows Server 2008, Enterprise Edition, and Windows 7 (Business or better). This is a 32-bit application, however it has been tested for Windows on both 32- and 64-bit operating system versions, and supports both in the Windows versions supported.

NOTE:

Windows Terminal Server is not supported. The installer becomes non-responsive with Data Execution Prevention enabled. This option is disabled by default on Windows Server 2008, but is enabled on a Windows Server 2008 machine running Terminal Server.

Also: You must disable User Access Control if you are installing on Vista or Windows Server 2008.

Also: Installer may halt when pre-existing bash sessions or cmd sessions left are open. Close all such sessions.

Finally: In Vista, you must either to disable User Account Control or run application server as service. Another option is to run as administrator on startappserver. In Vista, right click the startappserver icon and select run as administrator.

CAUTION:

To manage Windows systems—you must install this application on a Windows host.

- Linux—This application supports Redhat® (Enterprise® version 4, 4r5 or 5) and SUSE® (version 9 or 10) Linux, 64-bit only. See 32-bit Linux Libraries for some additional requirements.

32-bit Linux Libraries

For SuSE or Red Hat Enterprise 64 bit installations, you must identify the appropriate package containing 32-bit `libtcl8.4.so` (for the example below: `tcl-8.4.13-3.fc6.i386.rpm` for Red Hat).

NOTE:

Do not use any x86_x64 rpms; these would not install the 32-bit libraries.

Any 32-bit tcl rpm that is of version 8.4 and provides `libtcl8.4.so` works. You can download them from Sourceforge: http://sourceforge.net.

Download these, then issue the command:

```
rpm -ivh --force tcl-8.4.13-3.fc6.i386.rpm
```

This forces the installation of the 32-bit libraries on a 64-bit system. Ensure that your expect executable in your installation directory is properly linked by issuing the following commands:

```
[someone@RHEL5-64bit ~]$ which expect

/opt/dorado/oware3rd/expect/linux/bin/expect

[someone@RHEL5-64bit ~]$ ldd /opt/dorado/oware3rd/expect/linux/bin/expect

        linux-gate.so.1 =>  (0xffffe000)

       libexpect5.38.so => /opt/dorado/oware3rd/expect/linux/bin/
   libexpect5.38.so (0xf7fd2000)

       libtcl8.4.so => /usr/lib/libtcl8.4.so (0x0094c000)

       libdl.so.2 => /lib/libdl.so.2 (0x0033e000)

       libm.so.6 => /lib/libm.so.6 (0x00315000)

       libutil.so.1 => /lib/libutil.so.1 (0x00b8d000)

       libc.so.6 => /lib/libc.so.6 (0x001ba000)

       /lib/ld-linux.so.2 (0x0019d000)
```

Make sure that `libtcl8.4.so` maps to `/lib/libtcl8.4.so`

An Alternative for RedHat Linux

1. Copy /usr/lib/libtcl8.4.so from a 32-bit RH system to /usr/local/lib/32bit on your 64-bit RedHat system
2. As root, execute: ln –s /usr/local/lib/32bit/libtcl8.4.so /usr/lib/libtcl8.4.so

Supported Protocols

The following are supported protocols:

- TCP/IP
- SNMP
- HTTP
- UDP Multicast
- CIDR

Installing Perl

If you install Perl to take advantage of this application's use of Perl Scripting capabilities, you must install it on the path on the application server and mediation server host.

NOTE:

We recommend Perl version 5.10. Some applications also require Perl as well as the Perl module Net::Telnet.

This application does not package Perl. If you want to use the Perl scripting features (for example in Adaptive CLI group operations described in Chapter 22, Group Operations), you must make sure your system has Perl installed. You can find information about Perl at www.perl.com. Follow the downloads link to find the recommended distribution for your specific platform.

One of the recommended Perl packages is from ActiveState which can be found at:
www.activestate.com/activeperl/

Hardware Recommendations

The following describes recommended hardware minimums for this application. These minimums assume average usage levels, and no other software competing for resources. Increase the computing power of your hardware if your system experiences heavier loads.

- **Full Installation (Application server + Client)**—Pentium 4, 3.2 GHz CPU, 2G RAM, and 20G available disk space
- **Client only**—Pentium 4, 2.8 GHz, 1G RAM (512 MB minimum, 1G for optimum performance), and 1G available disk space.

Hard drive space requirements listed here, and other hardware requirements are based on expected maximum use for average installations and are only intended to be an approximate guide.

NOTE:

This software version is not compatible with Windows NT.

Trap Processing Speeds

The following describes event processing speeds for the mediation service, the portion of this application that communicates directly with the devices under management, and the application server, which receives events from the mediation service, processes them, and formats them so that a client can view them. The nominal sustainable rate and a burst rate are two variations on these performance numbers. The sustainable rate is what is expected during normal operation.

This application typically does not lose traps as they come in. It can handle the burst rate, but only for a short period falls behind and events are backed up. This is standard behavior for Event Monitoring systems.

Application server inserts event data into the database, updates alarm states in the database, executes propagation logic, and executes any necessary automation. Besides handling incoming events, application server also handles client requests from event or alarm views and these result in database queries.

NOTE:

The performance of the database significantly effects event processing.

Mediation is a service running in the application server. The mediation service correlates events against the inventory model, applies event filtering, and determines what actions, if any, should execute for an event. When events come into the system, from any protocol, they queue for processing by mediation. At regular intervals, mediation submits processed events to the application server for more processing against the database. The remaining queued events wait while the current batch is being committed.

The application immediately converts SNMP traps into events and then queues them for mediation. It handles syslog differently, spooling all messages on disk first and then discarding or escalating them to event status. By default, all syslog messages are escalated. Handling a large volume of events may involve some analysis of the events coming in and modifications to event definitions and processing rules.

The numbers here reflect both SNMP traps as well as Syslog messages. Syslog messages can be recieved at a higher rate without loss and are inspected very quickly, but escalated syslog messages must still go through general event processing and correlation.

Event type				
	SNMP		**Syslog**	
Service	Sustained (traps/s)	Burst (traps/s)	Sustained (msgs/s)	Burst (msgs/s)
Mediation	200	4000	200	20,000
Application	120	2000	120	10,000

NOTE:

Sustained counts reflect the number of events that pass through correlation and filtering. For example, 10,000 syslog messages may yield only 50 escalated events. Here, the sustained rate for syslog is low because we are assuming all messages are escalated. Higher volumes require more configuration to detect and ignore unwanted traps or messages at the mediation layer.

Swap Files and Services

Best practice is to set the swap file for Windows to at least 1536M (larger is better), with its minimum and maximum being set to the same value to avoid resizing and fragmentation of the swap file. Ideally, it would be on its own partition or drive, separate from the OS or database.

Also, best practice is to look at what else is running on the box, including third party software *and* Windows services (`services.msc`). Stop unnecessary services and reset their startup type to manual.

For example:

If netbios is enabled over TCP/IP, it should be disabled in the A*dvanced TCP/IP properties* (WINS tab) for each connection, and the netbios, netbt, netbios helper and browser services should be stopped and disabled. The netbios and netbt services are not visible from the services control panel applet, but can be stopped using `net stop netbios, net stop netbt`.

Software Space Requirements

You cannot install applications unless the target drive has the required free space. Here are the minimum requirements

Software / Platform	**Full Installation**	**Client Installation**
Application Only / Windows	2 G (plus)	330MB

The *Full* installation is really just a client plus database size. The same footprint exists for any type of installation with the actual databases being the only difference. Applications can add required space for client as well as additional space for database server. The 750MB difference in the numbers above is simply a default setting in installer that requires an additional 750MB for data space.

Client Password

The first time users log in to a client, they are prompted by the interface to change their password. The default login is *admin*, and the default password is blank (no text).

NOTE:

The password is encrypted in the database.

FTP Servers on Linux

The internal file server does not work on these operating systems. The following sections describe how to use their alternatives to that file server. Installation of FTP, TFTP, SFTP and SCP depends on having the server correctly configured on Linux.

The following installation instructions describe how to do this:

- Red Hat Linux FTP / TFTP on page 32—Installing on Red Hat Linux

Refer to the operating system documentation for details about these, or if your operating system is not specifically mentioned below.

3 Edit /etc/ftpd/ftpaccess, adding the following line:

```
    defumask 000
```

4 Execute inetconv

```
# inetconv
```

5 Verify the service is enabled

```
# svcs | grep tftp
    online         10:52:15 svc:/network/tftp/udp6:default
```

Red Hat Linux FTP / TFTP

The following are steps to set up FTP and TFTP on Red Hat Linux:

1 Confirm if FTP is installed by typing the following in a shell:

```
rpm -q vsftpd
```

The following is an example response (your version may differ):

```
vsftpd-2.0.5-10.el5
```

2 Modify the `vsftpd.conf` file which is in `/etc/vsftpd`

a. Become super user.

b. Edit `vsftpd.conf` file with a text editor.

c. Uncomment the line `#listen = YES`

d. Change `umask = 000` (must be at least `011`)

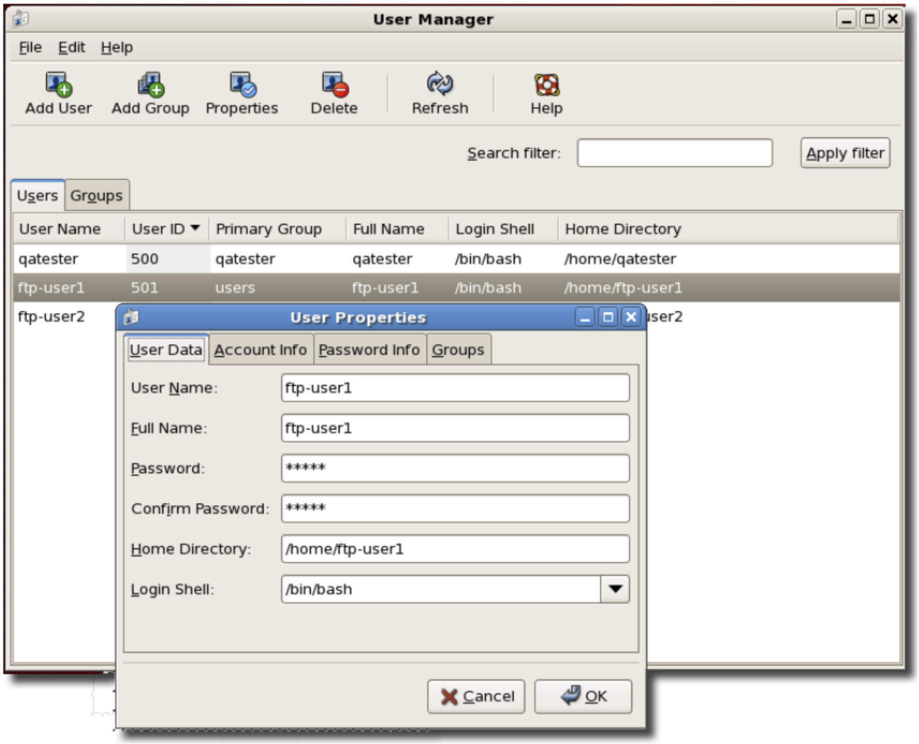
e. Save vsftpd.conf

f. Run this process to stop the FTP process: `/sbin/service vsftpd stop`

g. Run this to restart the FTP process: `/sbin/service vsftpd start`

h. Confirm the FTP process is running `netstat -a | grep ftp`

3 Create a user, for example, `ftp-user1` with the home directory = `/home/ftp-user1`



User Name	User ID	Primary Group	Full Name	Login Shell	Home Directory
qatester	500	qatester	qatester	/bin/bash	/home/qatester
ftp-user1	501	users	ftp-user1	/bin/bash	/home/ftp-user1
ftp-user2					ser2

User Name: ftp-user1

Full Name: ftp-user1

Password: *****

Confirm Password: *****

Home Directory: /home/ftp-user1

Login Shell: /bin/bash

4 Confirm TFTP is installed by running this command in a shell:

```
rpm -q tftp-server
```

The following is an example response (your version may differ)

```
tftp-server-0.42-3.1
```

5 Start TFTP with the following shell commands, once you are logged in as superuser:

```
/sbin/chkconfig -level 345 xinetd.d on
/sbin/chkconfig -level 345 tftp on
```

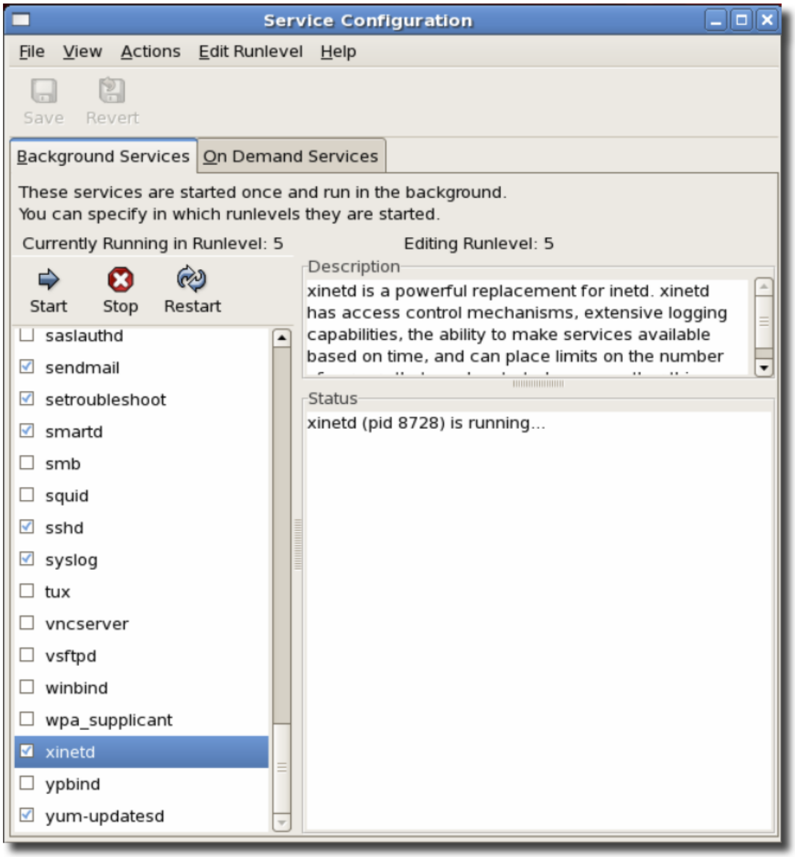
6 Modify the following in the TFTP file located in `/etc/xientd.d`

```
server_args = -u ftp-user1 -s /home/ftp-user1
```

This sets the same directory for ftp & tftp

```
disable = no
```

Save the file, then restart `xinetd` by going to System -> Administration -> Server settings -> Services, and enter the root password. Select `xinetd` a click on *Restart* or click *Stop*, then click *Start*.



These services are started once and run in the background.
You can specify in which runlevels they are started.

Currently Running in Runlevel: 5

Editing Runlevel: 5

☐ saslauthd
☑ sendmail
☑ setroubleshoot
☑ smartd
☐ smb
☐ squid
☑ sshd
☑ syslog
☐ tux
☐ vncserver
☐ vsftpd
☐ winbind
☐ wpa_supplicant
☑ xinetd
☐ ypbind
☑ yum-updatesd

xinetd is a powerful replacement for inetd. xinetd has access control mechanisms, extensive logging capabilities, the ability to make services available based on time, and can place limits on the number

xinetd (pid 8728) is running...

7 Run the following in a shell to verify TFTP is running: `netstat -a | grep tftp`. A response should indicate such a process is running.

Ports Used

You must sometimes configure this application's port availability on firewalls. Sometimes, excluding applications from firewall interference is all that is required (see Ports and Application To Exclude from Firewall on page 41).

The following are some of the standard port assignments for installed components. These are often configurable (even for "standard" services like FTP or HTTP), so these are the typical or expected port numbers rather than guaranteed assignments.

Destination Port(s)	Service	File(s)	Notes	Used from Client
HTTP/S (Web Client)				
8080[4]	oware.webservices.port	[user.root]\oware\lib\owweb services.properties	appserver	Yes
8443[4, 5, 7]	org.apache.coyote.tomcat4.CoyoteConnector (Apache)	[user.root]\oware\jboss-3.2.7\server\oware\deploy\jbossweb-tomcat41.sar\META-INF\jboss-service.xml	app/medserver	No
Other Ports				
n/a[5](ICMP)	ping		MedSrv -> NtwkElement, NtwkElement -> MedSrv, ICMP ping for connection monitoring.	
20[4, 5, 7] (TCP)	FTP Data Port	n/a	(Internally configurable), "MedSrv -> FTPSrv NtwkElement -> FTPSrv" medserver[1]	No
21[4, 5, 7] (TCP)	FTP Control Port	n/a	(Internally Configurable) "MedSrv -> FTPSrv NtwkElement -> FTPSrv" medserver[1]	No
22[4, 5, 7] (TCP)	SSH	n/a	MedSrv -> NtwkElement, secure craft access medserver[1]	No

Destination Port(s)	Service	File(s)	Notes	Used from Client
23[4, 5, 7] (TCP)	Telnet	n/a	MedSrv -> NtwkElement, non-secure craft access medserver[1]	Yes
25[4, 5, 7] (TCP)	com.dorado.mbeans.OWEmailMBean (mail)	[user.root]\oware\jboss-3.2.7\owareconf\oware-service.xml	AppSrv -> SmtpRelay, communication channel to email server from Appserver	No
69[4, 5, 7] (UDP)	TFTP	n/a	(Configurable internally), F, MedSrv -> TFTPSrv NtwkElement -> TFTPSrv medserver[1]	No
161[4, 5, 7] (UDP)	com.dorado.media tion.snmp.request.listener. port (SNMP), oware.media tion.snmp.trap.forward ing.source.port	[user.root]\oware\lib\owmediationlisteners.properties, [user.root]\oware\lib\owmediation.properties	MedSrv -> NtwkElement, SNMP request listener and trap forwarding source medserver[1]	No
162[4, 5] (TCP)	oware.media tion.snmp.trap.forwarding .des tination.port (SNMP)	[user.root]\oware\lib\owme diation.properties	NtwkElement -> MedSrv, SNMP trap forwarding destination port, medserver[1]	No
514[4, 5] (UDP)	com.dorado.mediation.syslog.port (syslog)		NtwkElement -> MedSrv (mediation syslog port) medserver[1]	No
1098[4, 5, 7] (TCP)	org.jboss.naming.Naming Service (JBOSS)	[user.root]\oware\jboss-3.2.7\owareconf\jboss-root-service.xml	AppSrv -> MedSrv MedSrv -> AppSrv user client ->AppSrv user client ->MedSrv, (JBOSS naming service), app/medserver	Yes

Destination Port(s)	Service	File(s)	Notes	Used from Client
1099[4, 5, 7] (TCP)	org.jboss.naming.Naming Service (JBOSS)	[user.root]\oware\jboss-3.2.7\owareconf\jboss-root-service.xml	MedSrv -> AppSrv, user client -> AppSrv, user client -> MedSrv, (JBOSS naming service & OWARE context server URL), app/medserver	Yes
1099[2, 4, 5, 7] (TCP)	OWARE.CONTEXT.SERVER.URL	 [user.root]\owareapps\installprops\lib\installed.properties [user.root]\owareapps\installprops\medserver\lib\installed.properties	MedSrv -> AppSrv, user client -> AppSrv. user client -> MedSrv. (JBOSS naming service & OWARE context server URL) client medserver[1]	Yes
1103[4, 5] (UDP)	jnp.reply.discoveryPort (JNP)	[user.root]\oware\lib\owappserver.properties	AppSrv -> MedSrv, AppSrv -> user client, (JNP reply discovery port), app/medserver	Yes[3]
1123[4, 5] (UDP)	jnp.discoveryPort (JNP)	[user.root]\oware\lib\owappserver.properties	MedSrv -> AppSrv, user client -> AppSrv, (JNP discovery port), app/medserver	Yes[3]
1812[4, 7] (TCP)	RADIUS port	[user.root]\oware\jboss-3.2.7\server\oware\conf\login-config.xml	AppSrv -> RADIUS Srv, Appserver (RADIUS client login enabled–optional)	No

Destination Port(s)	Service	File(s)	Notes	Used from Client
2506[4, 5, 7] (TCP)	JMS - SONICMQ_CLIENT_PORT (JMS)	[user.root]\oware\lib\owapp server.properties	MedSrv -> AppSrv user client -> AppSrv, (JMS - SonicMQ client port) app/medserver	Yes
2507[4, 7] (TCP)	JMS - SONICMQ_CONFIG_PORT	[user.root]\oware\lib\owapp server.properties	AppSrv -> AppSrv MedSrv -> AppSrv, (JMS - SonicMQ client port), app/ medserver	No
2508[4, 7]	JMS - SONICMQ_INTERBROKER_POR T (JMS)	[user.root]\oware\lib\owapp server.properties	AppSrv -> AppSrv, MedSrv -> AppSrv, (JMS - SonicMQ interborker port), app/medserver	No
3306[4, 7] (TCP)	com.dorado.jdbc.database_name.mysql	[user.root]\oware apps\install props\lib\installed.properties	AppSrv -> MySQLSrv, (JDBC database naming [MySQL]) appserver)	No
3100[4, 5, 7] (TCP) 3200[4, 5, 7]	org.jboss.ha.jndi.HANaming Service (JBOSS)	[user.root]\oware\jboss-3.2.7\owareconf\cluster-service.xml	AppSrv -> AppSrv, user client -> AppSrv AppSrv -> MedSrv MedSrv -> AppSrv user client -> AppSrv user client -> MedSrv (JBOSS HA JNDI HA Naming service [3100 is stub] app/medserver	Yes[3]
4445[4, 5, 7] (TCP)	org.jboss.invocation.pooled.server.PooledInvoker (JBOSS)	[user.root]\oware\jboss-3.2.7\owareconf\jboss–root-service.xml	AppSrv -> MedSrv MedSrv -> AppSrv user client -> AppSrv user client -> MedSrv, app/ medserver	Yes

Destination Port(s)	Service	File(s)	Notes	Used from Client
4446[4, 5, 7] (TCP)	org.jboss.invocation.jrmp.server.JRMPInvoker (JBOSS)	[user.root]\oware\jboss-3.2.7\owareconf\jboss–root-service.xml	(AppSrv ->AppSrv, AppSrv -> MedSrv, MedSrv -> AppSrv, user client -> AppSrv, user client -> MedSrv) app/medserver	Yes
5988, 5989	WBEM Daemon (5989 is the secure port) defaults		You can add ports and daemons in monitored services. These are only the default. WBEM requires one port, and only one, per daemon.	No
7800[2](TCP)	org.jboss.ha.framework.server.ClusterPartition (JBOSS)	[user.root]\oware\conf\cluster-service.xml	disabled - see UDP for same, (JBOSS HA frame work server cluster partition) TCP only	No
8009 (TCP)	org.mortbay.http.ajp.AJP13Listener	[user.root]\oware\jboss-3.2.7\server\oware\deploy\jbossweb-tomcat41.sar\META-INF\jboss-service.xml	Obsolete — appserver	No
8083 (TCP)	org.jboss.web.WebService (JBOSS)	[user.root]\oware\jboss-3.2.7\owareconf\jboss–root-service.xml	not used (JBoss web services) appserver	No
8093[4, 5. 7] (TCP)	org.jboss.mq.il.uil2.UILServerILService	[user.root]\oware\jboss-3.2.7\owareconf\uil2-service.xml	MedSrv -> AppSrv, user client -> AppSrv (JBOSS mq il uil2 UIL Server-IL Server), app/medserver (Jboss JMS)	Yes
8443[2,4, 5, 7]	org.apache.coyote.tomcat4.CoyoteConnector	[user.root]\oware\jboss-3.2.7\server\oware\deploy\jbossweb-tomcat41.sar\META-INF\jboss-service.xml	user client -> AppSrv (Apache Coyote Tomcat4 Coyote connector), appserver	No

Destination Port(s)	Service	File(s)	Notes	Used from Client
9001[4, 6, 7] (UDP)	mediation.listener.multicast.intercomm.port	[user.root]\lib\owmediation listeners.properties	MedSrv <-> MedSrv (mediation listener multicast intercommunications port) medserver[3]	No
31310[4, 6, 7] (TCP)	JBoss		AppSrv -> AppSrv	No
45566[4, 5] (UDP)	org.jboss.ha.framework.server.ClusterPartition	[user.root]\jboss-3.2.7\owareconf \cluster-service.xml	AppSrv -> Multicast, (JBoss HA frame work server cluster partition), UDP only	No
54027[4,7]	Process Monitor	[user.root]\oware\lib\pmstar tup.dat	mgmt client -> AppSrv, mgmt client -> MedSrv (process monitor local client for server stop/start/ status) app/ medserver	Yes

[2] Unused in standard configuration.

[3] Client does not connect to medserver on this port.

[4] This port is configurable.

[5]Firewall Impacting

[6]The most likely deployment scenarios will have all servers co-resident at the same physical location; as such, communications will not traverse through a firewall

[7]Bidirectional

To operate through a firewall, you may need to override default port assignments.

NOTE:

To configure ports, open their file in a text editor and search for the default port number. Edit that, save the file and restart the application server and client. Make sure you change ports on all affected machines.

The mediation service also establishes a socket connection to client on ports 6500 to 6510 for cut through. Such connections are specified in the `ezmediation/lib/ezmediation.properties file`.

```
[user.root] = $OWARE_USER_ROOT
```

Ports and Application To Exclude from Firewall

Exclude `java.exe`, tcp port 21 and udp port 69 from firewall interference to let the application function. The java process to exclude from firewall blocking is `<Installdir>\oware3rd\jdk[version number]\jre\bin\java.exe`.. The embedded database process is `mysqld-max-nt.exe` (in Windows, the path is `<installdir>oware3rd\mysql\[version number]\bin\mysql-max-nt.exe).` Consult your DBA for Oracle processes, if applicable.

Installed Third Party Applications

The following applications are installed with this software. Cited version numbers are subject to change without notice

- ant v1.6.5
- cygwin v1.5.24-2
- expect v5.26
- jboss v3.2.7
- JDK v1.6.0_01
- JLoox v3.0
- MySQL v5.0.45
- Open SSH v3.6.1-p1 includes OpenSSL v0.9.7b
- TCL v8.2
- OpenLDAP
- Jasper Reports v1.3.2
- J Free Charts v1.0.8

Windows Management Interface Ports

Windows Management Interface uses the following ports:

Protocol or Function	**Ports Used**
RPC, TCP	135,139,445,593
SNMP, UDP	161,162
Optional:	
WINS, TCP	42
UDP	42, 137
PrintSpooler, TCP	139, 445
TCP/IP PrintServer, TCP	515

These are relevant only if you are using any Windows-based server device driver.

2

Installation

Installation Overview and Prerequisites

The installation process installs the application, including its foundation class software. For hardware requirements, and other prerequisites, consult the sections following System Basics on page 27.

This application is incompatible with any other software using the standard SNMP ports (162, for example), or other raw sockets. Either stop the conflicting application before you install this one, or stop this one whenever you want to use the alternative. You may have to reboot to close conflicted sockets. To stop this application, you must close the client *and* stop the Application Server (see Stopping Servers on page 56).

NOTE:

Upgrading from a previous installation is automated, but best practice is to back up the existing system first to ensure data preservation. Some packages may have an install wizard option to back up the database before upgrading.

Quick Start

The typical sequence of events, including installation is the following:

- **Install the software**—See Installing the Application on page 47 for details.

- **Discover Network Devices**—See Chapter 12, Discovery in the *User Guide* for detailed instructions, or click *File -> Open -> Inventory -> Resource Discovery* and enter the IP addresses you want to discover. You may also have to enter SNMP and Telnet login/password combinations to fully discover equipment. Once you have discovered equipment, you can manage it.

- Begin Managing your network

You can also administer your application, setting up users, and equipment access passwords, and groups for both users and equipment, as you begin to use it.

Basic Network Considerations

This application communicates with devices over a network. In fact, you must be connected to a network for Application Server to start successfully. Firewalls, or programs using the same ports on the same machine where this application is installed can interfere with its ability to communicate with devices. See Ports Used on page 35.

Your corporate network may have barriers to communication with this software that are outside the scope of these instructions. Consult with your network administrator to ensure this application has access to the devices you want to manage with the Protocols described below.

NOTE:

One simple way to check connectivity with a device is to open a command shell with Start -> Run `cmd`. Then, type `ping [device IP address]` at the command line. If the device responds, it is connected to the network. If not, consult your network administrator to correct this. No useful information comes from disconnected devices.

Name Resolution

If you have server and client on different machines, this application requires resolution of equipment names, whether by host files or domain name system (DNS). The Application Server cannot respond to clients based on its IP address alone. It may be on a different network and therefore the client would be unable to connect.

Whether it uses the `OWARE.CONTEXT.SERVER` URL or not, when a client connects to the Application Server it receives a stub with the real URL used to communicate with RMI. This stub always returns a URL with the host name, if available.

If your network does not have DNS, you can also assign hostnames in `%windir%\system32\drivers\etc\hosts` on Windows®. You must assign a hostname in addition to an IP address in that file. Here are some example hosts file contents (including two commented lines where you would have to remove the # sign to make them effective):

```
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
127.0.0.1       localhost
```

CAUTION:
This software does not support installation to anything but the local file system. Avoid installing to shared drives.

Protocols

This application uses the following protocols: TCP/IP, SNMP, HTTP, UDP Multicast. You can bypass multicast, if it is disabled on your network. To allow a client to connect without multicast, add the following property to the client's `owareapps\installprops\lib\installed.properties` file.

```
OWARE.CONTEXT.SERVER.URL=jnp://[HostName]:1099
```

Fixed IP Address

OpenManage Network Manager is a web server, among other things, and so must be installed to a host with a fixed IP address. For demonstration purposes, you can rely on dynamic IP address assignment (DHCP) with a long lease, but this is not recommended for production installations.

Windows Prerequisites

This application requires a temp directory on the host where it is being installed. If the install launcher cannot extract a Java Virtual Machine (JVM), then it cannot run. The launcher extracts a JVM to a temp directory and then starts the installer main using this temp JVM.

Windows typically has a temp directory, `WINDOWS\temp`. Installation expects that TEMP or TMP environment variable exists and points to this temp directory (check in a command shell with `cd %TEMP%` or `cd %TMP%).`

You can also execute the `win_install.exe` installation from a command line to override temp directory locations with this command line:

```
win_install.exe -is:tempdir c:\mytemp
```

CAUTION:

The correct executable to install the application is win_install.exe. Setup.jar is an executable jar file that may appear to initiate the installation but installation will not be successful.

Although it is not always necessary, during installation or uninstallation best practice is to disable any virus protection software, and any other running application. Some applications have additional services (like Norton Unerase™) that prevent correct installation on some systems. Stop these in Services in Control Panel’s Administrative Tools.

This application cannot co-exist with other installations of Cygwin on the same Windows computer. Do not install it where Cygwin is already installed, either separately or as part of another application. If Cygwin is already installed, remove it before installing this application.

If they are present, turn off Microsoft Windows SNMP Services and Traps.

Linux Prerequisites

If you are installing on Linux, you must log in as a non-root user. Linux installation prompts you to run some additional scripts as root.

When installing to Linux, ensure you are installing as a user with the correct permissions, and are in the correct group. You must configure the installation directory so this user and group have all permissions (770, at least). You may install without any universal (“world”) permissions. However, you must create a home directory for the installing user.

NOTE:

All files created during installation respect a umask of 007. All files from setup.jar are 770. Files from ocpinstall -x are set for 660. Bin scripts from ocpinstall -x are 770.

Best practice is to install as the user designated as DBA and admin of the system. If necessary, create the appropriate user and login as this user for running the install program. The installing user must have create privileges for the target directory. By default, this directory is `/opt/dorado`.

CAUTION:

Linux sometimes installs a MySQL database with the operating system. Before you install this application, remove any MySQL if it exists on your Linux machine.

NOTE:

To set the environment correctly for command line functions, after installation, type `oware` (or `. /etc/.dsienv` in UNIX—[dot][space]/etc/[dot]dsienv) before running the specified command.
Also: This application can run on any Linux desktop environment (CDE, KDE, Gnome, and so on) but the installer will only install shortcuts for CDE.

System Capacity

System requirements for each element of your system vary depending how you use it. The numbers in this guide are suggestions only, not definitive recommendations.

You should base the minimum configuration of any system on expected peak load. Typically a configuration running all elements of the application on a single server spends 95% of its time idle and 5% of its time trying to keep pace with the resource demands. If you expect your system to perform an operation that could run create, modify or delete rules on tens or hundreds of thousands of business objects, your system requirements may be much higher. See System Basics on page 27 for more specific hardware requirements.

Paths

Paths in this document are often written as Linux represents them, with foreslashes (/) rather than Windows/DOS backslashes (\). The shell command `oware` makes any shell subsequently emulate a bash shell. That means either foreslash or backslash can accurately represent path separators as they may appear, depending on whether the `oware` command has set the environment to bash emulation. Most shell commands for this application are available in Windows/DOS equivalents structured to call the emulator, then a bash script. If you have difficulty using a command line script in Windows/DOS, then try it after you have run `oware`.

NOTE:

Run command line scripts with -? to see their parameters.

CAUTION:

Do not install to paths with spaces in their names.

Installing the Application

If you are installing the software on a machine with multiple Network Interface Cards (NICs), installation prompts you to select one IP address for the system you are installing.

1 Log in as a user with administrator's permissions on the Windows machine where you want to install the software or as any non-root account on Linux.

CAUTION:
You must install to Linux as a non-root user with the permission to create directories in the selected installation path. Installing to a directory that requires root level access fails.
Also: Using the Windows login "admin" to do the installation wipes out any pre-configured "admin" permissions that come with the application. Therefore, do not use "admin" as the installing user account.

Do not install as a Windows user with a space in your name.

2 If you are installing from CD, insert it into its drive. In Windows, installation autoruns. If the installer does not appear, or if you have disabled autorun, you can run `win_install.exe` from a file manager.

To install on Linux, run `linux_install`.

A dialog appears as the Setup program initializes InstallShield. Then a Welcome Screen appears, listing the package you are about to install, and reminding you to shut down other running software (this may include anti-virus software). Click *Next*.

```
linux_install -console
```

CAUTION:
You cannot install from a directory whose name begins with @.
Also: You must extract any compressed (zipped) installation source before executing the installation.

3 Installation performs a series of system checks to verify the target system is supported. If all checks pass, the license agreement appears. You must accept the license to proceed.

4 Click *Next*.

5 The next screen lets you select the directory where the application installs. If you want to install to a different directory, type the path or click *Browse*.

After confirming the installation location, click *Next*.

6 Select the setup type from the available options.

Full Installation—Installs Application Server, database server, mediation server, and client on the host.

Client Installation—This installs client software. It does not configure the machine to run a Mediation Agent or Application Server. A subsequent screen asks you to fill in the partition where this machine is a client.

NOTE:

To allow a client to connect without multicast, add the following property to the client's `owareapps\installprops\lib\installed.properties` file.

```
OWARE.CONTEXT.SERVER.URL=jnp://[HostName]:1099
```

NOTE:

This application supports a web client. See Web Client on page 147 for specifics about how to use it and make it use secure connections.

7 If installing to a multi-homed machine (multiple NICs), choose a default IP address for use by the software. Installation automatically records this address.

You can add the following properties to `owareapps\installprops\installed.properties` to override portions of the IP selection's impacts:

```
#
# specific interface used for all NMS initiated
# communications to the network
com.dorado.mediation.outbound.address=localhost
#
# specific interface used for binding mediation
# listeners such as SNMP trap listener
com.dorado.mediation.listener.address=localhost
#
# specific interface used for all northbound
# communications to external management system(s)
com.dorado.mediation.northbound.address=localhost
```

For any property, replace the *localhost* text with the correct IP. See **Overriding Properties on page 57** for more information.

8 The next screen in the full (not client) installation lets you confirm the partition name (by default this is the hostname of the Application Server), and includes radio buttons that let you select whether to install Application Server as a service—something that runs even when you are logged off.

9 and LinuxAn installation summary appears.

10 The setup program automatically installs all of the managed system software for your hardware configuration.

11 If you are installing on Linux, you must run a setup script in a separate shell, logged in as root user. Installation prompts you to run a generated script after the install phase finishes. This script records information in case you need technical assistance and installs some files as root. Open a new shell, log in as root, and run the listed script (`$OWARE_USER_ROOT/install/root/setup.sh`).

NOTE:

This step installs some essential environment files. It no longer checks for patches (the installation does that). The contents of patch_check.log.timestamp are now embedded in setup.log.

12 When you install the embedded database server (MySql), the installer either builds the database for first time use or prompts with options if a database already exists. Building an initial database may take ten minutes or more to complete. The screen that begins database installation prompts you to set the data directory, the initial and maximum size of the database.

CAUTION:

Ensure your Linux package has not already installed a version of the embedded database. If it has, uninstall that database before proceeding. **Also:** Do not configure and/or install a database larger than the available disk space.

NOTE:

Regardless of the initial database size, post-installation configuration of Database Aging Policies (DAP) can have a significantly impact on how fast it reaches its capacity. The default DAP for alarms, for example, never cleans open alarms from the database. Similarly, defaults for archiving event history may not suit your environment. Consult the *User Guide* for details about tuning these policies.

13 The Application Server installed as a service makes a prompt appear that lets you start the service without rebooting again. If you elect to start the Application Server service, a monitor icon appears in the Windows tray (typically the bottom right of your screen) that is yellow as Application Server begins running, and green when it is up and running.

To confirm Application Server is running, you can run `pmgetstatus` in a shell where you have sourced the Oware environment (`oware` in Windows, `. /etc/.dsienv` in Linux—type `[dot][space]/etc/[dot]dsienv`). Application Server must be running before you can open the client.

14 Finally, the application prompts you to click *Finish*. This completes the installation.

NOTE:

After you complete the installation, you may want to install Adobe Acrobat Reader. An installation is included with the installation CD, or you can download a free copy from the Adobe website. This application requires Acrobat to successfully print reports.

To start the client, either use the icons in the *Start* menu (in Windows), the icon on the desktop (Linux), or type `redcell` on a command line in a shell with the Oware environment.

When you license new features, you must restart the application server and client.

NOTE:

Since disabling legacy web services enhances performance, they are disabled by default. To enable them, add the following line to `$OWARE_USER_ROOT/owareapps/installprops/lib/installed.properties:`

```
com.dorado.core.ws.disable=falso
```

If you are not using legacy web services, disabling them enhances performance.

Default users initially have no password. Users must typically change this blank password with the first login. The login for the installing user is, by default *admin*.

Passwords are stored in the database, encrypted. You can also change this password later from the *Settings -> Change Password* menu item in the application.

Starting Application Server

You can stop, start and monitor the Application Server service, with command lines (`pmstopall`, `pmstartall`, and `pmgetstatus`), or use a system tray tool for controlling Application Server. As always, run `oware` in Windows, or `. /etc/.dsienv` in Linux before running command lines.

For security reasons, `pmstopall` has a security requirements similar to `stopappserver`. Here is a sample command line:

```
pmstopall <hostname>:1099 -u <username> -p <password>
```

Both `-u` and `-p` are optional parameters. If you omit `username`, the application assumes `OWAdmin` is the user. If you omit a password, the application assumes a blank password.

This service appears in the Windows Services dialog as OpenManage Network Manager.

Installation of Process Monitor System Tray Icon

To ensure the Process Monitor System Tray icon appears each time the system is restarted simply add the $OWARE_USER_ROOT/oware/bin/pmtray.exe binary to the *all users* startup folder (`C:\Documents and Settings\All Users\Start Menu\Programs\Startup`).

Update pmstartup.dat

Finally, modify the `application.server.active=` property in `$OWARE_USER_ROOT/oware/lib/pmstartup.dat` and change the default value from `false` to `true`. Once complete, reboot the system and the application server automatically starts and the system tray icon automatically appears in the user's startup folder.

pmgetstatus

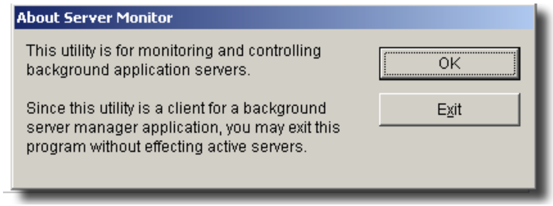
If you elect to autostart your Application Server, you can run the `pmgetstatus` script from a command line to see the status of Application Servers. If you run `oware` first in the shell where you run `pmgetstatus`, this script will automatically be on the path. Here is its usage (produced by typing the script name followed by `-?`):

```
Usage: pmgetstatus [-h <Server IP>] [-p <Server Port>] [-i <Iterations>]

[-r <Refresh Rate>]]

Oware utility for reporting status on managed server processes. By default,
   the local host is queried for 1 iteration.

Options:

   -h <Server IP>      -- Server host IP. Defaults to local host

(127.0.0.1).

    -p <Server Port>    -- Process monitor command port.

                           Default loaded from

c:/work/oware/lib/pmstartup.dat

    -i <Iterations>     -- Number of times to repeat command, -1 is

infinite (requires Ctl-C).

    -r <Refresh Rate>   -- Refresh rate of iterative command in seconds.

Default is 5.

                           Requires -i option.

    -?                  -- Show this help.
```

Windows Server Monitor

When you install your application as a service on Windows, you also install a server monitor. This monitor is a client to the server manager which controls starting and stopping of an application server.

Figure 2-1. Server Manager Client



About Server Monitor

This utility is for monitoring and controlling background application servers.

Since this utility is a client for a background server manager application, you may exit this program without effecting active servers.

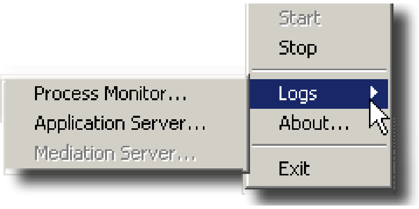
Double click the tray icon to display the about panel. *OK* closes this dialog, but maintains the icon in the tray, while *Exit* closes the Server Manager (client and tray icon).

The tray icons themselves indicate the current service condition.

Icon	Status
☒	Offline (no status available, or not controlled by server manager)
🟡	Running (initializing, or shutting down)
🟢	Ready
🔴	Stopped

You can also right-click the icon to see the client menu.

Figure 2-2. Process Monitor Client Menu



The logs item let you view logged items for Server Manager, or Application Server. You can *Start* or *Stop* the service(s) running on your host.

NOTE:

System changes can make the server monitor system tray icon disappear while the process is still running. If you cannot make your icon reappear, try running `pmtray -r` from a command line, then restart the server monitor.

Startup Properties

The values in `installed.properties` now set most properties for the process monitor to pass when starting a server. All command-line options for the `startappserver` script are now in `installed.properties` (see Overriding Properties on page 57). Command line arguments override these properties.

The following are properties you can set in `owareapps\installprops\lib\installed.properties` to configure servers:

- Default server partition name also used by client and mediation to locate a server

```
oware.client.partition.name=demo1
```

- Default interface used by servers and direct access cut-thru sessions.

```
oware.local.ip.address=192.168.0.10 [for example]
```

The IP address also appears in database connection properties:

```
com.dorado.meta_database.name=//192.168.0.10:3306/owmetadb
com.dorado.jdbc.database_name.mysql=//192.168.0.10:3306/owbusdb
```

To change the IP address, stop the server, set these properties to the new IP address and delete the content of the `oware/temp` directory. Then restart the server.

ipaddresschange

A simpler alternative to changing properties is to use the `ipaddresschange` script. If you were to install this application on a machine on one network, then move your machine to another network, the IP address from your original network remains hard-coded. You must change the application's IP address to reflect the new network for the software to function correctly. Here is how to do it, once you have connected the application server machine to the new network:

a. First, shut down the Oware Server Manager. Open a command shell (*Start -> Run* `cmd`, in Windows) then type: `net stop "Oware Server Manager"` (including the quote marks)

b. Next, find out what your new IP address is. To do this type `ipconfig` in the command shell you just opened, and make note of the IP Address that appears. You will need that number in a subsequent step.

c. Type `oware` at the command line. This sets the environment.

d. In the same shell, type `ipaddresschange -n [the IP address discovered in b]`

e. Restart Oware Server Manager by typing: `net start "Oware Server Manager"` (including the quote marks)

Your machine should then be able to connect to other devices on this network and function correctly.

NOTE:

After the utility is done, if you are using Server Monitor, its Icon in the program tray has an x through it. You must either reboot or use Windows' Administrative facility stop the oware server manager service and restart it.

- Use only https for web services and web clients

  ```
  oware.appserver.web.enable.https=false
  ```

- Set to true when there is no graphics adaptor available for server

  ```
  java.awt.headless=false
  ```

- To change the default HTTP/HTTPS port numbers for web application or web services, add the following properties to `owareapps/installprops/lib/installed.properties`:

  ```
  oware.appserver.web.http.port=[default port number:80]
  ```

```
oware.appserver.web.https.port=8443
```

You may then change the port values for these property entries and restart the Application Server. Special setup (outside the scope of this document) is necessary to run a web server on port numbers lower than 1024 on many operating systems.

CAUTION:
Do not change the system time while the Application Server is running. If you must change the system time, shut down the server before the change, and restart it afterwards.

Proactive Runtime Management

To insure OpenManage Network Manager continues to run smoothly long after you have installed it, best practice is to take the following precautions.

- Make sure you configure database archiving policies (DAPs) to suit your system, particularly if you have device messaging (typically alarms and syslog) that threaten to fill your database.
- Occasionally check the Audit Trails to ensure DAPs are running properly.
- Configure your syslog and alarm events to only catch significant ones.
- Configure devices to suppress their own messages if these messages are unimportant.

Updating an Existing Installation

Always consult the manuals and CD contents for upgrade instructions. Database changes may require a migration step to preserve your data when moving to a new version.

Best practice is to perform a complete backup of your system before attempting an upgrade. Provided you are dealing with the embedded MySQL database, some packages installs may prompt you to automatically back up the database. The wizard can also prompt you for a location. The filename is `backup.sql`.

If you do an update installation, even if you elect not to rebuild the database, installation always reseeds the system settings. If you have changed the default settings, you may want to export these before proceeding.

After files install, select whether you want the installation program to rebuild the database content, otherwise, the application keeps the existing one. The installation wizard begins copying the needed files.

If your installation fails, see `setup.log`, `db_setup.log` or `app_setup.log` in the destination directory for the installation for messages that may help fix the failure.

Cancelling the Installation

Once the installer finishes transferring files, the application is installed; you cannot cancel installation. Short of killing the installer process, you cannot cancel database initialization or component installation and seeding. The installer considers this portion of its work system configuration and not application installation so it cannot stop unless you kill the process. If you do manage to abort the install after file transfer completes (after the “creating uninstaller” message goes away), then you must run the uninstaller to remove the software.

CAUTION:

Cancellation is *not* recommended. You may strand processes that you must then manually shut down. Some directories and files would be left behind after the automatic rollback that occurs when cancelling an install.

Uninstalling

You can uninstall the software by using Windows’ control panel’s *Add/Remove programs* feature (or with `win_uninstall.exe`), or by running the following on Linux:

```
$OWARE_USER_ROOT/_uninst/linux_uninstall
```

or for console mode, run...

```
OWARE_USER_ROOT/_uninst/linux_uninstall -console -is:javaconsole.
```

NOTE:

If you uninstall in a shell rather than using the graphic uninstaller, uninstaller cannot uninstall its own directory. This produces some errors you can safely ignore in a console uninstallation. Use `cd /opt` and then `rm -rf [installation target directory]` to do final cleanup.

In graphic uninstallation, as in installation, click *Next* to continue through the screens as they appear. One such screen appears listing what you want to uninstall. Confirm that you want to remove all the listed installed components. You can optionally delete all the applications’ files and directories (complete removal).

CAUTION:

Uninstallation on MySql servers may delete the database and any application directories. The applications’ directories also contains any installed application components and device drivers.

The option to delete directories is primarily to support application developers having to uninstall and re-install the basic application platform without losing component files (like device drivers) on disk that were not part of the installation.

NOTE:

Deletion is recommended, but not required. It removes files created after installation; temp files, database files, cache files, and files extracted from OCP/DDP files. Overall, it is the best way to get a clean uninstallation. You can back up your oware/lib/*.properties files or overrides before uninstalling if you want to preserve them. An alternative is overriding properties See Overriding Properties on page 57 for more information.

When the software has been completely uninstalled on Windows, if prompted, you must reboot your computer to complete deletion of any locked files. Best practice is to reboot right away.

Uninstalling removes all installed files and files created by using the installed system (that it has permission to delete). It does *not* remove directories that were not created by this application's installation or runtime. User-created directories in the product's directory path remain after product removal.

NOTE:

Uninstaller may freeze on hosts with inadequate resources. **Also:** The uninstaller deletes uninstall.exe, if you press the cancel button. After the canceling uninstallation, several directories and files remaining on disk that require manually deletion to completely uninstall.

Stopping Servers

To stop the Application Server, you can either use the Application Server tray icon in Windows (see Starting Application Server on page 50), or stop the server from a command line. The command line to stop a server is `pmstopall`.

If you have not automated server startup, then you can use the `stopappserver` and `stopmedserver` scripts to stop these servers. Here is the syntax:

```
stopappserver <hostname>:1099 -u <username> -p <password>
stopmedserver <hostname>:1099 -u <username> -p <password>
```

Both `-u` and `-p` are optional parameters. If you omit `username`, the application assumes `OWAdmin` is the user. If you omit a password, the application assumes a blank password.

CAUTION:

Using Ctrl+C in the application server shell may stop the application server, but processes can linger which you must stop manually before you can successfully restart application server. One example occurs when the application server shell displays .... **failed to listen on trap port 162....** during startup. If this occurs, use task manager to stop WMIBeam and WMINotification processes. If such processes do not exist in task manager, reboot before starting application server.

If you have not logged in and changed the password for OWAdmin with the application's login screen the login to stop the server fails. By default, `OWAdmin` and the installing user have the role `OWServerAdmin`. Any user assigned this role can stop the appserver. Blank passwords are valid if they are defined for the user.

If you used `startappserver` in a shell to start the Application Server, you can stop the server by either interrupting that shell with Ctrl+C or by closing the shell. Ultimately, you can kill the Java processes on your machine to halt a server.

See Updating an Existing Installation on page 54 for additional notes about shutting down processes and services. If you uninstall when a server is active, the uninstallation will attempt to shut it down and failing that will prompt you to shut it down manually.

Linux Command Line Installation

You can run a Linux installation from a command line with text prompts that are equivalent to the graphic interface prompts described in Installing the Application on page 47, and the following pages. Here is the command line to run the text-only installation:

```
install/linux/linuxinstall -console
```

Modified Files

The following system files may be modified during root installation:

```
/etc/.dsienv - installed
/etc/my.cnf - installed
/etc/rc2.d/S75owaredb – installed
/etc/rc2.d/S76oware – installed
```

The rest of the installation installs program files, does the setup functions, and performs the initial database load.

Overriding Properties

Installation typically makes all of the modifications needed to properties files, but if your installation customizes some properties, best practice is not to change default properties, but to override them. This eliminates updates or new installations overwriting property files you have configured. Best practice also includes backing up the override file(s) as described below.

To override a property, put the property itself in `installed.properties` under `owareapps\installprops\lib`. You can override selected (high availability) mediation service properties in `owareapps\installprops\medserver\lib`. Application property values are loaded first and you can override those values here.

NOTE:

Installation updates or refreshes the appropriate properties in installed.properties, but does not overwrite the file. This means property additions you make are safe from installation changing them in this override file. New properties coming from an installation are appended to the files.

The following is an example of property file content to override an application

cache time-out:

```
#=============================================
# Dependencies
#=============================================
product.dependencies=redcell

#=============================================
# Application Overrides
#============================================
# set event template cache timeout to 1 minute
redcell.assurance.batch.processing.event.template.cache.expiration=60000
```

CAUTION:
If any of the dependency directory names (for example, `owareapps/redcell`) do not exist, then the application does *not* load override file.

Consult the comments in the properties files you are overriding for further information about specific properties.

Properties Loading

First the application loads all property files from the application (`/oware/lib`). Then it loads all property files from `owareapps\*\lib` (on the mediation service this is from `owareapps\*\med\lib`). A special property `product.dependencies` that lets you control the order that files are loaded. For example setting `product.dependencies=myApp` makes `owareapps` properties (other than myApp) load after myApp. The product name for this property is the name of the directory under `owareapps`. You can also specify multiple products with a comma (,) delimited list.

Prepend and Append Keywords

One reason to have dependent property loading is to modify a property used by another product. You may need to ensure that your value comes after the other products, or vice versa. When Java reads properties, its default behavior is to override the old value with the new when encountering an identically-named property. This would compel product maintainers to change a product whenever property file changes occurred in the product on which they depend. Such maintenance would increase geometrically, especially with multiple dependencies.

This application supports property appending or prepending through keywords. If you preface the property to be modified with append. or prepend., you can put your own value after or before the original property's value(s). You must be aware of the original property's delimiters and either add one at the beginning of your value if appending, or add one at the end of your value if prepending. For example: Given a pre-existing property: `oware.foo=original`

```
append.oware.foo=,newappend
```

This produces `oware.foo=original,newappend`

```
prepend.oware.foo=newprepend,
```

This produces `oware.foo=newprepend,original`

If the original property is null, the first character (if appending) or last character (if prepending) is stripped (to eliminate the separator) and the property created with the resulting value. Currently, properties permit only one instance of a keyword within a given property file.

Ports Used

This application uses the following ports. Ensure your firewalls or other network security measures do not block these ports.

Port Number	Used by...
1098	Naming service (JNDI)
1099	Naming service (JNDI)
3100	HA Naming Service (JNDI)
3200	HA Naming Service (JNDI RMI)
4444	JRMP invocation (RMI)
4445	Pooled JRMP invocation (RMI)
6500 to 6510	Mediation cut-through
80	HTTP
443	HTTPS
8093	JMS

The client HTTP cut-through goes directly to the device from the client. So, you must get to devices via port 8080 to cut-through to the embedded web server. Telnet cut-through goes directly to the application server as a proxy on ports 6500-6510.

The following ports are seldom required, but are listed here in case present or future functionality requires them:

Port	Used by...
23	Telnet
1103	JNP Discovery
1123	JNP REPLY

Linux Partition Information

Suggested partitioning includes separation into several partitions including /, swap, /usr, /opt, and /export/home.

- / **(root)**—The root partition contains everything that is not specifically placed on a slice/partition. The rule of thumb here is: Do not put data on this partition that is likely to grow significantly (logs, applications, data, and so on). This partition can be as little as 200MB, however best practice indicates as much as 2GB if space is available.

- **swap**—swap is the space allocated for the operating system to use as part of its virtual memory to augment physical memory. If something in memory has not been used for a while, the operating system will move it to disk temporarily. Recommendations for this are typically for two to three times the physical memory, however we usually determine the amount available based on physical memory. If you have 512MB, specify 1.5-2.0GB. As physical memory increases, still specify 1-2 times the physical memory so you have enough disk space for the operating system. The following are instructions about setting swap:
  a. Check your current swap space setting with `swap -l`

  b. su to root (if not already).

  c. Issue `mkfile (size required) (filename)`

  d. Execute `swap -a (pathname)`. this adds the swap file. You *must* use an absolute path name

  e. Check with `swap -l` to confirm the new swap addition.
- **/usr**—Typically holds operating system commands and utilities related to the operating system. `/usr` can also contain the documentation associated with these commands. This partition should be a minimum of 1.5GB for a full installation. Best practice is to specify 2GB and potentially more if you know you will be adding operating system utilities.
- **/etc**—We recommend this be located on the root partition, not on its own partition. The data here may change from time to time, but the typically does not grow significantly.
- **/var**—Best practice is to create a partition for `/var`. This contains the syslog data, print spool, mail, and so on. This partition could grow significantly from the required amount of disk space depending on the applications running on the system. We recommend you allow at least 2GB.
- **/opt**—The `/opt` partition holds application software that is added to the system. OpenManage Network Manager would be an application that should be installed here. The size of this partition should depend on the required disk space for applications including OpenManage Network Manager. Both the application's software and data reside in the same directory structure, however, so you can add more volumes to another partition.
- **/export/home**—`/export/home` is typically for user data. Most systems have user home drives specified in this space (for example: `/export/home/auser`). This should have enough space for all user data.
- **/<some_partition_name>**—With a RAID configuration, you can specify a large amount of disk space for data purposes.

You must also enable process monitor with the appropriate property set to `true` in `oware/lib/pmstartup.dat.` The property relates to either application server (`application.server.active=true` or `false`) or mediation server (`mediation.server.active=false` or `true`), not both.

Web Client on UNIX Systems

Xvfb must be running to have a web client work correctly. This is automated when you have application server start automatically. Confirm `xvfb` is running as follows:

```
>ps -ef | grep Xvfb

root 14860 14855 0 12:14:36 pts/3 0:00 /usr/X11R6/bin/Xvfb :1 -screen 0
   1152x900x8

dorado 16099 14502 0 14:51:24 pts/1 0:00 grep Xvfb
```

This is an example; the path that appears when you grep depends on your operating system.

Managing the Runtime Environment

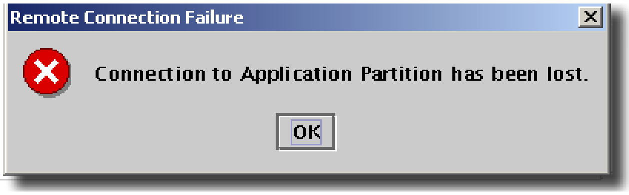
Runtime Requirements

This application runs as a thin client. It gets services from an application server, which must be up and running before any clients start.

Application Server

Clients do not run if they cannot connect to an application server. Instead, a warning appears and the clients shut down.

If a client loses connection to the application server (for example, if the application server restarts) a *Connection Lost* dialog appears. Click *Re-start* to reestablish the connection to the application server.



Remote Connection Failure

Connection to Application Partition has been lost.

When the Application Server finishes loading, the application server log displays `Rule Load Complete`. After you see this message you can start clients.

NOTE:

Clients may need two or three minutes to reestablish an application server connection if the server fails and goes down. You can also restart clients to reconnect them to the application server.

Server Options

Application server can run from a command line that lets you start up with several options. Consult Chapter 8, The Application Server for details.

Configuring the Server

Configuring the application server typically occurs during or immediately after its installation. Application server configuration settings are in `oware\lib` in the files `owappserverstartup.properties` and `owappserver.properties`, and you can edit these with any text editor. See Overriding Properties on page 57 for more information about configuring application server. See Chapter 6, Properties for additional details. See also the results of `startappserver -h` from a command line for additional command line options.

JMX Console

The JMX Console is a management tool to assist in fine-tuning the application's JMS environment. Once your application server is running, access this console in a browser at this URL: `http://localhost:8080/jmx-console.`

Mediation Service

The Mediation Service provides an interface to external systems and devices. Mediation Services come from one or more Mediation Agents. In a single host installation, application server typically also starts the mediation service.

Except for authentication (logins and passwords for devices) and connectivity to the managed network, device drivers automate most mediation configuration. For example, if you want to manage XYZ devices, connect your hardware to the network with those devices and install the application's XYZ device driver (XYZ is an example, not a real driver). You supply the login and password for those devices during device discovery.

NOTE:

Dell Device drivers are automatically installed with the application. Other types of device drivers are available too.

Default external protocols supported can include:

- General ASCII
- TL1
- SNMP
- Web Services
- ICMP
- MML
- Partial Q3

A Mediation Agent contains Managed Beans (MBeans) that manage the physical connections to a mediation target system or device. Connections might include communications with serial port devices, telnet sessions, TCP sockets, and external databases. The mediation agent executes dialogs with the mediation target (at the instruction of the client application) to retrieve and/or send data with the connection.

The Mediation Agent is essential for all operations involving communications with external systems and devices. If one is not running, you can still make administrative changes to the system, but it processes no traps or other external communication.

Database Timeout

When managing large networks or equipment with many interfaces, you may have to increase `the com.dorado.bom.lock_timeout` property in `owdatabase.properties`. Increase this setting based on the size of the equipment being managed. Generally, you should set this value to the maximum number of interfaces you expect your network elements to have. For example, if the element is expected to have 500 logical interfaces then the timeout value should be set to 500.

NOTE:

The minimum recommended timeout value is 60 seconds.

Client Logging

This application preserves the client log files by appending the user id and current timestamp to the log file name (otherwise files would be overwritten).

As a result, client log files are never overwritten; they accumulate in the log directory (`owareapps\redcell\logs`). Therefore, you must periodically clean up client logs files. The `client-log4j.xml` file in `owareapps\redcell\lib` directory controls the filename for the client log. By default, it contains the following setting:

```
${oware.user.root}/owareapps/redcell/logs/client-
   ${com.dorado.redcell.RCSessionId}.log
```

Here, `com.dorado.redcell.RCSessionId` is the user id and timestamp (`admin-1056133530200` for example). If you do not want to preserve the log file for each client session and want to overwrite the previous log file then modify the above line to -

```
${oware.user.root}/owareapps/redcell/logs/client.log
```

This means you do not need to periodically clean up log files.

Other Logging

The *getlogs* script is now included with your software. It creates a `logs.jar` file in the root installation directory, and moves any existing copy of `logs.jar` to `oware\temp`. This jar compresses all logs necessary for troubleshooting. Read the jar yourself, or forward this jar to technical support to help troubleshoot.

When troubleshooting (or contacting technical support), you may find pertinent information in logs located in the following directories:

```
..\oware\jboss-<version number>\server\oware\log

..\oware\temp\soniqmq.log

..\app_setup.log

..\db_setup.log
```

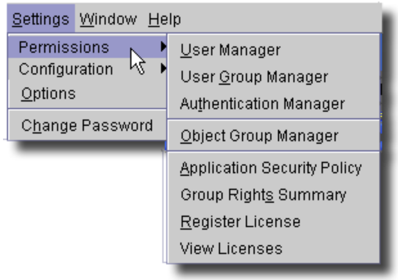
4

Security

Security Overview

This application enforces security several ways, including permissions, authentication, and security policies. The various Managers and interfaces that set and view security settings appear in the Permissions submenu, shown below. Access it by selecting *Settings* -> *Permissions*.

Figure 4-1. Permissions Submenu



You can also create resource roles (from *File* -> *Open* -> *Inventory* -> *Resource Roles*, see *Chapter 15*, *Resource Roles* for details). For each resource role the application automatically creates an object group and puts any resources in the role in that object group. You can then give users or user groups permissions against that object group.

CAUTION:

All users inherit OWPublic's permissions. You must remove OWPublic's read permissions from things in Object Group Manager to conceal those items.

Also: Functional permissions originate with users and user groups, and are application-wide. See Permissions on page 74 and All Permissions on page 76. When concatenated with other permissions they are additive (unions, not intersections).

Best practice when trying to restrict user access to particular functions is to create a user group (see User Group Manager on page 77), and assign the desired functional permissions to that group, then assign users (see User Manager on page 69) to that group.

Security Events

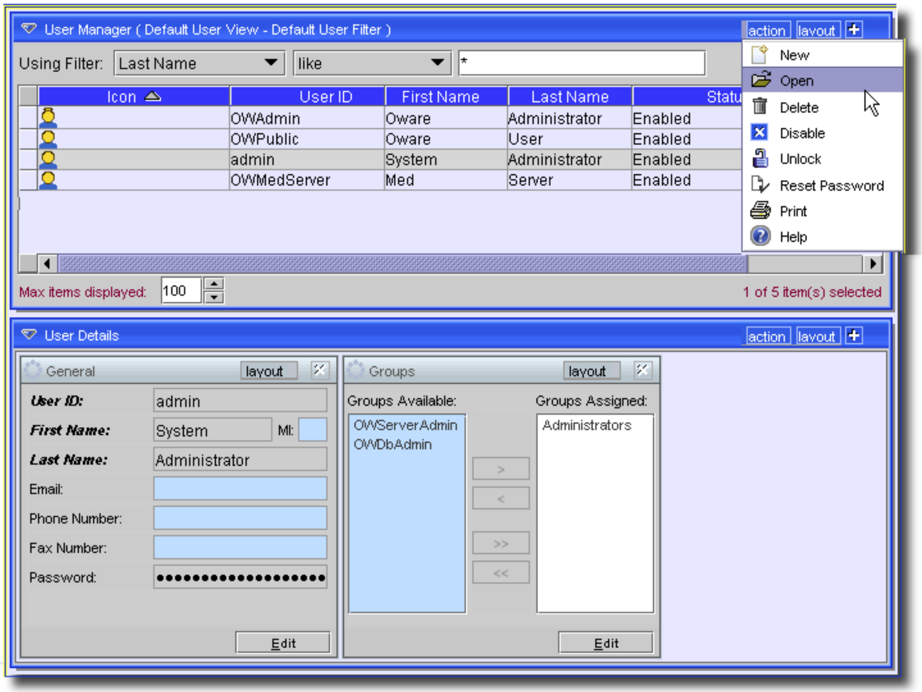
This application emits security events. The base security event is *OWSecurityEvent*. Here are the rest of the Security Events, with comments where their title does not make their function self-evident:

- **OWSecurityAccountResetEvent**
- **OWSecurityClientTerminationEvent** — Success of previous event request, emitted just before client termination.
- **OWSecurityLoggedOnEvent** — Response to previous event's request; user monitor listens to build list of active clients.
- **OWSecurityLogoffEvent**
- **OWSecurityLogonEvent**
- **OWSecurityPasswordChangeEvent**
- **OWSecurityPasswordResetEvent**
- **OWSecurityRequestEvent** — The base class extended by all OWSecurity* RequestEvents.
- **OWSecurityResponseEvent** — Base class extended by all non-OWSecurity*
- **OWSecurityUserDisabledEvent**
- **OWSecurityUserLockedOutEvent**

User Manager

The application's User Manager, shown below, lets you create and manage users, and associate information with them like passwords, group membership, and contact information. Select *Settings* -> *Permissions* -> *User Manager* to display the User Manager.

Figure 4-2. User Manager



User Manager (Default User View - Default User Filter)

Using Filter: Last Name like *

Icon	User ID	First Name	Last Name	Statu
	OWAdmin	Oware	Administrator	Enabled
	OWPublic	Oware	User	Enabled
	admin	System	Administrator	Enabled
	OWMedServer	Med	Server	Enabled

Max items displayed: 100

1 of 5 item(s) selected

User Details

General

User ID:	admin
First Name:	System
MI:	
Last Name:	Administrator
Email:	
Phone Number:	
Fax Number:	
Password:	•••••••••••••••••••

Groups

Groups Available: OWServerAdmin
OWDbAdmin

Groups Assigned: Administrators

The User Manager displays the *User ID*, *First* and *Last Name*, *Status* (enabled or disabled) and whether the user is *Locked Out*. The detail panels at the bottom of the screen display those for the selected user. They also display which groups the user belongs to of those available on the system.

Use the *Max Rows* field to limit the number of records that appear at once on screen. You can also filter the display to show a select subset of users, and can sort so users appear in the order you like.

Select a filter parameter (*UserID*, *Last Name*, *Groups*) from the top of this screen, enter the corresponding search text in the text field, and click *Go*.

Click on any column header to sort the display based on that column's contents. The initial click sorts the column in ascending order; the next click sorts in descending order. Subsequent clicks toggle the sort between ascending and descending.

The User Manager has these controls:

- **New** — Opens a dialog where you can add new users to the system. See Adding or Modifying a User on page 71 for more information.

NOTE:

Best practice is to add new users rather than making changes to administrative privileges.

- **Open** — Opens an edit dialog populated with the information for the selected user. See Adding or Modifying a User on page 71 for more information.
- **Delete**—Removes the selected user from the list (and the application).
- **Disable** — Prevents the selected user from logging on to the application by setting the user's Expiration Date to the current date.
- **Unlock** — Releases the lock on the selected user. (Locks are indicated by an entry in the *Locked Out* field.) Users are locked out if they try to log in with an incorrect password too many times (default = 4). When this happens the date and time of lock out appears in the *Locked out* column. Administrators can configure the number of attempts allowed users before they are locked out (see Login Policy on page 100).

  Unless otherwise configured, locked-out users cannot gain entry into the system until an administrator releases their locks. Unlocking a locked-out user lets the user's previous password work. Lock out lasts for a configurable amount of time (see Lockout Period on page 102), and by default, the lockout eventually expires regardless of whether an admin unlocks the account.
- **Reset Password** — Checks the *Force Password Change* checkbox in the user editor. This requires the selected user to change the password on the next login.

NOTE:

OWAdmin without any password exists by default as an alternative user with administrative privileges. If you want your installation to be extremely secure, delete this user, but understand that you will have to re-install if other, authorized administrators cannot log in for some reason.

- **Print** — Create an Acrobat file of the users that appear in the (filtered) list. You must have the free Acrobat reader installed for this work correctly.
- **Help** — Opens the online help for this screen.

Default Users

Installation automatically seeds the following users

- **OWMedServer**—An internal user (principal) used by the system. You can neither log in with this account nor delete it.
- **OWPublic**—An internal user that provides base permissions across all users. You can neither log in with this account nor delete it.

- **<installing user>**—The installing user is seeded during database creation during installation (not for client installations). The login is the operating system's name for the installing user. You can neither log in with this account nor delete it.

- **OWAdmin**—A seeded administrative account. You can log in with this account, and cannot disable it, but you can change its password. You cannot delete this account.

- **admin**—A seeded administrative account, which is the core application component. You can login using this account. You cannot disable this account, but you can change the password. You cannot delete this account.

Adding or Modifying a User

Click *New* to create a new User, or select an existing user and click *Open* to modify that user's properties. A User Editor appears with the following panels:

- General
- Permissions
- All Permissions

NOTE:

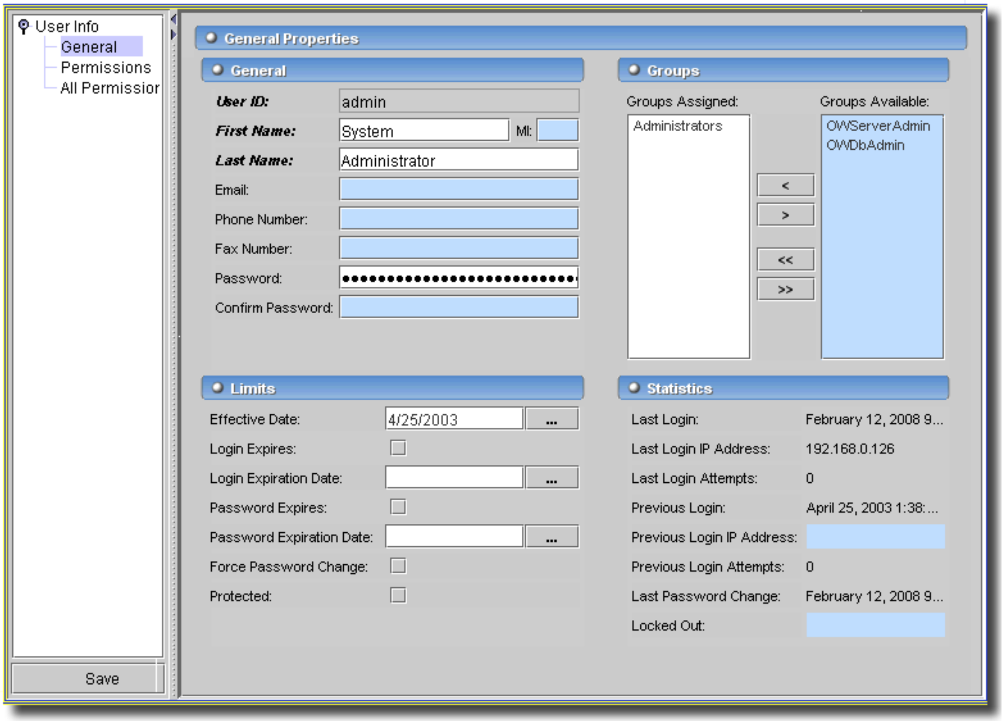
Windows user names should contain neither an apostrophe (') nor a space.

In addition to the user characteristics, you can associate the user with a Group and confer that group's set of permissions to the selected user.

General

The General tab lets you enter and edit identifying and contact information for the selected (or newly created) user.

Figure 4-3. User Manager: General Tab



User ID: admin

First Name: System MI:

Last Name: Administrator

Email:

Phone Number:

Fax Number:

Password: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Confirm Password:

Groups Assigned: Administrators

Groups Available: OWServerAdmin, OWDbAdmin

Effective Date: 4/25/2003 ...

Login Expires: □

Login Expiration Date: ...

Password Expires: □

Password Expiration Date: ...

Force Password Change: □

Protected: □

Last Login: February 12, 2008 9...

Last Login IP Address: 192.168.0.126

Last Login Attempts: 0

Previous Login: April 25, 2003 1:38:...

Previous Login IP Address:

Previous Login Attempts: 0

Last Password Change: February 12, 2008 9...

Locked Out:

The following are the fields on this tab (described when not self-evident):

General

- **User ID** — (Required) Enter an ID for this user. If you are modifying an existing user, this field is read-only. The User ID must be unique; if it matches an existing User ID, the application generates an error.
- **First Name** — First Name
- **Middle Name** — Middle Name
- **Last Name** — Last Name
- **Email** — Primary Email
- **Phone Number** — Select a phone number type from the drop-down list, then enter a phone number for the selected user.

- **Fax Number** — Select a fax number type from the drop-down list, then enter a fax number for the user.
- **Password** — (Required) Enter the password for this user. For security purposes, the characters appear as a series of asterisks. The default security does not require the password to contain mixed-case letters, numbers, or special characters. Once a user has been created, this field becomes read-only.
- **Confirm Password** — (Required) Re-enter the password for this user. If this entry does not match the Password entry, an error dialog appears and both password fields empty.

Limits

- **Effective Date** — (Required) The date when this account becomes effective. This field lets you create accounts in advance. The accounts remain dormant until the Effective Date arrives.
- **Login Expires** — Indicates whether the login for this user expires. If you select this option, the application activates the Expiration Date field.
- **Expiration Date** — Specifies the date on which the login expires. This field is not active unless you select the Login Expires option.

  Specify an expiration date by entering the date directly in the text field, in the proper format (by default: month/day/year). You can also click the Command button (...) and select a date from the calendar graphic that appears.

  If a user is disabled, typically by login failure, the Expiration Date becomes the current date. The user cannot log in again until you reset the Expiration Date to some future date or clear the *Login Expires* option.
- **Password Expires** — When selected, this option sets an expiration policy for the password of the associated user. If you set password expiration, you must set an expiration date. If you do not set password expiration, the password for this user never expires.
- **Password Expire Date** — This field is active only if you selected the *Password Expires* option.
- **Force Password Change**— The selected user must change the password on the next login.

Groups

The Groups portion of this screen lets you determine which user groups, if any, to associate with a user (see User Group Manager on page 77 for information about how to create the groups that appear here). Since you grant permissions to defined groups, you can grant or deny users access to certain functions based on their group associations.

Available groups appear in the left tab, and groups currently assigned to the selected user appear in the right tab. Use the controls in this tab to assign groups to or remove assignments from the current user.

Statistics

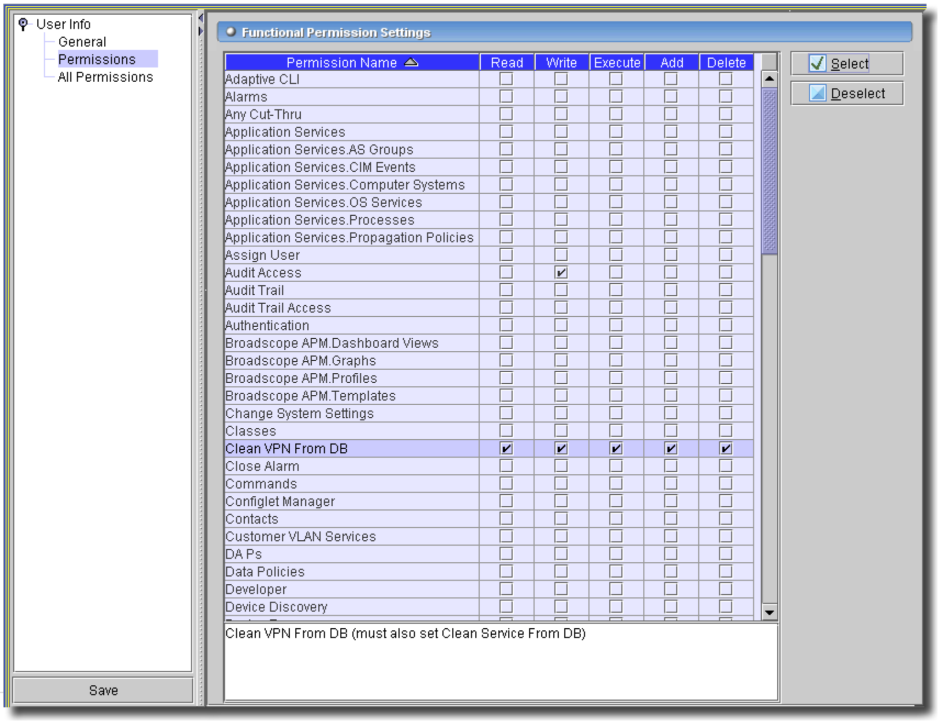
This portion of the screen displays statistics for the selected user.

- **Last Login** — The time and date of this user's last login.
- **Last Login IP Address** — The IP address of the host for this user's last login.
- **Last Login Attempts** — The number of attempts this user made when last trying to log in.
- **Previous Login** — The time and date of this user's previous login.
- **Previous Login IP Address** — The IP address of the host for this user's previous login.
- **Previous Login Attempts** — The number of attempts this user made when previously trying to log in.
- **Last Password change**— The time and date of this user's last password change.
- **Locked Out**— The time and date of lockout.

Permissions

This panel lets you configure permissions (also known as "functional permissions") for individual users which override those configured for groups (see Adding or Modifying a Group on page 78). The permissions displayed in this screen are only those of for the selected, individual user. To see the combined group and user permissions, see the All Permissions panel.

Figure 4-4. Functional Permissions



Permission Name	Read	Write	Execute	Add	Delete
Adaptive CLI	□	□	□	□	□
Alarms	□	□	□	□	□
Any Cut-Thru	□	□	□	□	□
Application Services	□	□	□	□	□
Application Services.AS Groups	□	□	□	□	□
Application Services.CIM Events	□	□	□	□	□
Application Services.Computer Systems	□	□	□	□	□
Application Services.OS Services	□	□	□	□	□
Application Services.Processes	□	□	□	□	□
Application Services.Propagation Policies	□	□	□	□	□
Assign User	□	□	□	□	□
Audit Access	□	☑	□	□	□
Audit Trail	□	□	□	□	□
Audit Trail Access	□	□	□	□	□
Authentication	□	□	□	□	□
Broadscope APM.Dashboard Views	□	□	□	□	□
Broadscope APM.Graphs	□	□	□	□	□
Broadscope APM.Profiles	□	□	□	□	□
Broadscope APM.Templates	□	□	□	□	□
Change System Settings	□	□	□	□	□
Classes	□	□	□	□	□
Clean VPN From DB	☑	☑	☑	☑	☑
Close Alarm	□	□	□	□	□
Commands	□	□	□	□	□
Configlet Manager	□	□	□	□	□
Contacts	□	□	□	□	□
Customer VLAN Services	□	□	□	□	□
DA Ps	□	□	□	□	□
Data Policies	□	□	□	□	□
Developer	□	□	□	□	□
Device Discovery	□	□	□	□	□

Clean VPN From DB (must also set Clean Service From DB)

Configure permissions by checking the actions that appear in the row with the permission. These determine a user's capabilities within the application.

NOTE:

The description in the lower panel also may indicate additional dependencies to take into account when configuring your permissions.

Generally, the following describes the effects of enabling these actions:.

Action	Default Behavior
read	When checked, this enables the *Edit* menu item on the action menu.
write	When checked, this enables the *Save* button within editors.
execute	When checked, this action lets you launch a particular manager and query for elements. Alternatively this action can control a specific application function, (typically described by the permission name) like provisioning a policy

Action	Default Behavior
add	This enables the *New* menu item on the action menu. If you do not check this action, then the *New* menu item does not appear.
delete	When checked, this enables the *Delete* menu item on the action menu within managers.

The functional permissions that use these actions—and their descriptions—appear in this screen. The description appears at the bottom of the screen when you select a permission's row.

You can click individual checkboxes classified by the columns for listed functional permissions' rows, or Ctrl+click to select entire rows or ranges of rows, and click the *Select* or *Deselect* buttons to check or uncheck all the actions in the row(s) selected.

Functional Permission Descriptions

You can configure the Functional Permission labels and descriptions that appear at the bottom of the Permissions screen (but not in the All Permissions screen). Do this in the `rcmsgs.properties` file in `owareapps\redcell\lib`. Messages there appear in two lines, configuring the label for the permission, and its description. For example:

```
Permission-AC.AdaptiveCLI.1=Adaptive CLI
Permission-AC.AdaptiveCLI.2=Adaptive CLI Editor and Manager Permissions
```

To alter either the label for a permission (line 1) or its description (line 2) simply edit this file with your favorite text editor, save it, then restart application server.

CAUTION:
Entries cannot contain special characters, and must be on a single line.

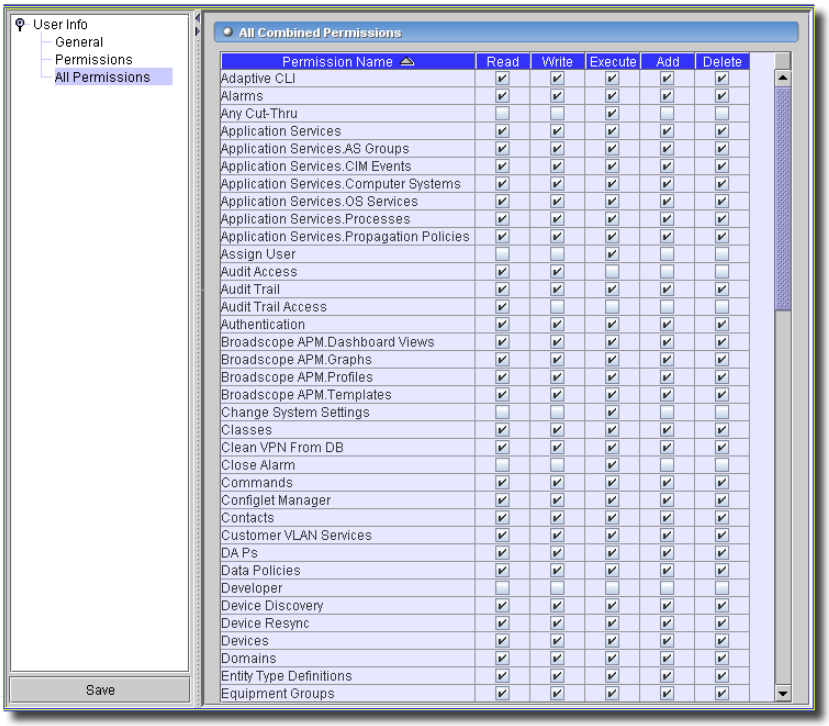
NOTE:

Functional permissions are cached on the client. Changes to permissions may take, by default, up to five minutes to be reflected on a running client.

All Permissions

This screen is like Permissions, and includes the union of permissions assigned an individual, and those assigned groups as described in Adding or Modifying a Group on page 78.

Figure 4-5. All Permissions



All Combined Permissions

Permission Name	Read	Write	Execute	Add	Delete
Adaptive CLI	☑	☑	☑	☑	☑
Alarms	☑	☑	☑	☑	☑
Any Cut-Thru	□	□	☑	□	□
Application Services	☑	☑	☑	☑	☑
Application Services.AS Groups	☑	☑	☑	☑	☑
Application Services.CIM Events	☑	☑	☑	☑	☑
Application Services.Computer Systems	☑	☑	☑	☑	☑
Application Services.OS Services	☑	☑	☑	☑	☑
Application Services.Processes	☑	☑	☑	☑	☑
Application Services.Propagation Policies	☑	☑	☑	☑	☑
Assign User	□	□	☑	□	□
Audit Access	☑	☑	□	□	□
Audit Trail	☑	☑	☑	☑	☑
Audit Trail Access	☑	□	□	□	□
Authentication	☑	☑	☑	☑	☑
Broadscope APM.Dashboard Views	☑	☑	☑	☑	☑
Broadscope APM.Graphs	☑	☑	☑	☑	☑
Broadscope APM.Profiles	☑	☑	☑	☑	☑
Broadscope APM.Templates	☑	☑	☑	☑	☑
Change System Settings	□	□	☑	□	□
Classes	☑	☑	☑	☑	☑
Clean VPN From DB	☑	☑	☑	☑	☑
Close Alarm	□	□	☑	□	□
Commands	☑	☑	☑	☑	☑
Configlet Manager	☑	☑	☑	☑	☑
Contacts	☑	☑	☑	☑	☑
Customer VLAN Services	☑	☑	☑	☑	☑
DA Ps	☑	☑	☑	☑	☑
Data Policies	☑	☑	☑	☑	☑
Developer	□	□	□	□	□
Device Discovery	☑	☑	☑	☑	☑
Device Resync	☑	☑	☑	☑	☑
Devices	☑	☑	☑	☑	☑
Domains	☑	☑	☑	☑	☑
Entity Type Definitions	☑	☑	☑	☑	☑
Equipment Groups	☑	☑	☑	☑	☑

This screen typically displays more checked permissions than the Permissions screen, since it shows the combination of User and Group permissions.

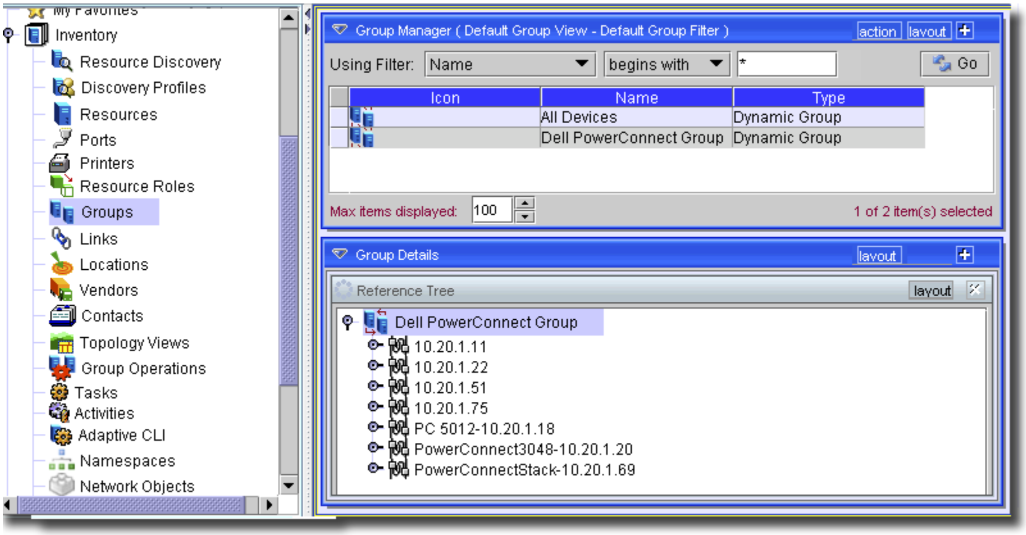
NOTE:

This screen appears only for individual users, not groups. You also cannot see the permission descriptions on this screen. For that, return to the Permissions screen.

User Group Manager

The User Group Manager lets you create user groups (see User Manager on page 69 for instructions about creating users themselves). The detail panels display the name, description and whether the group is protected. Open this manager from *Settings -> Permissions -> User Group Manager*. Initially, a Group is nothing more than a name and a description.

Figure 4-6. User Group Manager



Using Filter: Name begins with *

Icon	Name	Type
	All Devices	Dynamic Group
	Dell PowerConnect Group	Dynamic Group

Max items displayed: 100

1 of 2 item(s) selected

- Dell PowerConnect Group
  - 10.20.1.11
  - 10.20.1.22
  - 10.20.1.51
  - 10.20.1.75
  - PC 5012-10.20.1.18
  - PowerConnect3048-10.20.1.20
  - PowerConnectStack-10.20.1.69

Click *New* or select a group and click *Open* to modify a group. See *Adding or Modifying a Group* for a description of the editor. To remove a group, select it, then select *Delete*. You cannot delete some groups; for example, you cannot delete Administrators. Select *Copy* to duplicate an existing, selected user group. See Copying a User Group on page 79 for more about this process. You must re-name copied groups. Clicking *Help* opens context-sensitive help for this screen.

Once created, however, you can associate individual users with groups, and grant permissions to users based on their association with a group. By default, new groups have no permissions.

Adding or Modifying a Group

Adding groups and modifying groups are similar operations using the same interface.To add a new group, Click *New...* To modify an existing group, Select the group in the Group Manager and Click *Open...*

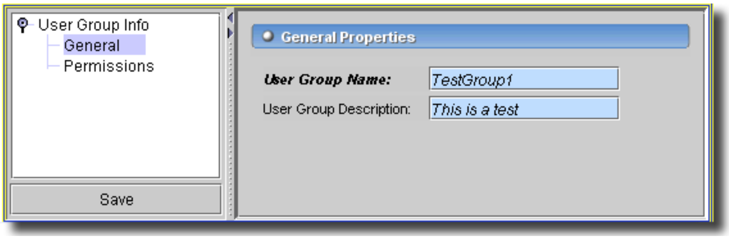
In both cases, an editor dialog appears. If you are editing an existing group, the dialog contains the information for that group. If you are creating a new group, the dialog is blank. The group editor contains two panels:

- General
- Permissions

General

This screen lets you label or describe a group

Figure 4-7. Group Editor



User Group Name: TestGroup1

User Group Description: This is a test

Enter or modify the appropriate information in the Group Editor's fields and click OK to save the entry. The following are the fields in this dialog:

Name — The name of the group (read-only if editing, rather than creating). This entry is required, and must be unique.

Description — A description of the group. This entry is optional.

Permissions

Use this screen as described in Permissions on page 74. Permissions (also known as "functional permissions" for individual users override those entered here, however best practice is to create only groups rather than individuals with overrides.

Copying a User Group

Currently in this application manages Device Authentication Configurations separately from User Groups. When you copy a user group like *Administrators*, the User Group manager does not coordinate Device Authentication Configurations that refer to the Administrators group.

For a new User Group to have access to existing devices you must manually add them to the approved groups list in the Authentication Configuration.

To do this, follow these steps for each device.

1 Open the Authentication Manager with the menu item *Settings* -> *Permissions* -> *Authentication Manager*.

2 Right click, or use *action* -> *Open* once you have selected the authentication credentials for the device you want the new group to access.

3 Select the User Group node and click *Add* in that screen.

4 In the subsequent screen, select the new group you want to add and click *OK*.

5 Click *Save* to save your Changes.

When you make a copy of any OpenManage Network Manager user group, you only copy a set of the current permissions. If an upgrade introduces new permissions, the copy is not updated; only OpenManage Network Manager seeded groups get updated.

Default Role and User

By default, a role (user group) and two users exist when you install your application. Here are the defaults:

- **Role**: Administrator

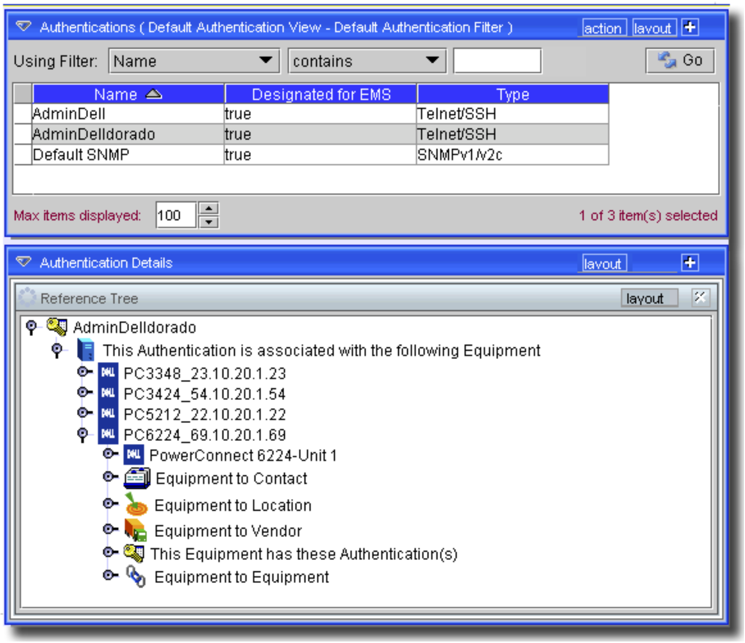
User: admin (a case-sensitive login).

Windows installations create a user with the same name as the login for whoever did the installation. This user is not attached to any role. It is also often unused.

Authentication Manager

The Authentication Manager lets you create and manage Authentication Objects, and, in the detail panels in its lower half, displays the devices associated with those authentications. These authentication objects let the application establish a set of credentials for various network elements, including login IDs and passwords. These restrict access to certain functions and/or information to authorized users.

Figure 4-8. Authentication Manager



Authentications (Default Authentication View - Default Authentication Filter)
action
layout
Go
Authentication Details
layout
Reference Tree
layout

Using Filter: Name contains

Name	Designated for EMS	Type
AdminDell	true	Telnet/SSH
AdminDelldorado	true	Telnet/SSH
Default SNMP	true	SNMPv1/v2c

Max items displayed: 100

1 of 3 item(s) selected

- AdminDelldorado
  - This Authentication is associated with the following Equipment
    - PC3348_23.10.20.1.23
    - PC3424_54.10.20.1.54
    - PC5212_22.10.20.1.22
    - PC6224_69.10.20.1.69
      - PowerConnect 6224-Unit 1
      - Equipment to Contact
      - Equipment to Location
      - Equipment to Vendor
      - This Equipment has these Authentication(s)
      - Equipment to Equipment

As with most managers, you can filter the authentication objects listed with the Filter at the top of the screen. Right click a listed authentication object, or click the *Action* button to display the following menu items:

- **New**—Opens an editor (see Creating and Modifying Authentication Objects, the next section).

- **Open**—Edits a selected authentication object (see Authenticator Editor on page 82).

- **Print**—Create an Acrobat report of the items displayed in the inventory (change the filter and click *Go* to change this display). You must have the free Acrobat reader installed for this to function. See Adobe's website to download and install this application.

- **Delete**—Removes the selected authentication object from those listed.

- **Import / Export**—This appears in the menu accessible in the *Action* button, and imports / exports information about all authentications as a text file. Exported files can serve as backups or as seed files, and can be imported by clients running on other servers.

CAUTION:
The exported file exposes passwords in plain text.

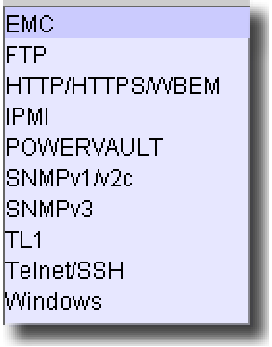
NOTE:
This report limits the number of columns to those that can fit on a single page width.

- **Help**—Opens the help for this screen.

Creating and Modifying Authentication Objects

The process for creating and editing Authentication Objects is similar to other managers: click *New* to create a new object, or select an existing object from the list and click *Open* to modify it. Delete an object by first selecting it and then clicking *Delete*. See the Authenticator Editor on page 82 for specific details about the entries associated with authentication objects.

Figure 4-9. Authentication Type



NOTE:
The types that appear in this dialog depend on the installed device drivers.

When performing deep discovery, you must typically have the correct device driver installed and at least one authentication object (for example: an SNMP authentication object specifying a public read community). If you want to interact with a device using a command-line interface (like Telnet), you must create a Telnet/SSH authentication object.

Authenticator Editor

The Authenticator Editor is the interface where you create and modify authentication objects. It contains the following pages: *General*, *Equipment*, and *User Groups*. The General page is different, depending on the Authentication Type. These types include:

- EMC
- FTP
- HTTP/HTTPS/WBEM
- SNMP v1/v2
- SNMP v3
- Telnet / SSH
- Windows

NOTE:

The Audit section of this manager catalogs actions in which the application used the authentication.

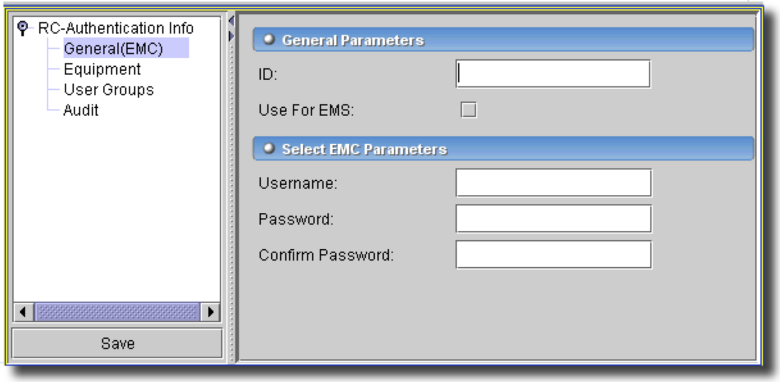
NOTE:

Check the *Use for EMS* checkbox in your authentications. This lets the entire element management system (EMS) use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them. This is necessary for other (non-admin) users to do discrete configuration.

EMC

Configure authentication for EMC in this screen.

Figure 4-10. General (EMC) Page



General Parameters

ID:

Use For EMS: □

Select EMC Parameters

Username:

Password:

Confirm Password:

Enter the following fields:

General Parameters

- **ID**—The EMC authentication object name.

- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them.

  If none of the associated credentials are marked *Use for EMS* then the software chooses the set of authentications to which the current user has access. Administrators typically use this capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

NOTE:

Resync fails if you do not check this box.

Select EMC Parameters

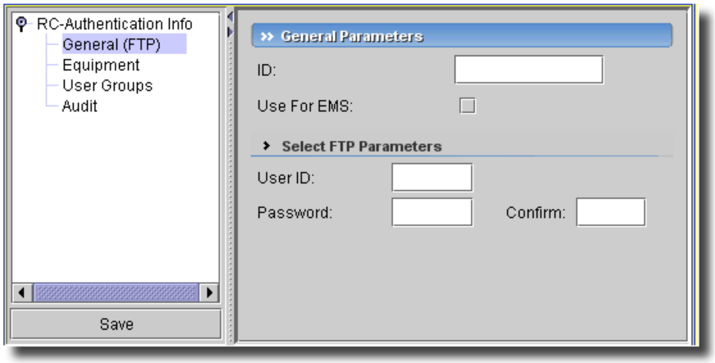
- **User Name** — The User ID that this object uses to login to EMC devices.
- **Password** — The password for the User ID this object uses.
- **Confirm Password** — Confirm the password.

Confirm your entries here with *File -> Save* or by clicking on the *Save* icon or button.

FTP

You can also enter authentication information for FTP:

Figure 4-11. General (FTP) Page



Enter the following fields:

General Parameters

- **ID**—The FTP authentication object name.
- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them.

If none of the associated credentials are marked *Use for EMS* then the software chooses the set of authentications to which the current user has access. Administrators typically use this capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

NOTE:

Resync fails if you do not check this box.

Select FTP Parameters

- **Password** — The password for the User ID this object uses.

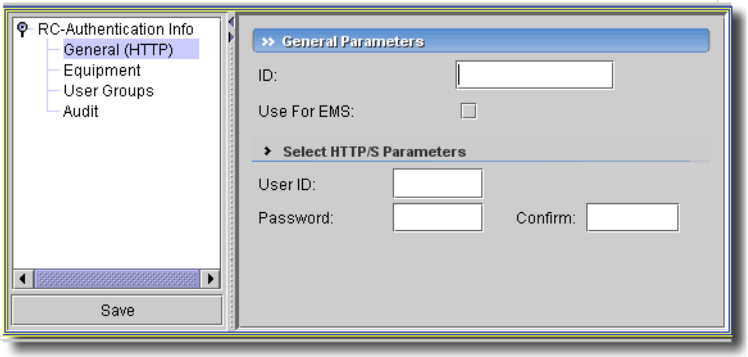
- **Confirm Password** — Confirm the password.

Confirm your entries here with *File -> Save* or by clicking on the *Save* icon or button.

HTTP/HTTPS/WBEM

These authentication objects serve as logins for http or https connections.

Figure 4-12. General (HTTP/HTTPS) Page



Here are the fields:

General Parameters

- **ID**—A unique identifier for this authentication object.

- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them.

  If none of the associated credentials are marked *Use for EMS* then the software chooses the set of authentications to which the current user has access. Administrators typically use this

capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

NOTE:

Resync fails if you do not check this box.

Select HTTP/HTTPS Parameters

- **UserID**—The login ID.

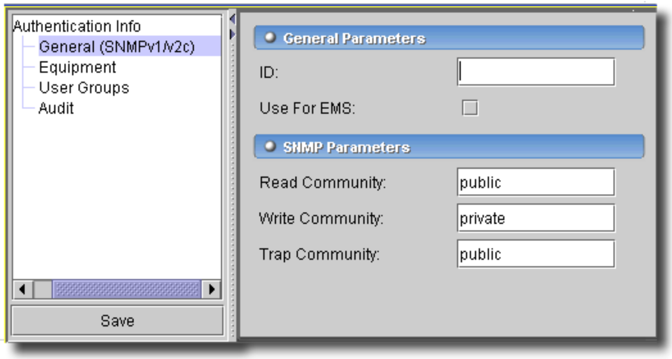
- **Confirm Password** — Confirm the password.

Confirm your entries here with *File -> Save* or by clicking on the *Save* icon or button.

SNMP v1/v2

Enter information for v1 or v2 SNMP authenticators through the General (SNMP) page, shown below. Some fields — Read Community, Write Community, and Trap Community—pre-fill with default values.

Figure 4-13. Authenticator Editor — General (SNMP) Page



General Parameters

ID:

Use For EMS: □

SNMP Parameters

Read Community: public

Write Community: private

Trap Community: public

The following are the fields in the General (SNMP) page:

General Parameters

- **ID** — (Required) This entry must be unique; it identifies the authentication object.

- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them.

  If none of the associated credentials are marked *Use for EMS* then the software chooses the set of authentications to which the current user has access. Administrators typically use this

capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

NOTE:

Resync fails if you do not check this box.

Select HTTP/HTTPS Parameters

- **Read Community** —The default is *public*.

- **Write Community** —The default is *private*.

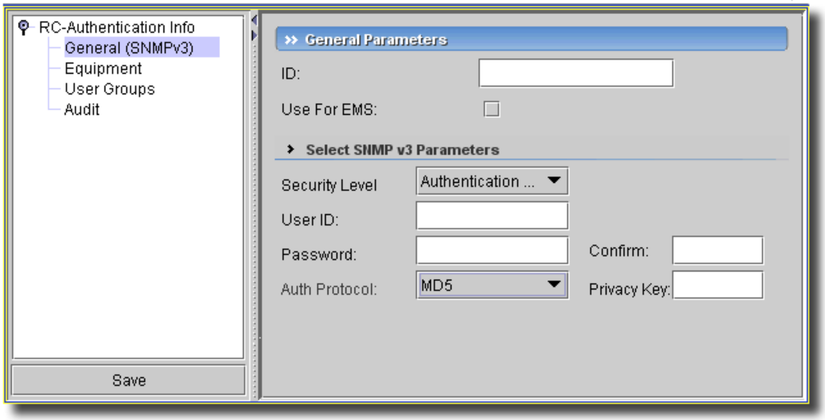
- **Trap Community**— The default is *public*.

Confirm your entries here with *File* -> *Save* or by clicking on the *Save* button or icon.

SNMP v3

Enter information for v3 SNMP authenticators through the General (SNMP) page, shown below. Some fields — Version, Read Community, Write Community, and Trap Community, pre-fill with default values.

Figure 4-14. Authenticator Editor — General (SNMP) Page



ID:

Use For EMS: □

Security Level: Authentication ...

User ID:

Password:

Confirm:

Auth Protocol: MD5

Privacy Key:

If you must process SNMP v3 informs from the device, you must supply the OpenManage Network Manager mediation server's SNMP v3 engineID in the Management Interfaces screen in Resource editor. The value for the engineID appears in the mediation and application server logs. It appears near the text `Server Ready`. For example:

2010-01-06 14:30:04,578 78235 INFO [com.dorado.core.mediation.snmp.SRSnmpSession] SNMP EngineID: 00 00 00 63 00 01 00 a1 c0 a8 86 b1

Changing the value of engineID may have important side-effects, altering both the acceptable SNMP community string and command line password for a device. If this occurs, re-configure the device's authorized users.

CAUTION:

When creating the SNMPv3 user account for OpenManage Network Manager ensure that all MIBs are included in that user's view. If you discover a device using SNMPv3 but do not expose, for example, the RFC1213 system MIB to the user account initiating this discovery OpenManage Network Manager looks like it cannot communicate using SNMPv3.

This screen has the following fields:

General Parameters

- **ID** — (Required) This entry must be unique; it identifies the authentication object. The ID is only a label name under which you store the authentication and has no effect on the SNMPv3 Authentication itself.
- **Use for EMS**—Disregard. This entity does not support SNMP v3.
- **Select SNMP v3 Parameters**—From the pick list.
- **Security Level**—Defines the three security levels that can be used. They are:

  No Authentication–Sends SNMP messages without authentication and without privacy. This requires only a valid User ID, known by the device's SNMP agent.

  Authentication (No Privacy)—Sends SNMP messages with authentication but without privacy. Requires only a valid User ID and a password.

  Authentication with Privacy—Sends SNMP messages with authentication and privacy. This requires a valid User ID, password, authentication Protocol and Privacy Key.

NOTE:

Supported authentications include: No authentication No privacy, MD5 or SHA Authentication with No privacy*, and MD5 Authentication with DES. Privacy encryption 3DES and AES are not currently supported.

- **User ID**—Specifies the User Name for this object. The Security user name represents the user in a format that is Security Model-independent.
- **Password** — Specify the password for this user.
- **Confirm Password** — Confirm the password.
- **Authentication Protocol** — Select the protocol from the pick list (*MD5* or *SHA*). Used with the Privacy Key to produce a secret key in which to validate the connection.

- **Privacy Key**— Enter the privacy key. The application uses this to generate a secret key. Specifying MD5 requires the privacy key to be 16 characters long while SHA requires the privacy key to be 20 characters long.

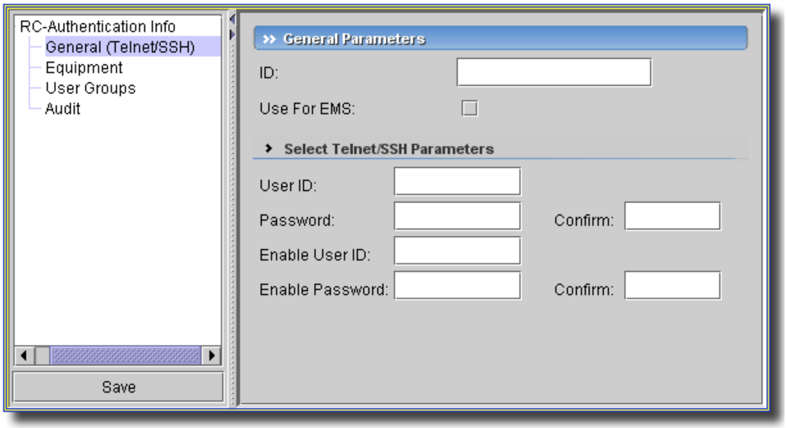
CAUTION:
OpenManage Network Manager does note support the same user ID with different authentication schemes in the same deployment. If you need to deploy a portion of the network with SHA and another with MD5 you must use different user IDs.

Confirm your entries here with *File* -> *Save* or by clicking on the *Save* button or icon.

Telnet / SSH

You can use Telnet / SSH authentication objects for either SSH (default: port 22) or Telnet (default: port 23) logins. Select which type of login by selecting the port when you use them in the Resource Discovery Wizard.

Figure 4-15. General (Telnet / SSH) Page



The following are the authentication object fields for Telnet/SSH (ASCII) logins. For additional SSH information, refer to SSH Strict Host Key Checking on page 91.

General Parameters

- **ID**—The Telnet or SSH authentication object name.
- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them.

  If none of the associated credentials are marked *Use for EMS* then the software chooses the set of authentications to which the current user has access. Administrators typically use this

capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

NOTE:

Resync fails if you do not check this box.

Select Telnet / SSH Parameters

- **User ID**—The user login.
- **Password / Confirm**— The password for the User ID this object uses.
- **Enable User ID**—The user login, if the device needs a different login for an enabled user. Consult your device's manuals for more about this.
- **Enable Password / Confirm Enable Password**—The user password (and confirmation), if the device needs a different password for an enabled user.

Secure WBEM Access

Some monitoring capabilities require root access, even if you securely log into the UNIX host. In this case, when configuring this secure (SSH) login, use the Authentication Manager's Telnet authentication editor to configure su as an Enable User ID, and the root user's password as the Enable Password. For other WBEM access, configure authentication as an HTTP/HTTPS login / password, and select WBEM as the protocol after you have selected the WBEM authentication.

Confirm your entries here with *File -> Save* or by clicking on the *Save* icon or button.

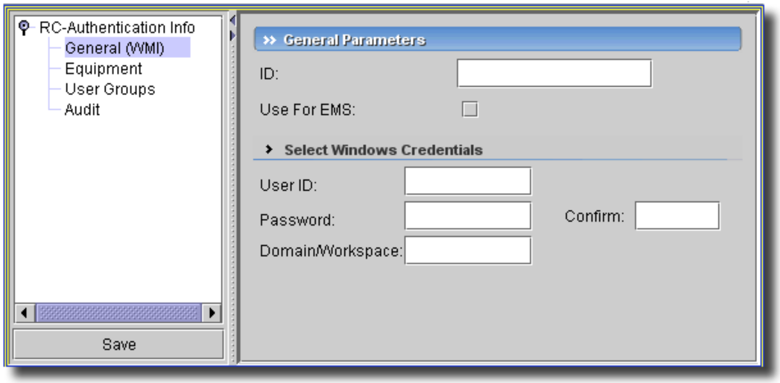
Required Security Levels

Access to some system command modes on devices may be defined by specifying an access privilege level for a user account. For example, some devices require access privilege level 15 to access Enable (privileged) mode. This application requires the user account for authenticating with and managing a device has a privilege level of 15. Ensure that user accounts associated with Authentication objects are configured on the device with root privileges and has both read and write access. Consult your equipment's manuals for instructions about how to set up user access.

Windows

These authentication objects serve as logins for Windows (WMI) connections.

Figure 4-16. General (Windows) Page



Before you can expect to manage servers with a Windows Management Interface driver, you must download and install the latest version of the Microsoft.Net™ framework. The WMI login for this software must also be credentials must be for a domain user who also belongs to the administrator group on the WMI device for complete functionality. Both this and .NET installation are requirements for any installation managing WMI devices. The WMI authentication screen has the following fields:

General Parameters

- **ID**—A unique identifier for this authentication object.
- **Use for EMS**—Checking this lets this application—the entire element management system (EMS)—use this authentication. Otherwise, authentications are only available to individual users who have permissions to use them.

  If none of the associated credentials are marked *Use for EMS* then the software chooses the set of authentications to which the current user has access. Administrators typically use this capability to control access to cut-thru session capabilities (read vs. read-write) when a command line interface is present to the managed device.

NOTE:

Resync fails if you do not check this box.

Select Windows Credentials

- **UserID**—The login ID.
- **Domain / Workspace**—Enter the Windows domain.

Confirm your entries here with *File* -> *Save* or by clicking on the *Save* icon or button.

Equipment

The Equipment page provides an interface through which you can associate managed resources with the authentication object you are creating or editing.

- **To add equipment**—Click *Add*. The Select *Equipment* page appears.

  Click an equipment object in the list to select it; the selected object then appears in the lower pane. A turn key icon appears if the selected object contains subcomponents (cards and ports, for example); click on the turn key to display a tree representation of those subcomponents. Click on any individual item in the tree to select it; click *OK* to add the selected resource to the list associated with the authentication object.

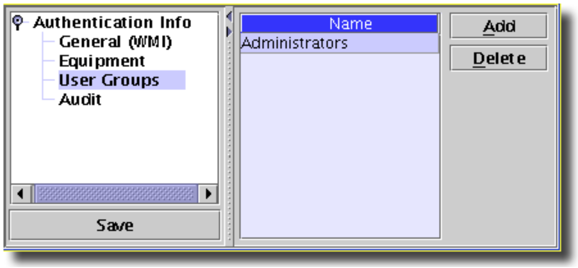
- **To Delete Equipment** — Select the equipment object in the list and click *Delete*.

⚠ **CAUTION:**
If you add an authentication to a device in Resource Editor, Authentication Manager / Editor appears as a selector / new authentication creation screen. If you create a new authentication object, do not also add the device to the Equipment panel of Authentication Editor.

User Groups

This page lets you associate User Groups with authentication objects. The created authentication object is visible only to users who are members of the associated group. The initial display (Figure 4-17 is an example) lists the groups associated with this object.

Figure 4-17. User Groups Page



To add a group, click *Add*. To remove a group from the list, select it and click *Delete*. When adding groups, the Group Manager dialog, appears. (For more information on the Group Manager, see User Group Manager on page 77.)

Select a group from the displayed list (or click *New...* to define a new group) and click OK to implement your selection.

SSH Strict Host Key Checking

The following describes how to setup SSH strict host key checking and how to populate the `known_hosts` file. The following sections describe:

- Enabling Strict Host Key Checking
- Populating the SSH known_hosts File
- Troubleshooting SSH
- SSH HostKey Errors

Enabling Strict Host Key Checking

To enable strict host key checking you need to configure a host entry in the SSH configuration file setting `StrictHostKeyChecking` to yes. The default SSH configuration file located in `$OWARE_USER_ROOT/owareapps/ezmediation/lib/default_ssh_config`. Make a copy of this file, renaming it to `ssh_config`. In the copied file set the property `StrictHostKeyChecking` to `yes` for example.

```
Host *
  StrictHostKeyChecking yes
```

To specify settings for a specific host the entry would look something like

```
Host 192.168.1.118
  StrictHostKeyChecking yes
```

Comments at beginning of configuration file describe other options.

You must do this change on each mediation server and on each application server if they are providing mediation services.

Once you have enabled strict host key checking you may see an error dialog that indicates host key rejection. (Message: `SSH Host Key rejected for [user] against [host IP address] using SSH v2`) This indicates that you need to update your `known_hosts` file.

Populating the SSH known_hosts File

The `known_hosts` file is in the installation directory at `~/.ssh/known_hosts` (On Linux, that is the OpenManage Network Manager running user's home directory (for example `/root` or `/export/home/username.` On Windows it is the same as `$OWARE_USER_ROOT`). If you enable strict host key checking you must make sure that this file has all the host keys for all devices you plan to manage that support SSHv2.

One way to populate the `known_hosts` file is to connect to each device on the command line in a way that it will add a host entry to the `known_hosts` file. Below is an example session on Windows.

```
C:\Dell>oware
```

```
~:ssh -o StrictHostKeyChecking=ask -l admin 192.168.1.118

The authenticity of host '192.168.1.118 (192.168.1.118)' can't be
   established.

RSA key fingerprint is 90:b7:2a:e0:64:30:6a:74:9c:e8:7b:75:61:48:52:7b.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.1.118' (RSA) to the list of known
   hosts.

admin@192.168.1.118's password:

Last login: Thu Sep 10 14:23:08 2009 from 10.35.35.2

--- JUNOS 9.5R1.8 built 2009-04-13 19:25:06 UTC

admin@M5-118>
```

After this you should see an entry in `~/.ssh/known_hosts` that looks similar to the following

```
192.168.1.118 ssh-rsa AAAAB3NzaC1yc2EAAAAB

                      IwAAAIEAlpZUs99PM1fI

                      2DWtpV/pc2YVK8CvRVQg

                      DOnvBcS7HFc5IECr+bF1

                      o6PfEijQ8TILILbJRFtD

                      bJeZOK0+0cJs8lRNNT3R

                      j9b79AMCVH0syGiPm7+d

                      OkqiVVa8FtSkz8VxgpiL

                      MI959xVr1WKLXsvAtj6b

                      DbCdN0golL9/h8H8+uk=
```

The problem with this approach is that you must restart the server after the `known_hosts` file has been populated for the changes to take effect.

To populate the `known_hosts` file without having to restart the server, follow these steps:

1. Add an entry in the `ssh_config` file setting `StrictHostKeyChecking` to *no* for the devices you want to add to the known_hosts file.
2. Connect to each of the devices in OpenManage Network Manager using SSHv2 credentials. This adds an entry to the `known_hosts` file.
3. Remove the entry added to the `ssh_config` file or change the setting `StrictHostKeyChecking` to *yes*.

Troubleshooting SSH

To trouble shoot SSH configuration issues and host keys debug output can be helpful. Turn on log4j debug for `com.dorado.mediation.cli` and you should see debug that looks something like the following (d:\Dell is $OWARE_USER_ROOT in the following):

```
loading SSH config from 'd:\Dell\owareapps\ezmediation\lib\ssh_config'
loading host '*'
  adding property 'compression.s2c' = 'none'
  adding property 'compression.c2s' = 'none'
  adding property 'StrictHostKeyChecking' = 'no'
Loaded SSH Config:
Host '*'
   StrictHostKeyChecking 'no'
   compression.s2c 'none'
   compression.c2s 'none'

Host keys in d:\Dell\.ssh\known_hosts
-->192.168.1.118 ssh-rsa 90:b7:2a:e0:64:30:6a:74:9c:e8:7b:75:61:48:52:7b
-->194.78.112.59 ssh-rsa 54:ca:2b:41:83:41:9b:d8:df:b9:a3:59:73:b2:28:0c
```

SSH HostKey Errors

Example error messages:

- A failed Direct Access Cut-Through attempt to a device that did not have its host key in the known_hosts file displays `ERROR - reject Hostkey: [host IP address]`
- The audit trail output for a resync operation to a device that did not have its host key in the `known_hosts` file displays `SSH HostKey was rejected` in the audit messages.

RADIUS Authentication

If you want to use RADIUS authentication for this application's clients, you must create a RADIUS user matching the login in the application (and assign that user the correct groups and functional permissions in the application).

The property file that needs to change is on the application server(s) in

```
oware\jboss-<version number>\server\oware\conf\login-config.xml.
```

By default, RADIUS authentication is commented out in this file. To use RADIUS, uncomment this section (changing <!-- to < and --> to >). Then, configure the options (example server, secret, prompts, NAS-IP-Address).

Here is an example of the application’s freeradius implementation on helix.

```
<authentication>
           <!--login-module code = "com.theorem.radius3.login.RADIUSLogin"
             flag = "sufficient">
             <module-option name = "authtype">CHAP</module-option>
             <module-option name = "debug">true</module-option>
             <module-option name = "server">127.0.0.1</module-option>
             <module-option name = "port">1812</module-option>
             <module-option name = "timeout">1</module-option>
             <module-option name = "secret">secret</module-option>
             <module-option name = "namePrompt">Name:</module-option>
    <module-option name = "passwordPrompt">Password:</module-option>
    <module-option name = "NAS-IP-Address">@127.0.0.1</module-option>
    <module-option name = "NAS-Port">#1</module-option>
    <module-option name = "Framed-Protocol">#PPP</module-option>
             <module-option name = "Service-Type">#Login</module-option>
           </login-module-->
           <login-module code = "com.dorado.extensions.OWLoginModule"
             flag = "sufficient">
           </login-module>
       </authentication>
```

NOTE:

This application logically ANDs the RADIUS authentication policies with its internal security policies.

To disable authentication against OpenManage Network Manager, the second login module needs to be removed or commented out in XML. (Comments in XML are bracketed with `<!--` and `-->`.)

```
<!--
<login-module code = "com.dorado.extensions.OWLoginModule"
flag = "sufficient">
</login-module>
-->
```

Radius Use Cases

To clarify use of Radius authentication, consider the following use cases:

NOTE:

These assume both authentication sources are enabled in login-config.xml as described in RADIUS Authentication. This queries both sources uniquely.

Scenario 1:

1 Create account *test* with password *test* in RADIUS.

2 Create account *test* with password *test* in OpenManage Network Manager.

3 Login to OpenManage Network Manager using *test/test*

Expected Result:

User *test* can log into OpenManage Network Manager via RADIUS authentication

Scenario 2:

1 Create account *test* with password *test* in RADIUS.

2 Create account *test* with password *test* in OpenManage Network Manager

3 Login to OpenManage Network Manager using *test/test*

Expected Result:

User *test* can log into OpenManage Network Manager via RADIUS authentication

Scenario 3:

1 Create account *test* with password *test* in RADIUS.

2 Create account *test* with password *test* in OpenManage Network Manager

3 Login to OpenManage Network Manager using *test/test123*

Expected Result:

User *test* cannot log into OpenManage Network Manager via RADIUS authentication.

Scenario 4:

1 Create account *test* with password *test* in OpenManage Network Manager.

2 Login to OpenManage Network Manager using *test/test*. Note that *test/test* account is not in RADIUS server.

Expected Result:

User *test* is unable to login to OpenManage Network Manager.

Scenario 5:

1 Login to OpenManage Network Manager using *abc/abc*. Note that *abc/abc* account is not on RADIUS or OpenManage Network Manager.

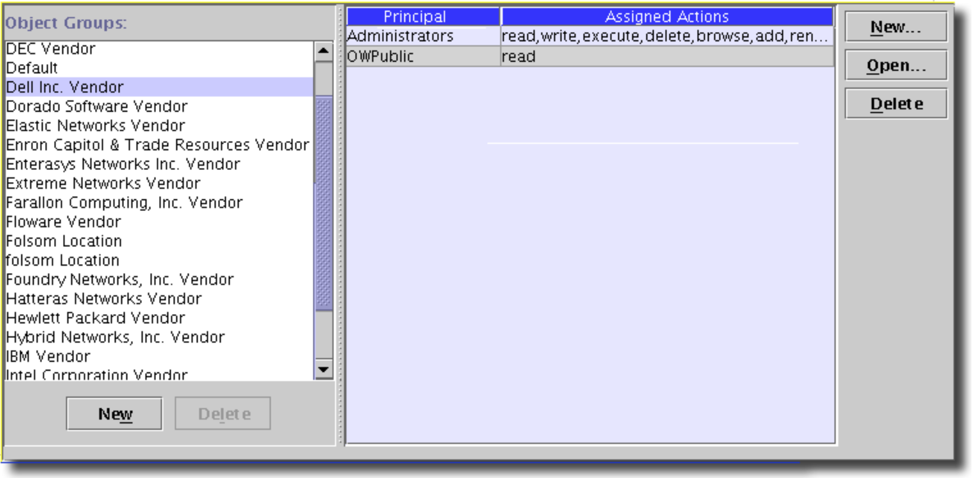
Expected Result:

User *abc* is unable to login to OpenManage Network Manager.

Object Group Manager

The Object Group Manager lets you group objects and then associate them with individual users or user groups. Open it with the *Settings -> Permissions -> Object Group Manager* menu item. Permissions are attached to each association. For example, you can associate the principals *Administrators* and *Trainees* with a Dell Vendor object group, and can attach one set of permissions (*read*, *write*) to the association between Administrators and the Dell Vendor object group, while attaching another set of permissions (read) to the association between Trainees and the Dell Vendor object group.

Figure 4-18. Object Group Manager



Object Groups:

DEC Vendor
Default
Dell Inc. Vendor
Dorado Software Vendor
Elastic Networks Vendor
Enron Capitol & Trade Resources Vendor
Enterasys Networks Inc. Vendor
Extreme Networks Vendor
Farallon Computing, Inc. Vendor
Floware Vendor
Folsom Location
folsom Location
Foundry Networks, Inc. Vendor
Hatteras Networks Vendor
Hewlett Packard Vendor
Hybrid Networks, Inc. Vendor
IBM Vendor
Intel Corporation Vendor

Principal	Assigned Actions
Administrators	read,write,execute,delete,browse,add,ren...
OWPublic	read

This application also provides “natural groupings,” automatically creating a dynamic object group whenever you add an entity belonging to one of the natural groups the system. The following are some examples of natural groups:

- **Object Vendor** — All objects that refer to a particular vendor.

- **Location** — All objects that refer to a given location.

- **Role** — Within this application, objects can refer to a role. The role can describe the use those objects have within the network — core router, for example, as opposed to edge router.

NOTE:

You cannot make individual interfaces part of an object group, but you can assign a role to them. Roles make natural groups, and you can use those role-based groups to manage the access to individual interfaces.

The system administrator and add-on products can add other groups to this list, and can add objects to those groups.

To add a new object group, click *New* below the list of available groups and name the group in the subsequent screen. Accept that name to add it to those listed.

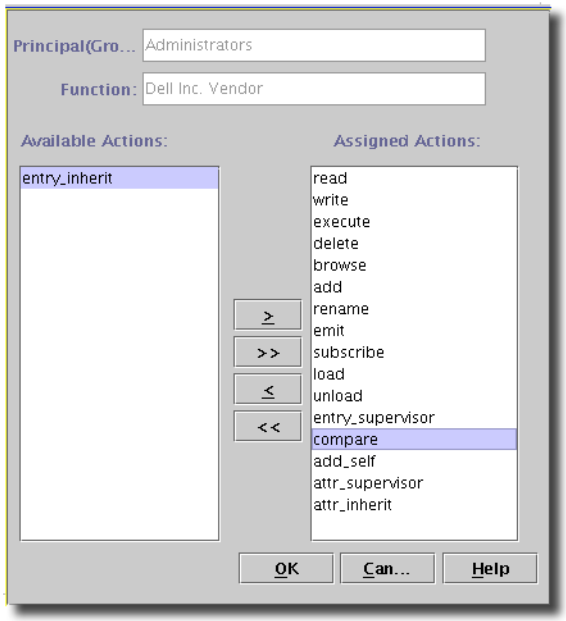
CAUTION:

All users inherit OWPublic's permissions. You must remove OWPublic's read permissions from things in Object Group Manager to conceal those items.

Adding or Modifying Object Groups

When you click *New*, you can create a new association between either user or object groups and permissions. Select from *User Groups* (see User Group Manager on page 77 for instructions about how to make and manage these groups) or individual users (see User Manager on page 69 for more information about these). The button at the top right of this screen toggles between individual users and groups displayed in the pick list in the top center of the screen (Figure 4-19).

Figure 4-19. Adding Object Group Permissions



Principal(Gro... Administrators

Function: Dell Inc. Vendor

Available Actions:

entry_inherit

Assigned Actions:

read
write
execute
delete
browse
add
rename
emit
subscribe
load
unload
entry_supervisor
compare
add_self
attr_supervisor
attr_inherit

Select a *Principal (Group or User)*, if you are creating new permissions. Otherwise this and the *Function* field, reminding you of the object group previously selected, are read-only. Then use the selection lists below to arrange the available permissions. Click *OK* to confirm your selection.

CAUTION:

Because devices can belong to different object groups, restricting permissions to a single group may not remove a device from a prohibited user’s control. Permissions for *Vendor, Location, Role*, manually created *Object Group* and *Services* are applied with a logical AND, so similar advice applies about them.

Application Security Policy

The Application Security interface lets you specify security policies governing user login and passwords. Open the Application Security Policy page by selecting *Settings -> Permissions -> Application Security Policy.*

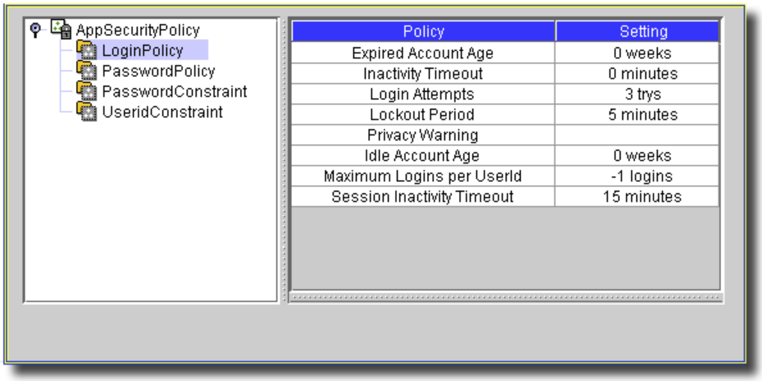
The following are types of application security policies described in this section:

- Login Policy
- Password Policy
- Password Constraint

Login Policy

The LoginPolicy section of the Application Security Policy page sets policies about user logins. These policies govern the message that appears in the login screen and the various security measures applied to user's attempts to log in.

Figure 4-20. Login Policy Page



- AppSecurityPolicy
  - LoginPolicy
  - PasswordPolicy
  - PasswordConstraint
  - UseridConstraint

Policy	Setting
Expired Account Age	0 weeks
Inactivity Timeout	0 minutes
Login Attempts	3 trys
Lockout Period	5 minutes
Privacy Warning	
Idle Account Age	0 weeks
Maximum Logins per UserId	-1 logins
Session Inactivity Timeout	15 minutes

The individual policies available from the Login Policy Page are:

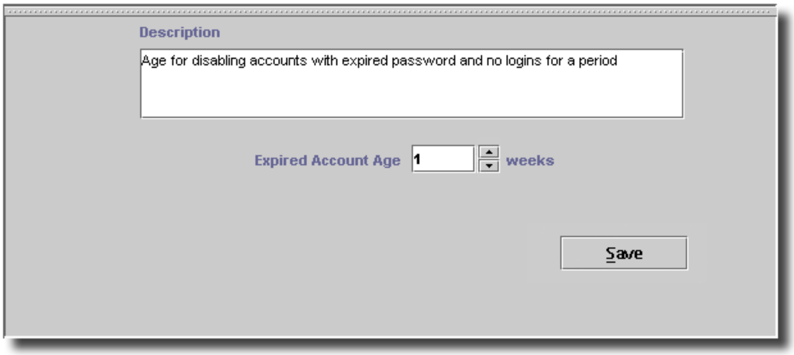
- Expired Account Age
- Inactivity Timeout
- Login Attempts
- Lockout Period
- Privacy Warning
- Idle Account Age
- Maximum Logins per UserId
- Session Inactivity Timeout

Each Login Policy appears in the list along with its current setting. Edit a policy by clicking it; an editor appropriate to that setting appears in the lower portion of the page.

Expired Account Age

The Expired Account Age setting determines how many weeks an account can remain active if it has an expired password and no logins. Once this threshold is reached, the account is disabled and can only be reactivated by an administrator.

Figure 4-21. Expired Account Age


Description

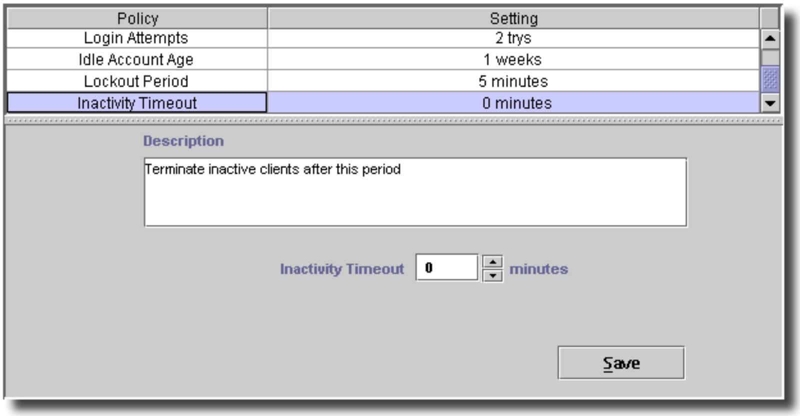
Age for disabling accounts with expired password and no logins for a period

Expired Account Age 1 weeks

Inactivity Timeout

The Inactivity Timeout setting determines how long a terminal can remain inactive before the client is shut down. A setting of 0 effectively disables this setting, allowing users to remain inactive indefinitely.

Figure 4-22. Inactivity Timeout


Policy	Setting
Login Attempts	2 trys
Idle Account Age	1 weeks
Lockout Period	5 minutes
Inactivity Timeout	0 minutes

Description

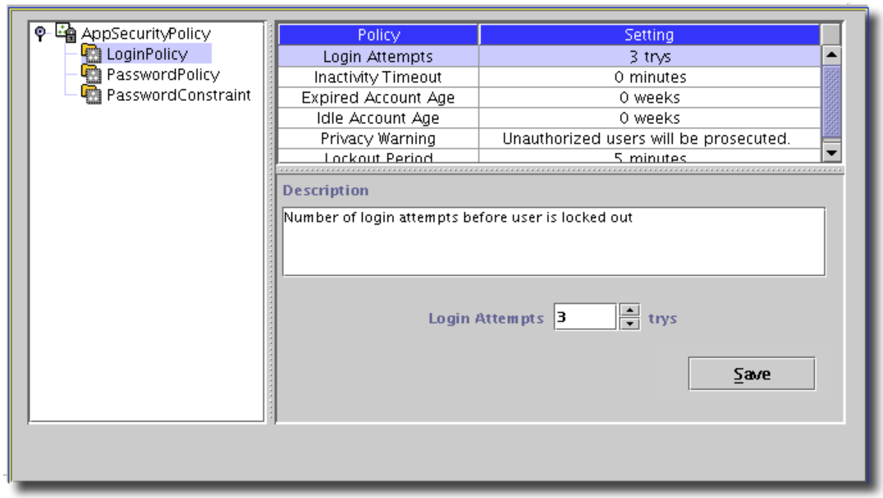
Terminate inactive clients after this period

Inactivity Timeout 0 minutes

Login Attempts

The Login Attempts setting specifies how many consecutive unsuccessful login attempts are allowed before a user is locked out.

Figure 4-23. Login Attempts



Policy	Setting
Login Attempts	3 trys
Inactivity Timeout	0 minutes
Expired Account Age	0 weeks
Idle Account Age	0 weeks
Privacy Warning	Unauthorized users will be prosecuted.
Lockout Period	5 minutes

Description

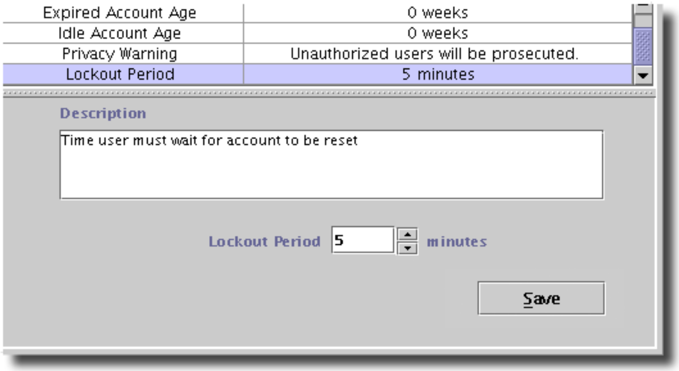
Number of login attempts before user is locked out

Login Attempts 3 trys

Lockout Period

The Lockout Period determines how long a user must wait, after a failed login attempt, before a new attempt is allowed.

Figure 4-24. Lockout Period



Expired Account Age	0 weeks
Idle Account Age	0 weeks
Privacy Warning	Unauthorized users will be prosecuted.
Lockout Period	5 minutes

Description

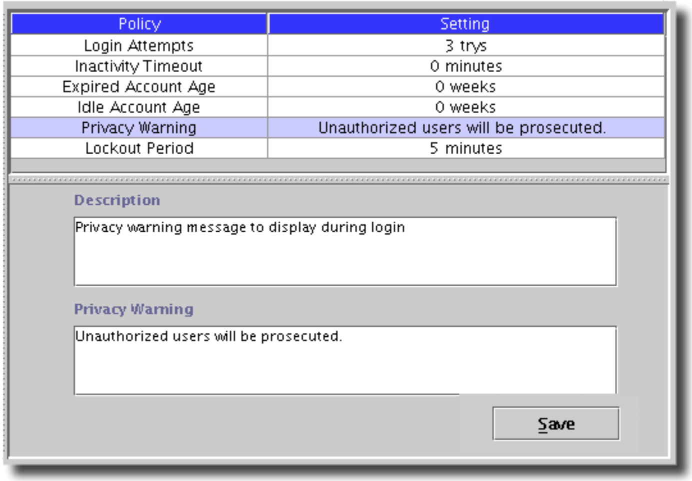
Time user must wait for account to be reset

Lockout Period 5 minutes

Privacy Warning

The Privacy Warning appears every time a user logs on. Enter your desired text in the Privacy Warning field and click *Save* to implement the change.

Figure 4-25. Privacy Warning



Policy	Setting
Login Attempts	3 trys
Inactivity Timeout	0 minutes
Expired Account Age	0 weeks
Idle Account Age	0 weeks
Privacy Warning	Unauthorized users will be prosecuted.
Lockout Period	5 minutes

Description

Privacy warning message to display during login

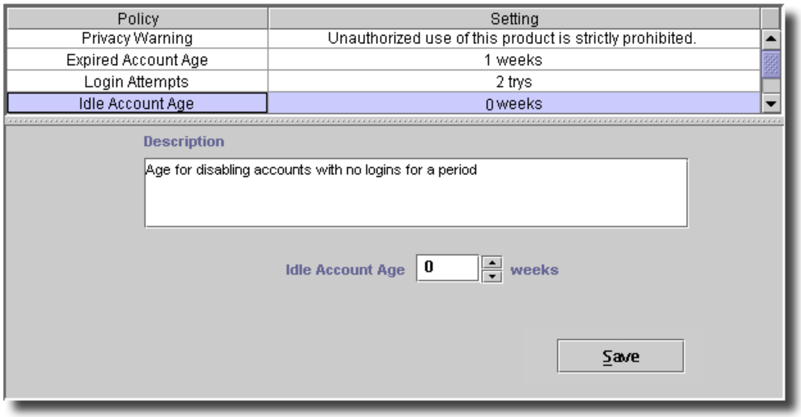
Privacy Warning

Unauthorized users will be prosecuted.

Idle Account Age

The Idle Account Age determines how long an account can remain inactive (have no logins) before it is disabled.

Figure 4-26. Idle Account Age



Policy	Setting
Privacy Warning	Unauthorized use of this product is strictly prohibited.
Expired Account Age	1 weeks
Login Attempts	2 trys
Idle Account Age	0 weeks

Description

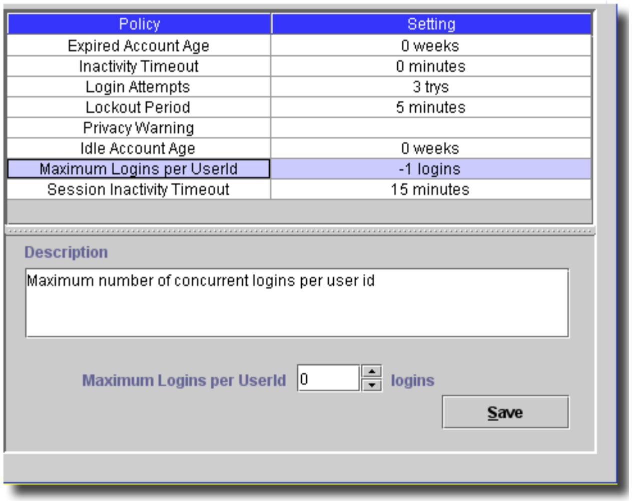
Age for disabling accounts with no logins for a period

Idle Account Age 0 weeks

Maximum Logins per UserId

This screen determines how many times a single user can log in concurrently. The default is -1, which means as many as the hardware will bear.

Figure 4-27. Maximum Logins per UserId



Policy	Setting
Expired Account Age	0 weeks
Inactivity Timeout	0 minutes
Login Attempts	3 trys
Lockout Period	5 minutes
Privacy Warning	
Idle Account Age	0 weeks
Maximum Logins per UserId	-1 logins
Session Inactivity Timeout	15 minutes

Description

Maximum number of concurrent logins per user id

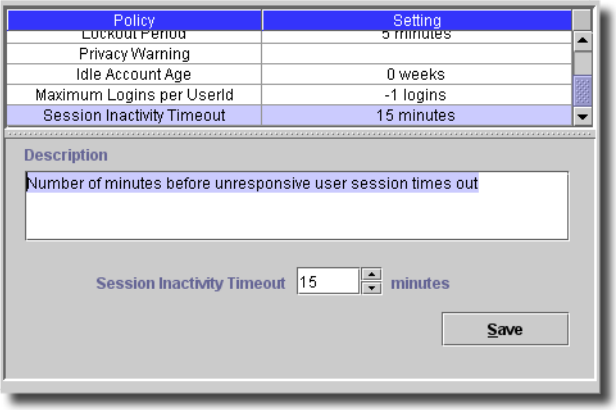
Maximum Logins per UserId 0 logins

Select a number with the spinner and click *Save* to change the default.

Session Inactivity Timeout

This configures the number of minutes before an unresponsive user session times out.

Figure 4-28. Session Inactivity Timeout



Policy	Setting
Lockout Period	5 minutes
Privacy Warning	
Idle Account Age	0 weeks
Maximum Logins per UserId	-1 logins
Session Inactivity Timeout	15 minutes

Description

Number of minutes before unresponsive user session times out

Session Inactivity Timeout 15 minutes

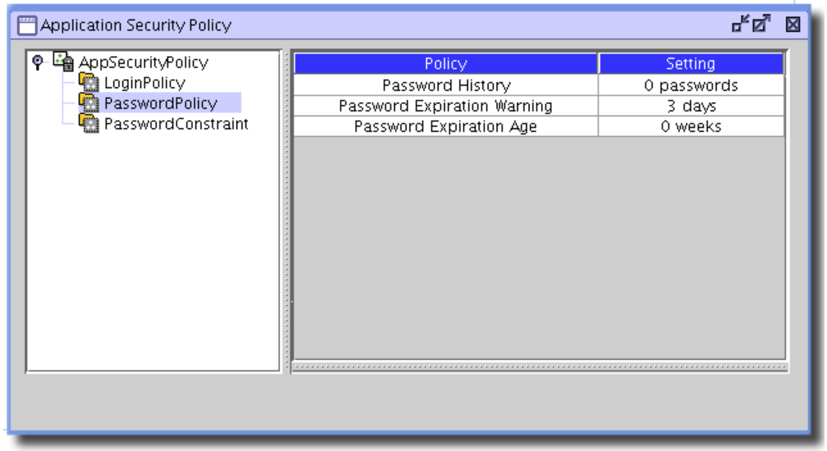
The default is 15 minutes. Select a number with the spinner and click *Save* to change the default.

Password Policy

The settings associated with Password Policy determine whether (and how long) users can keep passwords, how many unique passwords a user must have before the oldest can be re-used, and how much warning they get before their password expires.

Display the password policies by clicking the PasswordPolicy icon in the navigation page. The individual policies appear in the right page.

Figure 4-29. Application Security Policy Page — Password Policies



Policy	Setting
Password History	0 passwords
Password Expiration Warning	3 days
Password Expiration Age	0 weeks

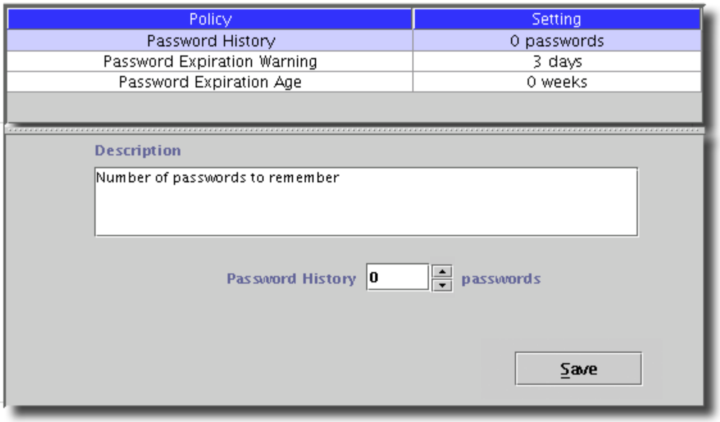
Edit a policy by clicking it; an editor appropriate to that policy appears in the lower portion of the page. This policy editor lets you manage the following:

- Password History
- Password Expiration Warning
- Password Expiration Age
- Allow Password Reuse
- Minimum Password Length
- Require a special character
- Require a number
- Require Mixed Case
- Allow UserId in Password
- Allow Reverse UserId in Password
- Allow Same Character Consecutively
- Require Password Match Regular Expression

Password History

Enter the *Password History* setting in conjunction with the *Allow Password Reuse* setting (see Allow Password Reuse on page 109). If password reuse is not allowed, the system tracks passwords in a FIFO (First In, First Out) queue, up to the number specified by this setting.

Figure 4-30. Password History



Policy	Setting
Password History	0 passwords
Password Expiration Warning	3 days
Password Expiration Age	0 weeks

Description

Number of passwords to remember

Password History 0 passwords

You can reuse an old password after the specified a number (plus one) of other passwords have been used. For example: If you do not enable *Allow Password Reuse* and Password History is set to two, a user's sequence of passwords might look like this:

```
House*Magnet

Fig@Bumper

Rose-Window

Standard+Disclaimer

House*Magnet
```

You can reuse `House*Magnet`, since 2+1 other passwords have been used since `House*Magnet`.

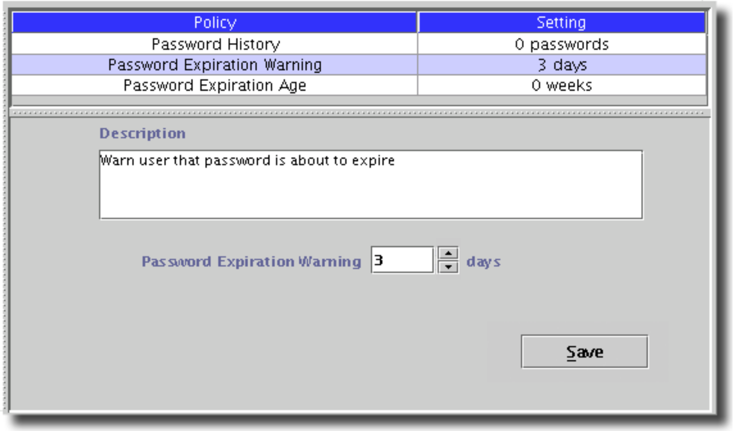
NOTE:

A setting of 0 effectively enables immediate password reuse even if you do not set Allow Password Reuse.

Password Expiration Warning

This warning goes to users whose password is about to expire. The setting determines, in days, how much advance warning they receive (the warning appears every login attempt during the warning period). Enter a value directly in the *Password Expiration Warning* field, or use the up and down arrows to change the displayed value.

Figure 4-31. Password Expiration Warning



Policy	Setting
Password History	0 passwords
Password Expiration Warning	3 days
Password Expiration Age	0 weeks

Description

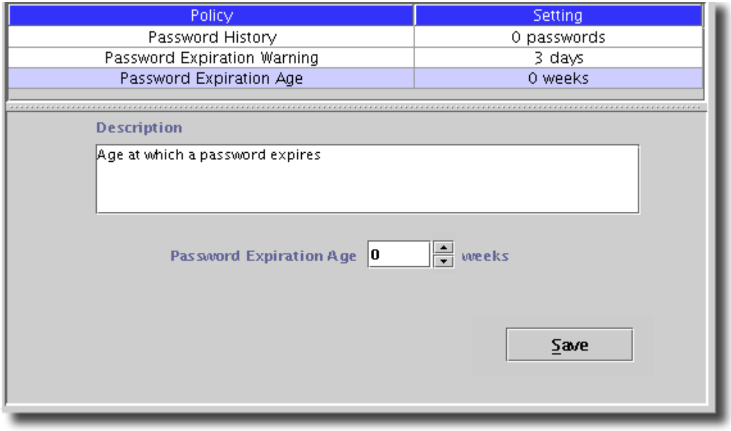
Warn user that password is about to expire

Password Expiration Warning 3 days

Password Expiration Age

The Password Expiration Age setting determines how long a user can keep a password before a new one must be selected. Enter a value directly in the Password Expiration Age field, or use the up and down arrows to change the displayed value.

Figure 4-32. Password Expiration Age



Policy	Setting
Password History	0 passwords
Password Expiration Warning	3 days
Password Expiration Age	0 weeks

Description

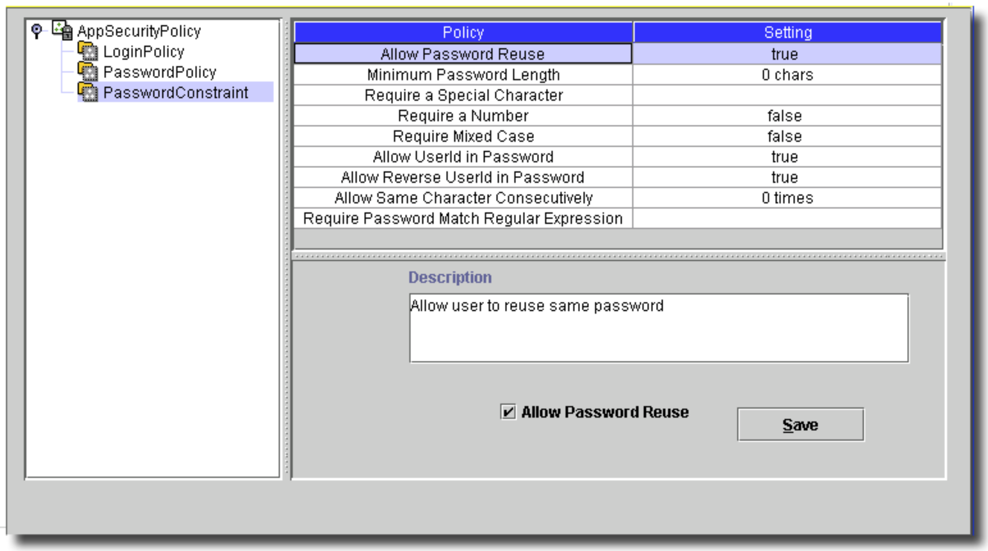
Age at which a password expires

Password Expiration Age 0 weeks

Password Constraint

Password Constraint policies specify how you can construct passwords. Display them by clicking the PasswordConstraint icon in the navigation page. The display shows each policy and its current setting. Edit a policy by selecting it; the edit dialog appears in the lower portion of the page.

Figure 4-33. Password Constraint



Policy	Setting
Allow Password Reuse	true
Minimum Password Length	0 chars
Require a Special Character	
Require a Number	false
Require Mixed Case	false
Allow UserId in Password	true
Allow Reverse UserId in Password	true
Allow Same Character Consecutively	0 times
Require Password Match Regular Expression	

Description

Allow user to reuse same password

☑ Allow Password Reuse

This includes the following sections:

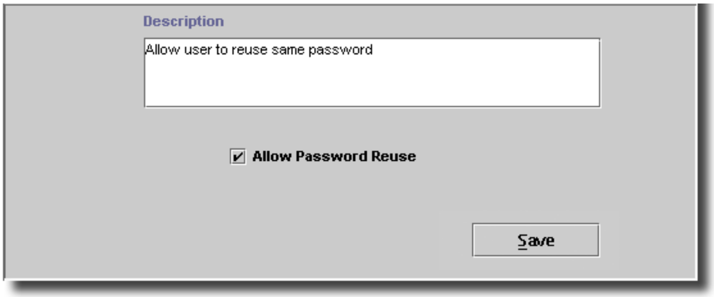
- Allow Password Reuse
- Allow UserId in Password
- Require Mixed Case
- Require a number
- Require Mixed Case
- Allow UserId in Password
- Allow Reverse UserId in Password
- Allow Same Character Consecutively
- Require Password Match Regular Expression

You can set the initial, default password too. See General on page 117 for more information.

Allow Password Reuse

This determines whether users can reuse their password immediately after it has expired. If this option is not selected, users must select a different password each time their password expires. The number of new passwords that must be used before an old password is reused is then determined by the Password History on page 106.

Figure 4-34. Allow Password Reuse



Description

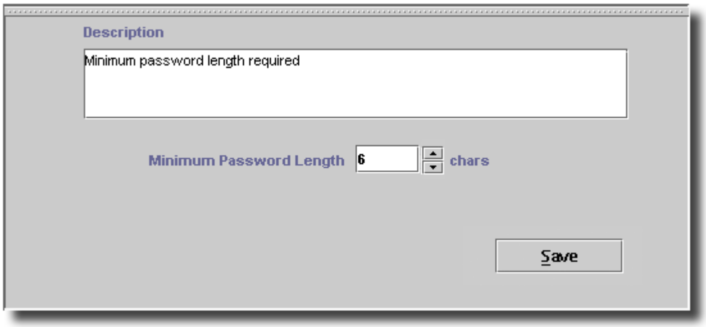
Allow user to reuse same password

☑ Allow Password Reuse

Minimum Password Length

This setting specifies the minimum length of a password. Enter a value directly in the *Minimum Password Length* field, or click the up or down arrows to change the displayed value.

Figure 4-35. Minimum Password Length



Description

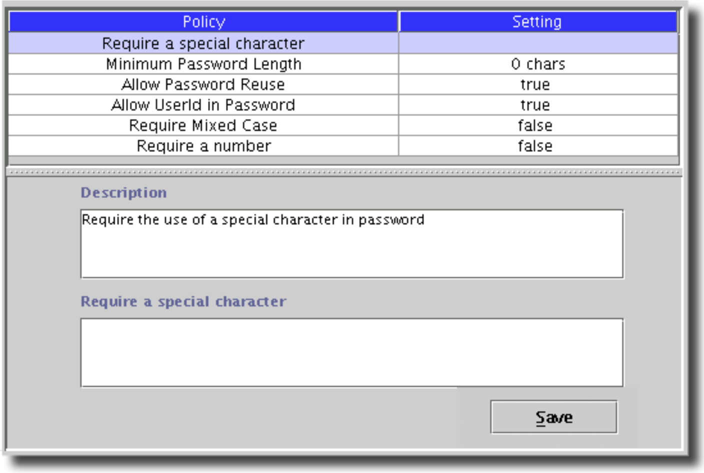
Minimum password length required

Minimum Password Length 6 chars

Require a special character

This requires a special character be part of a user's password — house*magnet, for example. Activate this option by entering the special characters considered acceptable in the *Require a special character* field. In the example above, an asterisk (*) is among the acceptable special characters.

Figure 4-36. Require a special character



Policy	Setting
Require a special character	
Minimum Password Length	0 chars
Allow Password Reuse	true
Allow UserId in Password	true
Require Mixed Case	false
Require a number	false

Description

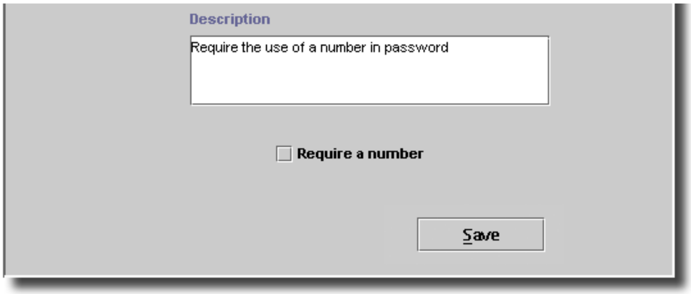
Require the use of a special character in password

Require a special character

Require a number

This specifies whether users must include a number in their passwords — *house2magnet*, for example.

Figure 4-37. Require a number



Description

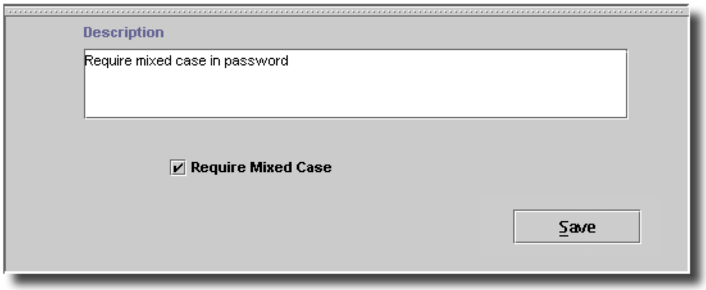
Require the use of a number in password

□ Require a number

Require Mixed Case

This requires a user's password to include both upper and lowercase characters — `HouseMagnet`, for example.

Figure 4-38. Require Mixed Case



Description

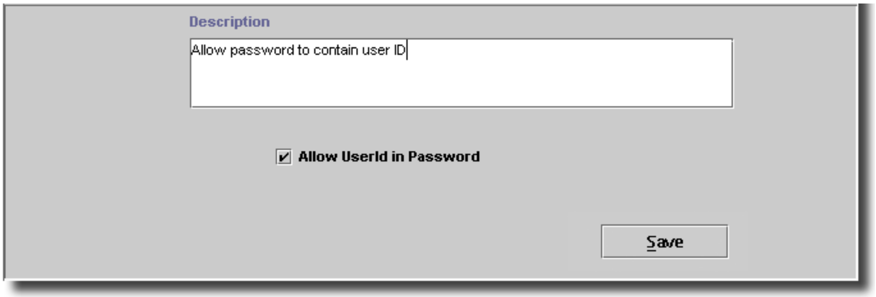
Require mixed case in password

☑ Require Mixed Case

Allow UserId in Password

This lets users include their User ID in their passwords. For example, user MyUser could to create *house*MyUser*magnet* as a password.

Figure 4-39. Allow UserID in Password



Description

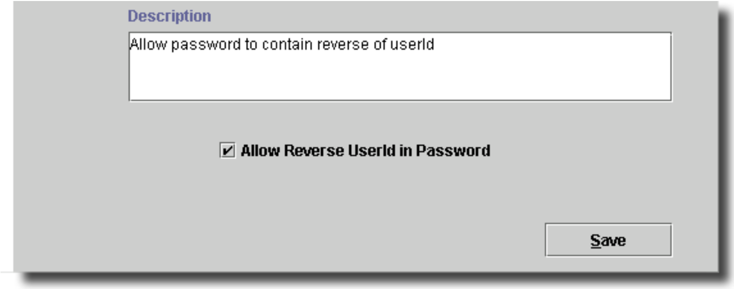
Allow password to contain user ID

☑ Allow UserId in Password

Allow Reverse UserId in Password

This lets users include a backward version of their User ID in their passwords. For example, user MyUser could to create *house*resUyM*magnet* as a password.

Figure 4-40. Allow UserID in Password



Description

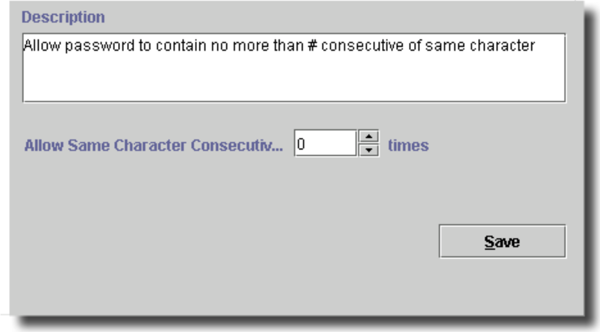
Allow password to contain reverse of userId

☑ Allow Reverse UserId in Password

Allow Same Character Consecutively

This lets users include consecutive identical characters in their passwords. For example, user you could to create *hooooouse*MyUser*magnet* as a password.

Figure 4-41. Allow UserID in Password



Description

Allow password to contain no more than # consecutive of same character

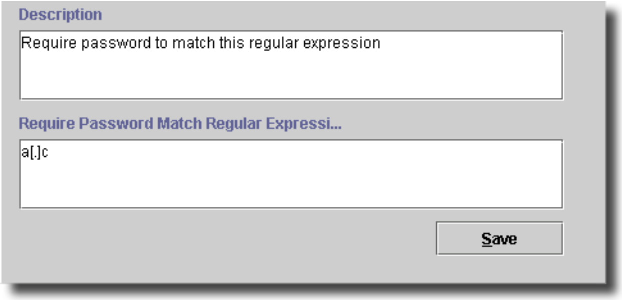
Allow Same Character Consecutiv... 0 times

Use the spinner to select how many consecutive characters to permit.

Require Password Match Regular Expression

This lets administrators restrict passwords to those that match a regular expression.

Figure 4-42. Allow UserID in Password



Description

Require password to match this regular expression

Require Password Match Regular Expressi...

a[.]c

For example, this allows administrators to supply an expression like this:

```
[^[:digit:]\\\'\;\"\:\?\/\>\<\,\.\=\-].*([[:digit:]\\\'\;\"\:\?\/
  \>\<\,\.\=\-]).*[^[:digit:]\\\'\;\"\:\?\/\>\<\,\.\=\-]
```

This expression specifies that the password must contain, but not start or end with, a numeric or special character, where a special character is defined as any of the following: \";:?/><,.=-

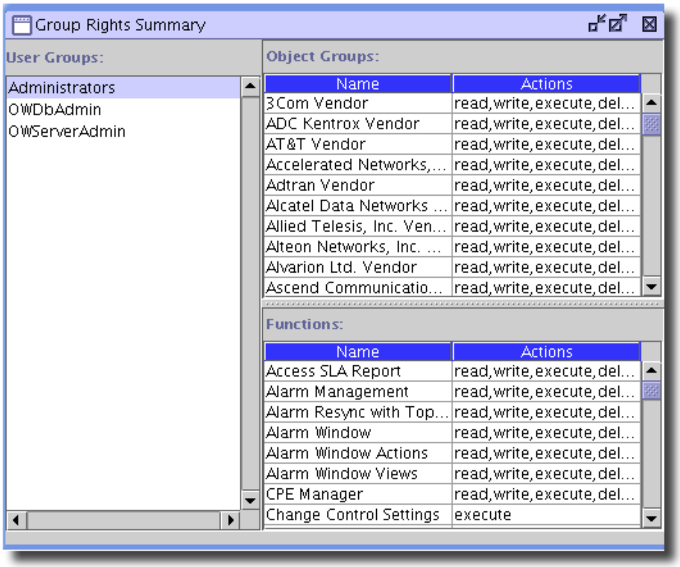
Permitted regular expressions are of the type "RE_SYNTAX_POSIX_AWK". This specifies, among other things, that special characters must be escaped using the backslash.

This policy defaults to an empty regular expression.

Group Rights Summary

The Group Rights Summary page provides a read-only summary of user groups, as defined in the User Group Manager on page 77, and each group's assigned functions and actions, as defined in the *Functional Permissions* Section.

Figure 4-43. Group Rights Summary Page



Group Rights Summary

User Groups:

- Administrators
- OWDbAdmin
- OWServerAdmin

Object Groups:

Name	Actions
3Com Vendor	read,write,execute,del...
ADC Kentrox Vendor	read,write,execute,del...
AT&T Vendor	read,write,execute,del...
Accelerated Networks,...	read,write,execute,del...
Adtran Vendor	read,write,execute,del...
Alcatel Data Networks ...	read,write,execute,del...
Allied Telesis, Inc. Ven...	read,write,execute,del...
Alteon Networks, Inc. ...	read,write,execute,del...
Alvarion Ltd. Vendor	read,write,execute,del...
Ascend Communicatio...	read,write,execute,del...

Functions:

Name	Actions
Access SLA Report	read,write,execute,del...
Alarm Management	read,write,execute,del...
Alarm Resync with Top...	read,write,execute,del...
Alarm Window	read,write,execute,del...
Alarm Window Actions	read,write,execute,del...
Alarm Window Views	read,write,execute,del...
CPE Manager	read,write,execute,del...
Change Control Settings	execute

To display the information for a user group, select that group in the left (User Groups) page.

5

Licensing and System Controls

Overview

Some capabilities for this application require licensing. You can install licenses as instructed in Licenses below, and can view installed licenses with the License Viewer, also described below.

The various panels that populate the Controls Manager provide for configuration of application modules and services. Select *Settings* -> *Configuration* -> *Control Settings* to display the Controls Manager. This Manager consists of tabbed panels representing groups of functions. Those functions appear in this section in alphabetical order.

NOTE:

The configuration of the Controls Manager depends upon the specific installation. The examples in this section demonstrate one possible configuration, but do not exhaust all possibilities. Some controls may do nothing without additional, installed options.

- General
- Properties

CAUTION:

If you see a panel in the application, but not in the document, changes to that panel are unsupported in your version of the application.
Also: The Change System Settings functional permission must permit users to Execute, or no Control settings changes are possible. See Adding or Modifying a User on page 71 and Permissions on page 74 for more about these.

Licenses

Some products require you to register a license. Use the *Settings* -> *Permissions* -> *Register License* menu item to open a dialog that lets you locate the license file. Select the file, and click *Register License* in the dialog, and you can use the licensed product.

Here are the steps to register a license file in this application:

1 Copy the `license.xml` file to an accessible local directory, for example the `owareapps` directory.

2 Open *Settings* -> *Permissions* -> *Register License.*

3 In the *Select License File* window browse to the `license.xml` file location and select the file.

4 Click the *Register License* button to import and register the license file.

5 The *License File Registered* dialog should appear. Click *OK*.

The License is now registered and the licensed product/functionality is now available.

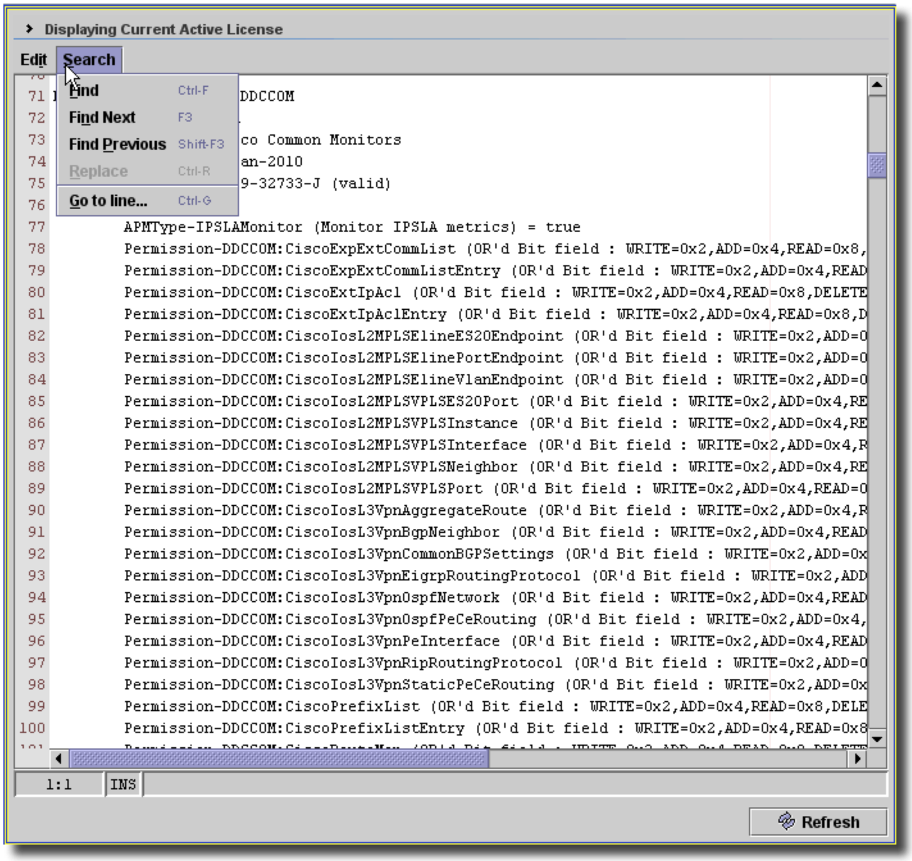
NOTE:

Importing a license may not immediately take effect. If this occurs you must restart application server or wait at least 15 minutes.

License Viewer

Open the application's license viewer with *Settings -> Permissions -> View Licenses*. This viewer displays the currently available licenses for the application.

Figure 5-1. License Viewer



```
                        DDCCOM
                        .
                        co Common Monitors
                        an-2010
                        9-32733-J (valid)

        APMType-IPSLAMonitor (Monitor IPSLA metrics) = true
        Permission-DDCCOM:CiscoExpExtCommList (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,
        Permission-DDCCOM:CiscoExpExtCommListEntry (OR'd Bit field : WRITE=0x2,ADD=0x4,READ
        Permission-DDCCOM:CiscoExtIpAcl (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,DELETE
        Permission-DDCCOM:CiscoExtIpAclEntry (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,D
        Permission-DDCCOM:CiscoIosL2MPLSElineES20Endpoint (OR'd Bit field : WRITE=0x2,ADD=0
        Permission-DDCCOM:CiscoIosL2MPLSElinePortEndpoint (OR'd Bit field : WRITE=0x2,ADD=0
        Permission-DDCCOM:CiscoIosL2MPLSElineVlanEndpoint (OR'd Bit field : WRITE=0x2,ADD=0
        Permission-DDCCOM:CiscoIosL2MPLSVPLSES20Port (OR'd Bit field : WRITE=0x2,ADD=0x4,RE
        Permission-DDCCOM:CiscoIosL2MPLSVPLSInstance (OR'd Bit field : WRITE=0x2,ADD=0x4,RE
        Permission-DDCCOM:CiscoIosL2MPLSVPLSInterface (OR'd Bit field : WRITE=0x2,ADD=0x4,R
        Permission-DDCCOM:CiscoIosL2MPLSVPLSNeighbor (OR'd Bit field : WRITE=0x2,ADD=0x4,RE
        Permission-DDCCOM:CiscoIosL2MPLSVPLSPort (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0
        Permission-DDCCOM:CiscoIosL3VpnAggregateRoute (OR'd Bit field : WRITE=0x2,ADD=0x4,R
        Permission-DDCCOM:CiscoIosL3VpnBgpNeighbor (OR'd Bit field : WRITE=0x2,ADD=0x4,READ
        Permission-DDCCOM:CiscoIosL3VpnCommonBGPSettings (OR'd Bit field : WRITE=0x2,ADD=0x
        Permission-DDCCOM:CiscoIosL3VpnEigrpRoutingProtocol (OR'd Bit field : WRITE=0x2,ADD
        Permission-DDCCOM:CiscoIosL3VpnOspfNetwork (OR'd Bit field : WRITE=0x2,ADD=0x4,READ
        Permission-DDCCOM:CiscoIosL3VpnOspfPeCeRouting (OR'd Bit field : WRITE=0x2,ADD=0x4,
        Permission-DDCCOM:CiscoIosL3VpnPeInterface (OR'd Bit field : WRITE=0x2,ADD=0x4,READ
        Permission-DDCCOM:CiscoIosL3VpnRipRoutingProtocol (OR'd Bit field : WRITE=0x2,ADD=0
        Permission-DDCCOM:CiscoIosL3VpnStaticPeCeRouting (OR'd Bit field : WRITE=0x2,ADD=0x
        Permission-DDCCOM:CiscoPrefixList (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8,DELE
        Permission-DDCCOM:CiscoPrefixListEntry (OR'd Bit field : WRITE=0x2,ADD=0x4,READ=0x8
```

Licenses appear listed in this screen. Click *Refresh* to query for additional licenses. You can search licenses with the *Search* menu items, and *Copy* file contents with the *Edit* menu items (the text here is read-only).

Customer Settings

This screen controls universal settings for your software.

General

The General panel lets you specify the product name and screen appearance.

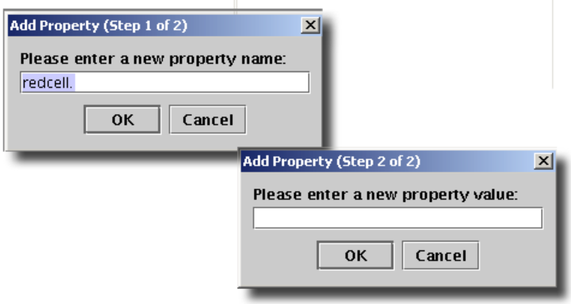
- **Product Name:**—Enter a product name in the *Product Name* field.
- **Title**—This text appears in the portal form title bar.
- **Branding Panel Height**—The height (in pixels) of the panel that appears under the menus.
- **Status Panel Height**—The height (in pixels) of the panel that appears beneath the work area in the portal form.

Properties

The Properties control panel provides an interface into the application's `settings.txt` file (in `owareapps\redcell\db`) and lets you view, add, delete, edit, and sort the entries in that file. The contents of this panel may vary if you have optional products or drivers installed.

The Properties panel features the following controls:

- **Add**—Opens a two-step dialog through which you can add a new property. Both steps appear below. In the first step, enter the name of the new property and click *OK*. Then enter a value for the new property and click *OK* to save it.



Add Property (Step 1 of 2)

Please enter a new property name:

redcell.

Add Property (Step 2 of 2)

Please enter a new property value:

- **Edit**—Opens a two-step dialog populated with the selected property. Change the name or path as appropriate and click *OK* to move to the second step. Specify the appropriate property value in the second dialog and click *OK* to implement your changes.
- **Remove**—Deletes the selected property from the list.
- **Copy**—Makes a copy of the selected property.

- **Move Up/Down**—Orders the list appearance. Note that the list is exported to the `settings.txt` file in the order of this panel; changing the sort order also changes the export order. This is for readability only.
- **Sort**—Sorts the listed properties alphabetically. A subsequent dialog asks you to confirm that you also want to change the order of properties exported to a `settings.txt` file.

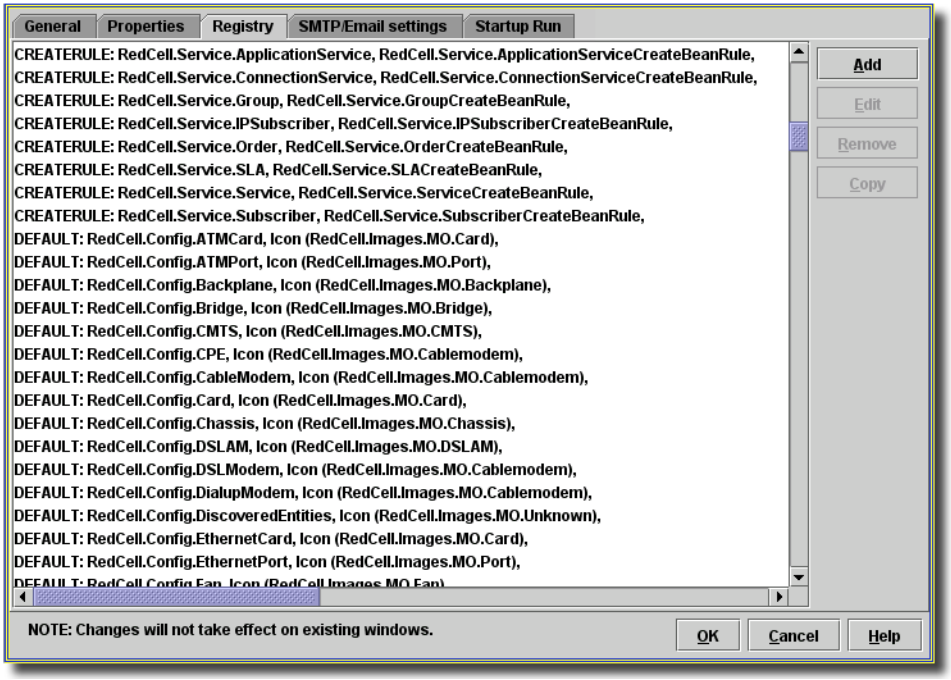
NOTE:

Settings for alarm count and view size settings may have a performance impact.

Registry

The Registry panel provides a graphical interface to manage the application's registry. The Registry lets the application access new classes. The parameters for each individual registry item determine how to interpret the entry, and let you specify default values and behaviors for that entry.

Figure 5-2. Registry Panel



```
CREATERULE: RedCell.Service.ApplicationService, RedCell.Service.ApplicationServiceCreateBeanRule,
CREATERULE: RedCell.Service.ConnectionService, RedCell.Service.ConnectionServiceCreateBeanRule,
CREATERULE: RedCell.Service.Group, RedCell.Service.GroupCreateBeanRule,
CREATERULE: RedCell.Service.IPSubscriber, RedCell.Service.IPSubscriberCreateBeanRule,
CREATERULE: RedCell.Service.Order, RedCell.Service.OrderCreateBeanRule,
CREATERULE: RedCell.Service.SLA, RedCell.Service.SLACreateBeanRule,
CREATERULE: RedCell.Service.Service, RedCell.Service.ServiceCreateBeanRule,
CREATERULE: RedCell.Service.Subscriber, RedCell.Service.SubscriberCreateBeanRule,
DEFAULT: RedCell.Config.ATMCard, Icon (RedCell.Images.MO.Card),
DEFAULT: RedCell.Config.ATMPort, Icon (RedCell.Images.MO.Port),
DEFAULT: RedCell.Config.Backplane, Icon (RedCell.Images.MO.Backplane),
DEFAULT: RedCell.Config.Bridge, Icon (RedCell.Images.MO.Bridge),
DEFAULT: RedCell.Config.CMTS, Icon (RedCell.Images.MO.CMTS),
DEFAULT: RedCell.Config.CPE, Icon (RedCell.Images.MO.Cablemodem),
DEFAULT: RedCell.Config.CableModem, Icon (RedCell.Images.MO.Cablemodem),
DEFAULT: RedCell.Config.Card, Icon (RedCell.Images.MO.Card),
DEFAULT: RedCell.Config.Chassis, Icon (RedCell.Images.MO.Chassis),
DEFAULT: RedCell.Config.DSLAM, Icon (RedCell.Images.MO.DSLAM),
DEFAULT: RedCell.Config.DSLModem, Icon (RedCell.Images.MO.Cablemodem),
DEFAULT: RedCell.Config.DialupModem, Icon (RedCell.Images.MO.Cablemodem),
DEFAULT: RedCell.Config.DiscoveredEntities, Icon (RedCell.Images.MO.Unknown),
DEFAULT: RedCell.Config.EthernetCard, Icon (RedCell.Images.MO.Card),
DEFAULT: RedCell.Config.EthernetPort, Icon (RedCell.Images.MO.Port),
DEFAULT: RedCell.Config.Fan, Icon (RedCell.Images.MO.Fan)
```

NOTE: Changes will not take effect on existing windows.

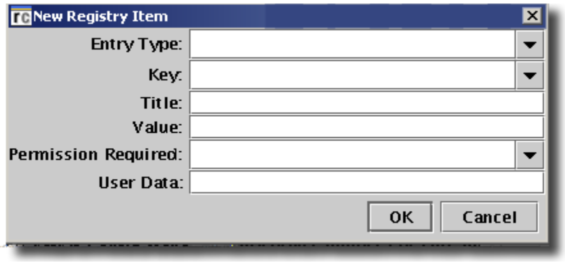
CAUTION:

Changes to this panel are *not* recommended. Changes here can impair the application.

The Registry panel has the following controls:

Add—Displays the *Editing Registry Item* dialog, where you can specify a new class. The class must already exist (created in the Oware Creation Center). Add an entry by filling out the fields in the *Editing Registry Item* dialog, shown below. Click *OK* to add the entry to the database.

Figure 5-3. Registry Edits

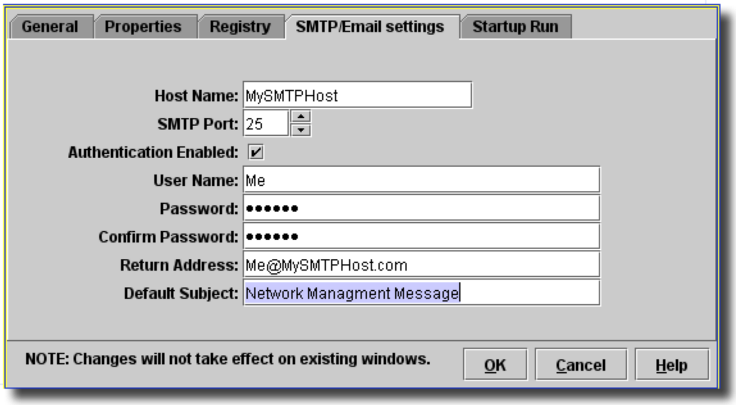


- **Edit**—Opens a dialog populated with the selected class. Make the appropriate changes and click *OK* to implement your changes.
- **Remove**—Deletes the selected class from the list.
- **Copy**—Makes a copy of the selected entry.

SMTP / Email Settings

This screen sets up the Simple Mail Transport Protocol (SMTP) and other e-mail settings for this application to send mail.

Figure 5-4. SMTP / Email Settings



Host Name: MySMTPHost
SMTP Port: 25
Authentication Enabled: ☑
User Name: Me
Password: ••••••
Confirm Password: ••••••
Return Address: Me@MySMTPHost.com
Default Subject: Network Managment Message

NOTE: Changes will not take effect on existing windows.

This screen has the following fields:

- **Host Name**—The name of the SMTP server.
- **SMTP Port**—Use the spinner to enter the port for SMTP on the named host.
- **Authentication Enabled**—Check to enable authentication on this host.

6

Properties

Overview

You can modify the application through the `.properties` files, typically in `oware\lib`, `oware\medserver\lib` and in `owareapps\<application>\lib`, for example: `owareapps\redcell\lib`. These are text files you can edit with any text editor. The application does not modify local files during the course of normal system operations. When an administrator or user modifies files, like properties or seed files, best practice is to note which files changed and back up that data. (This application stores all its operational data in its database.)

Particularly if you reinstall your application, installation recreates some properties files in their original form. If you modified those files since the original installation, reinstallation overwrites any changes. Therefore, it is safest to use the application's override capacity (see Overriding Properties on page 126), or to back up these files. See Properties Files on page 129 for files which may change through daily operation, and must therefore be restored from backup (unless you override properties) after reinstallation.

Commonly Modified Properties

Among other things, properties files configure the application's e-mail and use the Win32 print driver and scheduler defaults. Pound signs (#) indicate comments.

See Overriding Properties on page 126 for advice about modifying properties. You can override individual properties, regardless of where the originals are located.

Alarm and Resource Manager Refresh Rate

The following properties (in `redcell.properties`) specify the Alarm and Resource managers' refresh rate. Values for these properties are in seconds, and specify the interval between the processing for querying and displaying information rather than absolute intervals. For example, if your hardware takes 20 seconds to query and display data, and the refresh rate value is 30 seconds, then a new screen appears every 50 seconds (the processing time plus the interval).

The minimum refresh rate value allowed is currently 10 seconds. These are commented out by default.

```
com.dorado.redcell.manager.polling.AlarmManager
com.dorado.redcell.manager.polling.ResourceManager
```

You must close and restart the client for this to take effect.

Max Items Displayed

The *Max Items Displayed* field appears in the Resources, Alarm and Event History managers' screens (and several others). By default, the most this maximum can be for Resources, Alarm, and Event History is 5000 items. You can increase this maximum to as much as 10,000 by altering the following properties:

```
com.dorado.redcell.manager.max.rows.AlarmManager=9999
com.dorado.redcell.manager.max.rows.ResourceManager=9999
com.dorado.redcell.manager.max.rows.EventHistoryManager=9999
```

NOTE:

The "9999" number indicates a maximum of 10,000 items.

CAUTION:

Selecting large max numbers can have adverse performance impacts.

These appear commented out in the `redcell.properties` file, but are best altered in `installed.properties`, to avoid losing any alteration on upgrade.

E-mail Settings

These entries can specify the SMTP host name and return address in `installed.properties.` The following describes an alternative to the graphic user interface described in SMTP / Email Settings on page 119. The application uses this host name whenever it sends an e-mail; it uses the return address when e-mailing alarms from the Alarm Window, for example.

```
#redcell.smtphost=(put SMTP server name or IP here)
#redcell.smtphost.authentication.enabled=true
#redcell.smtphost.username=(user name here)
#redcell.smtphost.password=(password here)
#redcell.returnaddress=(return address)
#redcell.notification.message=(default message subject)

# EXAMPLE values
#redcell.smtphost=postoffice.myserver.com
#redcell.smtphost.authentication.enabled=true
#redcell.smtphost.username=John
#redcell.smtphost.password=secret
#redcell.returnaddress=EMAIL@postoffice.myserver.com
```

Typically, you can send e-mail within your SMTP host's domain without a login or password. The `SMTP.properites` (or `installed.properties` override) e-mail configuration overrides the following, if you need to set login and password.

In the unusual event that you must send mail outside your domain, set the login/password for the application in three properties that are now in `redcell.properties` for connecting to SMTP server using username and password.

```
redcell.smtphost.authentication.enabled=false

redcell.smtphost.username=admin

redcell.smtphost.password=password
```

Set the `redcell.smtphost.authentication.enabled` property to *true* and provide the username and password information for authenticating the application server with SMTP Server.

To receive email from event templates that trigger e-mails, the destination user must have an e-mail address in this software. See User Manager on page 69 for details. To e-mail from actions/ mapping, you just need to type in email account in the actions and then map the actions. No need to add anything to the user manager.

Win32 Print Driver

This Boolean value lets the application use the Win32 custom print driver.

```
# Set to true to enable the use of the

# Win32 custom print driver,

# which speeds up printing of large reports in the application.

StyleReport.useCustomDriver=true
```

Printer Properties

The following polling properties are in `oware\lib\owmediation.properties`. Increase them if you manage a network with more than 1000 printers. As with all properties, best practice is to override them (see Overriding Properties on page 126).

```
# Polling Engine Properties

# The properties below should be used for controlling the network 
bandwidth

# and managing the number of network entities.


# The property specifies a threshold limit, which if crossed will put the

# pending subscriptions on hold till the threshold is recovered.

oware.mediation.polling.max.network.bytes=10240000
```

```
# This property defines the max number of subscriptions in a time slot.

oware.mediation.polling.max.subscriptions.per.timeslot=25


# This property defines the timeslot bandwidth.

oware.mediation.polling.max.bytes.per.timeslot=1024000


# This property defines the thread pool size used for executing
subscriptions.

# This property should be changed depending on the network entities to be
polled.


oware.mediation.polling.mbean.thread.pool.size=10
```

NOTE:

These properties are relevant only if you have a printer driver installed.

Defaults

This section of the properties file sets the default runtime of the application scheduler and specifies whether or not a reverse lookup, to associate a host name with an IP address, occurs during discovery.

```
# Defaults

#

redcell.scheduler.defaulttime=02:00


#

# if true, reverse lookup is performed in GenericDiscoveryRule

# (scheduled Device Discovery) to obtain host name.

# if false, host name is populated with IP address

#

redcell.discovery.usedns=true
```

NOTE:

This default time is in 24-hour format. The 02:00 default is 2AM. For 2PM, enter 14:00.

installed.properties

This file (owareapps\installprops\lib\installed.properties) contains defaults installed with your package. An example of this file appears below. Installation automates the insertion of the [host name] variable:

```
#************************************************************
#  The following properties override those found in         *
#  oware/lib/*.properties in order to establish valid       *
#  properties for this installation.                        *
#************************************************************


oware.database.host=[host name ]
com.dorado.bom_dbms.preferred_db_type=rdbms
oware.installed.package.name=[Package Name]
oware.installed.package.version=[Package Version]
OWARE.CONTEXT.SERVER.URL=jnp://[host name]:1099
```

The OWARE.CONTEXT.SERVER.URL, when present, disables an otherwise dynamic lookup of this server. Devices that do not support multicast (for example, some Dell switches) require this be a static address—the URL in this property. You would have to use this property when connecting to an application server through a VPN that restricts multicast traffic. You must list all additional servers, comma-delimited (OWARE.CONTEXT.SERVER.URL=jnp://[host1]:1099, jnp://[host2]:1099...), if you have a clustered installation.

Dell installations explicitly set the server URL on clients. This URL assumes the application server is running on the default port range. If ports conflict, use the -n [Node Number] parameter in a command line to start application server so it uses something other than a default port range.

If your client cannot connect and the server log shows it cannot bind to port 1099 (or 11099, and so on), then stopping application server from the client does not work; client applications cannot communicate with the application server. In this case, to stop application server, you must kill the java.exe processes on the server machine. The tray icon should then indicate the application server is stopped.

To change the port range for application server, modify the node number property for appserver in oware\lib\pmstartup.dat. By default (upon installation) the property is as follows:

```
application.server.node.number=0
```

To use a different part range, change zero (0) to 1, 2 or 3.

Once the application server starts and listens (no bind errors), you still have to change port settings for the client connections. For each installation (server and client) modify a URL setting in `owareapps\installprops\lib installed.properties`. An example of default setting (hostname varies) would be as follows:

```
OWARE.CONTEXT.SERVER.URL=jnp://hostname:1099
```

The application server node number should prefix the `1099` port if greater than 0. For example, using `application.server.node.number=1` in `pmstartup.dat` would imply all installations need the following setting in installed.properties:

```
OWARE.CONTEXT.SERVER.URL=jnp://hostname:11099
```

NOTE:

For a complete list of port settings and protocols used by this application, see Ports Used on page 35.

Overriding Properties

Best practice is not to change default properties, but to override them. This eliminates updates or new installations overwriting property files you have tuned. If you override values, then backing up the override file(s) is essential.

To override a property controlling all but mediation, put it in a file (whose name ends in `.properties`) in the following directory under `owareapps`: `installprops\lib`. You can override mediation server properties in `owareapps\installprops\medserver\lib`. Application property values are loaded first and you can override those values here.

The following is an example of property file content to override a cache timeout:

```
#============================================
# Dependencies
#============================================
product.dependencies=redcell

#============================================
# OpenManage Network Manager Assurance Overrides
#============================================
# set event template cache timeout to 1 minute
redcell.assurance.batch.processing.event.template.cache.expiration=60000
```

If you have more than one product dependency, add another product.dependency property.

CAUTION:
If any of the dependency directory names (for example, `owareapps\redcell`) do not exist, then the application does *not* load the override file.

Consult the comments in the properties files you are overriding for further information about specific properties.

Mediation Event Management Properties

Several property file settings configure batching operations of SNMP traps at the Mediation Agent before those are sent to the rules in Application Server. The property file settings allow administrators flexibility so that processing and batching can accommodate the particular network environment. Settings like the number of traps include in a batches, which traps to reject, correlation and others are available. The maximum number of traps that can be configured into a single batch is 2,000.

Event services are deployed as managed beans. Initial setting come from the following files:

- Service configuration for an application server is in `owareapps/eventmgmt/server/conf/em-service.xml`
- Service configuration for mediation is in `owareapps/eventmgmt/server/conf/em-med-service.xml`

You can see active settings and possibly modify them by using the JMX console from a browser:

```
http://serverIP/jmx-console on Windows

http://serverIP:8080/jmx-console on Linux
```

The default user/password is `admin/dorado.` Set a filter to oware:* for a more concise view of the relevant settings

Some settings require that a service is stopped and restarted for the setting to take effect. Only changes made to server/conf files on disk will take effect after a restart.

- See `NotificationProcessingMBean` for event processing settings
- See `OWSysLogMBean` for syslog listener queue and archive settings

Here are some examples of exposed service settings for Event Management:

```
<!--
   | NotificationProcessingMBean
 -->
  <mbean code="com.dorado.assure.mediation.NotificationProcessingMBean"
         name="oware:service=NotificationProcessingMBean">
    <attribute name="TransportBatchSize">2000</attribute>  <!--# events-->
    <attribute name="TransportBatchInterval">500</attribute>  <!--#
milliseconds-->
    <attribute name="ServerRetryInterval">5</attribute>  <!--# seconds-->
    <attribute name="ServerRefreshInterval">30</attribute>  <!--# seconds--
   >
    <attribute name="SuppressUnknownSource">false</attribute>
    <attribute name="SuppressInformational">false</attribute>
```

NOTE:

Setting SuppressUnknownSource to true rejects all event from unknown sources—without historical event records. Setting SuppressInformational to true rejects all events that do not produce an alarm, correlation or automation (not necessarily just events of informational severity). Basically it suppresses events that are only inserted in history.

```
<attribute name="QueueBatchSize">1000</attribute>  <!--# entries-->

    <attribute name="QueueFileBufferSize">131072</attribute>  <!--# bytes--
   >

    <attribute name="QueueFileName">@OWARE_USER_ROOT@/owareapps/eventmgmt/
   temp/event_spool.

dat</attribute>

    <attribute name="QueueMaxFileSize">20971520</attribute>  <!--# bytes-->

    <attribute name="QueueMaxSize">100000</attribute>  <!--# entries-->

    <depends>oware:service=HAServiceController</depends>

  </mbean>


<!--

   | SNMPListenerMBean

 -->

  <mbean code="com.dorado.assure.mediation.SNMPListenerMBean"

         name="oware:service=EMSNMPListenerMBean">

    <attribute name="V3AuthRefreshInterval">60</attribute>  <!--# seconds--
   >

    <depends>oware:service=NotificationProcessingMBean</depends>

  </mbean>


<!--

   | SysLogMBean

 -->

  <mbean code="com.dorado.assure.mediation.OWSysLogMBean"

         name="oware:service=EMSysLogMBean">

    <attribute name="SpoolZipLevel">1</attribute>

    <attribute name="SpoolReset">true</attribute>

    <attribute name="QueueLimit">50000</attribute>

    <attribute name="QueueFetchPref">5000</attribute>
  <attribute name="MaxQueueReadSize">50000</attribute>

  <attribute name="SpoolFileName">syslog_spool.dat</attribute>

  <attribute name="SpoolPath">@OWARE_USER_ROOT@/owareapps/eventmgmt/
 temp</attribute>

  <attribute name="SpoolSize">5242880</attribute>

  <attribute name="ArchiveMaxLength">52428800</attribute>

  <attribute name="ArchiveEnabled">false</attribute>

  <attribute name="ArchivePath">@OWARE_USER_ROOT@/owareapps/eventmgmt/
 archive</attribute>

  <attribute name="ArchiveZip">true</attribute>

  <depends>oware:service=NotificationProcessingMBean</depends>

</mbean>
```

Properties Files

The following files contain properties that might be modified by the application’s users and administrators. Best practice is to override any properties you want to change in these files. See Overriding Properties on page 126 for instructions.

NOTE:

Client installations where no DNS exists (for example across a VPN) require you to replace your application server’s local host name with its IP address in the application’s properties files in `oware\lib` and `oware\medserver\lib`.

Best practice is to backup these files, or those that override them. All paths are given relative to the installation directory. Note that this is not an exhaustive list. Some properties files are unique to addons or third-party products, and are not included.

oware\addons\ezmediation\lib

allmsgs_en_US.properties

jaxb-xjc-1.0-ea.jar

owclasspath.properties

owezcli.properties

owezexports.jar

owezmediation.jar

oware\addons\transactionengine\lib

temsgusenglish.properties

transengine.properties

oware\addons\workflow\lib

workflowapp.properties

workflowbase.properties

workflowdemo.properties

workflowlogicon.properties

oware\addons\workflow\resourcebundles

workflowmsg_en_US.properties

oware\examples\ClusterMonitor\Cluster

Cluster.properties

oware\lib

Oware.properties

allmsgs_en_US.properties

debugger.properties

<username>_formsettings.properties

owappserver.properties

owappserverstartup.proper

owcorba.properties

owdatabase.properties

oweditorsettings.properti

owfc.properties

owfc_web.properties

owframework.properties

owimportjdbctables.properties

owjdbcstorage.properties

owjms.properties

owlicense.properties

owlogicworkspace.properties

owmediation.properties

owmediationlisteners.prop

owmisc.properties

owpartition.properties

owsce.properties

owsecurity.properties

owstoredprocedures.properties

owwebservices.properties

services.properties

oware\medserver\lib

Oware.properties

owappserverstartup.proper

owexternalapp.properties

owinternal.properties

owlicense.properties

owmediation.properties

owmediationlisteners.prop

owmisc.properties

owsecurity.properties

owareapps\assure\lib

asmsgs_en_US.properties

assure.properties

assurecompmgr.properties

sla.properties

owareapps\redcell\lib

owuserappserver.properties

owuserclasspath.properties

rccompmgr.properties

rcmsgsusenglish.properties

redcell.properties

7

Database Management

Introducing Databases

This chapter discusses database management procedures. This discussion includes installation with the embedded MySQL database.

In addition to correctly sizing your database, best practice is to develop a plan to regularly back up the database, including steps to verify this backup with recovery. The frequency of backups depends upon your environment, but you should back up often enough to minimize data loss.

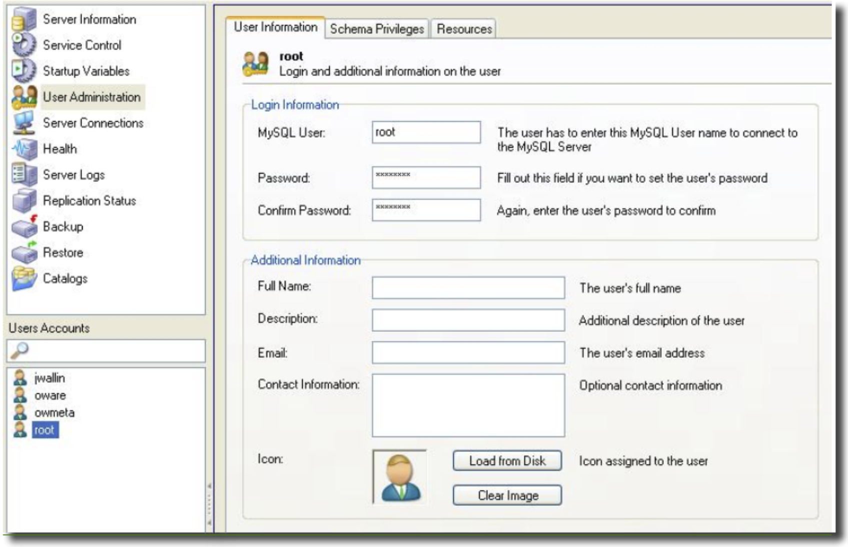
The following describes administration for the basic database, installed with the application. If your system has the optional performance monitoring add-on, then you may also want to install a separate database for performance data. Consult the performance monitoring chapter in the *User Guide* for instructions about how to do this.

Administration Basics

You can download the MySQL administrator and, can get its manual at *dev.mysql.com/downloads/mysql/5.0.html* (GUI tools and Documentation links). This optional tool has a graphical user interface, and provides an overview of the MySQL settings. It displays performance indicators graphically, making it easier to determine and tune server settings.

Start this tool to view databases. When you install the embedded database, installation creates two databases: `owmetadb` and `owbusdb`. The installation also creates a `root` and `<O/S user>` login (users *oware* and *owmeta* are created, too).

Figure 7-1. MySQL Users



root
Login and additional information on the user

Login Information

MySQL User: root — The user has to enter this MySQL User name to connect to the MySQL Server

Password: ******** — Fill out this field if you want to set the user's password

Confirm Password: ******** — Again, enter the user's password to confirm

Additional Information

Full Name: — The user's full name

Description: — Additional description of the user

Email: — The user's email address

Contact Information: — Optional contact information

Icon: — Icon assigned to the user

The default password for database access is *dorado*. Read the tool's instructions for specifics about how to use it.

Database Security

The properties that control the default user and password for databases are in

```
oware/lib/owdatabase.properties
```

They are these properties with their default values:

```
## Database logon name
com.dorado.jdbc.user=oware
## Database logon password
com.dorado.jdbc.password=dorado
##******
```

You can change the password after installation, but not the username. If you change the password in a database tool for either Oracle or the embedded database, you must change it in these properties.

CAUTION:
Best practice is to change the default password. You must change it in both the database and the above properties.

NOTE:

As always, properties in `owareapps/installprops/lib/installed.properties` override those in other property files, and are preserved if you upgrade your software.

Database Timeout

When managing large networks or equipment with many interfaces, you may have to increase a timeout property: the `com.dorado.bom.lock_timeout` property in `owareapps\installprops\lib\installed.properties` (originally in `owdatabase.properties`).

Copy that property into `installed.properties`, then increase this setting based on the equipment managed. Generally, you should set this value to the maximum number of interfaces you expect your network elements to have. For example, if the element is expected to have 500 logical interfaces then the timeout value should be set to 500.

NOTE:

The minimum recommended timeout value is 60 seconds.

Database Emergency E-mail

To send an e-mail notification to emergency support contacts, if the OpenManage Network Manager database becomes unavailable do the following:

1 In the file `owareapps/installprops/lib/installed.properties` add the following property:

```
oware.monitor.database=true
```

2 Ensure that the following Email MBean properties are set:

```
SMTPHost
```

```
DefaultSenderAddress
```

```
EmergenyContacts
```

The `emergenyContacts` attribute is a comma-separated list of e-mail addresses for the recipients of emergency notifications. The following describes where to set these:

Open the file `$OWARE_USER_ROOT/oware/jboss-3.2.7/owareconf/oware-service.xml` in a text editor. The following section contains the configuration for the email MBean:

```
<!-- Email MBean -->

<!-- Change the SMTP Host attribute below to point to the right SMTP server
   -->

   <mbean code="com.dorado.mbeans.OWEmailMBean"

       name="oware:service=OWEmailMBean">

       <attribute name="SMTPHost">smtp.MyMail.com</attribute>

       <attribute name="Port">25</attribute>

       <attribute name="UserName"></attribute>

       <attribute name="EmergencyContacts"></attribute>

<attribute name="DefaultSenderAddress">Me@MyMail.com</attribute>

       <attribute name="MaxRatePerMinute">200</attribute>

       <depends>jboss:service=@PART_NAME@Partition</depends>

       <depends>oware:service=ClusterPrimaryDesignator</depends>

       <depends>jboss.j2ee:jndiName=RuleEngine,service=EJB</depends>

   </mbean>
```

This file’s settings override the Graphical User Interface settings for mail described in the *Properties* chapter of the *Administration Section*.

Embedded Database Sizing

The initially installed Embedded Database is a relatively small instance—possibly too small for your application. This is important to note because errors occur when you reach the size limit of the database. Therefore, after installing, you may want to resize the Embedded Databases to fit your application. See Modifying the MySQL File Systems for instructions about modifying an existing, installed system.

NOTE:

If you are planning to use your system for Active Performance Monitoring, best practice is to store performance data in a separate database. This improves performance. See Creating or Updating a Monitor on page 771 in that chapter in the *User Guide*.

Modifying the MySQL File Systems

If you have upgraded from older operating systems (Windows® 3.1, for example), you may still have a FAT file system that limits your database size or expansion beyond 2GB. The database is a file as far as the operating system is concerned, and FAT limits file size. There is also a 4GB limit on early versions of NTFS that may linger because of upgrades.

To change the installed database sizes, you must edit the configuration file:

- Windows: `%SystemRoot%\my.ini`

The following line controls maximum database size (at end):

```
innodb_data_file_path = d:/work/oware3rd/mysql/ibdata/
ibdata1:600M:autoextend:max:2000M
```

To recreate database after modifying config file, use the following command from the application server:

```
        loaddb -q -d -m
```

Syntax details:

```
innodb_data_file_path =
pathtodatafile:sizespecification;pathtodatafile:sizespecification;...
```

```
innodb_data_file_path = ...
;pathtodatafile:sizespecification[:autoextend[:max:sizespecification]]
```

If you specify the last datafile with the *autoextend* option, InnoDB will extend the last datafile if it runs out of free space in the tablespace. The increment is 8 MB at a time. An example:

```
                    innodb_data_file_path = /ibdata/ibdata1:100M:autoextend
```

This instructs InnoDB to create just a single datafile whose initial size is 100 MB and which is extended in 8 MB blocks when space runs out.

If the disk becomes full you may want to add another datafile to another disk, for example. Then you must look at the size of `ibdata1', round the size downward to the closest multiple of 1024 * 1024 bytes (= 1 MB), and specify the rounded size of `ibdata1' explicitly in `innodb_data_file_path`. After that you can add another datafile:

```
innodb_data_file_path = /ibdata/ibdata1:988M;/disk2/
ibdata2:50M:autoextend
```

Be cautious on filesystems where the maximum file-size is 2 GB. InnoDB is not aware of the operating system's maximum file-size. On those filesystems you might want to specify the max size for the datafile:

```
innodb_data_file_path = /ibdata/ibdata1:100M:autoextend:max:2000M
```

Some additional caveats:

- You must use foreslashes (/) instead of backslashes (\) when you specify the path.
- The subdirectory iblogs must be used by MySQL exclusively
- Make sure you enough disk space available on the data path specified

- You can add as many entries as you like. However, you can use `initial, max` and `autoextend` only in the last entry, and must change the first entry to reflect the actual size of the database.
- The name of filepath must be valid on the filesystems. However, you must always have your leaf directory in the path as ibdata.

Database Backup / Restoration

The recommended procedures for database backup and restoration for the embedded database follows. Best practice is to develop backup plans using these procedures for the sake of database reliability.

For MySQL (embedded) databases, use this database's native backup/restore utilities, described in the following section, to backup the `owbusdb` database. Refer to the manual available at *dev.mysql.com/downloads/mysql/5.0.html* for instructions about backup and restoration.

MySQL Backup / Restore

Follow these instructions to back up and restore the embedded Mysql database using native MySQL utilities on a command line. Default MySQL Backup and Default MySQL Restoration describe this process within this application:

Backup

Open a command shell (*Start* -> *Run* `cmd`, in Windows), and then type the following at the prompt replacing USERNAME and DATABASE. By default, the databases are `owbusdb` and `owmetadb`.

```
mysqldump -a -u USERNAME --password=[name] DATABASE > FILENAME.mysql
```

This writes the DATABASE to a plain-text file called `FILENAME.mysql`. This file is a full backup with which you can fully restore your database in case of problems.

NOTE:

Defaults for the database are oware (login) and dorado (password).

Restoring

Restoring from `FILENAME.mysql` is a three step process. This occurs, again, in a command shell:

1 Drop the database:

```
mysqladmin -u USERNAME -p drop DATABASE
```

or

```
mysqadmin -u USERNAME --password=[password] drop DATABASE
```

NOTE:

Red Hat Linux requires rm -rf owmetadb to drop this database.

2 Recreate the database

```
mysqladmin -u USERNAME -p create DATABASE
```

or

```
mysqadmin -u USERNAME --password=[password] create DATABASE
```

3 Import the backup data

```
mysql -u USERNAME -p DATABASE < FILENAME.mysql
```

or

```
mysql  -u USERNAME --password=[password] DATABASE < FILENAME.mysql
```

Default MySQL Backup

The following command lines back up owbusbd and owmetadb to a file. The following also assumes you have run the oware command in the shell, and have changed directories to owareapps/db_backup.

```
mysqldump -a -u oware --password=dorado owbusdb > owbusdb.mysql
mysqldump -a -u oware --password=dorado owmetadb > owmetadb.mysql
```

Note that this example uses the default user name (oware), default password (dorado), and backs up both the owbusdb and owmetadb databases.

Default MySQL Restoration

Restoration is the three-step process outlined above:

1 Remove existing database

```
mysqladmin -u oware --password=dorado drop owmetadb
mysqladmin -u oware --password=dorado drop owbusdb
```

2 Create a new database

```
mysqladmin -u oware --password=dorado create owmetadb
mysqladmin -u oware --password=dorado create owbusdb
```

3 Import the data previously backed up.

```
mysql -u oware --password=dorado owmetadb < owmetadb.mysql
mysql -u oware --password=dorado owbusdb  < owbusdb.mysql
```

8

The Application Server

Introducing the Application Server

The Application Server is the central engine for all components on both server and client systems, relieving clients of significant programming infrastructure overhead. The Application Server is a set of Enterprise JavaBeans (EJBs) embedded within EJBs provide remote access from clients to other components—the Virtual Rule Machine (VRM), Mediation Services, the Event Channel, and other services. For example, a client application that needs to check information in the classes database does not access application databases directly. Instead, the Application Server's EJB mediates any insertions, queries, updates, or deletes.

Starting the Server

You must start Application Server so you can use most of the Execution Center (OEC) components.

NOTE:

You can ensure command lines referred to in the following steps have set your command shell environment correctly with the `oware` command (in Windows®).

To start application server, from the command line enter `startappserver`. Once an Application Server starts, the name of the log file appears in its shell. To see its progress, use this command:

```
tail -f <logname>
```

Logging

When you start application server as a service any console output writes to a log file in `$OWARE_ROOT/jboss_<version number>/server/oware/log` (for mediation, see `$OWARE_ROOT/jboss_<version number>/server/owaremed1/log`). If you want to see the console output as it is generated, then run `startappserver` at a command line rather than having it start as a server.

Command Line Options

The following is a transcript of this command line:

```
startappserver -?
```

Read this to understand the options available when starting application server, particularly for clustering.

Properties Best Practices

Best practice is to configure application and mediation servers by overriding properties that configure them. If you do not override properties settings, any upgrade to your software resets them to the defaults. Override properties in the files `owareapps\installinfo`. You can read the properties files overridden in `oware\lib` and in `owareapps\ <application name>\lib` for details about what can change. If you put a property in a file with a `properties` extension in `owareapps\installinfo`, that value overrides the defaults.

NOTE:

For better performance when overriding, use the IP address rather than *localhost* for the database server name.

9

Starting The Application

Overview: Starting the Application

This application enforces security at the client level. You must have a valid user ID and password to log on to the application and use its features. You must also have an installed license (see Installing Licensing on page 144).

Before you can start to use this application, you must start Application Server. Starting Application Server starts both application server and mediation service “daemons” on UNIX.

The tray icons (in the lower right corner of the Windows start bar) indicate the current service condition.

Icon	Status
☒	Offline (no status available, or not controlled by server manager)
▶	Running (initializing or shutting down)
▶	Ready
●	Stopped

You can also right-click the icon to see the client menu.

The *logs* items let you see the recorded logs for the application. You can *Start* or *Stop* the service(s) running on your host, and, with the *About* menu item, display the Server Manager about box.

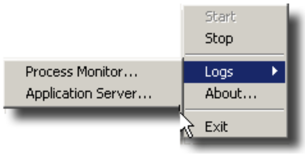
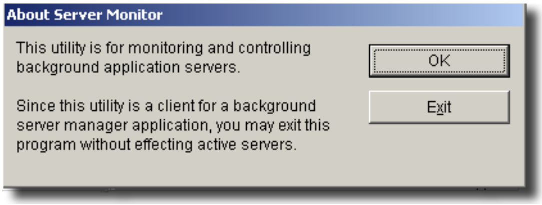


Figure 9-1. About Process Monitor



About Server Monitor

This utility is for monitoring and controlling background application servers.

Since this utility is a client for a background server manager application, you may exit this program without effecting active servers.

NOTE:

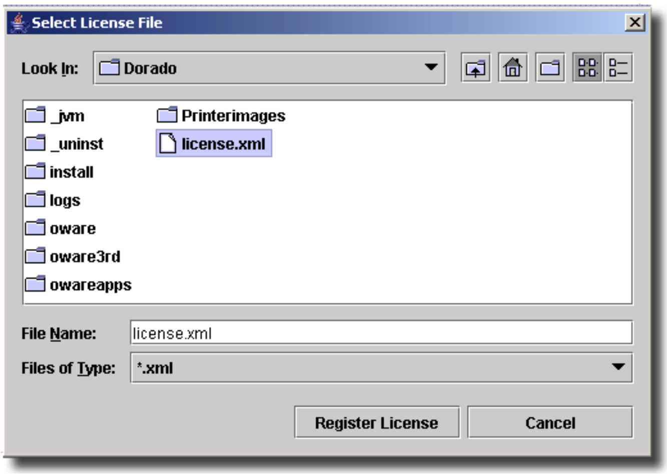
System changes can make the server manager system tray icon disappear in Windows while the process is still running. If you cannot make your icon reappear, try running `pmtray -r` from a command line, then restart the server manager with `pmtray`.

To start the application client from Windows, select the application icon from the Start menu

Installing Licensing

You can install licenses for basic Application Server functionality, and for extended functionality for clients, drivers and applications. You can always install these from the *Settings -> Permissions -> Register License* menu item in the application client. Select the license file in that dialog on any client, and the Application Server will store the permissions to use that functionality on the database.

Figure 9-2. License File Selection



Select License File

Look In: Dorado

File Name: license.xml

Files of Type: *.xml

Application Server now requires a license. It should be installed by default, but if it is unavailable for any reason the Application Server shuts down and will not start.

To install the license from a command line before you start Application Server, run the following commands in a command shell (In Windows, open a command shell with *Start -> Run* `cmd`):

```
>oware
>licenseimporter g:\path\license.xml
```

When it is finished, you should see:

```
importing.....done
```

The `g:\path` portion of this command line is an example. Correct it to wherever you have stored your license file—typically on the directory where you installed from.

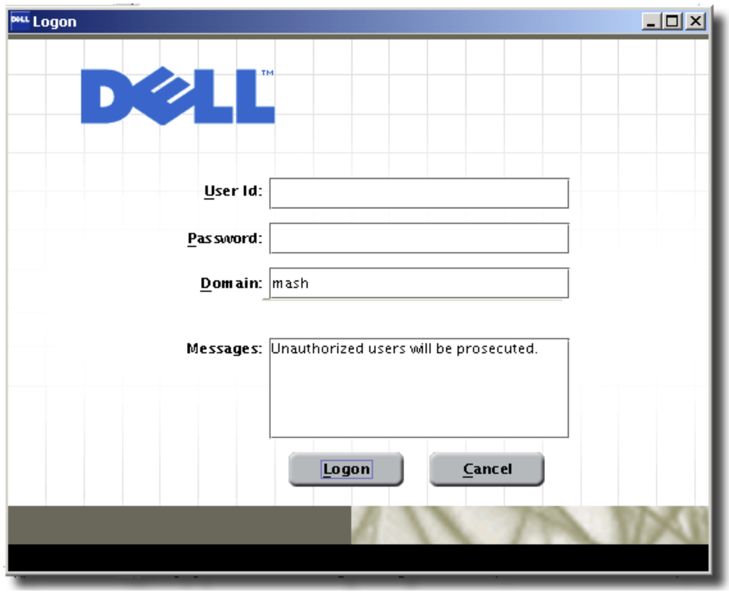
NOTE:

If you import a license that, for example, changes the application's capabilities, it does not immediately take effect. You must restart application server or wait at least 15 minutes.

Logging On

To log on, type a valid user name and password at the logon prompt. The default user name/ password is *admin/[blank]*. The application prompts you to change the password the first time it starts

Figure 9-3. Login Prompt



User Id:

Password:

Domain: mash

Messages: Unauthorized users will be prosecuted.

The *Domain* field is the Application Server partition (defaulting to the hostname of the Application Server in a single-server installation).

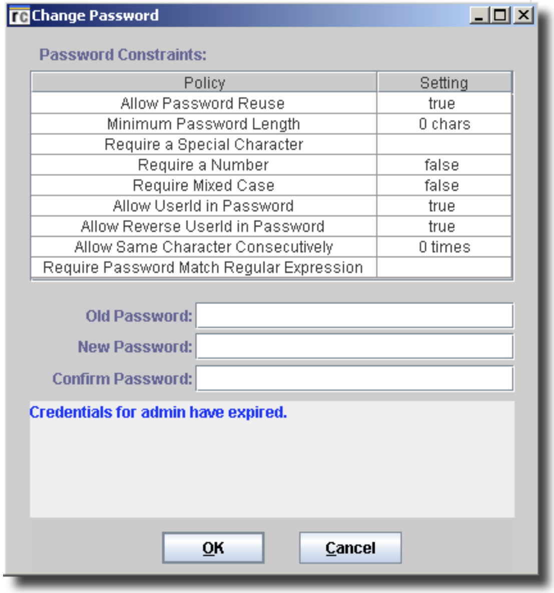
NOTE:

Best practice for security in a production installation is to change your password from the default.

Change Password

After your initial login, the application prompts you to change the password. By default, this does not restrict the password to having special character(s), or number(s). It also allows both upper and lower case letters for the new password.

Figure 9-4. Change Password Dialog



Change Password

Password Constraints:

Policy	Setting
Allow Password Reuse	true
Minimum Password Length	0 chars
Require a Special Character	
Require a Number	false
Require Mixed Case	false
Allow UserId in Password	true
Allow Reverse UserId in Password	true
Allow Same Character Consecutively	0 times
Require Password Match Regular Expression	

Old Password:

New Password:

Confirm Password:

Credentials for admin have expired.

You can set password constraints in the application (provided you have permissions to do so). See the online help for details.The *Settings -> Change Password* menu item lets you change your password later.

Disabled Accounts

By default, you have three chances to enter the correct password before the system aborts the login. System administrators can change this number. The system does not let someone log on to an account disabled by too many log on retries. The administrator can also disable an account, in which case the lock-out period does not apply. A system administrator must re-enable the account before the user can access the application, or the login lockout period must have passed. See the *Administration Section* for instructions about how to configure the lockout period.

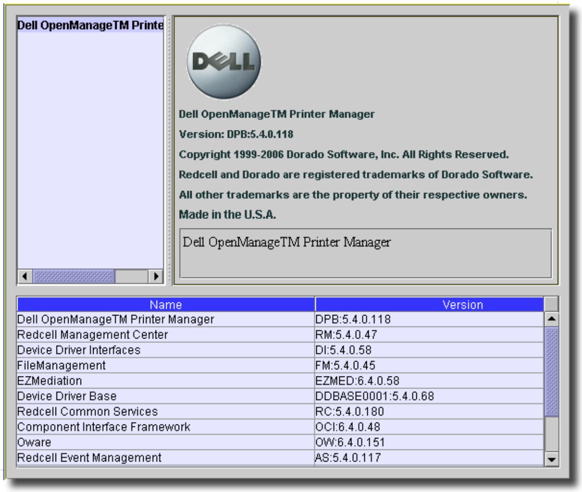
Application Server

The Application Server lets the system process incoming events and communicate with resources and network devices. If the client application cannot connect to an Application Server, a warning message appears and the client does not launch.

The About Box

To see which products are installed, and what versions, select the *Help -> About* menu item.

Figure 9-5. About Box



Dell OpenManageTM Printe

Dell OpenManageTM Printer Manager

Version: DPB:5.4.0.118

Copyright 1999-2006 Dorado Software, Inc. All Rights Reserved.

Redcell and Dorado are registered trademarks of Dorado Software.

All other trademarks are the property of their respective owners.

Made in the U.S.A.

Dell OpenManageTM Printer Manager

Name	Version
Dell OpenManageTM Printer Manager	DPB:5.4.0.118
Redcell Management Center	RM:5.4.0.47
Device Driver Interfaces	DI:5.4.0.58
FileManagement	FM:5.4.0.45
EZMediation	EZMED:6.4.0.58
Device Driver Base	DDBASE0001:5.4.0.68
Redcell Common Services	RC:5.4.0.180
Component Interface Framework	OCI:6.4.0.48
Oware	OW:6.4.0.151
Redcell Event Management	AS:5.4.0.117

The about box appears with the products listed on the left, and the version information for the selected product on the right. About boxes for device drivers list supported devices and their operating systems.

Logging Off

When you close the application, it asks if you want to *Show Editor* (with any pending edits), *Close*, *Close ALL*, *Close All & Exit*, or *Cancel* your request to log off. In any case, a confirmation dialog appears whenever you exit the client application.

Web Client

This application now offers a portion of its functionality as a web client. To view the web client, open a browser (Internet Explorer® 6.0 or later, or Firefox® 1.5.0.3 or later) and open the following URL:

```
http://[appserver]:[port number]/
```

The “`[apppserver]`” text should be the name of the Application Server host.The `[port number]` defaults to 80 or 8080, depending on the installed operating system. For Windows, 80 (equivalent to leaving `[port number]` blank) is the default. For other platforms, specify 8080 after a colon. If you have a popup blocker installed, you may have to click a link in the first web page that opens. When the web client opens, it presents a login screen. Once you log in, a subset of the application's services appear on the left navigation pane.

NOTE:

When you first log in, you may have to restart the browser once you have reset your password.

For information about how to use the interface for web client capabilities, consult the relevant portion of this guide.

CAUTION:

When you start a Web client, you must have a screen resolution of at least 1024x768. A warning message appears if you do not have this screen resolution, and while you can see the client, you can work with it only with difficulty. If all fields in a screen do not appear, resize the browser.

Also: Firefox is an open source browser, so many variations are available. Supported versions come from www.mozilla.com. If you get an unsupported version, you may see a message like *Unexpected errors may occur.*

In some cases the main title bar of the browser may not reflect which editor was just opened.

Re-sizing the browser can sometimes interfere with screen appearance. Other times, frame elements do not automatically update. For example, deleting a layout does not update the available layout list visible from the toolbar. To resolve such issues, refresh the entire browser (Ctrl+R, or F5, or re-size the window).

Linux / Windows Browser

When trying to display a Linux application server with a Windows client browser, you may see an error message. To fix this, put `java.awt.headless = true` into `owareapps/installprops/lib/installed.properties` and restart application server.

Online Help for Web Client

Online help does not work with the web client. On the other hand, the Acrobat version of the *User Guide* is the source of online help, and could offer the same kind of information if copied to the computer where the web client runs. You must have Acrobat installed on that client, but can refer to the *User Guide*'s version of online help there.

Secure Web Client Connections

Web client connections enable HTTP and HTTPS by default on their respective ports. To make your client connection completely secure, you can disable HTTP and use HTTPS on port 443 in Windows, or 8443 in Linux (rather than HTTP on 80—the unwritten default).

For a connection that is exclusively secure (HTTPS only, HTTP disabled), you must add a property to `owareapps/installprops/lib/installed.properties` with a text editor. Here is that property:

```
appserver.web.enable.https=true
```

This disables the HTTP connector thereby securing the server. To use HTTPS, then, use a URL like this:

```
https://MyAppserver:443
```

To force the client to use HTTPS (secure) for web connections to the server (such as opening the toner ordering pages) add the following line to `owareapps/installprops/lib/installed.properties` (this will be the same file as above when addressing this issue with the client when running locally on the server).

```
appserver.enable.https=true
```

You may also start the Application Server with a `-e` parameter, to initiate the secure connection. The command line is `startappserver -e.` Doing so disables the HTTP connection. Without the `-e` option, OpenManage Network Manager supports both HTTP and HTTPS connections.

Web vs. Java Clients

Web clients are more limited than Java clients. For example, the “are you sure you want to do this?” confirming dialog boxes that appear on Java clients do not appear on the web. The following outlines specific features supported by web and Java clients:

Web Client	Java Client
Inventory	
Resource Discovery	Resource Discovery
Discovery Profiles	Discovery Profiles
Resources	Resources
Ports	Ports
Printers	Printers
Resource Roles	Resource Roles
Groups	Groups
Links	Links
Locations	Locations
Vendors	Vendors
Contacts	Contacts
	Topology Views
Group Operations	Group Operations
	Network Objects - nameSpaces
	Network Objects
	Pools
	Pool Allocations
Subnets	Subnets
Event Services	
Alarms	Alarms
Event History	Event History
Actions	Actions
Event Processing Rule	Event Processing Rule
Event Definitions	Event Definitions
Application Services	Application Services
Application Services	
Processes	Processes
OS Services	OS Services
Application Services	Application Services
AS Groups	AS Groups

Web Client	Java Client
Propagation Policies	Propagation Policies
File management	
	Configuration Files
	OS Images (firmware deployment)
Configuration Labels	Configuration Labels
	Configuration Generation
	Templates
	Schemas
	OS/Firmware Download and Save (on appserver)
File Servers	File Servers
Active Monitoring	
Monitors	Monitors
Dashboard Views	Dashboard Views
Retention Policies	Retention Policies
Reports	
Reports	Reports
Report Templates	Report Templates
System Services	
Audit Trails	Audit Trails
Commands	Commands
Data Policies	Data Policies
DB Aging	DB Aging
Filters	Filters
Heartbeat	Heartbeat
MIB Browser	MIB Browser
Schedules	Schedules
Thresholds	Thresholds
Views	Views

NOTE:

This table lists capabilities for product installations that may differ from yours.

Licensing Web Client

To run the web client, you must have its license installed on the Application Server. See Installing Licensing on page 144 for instructions about installing a license if you do not have one installed.

10

Navigation

Overview

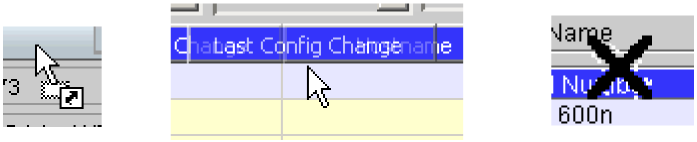
This section explains how to navigate the application. The application’s Portal consists of the following sections:

- Toolbar
- Menu Bar
- Work Area

Drag and Drop

This software lets you drag and drop columns within screens that display information in tables. One caveat: since the screen has so much information, the “drop zone” can sometimes be small.

Figure 10-1. Drag and Drop Cursors



Java Client **Web Client** **Column Deletion Cursor**

NOTE:

To drag a new column onscreen from the “+” menu, you must drop it over a column header or empty space.

You can also drag and drop panels to relocate them within *Details* screens. The cursor appearance changes when you do this (Web and Java clients differ). To delete a column from the display, drag it *up* off the table, an “X” appears at the cursor when the column deletion is in progress. You can add columns with the *Available Attribute List* button (the plus sign) as explained in Title Bar on page 155.

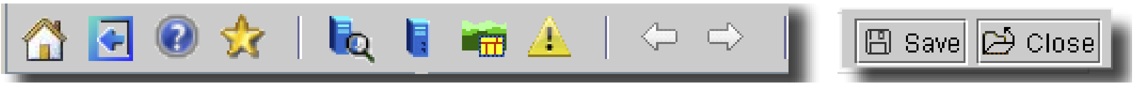
NOTE:

You must drag columns from the Available Columns list onto the columns already displayed. You cannot successfully drag and drop them elsewhere on the screen. Access the Available Columns list with the plus to the right of the Layout button.

Toolbar

The toolbar at the top of the initial screen is always visible.

Figure 10-2. Toolbar (two pieces of the same bar)



Hover the cursor over an icon for a text description. The following are in order, left-to-right. These icons are active (not grayed out) only when relevant:

- **Home**—The initial home page for the admin user is a screen that prompts that user to discover devices on the network. Otherwise, it opens the screen you have specified as your home page. See Settings -> Options on page 164 for how to set a home page. By default, after you finish initial discovery this is the QuickView that includes a count and list of alarms, and the panels visible in the manager described in Chapter 13, Resources.

Figure 10-3.

- **Discovery Wizard**—Opens the discovery wizard.
- **Show / Hide Navigation Window**—This toggles the appearance / disappearance of the left panel of the screen. This has a tree of icons you can click to activate each of the application's features.
- **Help**—Opens the Online Help. (See How to Get Help on page 184).
- **Set Home Page / Favorites**—Opens a screen described in Settings -> Options on page 164 that lets you select the home page and favorites in the work area.
- **Resources**—Opens Resources manager. (See Chapter 13, Resources)
- **Topology**—Opens a topology view displaying all devices. (See Chapter 21, Topology Views).
- **Monitoring View**—Opens an Quickview layout (See above).
- **Prev/Next**—These cycle back and forth through the open screens (listed in the *Windows* menu).
- **Save**—Write the results of your changes in the screen open in the work area to the database. Ctrl+S is the keyboard shortcut.
- **Close**—Closes the active, selected layout in the work area. Ctrl+F4 is the equivalent keyboard shortcut.

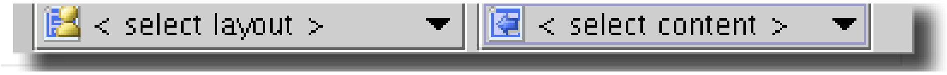
NOTE:

If you close individual sub-screens, in effect you are editing the layout (you can even close all content in a layout). The next time you open that layout, the deleted screens do not appear. If you want close the entire layout without editing it, use the close button on the toolbar.

Layout Bar

Between the toolbar icons and buttons, two pick lists let you quickly select layouts.

Figure 10-4. Layout Bar



This lets you alter the following:

- **<Select Layout>**—This pick list lets you select from layouts configured in Layout -> New / Edit / Delete on page 162. Some layouts come with the application, and appear in this list by default, for example, Quickview.
- **<Select Content>**—This pick list lets you select available content for a selected layout. The content appears as an additional panel in the existing display. You can select among choices like *Contact Manager*, *Event History*, and so on. You can close existing content panels with the 'x' in their upper right corner. When you add content, the application preserves the altered layout, with additional content, later logins by the same user.

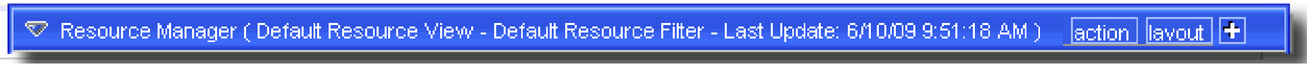
NOTE:

The content added goes in the wide column only.

Title Bar

Managers' title bars also provide buttons that let you perform actions and modify layouts relevant to the screen.

Figure 10-5. Title Bar


Resource Manager (Default Resource View - Default Resource Filter - Last Update: 6/10/09 9:51:18 AM)
action
layout
+

The title bar displays the manager name, filter name, and the time when the screen below last updated, whether automatically, or from pressing the *Go* button to activate Filtering and Searching.

In addition to the features on the Title Bar, the following are available there:

- Action Button / Right-Click Menu
- Layout Button
- Available Attribute List (+)

The title bar includes a *Triangle* at its left end that lets you click it to toggle whether the connected window appears below the title bar. It also includes a *Close Button*, the X at the top right of the panel’s toolbar closes that panel. Closing a panel modifies the layout from the default. If you close a panel in a layout, then when you re-open it, your personal layout (with the closed panel) appears onscreen. If you close all the panels with these Xs, then the layout will be blank. Add panels to the screen as described in Layout -> New / Edit / Delete on page 162. To close a layout without deleting panels, use the Toolbar button. To re-open a layout (as you last modified or created it), use the Layout Bar.

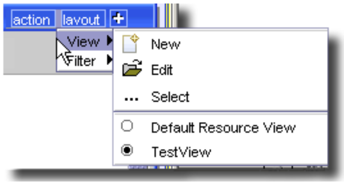
Action Button / Right-Click Menu

You can access the menu to manipulate items appearing on a screen either with the *action* button in the right end of the title bar, or by right-clicking a selected item. The menu items that appear when you do this depend on which application elements and device drivers you have installed.

Layout Button

In addition to the Layout Bar, a *layout* menu button appears when you click the *layout* button next to the *action* button at the top of most screens. This lets you create, edit and select from the available *View* and *Filter* options.

Figure 10-6. Layout Menu.



You can create a view, displaying a different arrangement of columns, or edit an existing view. At the bottom of this menu are available views, from which you can select. See View Editor on page 754 for a description of the screen that appears when you create or modify views.

NOTE:

In some managers, altering the default view means all users will see that alteration. If you want a view that is uniquely your own, create a new one.

Similarly, when you select *Filter* you can create, edit or select from available filters. See Filter Editor on page 736 for a description of the screen that appears when you create or modify filters. See Filtering and Searching on page 158 for a look at how filters appear and are immediately modifiable.

The list of the available views or filters that appears at the bottom of this menu depends on what you have installed and configured, and is limited to 25 filters. If you have more than that maximum, click ...*Select* to open the appropriate manager view where you can select from all available filters.

NOTE:

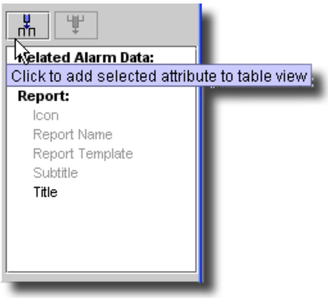
Some applications seed filters, so filters other than those you have created may appear listed. Some managers can display screens other than views and filters too. For example, the Topology screen's layout button displays other Topology Views in this list.

Move Up / Down / Left / Right—This selection appears in some *layout* menus—in detail panels, for example. These relocate the selected panel in the screen. Other panels automatically relocate to accommodate the moved panel.

Available Attribute List (+)

The *Available Attribute List* button (a plus sign when the panel is closed, a minus sign when it is open) in the title bar toggles the appearance of a list of attributes that appear as columns in the screen to the left.

Figure 10-7. Available Attribute List Toggle



Click to add selected attribute to table view

You can double-click a displayed attribute, or click the *Insert Column* button at the top of this panel to add it to the columns displayed. You can add more than one if you Ctrl + click to select multiple attributes. Attributes whose names appear gray are already in the display. Select a gray attribute and click the *Remove Column* button to delete that column from the display. You can also right-click to select *Insert / Remove Column*, or click and drag the attribute / column on or off of the list.

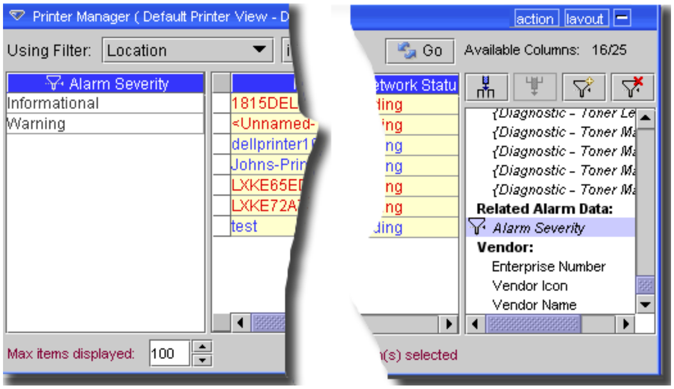
Displayed numbers like *Available Columns 2/25* mean that two of the available 25 slots for columns are in use. The first number is the count of columns in the screen. The second number is the maximum allowed.

Click the *Layout -> Edit Layout* to edit layouts more broadly (see Layout -> New / Edit / Delete on page 162).

Quick Group

One additional feature that appears in some managers is the *Quick Group*. With this, you can display devices grouped by selected attributes. Click the plus (+) sign in the upper right corner of the list in the manager to display the available attributes on the right.

Figure 10-8. Quick Group



As described above, you can click the left two icons above the attribute panel to add or remove a selected attribute from the displayed columns in the list of equipment. You can also drag an attribute name to the list to display it there as a column.

The two icons on the right above the attribute panel let you display groups (or un-group displays) of devices based on the attributes selected. When you select Quick Group attributes, those names appear in a panel to the left of the list of equipment. Click on an attribute value in that right panel to display the devices with this value. For example, devices whose last alarm is *Informational* appear when you click that attribute value in the left panel. If you select all values—or none—all devices appear, provided they conform to the filter selected at the top of this screen.

NOTE:

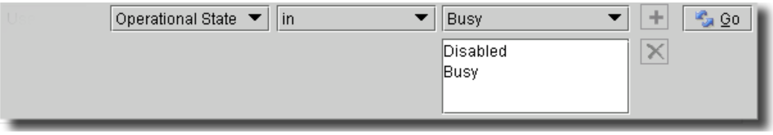
The filtered view and Max Items number limit the devices you can Quick Group together. You must click Go after you revise either the filter or Max Items before applying a Quick Group to a revised list.

You do not need to leave the attribute panel open to use the Quick Group panel on the left. Click the minus (-) icon at the top right of this screen to close the attribute panel.

Filtering and Searching

Filters appear at the top of most managers. A filter like *Name Like ** displays all items (<*unique ID*> *like / equals / begins with ** is the typical default). Manipulate the pick lists to create more restrictive filters.

Figure 10-9. Filter



Filters consist of an attribute (equipment attributes like *Operational State*), an operator (like *in / not in*, *is / is not*) and a match term (like *Active*, *Busy*). Some operators like *in / not in* permit multiple match terms. To enter multiple match terms, select a term in the far right pick list, then click the plus sign (+). You can also select listed match terms and delete them (X). For other managers, you can create a different kind of filter.

Click Go to filter the display, or to refresh an existing filter's displayed list of items. This describes creating new filters, and editing existing ones. See also Multiple Criteria Filters described in the next section and Chapter 28, Filters.

CAUTION:

Unless you create a filter and save them, filters you make here are not preserved. Filters (and views) created by one user are not visible to other users.

NOTE:

The like operator requires you to use one or more wildcards for it to be effective.

IP address searches are limited. For example, you can now search for an address like 192.168 (the equivalent of the /16 mask), but not for one like only 192. Some examples of the limitations for this search:

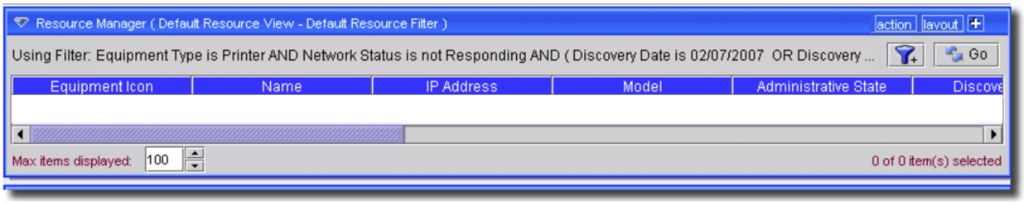
What does not work: a, abc, abc123, * 123,*123a234*,*123a234*, 192.168. 1.118

What does work: *, ?, 1, *1, 1*, *1*, *123,123*, *123*, 192.168.1.118, *.192.*.118, 192.*118, *.*.*.118, *.1?8.*.118.

Multiple Criteria Filters

You can see filters with more than two criteria in a read only summary filter mode. Notice that a plus (+) sign appears next to the filter icon.

Figure 10-10. Multiple Filter Criteria - Summary



Resource Manager (Default Resource View - Default Resource Filter)

Using Filter: Equipment Type is Printer AND Network Status is not Responding AND (Discovery Date is 02/07/2007 OR Discovery ...

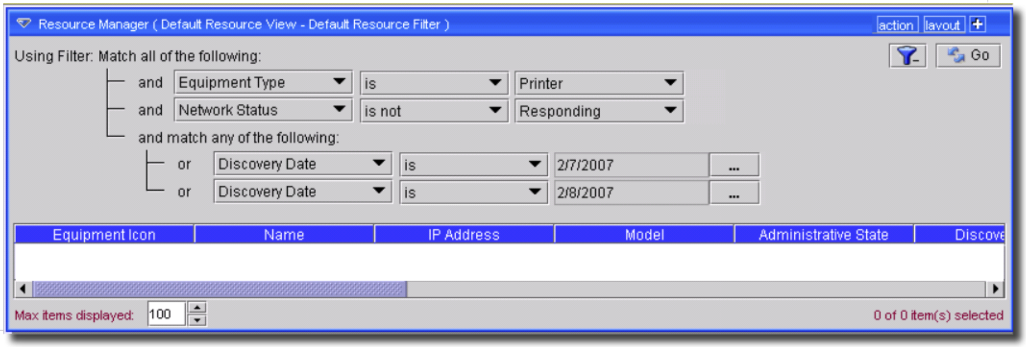
Equipment Icon	Name	IP Address	Model	Administrative State	Discove

Max items displayed: 100

0 of 0 item(s) selected

While in this summary mode, click the funnel-and-plus button to see an expanded tree view where you can change the filter criteria parameters (attributes, operands and values). The changes to this tree's elements alter the multiple criteria filter itself. Click the funnel-and-minus on the expanded screen to display the summary screen.

Figure 10-11. Multiple Filter Criteria - Expanded


Resource Manager (Default Resource View - Default Resource Filter)
action
layout
Go

Using Filter: Match all of the following:

and Equipment Type | is | Printer

and Network Status | is not | Responding

and match any of the following:

or Discovery Date | is | 2/7/2007 ...

or Discovery Date | is | 2/8/2007 ...

Equipment Icon	Name	IP Address	Model	Administrative State	Discove

Max items displayed: 100

0 of 0 item(s) selected

You can click the *Go* button in either the summary and expanded filter to see the effect of the filter. The funnel-and-plus does not appear when a filter can appear in the available space (when it does not have enough criteria to require this summary / expanded view pair).

Updates in the database that could cause changes to a derived attribute (column headings are typically italic for such attributes) are typically not automatically reflected in the manager. Click Go to update such attributes.

Menu Bar

The application's menus mirror many of the functions those available in the Navigation Window. Here are a few commonly encountered menu items:

File

- **Open**—Opens submenus like *Inventory*, and other installed options. *File -> Open -> Inventory*, for example, has a menu item for each Inventory node in the navigation window. Menu node equivalents also appear under other application names (for example: Alarms). The subnodes and menu items both open screens in the work area.

- **Home**—Return to the selected home page.

- **Close**—Closes the top screen open in the work area. Ctrl+F4 is the keyboard shortcut.

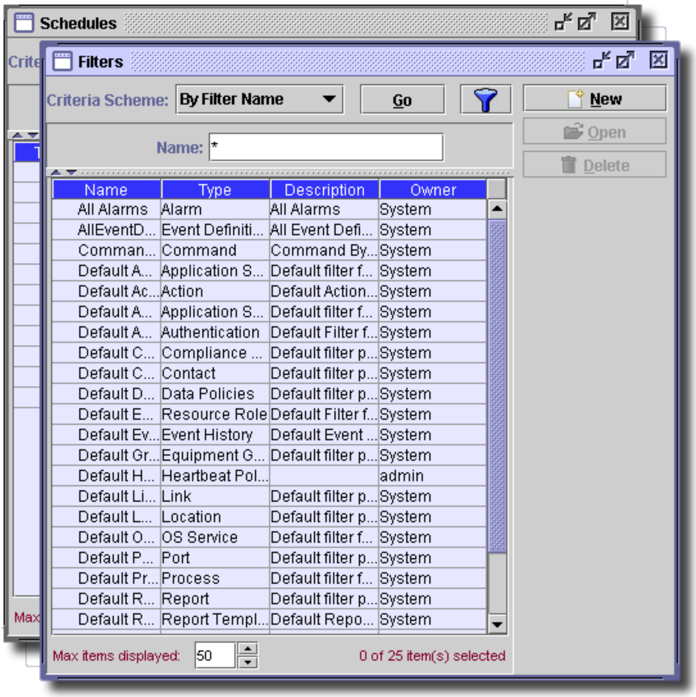
- **Close All**—Closes all screens open in the work area.

- **Exit**—Close the client application. Ctrl+X is the keyboard shortcut. Ctrl+X, by itself will not close the client in its entirety if there are pending edits (a dialog appears requesting confirmation).

View

- **Launcher**—lets you pick between Multiple Document Interface (MDI) and Browser views. The MDI view lets you see several screens overlapping in the work area (Figure 10-12).

Figure 10-12. MDI View



Criteria Scheme: By Filter Name

Name: *

Name	Type	Description	Owner
All Alarms	Alarm	All Alarms	System
AllEventD...	Event Definiti...	All Event Defi...	System
Comman...	Command	Command By...	System
Default A...	Application S...	Default filter f...	System
Default Ac...	Action	Default Action...	System
Default A...	Application S...	Default filter f...	System
Default A...	Authentication	Default Filter f...	System
Default C...	Compliance ...	Default filter p...	System
Default C...	Contact	Default filter p...	System
Default D...	Data Policies	Default filter p...	System
Default E...	Resource Role	Default Filter f...	System
Default Ev...	Event History	Default Event ...	System
Default Gr...	Equipment G...	Default filter p...	System
Default H...	Heartbeat Pol...		admin
Default Li...	Link	Default filter p...	System
Default L...	Location	Default filter p...	System
Default O...	OS Service	Default filter f...	System
Default P...	Port	Default filter p...	System
Default Pr...	Process	Default filter f...	System
Default R...	Report	Default filter p...	System
Default R...	Report Templ...	Default Repo...	System

Max items displayed: 50

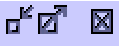
0 of 25 item(s) selected

NOTE:

You can cascade and tile MDI windows from the *Window* menu.

When you have MDI windows open, the upper right corner has icons that let you (from left to right) minimize, maximize and close the window. Closing the window is equivalent to *Cancel*. It abandons edits

Figure 10-13. Minimize, Maximize, and Close MDI Window



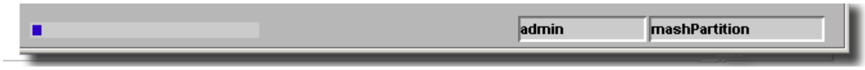
Browser view fills the work area with the selected screen(s). Use the *Windows* menu (or Ctrl+F6) to cycle between screens.

The checkboxes in this menu let you enable (or uncheck and disable) the following:

- **Show Toolbar—**Displays/hides the toolbar (see Toolbar on page 154).

- **Show Status Bar** (the bottom of the portal screen)

Figure 10-14. Status Bar



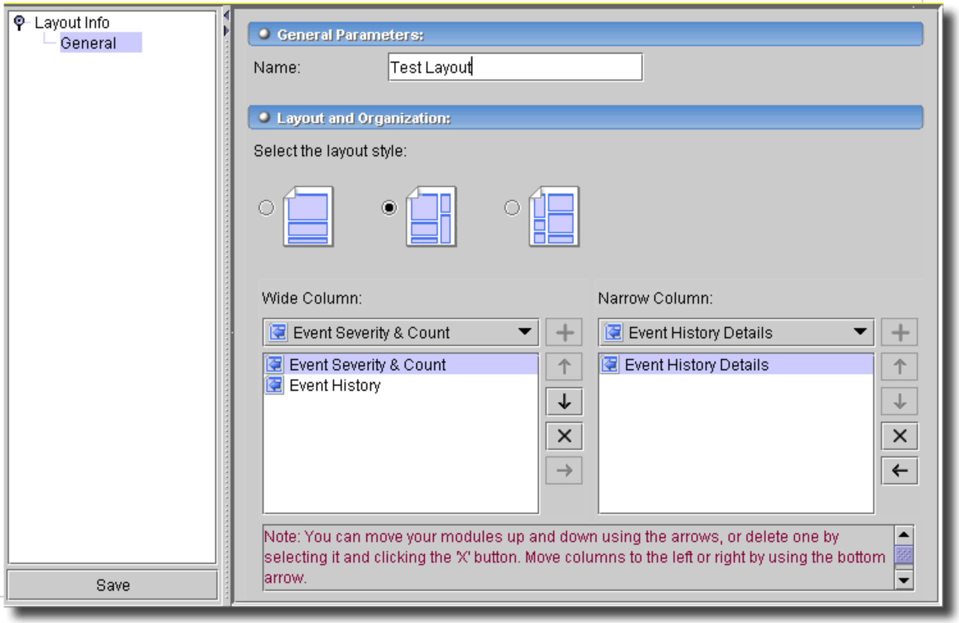
admin | mashPartition

To the left of the status bar text, a progress bar appears that tracks current operations' progress. The left text displays the logged in user, and the right text displays the partition name where application server is running. This partition name turns red when the client loses connection to the application server.

Layout -> New / Edit / Delete

This menu appears when applicable. It lets you create (*New*), *Edit* or *Delete* a layout for the application. The first two menu options open the layout editor.

Figure 10-15. Layout Editor



General Parameters:

Name: Test Layout

Layout and Organization:

Select the layout style: ○ ● ○

Wide Column: Event Severity & Count
- Event Severity & Count
- Event History

Narrow Column: Event History Details
- Event History Details

Note: You can move your modules up and down using the arrows, or delete one by selecting it and clicking the 'X' button. Move columns to the left or right by using the bottom arrow.

Several default layouts appear for each user. If you modify one of these, the application saves it to the database, and it becomes uniquely yours (while retaining the same name as the default layout). Whenever you log on, this modified layout is available to you (or to the originating user). The layout editor lets you configure the following:

General Parameters

- **Name**—A unique identifier for this layout.

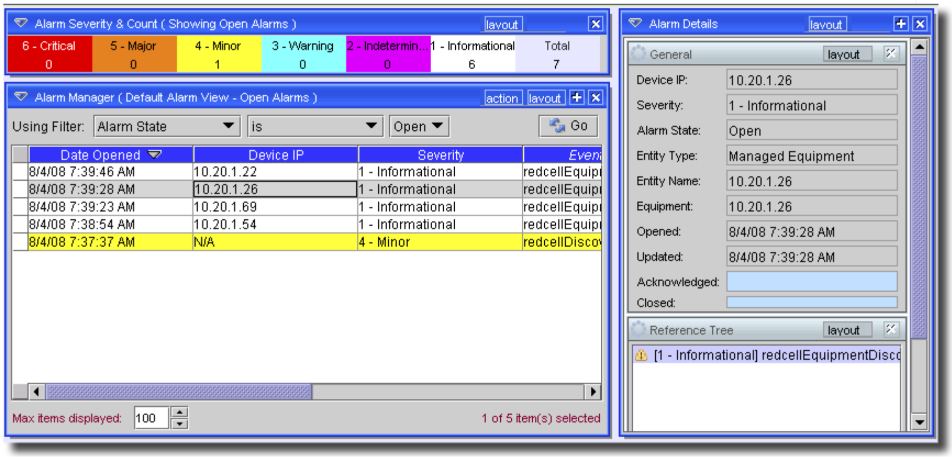
Layout and Organization

- **Select the layout style**—Select a radio button for the layout style you want. These include single column, two column with the narrow column on the right, and two column with the narrow column on the left. The appropriate column content selectors appear when you select a radio button.
- **Narrow / Wide Column**—Use the pick list(s) below these labels to select from available layout column contents. Once you find the item on the list, click the plus sign (+) to add it to the rows below the pick list. The up/down arrows next to these rows to re-order rows. The X removes selected content, and the right/left arrows move selected content between columns.

You can select related components with complementary displays. For example, *Alarm* and *Alarm Details*. When you select an Alarm in *Alarms*, the details of that port appear in the *Alarm Details* panel.

Click *Save* to make this layout available from the layout bar (see Layout Bar on page 155). The result of selecting a layout is that the screen appearance reflects your selections.

Figure 10-16. Layout Appearance



Alarm Severity & Count (Showing Open Alarms)
layout

6 - Critical	5 - Major	4 - Minor	3 - Warning	2 - Indetermin...	1 - Informational	Total
0	0	1	0	0	6	7

Alarm Manager (Default Alarm View - Open Alarms)
action
layout

Using Filter: Alarm State | is | Open | Go

Date Opened	Device IP	Severity	Even
8/4/08 7:39:46 AM	10.20.1.22	1 - Informational	redcellEquipi
8/4/08 7:39:28 AM	10.20.1.26	1 - Informational	redcellEquipi
8/4/08 7:39:23 AM	10.20.1.69	1 - Informational	redcellEquipi
8/4/08 7:38:54 AM	10.20.1.54	1 - Informational	redcellEquipi
8/4/08 7:37:37 AM	N/A	4 - Minor	redcellDisco

Max items displayed: 100

1 of 5 item(s) selected

Device IP:	10.20.1.26
Severity:	1 - Informational
Alarm State:	Open
Entity Type:	Managed Equipment
Entity Name:	10.20.1.26
Equipment:	10.20.1.26
Opened:	8/4/08 7:39:28 AM
Updated:	8/4/08 7:39:28 AM
Acknowledged:	
Closed:	

[1 - Informational] redcellEquipmentDisco

Notice that screens listing items displayed have a *Max Items* field at their bottom. Limiting items displayed with a maximum number improves database search times. The default is typically 100.

Settings

This menu contains the following items:

Settings -> Permissions

This menu lets you open *User Manager*, *User Group Manager*, *Authentication Manager*, *Object Group Manager*, *Application Security Policy*, *Group Rights Summary*, and *View* and *Register License* items. The *Administration Section* describes these items.

Settings -> Configuration

This menu lets you open *Control Settings* and *Inventory Config* (Inventory Config on page 174) editors. The application'sA*dministration Section* describes most of these items.

Settings -> Options

The screen that appears after you select this menu item lets you select the default page that appears when you open the application (the *Set Home page* button), or move a navigation tree node to or from the *Favorites* node (the *Add / Remove Favorites* button). Click *OK* at the bottom of this screen to confirm your choice, or *Cancel* to abandon any changes made.

NOTE:

You can also right-click a node on the navigation window and select *Set as Home Page* from the subsequent menu.

You can select a layout and make it a home page, but you cannot select a layout and make it a Favorite.

Settings -> Change Password

This opens a dialog that lets the logged in user change his password.

Window

The *Window* menu lets you select which screen appears in the work area if you have more than one open. *Next* and *Previous* arrows cycle through the open screens, while *Cascade* and *Tile* arrange them.

NOTE:

If you open more than 20 windows, the `Too Many Windows` error message appears. To change the default of 20, set a property `redcell.open_window_warning_level=nn`, where `nn` is the number of windows. Best practice for good performance is to select fewer windows, or leave the default.

Help

This menu item lets you open *Help* for the open screen, or the entire online help text table of contents (*Help Topics*), or the *About* box. *Help -> Product Updates* opens a website where you can find additional updates and add-ons for this software.

Hiding and Displaying the Navigation Window

You can conceal the navigation window to increase the size of your work area. To hide the navigation window click on small arrows on the bar between it and the work area. This is a toggle; click those arrows again to redisplay the navigation window. Or, to resize it, drag the bar to a new location.

NOTE:

By default, the navigation window collapses the tree it displays. You can click the nodes to un-collapse it.

Work Area

The work area displays the application's managers, wizards, and editors. You can change the display of the items in this area between an HTML browser view and an MDI (Multiple Document Interface) view by selecting *View -> Launcher*, then selecting the desired view.

Column Titles

You can edit the column titles that appear in editors. See the Inventory Config on page 174 for instructions about how to modify these and other display characteristics.

Color Conventions

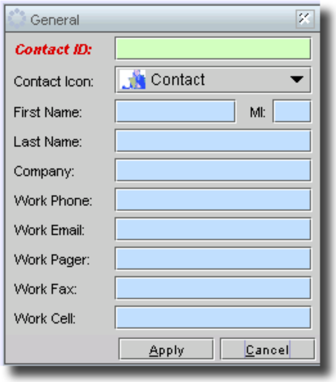
In some screens, blank fields have a blue background. These change to green when you change a field's contents, then click *Apply*. The green backgrounds persist until you save them to the database. If saving succeeds, background turns white, if it fails, then the green remains visible.

Mandatory fields have *bold italic* labels. If you do not enter a mandatory field when you edit a panel, a Validation error appears and the mandatory field label font turns red bold italic, and the background remains green. Labels with a violet background, and bold dark blue text indicate a warning is associated with the attribute value.

Detail Panels

When you select items at the top of a screen, frequently the details of those items appear in the *Detail Panels* at the bottom of the screen (though these do not appear in all screens).

Figure 10-17. Detail Panels



The *Edit* button appears at the bottom of detail panels if you can edit their contents. *Cancel* your edit if you want to return to the previous parameters.

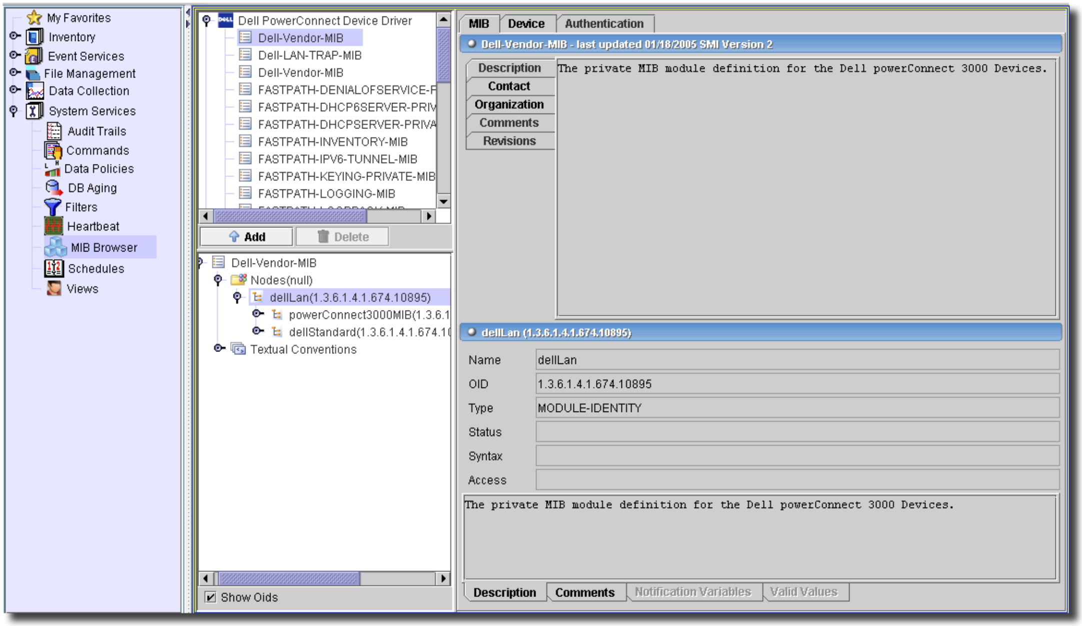
NOTE:

To refresh detail panels, select another item in the manager, then re-select the one for which you want details refreshed.

MIB Browser

Direct access SNMP sessions open a MIB browser where you can examine existing MIBs, or (with the *Add* button) add more MIBs.

Figure 10-18. Direct Access SNMP



The private MIB module definition for the Dell powerConnect 3000 Devices.

Name	dellLan
OID	1.3.6.1.4.1.674.10895
Type	MODULE-IDENTITY
Status	
Syntax	
Access	

The private MIB module definition for the Dell powerConnect 3000 Devices.

You can also open this screen directly from the navigation panel's *MIB Browser* icon, or from the *File -> Open -> System Services* menu, and examine selected MIBs there.

This screen displays available MIBs in the upper left corner. Click *Add* to load any additional MIBs. Select a listed MIB, and a tree of its nodes appear in the lower left corner. The selected node's description appears in the right panels. Check the *Show Oids* checkbox below this left screen, and the OIDs for each MIB Node appear to the right of the name in the tree display. The display of node details on the right has the following fields and sections (including the OIDs):

MIB Tab

This screen displays the MIB information for the *Description*, *Contact*, *Organization*, *Comments* and *Revisions* of the selected MIB. The bottom of this screen displays available *Description*, *Comments*, *Notification Variables*, and *Valid Values* for the selected MIB node. (*Comments*, *Notification Variables*, and *Valid Values* accompany this MIB tab.)

The *Description* area includes the *Name*, *OID* (object identifier), *Type*, *Status*, *Syntax*, and type of *Access* (for example: read-only), in addition to a text description area. Some MIB nodes may also display name/value pairs in the lowest part of this tab.

Devices Tab

The *Device* tab includes the MIB *Property* and *Value* fields. Multiple pairs like these can appear on this screen. You can see the selected values at the bottom of this tab. You can also *Refresh* the values with that button, or *Export* the values in a comma-separated value (.csv) file that resembles the following:

```
"instance","sysApplInstallPkgManufacturer"

"1.3.6.1.2.1.54.1.1.1.1.2","1.3.6.1.2.1.54.1.1.1.1.2"
```

Authentication Tab

The *Authentication* tab displays the *IP Address*, *Port*, *Read Community*, (SNMP) *Version*, *Timeout* and *Retries* for the SNMP session authentication.

11

Common Operations

Overview

This section discusses conventions used throughout these guides (online and print) and operations common to the application.

Conventions

The following conventions appear throughout this information:

Selecting Items From Menus

The phrase "select *Inventory* -> *Locations* from the *File* -> *Open* -> menu or the Navigation Window" means you should do one of the following:

- Click on the menu item listed. (*Inventory* is a subitem in the *Open* menu item in the *File* menu.)
- Click on the *Inventory* node to expand it in the Navigation Window, then click on *Locations*.

NOTE:

This can also indicate sub-nodes on a tree like the navigation window. For example: Inventory -> Locations

The Command, X and Eraser Buttons

The command button has an ellipsis (...) on it and appears whenever the command's completion may need additional steps.

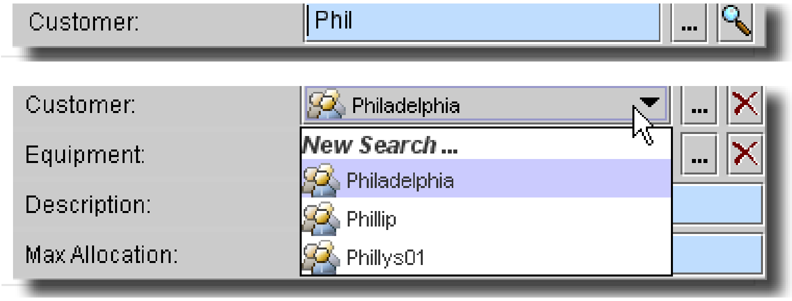
Clicking on this button displays another dialog that typically lets you select an entry for an adjacent field.

The X or eraser button clears the adjacent field. Often it appears next to a field with a command button at the other end.

Search Fields

Throughout this application, some fields let you search for the desired result.

Figure 11-1. Search Fields



Customer: Phil

Customer: Philadelphia

Equipment:

Description:

Max Allocation:

To use this feature, enter <search text> that is a partial match for the item you want then click the search icon (magnifying glass) to display the first match. Clicking the drop-down list that replaces the match field displays all matches. To clear the selection, click the red X at the right. Clicking the command button (...) still opens a selector with all available matches. If you already have a selection, then the delete (X) button conceals the search button.

Search (the magnifying glass icon) is slightly different depending on the context, and whether the applicable driver or service type specifies a default filter for the entity (not just the attribute) you are editing.

- **Selecting top level devices**—If the service type or driver specifies a filter, OpenManage Network Manager looks for the filter's default attribute (usually *Name*), populates it with the specified <search text>, and runs the filter.

  If no filter exists, OpenManage Network Manager can create one from the contents of the search field. If you enter either an IP or hostname, it queries top level devices for those where "IP = <search text> OR Name contains <search text>." See Filtering and Searching on page 158 for more about IP address searching.

- **Selecting subcomponents**—If a filter exists, OpenManage Network Manager looks for the default attribute (usually *Name*) and filters on that attribute based on <search text>.

  If no filter exists, OpenManage Network Manager creates one from the <search text>. For example, entering the port name—fxp0/0/0—runs "Name contains fxp0/0/0" as a filter.

  You can also type in first part of the chassis, followed by a colon and information about the port. For example: 192.168.1.118 : fxp0/0 filters for "Chassis ip = 192.168.1.118 OR Chassis Name contains 192.168.1.118 and Port Name contains fxp0/0"

- **Selecting anything else**—If the service type or driver specifies a filter, OpenManage Network Manager looks for the default attribute (Name usually) runs that filter, specifying <search text>.

If the service type or drive specifies no filter, OpenManage Network Manager uses the default filter for that attribute (not the whole screen, just the field), inserting the filter <search text>.

NOTE:

Hover your cursor over the <search text> field to see a tooltip outlining its filtering possibilities.

The GO Button

To save loading the query time, you can configure the application so managers do not automatically run their default filter when you open them (running this filter is the default behavior).

When you open a typical manager, you can then select a filter and click on *Go* to display all appropriate matches. Likewise, when you create a new record the manager may not automatically refresh. You must click on *Go* or *Refresh* to refresh the display.

Open / View and Import / Export

Users without write permission see *View* rather than *Edit* or *Open*. The application may gray out *Import* or *Export* menu items if permissions do not exist to use them.

Accelerators / Shortcuts

Whenever you see a letter underlined in the title of a menu or button, you can select that menu or button with Alt + [the letter]. Other shortcuts appear in the menus themselves.

Notes, Cautions, Tips, and Warnings

This manual uses the following formats to call your attention to important information.

NOTE:

Helps you apply the best practices, techniques and procedures described in the text.

NOTE:

Calls your attention to related information of special importance.

CAUTION:

System damage may follow the described action.

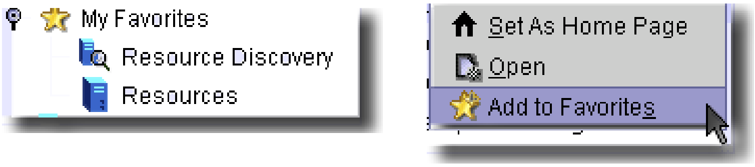
Common Operations

The following operations appear throughout the application. Rather than discuss these operations repeatedly as they occur, explanations appear here.

Creating My Favorites

By default, two nodes of the navigation pane appear in *My Favorites* at its top: *Resource Discovery*, and *Resources*.

Figure 11-2. My Favorites, and *Add to Favorites*



Right-click any node in the navigation pane and select *Add to Favorites* to duplicate it in the *My Favorites* node.

Saving

Some dialogs have a *Save* button to save the results of your actions with that screen. If you do not see such a button, however, you can still use the toolbar *Save* icon and menu item *File* -> *Save* with the same effect. You can also click the *Save* button whenever present within a screen itself to save your edits.

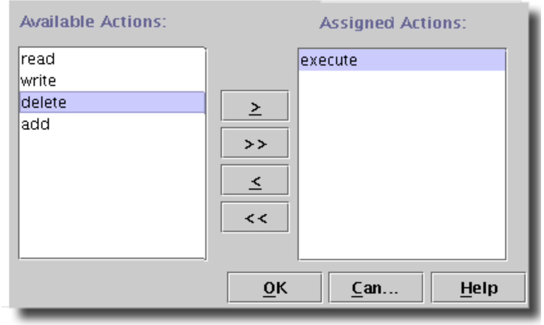
Previous

Some screens have a *Back* or *Previous* button. These are typically wizards, and the button allows you to return to the previous step. The larger screen also contains a pair of *Prev* / *Next* arrows in the toolbar (see Toolbar on page 154). These let you cycle through the screens visible in the Windows menu (open screens)

Moving Items Between Lists

Many dialogs let you move items from one list to another.

Figure 11-3. Moving Between Lists



To move a single item from one list to another, select it and click on the > or < button. To move several items from one list to another, hold down the *Ctrl* key while clicking on the desired items. Click on the > or < buttons. To move all items from one list to another, click on the >> or << button, if it is available. You can see such lists in the Discovery Wizard when you select authentication objects.

Sorting Columns in Managers

You can sort lists of items in a column. To do so, click on the column heading. Clicking on the heading again reverses the sort order. An arrow appears in the column to indicate it is the one sorted.

Column headings in italics indicate that the data is derived. Sorting on these columns will not affect the resulting data set when the filter is applied.

Column headings in normal text indicate that the data is not derived. Sorting on these columns will affect the resulting data set when the filter is applied so the data is in order when retrieved from the database.

For example: If the database includes a column called Name and there are 6 rows in the database with the values Alan, Aaron, Edgar, Fred, Albert and Lance. When requesting a result set whose maximum size is 3 if no sorting is applied to the name column then Alan, Aaron and Edgar appear. If you sort the name column in ascending order, query results would include Aaron, Alan and Albert. If you sort that column in descending order the result set would return Lance, Fred and Edgar. If the Name column included only derived values (the column heading appears italicized), then sorting on the column would not affect the result set and a query would always display Alan, Aaron and Edgar, sorted either as Aaron, Alan, Edgar or Edgar, Alan, Aaron.

Setting Subnets

Many devices managed by this software set IP address and subnet combinations. Within the limitations of your network and devices, the following suggests some typical subnet calculations.

Consider this Class C subnet example:

> 192.168.10.33 with a subnet mask of 255.255.255.224

To calculate the subnet and broadcast address of that IP address:

> 256 - 224 = 32.

Subnets therefore repeat in increments of 32 (32, 64, 96...etc.) 192.168.10.33 must therefore be part of the 192.168.10.32 subnet. The next subnet is 64, so the broadcast address is 63 (the number just before the next subnet). The valid host range for this subnet is 10.33 - 10.62.

Another (class C) example:

> 192.168.10.33 with a subnet mask of 255.255.255.240.

To calculate the subnet and broadcast address of that IP address:

> 256 - 240 = 16.

Subnets therefore repeat in increments of 16 (16, 32, 48...etc.) This address must therefore be part of the 192.168.10.32 subnet, and the broadcast address is 47. The valid host range is 33 - 46.

Class B subnets are a little more complex. For example:

172.16.10.33 subnet mask: 255.255.255.224.

Subnets repeat in increments of 32 (256-224 = 32; 32, 64, 96...etc.). This is between 10.32 and 10.64, and the broadcast address is 10.63.

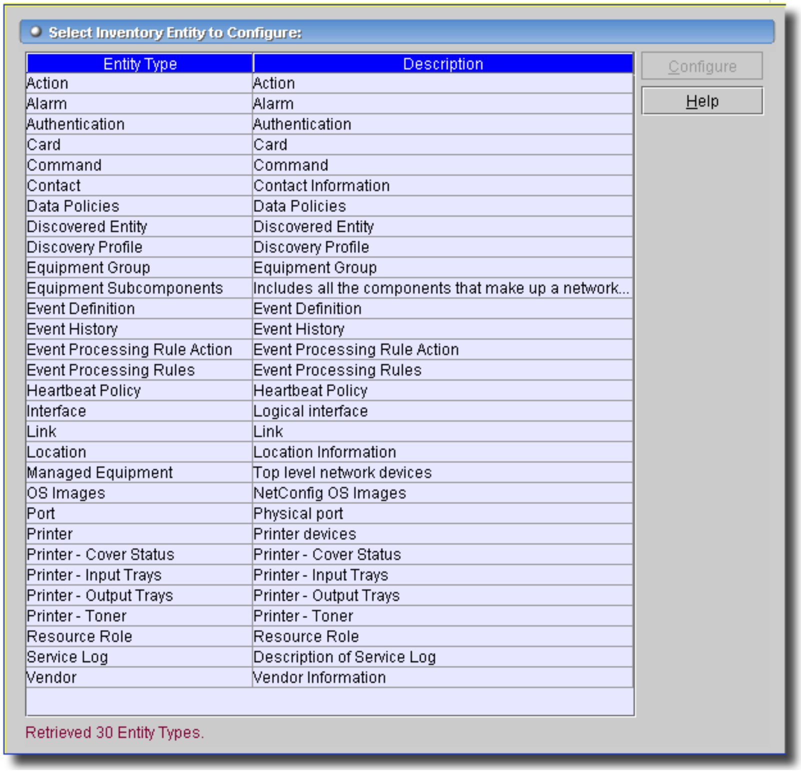
NOTE:

Free subnet calculators are available on the internet.

Inventory Config

You can configure custom fields and appearance of text in the application's filters, managers and editors with the Inventory Config manager, however only managers support changed text appearance done in the Config Editor. Access these capabilities through *Settings -> Configuration -> Inventory Config*.

Figure 11-4. Inventory Config Manager



Select Inventory Entity to Configure:

Entity Type	Description
Action	Action
Alarm	Alarm
Authentication	Authentication
Card	Card
Command	Command
Contact	Contact Information
Data Policies	Data Policies
Discovered Entity	Discovered Entity
Discovery Profile	Discovery Profile
Equipment Group	Equipment Group
Equipment Subcomponents	Includes all the components that make up a network...
Event Definition	Event Definition
Event History	Event History
Event Processing Rule Action	Event Processing Rule Action
Event Processing Rules	Event Processing Rules
Heartbeat Policy	Heartbeat Policy
Interface	Logical interface
Link	Link
Location	Location Information
Managed Equipment	Top level network devices
OS Images	NetConfig OS Images
Port	Physical port
Printer	Printer devices
Printer - Cover Status	Printer - Cover Status
Printer - Input Trays	Printer - Input Trays
Printer - Output Trays	Printer - Output Trays
Printer - Toner	Printer - Toner
Resource Role	Resource Role
Service Log	Description of Service Log
Vendor	Vendor Information

Retrieved 30 Entity Types.

In the initial screen the *Entity Type* and *Descriptions* appear listed in rows. Select a row and click *Configure* to edit settings for this type. The Config Editor appears.

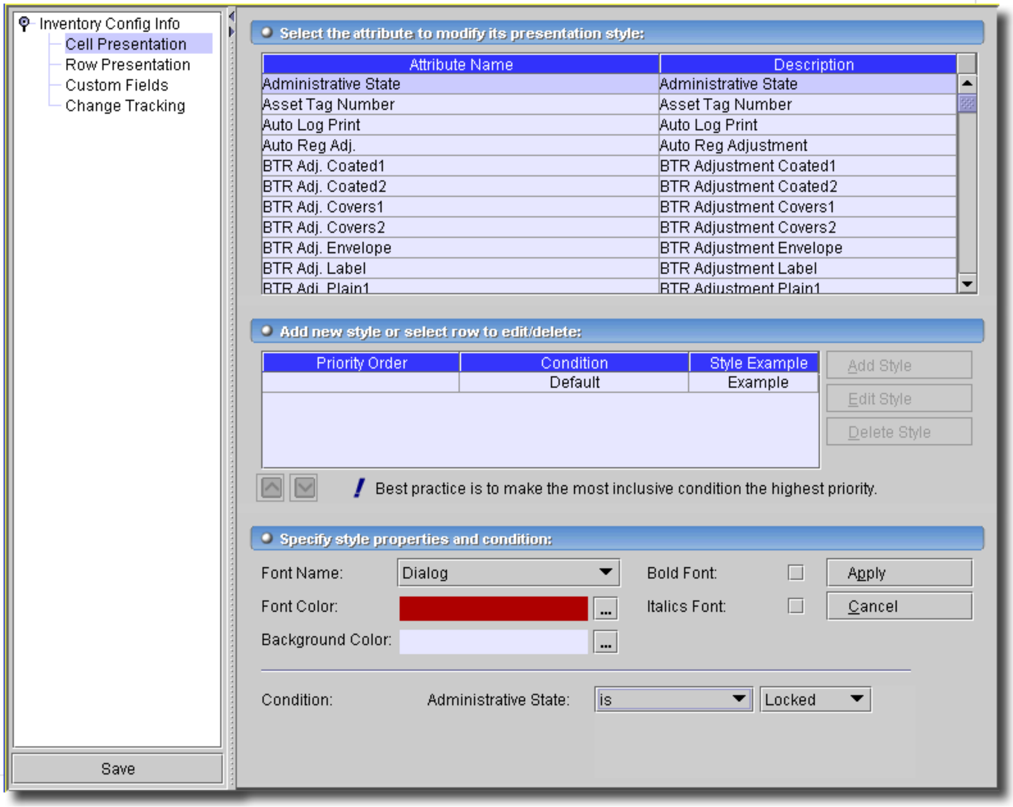
NOTE:

You must restart the client and server to see the effect of some changes in this editor. Client restart is necessary to see the effects of presentation style changes, and application restart is necessary to see the effects of change tracking alterations, or custom fields.

Config Editor

The config editor lets you alter the presentation of information in screens and reports, it lets you configure custom fields, and change the type of tracking the application performs

Figure 11-5. Config Editor - Cell Presentation.



Select the attribute to modify its presentation style:

Attribute Name	Description
Administrative State	Administrative State
Asset Tag Number	Asset Tag Number
Auto Log Print	Auto Log Print
Auto Reg Adj.	Auto Reg Adjustment
BTR Adj. Coated1	BTR Adjustment Coated1
BTR Adj. Coated2	BTR Adjustment Coated2
BTR Adj. Covers1	BTR Adjustment Covers1
BTR Adj. Covers2	BTR Adjustment Covers2
BTR Adj. Envelope	BTR Adjustment Envelope
BTR Adj. Label	BTR Adjustment Label
BTR Adj. Plain1	BTR Adjustment Plain1

Add new style or select row to edit/delete:

Priority Order	Condition	Style Example
	Default	Example

Best practice is to make the most inclusive condition the highest priority.

Specify style properties and condition:

Font Name: Dialog

Font Color: 🟥

Background Color:

Bold Font: □

Italics Font: □

Condition: Administrative State: is Locked

It has the following sub-panels

- Cell Presentation
- Row Presentation
- Custom Fields

- Change Tracking
- Topology Presentation

NOTE:

Not all types of data support all the example options that appear here.

NOTE:

Some fields are ambiguously named. If you want to make *Vendor Name* bold and red, you can do so in the *Vendors* manager, but that change does not appear in the *Resources* screen (change the *Vendor Name* field in *Managed Equipment* if you want that). You must also close and re-open screens where you want such changes to occur for them to be visible.

The following sections describe these panels.

Cell Presentation

This panel configures the appearance (font, color, and so on) of attributes in cells in managers. When you select a listed attribute in the upper panel its applicable presentation styles appear in the middle of the screen. The *default* style appears for all items. With the buttons to the right of the styles, you can *Add Style*, *Edit Style*, or *Delete Style*. You must select a listed style to do the last two.

When you add, or edit a style, the panel labelled *Specify style properties and conditions* appears in the lowest panel. This has the following fields and pick lists:

- **Font Name**—Select from a pick list of available fonts.
- **Font Color**—Select the font color picker that appears when you click the Command Button (...) to the right of the displayed color.
- **Background Color**—Select the background of the cell displaying the attribute information from the color picker that appears when you click the Command Button (...) to the right of the displayed color.
- **Bold Font**—Check to activate.
- **Italics Font**—Check to activate.
- **Condition**—This portion of the panel makes the display reflect an attribute condition. The attribute already appears, by default. Specify the condition by selecting an operator and value (some fields permit a range of values).

Click A*pply* to accept your edits, and list the condition in *Priority Order*. Click *Cancel* to abandon them.

The condition then appears as a row in the middle of this screen. The first column of this table indicates its priority (the lower the number, the higher the priority). You can change priority order of selected rows with the up/down arrows below this list. The second column is a reminder of the *Condition* you set, and the third is an example of what text looks like when the attribute fits the condition.

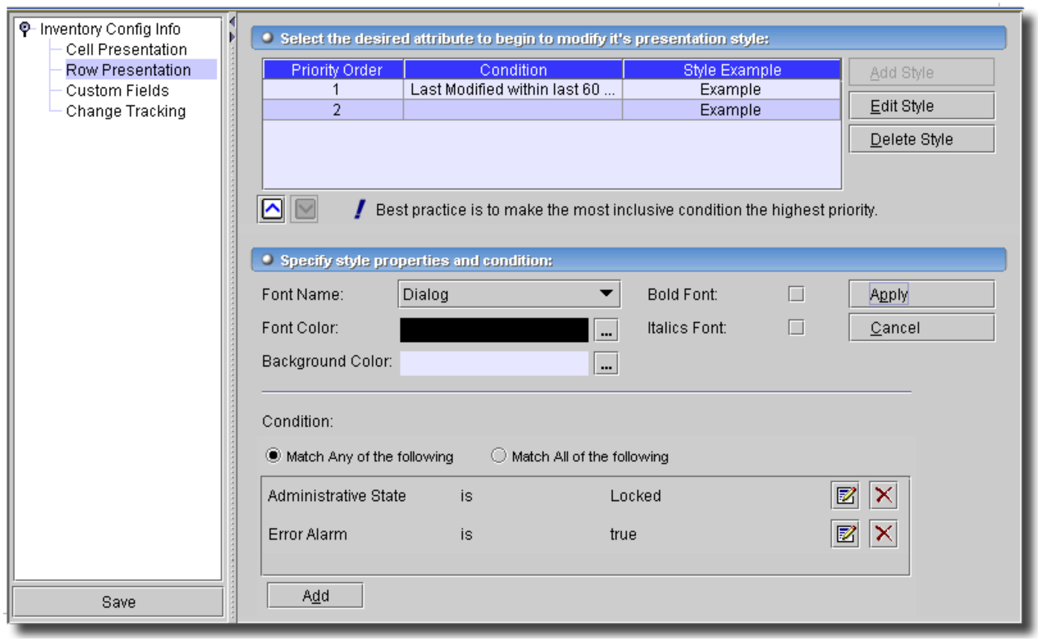
NOTE:

Best practice makes the most inclusive condition the highest priority.

Row Presentation

This panel configures the appearance of rows of attributes in managers.

Figure 11-6. Config Editor - Row Presentation



- Inventory Config Info
  - Cell Presentation
  - Row Presentation
  - Custom Fields
  - Change Tracking

Save

Select the desired attribute to begin to modify it's presentation style:

Priority Order	Condition	Style Example
1	Last Modified within last 60 ...	Example
2		Example

Best practice is to make the most inclusive condition the highest priority.

Specify style properties and condition:

Font Name: Dialog

Font Color: ...

Background Color: ...

Bold Font: □

Italics Font: □

Condition:

● Match Any of the following ○ Match All of the following

Administrative State	is	Locked
Error Alarm	is	true

With the buttons to the right of the styles, you can *Add Style*, *Edit Style*, or *Delete Style*. You must select a listed style to do the last two.

When you add, or edit a style, the panel labelled *Specify style properties and conditions* appears in the lowest panel. This has the following fields and pick lists:

- **Font Name**—Select from a pick list of available fonts.

- **Font Color**—Select the font color picker that appears when you click the Command Button (...) to the right of the displayed color.

- **Background Color**—Select the background of the cell displaying the attribute information from the color picker that appears when you click the Command Button (...) to the right of the displayed color.
- **Bold Font**—Check to activate.
- **Italic Font**—Check to activate.
- **Condition**—Select whether you want to *Match Any* or *Match All* of the conditions you add. The display then reflects an attribute condition. The attribute already appears, by default. Specify the condition by clicking *Add*, then selecting an attribute, operator and value (some fields permit a range of values). Click the green check mark to accept a single condition, or the click the blue curved arrow to cancel editing and revert to whatever existed before you began editing. You can add more than one. You can also remove conditions by clicking the red "X," or edit an existing condition by clicking the notepad icon.

Apply to accept your edits, and list the condition in *Priority Order*. Click *Cancel* to abandon them.

The condition then appears as a row at the top of this screen. The first column of this table indicates its priority (the lower the number, the higher the priority). You can change priority order of selected rows with the up/down arrows below this list. The second column is a reminder of the *Condition* you set, and the third is an example of what text looks like when the attribute fits the condition.

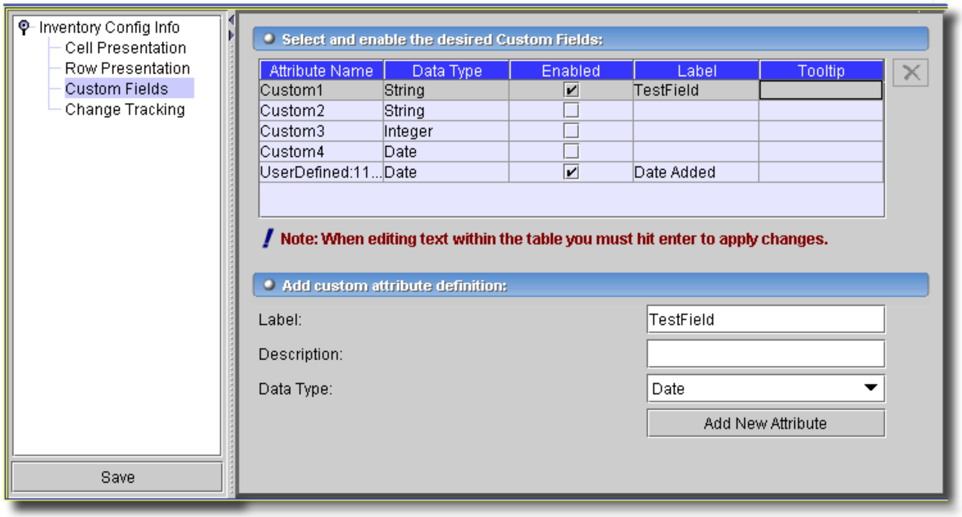
NOTE:

Best practice makes the most inclusive condition the highest priority.

Custom Fields

You can create custom fields for the selected entity type in this screen. The fields here depend on the entity you select in Inventory Config on page 174.

Figure 11-7. **Config Editor - Custom Fields**



Select and enable the desired Custom Fields:

Attribute Name	Data Type	Enabled	Label	Tooltip
Custom1	String	☑	TestField	
Custom2	String	□		
Custom3	Integer	□		
Custom4	Date	□		
UserDefined:11...	Date	☑	Date Added	

Note: When editing text within the table you must hit enter to apply changes.

Add custom attribute definition:

Label: TestField

Description:

Data Type: Date

This screen lets you edit rows describing custom fields directly. Click in a column and start typing (some are read-only). The following are the columns:

- **Attribute Name**—This is a simple identifier, like *Custom1*, *Custom2*, and so on. (read only). For example, you could create an attribute for *Data Center ID* and have that appear for searches and sorts.
- **Data Type**—This describes the data type of the custom attribute (*String, Integer, Date, Boolean*–read only). When you select *Boolean* the field is a checkbox.
- **Enabled**—Check *Enabled* to activate the selected custom field.
- **Label**—The label that precedes the custom field(s) on the screen.
- **Tooltip**—The tip that appears when you hover the cursor over the custom field.

Add User-Defined Attribute

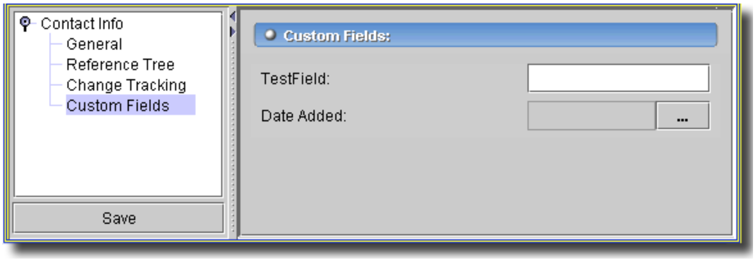
Use the *Add New Attribute* button to create additional attributes you have configured in the lowest panel on this screen.

NOTE:

You must restart the client screen where these fields appear to see the effect of changes in this editor.

Once you configure these labels, they appear in the editor appropriate to the Inventory Type selected.

Figure 11-8. Custom Field in Editor



TestField:

Date Added: ...

Find an example of the equipment in the Resources manager, select it, and click *Open* to see the custom field. You can also create filters to display equipment based on custom field contents.

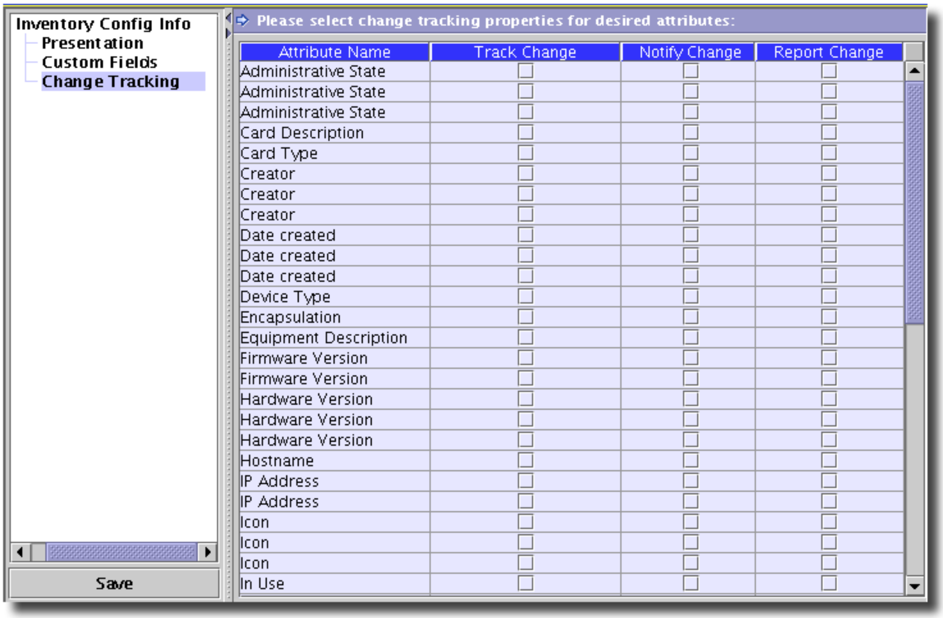
NOTE:

If you use the pre-existing custom attributes in this editor (re-labeled for your purposes), they have a dedicated column in the database so you can search and filter based on their values. User Defined attributes are not searchable, so you can capture, display and report on the attributes, but cannot filter on them.

Change Tracking

This panel lets you select types of notifications for the selected inventory type.

Figure 11-9. Config Editor - Change Tracking



Please select change tracking properties for desired attributes:

Attribute Name	Track Change	Notify Change	Report Change
Administrative State	□	□	□
Administrative State	□	□	□
Administrative State	□	□	□
Card Description	□	□	□
Card Type	□	□	□
Creator	□	□	□
Creator	□	□	□
Creator	□	□	□
Date created	□	□	□
Date created	□	□	□
Date created	□	□	□
Device Type	□	□	□
Encapsulation	□	□	□
Equipment Description	□	□	□
Firmware Version	□	□	□
Firmware Version	□	□	□
Hardware Version	□	□	□
Hardware Version	□	□	□
Hardware Version	□	□	□
Hostname	□	□	□
IP Address	□	□	□
IP Address	□	□	□
Icon	□	□	□
Icon	□	□	□
Icon	□	□	□
In Use	□	□	□

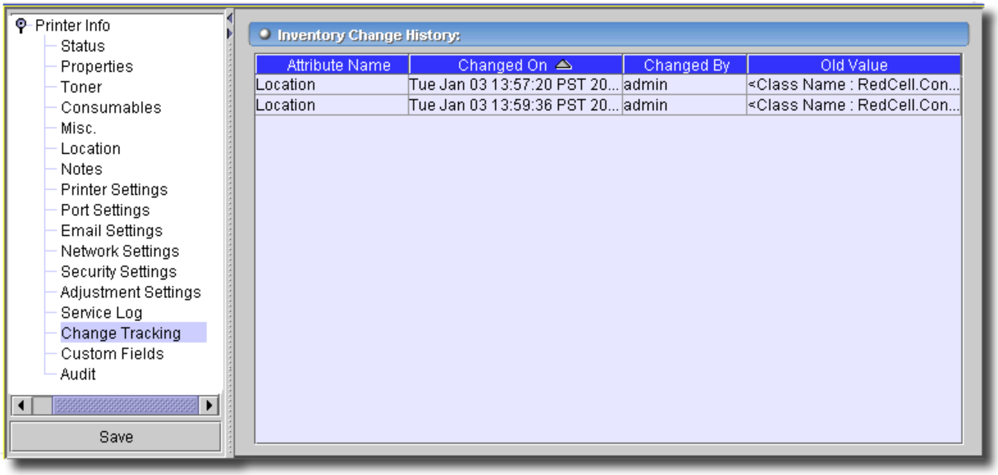
Setting up change tracking is an administrative task. You must first use the *Inventory Config* screen to select a type of inventory, then configure *Change Tracking* for that type. Select the attributes to track in the *Change Tracking* screen. You no longer must re-start the application server after having selected which attributes to track before any changes become visible.

If you do not have the correct authentication or permission to access the devices for which you want to perform change tracking, your system may be unable to retrieve attribute values and track changes may fail. The application server may display “unable to retrieve attribute” errors in such cases.

The listed attributes (the left column) vary, depending on the inventory type you selected in Inventory Config on page 174. Check one of the following three columns to change the tracking for the selected attribute:

- **Track Change**—Check to enable change tracking. This produces a log of changes for the selected inventory type and attribute. These typically appear in an Change Tracking editor panel.

Figure 11-10. Change Tracking



Inventory Change History:

Attribute Name	Changed On	Changed By	Old Value
Location	Tue Jan 03 13:57:20 PST 20...	admin	<Class Name : RedCell.Con...
Location	Tue Jan 03 13:59:36 PST 20...	admin	<Class Name : RedCell.Con...

This history enumerates the changes *Attribute Name*, when it was *Changed on*, who it was *Changed by* and the *Old Value* in the rows of its display.

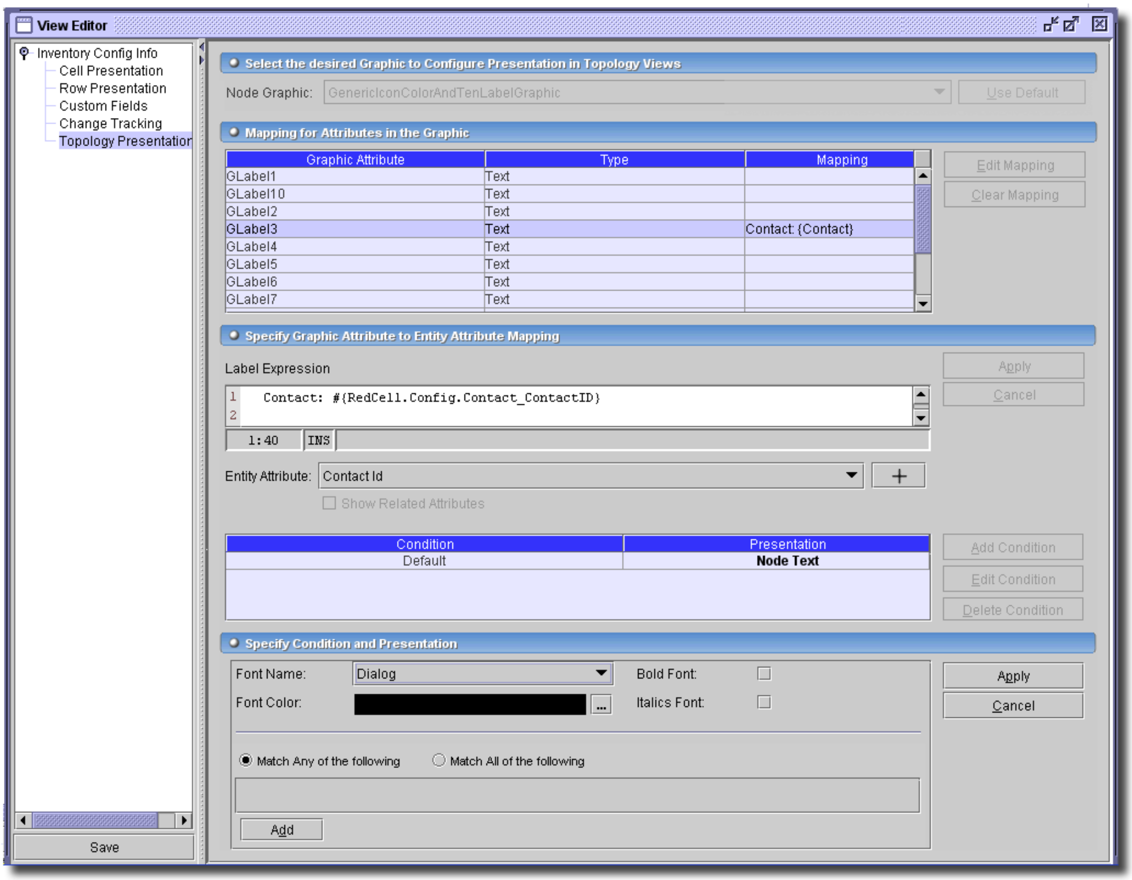
- **Notify Change**—Emit Change Notification which can trigger an action.
- **Report Change**—Save Changes for Reports, applicable if you have the Reports module installed.

Click *Save*, and the changes in presentation, custom fields and tracking are preserved in the database for the selected inventory entity type.

Topology Presentation

This screen configures the presentation of some entities you can display in Topology views (see Chapter 21, Topology Views).

Figure 11-11.   Topology Presentation



View Editor

- Inventory Config Info
  - Cell Presentation
  - Row Presentation
  - Custom Fields
  - Change Tracking
  - Topology Presentation

Save

Select the desired Graphic to Configure Presentation in Topology Views

Node Graphic: GenericIconColorAndTenLabelGraphic   Use Default

Mapping for Attributes in the Graphic

Graphic Attribute	Type	Mapping
GLabel1	Text	
GLabel10	Text	
GLabel2	Text	
GLabel3	Text	Contact: {Contact}
GLabel4	Text	
GLabel5	Text	
GLabel6	Text	
GLabel7	Text	

Edit Mapping   Clear Mapping

Specify Graphic Attribute to Entity Attribute Mapping

Label Expression

```
Contact: #{RedCell.Config.Contact_ContactID}
```

1:40 INS

Apply   Cancel

Entity Attribute: Contact Id   +

□ Show Related Attributes

Condition	Presentation
Default	**Node Text**

Add Condition   Edit Condition   Delete Condition

Specify Condition and Presentation

Font Name: Dialog   Bold Font: □

Font Color: ...   Italics Font: □

● Match Any of the following   ○ Match All of the following

Add

Apply   Cancel

The screens vary, depending on the entity you are editing, the following describes a representative example. The *Contact*-related screen displays the following:

Select the desired Graphic

- **Node Graphic**—Select the desired graphic when this entity appears in Topology screens from the pick list. The contents of the next section (Mapping for Attributes in the Graphic) depends on the graphic you select here. Installation seeds the available graphics on the pick list. If you do not select a graphic, the application uses the default. You can click *Use Default* to return a selected graphic to the default.

If you select a *Link* as the entity type, no such selection is possible. Nevertheless, in general terms, you can configure the link's attributes (*Pattern*, *Width*, *Color*, *Label* and so on) as described below.

Mapping for Attributes in the Graphic

This portion of the screen displays the attributes associated with the selected graphic (or other entity). With the buttons to the right of this portion of the screen, you can *Clear Mapping* which removes any previous association for the attribute, or *Edit Mapping* which opens the editor below this screen.

Specify Graphic Attribute to Entity Mapping

This portion of the screen displays a text area (*Label Expression*) in which the selected *Entity Attribute* mappings appear. To enter such a mapping, select an *Entity Attribute* from the pick list next to that label and click the plus (+) to its right. The programmatic text designation for that attribute appears in the *Label Expression* text area. For example: `#{Redcell.Config.Contact_ID}.` You can also enter a combination of such designations and fixed, non-variable text you type in. For example:

```
Contact:#{Redcell.Config.Contact_Contact_ID}
```

This configures the Topology display for a contact as the word “Contact:” followed by the contact ID.

NOTE:

If you select a graphic, like `#{Redcell.Config.Contact_Contact_Icon}`, then only the text label for that icon appears in text fields. This editor does not correct you if you select a graphic in a text field.

Click *Apply* to accept your edits and alter the list at the top of this screen, or *Cancel* to abandon them.

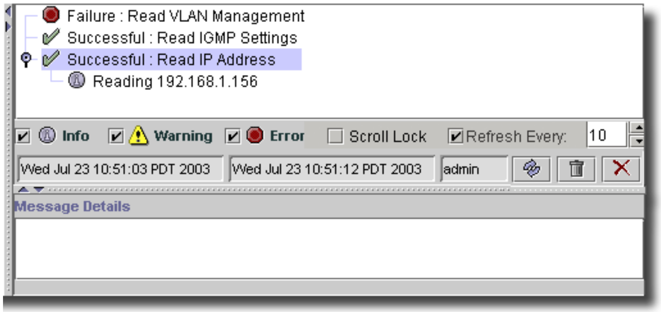
Specify Condition and Presentation

Finally, you can set the appearance of these configured attributes to alter based on filters. Click *Add Condition* to open an editor at the bottom of the screen to create such a condition (or *Edit Condition* to alter an existing, selected condition). Specifying conditions is like creating filters as described in Filtering and Searching on page 158. When the filter is satisfied, the appearance (presentation) configured applies within the Topology view. Click *Apply* to accept your edits, or *Cancel* to abandon them.

Audit / Results

The result of many application actions appears in a job status screen. These are preserved and catalogued in Audit Trail Manager.

Figure 11-12. Results Screen



- ● Failure : Read VLAN Management
- ✓ Successful : Read IGMP Settings
- ✓ Successful : Read IP Address
  - Reading 192.168.1.156

☑ Info ☑ Warning ☑ Error □ Scroll Lock ☑ Refresh Every: 10

Wed Jul 23 10:51:03 PDT 2003 | Wed Jul 23 10:51:12 PDT 2003 | admin

Message Details

At its top, this screen displays a series of actions and sub-actions as a tree. When you select an individual action, *Message Details* (if available) appear in the lowest panel. The bar between these two panels lets you check the type of messages to display (*Info*, *Warning*, *Error*) and displays the time/date of the beginning and end of the selected message's action, and the user who initiated it. It also lets you fine-tune the refresh rate of the screen (refresh is slow by default, for performance sake) and includes a checkbox to stop the screen from scrolling (*Scroll Lock*). Icons to the right of the time/date information let you refresh the screen, let you refresh the view, remove the current job from the view, or cancel a selected running job, respectively.

How to Get Help

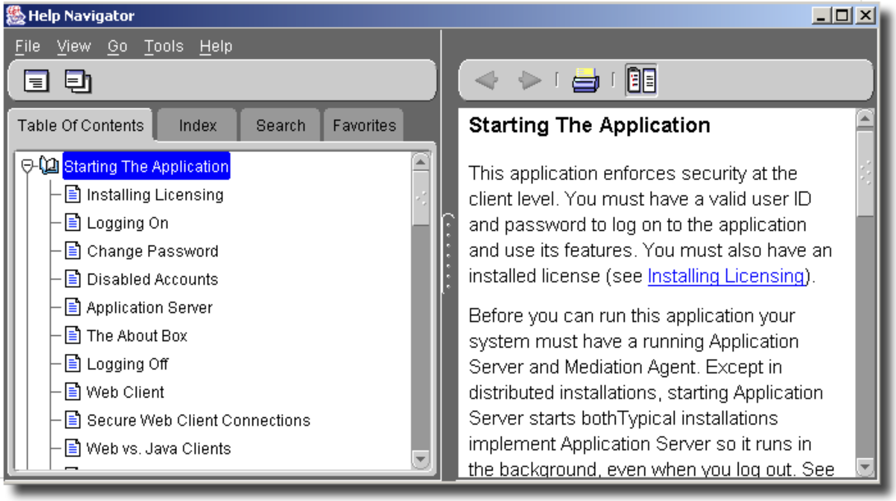
This application ships with guides in Acrobat form, and an online help system. To access the electronic version of the manuals you must have Acrobat Reader installed. See the installation CD for information about viewing Acrobat files, and for an installation of that free reader.

The helpset may contain information about features your installation does not have. Typically you can license these features (or simply ignore the help, if it is not relevant).

Online Help

You can access the online help by opening the *Help -> Help topics* menu item, clicking on the *Help* icon in the Toolbar, or by pressing the F1 key. This displays the Online Help Table of Contents, or a screen appropriate for the context.

Figure 11-13. Online Help System



Starting The Application

This application enforces security at the client level. You must have a valid user ID and password to log on to the application and use its features. You must also have an installed license (see Installing Licensing).

Before you can run this application your system must have a running Application Server and Mediation Agent. Except in distributed installations, starting Application Server starts bothTypical installations implement Application Server so it runs in the background, even when you log out. See

Pressing F1 typically displays help relevant to the screen that has focus in your application. Double-click a topic to open that topic in the right panel. You can also find relevant help topics by searching the *Index* tab, or with a full-text search from the *Search* tab. You can also add topics to the *Favorites* tab with *Tools -> Add to Favorites* (or Ctrl+T).

At its top, the panel displaying topics has (left-to-right) a button to restore focus to the *Navigator* (table of contents/index/search) panel, forward and back arrows to let you scroll though several topics, a print button, and dock/undock icons that let you combine/un-combine the *Navigator* and *Help Topic* windows.

NOTE:

Although index entries are frequent, they cannot comprehensively list every topic for which you may need help. When you cannot find the index entry you want, use the *Search* tab to perform a full-text search of the helpset. A similar feature exists for the Acrobat equivalent of the helpset, the manuals.

CAUTION:

Because of the flexibility of this software, help and manuals may describe features unavailable for your system. This can be true either because you do not have permissions to access everything, or because you do not have some options installed.

Troubleshooting

You can now use the `getlogs` script to package relevant logs if you need technical support. This script creates a `logs.jar` file in the root installation directory, and moves any existing copy of `logs.jar` to `oware\temp`. This jar compresses all logs necessary for troubleshooting. Read the jar yourself, or forward this jar to technical support to help troubleshoot.

Common Problems

The following are common problems you may want to check as part of your troubleshooting routine:

- Monitored devices must be configured to connect and send SNMP traps to the element management system.
- External FTP servers are preferable to internal, for performance reasons, and, if necessary, the network equipment using FTP to send/receive configuration files must have it enabled. If Backup / Restore fails, typically this means the FTP / TFTP server is offline or incorrectly configured. Check in the File Server Manager to correct this.

Troubleshooting Tips

The following are helpful tips when troubleshooting your application:

- **Connectivity to devices**—When devices are not discovered, ensure they are connected to the network with the `ping` command. Type the following:

```
ping <device IP address>
```

on a command line. If successful, several messages like the following appear:

```
Reply from <device IP address>: bytes=32 time=1ms TTL=128
```

- **Correct community strings/passwords**—Verify SNMP community strings and command line passwords are accurate if you have difficulty connecting to a device that responds to `ping.` You can inspect these in the *Settings* -> *Permissions* -> *Authentication Manager.* You must re-enter passwords concealed by asterisks.

- **Firmware and Operating Systems**—Verify the equipment's firmware and operating systems are among those supported. Supported firmware and operating systems appear listed in the application's *About* screens.

For more troubleshooting tips, consult the Administration Section.

12

Discovery

Resource Discovery Overview

Discovery is how the application identifies and catalogs network elements. Once discovery identifies a network element, you can create Resources, so the application can communicate with the element. The type and depth of discovery depends on installed applications and device drivers.

Discovery based on installed drivers consists of physical discovery and (potentially) link discovery. Physical discovery represents the device and all of its sub-components including modules, ports and interfaces. Link Discovery represents established links between neighbor devices, based upon protocol type.

You can do discovery interactively, as described in Resource Discovery on page 192, or you can set it up in advance as described in Resource Discovery Profiles on page 204 and schedule it for automatic execution, as described in Schedule on page 207.

Once discovery finds a device, it classifies that device as a Discovered Entity in the Resources manager unless the installed device drivers override this description and more accurately describe the discovered device.

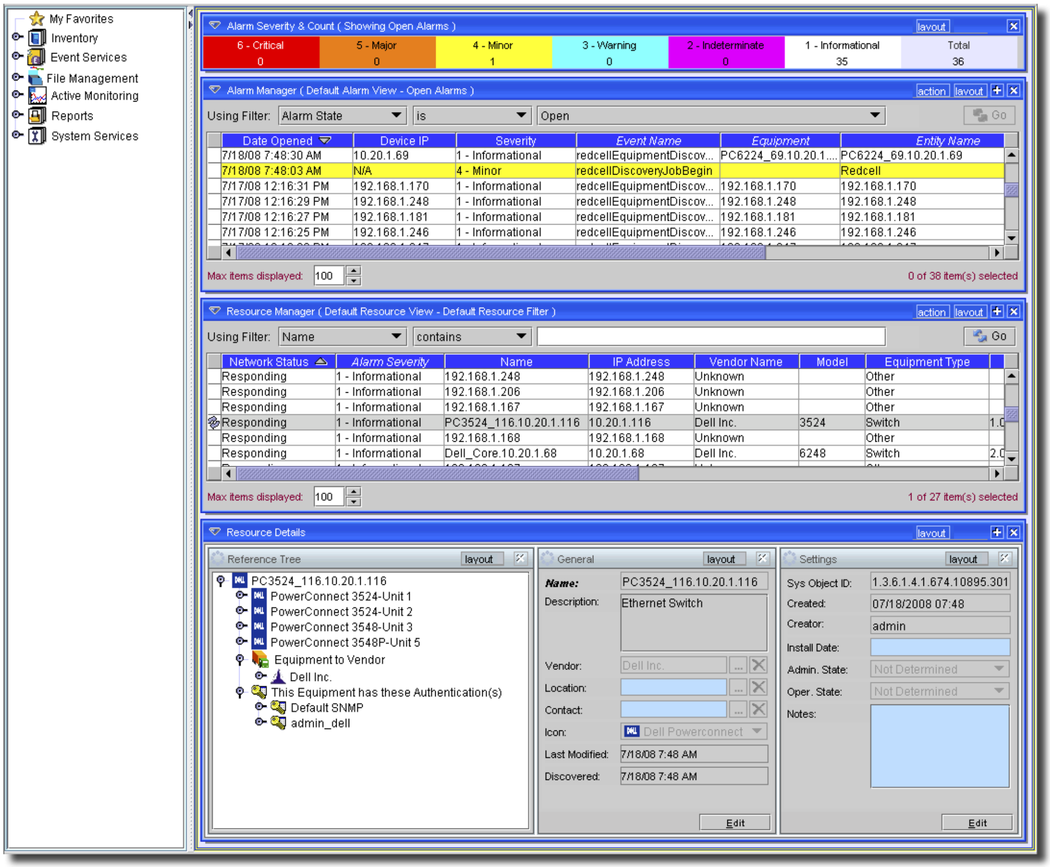
NOTE:

Expect longer discovery times if the discovered devices support OpenManage Network Manager’s pools, since the database retrieves additional data for those devices.

Discovery for admin User

The first time a OpenManage Network Manager client screen appears, after logging in, *admin* users get a special shortcut screen that offers discovery. Clicking *Begin Discovery* the discovery wizard opens for initial discovery of devices on your network. After completing discovery, by default, a QuickView layout appears with the discovered devices.

Figure 12-1. QuickView Layout



6 - Critical	5 - Major	4 - Minor	3 - Warning	2 - Indeterminate	1 - Informational	Total
0	0	1	0	0	35	36

Using Filter: Alarm State | is | Open

Date Opened	Device IP	Severity	Event Name	Equipment	Entity Name
7/18/08 7:48:30 AM	10.20.1.69	1 - Informational	redcellEquipmentDiscov...	PC6224_69.10.20.1....	PC6224_69.10.20.1.69
7/18/08 7:48:03 AM	N/A	4 - Minor	redcellDiscoveryJobBegin		Redcell
7/17/08 12:16:31 PM	192.168.1.170	1 - Informational	redcellEquipmentDiscov...	192.168.1.170	192.168.1.170
7/17/08 12:16:29 PM	192.168.1.248	1 - Informational	redcellEquipmentDiscov...	192.168.1.248	192.168.1.248
7/17/08 12:16:27 PM	192.168.1.181	1 - Informational	redcellEquipmentDiscov...	192.168.1.181	192.168.1.181
7/17/08 12:16:25 PM	192.168.1.246	1 - Informational	redcellEquipmentDiscov...	192.168.1.246	192.168.1.246

Max items displayed: 100

0 of 38 item(s) selected

Using Filter: Name | contains

Network Status	Alarm Severity	Name	IP Address	Vendor Name	Model	Equipment Type	
Responding	1 - Informational	192.168.1.248	192.168.1.248	Unknown		Other	
Responding	1 - Informational	192.168.1.206	192.168.1.206	Unknown		Other	
Responding	1 - Informational	192.168.1.167	192.168.1.167	Unknown		Other	
Responding	1 - Informational	PC3524_116.10.20.1.116	10.20.1.116	Dell Inc.	3524	Switch	1.0
Responding	1 - Informational	192.168.1.168	192.168.1.168	Unknown		Other	
Responding	1 - Informational	Dell_Core.10.20.1.68	10.20.1.68	Dell Inc.	6248	Switch	2.0

Max items displayed: 100

1 of 27 item(s) selected

PC3524_116.10.20.1.116
- PowerConnect 3524-Unit 1
- PowerConnect 3524-Unit 2
- PowerConnect 3548-Unit 3
- PowerConnect 3548P-Unit 5
- Equipment to Vendor
  - Dell Inc.
- This Equipment has these Authentication(s)
  - Default SNMP
  - admin_dell

Name: PC3524_116.10.20.1.116
Description: Ethernet Switch
Vendor: Dell Inc.
Location:
Contact:
Icon: Dell Powerconnect
Last Modified: 7/18/08 7:48 AM
Discovered: 7/18/08 7:48 AM

Sys Object ID: 1.3.6.1.4.1.674.10895.301
Created: 07/18/2008 07:48
Creator: admin
Install Date:
Admin. State: Not Determined
Oper. State: Not Determined
Notes:

Consult the online help for additional information.

Preventing Discovery Problems

The following describes some preventive practices to do when you discover a mixed vendor / mixed class network.

NOTE:

You can now use the Inspect step of Discovery to prevent problems before completing discovery itself. See Inspect on page 200.

1 Discover the device.

2 If there are any problems with any devices, then telnet to any problem devices and verify that telnet works / authentication is good.

3 If there are SNMP problems, use this application's SNMP tool.

Here's how to use that SNMP tool:

1 With the application server running, open a shell (*Start* -> *Run* `cmd`). In that shell, type the following commands (followed by [Enter]):

2 `oware`.

3 `snmpapitalk`.

4 `dest` <IP address of device you want to talk to>

5 `read` <read community>

6 `get` <snmpoid>. For the snmpoid, you can use syslocation or sysname

A response should appear. If the device does not respond, then there is a problem with either the community string, a firewall or some other network problem. Resolve this before proceeding with discovery.

Managing Devices with the Core Device Driver

This application can discover and manage most IT infrastructure devices on your network. The application's core discovery and management functionality works for most SNMP-enabled devices without using Standard Device Drivers, and enters an Unclassified Device in the database when discovery encounters such an SNMP-enabled device. Installing the Enterprise MIBs of a particular device type as described in MIB Browser on page 166 enables the greatest amount of functionality. The following is potentially available for such devices:

- Best-effort Device Discovery (using Entity MIBs).
- Inventory Tracking and Reporting.
- SNMP Event Reception / Alarm propagation.
- Performance Monitoring using SNMP MIB OIDs

This application automatically classifies devices detected with forwarding enabled as routers.

NOTE:

Third party devices on your network may appear as Dell Powerconnect switches during *OpenManage Network Manager* discovery. While you may be able to manage these devices with *OpenManage Network Manager*, they are not supported, and count against your licensed limit of unknown devices. You may choose to delete the non-supported devices from *OpenManage Network Manager* Resources or continue to manage these third party devices without support from Dell.

To enable full management functionality, including “deep discovery,” and advanced configuration and provisioning capabilities, you must install the applicable Standard Devices Driver(s) to match your network’s devices. (see Database Aging Policy Editor on page 718)

NOTE:

This software supports interface statistics collection only for devices which have a standard device driver installed.

Example Workflow

The Resource Discovery screen sets up the process of retrieving network and device information for the OpenManage Network Manager database.

1 Select Resource Discovery from the File -> Open -> Inventory menu, or from the Navigation Window, or by clicking the magnifying glass icon in the toolbar to launch the Discovery screen, open to the Discovery tab.

2 Click the *New* icon (far left) under Select Authentication.

3 The New / Edit Authentication screen appears. Select the Type of authentication, and fill in the IP/Password fields as appropriate for the devices you want to discover. Click A*pply* to return to the original screen.

NOTE:

You can change the Timeout, Retries and Port for authentications on this screen. Make sure you adjust the defaults to accommodate your network conditions.

4 Repeat the New authentication creation for as many authentications as are required. You will typically need two authentications for each device, an SNMP authentication and a Telnet / SSH authentication.

5 When you have configured the last of the authentications, enter the IP address(es) of the device(s) you want to discover in the Discovery tab's IP Address field under Select Network Type and Address. Notice that you can enter ranges as well as individual addresses, can retrieve these addresses from a text file, and so on. The section below provides a complete description of valid entries.

6 As you enter IP addresses, select the authentication that goes with each device by clicking the second-from-the-left icon under Select Authentication.

7 Click A*pply* to accept the device / authentication combination.

8 The Select Network Address(es) and Authentication(s) screen appears. Notice that you can click A*dd* to increase the list of addresses, *Edit* to revise what you have entered or *Remove* to delete a listed item. Notice also that you can re-order the selection, and the order in which devices are discovered, with the up/down top/bottom arrows below these buttons.

9 Click the Options tab to see additional Discovery features.

Notice that you can Select Discovery Options, Select Filtering Options (Not Available for Inspection), and Select Discovery Activities (Listed in Execution Order). The Activities default to one list, but you can add any Activity available in OpenManage Network Manager with the Select Activity command button (...) and search.

For the sake of this exercise, we will accept all defaults here.

10 Returning to the Discovery tab, click the Inspect button at the bottom of the screen. This previews discovery so you can confirm whether the target devices are online and the authentications you have configured are correct.

Notice that you can revise the authentications (including timeout and retry) with the hammer/wrench icon.

11 When you revise an authentication, you can also select the device and click *Test* to re-test it with the revision. Click A*pply* to accept your changes.

12 Once the A*uth Status* column of this screen displays the green check mark and *Ready to Discovery* message, click the *Discover* button.

13 A standard OpenManage Network Manager A*udit* screen appears (see Chapter 24, Audit Trails), and the resources discovered appear in the *Resources* manager, and the OpenManage Network Manager database.

Resource Discovery

The Resource Discovery screen sets up the process of retrieving network and device information for the OpenManage Network Manager database See Example Workflow on page 190 for an example of how to use this capability.

To begin, select *Resource Discovery* from the *File* -> *Open* -> *Inventory* menu, or from the Navigation Window, or by clicking the magnifying glass icon in the toolbar to launch the Discovery screen, open to the *Discovery* tab.

The *Discovery Tab* lets you select discovery targets in its upper panel (Select Network Type and Address), and combine them with authentications you configure in its lower panel (Select Authentication). You can also create new, or edit existing authentications with the New / Edit Authentication screen.

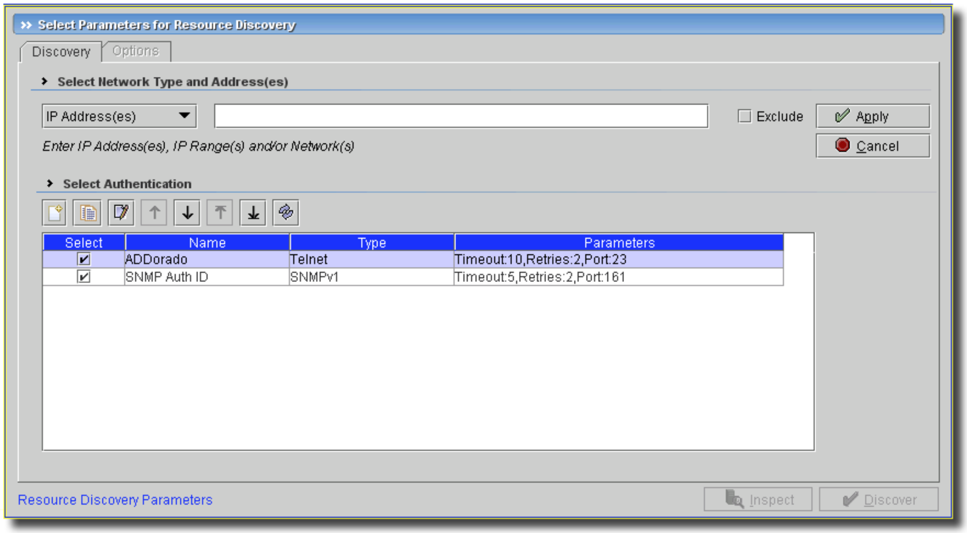
Check the *Exclude* checkbox to exclude the entry from discovery, and click *Cancel* to abandon your edits. Click A*pply* to accept the target and authentication combination you configure. This opens the Select Network Address(es) and Authentication(s) screen.

Clicking the *Inspect* button at the bottom of the screen previews discovery so you can confirm whether the target devices are online and the authentications you have configured are correct. See Inspect on page 200 for details of this process. If you click *Discover*, you initiate the discovery process that queries devices, storing them in the OpenManage Network Manager database. See *Discover on page* 202 for details.

Select Network Type and Address

On this screen, select the types of targets with a pick list at the top left corner, and fill in the data in the field to the right of this pick list.

Figure 12-2. Resource Discovery—Discovery Tab



Select Parameters for Resource Discovery
Discovery
Options
Select Network Type and Address(es)
□ Exclude
Apply
Cancel
Select Authentication
Resource Discovery Parameters
Inspect
Discover

IP Address(es)

Enter IP Address(es), IP Range(s) and/or Network(s)

Select	Name	Type	Parameters
☑	ADDorado	Telnet	Timeout:10,Retries:2,Port:23
☑	SNMP Auth ID	SNMPv1	Timeout:5,Retries:2,Port:161

The following are the types of target entries available

- **IP Address(es)**—In this field, you can enter many IP addresses, rather than one-at-a-time. This accepts entries in the following formats:

  –IP Address: 192.168.0.1

  –IP Range: 192.168.0.1-192.168.0.10

  –CIDR Network Format: 192.168.0.1/24

  –Network with Subnet Mask: 192.168.0.1/255.255.255.0

  –Multiples of any of the above is valid, separated by commas. 192.168.0.1,192.168.0.1-192.168.0.10,192.168.0.1/24, ….

  Entries in this field are validated to be IP addresses.

- **Hostname**—the name of the host you want to discover
- **CIDR Address**—For example: *Net* 192.168.0.0 / 24.

- **File**—A text list of IP addresses, one per line. Use the command button (...) to open a file browser, or type in the fully qualified path and filename.

⚠ **CAUTION:**

This text file does not support wildcards like the asterisk (*). Also: Best practice is to use a plain text editor to produce this file. Using formatted text (like Wordpad) can prevent OpenManage Network Manager from seeing the list of IP addresses.

- **Multicast SLP—** (Service Location Protocol) SLP dynamically locates services in the network. By default, some devices are SLP enabled which means they respond to SLP multicast packets with their service information. Management systems use this information to identify, locate and establish communication with them without any user inputs. This application's discovery supports SLP version 1.
- **SNMP Broadcast** —Every network comes with a broadcast address which can broadcast received packets to all the hosts in the network. For example, consider a network 192.168.0.1 - 192.168.0.254 with subnet mast 255.255.255.0 and broadcast address 192.168.0.255. If you send an SNMP packet to the broadcast address 192.168.0.255 from host 192.168.0.49, the packet gets broadcast to all the hosts from 192.168.0.1 to 192.168.0.254. All the SNMP enabled devices with respond to this request and send the response back to the host 192.168.0.49. This discovery option helps in locating new SNMP devices in the network without knowing the actual IP Address.

NOTE:

For Inspect or Discover OpenManage Network Manager imposes a limit of 65,535 addresses in a single discovery or inspection. You can alter some properties that configure these limits resource discovery.

```
# This property reflects the maximum number of discovery addresses possible
   in one discovery pass

redcell.discovery.maxcount=65535

# This property determines the threshold when a warning is displayed to the
   user if a number discovey addresses is exceeded

redcell.discovery.warningcount=100
```

Select Authentication

A panel appears at the bottom of the initial discovery screen with a list of available authentications. A row of icons appears at the top of this panel to let you *Create New* authentications, *Select Existing* authentications, or *Edit Selected* authentications. See New / Edit Authentication on page 196 for the more about the screen that appears for *New* and *Edit* selections.

NOTE:

When you *Select Existing*, you can still alter the *Type, Port, timeout* and *retries* for those credentials so you can use a Telnet authentication for an SSH connection to the device, and so device interactions take network connection speeds into account as discovery proceeds.

Up/down/top/bottom icons also appear in this toolbar so you can rearrange the order of these authentications. To move checked (*Select*ed) items to the top of the list, click *Resort*.

Click the *Select* icon or the checkbox in the list of authentications to use them with the selected item. Discovery targets often have multiple authentications, and you can check any number of those available.

When you select multiple authentication credentials, OpenManage Network Manager tries each one in the listed order. Best practice is to list the credentials more likely to succeed for the majority of devices first. Discovery does take longer when you add more credentials.

Once discovery identifies the device, its device driver can report additional authentication needs. Therefore, discovery results may change, depending on their order. For example if you specify SNMP and WMI credentials when discovering a Windows server, the server may respond to the SNMP request, but since OpenManage Network Manager cannot identify the device with the SNMP results, discovery then tries the WMI credentials. Here, OpenManage Network Manager would discover the device with both SNMP and WMI credentials since both were valid for that server. On the other hand if the order was WMI first, then SNMP, the device ultimately connects only with the WMI credentials because WMI can identify the target and discovery would not use the SNMP credentials.

Generally speaking, OpenManage Network Manager tries the SNMP credential first to identify the Equipment type with the sysObjectID. Once OpenManage Network Manager identifies the equipment type, the appropriate device driver requests and credentials let OpenManage Network Manager establish a CLI login and interrogate the device further for “deep” discovery. If discovery fails to get a valid SNMP authentication, then the device appears as an *UNKNOWN* entity. Using Inspect before discovery can disclose which credentials fail.

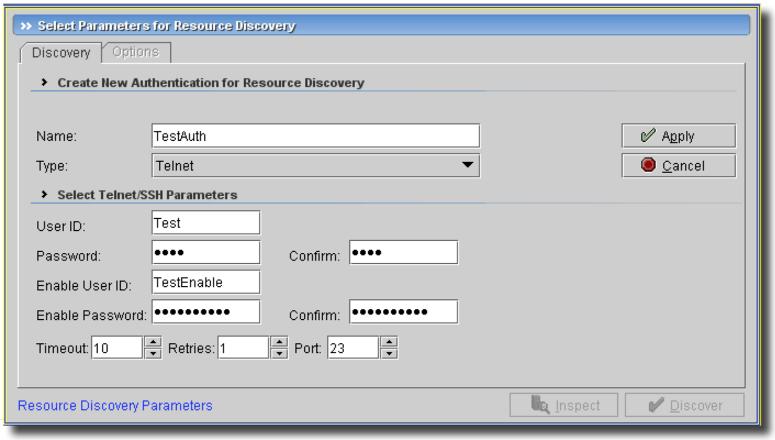
Discovery remembers the commonly used Authentications. When a device is discovered with a particular authentication, OpenManage Network Manager remembers it for on the next discovery execution. Remembered Authentications don't apply to Resource Profiles during editing or execution.

Click A*pply* to accept your edits, or *Cancel* to abandon them. You can then configure the Options tab.

New / Edit Authentication

You can select authentication(s) to go with a selected discovery target with the checkboxes that appear in the list of existing authentications in the Select Authentication panel. In addition, you can *Add* or *Edit* authentications to associate with that target. When you *Add* an authentication, or *Edit* an existing one, an authentication editor opens in the bottom of the screen.

Figure 12-3. Discovery—Authentication Editor



Select Parameters for Resource Discovery

Create New Authentication for Resource Discovery

Name: TestAuth

Type: Telnet

Select Telnet/SSH Parameters

User ID: Test

Password: •••• Confirm: ••••

Enable User ID: TestEnable

Enable Password: •••••••••• Confirm: ••••••••••

Timeout: 10 Retries: 1 Port: 23

Select or create the *Name* for the authentication, and select the *Type* from the pick list. See the *Administration Section* for details about what to expect for the different types.

NOTE:

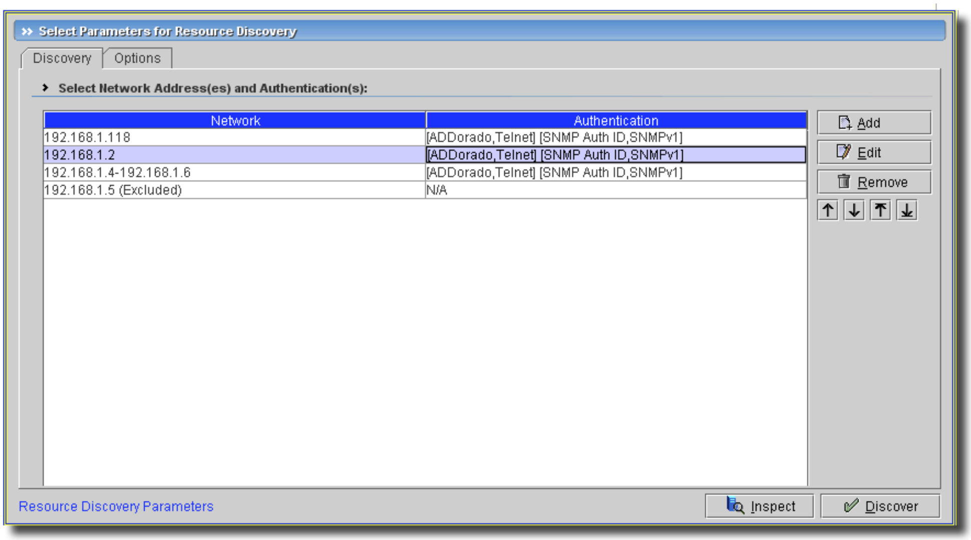
Ensure the type selected matches the management interface on the equipment you want to discovery. You can use some single authentications in different types, for example: Telnet and SSH.

Notice that you can also alter the *Timeout*, *Retries*, and *Port* for the authentication at the bottom of this screen, so the authentication fits with your network's connection speed.

Select Network Address(es) and Authentication(s)

This screen displays the discovery target devices and authentications you have selected and configured.

Figure 12-4. Selected Targets


Select Parameters for Resource Discovery
Discovery
Options
Select Network Address(es) and Authentication(s):
Add
Edit
Remove
Resource Discovery Parameters
Inspect
Discover

Network	Authentication
192.168.1.118	[ADDorado,Telnet] [SNMP Auth ID,SNMPv1]
192.168.1.2	[ADDorado,Telnet] [SNMP Auth ID,SNMPv1]
192.168.1.4-192.168.1.6	[ADDorado,Telnet] [SNMP Auth ID,SNMPv1]
192.168.1.5 (Excluded)	N/A

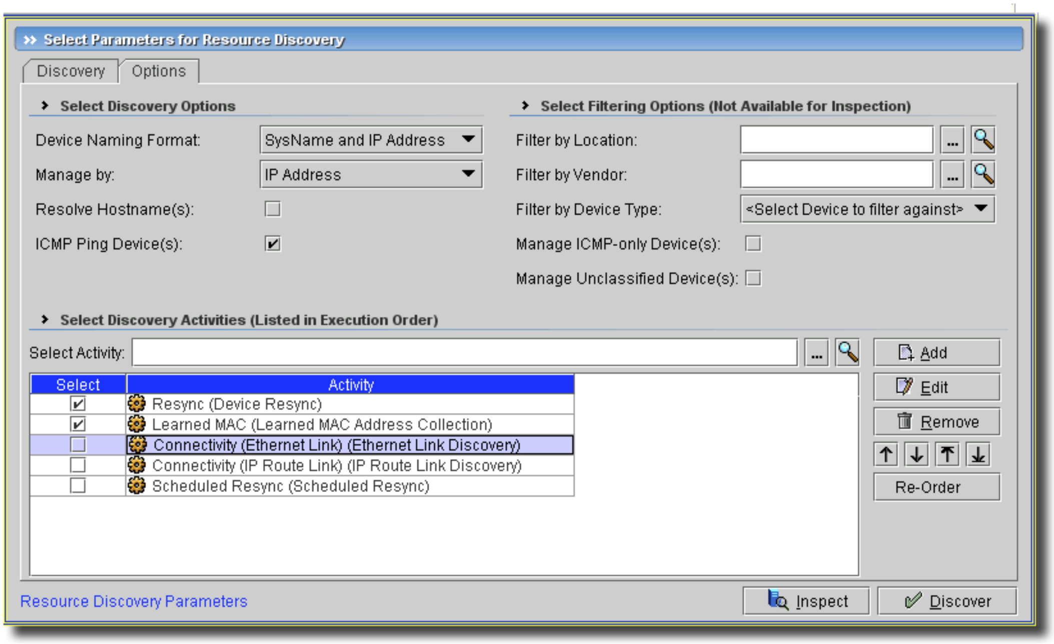
You can *Add* more devices with that button to the right of the list, or *Edit* a selected target to reconfigure the authentication. Doing so opens the Select Network Type and Address screen again. Click *Remove* to delete a listed target, and use the up/down/top/bottom buttons to re-order selected targets.

After you have configured this tab, you can configure global discovery Options with that tab, click the Inspect button or click the Discover button

Options

This screen lets you configure a variety of global discovery options for the targets configured in the *Discovery* tab (described in the Resource Discovery section)

Figure 12-5. Resource Discovery—Options Tab



Select Parameters for Resource Discovery
Discovery
Options
Select Discovery Options
Select Filtering Options (Not Available for Inspection)
Select Discovery Activities (Listed in Execution Order)
Add
Edit
Remove
Re-Order
Resource Discovery Parameters
Inspect
Discover

Device Naming Format: SysName and IP Address

Manage by: IP Address

Resolve Hostname(s): □

ICMP Ping Device(s): ☑

Filter by Location:

Filter by Vendor:

Filter by Device Type: <Select Device to filter against>

Manage ICMP-only Device(s): □

Manage Unclassified Device(s): □

Select Activity:

Select	Activity
☑	Resync (Device Resync)
☑	Learned MAC (Learned MAC Address Collection)
□	Connectivity (Ethernet Link) (Ethernet Link Discovery)
□	Connectivity (IP Route Link) (IP Route Link Discovery)
□	Scheduled Resync (Scheduled Resync)

This screen contains the following sections:

- Select Discovery Options
- Select Filtering Options (Not Available for Inspection)
- Select Discovery Activities (Listed in Execution Order)

These have the following fields, checkboxes and options:

Select Discovery Options

- **Device Naming Format**—This determines how the device appears, once discovered. The default is *SysName and IP Address*. SNMP interactions are what typically retrieve *Sysname*. Other options include *Hostname and IP Address*, *SysName*, *Hostname*, and *IP Address*. If discovery does not resolve the *SysName* or *Hostname*, and you selected it either by itself or in combination with *IP Address*, the *IP Address* still appears in the *Name* field.

- **Manage by**—Select whether to managed discovered items by *IP Address* or *hostname* with the pick list.

- **Resolve Hostname(s)**—When checked, this requests that discovery find not just IP addresses, but also resolve hostnames.

- **ICMP Ping Device(s)**—Check to send an ICMP ping to the target devices. Checking this activates the next checkbox.

Select Filtering Options (Not Available for Inspection)

This portion of the screen lets you configure filters for discovery targets. Inspect does not use what you configure here. It has the following fields and checkboxes:

- **Filter By**...Entering items in these fields activates the *Vendor*, *Location*, and *Device Type* filters. Use the command (...) or search buttons to the right of *Vendor* or *Location* to select these for your discovery. You can also confine discovery to the type of device selected in the *Device Type* pick list.
- **Manage ICMP-only Device(s)**—Check to manage target devices that respond only to ICMP ping. Managing these means that their presence is recorded in the OpenManage Network Manager database, but such management is necessarily more limited than devices that respond to more than ping.
- **Manage Unclassified Device(s)**—Check to manage target devices that do not respond to a specific device driver, but which still may return some information with SNMP or another protocol. See Managing Devices with the Core Device Driver on page 189 for more information.

Select Discovery Activities (Listed in Execution Order)

This portion of the screen lists activities to perform after discovery. Use the *Select Activity* field along with the command (...) and search buttons to its right to find activities. Selecting here lets you select from those listed by default. Click *Add* to list a selected activity below, checked as *Selected*. Some activities appear automatically (from the *default* discovery profile). Check those you want to activate.

The *Edit* button lets you configure the selected Activity's parameters, if that is available and appropriate. The editor also appears if you *Add* a task with configurable parameters. If you select an activity that requires user input, the standard attribute selection screen(s) for that activity appear during Discovery. Fill in the required attributes, and Discovery continues.

Remove deletes the selected activity from the list.

Activities that often appear (your package may vary) include *Resync (Device Resync)*, and *Learned MAC Address* collection. These let you discover subcomponents and learned MAC addresses for a device after you have discovered it. See Scheduling Learned MAC Discovery on page 630.

Other activities that typically appear here (unchecked by default) include *Ethernet Link Discovery*, *IP Route Link Discovery*, and *Scheduled Resync*.

NOTE:

You can add a task to add discovered devices to OpenManage Network Manager's heartbeat. You can configure what appears by default as described in Resource Discovery Profiles on page 204.

You can also use the up/down/top/bottom arrows to reorder selected rows, reordering what activities discovery executes. Regardless of the row order, however, device-based tasks run first, and group-based tasks (like link discovery) run last, since groups depend on their member information.

Clicking *Reorder* moves the activities with *Select* checked to the top of the list.

After you have configured this tab, you can click the Inspect button or click the Discover button.

Inspect

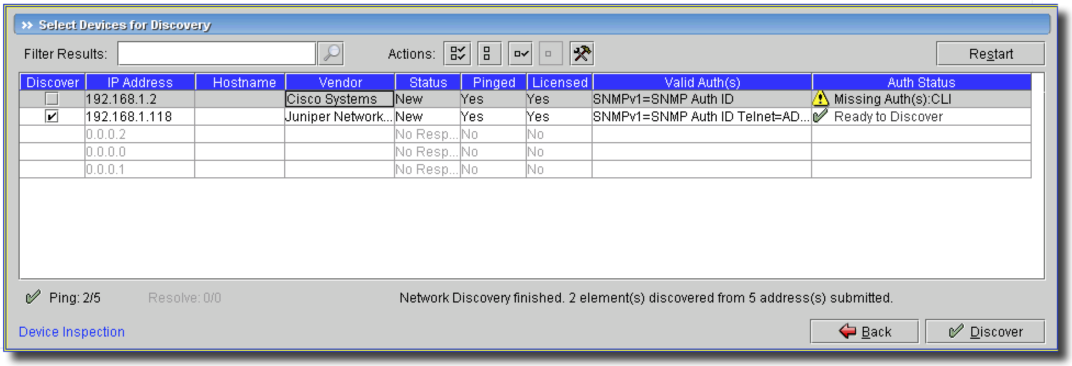
Clicking the *Inspect* button lets you validate the selected authentication credentials, displaying the devices' responses to the credentials you have set up in the Resource Discovery screen. Columns in the listed devices let you select which devices to *Discover* (by checking that checkbox), the *IP Address*, *Hostname*, *Vendor*, *Status*, whether the device was *Pinged* (and responded), whether OpenManage Network Manager management is *Licensed* for the device, the *Valid Auths*, and the status of selected authentications (*Auth Status*).

NOTE:

Inspection simplifies some manual steps that you can still do yourself. You can manually telnet to a device to verify that you have the correct authentication information. You can also examine the device's config file and verify that the SNMP community string is correct.

You can filter the results that appear listed in this screen by entering the text to search for in *Filter Results* at its top. You can also *Select* or *Deselect Device(s)*, and *Change Authentication* with the icons to the right of the filter. You can also use the *Discover* column's checkbox to select items to discover.

Figure 12-6. Discovery—Inspect/Authentications



Discover	IP Address	Hostname	Vendor	Status	Pinged	Licensed	Valid Auth(s)	Auth Status
□	192.168.1.2		Cisco Systems	New	Yes	Yes	SNMPv1=SNMP Auth ID	⚠ Missing Auth(s):CLI
☑	192.168.1.118		Juniper Network...	New	Yes	Yes	SNMPv1=SNMP Auth ID Telnet=AD...	✓ Ready to Discover
	0.0.0.2			No Resp...	No	No		
	0.0.0.0			No Resp...	No	No		
	0.0.0.1			No Resp...	No	No		

✓ Ping: 2/5 Resolve: 0/0 Network Discovery finished. 2 element(s) discovered from 5 address(s) submitted.

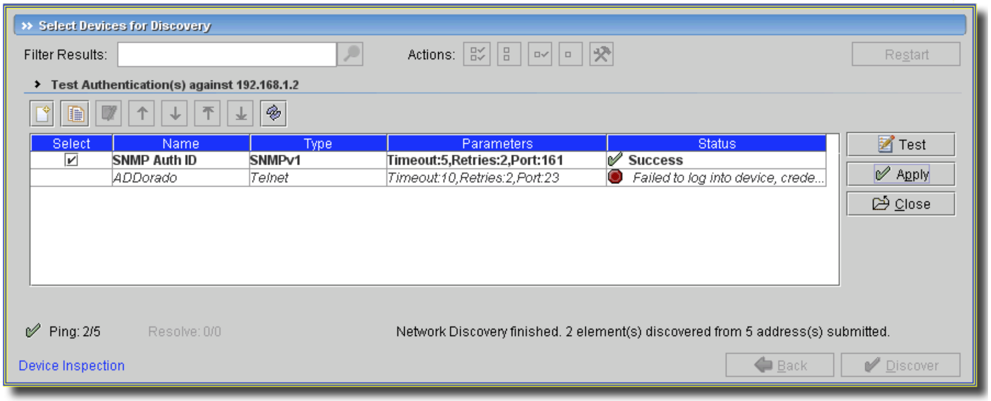
The columns in this screen display the *IP Address*, *Hostname*, and *Vendor* of inspected devices. It also displays *Status* (like New, or No Response), whether the device responded when *Pinged*, whether it is *Licensed* to be managed by OpenManage Network Manager, the list of *Valid Auth(s)* (validated authentication credentials), and the *Auth Status* that lets you know whether a device is ready to discover, or has missing or invalid auths. In this last case of missing or invalid credentials, you can click the *Change Authentication* icon.

From left to right, the icons let you select all devices for discovery, unselect them, select and unselect a single device, and change authentications. When you click *Change Authentication*, a screen like Select Network Address(es) and Authentication(s) screen appears. Use this screen to repair or replace invalid authentications.

All available authentications appear, with those connected to the device selected appearing checked. You can *Add*, *Select Edit*, and re-order these with the buttons above the list.

If you click *Test*, OpenManage Network Manager tests the selected authentication on the selected device. A green check icon appears next to working authentications, a red octagon appears next to those that fail, the yellow triangle icon indicates partial success—an option with multiple targets and authentications.

Figure 12-7. Testing Authentication



Test Authentication(s) against 192.168.1.2

Select	Name	Type	Parameters	Status
☑	SNMP Auth ID	SNMPv1	Timeout:5,Retries:2,Port:161	✓ Success
	ADDorado	Telnet	Timeout:10,Retries:2,Port:23	● Failed to log into device, crede...

✓ Ping: 2/5 Resolve: 0/0

Network Discovery finished. 2 element(s) discovered from 5 address(s) submitted.

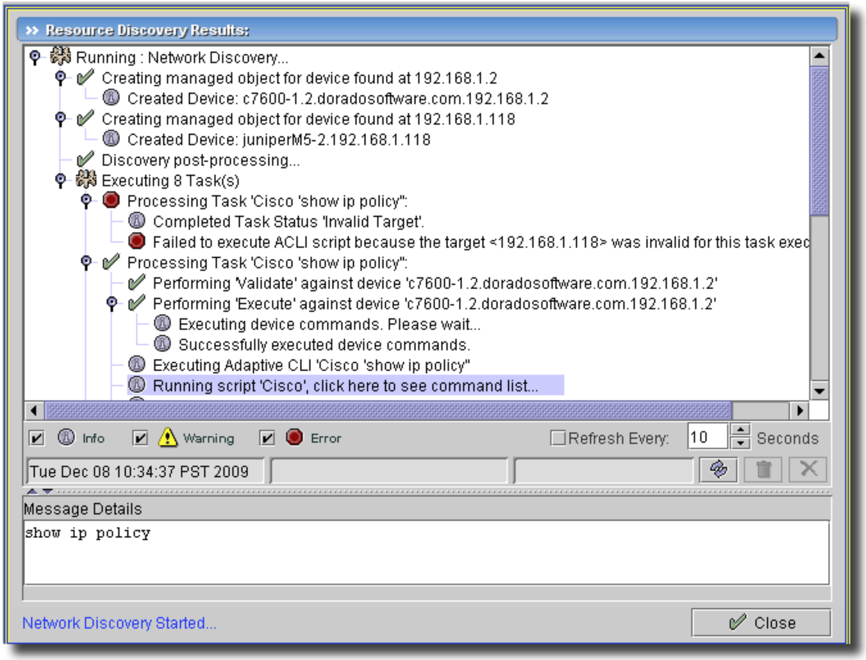
Click *Apply* after you have corrected or modified any invalid authentications with the *Change Authentications* button, or click *Close* to close this panel without modification. Notice that you can also change ports, timeouts and retries in the existing authentications with *Edit*.

After you have configured what is necessary in this screen, you can click the *Back* button to return to discovery setup (in Resource Discovery or Options) or click the Discover button.

Discover

Clicking the *Discover* button actually executes the discovery you have configured, storing the information retrieved from devices in the OpenManage Network Manager database.

Figure 12-8. Discovery—Results



Resource Discovery Results:

```
Running : Network Discovery...
    Creating managed object for device found at 192.168.1.2
        Created Device: c7600-1.2.doradosoftware.com.192.168.1.2
    Creating managed object for device found at 192.168.1.118
        Created Device: juniperM5-2.192.168.1.118
    Discovery post-processing...
    Executing 8 Task(s)
        Processing Task 'Cisco 'show ip policy'':
            Completed Task Status 'Invalid Target'.
            Failed to execute ACLI script because the target <192.168.1.118> was invalid for this task exec
        Processing Task 'Cisco 'show ip policy'':
            Performing 'Validate' against device 'c7600-1.2.doradosoftware.com.192.168.1.2'
            Performing 'Execute' against device 'c7600-1.2.doradosoftware.com.192.168.1.2'
                Executing device commands. Please wait...
                Successfully executed device commands.
            Executing Adaptive CLI 'Cisco 'show ip policy''
            Running script 'Cisco', click here to see command list...
```

☑ Info ☑ Warning ☑ Error ☐ Refresh Every: 10 Seconds

Tue Dec 08 10:34:37 PST 2009

Message Details

```
show ip policy
```

Network Discovery Started...

Clicking this button displays a standard OpenManage Network Manager audit screen. This displays the messages between OpenManage Network Manager and the discovered devices, including the post-discovery activities. Select a message in the top of the screen to see the time and date it occurred in mid-screen, and the contents of some messages in the *Message Details* panel at the bottom of this screen. See Chapter 24, Audit Trails for details of how to revisit this screen after discovery is complete.

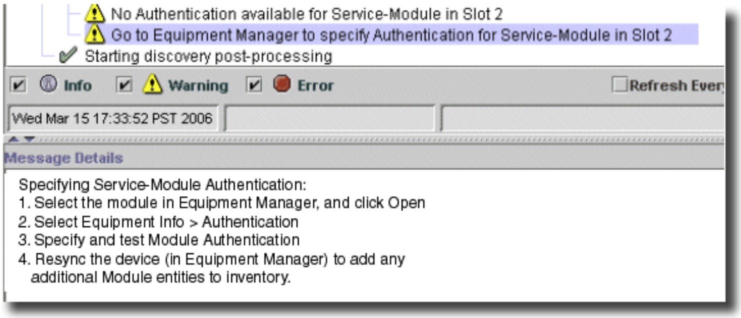
You can click *Close* at any time. If you click it before the *Equipment Discovery Finished* message appears, discovery continues in the background.

The final discovery panel, whether appearing for a Resource Discovery Profile or at the end of the a conventional basic / advanced discovery process presents asynchronous information. If you click *Finish* before the process is done, the discovery process still continues. While that is occurring you may not see elements being discovered in their resync schedule until the discovery job is actually complete. Executing scheduled resync while discovery is still ongoing may result in exceptions.

NOTE:

Some devices may require further authentication to access modules within them. Consult the device driver documentation for additional information.

Figure 12-9. Discovery Audit Requests Module Authentication



⚠ No Authentication available for Service-Module in Slot 2
⚠ Go to Equipment Manager to specify Authentication for Service-Module in Slot 2
✓ Starting discovery post-processing

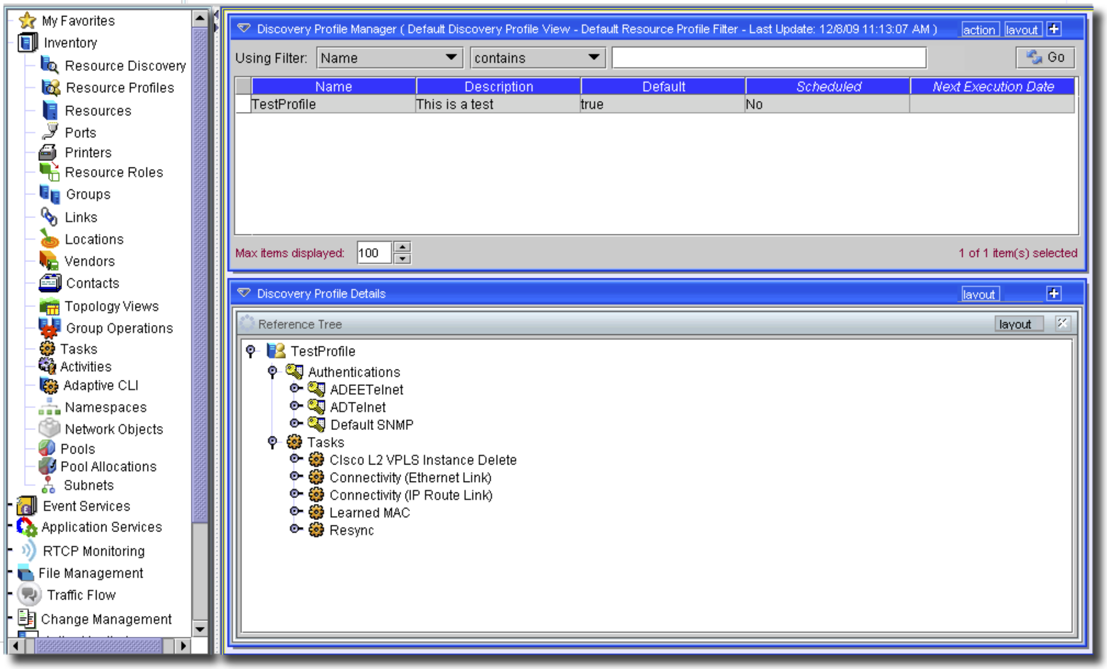
Wed Mar 15 17:33:52 PST 2006

Specifying Service-Module Authentication:
1. Select the module in Equipment Manager, and click Open
2. Select Equipment Info > Authentication
3. Specify and test Module Authentication
4. Resync the device (in Equipment Manager) to add any additional Module entities to inventory.

Resource Discovery Profiles

Creating a Resource Discovery Profile lets you store information about what you want to discover, along with any authentication needed for that device. Profiles let you store the parameters for discovery, and configure defaults for manual discovery, so you can easily execute (or schedule) repeated discoveries. To use profiles, either click *Execute* on the Profile Manager screen, or go to the scheduler (see Chapter 30, Schedules) and set up a schedule to run the profile. You can even have recurring discovery to keep your database description of discovered entities current with any changes.

Figure 12-10. Discovery Profiles



Discovery Profile Manager (Default Discovery Profile View - Default Resource Profile Filter - Last Update: 12/8/09 11:13:07 AM)

Using Filter: Name contains

Name	Description	Default	Scheduled	Next Execution Date
TestProfile	This is a test	true	No	

Max items displayed: 100

1 of 1 item(s) selected

The Discovery Profiles manager has the following *action* or right-click menu items:

- **New**—Create a new profile. See Creating and Editing Resource Discovery Profiles.
- **Open**—Edit an existing, selected profile. See Creating and Editing Resource Discovery Profiles.
- **Delete**—Delete an existing, selected profile.
- **Discover**—Use the selected profile(s) and perform discovery. The *Audit* screen then appears, displaying the messages between this software and the device.

- **Inspect**—Inspect the selected profile(s). See Inspect on page 200 for details.

- **Import / Export**—Import or export the listed profiles from/to an XML file.

CAUTION:
If the imported profiles refer to authentication credentials that do not exist on the system to which you have imported them, they do not work.

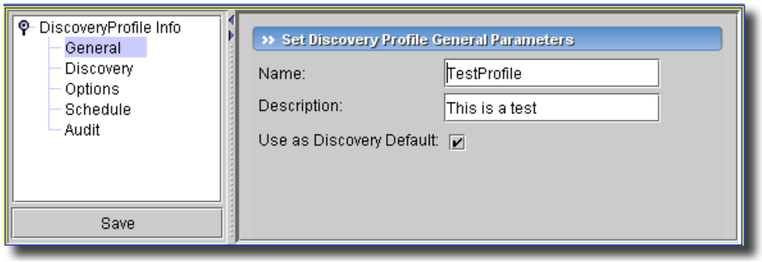
- **Help**—Open the online help for this screen.

The *Reference Tree* detail panel at the bottom of this manager displays a selected Profile’s authentications and tasks.

Creating and Editing Resource Discovery Profiles

Open the *Resource Profiles* manager, and click *New* to create a profile, or *Open* to modify an existing, selected profile.

Figure 12-11. Discovery Profile Editor - General Tab



Name: TestProfile

Description: This is a test

Use as Discovery Default: ☑

This editor has the following tabs:

- General
- Discovery
- Options
- Schedule
- Audit

Click *Save* to preserve the profile you have edited. Click *Go* in the manager that appears in *Resource Discovery Profiles* to see the profile listed.

General

This tab labels and classifies the discovery profile. It has the following fields:

- **Name**—An identifier for the profile.

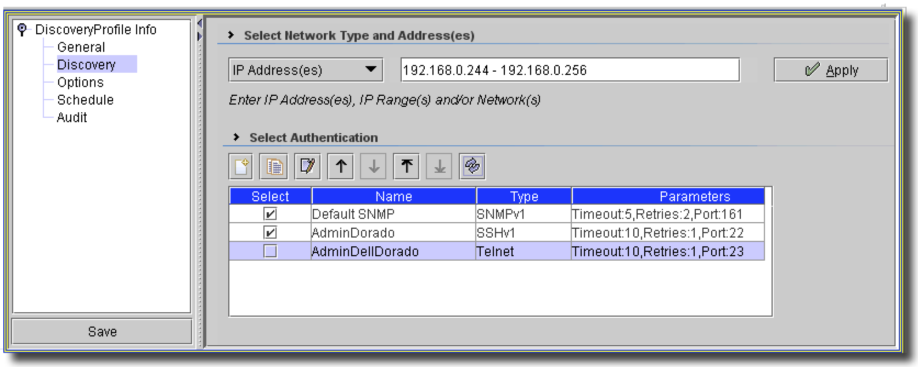
- **Description**—A text description of the profile.

- **Use as Discovery Default**—Check to make this profile the default discovery profile. Its parameters, including the selected device credentials, appear by default in the Resource Discovery screen.

Discovery

Configure fields in this tab to specify the devices and methods of discovery.

Figure 12-12. Discovery Profile Editor - Discovery Tab



Select Network Type and Address(es)

IP Address(es): 192.168.0.244 - 192.168.0.256

Enter IP Address(es), IP Range(s) and/or Network(s)

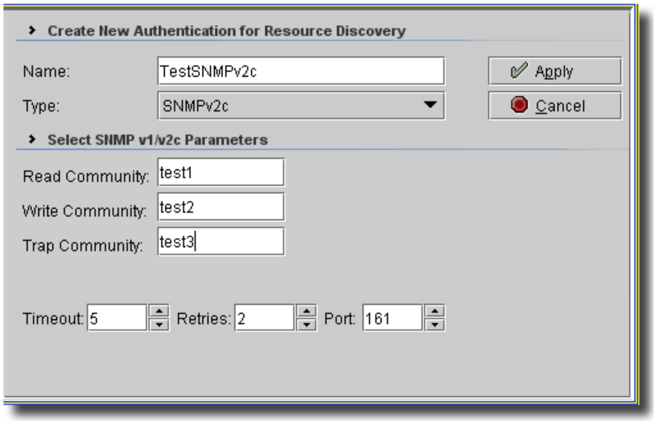
Select Authentication

Select	Name	Type	Parameters
☑	Default SNMP	SNMPv1	Timeout:5,Retries:2,Port:161
☑	AdminDorado	SSHv1	Timeout:10,Retries:1,Port:22
□	AdminDellDorado	Telnet	Timeout:10,Retries:1,Port:23

This tab works like the one described in Resource Discovery on page 192. Consult that section for details about how to enter discovery targets and authentications.

Notice that even when you provide an existing credential, you can re-configure the timeout, retry and port parameters for that credential. You can also click the *click to create New Authentication* and configure new credentials.

Figure 12-13. New Authentication



Create New Authentication for Resource Discovery

Name: TestSNMPv2c

Type: SNMPv2c

Select SNMP v1/v2c Parameters

Read Community: test1

Write Community: test2

Trap Community: test3

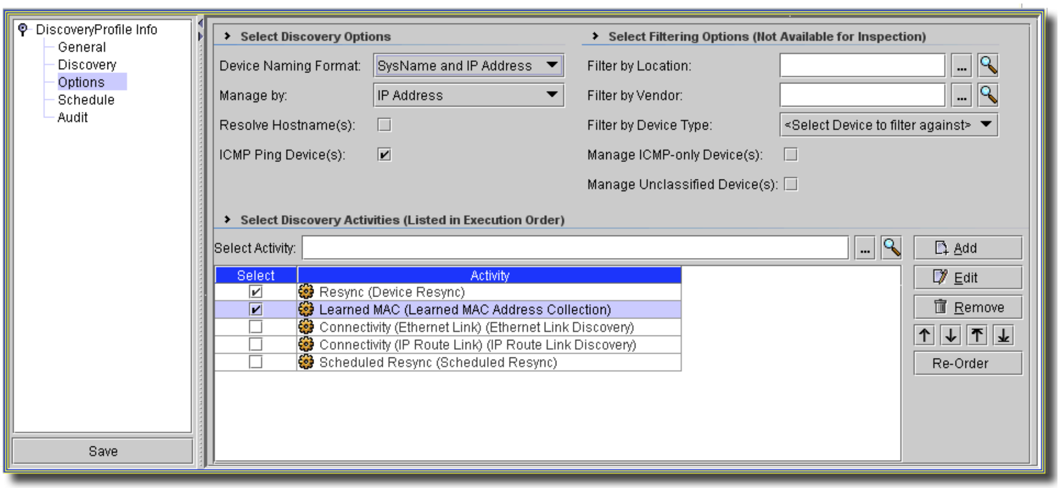
Timeout: 5 Retries: 2 Port: 161

Enter the identifying *Name*, select the type (here SNMPv2c), and enter the parameters for the authentication, including the timeout, retries and port.

Options

This tab lets you configure global options for the Resource Discovery Profile as described in Options on page 198.

Figure 12-14. Discovery Profile Editor - Options Tab



Select Discovery Options

Device Naming Format: SysName and IP Address

Manage by: IP Address

Resolve Hostname(s): □

ICMP Ping Device(s): ☑

Select Filtering Options (Not Available for Inspection)

Filter by Location:

Filter by Vendor:

Filter by Device Type: <Select Device to filter against>

Manage ICMP-only Device(s): □

Manage Unclassified Device(s): □

Select Discovery Activities (Listed in Execution Order)

Select Activity:

Select	Activity
☑	Resync (Device Resync)
☑	Learned MAC (Learned MAC Address Collection)
□	Connectivity (Ethernet Link) (Ethernet Link Discovery)
□	Connectivity (IP Route Link) (IP Route Link Discovery)
□	Scheduled Resync (Scheduled Resync)

Schedule

This is the standard OpenManage Network Manager schedule information screen described in Schedule Info on page 750. You can also initiate scheduled profile discovery from the OpenManage Network Manager schedule manager described in that chapter.

Audit

This screen records the history of this profile’s use. See Chapter 24, Audit Trails for more information about audits and how the application saves them.

13

Resources

The following sections describe screens available in this manager

- Introducing Resources
- Dell PowerConnect Device Driver
- Dell PowerConnect B-Series Device Driver
- Dell PowerConnect J-series Device Driver

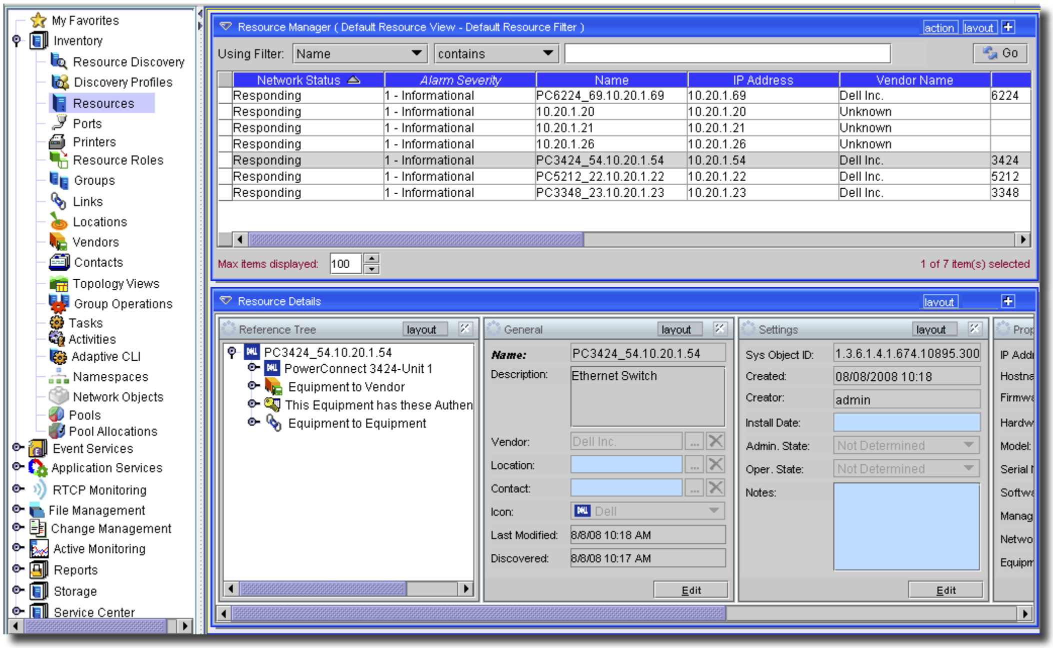
Introducing Resources

The Resources manager lets you manage devices you have discovered or created on your network. Optional applications and device drivers may increase the basic functionality described here, so your screens may not exactly match those appearing on the following pages.

The Resources manager lets you view device-specific information, both general (name, type, location, contact) and technical (vendor, subcomponents, and so on). Select and *Open* resources for edit to view additional information.

To open the Resources Manager, select *Inventory* -> *Resources* from the *File* -> *Open* menu or from the Navigation Window and click *Go*. You can then view all discovered or created resources.

Figure 13-1. Resources



Resource Manager (Default Resource View - Default Resource Filter)

Using Filter: Name contains

Network Status	Alarm Severity	Name	IP Address	Vendor Name	
Responding	1 - Informational	PC6224_69.10.20.1.69	10.20.1.69	Dell Inc.	6224
Responding	1 - Informational	10.20.1.20	10.20.1.20	Unknown	
Responding	1 - Informational	10.20.1.21	10.20.1.21	Unknown	
Responding	1 - Informational	10.20.1.26	10.20.1.26	Unknown	
Responding	1 - Informational	PC3424_54.10.20.1.54	10.20.1.54	Dell Inc.	3424
Responding	1 - Informational	PC5212_22.10.20.1.22	10.20.1.22	Dell Inc.	5212
Responding	1 - Informational	PC3348_23.10.20.1.23	10.20.1.23	Dell Inc.	3348

Max items displayed: 100

1 of 7 item(s) selected

Resource Details

Reference Tree

- PC3424_54.10.20.1.54
  - PowerConnect 3424-Unit 1
  - Equipment to Vendor
  - This Equipment has these Authen
  - Equipment to Equipment

General

Name:	PC3424_54.10.20.1.54
Description:	Ethernet Switch
Vendor:	Dell Inc.
Location:	
Contact:	
Icon:	Dell
Last Modified:	8/8/08 10:18 AM
Discovered:	8/8/08 10:17 AM

Settings

Sys Object ID:	1.3.6.1.4.1.674.10895.300
Created:	08/08/2008 10:18
Creator:	admin
Install Date:	
Admin. State:	Not Determined
Oper. State:	Not Determined
Notes:	

Prop

IP Addr
Hostna
Firmwa
Hardw
Model:
Serial I
Softwa
Manag
Netwo
Equipm

NOTE:

You must click Go to refresh this list after some operations. Resources displayed here refresh every 60 seconds, unless you modify or override the default interval as specified in `redcell.properties`.

In the default view, resources appear listed in the top of the screen, and details of a selected resource appears at the bottom in detail panels. As is typical for such screens with tables, you can add or delete columns in the top of screen panel, and you can add or delete detail panels at the bottom of the screen. See Chapter 31, Views, too.

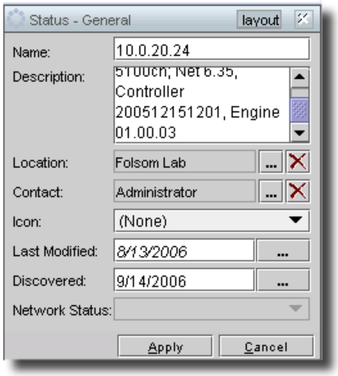
NOTE:

You can now add Customer Company Name as a Resources manager column.

Detail Panels

The detail panels that appear at the bottom of this screen by default have some conventions. See the sections following Editing Resources on page 217 for a description of the kinds of information that can appear in the detail panels. This section describes the Editor screens that may contain several such panels

Figure 13-2. Detail Panel



Name: 10.0.20.24

Description: 5100ch; Net 6.35, Controller 200512151201, Engine 01.00.03

Location: Folsom Lab

Contact: Administrator

Icon: (None)

Last Modified: 8/13/2006

Discovered: 9/14/2006

Network Status:

Click *Edit* to alter the contents of the panel, and *Apply* to accept your changes (*Cancel* leaves edit mode without saving changes). Another convention is that writable fields without contents appear light blue. Once you write in them, the fields turn green until they are saved to the database. If the save fails, then the green remains visible. The editor screens covered in General on page 218 and Reference Tree on page 221 describe several default panels.

Menus

The following are the controls available for managed resources. To use them, either right-click a selected resource, or select the resource and click the *Action* button. The actual appearance of the menus that appear next depends on what components you have installed. Menu items described below are also accessible in the *Action* button menu at the top right of the panel displaying the resources.

The specifics of menu items here appear in Action Button / Right-Click Menu on page 156.

The *Add to Group* context menu item lets you add the selected resource to a group (you can also select *New Group* to create a new group). See Groups Manager on page 635 for details.

Filtering the List of Resources

The Resource Manager displays a list of objects matching the selected filter. Select a different filter from the *Criteria Schemas* drop-down list to view resources matching different filter criteria. See *Chapter* 28, *Filters* for information about creating or editing filters.

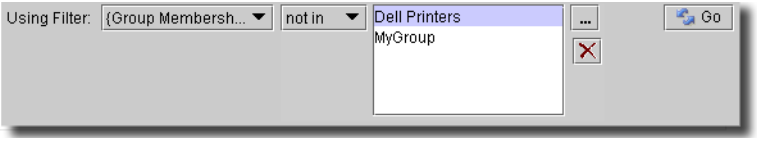
CAUTION:

Unless you create a filter and save it as described in Chapter 28, Filters, filters you make here are not preserved.

NOTE:

You can now filter on group membership. See Chapter 16, Groups for details about setting up such groups.

Figure 13-3. Filtering on Group Membership



Using Filter: {Group Membersh... not in

Dell Printers
MyGroup

NOTE:

Click the command button (...) to select one or more groups, and use the red "X" to delete a selected group. The operators are *in* and *not in*.

The IP data type now supports a *LIKE* operator. When you select *LIKE* in a filter, you can use a question mark (?) to replace a digits within the IP address. This means you can retrieve all IP addresses that contain 192.168.1??.???, for example.

For additional filtering and display options, see Quick Group on page 157 and Available Attribute List (+) on page 157. These describe the possibilities presented when you open the manager's attribute list by clicking the plus (+) to the right of the *Layout* button.

Limiting the Result Set

Information appears below the filter name indicating how many records the query found and how many are listed. To alter the maximum number of resources displayed, enter a number in the *Max Rows to Return* box (or use the up and down arrows to the right of the number field). Click *OK* to save your changes.

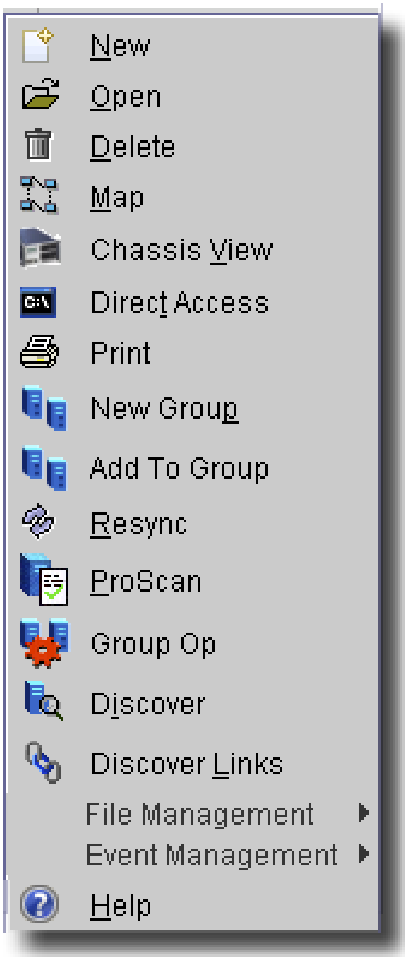
NOTE:

This feature ensures that you do not waste significant time while the application attempts to resolve a large or mistakenly unreasonable query. Where a query reaches the maximum result size, narrow the search criteria. If you cannot narrow the criteria, increase the maximum result size to handle the query.

Action Button / Right-Click Menu

Click the *action* button on the right of the title bar to expose a menu with additional capabilities for this screen. This menu's contents are also typically available when you right click a listed item (on web clients, you must use the action button on web clients). The exact contents of the menu depend on the installed options. These can include the following:

Figure 13-4. Action Menu



- **New**—Create a new resource. This opens a selector screen describing the type of (sub)component, then (once you have made your selection) the editor screen. The types you can select are organized in nodes in the screen that opens after you click *New*.

- **Delete**—Remove the listed resource.

- **Open**—Open the Resource Editor for the selected resource.

- **Map**—Open a topology view.
- **Direct Access**—Open a telnet, SNMP or http session to the selected resource. First, respond to the screen where you select the kind of session. After you select, a command line shell (for Telnet Sessions), MIB viewer screen (for SNMP Sessions) or web page in a browser opens that is connected to the device, using the associated authentication. See Direct Access Details on page 215 for more information.

NOTE:

Devices discovered without a supporting device driver installed support Direct Access functionally with telnet and SSHv1 (not SSHv2).

Telnet sessions are synchronous. You cannot interrupt a command in progress with another command you send, unless you have enabled something that periodically prompts for additional commands (for example enabling line continuation prompts).

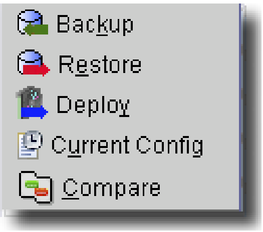
- **Print**—Create an Acrobat report of the printers displayed in the inventory (change the filter and click *Go* to change this display). You must have the free Acrobat reader installed for this to function. See www.adobe.com to download and install this application.

NOTE:

This report limits the number of columns to those that can fit on a single page width.

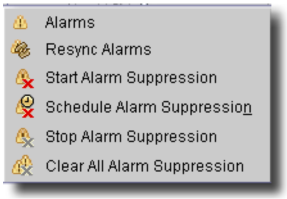
- **New Group**—Create a new equipment group.
- **Add to Group**—Add the selected to an existing group.
- **Resync**—Re-query the resource for up-to-date information.
- **Group Op**—Opens the Group Operations wizard with the selected group of devices as the group.
- **Discover**—Open the discovery wizard.
- **File Management**—If this option is installed, this sub-menu appears. It lets you *Backup*, *Restore*, *Deploy* (firmware), view the *Current Config*, and *Compare* configurations on the selected device

Figure 13-5. File Management Context Menu



- **Event Management**—Opens a submenu that includes the following:

Figure 13-6. Event Management



Alarms–Opens an Alarm window displaying the alarms filtered so they are only those related to the selected resources. You can change the filter manually to fine tune the display.

Resync Alarms—Re-queries the database for alarms for the selected device(s) to update topology. A confirming dialog appears if you select this menu item. Click *OK* to dismiss it.

-

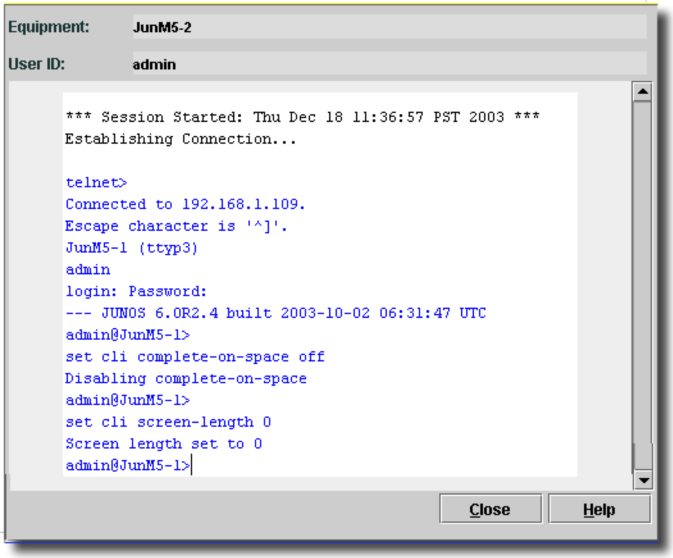
-

- **Key Metrics**—If Performance Monitoring is installed in your system, this opens the key metrics screen. See Key Metrics in Resources Editor on page 791.**Help**—Opens the online help for the Resources screen.

Direct Access Details

Direct access offers three different screens (Telnet Sessions, SNMP Sessions, and a web browser for HTTP) to communicate with a device after you have selected this action menu option

Figure 13-7. Telnet Direct Access



Equipment: JunM5-2

User ID: admin

```
*** Session Started: Thu Dec 18 11:36:57 PST 2003 ***
Establishing Connection...

telnet>
Connected to 192.168.1.109.
Escape character is '^]'.
JunM5-1 (ttyp3)
admin
login: Password:
--- JUNOS 6.0R2.4 built 2003-10-02 06:31:47 UTC
admin@JunM5-1>
set cli complete-on-space off
Disabling complete-on-space
admin@JunM5-1>
set cli screen-length 0
Screen length set to 0
admin@JunM5-1>
```

NOTE:

For direct access to devices configured without an enable password, create login credentials for such devices that do not include any enable information, only a user ID and password. You would then enter enable mode manually, after the direct access window opens. On the other hand, if the device does have an enable password, direct access enters enable mode without any manual intervention, provided the login credential contains the enable login and password information.

Telnet Sessions

You must mouse click in the Telnet Direct Access screen to begin typing there. You can configure logging in `/owareapps/ezmediation/lib/ezmediation.properties`.

NOTE:

This cut thru shell includes automatic command line completion.

NOTE:

Network security must permit communication between the client and application server. The application's mediation service initiates a protocol flow with the client. In that flow is the actual data of the telnet session between the mediation server and the device. Consult the *Administration Section* for details of ports and flows.

Telnet direct access automatically logs on to devices using the authentication credentials (EZMediation Authentication Dialog) provided by device drivers. It is integrated with this software's audit trail, providing key stroke logging for every telnet/SSH session with the device. It automatically logs out if the session stays idle for a long time.

You may see the following error messages related to cut thru dialogs:

- SSH v2 Protocol

Invalid server's version string – Cut thru tried to use SSH protocol version v2 to connect to the device running SSH protocol v1

A*uth fail* – Authentication Failure, please validate the user name and password used for cut thru with the device.

- SSH v1 Protocol

Login & password not accepted - Authentication Failure, please validate the user name and password used for cut thru with the device.

SNMP Sessions

This option opens a MIB browser. See MIB Browser on page 166 for details about this screen.

Editing Resources

When you want to create a new component or sub-component, click *New,* and select the type you want to create from the subsequent screen. The Resource Editor appears when you create or modify resources. Use *action -> Open* or right click a selected device and select *Open* from the menu that appears. The following sections describe these panels (and detail panels):

- General (*General, Properties, Settings* detail panels)
- Reference Tree
- Object Groups
- Custom Attributes
- Management Interfaces
- Authentication
- Equipment Roles
- Discovery
- Audit

The precise configuration of the Resources Editor depends upon the specific installation and the type of resource selected, as well as any customization that has been applied to the product. The panels described here are representative. Your installation’s appearance may vary, depending on the applications you have installed and the device drivers you have installed. Some screens, for example Change tracking (see Change Tracking on page 180), are described elsewhere because they appear throughout the application.

You can modify all default values. You can also set other values, including device-specific general (name, description, location) and technical (IP address, vendor, model) information. You can also set resource behavior and the resource icons. Note that the resource name must be unique.

NOTE:

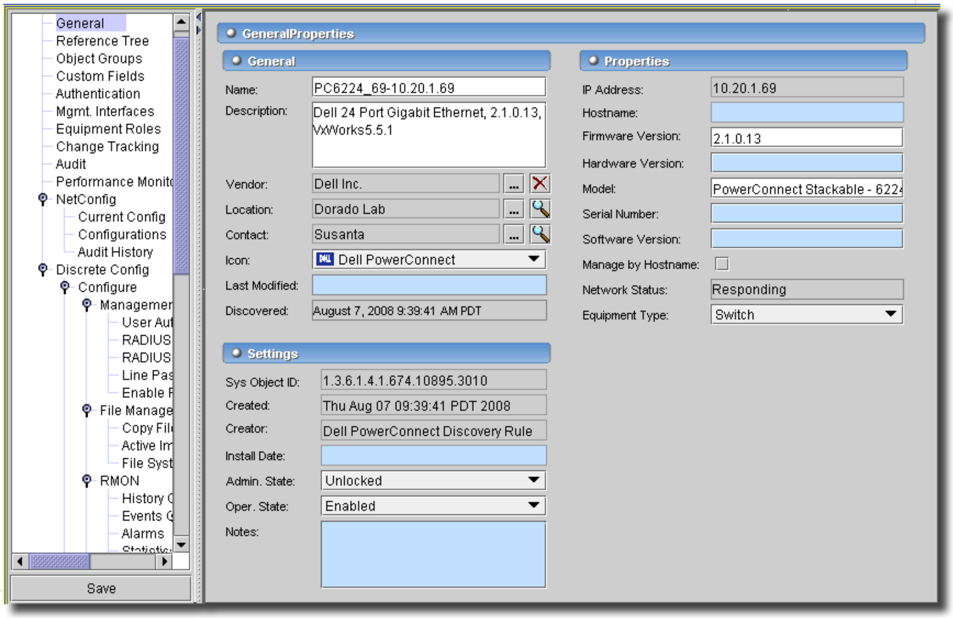
Some discovery processes occur even after you click *Finish* in the discovery wizard. If you want to edit a device's routing protocol settings, for example, best practice is to wait a few minutes after discovery finishes—otherwise these screens may be incorrect or not appear.

Click the *Save* button, or *File* -> *Save* after you have made any changes in these screens to preserve any edits.

General

The General panel lets you provide descriptive information for resources, and associate it with a location and a contact.

Figure 13-8. Resources Editor—General Panel (alternatives)



GeneralProperties

General

Name: PC6224_69-10.20.1.69

Description: Dell 24 Port Gigabit Ethernet, 2.1.0.13, VxWorks5.5.1

Vendor: Dell Inc.

Location: Dorado Lab

Contact: Susanta

Icon: Dell PowerConnect

Last Modified:

Discovered: August 7, 2008 9:39:41 AM PDT

Settings

Sys Object ID: 1.3.6.1.4.1.674.10895.3010

Created: Thu Aug 07 09:39:41 PDT 2008

Creator: Dell PowerConnect Discovery Rule

Install Date:

Admin. State: Unlocked

Oper. State: Enabled

Notes:

Properties

IP Address: 10.20.1.69

Hostname:

Firmware Version: 2.1.0.13

Hardware Version:

Model: PowerConnect Stackable - 622

Serial Number:

Software Version:

Manage by Hostname: □

Network Status: Responding

Equipment Type: Switch

The exact appearance of this panel depends on the device queried, and applications and device drivers installed in your system.

The fields Contact, Location, Serial Number, Software Version, Hardware Version, Firmware Version, Model, Creator and Created date fields are limited to 50 characters. If your entry exceeds that limit, the software automatically truncates it (from the right).

The following are the fields on this panel (the sub-panels can appear as details panels in the *Resources* screen:

General

- **Name**—The name of the resource; this name must be unique, and limited to 255 characters. The application automatically truncates names at this length, removing discovered or appended characters after 255. Discovery automatically adds the IP address to the end of the discovered name, but even that is truncated if the name's length exceeds 255 characters.
- **Description**—A description of the resource.
- **Vendor**—The vendor that manufactures/distributes this resource. Click the Location search button (the magnifying glass) or command button (...) to select a vendor from the Vendor Manager. See Chapter 19, Vendors, for more information.
- **Contact**—The application's recorded contact for this resource. Click the Contact search button (the magnifying glass) or command button (...) to select a contact from the Contact Manager. See Chapter 20, Contacts, for more information.
- **Location**—The application's recorded location of the resource. Click the Location search button (the magnifying glass) or command button (...) to select a location from the Location Manager. See Chapter 18, Locations for more information.
- **Icon**—Associates the resource with an icon. Select one from the drop-down list.
- **Last Modified**—The date for this resource's configuration's last modification.
- **Discovered**—The time and date this resource was discovered.

NOTE:

The application stores Location, Contact, and some other fields in its database, not on the device.

Settings

- **SysObjectID**—The SysObjectID of the resource.
- **Created**—(Read-only) The creation date and time of the database record, typically during discovery, for the resource.
- **Creator**—(Read-only) The user who created the resource.
- **Installed Date**—Date the resource was installed.
- **Administrative State**—One of three descriptive values, selected from a drop-down menu. The options are:

  Locked—Device use is prohibited.

  Shutting Down—Only existing users can use the device.

  Unlocked—Normal use of device is permitted.
- **Operational State**—One of following possible values, selected from a drop-down menu, describing the availability of the resource.

  Disabled—Inoperable because of a fault, or resources are unavailable.

  Enabled—Operable and available for use.

Active—Device is operable and currently in use with operating capacity available to support further services.

Busy—Operable and currently in use with no operating capacity to spare.

- **Notes**—Text notes. You must click *Save* for these to persist.

Properties

IP Address—The IP address of the resource.

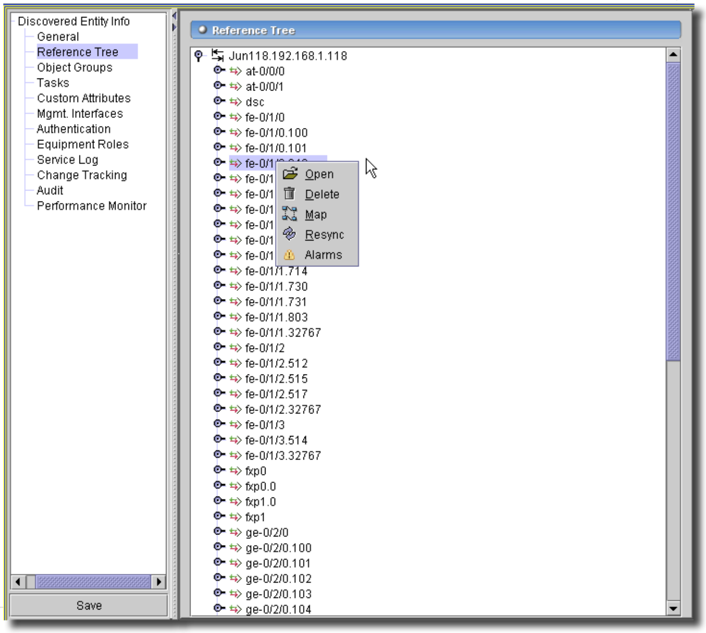
- **Hostname**—The DNS name of the resource; this name must be unique.
- **Firmware Version**—This resource's firmware version.
- **Hardware Version**—This resource's hardware version.
- **Model**—The resource's model number.
- **Serial Number**—The selected resource's serial number.
- **Software Version**—The selected resource's software version.
- **Manage by Hostname**—Check this to resolve DNS rather than use an IP address to manage this resources.
- **Equipment Class**—The class where the application stores this resource. If this is a discovered object, the application automatically stores it in `DiscoveredEntities`, unless a device driver automates storing it as another class.
- **Network Status**—The status of the resource in the network. For example: *Responding* means this application can, via some network protocol, get the device to respond. *Not Responding* means the device does not respond to the protocol. *Indeterminate* means the monitoring software has not tried to reach the device or there was some other error which prevented us from determining one of the other two statuses.

  The appearance of *Network Status* depends on heartbeat policy. If you disable heartbeat policy (for example, for performance reasons) then a status may appear, but it is not meaningful.
- **Equipment Type—**Select the type of equipment from the pick list.

Reference Tree

The *Reference Tree* displays the selected resource's connection to subcomponents, authentications, contacts, locations and vendors.

Figure 13-9. Preview Detail Panel

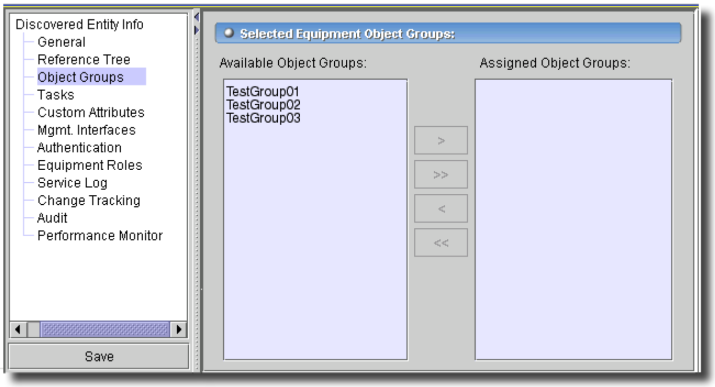


To change anything in a sub-component, select the node and right-click (select *Open*) or double-click the node in the *Preview* detail panel. You can also right-click and select *Map* to see the selected node displayed in a topology. Selecting *Delete* removes the node, *Resync* re-queries the device to retrieve updates about the node, and *Alarms* displays any alarms associated with the selected node.

Object Groups

This panel shows a list of Object groups to which the resource has been assigned. Object Groups are defined in the Object Group Manager.

Figure 13-10. Resource Editor—Object Groups Panel



TestGroup01
TestGroup02
TestGroup03

These groups control which users may view and/or edit device information. See your the *Administration Section* for more information about the Object Group Manager where you make them.

NOTE:

Only User-Created Groups appear in this window.

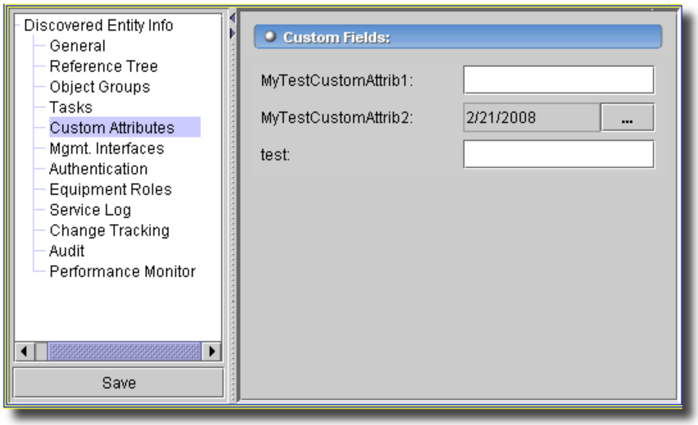
NOTE:

You cannot make individual interfaces part of an object group, but you can assign a role to them. Roles make natural groups, and you can use those role-based groups to manage the access to individual interfaces.

Custom Attributes

This panel displays any configured custom attributes for the selected device.

Figure 13-11. Custom Attributes



Custom Fields:

MyTestCustomAttrib1:

MyTestCustomAttrib2: 2/21/2008

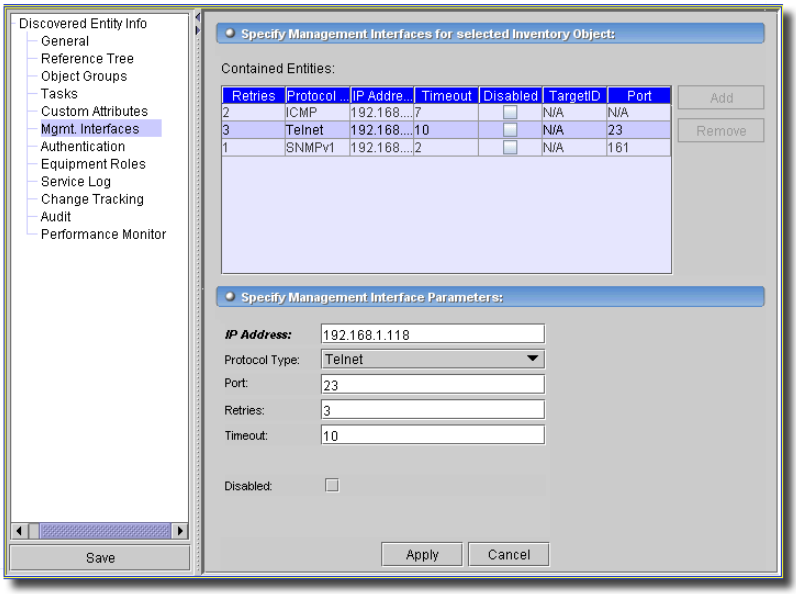
test:

See Custom Fields on page 178 for more about creating or modifying these.

Management Interfaces

Click *Add* to create a new Management Interface to add to the Management Interfaces list.

Figure 13-12. Management Interface Editor (alternatives)



Specify Management Interfaces for selected Inventory Object:

Contained Entities:

Retries	Protocol ...	IP Addre...	Timeout	Disabled	TargetID	Port
2	ICMP	192.168....	7	☐	N/A	N/A
3	Telnet	192.168....	10	☐	N/A	23
1	SNMPv1	192.168....	2	☐	N/A	161

Specify Management Interface Parameters:

IP Address: 192.168.1.118

Protocol Type: Telnet

Port: 23

Retries: 3

Timeout: 10

Disabled: ☐

Select an existing, listed interface and click the *Edit* button in the lowest panel to alter it. Click *Apply* to accept your edits, or *Cancel* to abandon them. The following are the fields on the Management Interface Editor(s):

- **IP Address**—The IP address of the Management Interface.

- **Protocol Type**—The Management Interface type; select from the following alternatives: *FTP HTTP, HTTPS, ICMP, IPMI, LDP, PORT9100, SNMP (v1,2,3), SSH, SSHv2, Simple Telnet, TL1, Telnet, WMI, WBEM, XNM-Clear-Text, XMN-SSL*. The listed alternatives may vary depending on what you have installed.

- **Port**—The Management Interface port.

- **Retries**—Enter a number of retries for the interface.

- **Timeout**—Enter the seconds before timeout occurs.

- **Engine / Target ID**—Engine ID is for SNMP v3. Target ID is for other interfaces.

NOTE:

For the application to correctly receive SNMP v3 traps, you must configure the authentication for a device in the Resource Editor Authentication (Management Interfaces) screen. See Authentication on page 225.

Disabled—Check to disable the interface.

NOTE:

Which editor fields that appear may depend on the type of interface you are editing.

SNMP v3

To configure your software for SNMP v3 traps, you must do the following:

- Confirm the deviceNetManager has an SNMP v3 management interface. If none exists, you must also create one. (See Management Interfaces on page 223). Configure the SNMP v3 management interface with the correct Engine ID from the device. This Engine ID is only required for receiving traps from the device.
- You must also configure authentication by selecting that screen in the Resources Editor. If no SNMPv3 authentication exists, you must create one.

Informs

For the application to correctly receive and acknowledge SNMP v3 traps, you must configure the authentication for a device in the Resource Editor Management Interfaces screen.

To properly configure this software to receive informs:

1 Discover the device using SNMP v3.

2 Edit the device's SNMP v3 management interface, setting the SNMP v3 Engine ID/Target ID:

The Engine ID/Target ID for the System concatenates 00000063000100A1 with the local IP address (in hex). For example, if the IP Address is 192.168.0.154 then the Engine ID is 00000063000100A1C0A8009A.

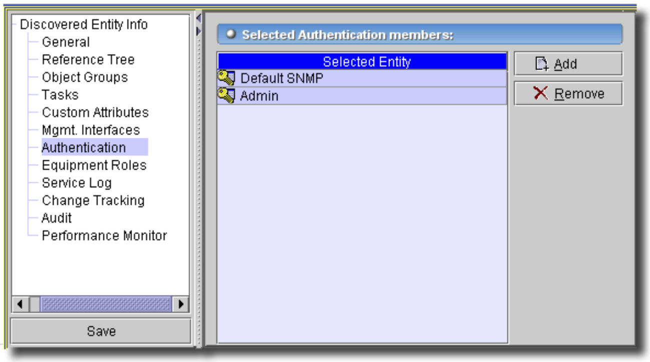
The first portion of the Engine ID is always 00000063000100A1, and the value of `oware.local.ip.address` property in `installed.properties` provides four decimal values that, when converted to HEX, provide the remainder of the Engine ID. You must set this number on the SNMP V3 management interface of the managed device.

3 Assuming the device is configured correctly to send informs, the informs appear in the Alarm window as subtype *inform*.

Authentication

This panel displays authentication profiles configured for the selected Resource. The Data Collection and Resynchronization rules use these profiles to establish a connection to the device.

Figure 13-13. Resource Editor—Authentication Panel (alternatives)



Selected Entity
Default SNMP
Admin

OpenManage Network Manager must have user access to devices commensurate with its power to read or write to the device. If this means “root” or “superuser” authentication, then that access must be what the application uses before all capabilities are available.

The Authentication panel lets you click *Remove* to delete a selected authentication, or *Add* to enter a new one. The *Add* button opens a selection screen that looks like Authentication Manager.

This screen configures the application database, not the selected resource. For changes here to take effect so authentication can provide information for other panels, you must click Save, close the Resource Editor, and re-open it.

CAUTION:
If you add an authentication, before it can be effective, you must associate it with Management Interfaces. Make sure the device has a management interface to match the authentication. Without this, resync fails.

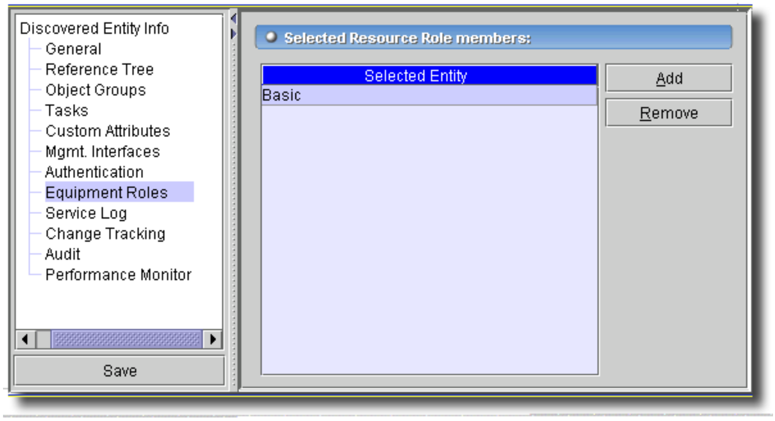
NOTE:

Device discovery or resync can fail if network or device latency delays authentication beyond the time–outs specified here. You can increase timeouts if these fail, or simply take your network's latency into account when you set authentication timeouts in the first place.

Equipment Roles

Some managed objects have this screen rather than a *Roles* field in the *General* panel.

Figure 13-14. Equipment Roles

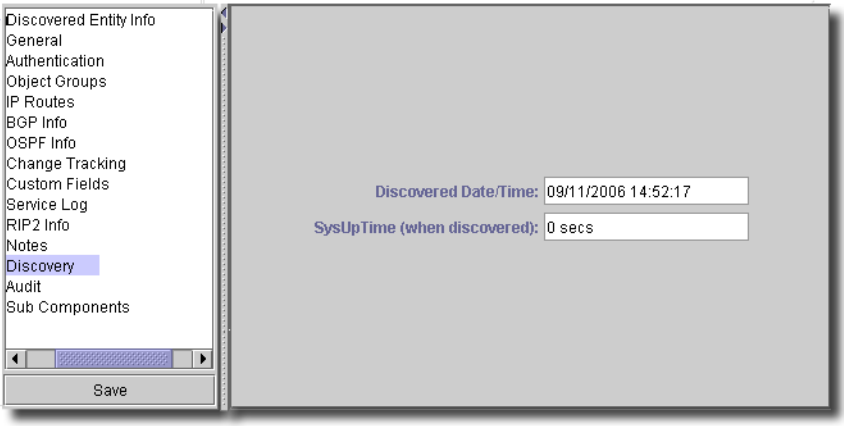


Click *Add* to select a role to list here, or select a role and click *Remove* to remove it. See *Chapter 15, Resource Roles* for more about roles.

Discovery

This panel displays information only for *DiscoveredEntities* (otherwise unclassified managed objects).

Figure 13-15. Resource Editor—Discovery Panel



Discovered Date/Time: 09/11/2006 14:52:17

SysUpTime (when discovered): 0 secs

It appears with the following fields:

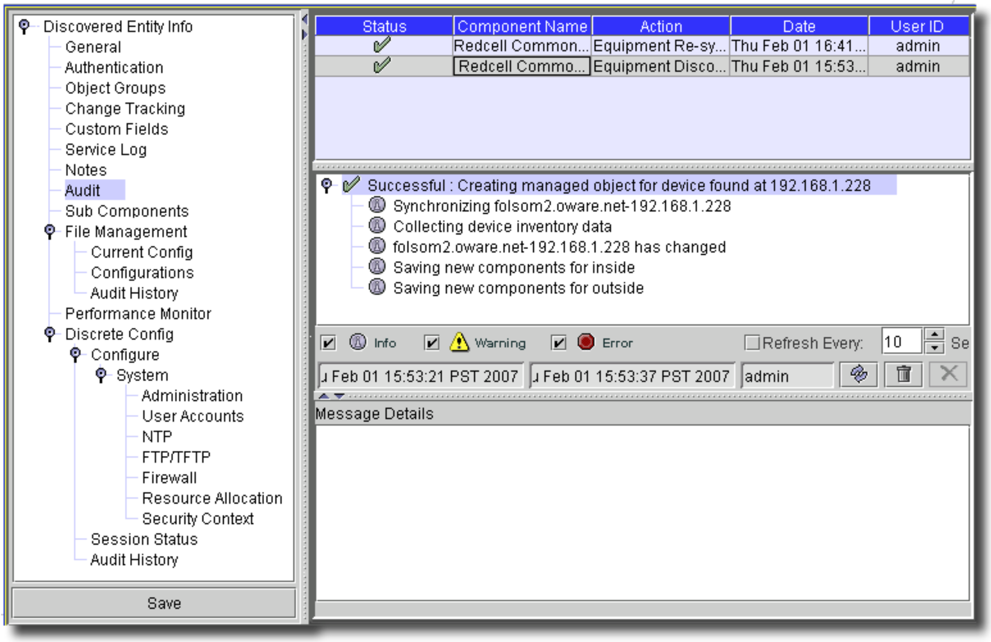
- **Discovered Date / Time—**The time this resource was first discovered.

- **SysUpTime (when discovered)** —The amount of uptime (measured since first discovery)

Audit

This screen catalogs the actions involving the selected device, notification, report, and so on.

Figure 13-16. Resources Manager—Audit



Status	Component Name	Action	Date	User ID
✓	Redcell Common...	Equipment Re-sy...	Thu Feb 01 16:41...	admin
✓	Redcell Commo...	Equipment Disco...	Thu Feb 01 15:53...	admin

```
✓ Successful : Creating managed object for device found at 192.168.1.228
    Synchronizing folsom2.oware.net-192.168.1.228
    Collecting device inventory data
    folsom2.oware.net-192.168.1.228 has changed
    Saving new components for inside
    Saving new components for outside
```

☑ Info ☑ Warning ☑ Error ☐Refresh Every: 10 Se

Feb 01 15:53:21 PST 2007 | Feb 01 15:53:37 PST 2007 | admin

Message Details

It also can appear in connection with other portions of this application and with optional add-ons. Its location within the tree of nodes tells which portion of the application the audit panel tracks. The topmost audit trail node lists general audit trails and those for any other such audit panels.

Actions appear in a list, at the top of the panel, then in more detail in the middle of the panel. The lowest part of the panel displays details of individual messages. This panel also appears in the optional Group Operations screens.

NOTE:

The *Refresh* button at the bottom of Resource Editor screens retrieves current information from the device. Any pending edits are lost. To confirm edits, click *Configure.*

Dell PowerConnect Device Driver

Sections here discuss the Dell™ PowerConnect™ Device Driver-related panels, and how this device driver changes Resource Editor and other aspects of the application's operation. The exact appearance and order of the screens described here depends on the device selected in Resource Manager.

Not all fields described below appear in all screens, just as all features are not supported by all models. Screen and tree appearance may vary slightly, even if they are supported. See also Dell Default Screens on page 370, and Additional Dell Screens on page 394 for a description of the screens that appear when you discover those devices.

Supported Powerconnect systems include the following models: PC3424, PC3424P, PC3448, PC3448P, PC3524, PC3524P, PC3548, PC3548P, PC5316M, PC5324, PC5424, PC5448, PC6024, PC6024F, PCM6220, PC6224, PC6224F, PC6224P, PC6248, PC6248P, PCM6348, PC8024, PCM8024 and PC8024F. (See the *Help > About* box for firmware details). Dell has discontinued support for the PC3024, PC3048, PC3324, PC3348, PC3248, PC5012, PC5212, and PC5224 models, although this software may still discover and manage these.

PowerConnect M-Series Discovery and Resync

The Dell PowerConnect modular switches for blade servers (like the PCM8024, PCM6324, and PCM6220) support two modes: *simple* and *normal*.

When it is in simple mode on initial discovery, this application discovers the top level device alone, without sub-components. Discovery finds no equipment features except *System Settings*. No backup / restore / deploy features are available, either.

If you change the device to *normal* and resync, discovery finds the device's sub-components, and backup / restore / deploy features and other features besides *System Settings* become available. Resource editor screens configure the device as long as the mode is *normal*.

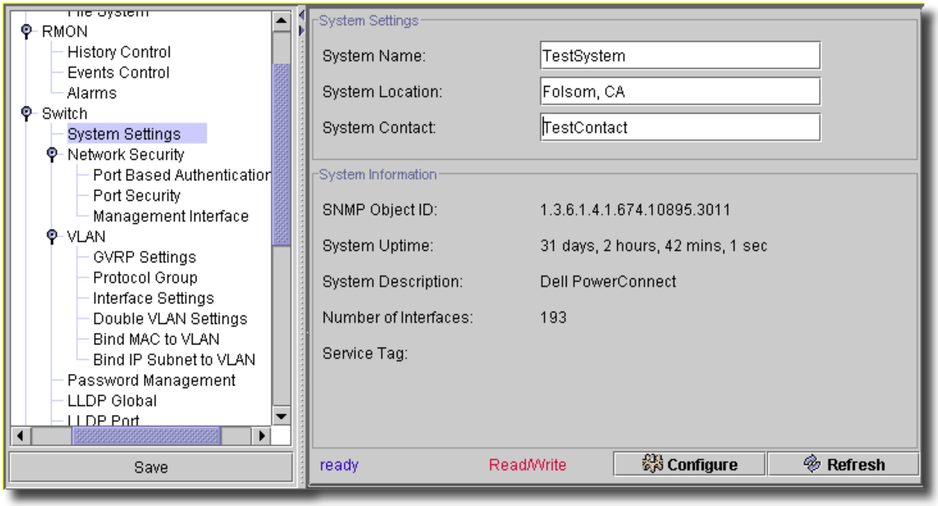
If you discover the switch in *normal* mode, all features are discovered and available, including configuration / backup / deploy. If you change the mode of the device to *simple*, but do not resync, sub-components still appear, as do the other features, but any attempt to read/write produces an error message saying that the operation is impossible because of the mode change, and advises a resync.

If you change the device's mode to *simple* and resync, previously discovered sub-components are deleted, and only the top level device appears. *System Settings* is the only resource editor screen that works, and backup / restore and deploy are not supported.

System Settings

This screen lets you manage basic system settings for a selected device.

Figure 13-1. System Settings



System Settings

System Name: TestSystem

System Location: Folsom, CA

System Contact: TestContact

System Information

SNMP Object ID: 1.3.6.1.4.1.674.10895.3011

System Uptime: 31 days, 2 hours, 42 mins, 1 sec

System Description: Dell PowerConnect

Number of Interfaces: 193

Service Tag:

ready Read/Write

The following are fields on this screen, defined when not self-evident:

- **System Name**—Text.

- **System Location**—Text

- **System Contact**—Text

- The following are read-only fields:

- **SNMP Object ID**—Switch SysObjId

- **System Up Time**—Switch Uptime

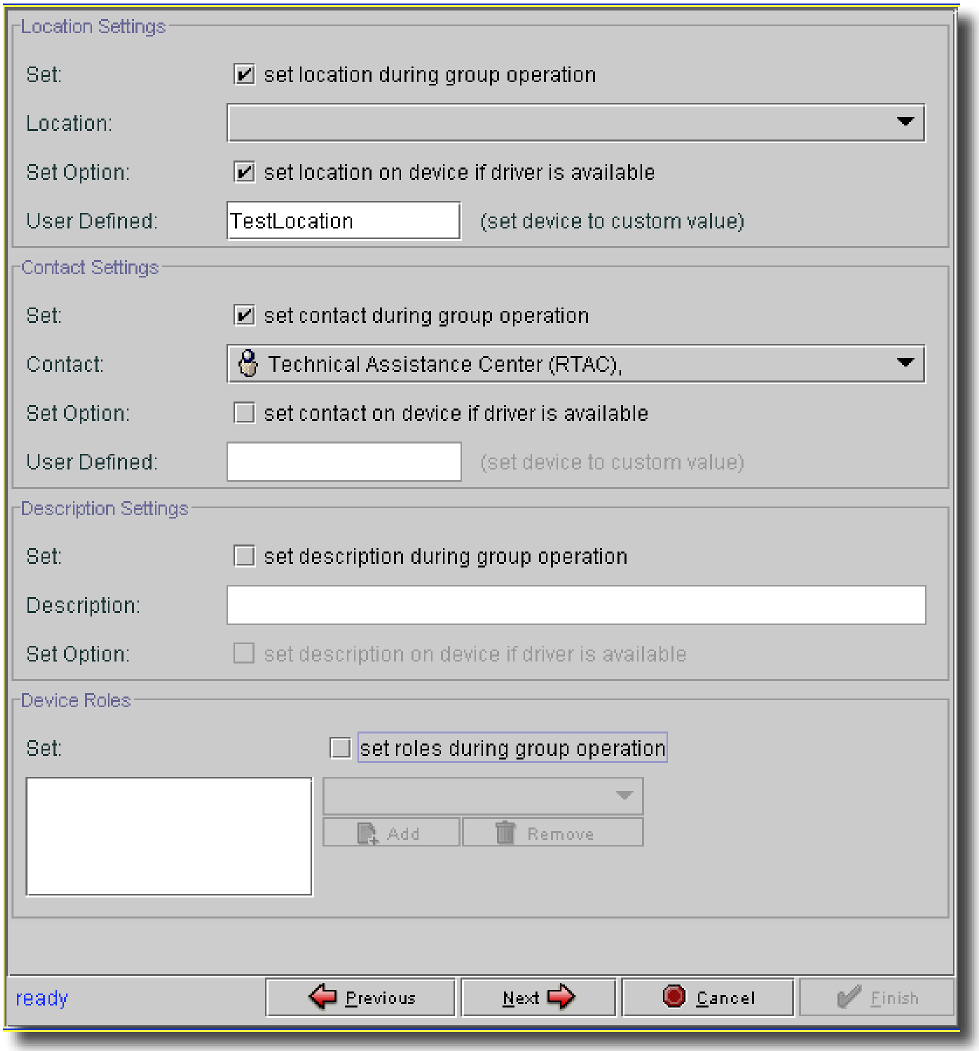
- **System Description**—A text description of the system

- **Number of Interfaces**—The number of interfaces

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed (and any edits are lost).

A screen where you can set the read-only fields appears in the Group Operations Wizard (Figure 13-2).

Figure 13-2. Systems Settings in Group Operations Wizard



Location Settings

Set: ☑ set location during group operation

Location:

Set Option: ☑ set location on device if driver is available

User Defined: TestLocation (set device to custom value)

Contact Settings

Set: ☑ set contact during group operation

Contact: Technical Assistance Center (RTAC),

Set Option: □ set contact on device if driver is available

User Defined: (set device to custom value)

Description Settings

Set: □ set description during group operation

Description:

Set Option: □ set description on device if driver is available

Device Roles

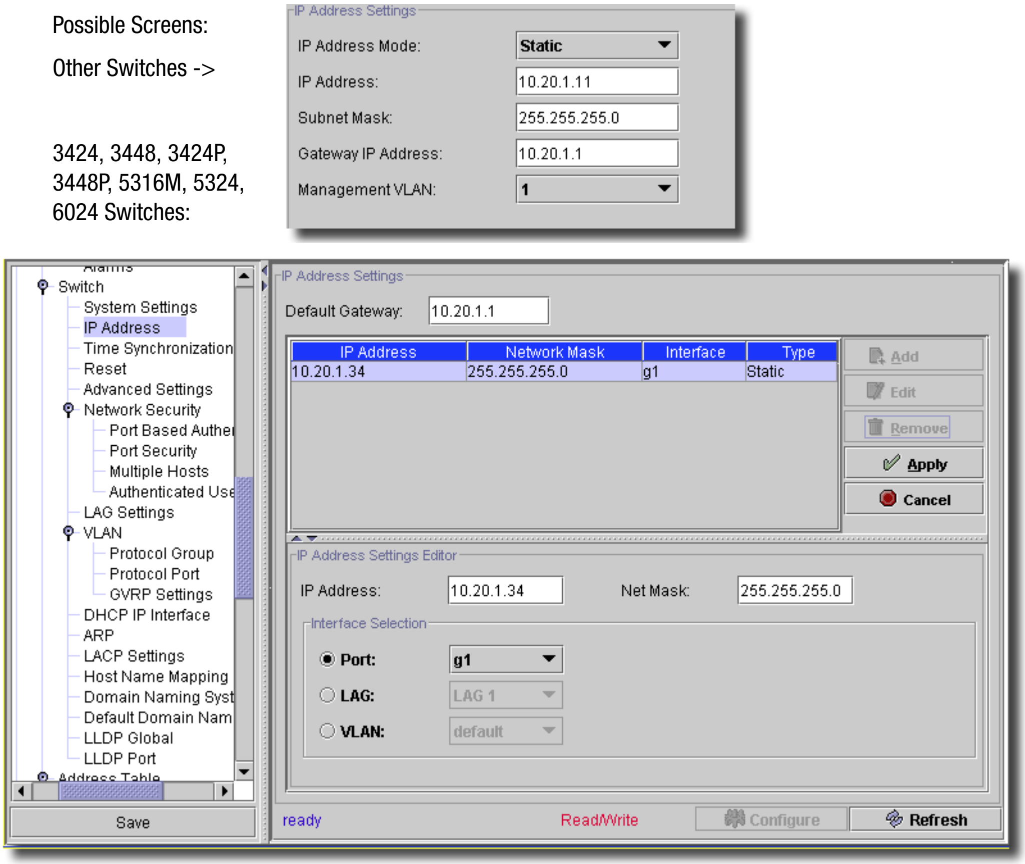
Set: □ set roles during group operation

See Group Operations Wizard on page 691 for more information.

IP Address

This screen lets you manage IP Address settings for a selected device. Not all fields described here appear in all screens—the exact appearance depends on the selected device.

Figure 13-3. IP Address Setting



Possible Screens:

Other Switches ->

IP Address Settings

IP Address Mode: Static

IP Address: 10.20.1.11

Subnet Mask: 255.255.255.0

Gateway IP Address: 10.20.1.1

Management VLAN: 1

3424, 3448, 3424P, 3448P, 5316M, 5324, 6024 Switches:

IP Address Settings

Default Gateway: 10.20.1.1

IP Address	Network Mask	Interface	Type
10.20.1.34	255.255.255.0	g1	Static

IP Address Settings Editor

IP Address: 10.20.1.34

Net Mask: 255.255.255.0

Interface Selection

● Port: g1

○ LAG: LAG 1

○ VLAN: default

ready

Read/Write

Two types of screens can appear here, depending on the equipment. One has fields to fill in (all are described below), the other has a list of IP addresses. Click *Remove* to delete listed items in that screen. The top of this latter screen lets you enter the *Default Gateway* for the selected device. Click *Add* (or *Edit* when you select an address listed) to open the editor on the lower panel. Click *Apply* to enter an address you have edited, or *Cancel* to abandon your edits. Not all fields appear for all devices. All fields are mandatory. This screen has settings for the following (described when not self-explanatory):

- **IP Address Mode**—Possible modes: *Static*, *DHCP*, *BOOTP* (does not appear in all screens). If you select *Static* mode, when it appears, it enables the following three fields (otherwise, these are not write-able):

- **IP Address**—The IP Address.

- **Net Mask / Subnet Mask**—The net or subnet mask.

- **Gateway IP Address**—The gateway's IP address.

- **Port**—Select a port from the pick list

- **LAG**—Select a LAG from the pick list.

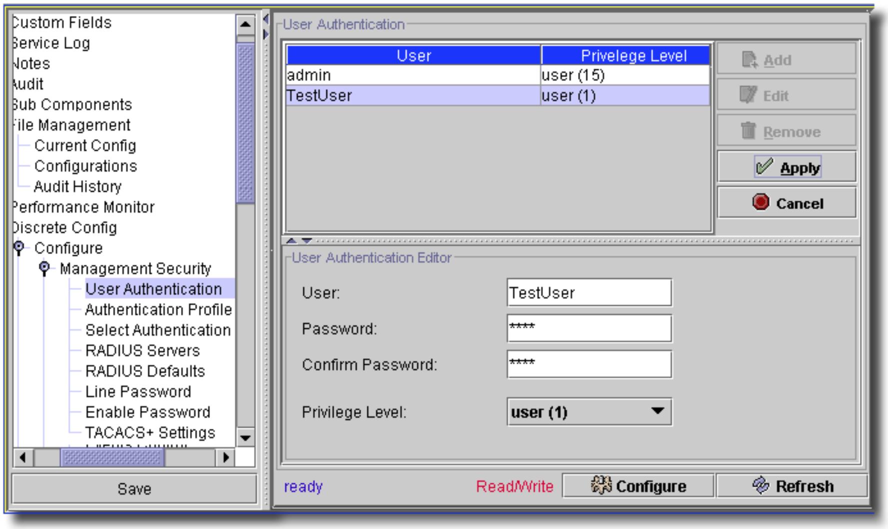
- **VLAN / Management VLAN**—Select a VLAN from the pick list.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Management Security -> User Authentication

This screen is for all supported Dell equipment. The bottom panel is blank, and the *Add*, *Edit*, *Remove* buttons do not appear grayed out when you select a line in the table. If you click Add or select a line and click Edit, the editor panel appears with editable fields for the line, described below.

Figure 13-4. User Authentication



User	Privelege Level
admin	user (15)
TestUser	user (1)

User: TestUser

Password: ****

Confirm Password: ****

Privilege Level: user (1)

The screen displays current users on the switch. When editing or adding, columns and editor fields below appear. following are fields on this screen (some may not appear for all devices):

- **User**—Encrypted text, read-only once modified.

- **Password**—Encrypted password.

- **Confirm New Password**—Encrypted password. Mandatory if password protection is enabled.
- **Privilege Level**—Select from pick list.

NOTE:

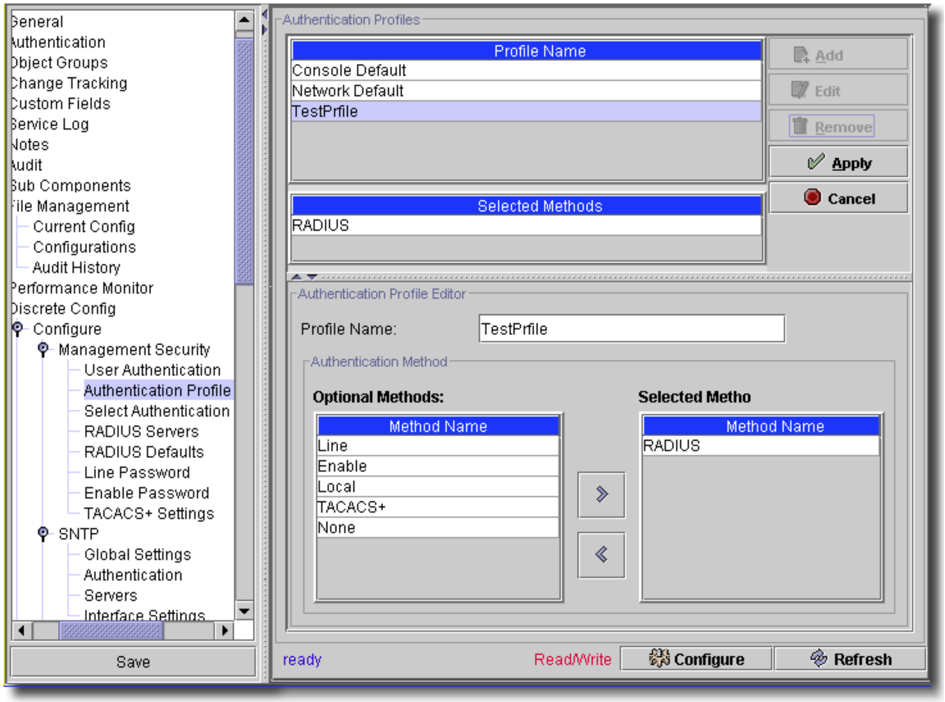
You can sort columns by clicking on them. The sorted column has an arrow in it.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Management Security Authentication Profile

This screen lets you enable/disable an http interface, and sets the port, if enabled.

Figure 13-5. Authentication Profile



Profile Name
Console Default
Network Default
TestPrfile

Selected Methods
RADIUS

Profile Name: TestPrfile

Optional Methods:

Method Name
Line
Enable
Local
TACACS+
None

Selected Metho

Method Name
RADIUS

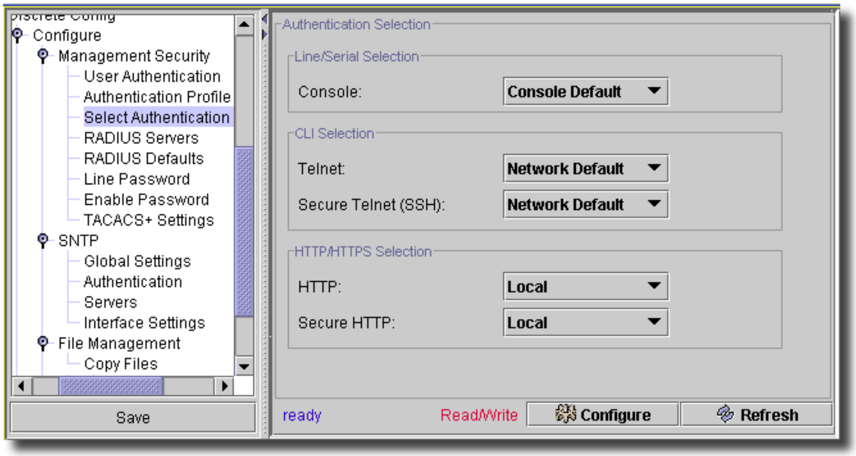
This appears only for some devices, and comes in several forms, depending on the device's capabilities. Some devices let you set authentication for HTTP, HTTPS, SSH, and an Authentication Sequence. Others let you Add and Edit profiles and their methods for the selected device that include TACACS+ and RADIUS. (see Figure 13-5). Click *Add* or *Edit* to open the editor in the bottom panel of this screen, and name and select the methods from those available. Click *Apply* to accept your edits (visible in the top panel). You can see the selected methods for an existing profile in the middle of the screen.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Management Security -> Select Authentication

This screen does not appear for all devices.

Figure 13-6. Select Authentication



Authentication Selection

Line/Serial Selection

Console: Console Default

CLI Selection

Telnet: Network Default

Secure Telnet (SSH): Network Default

HTTP/HTTPS Selection

HTTP: Local

Secure HTTP: Local

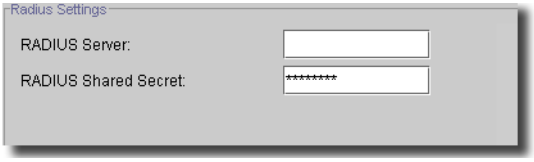
In it you can select the authentication to use with the device you are editing with the relevant pick lists.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Radius Settings

Depending on the selected equipment all or some of the following fields appear in Resource Editor.

Figure 13-7. Radius Settings

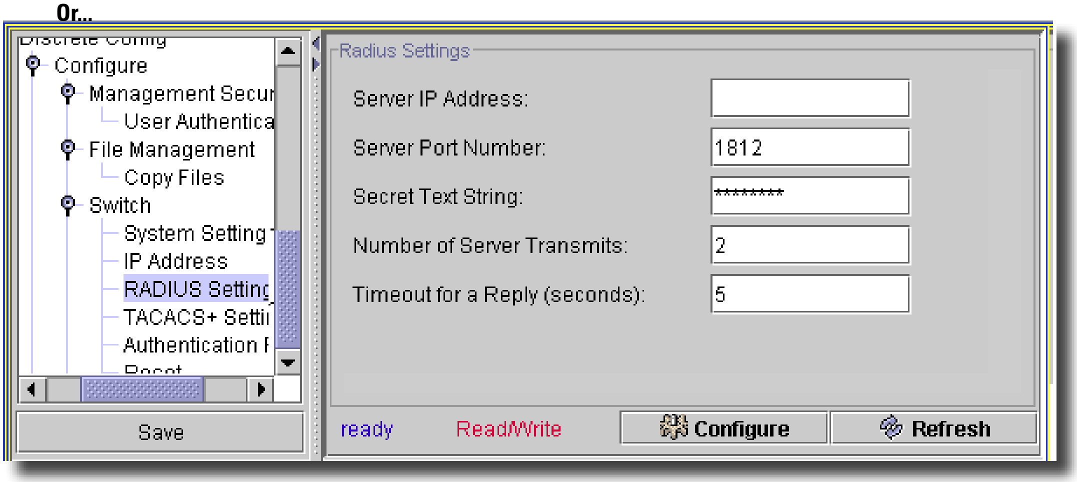


Radius Settings

RADIUS Server:

RADIUS Shared Secret: ********

Or...



Radius Settings

Server IP Address:

Server Port Number: 1812

Secret Text String: ********

Number of Server Transmits: 2

Timeout for a Reply (seconds): 5

The following are fields, described when not self-evident, on this screen. All are mandatory unless otherwise described.

- **Default Timeout for Reply**—In Seconds.

- **Default Retries**—the number of retries.

- **Default Dead Time (minutes)**—Minutes of dead time.

- **Default Shared Secret / Default Text String / Confirm**—Appears as a password, and is encrypted (1 - 128 characters).

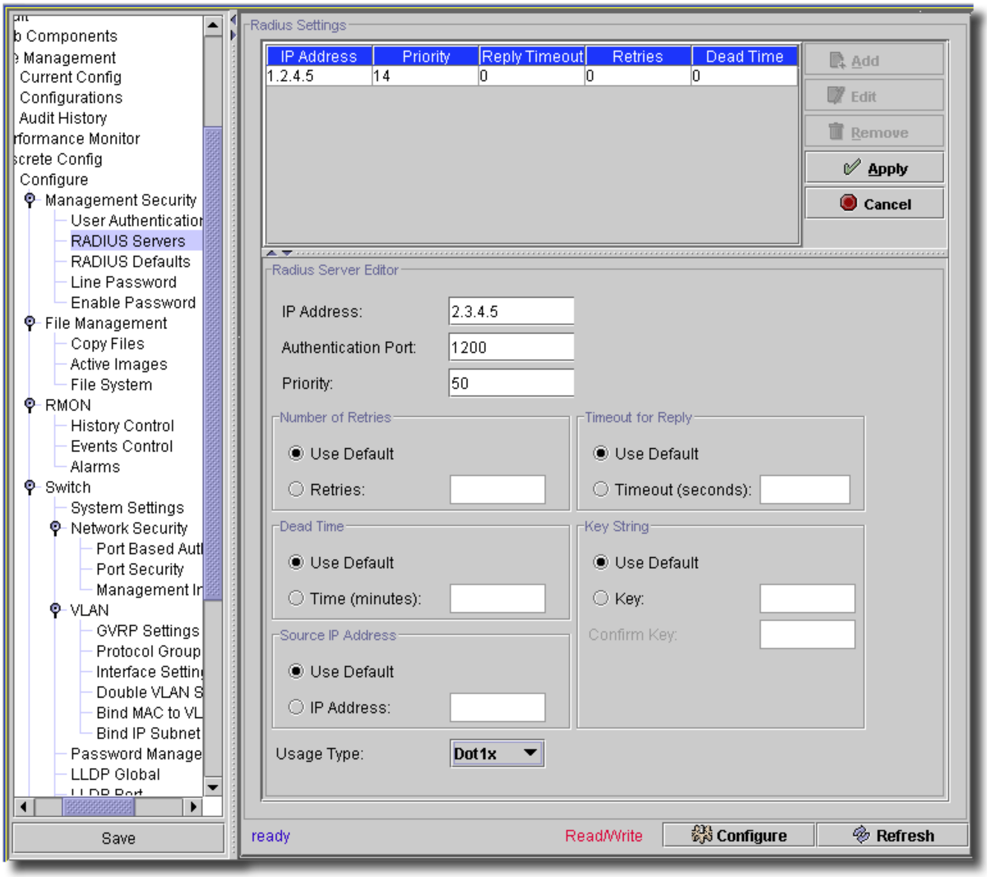
- **Default Source / Server IP Address**—Enter 0.0.0.0 for any address.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Management Security -> RADIUS Servers

This screen appears for some equipment.

Figure 13-8. RADIUS Servers



Radius Settings

IP Address	Priority	Reply Timeout	Retries	Dead Time
1.2.4.5	14	0	0	0

Radius Server Editor

IP Address: 2.3.4.5

Authentication Port: 1200

Priority: 50

Number of Retries

● Use Default

○ Retries:

Timeout for Reply

● Use Default

○ Timeout (seconds):

Dead Time

● Use Default

○ Time (minutes):

Key String

● Use Default

○ Key:

Confirm Key:

Source IP Address

● Use Default

○ IP Address:

Usage Type: Dot1x

Click *Add* (or *Edit* when you select a server listed) to open the editor on the lower panel. This screen has settings for the following (described when not self-explanatory):

Radius Server Editor

- **IP Address**—The IP address of the radius server.

- **Authentication Port**—The port where server authentication occurs.

- **Priority**—Lower numbers are higher priorities. Valid values are 0 - 65535

- **Number of Retries**—The number of times to retry authentication.

- **Timeout for Reply**—Authentication timeout for reply.

- **Dead Time** (0-2000) - Specifies the amount of time (in seconds) that a RADIUS server is bypassed for service requests. The range is 0-2000.

- **Key String**—The authentication key string, between 1 - 16 characters.

Source IP Address—Select *Use Default* or specify the source. 0.0.0.0 disables this.

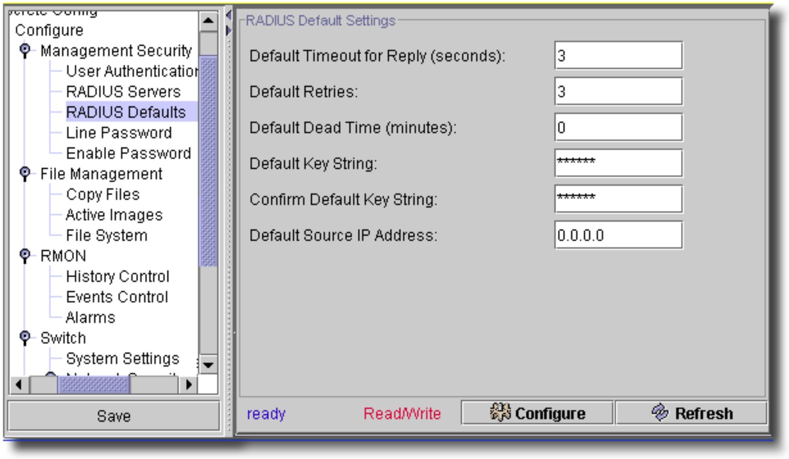
- **Usage Type**—Select from the pick list (*All*, *Login*, *Dot1x*). This field does not appear on all device's screens.

Click *Apply* to apply table entry edits, and *Configure* to implement any changes. *Cancel* abandons your table entry edits and *Refresh* re-populates the list.

Management Security -> RADIUS Defaults

This screen appears when you edit some devices.

Figure 13-9. RADIUS Defaults



Default Timeout for Reply (seconds): 3

Default Retries: 3

Default Dead Time (minutes): 0

Default Key String: ******

Confirm Default Key String: ******

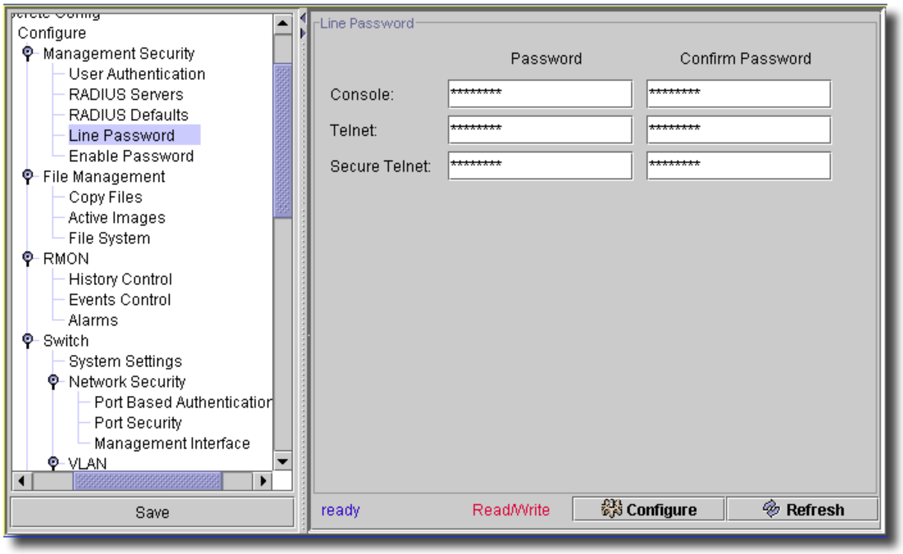
Default Source IP Address: 0.0.0.0

Enter the desired defaults, then click *Configure* to implement them. Click *Refresh* to retrieve current defaults.

Management Security -> Line Password

The Line Password screen contains fields for defining line passwords for management methods.

Figure 13-10. Line Password



Line Password

	Password	Confirm Password
Console:	*********	*********
Telnet:	*********	*********
Secure Telnet:	*********	*********

The screen includes the following fields:

- **Password for Console/Telnet/Secure Telnet** (0-159 Characters)—The line password for accessing the device in a console, Telnet, or Secure Telnet session. Passwords can contain a maximum of 159 characters.

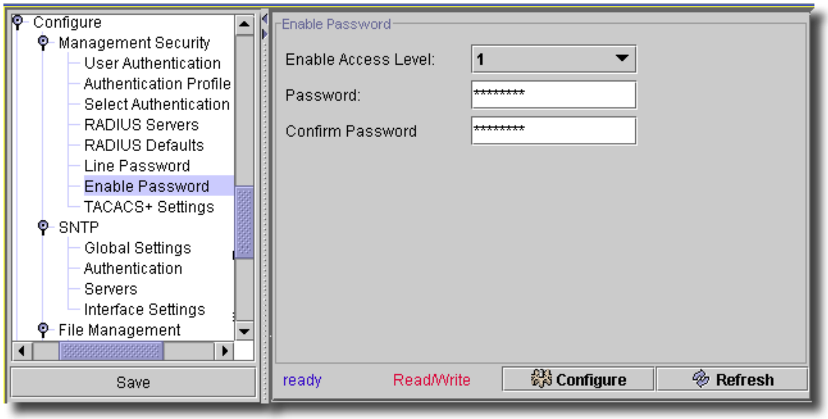
- **Confirm Password**—Confirms the new line password. The password appears as asterisks.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Management Security -> Enable Password

The Modify Enable Password screen sets a local password to control access to Normal, Privileged, and Global Configuration.

Figure 13-11. Enable Password



Enable Password

Enable Access Level: 1

Password: *********

Confirm Password *********

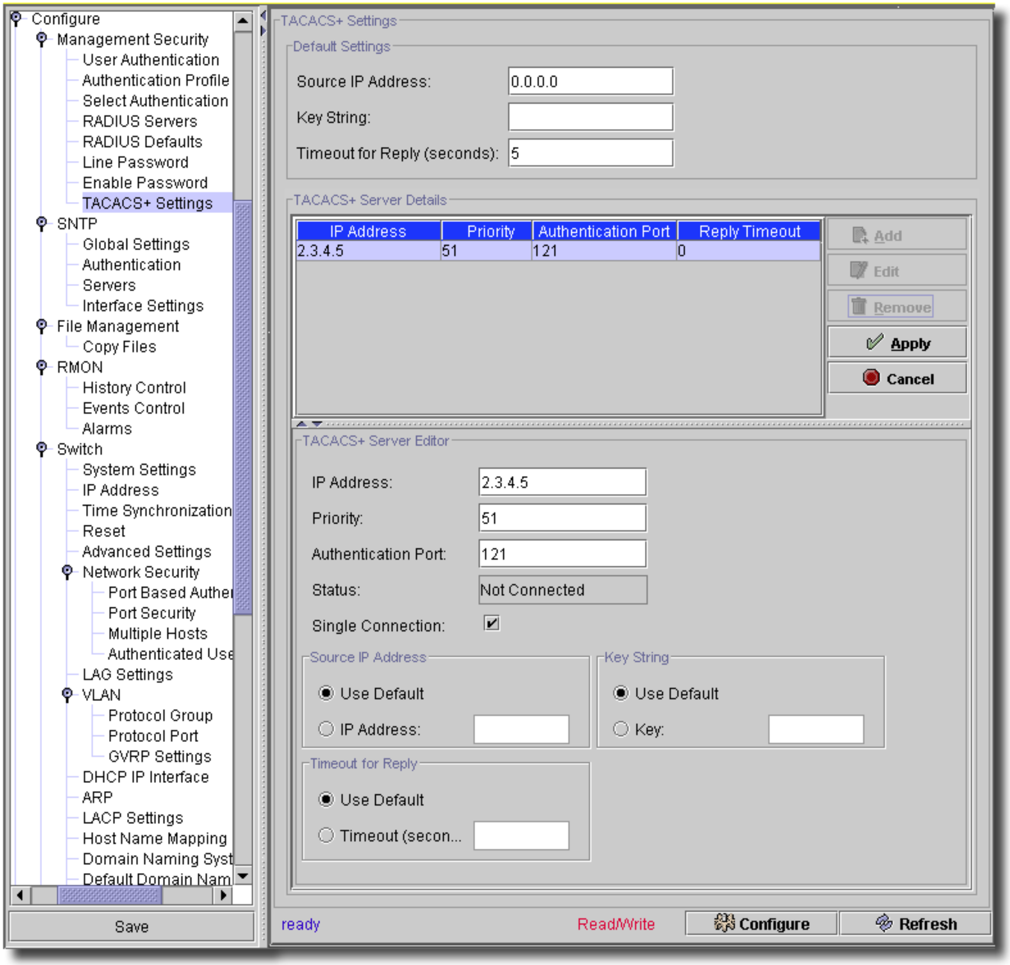
The screen includes the following fields:

- **Enable Access Level**—Access level associated with the enable password. Possible field values are 1-15. This does not appear in some screens.
- **Password** (0-159 Characters)—The currently configured enable password.
- **Confirm Password**—Confirms the new enable password. The password appears as asterisks.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

TACACS+ Settings

The following fields—or a subset of them—appear in the Editor to manage TACACS+ Settings.



Source IP Address: 0.0.0.0

Key String:

Timeout for Reply (seconds): 5

IP Address	Priority	Authentication Port	Reply Timeout
2.3.4.5	51	121	0

IP Address: 2.3.4.5

Priority: 51

Authentication Port: 121

Status: Not Connected

Single Connection: ☑

● Use Default

○ IP Address:

● Use Default

○ Key:

● Use Default

○ Timeout (secon...

Figure 13-12. TACACS+ Settings

The following are the fields on this screen. All are mandatory unless otherwise described. Not all fields appear for all devices.

Default Settings

- **Source IP Address**—The source of TACACS+ authentication.

- **Secret Text String / Key String**—The TACACS+ key. Appears as a password, and is encrypted.

- **Timeout for Reply (seconds)**—

In the middle of this screen, you can add alternative TACACS+ servers to the default specified above. Click *Add* (or *Edit* if you want to edit a selected, existing server), and the *TACACS+ Server Editor* appears in the lowest panel on this screen. Click *Delete* to remove a listed, selected server. Click *Apply* to accept your server edits, and list the server, or *Cancel* to abandon those edits.

TACACS+ Server Editor

- **IP Address**—The address of the TACACS+ server.

- **Priority**—The priority of this server

- **Authentication Port**—The port for authentication

- **Status**—A read-only indication of the server's status (for example: *not connected*).

- **Single Connection**—Check to enable single connection

For the following radio buttons, you can either accept *Use Default*, or specify your own: *Source IP, Key String*, and/or *Timeout for Reply*

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

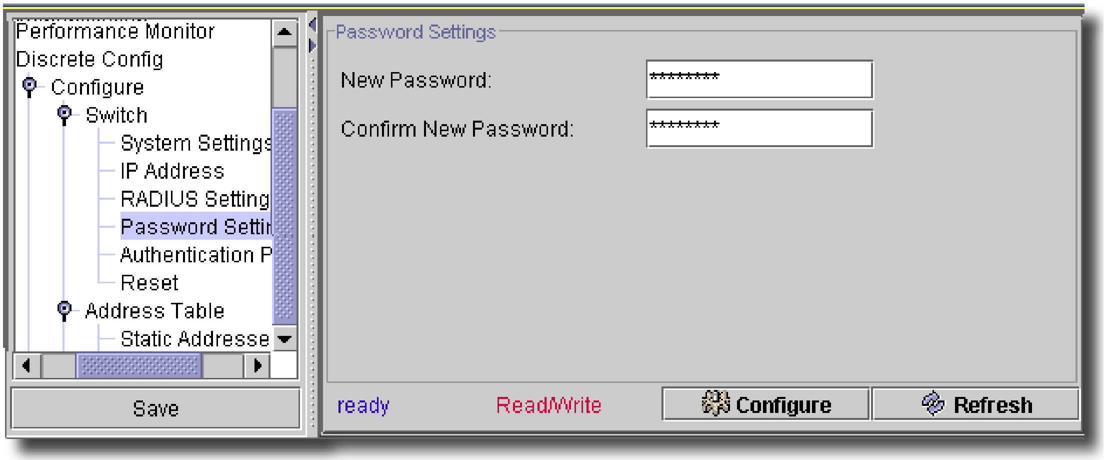
NOTE:

This screen can also appear within the Group Operation Wizard

Password Settings

This screen appears for several models (but not all) of Dell equipment.

Figure 13-13. Password Settings



New Password: *********

Confirm New Password: *********

The following are fields on this screen:

- **New Password**—Encrypted password.

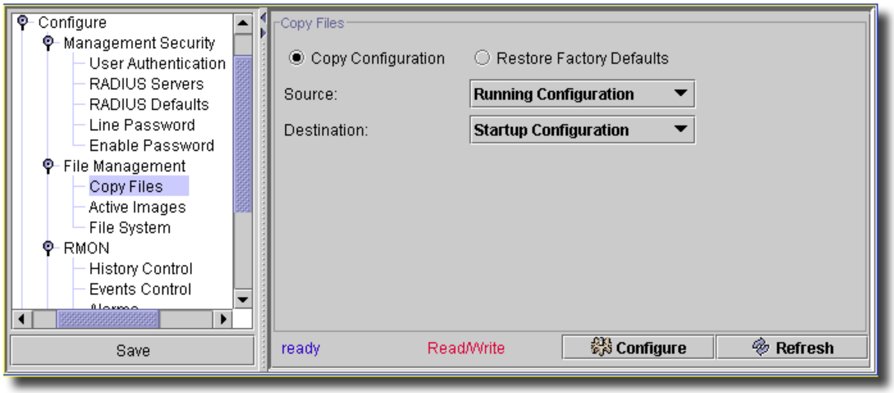
- **Confirm New Password**—Encrypted password. Mandatory if password protection is enabled.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

File Management -> Copy Files

You can copy and delete files from the Copy Files screen.

Figure 13-14. Copy Files.



Copy Files

● Copy Configuration ○ Restore Factory Defaults

Source: Running Configuration

Destination: Startup Configuration

After a configuration change user is presented with an option to copy running to startup config. The screen includes the following fields:

- **Copy Configuration**—When selected, copies either the *Running Configuration*, *Startup Configuration* or *Backup Configuration* files. Select possible values in the pick lists below (disabled if you select *Restore Configuration Factory Defaults*):

  Source—Copies either the *Running Configuration*, *Startup Configuration* or *Backup Configuration* files.

  Destination—The file to which the *Startup Configuration* or *Backup Configuration* file is copied.

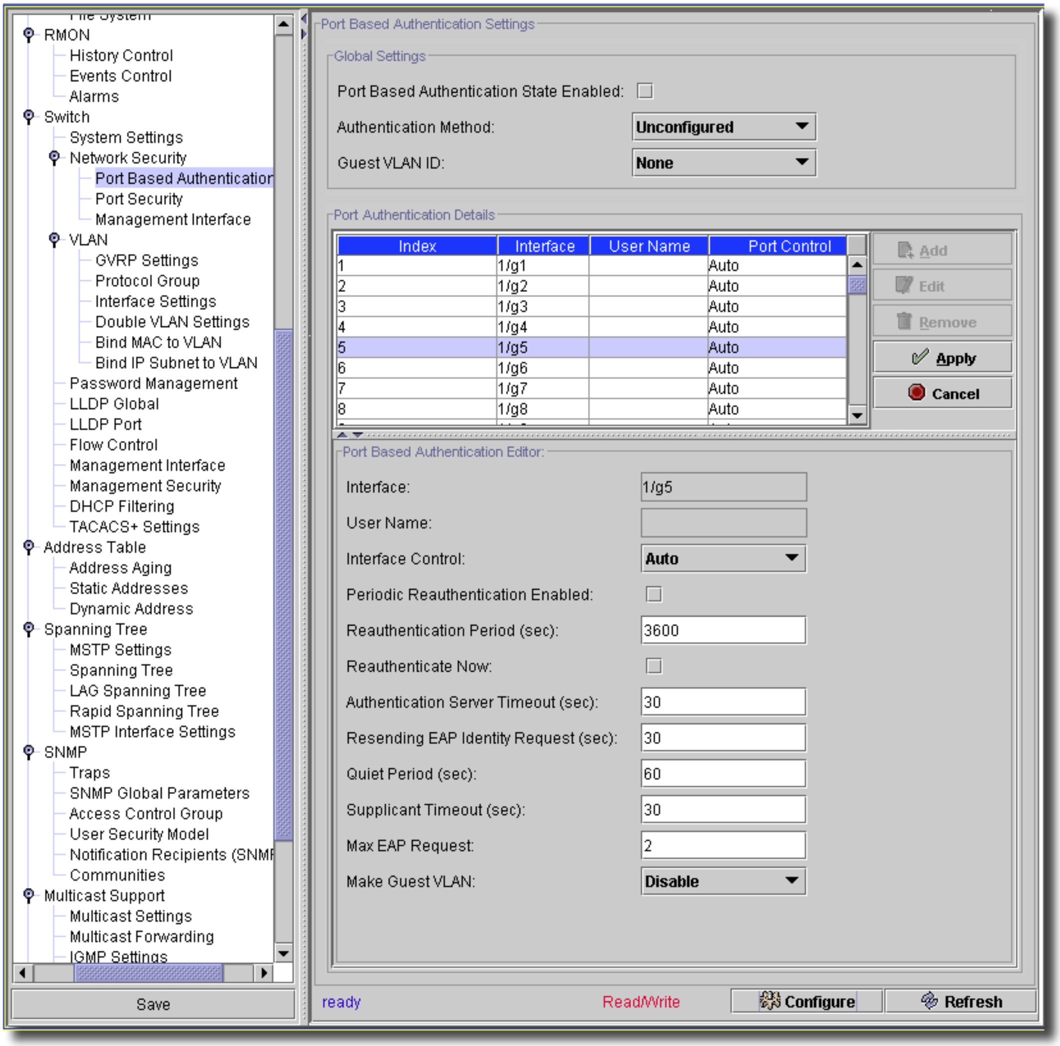
- **Restore Configuration Factory Defaults**—When selected, specifies that the factory configuration default files should be reset. When unselected, maintains the current configuration settings.
- **New File Name**—On some (34xx) switch models, this checkbox and field appears. Check to activate and then fill in the new file name.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Port Based Authentication

The Port Based Authentication screen for the 53xx switches contains fields for configuring port-based authentication.

Figure 13-15.   Port Based Authentication



Port Based Authentication Settings

Global Settings

Port Based Authentication State Enabled: □

Authentication Method: Unconfigured

Guest VLAN ID: None

Port Authentication Details

Index	Interface	User Name	Port Control
1	1/g1		Auto
2	1/g2		Auto
3	1/g3		Auto
4	1/g4		Auto
5	1/g5		Auto
6	1/g6		Auto
7	1/g7		Auto
8	1/g8		Auto

Port Based Authentication Editor:

Interface: 1/g5

User Name:

Interface Control: Auto

Periodic Reauthentication Enabled: □

Reauthentication Period (sec): 3600

Reauthenticate Now: □

Authentication Server Timeout (sec): 30

Resending EAP Identity Request (sec): 30

Quiet Period (sec): 60

Supplicant Timeout (sec): 30

Max EAP Request: 2

Make Guest VLAN: Disable

ready   Read/Write

You can *Edit* listed settings for the selected device in this screen (*Add* and *Remove* are disabled). Select an existing port authentication configuration listed in the upper portion of the screen and click *Edit*; the editor opens. This screen contains the following fields:

- **Port Based Authentication State Enabled**— When checked, enables port based authentication on the device.

- **Authentication Method**—The Authentication method used. The pick list values include:

None—No authentication method is used to authenticate the port.

RADIUS—The RADIUS servers does port authentication.

RADIUS, None—The RADIUS server first does port authentication. If the port is not authenticated, then no authentication method is used, and the session is permitted.

Click *Remove* to delete a selected, listed item. You can *Add*, *Edit* or *Remove* port authentications for the selected device in this screen. When you click *Add* (or select an existing authentication listed in the *Port Authentication Details* portion of the screen and click *Edit*) the *Port Based Authentication Editor* opens (the lower portion of the screen) with the following fields:

- **Interface**—Contains an interface list.

User Name—The user name as configured in the RADIUS server.

- **Interface Control**—Defines the port authorization state. The possible field values include:

Authorized—Set the interface state to authorized (permit traffic).

Unauthorized—Set the interface state to unauthorized (deny traffic).

Auto—Authorize state is set by the authorization method.

- **MAB**—MAC authentication bypass. Check to enable.

- **Periodic Reauthentication Enabled**—Reauthenticates the selected port periodically, when enabled. The reauthentication period is defined in the *Reauthentication Period (300-4294967295)* field.

- **Reauthentication Period** (300-4294967295)—Indicate the period for the selected port to be reauthenticated. The field value is in seconds. The field default is 3600 seconds.

- **Reauthenticate Now**—Permits immediate port reauthentication, when selected.

- **Authentication Server Timeout** (1-65535)—Defines the period that lapses before the device resends a request to the authentication server. The field value is in seconds. The field default is 30 seconds.

- **Resending EAP Identity Request** (1-65535)—Defines the period that lapses before EAP request are resent. The field default is 30 seconds.

Quiet Period (0-65535)—The number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.

- **Supplicant Timeout** (1-65535)—The amount of time that lapses before EAP requests are resent to the user. The field value is in seconds. The field default is 30 seconds.

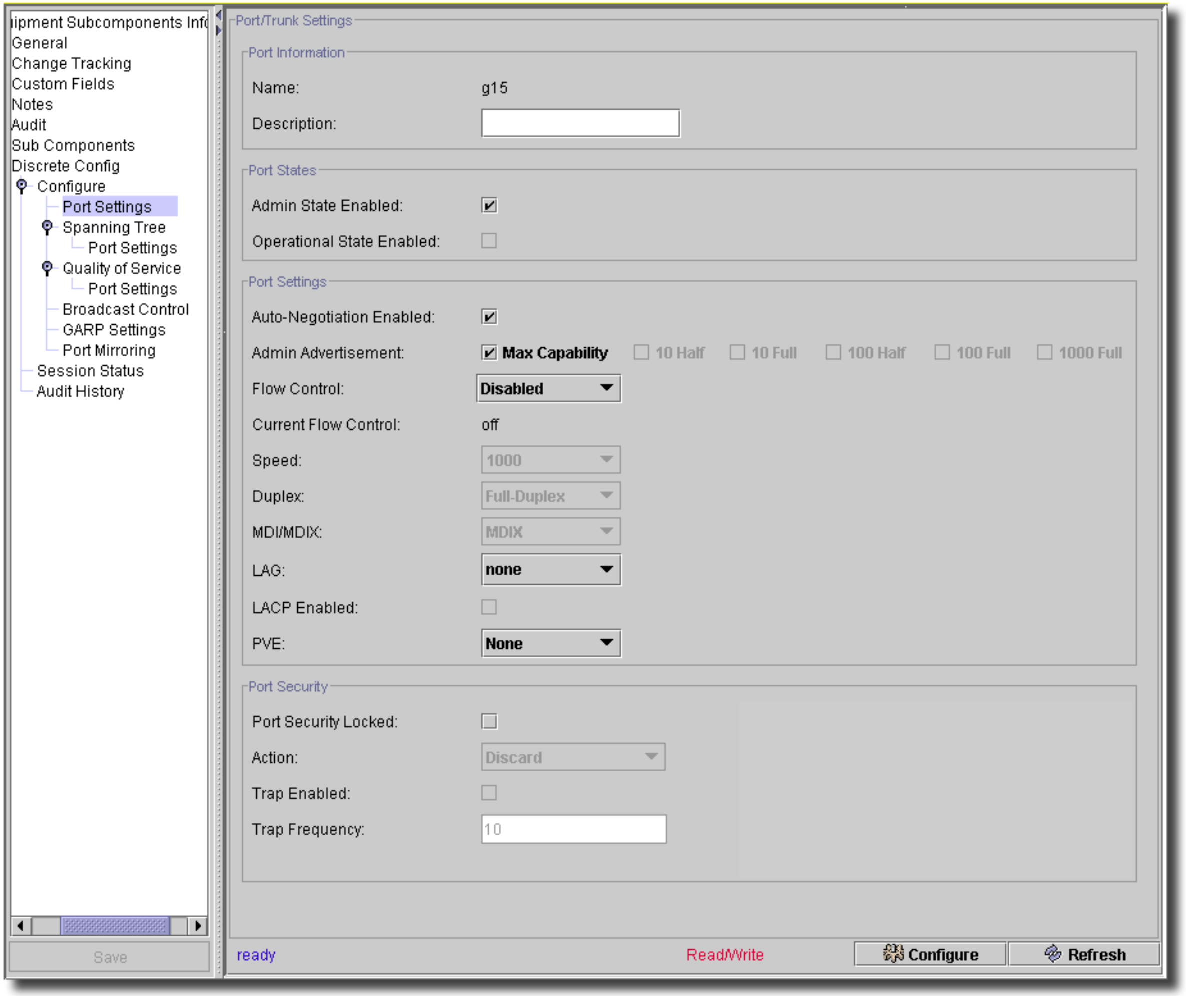
- **Max EAP Requests** (1-10)—The total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries

- **Make Guest VLAN**—Select *Enable* or *Disable*.

Port and Trunk Settings

Instead of duplicating most of the attributes below on another panel, you can place the port in or out of a trunk in one operation.

Figure 13-16. Port and Trunk Settings



Port/Trunk Settings

Port Information

Name: g15

Description:

Port States

Admin State Enabled: ☑

Operational State Enabled: □

Port Settings

Auto-Negotiation Enabled: ☑

Admin Advertisement: ☑ Max Capability □ 10 Half □ 10 Full □ 100 Half □ 100 Full □ 1000 Full

Flow Control: Disabled

Current Flow Control: off

Speed: 1000

Duplex: Full-Duplex

MDI/MDIX: MDIX

LAG: none

LACP Enabled: □

PVE: None

Port Security

Port Security Locked: □

Action: Discard

Trap Enabled: □

Trap Frequency: 10

ready Read/Write

This screen lets 60xx switches (firmware v2.0 and above) implement private edge VLANs.

When you open selected Dell equipment from Resource Manager, right-click a port in the *Reference Tree* details panel and select *Open*. Then click on the Port Settings node. You can then add a port to trunk group. You must disable *Auto-Negotiation* to add port to the Trunk Members.

The following are fields on this screen (not all appear with all devices). Text fields are mandatory unless described otherwise.

Port Information

- **Name—**Read-only description of the selected device.

- **Description**—Optional text describing this setting.

Port States

- **Admin State Enabled**—Checkbox. Enables or disables traffic forwarding through the port.

- **Operational State Enabled**—Checkbox. When the port is operationally active it is receiving and transmitting traffic.

Port Settings

- **Auto-Negotiation Enabled**—Checkbox. See other fields for impacts from selecting this. You must disable *Auto-Negotiation* to add a port to the Trunk Members. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.

- **Admin Advertisement—**Visible only if this is available on the selected device and port. Defines the auto-negotiation setting the device advertises. You can select *Max Capability*, *10 Half*, *10 Full*, *100 Half*, *100 Full*, or *1000* with the checkboxes on this line. For example, 10 Half indicates that the device advertises for a 10 mbps speed LAG and half duplex mode setting.

- **Flow Control**—Select from pick list. Enabled only if you disable Auto-Negotiation, for some switches.

- **Current Flow Control**—Read only. Possible values: *None*, *Back-Pressure*. Enables or disables flow control or enables the auto negotiation of flow control on the port.

- **Speed**—Select a speed from the pick list alternatives. Enabled only if you disable Auto-Negotiation.

- **Duplex**—Select the type of duplexing from the pick list. Enabled only if you disable *Auto-Negotiation*.

- **MDI/MDIX—**Select from the pick list. This lets the device decipher between crossed and uncrossed cables. Hubs and switches are deliberately wired differently from end stations so that when a hub or switch is connected to an end station, the network can go straight through Ethernet cable, and the pairs match. When you connect two hubs/switches to each other, or two end stations to each other, a crossover cable ensures that the correct pairs are connected. Auto MDIX does not operate on FE ports if auto negotiation is disabled. The possible field values are:

  Auto–Automatically detects the cable type.

  MDIX–For hubs and switches.

  MDI–For end stations.

- **Trunk / LAG** —Field title depends on switch. Select from pick list. This is a list of possible trunks.

- **LACP Enabled**—Check to enable LACP.

- **PVE**—Appears only if enabled on the selected device and port.This is for 60xx devices, with firmware v2.0 and above. Select from pick list. This enables a port as a Private VLAN Edge (PVE) port. When a port is defined as PVE, it bypasses the Forwarding Database (FDB), and forwards all Unicast, Multicast and Broadcast traffic to an uplink (except MAC-to-me packets). Uplinks can be a port or LAG. Traffic from the uplink is distributed to all interfaces.

Port Security

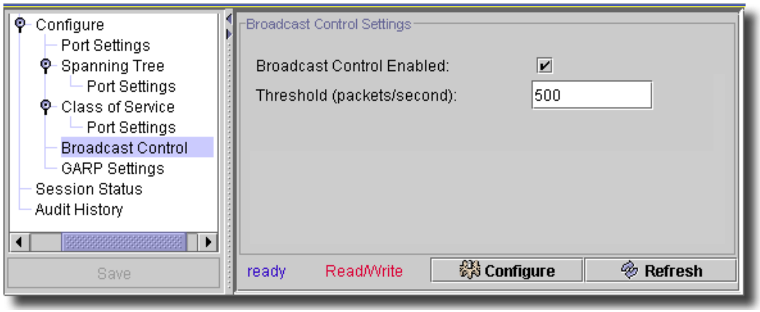
- **Port Security Locked / Enabled**—Checkbox. Not on all device screens.
- **Intrusion Shutdown and Trap Shutdown**—Select from the pick list. Value Values: *none, trap, shutdown, trap and shutdown*. Not on all device screens.
- **Dynamic Address Learning**—Select from *Enabled / Disabled*. A tooltip reminds you that this setting applies to all ports. Not on all device screens.
- **Action**—Select from pick list. For example: *Discard*. Not on all device screens.
- **Trap Enabled**—Check to enable security traps. Not on all device screens.
- **Trap Frequency**—Enter a number of seconds between security traps. Not on all device screens.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Broadcast Control

If you enable broadcast control, the application validates ranges, depending on the device being configured.

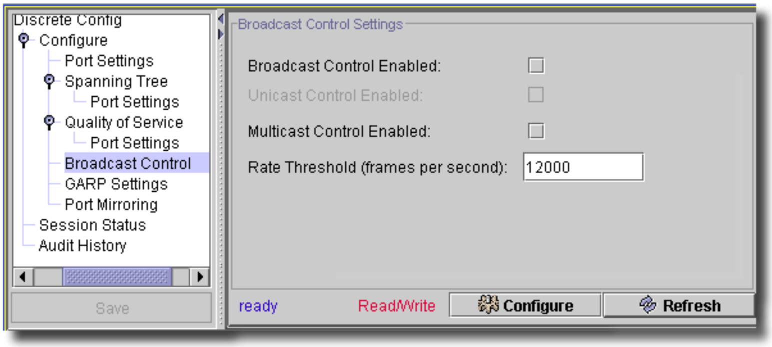
Figure 13-17. Broadcast Control



Broadcast Control Settings

Broadcast Control Enabled: ☑

Threshold (packets/second): 500



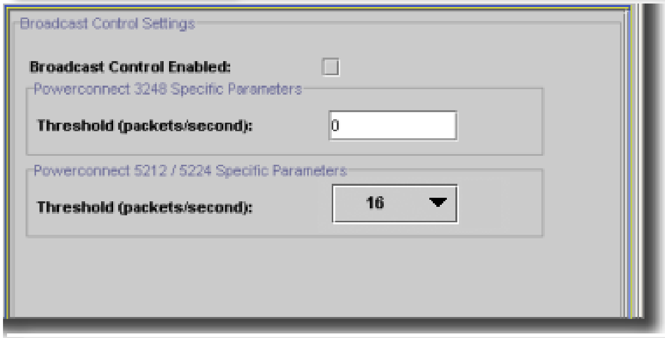
Broadcast Control Settings

Broadcast Control Enabled: □

Unicast Control Enabled: □

Multicast Control Enabled: □

Rate Threshold (frames per second): 12000



Broadcast Control Settings

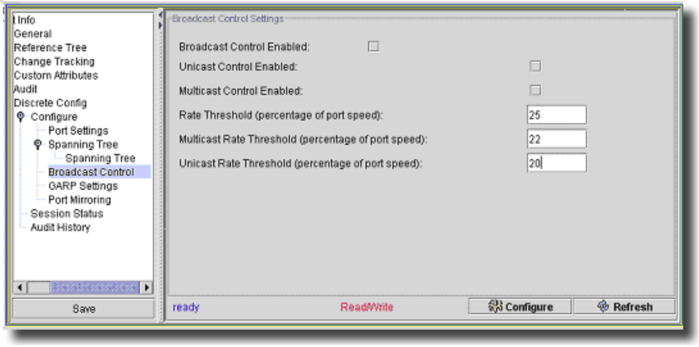
Broadcast Control Enabled: □

Powerconnect 3248 Specific Parameters

Threshold (packets/second): 0

Powerconnect 5212 / 5224 Specific Parameters

Threshold (packets/second): 16



Broadcast Control Settings

Broadcast Control Enabled: □

Unicast Control Enabled: □

Multicast Control Enabled: □

Rate Threshold (percentage of port speed): 25

Multicast Rate Threshold (percentage of port speed): 22

Unicast Rate Threshold (percentage of port speed): 20

The following are checkboxes that can appear on this screen:

- **Broadcast Control Enabled**

- **Unicast Control Enabled**

- **Multicast Control Enabled**

- **Rate Threshold (frames/second)**—Select from options available on the pick list, or type a figure in the text field (the tooltip specifies a valid range), depending on the device. If more than one of these fields appears in the screen, a label describes the device for which the threshold applies. This field has unique ranges per families of equipment.

- **Multicast Rate Threshold (frames/second)**—When this field appears, as for the *Rate Threshold*, enter a mulitcast rate threshold as a percentage of port speed.

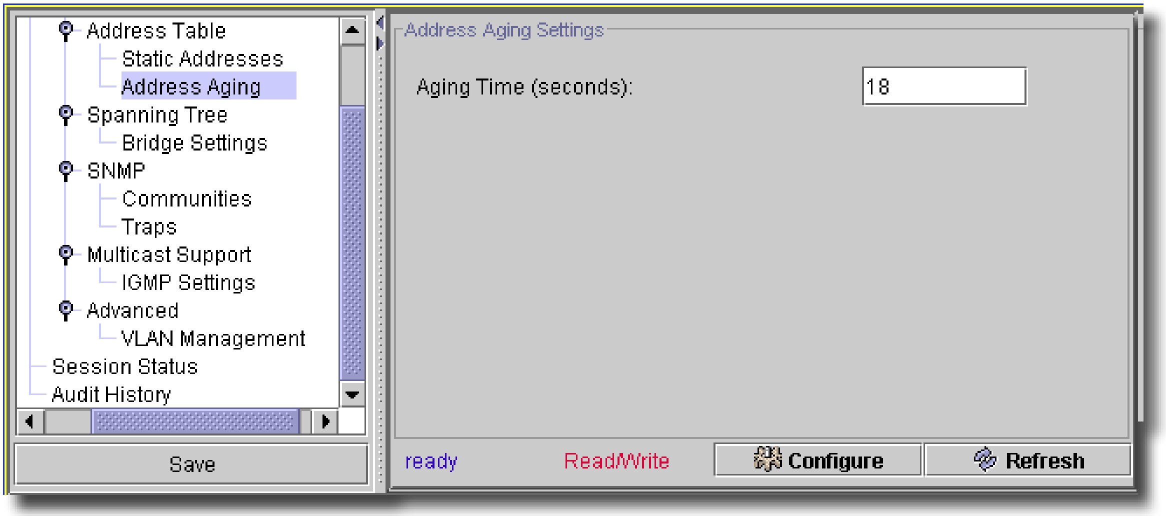
- **Unicast Rate Threshold (frames/second)**—When this field appears, as for the *Rate Threshold*, enter a unicast rate threshold as a percentage of port speed.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Address Table -> Address Aging

This screen lets you manage IP Address aging.

Figure 13-18. Address Aging

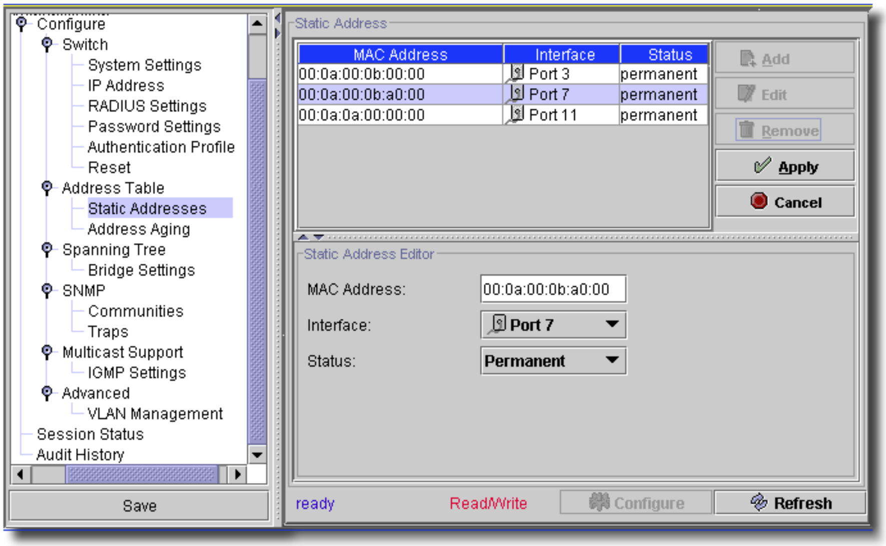


Aging Time (seconds): 18

This screen lets you edit the *Aging Time (seconds)* field. The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Address Table -> Static Addresses

This screen appears for some devices.



MAC Address	Interface	Status
00:0a:00:0b:00:00	Port 3	permanent
00:0a:00:0b:a0:00	Port 7	permanent
00:0a:0a:00:00:00	Port 11	permanent

MAC Address: 00:0a:00:0b:a0:00

Interface: Port 7

Status: Permanent

Figure 13-19. Static Addresses

Add Edit, or *Remove* static addresses (*VLAN ID*, *MAC Address*, *Interface*, and *Status)* on a device with the buttons at the bottom of the listed addresses on the left. Click *Apply* to enter your edits (*Cancel* to abandon them). The Static Address Editor has the following fields:

- **VLAN ID**—Select an ID from the pick list. (Does not appear for all devices.)

- **MAC Address**—Enter a MAC address in the format xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx.

- **Interface**—Select from the pick list.

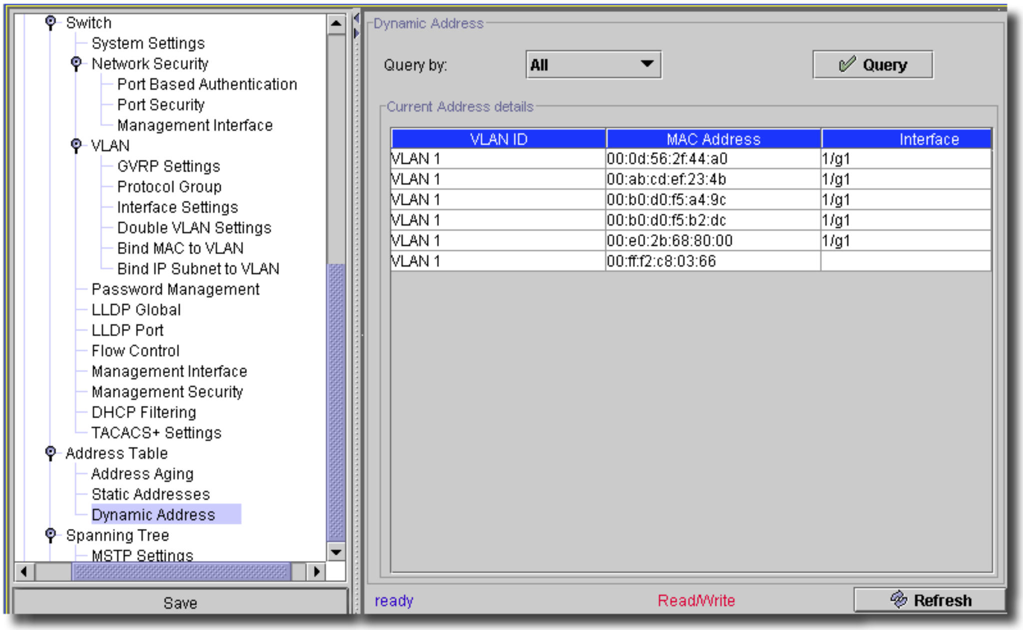
- **Status**—Select from *Secure*, *Permanent*, *Delete on Resent*, *Delete on Time Out*

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Address Table -> Dynamic Address

The Dynamic Address Table contains specific dynamic MAC Address information, including the VLAN ID, ports associated with the MAC address, and the MAC address. It does not appear on all switches.

Figure 13-20. Dynamic Address Table



Query by: All

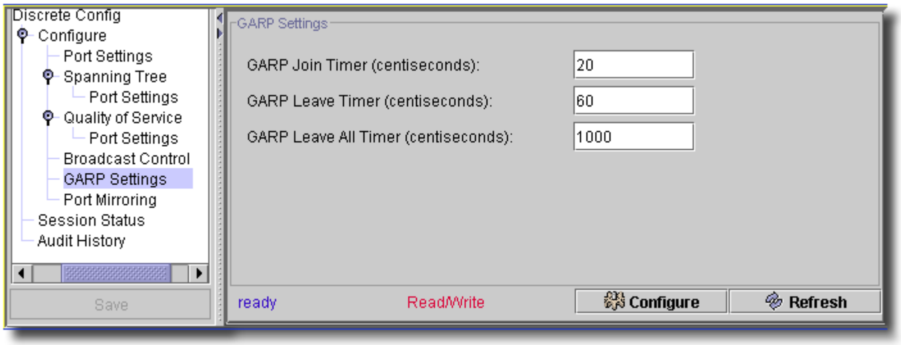
VLAN ID	MAC Address	Interface
VLAN 1	00:0d:56:2f:44:a0	1/g1
VLAN 1	00:ab:cd:ef:23:4b	1/g1
VLAN 1	00:b0:d0:f5:a4:9c	1/g1
VLAN 1	00:b0:d0:f5:b2:dc	1/g1
VLAN 1	00:e0:2b:68:80:00	1/g1
VLAN 1	00:ff:f2:c8:03:66	

Select query parameters with the pick lists at the top of this screen, then click *Query* (or *Refresh)* to renew the device information on this screen.

GARP Settings

When equipment permits GARP settings, a screen with the following is available when you open a port to edit (right-click on a port in the *Reference Tree* details panel and select *Open*).

Figure 13-21. GARP Settings



GARP Join Timer (centiseconds): 20

GARP Leave Timer (centiseconds): 60

GARP Leave All Timer (centiseconds): 1000

The following are fields on this screen. All are mandatory. Values are in centiseconds (hundredths of a second), and are valid for ranges that vary according to device. A typical range would be between 2-2147483647 (except models 6224, 6248, see the tooltip on these fields for the accurate range).

- **GARP Join Timer**—Range: 10 - 100

- **GARP Leave Timer**—Range: 30 - 600 (must be at least three times the *Join Timer* figure.

- **GARP Leave All Timer**—Range: 200 - 6000 (must be greater than the *Leave Timer*).

NOTE:

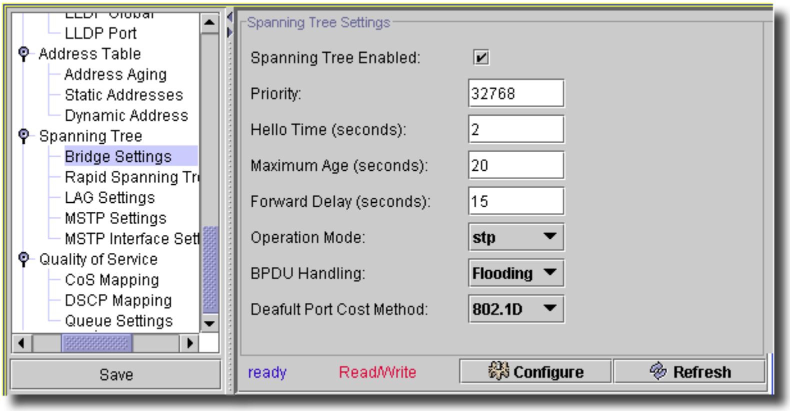
This screen can also appear within the Group Operation Wizard. See Group Operations Wizard on page 691.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Spanning Tree -> Bridge Settings

This screen lets you manage Spanning Tree Bridge Settings.

Figure 13-22. Spanning Tree–Bridge Settings



Spanning Tree Settings

Spanning Tree Enabled: ☑

Priority: 32768

Hello Time (seconds): 2

Maximum Age (seconds): 20

Forward Delay (seconds): 15

Operation Mode: stp

BPDU Handling: Flooding

Deafult Port Cost Method: 802.1D

The following are fields on this screen. They are all mandatory:

- **Spanning Tree Enabled**—Check to enable
- **Priority**—Valid Values: 0-65535.
- **Hello Time (seconds)**—Valid Values: 1-10
- **Maximum Age (seconds)**—Valid Values: 6-40
- **Forward Delay (seconds)** —Valid Values: 4-30
- **Operation Mode**—Select from the values on the pick list (does not appear on all screens).
- **BPDU Handling**—For bridge protocol data unit handling, select from the values on the pick list. Options include *Filtering*, and *Flooding*.
- **Default Port Cost Method**—Select from the values on the pick list (does not appear on all screens).

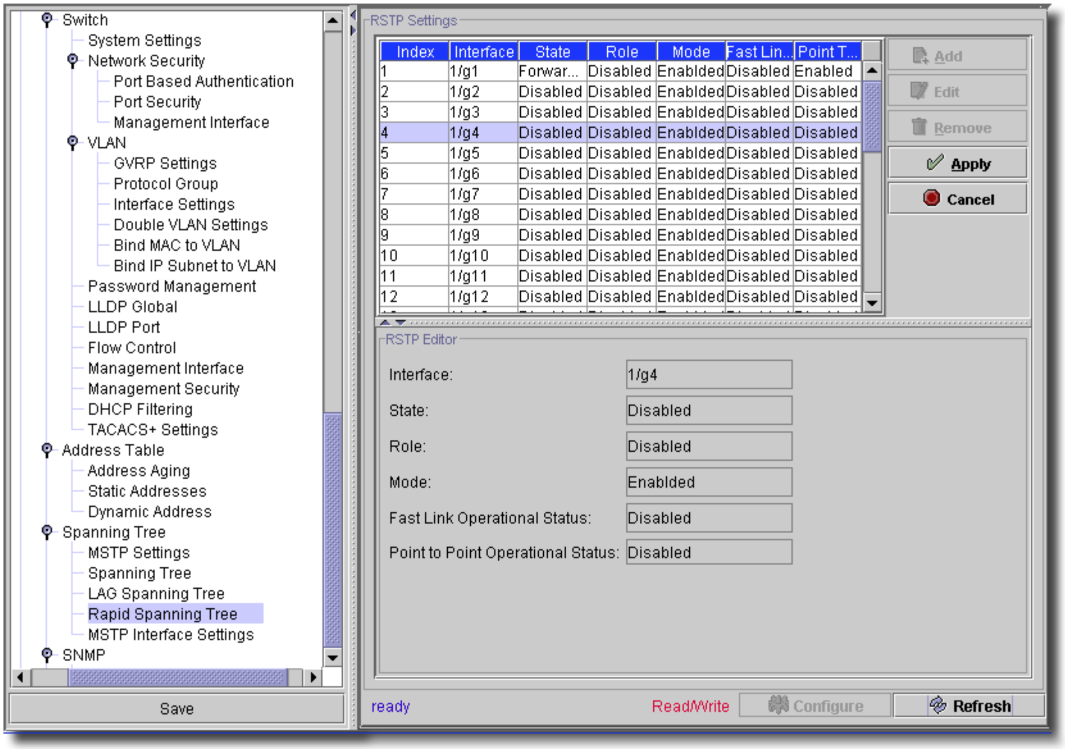
The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Spanning Tree -> Rapid Spanning Tree

While Classic Spanning Tree guarantees preventing L2 forwarding loops in a general network topology, convergence can take up to 30-60 seconds. The convergence time is considered too long for many applications. Faster convergence can often be obtained by using the Rapid Spanning Tree Protocol (RSTP).

RSTP has the following different port states: Disabled, Learning, Discarding, and Forwarding. You can enable Rapid Spanning Tree is enabled on the STP Global Settings page.

Figure 13-23. Rapid Spanning Tree



Index	Interface	State	Role	Mode	Fast Lin...	Point T...
1	1/g1	Forwar...	Disabled	Enablded	Disabled	Enabled
2	1/g2	Disabled	Disabled	Enablded	Disabled	Disabled
3	1/g3	Disabled	Disabled	Enablded	Disabled	Disabled
4	1/g4	Disabled	Disabled	Enablded	Disabled	Disabled
5	1/g5	Disabled	Disabled	Enablded	Disabled	Disabled
6	1/g6	Disabled	Disabled	Enablded	Disabled	Disabled
7	1/g7	Disabled	Disabled	Enablded	Disabled	Disabled
8	1/g8	Disabled	Disabled	Enablded	Disabled	Disabled
9	1/g9	Disabled	Disabled	Enablded	Disabled	Disabled
10	1/g10	Disabled	Disabled	Enablded	Disabled	Disabled
11	1/g11	Disabled	Disabled	Enablded	Disabled	Disabled
12	1/g12	Disabled	Disabled	Enablded	Disabled	Disabled

Interface: 1/g4

State: Disabled

Role: Disabled

Mode: Enablded

Fast Link Operational Status: Disabled

Point to Point Operational Status: Disabled

You can *Add*, *Edit* or *Remove* RSTP settings for the selected device in this screen (although some devices restrict actions to viewing the settings when you click *Edit*). Click *Remove* to delete a selected, listed item. When you click *Add* (or select an existing interface listed in the *RSTP Settings* portion of the screen and click *Edit*) the *RSTP Editor* opens (the lower portion of the screen) with the following fields:

- **Interface**—Port or LAG on which Rapid STP is enabled.

- **State**—*Enabled* or *Disabled*. (Does not appear for all devices)

- **Role**—The port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:

  Root—Provides the lowest cost path to forward packets to root device.

  Designated—The port or LAG via which the designated device is attached to the LAN.

  Alternate—Provides an alternate path to the root device from the root interface.

  Backup—Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

  Disabled—The port is not participating in the Spanning Tree (the port’s link is down).

- **Fast Link Operational Status**—Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
- **Point-to-Point Admin Status**—*Auto/Enable/Disable* establishing a point-to-point link, or specifies that the device to *auto*matically establish a point-to-point link.

  To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and the LCP negotiates any optional facilities, the originating PPP sends Network Control Protocol (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can go over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs.
- **Point-to-Point Operational Status**—The Point-to-Point operating state. This is the actual device port link type.
- **Activate Protocol Migrational Test**—When selected, enables PPP sending Link Control Protocol (LCP) packets to configure and test the data link. It may differ from the administrative state.

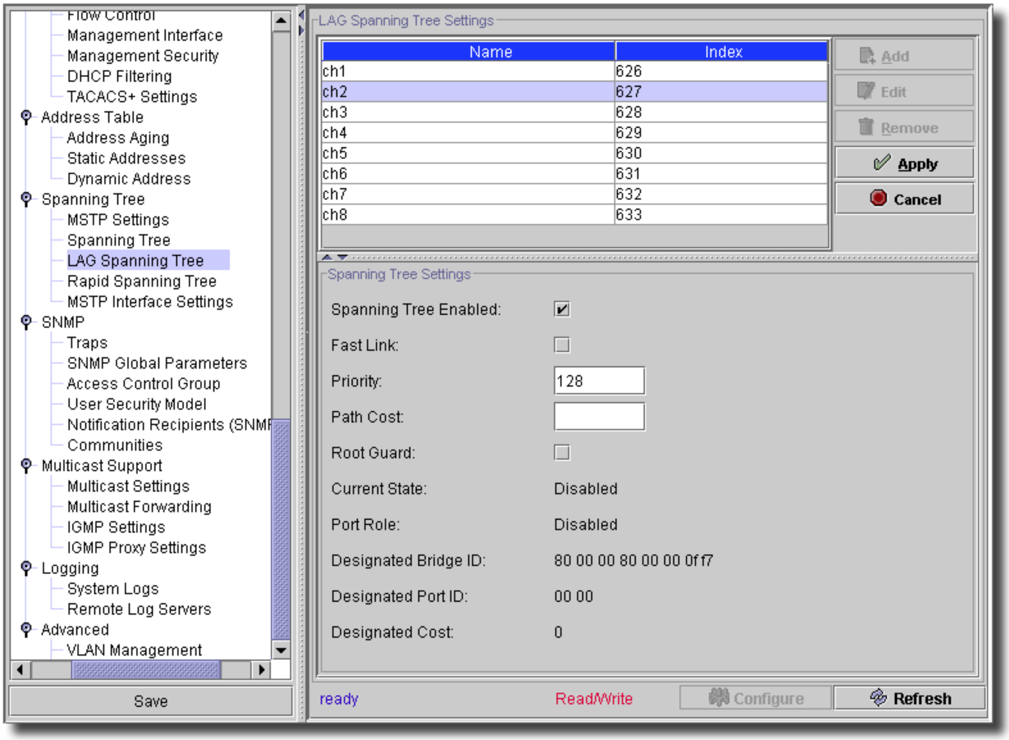
Click A*pply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Spanning Tree -> LAG Settings

The Spanning Tree LAG Settings screens contains fields for assigning Spanning Tree Protocol (STP) aggregating port parameters.

Figure 13-24. Spanning Tree -> LAG Spanning Settings



Name	Index
ch1	626
ch2	627
ch3	628
ch4	629
ch5	630
ch6	631
ch7	632
ch8	633

Spanning Tree Enabled: ☑

Fast Link: □

Priority: 128

Path Cost:

Root Guard: □

Current State: Disabled

Port Role: Disabled

Designated Bridge ID: 80 00 00 80 00 00 0f f7

Designated Port ID: 00 00

Designated Cost: 0

You can *Add*, *Edit* or *Remove* LAG Spanning Tree settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you click *Add* (or select an existing interface listed in the *LAG Spanning Tree Settings* portion of the screen and click *Edit*) the *LAG Spanning Tree Editor* opens (the lower portion of the screen) with the following fields:

Spanning Tree Enabled—Enables or disables STP on the LAG.

- **Fast Link**—Enables Fast Link mode for the LAG. If Fast Link mode is enabled for a LAG, it is automatically put in the Forwarding state when the LAG is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.

- **Priority**—Priority value of the LAG. The priority value influences the LAG choice when a bridge has two looped ports. The priority value is between 0-240, in increments of 16.

- **Path Cost** (1-200000000)—The LAG’s contribution to the root path cost. The path cost is adjusted to a higher or lower value, and forwards traffic when a path is rerouted. The path cost has a value of 1 to 200000000. If the path cost method is short, the LAG cost default value is 4. If the path cost method is long, the LAG cost default value is 20000.
- **Root Guard**—Check to enable.
- **Current State**—Current (read-only) STP state of a LAG. If enabled, the LAG state determines what forwarding action occurs with traffic. If the bridge discovers a malfunctioning LAG, the LAG is placed in the *Broken* state. Possible LAG states are:

Disabled—The LAG link is currently down.

Blocking—The LAG is blocked and cannot forward traffic or learn MAC addresses.

Listening—The LAG is in the listening mode and cannot forward traffic or learn MAC addresses.

Learning—The LAG is in the learning mode and cannot forward traffic, but it can learn new MAC addresses.

Forwarding—The LAG is currently in the forwarding mode, and it can forward traffic and learn new MAC addresses.

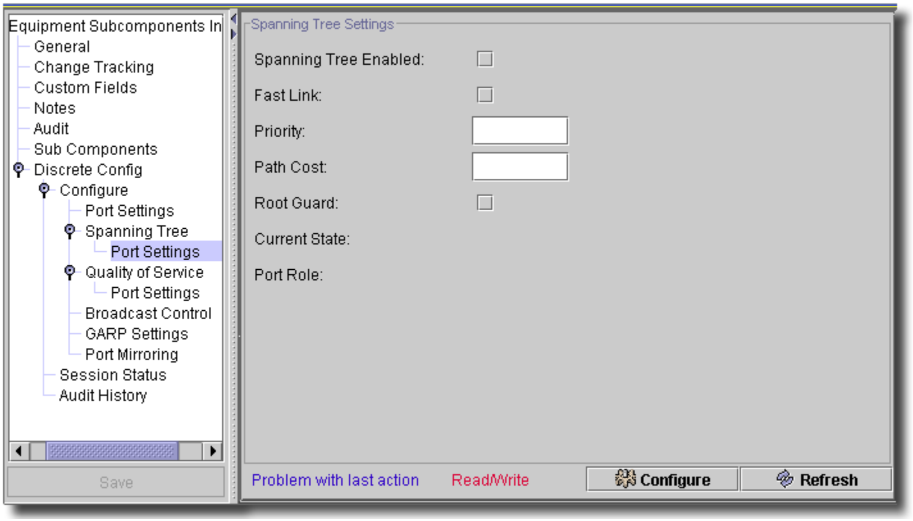
Broken—The LAG is currently malfunctioning and cannot be used for forwarding traffic.

The remaining, read-only fields display the Designated *Bridge ID*, *Port ID*, and *Cost*.

Spanning Tree -> Port Settings

This screen lets you manage Spanning Tree Port Settings.

Figure 13-25. Spanning Tree -> Port Settings



Spanning Tree Settings

Spanning Tree Enabled: □

Fast Link: □

Priority:

Path Cost:

Root Guard: □

Current State:

Port Role:

Problem with last action   Read/Write

The screen appearance varies, depending on the model of the selected device. The following are fields that may be on this screen. When they appear, they are all mandatory:

- **Spanning Tree Enabled**—Checkbox.
- **Fast Link**—Checkbox.
- **Priority**—Valid Values: 0-65535. For 53X switches, this is 0-255 in steps of 16.
- **Path Cost**—Valid Values: 1-10
- **Current State**—A read-only report of the current state.
- **Port Rate**—Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state. (Does not appear in all switch's screens.)

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

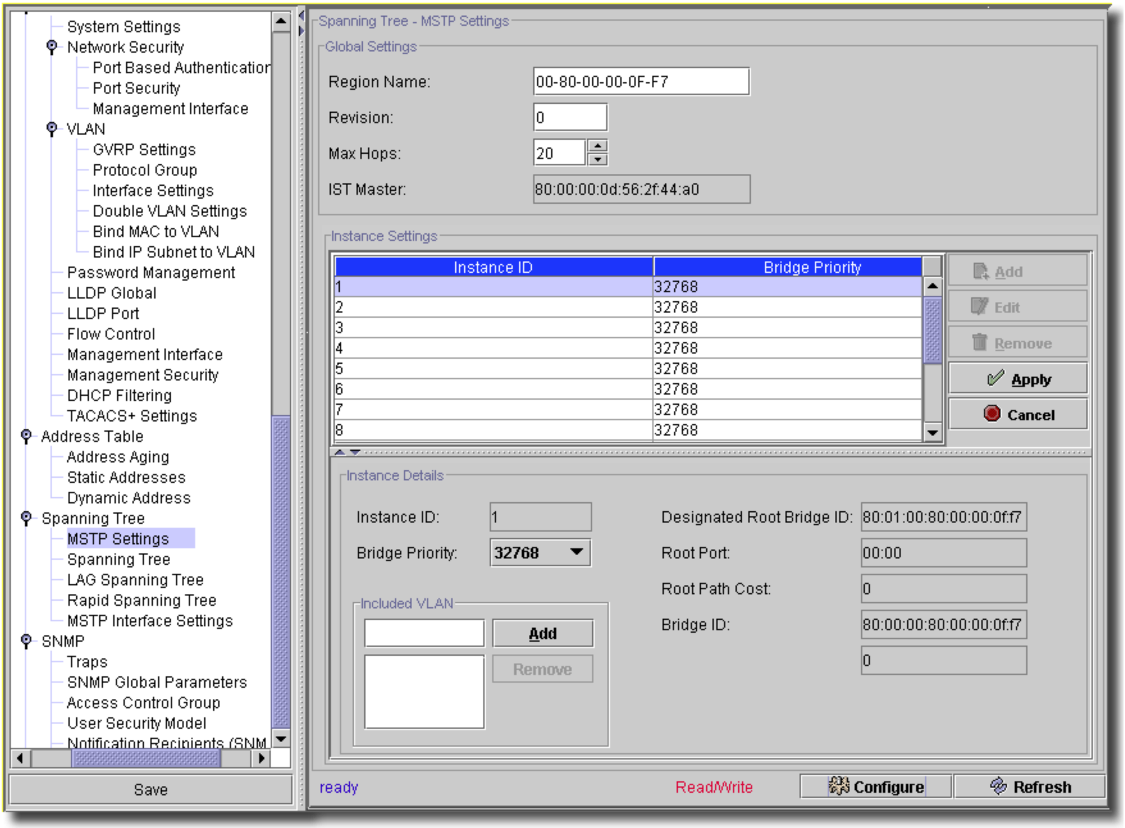
Spanning Tree -> MSTP Settings

This screen manages Multiple Spanning Tree Protocol (MSTP) Settings. The MSTP operation maps VLANs into STP instances.

MSTP provides a alternative load balancing scenarios. For example, while one STP instance blocks port A, the same port can be in its Forwarding State in another STP instance. The MSTP Settings page allows defining up to sixteen MSTP instances for the device.

In addition, packets assigned to various VLANs are transmitted along different paths within Multiple Spanning Trees Regions (MST regions). Regions are one or more interconnected Multiple Spanning Tree bridges with identical MSTP configuration. In configuring an MST, the MST region to which your device belongs is defined. A configuration consists of the name, revision and region to which your device belongs.

Figure 13-26. MSTP Settings



Spanning Tree - MSTP Settings

Global Settings

Region Name: 00-80-00-00-0F-F7

Revision: 0

Max Hops: 20

IST Master: 80:00:00:0d:56:2f:44:a0

Instance Settings

Instance ID	Bridge Priority
1	32768
2	32768
3	32768
4	32768
5	32768
6	32768
7	32768
8	32768

Instance Details

Instance ID: 1

Bridge Priority: 32768

Included VLAN

Designated Root Bridge ID: 80:01:00:80:00:00:0f:f7

Root Port: 00:00

Root Path Cost: 0

Bridge ID: 80:00:00:80:00:00:0f:f7

0

The MSTP Settings page contains the following fields:

Global Settings

- **Region Name (1-32)**—Specifies a user-defined MST region name.
- **Revision (0-65535)**—Specifies unsigned 16-bit number that identifies the revision of the current MST configuration. The revision number is required as part of the MST configuration.
- **Max Hops (1-40)**—Specifies the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information ages out. The default field value is 20.
- **IST Master**—Indicates the Internal Spanning Tree Master ID. The IST Master is the root of the specified instance and its ID number is 0.

Instance Settings

To add instances, click *Add* (or click *Edit* to modify an existing, selected instance). You can delete a listed instance by selecting it, then clicking *Remove*. Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits. If you are editing an instance, the following appears:

Instance Details

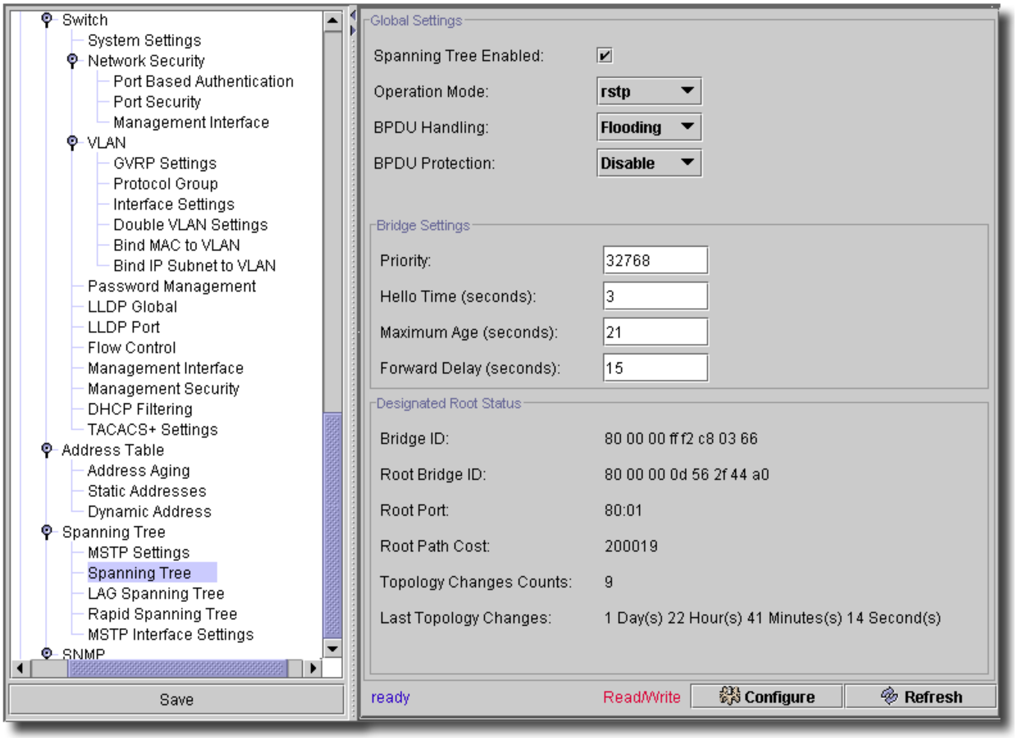
- **Instance ID**—Specifies the ID of the spanning tree instance. The field range is 1-15.
- **Bridge Priority (0-61440)**—Specifies the device priority for the selected spanning tree instance.
- **Included VLANs**— Maps the selected VLANs to the selected instance. Every VLAN belongs to one instance only. Enter a VLAN in the field above the list, then click *Add*. Select one, then click *Remove* to delete it.
- **Designated Root Bridge ID**—Indicates the ID of the bridge with the lowest path cost.
- **Root Port**—Indicates the root port of the selected instance.
- **Root Path Cost**—Indicates the path cost of the selected instance.
- **Bridge ID**—Indicates the bridge ID of the selected instance.
- **Remaining Hops**—Indicates the number of hops remaining to the next destination.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Spanning Tree -> Spanning Tree

This screen manages global, Bridge, and root status for the selected device’s spanning tree

Figure 13-27. Spanning Tree -> Spanning Tree.



Global Settings

Spanning Tree Enabled: ☑

Operation Mode: rstp

BPDU Handling: Flooding

BPDU Protection: Disable

Bridge Settings

Priority: 32768

Hello Time (seconds): 3

Maximum Age (seconds): 21

Forward Delay (seconds): 15

Designated Root Status

Bridge ID: 80 00 00 ff f2 c8 03 66

Root Bridge ID: 80 00 00 0d 56 2f 44 a0

Root Port: 80:01

Root Path Cost: 200019

Topology Changes Counts: 9

Last Topology Changes: 1 Day(s) 22 Hour(s) 41 Minutes(s) 14 Second(s)

This screen has the following fields:

Global Settings

- **Spanning Tree Enabled**— Check to enable.
- **Operation Mode**— Select from the pick list. Choices include *Classic STP, Rapid STP,* and *Multiple STP.*
- **BDPU Handling**— Specifies BPDU packet handling when the spanning tree is disabled on an interface. The possible field values are *Filtering* and *Flooding*. The default value is *Flooding*.
- **BDPU Protection**— Disables a port in case a new switch tries to enter the already existing Spanning Tree (STP) topology. This keeps switches not originally part of an STP from influencing the STP topology.

Bridge Settings

- **Priority—** (0-61440). Specifies the bridge priority value. When switches or bridges are running STP, each are assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge.
- **Hello Time—** (1-10). Specifies the switch Hello time, which indicates the amount of time in seconds a root bridge waits between configuration messages. The default value is 2.
- **Maximum Age (seconds)—** Specifies the switch maximum age time, which indicates the amount of time in seconds a bridge waits before implementing a topological change. The default value is 20.
- **Forward Delay (seconds)—** (4-30). Specifies the switch forward delay time, which indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default value is 15.

Designated Root Status

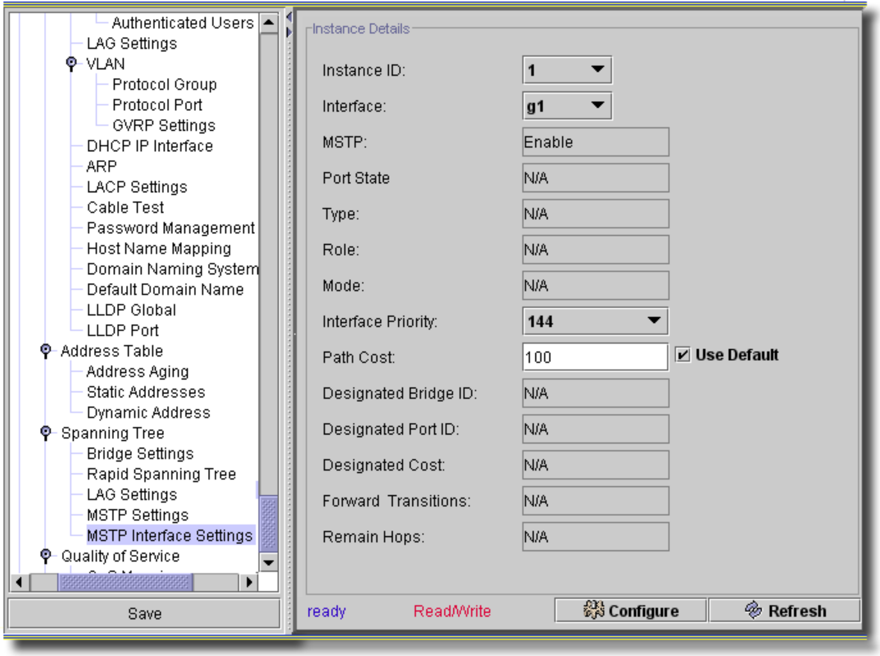
- **Bridge ID—** Displays the bridge ID.
- **Root Bridge ID—** Displays the root bridge ID.
- **Root Port—** Displays port number that offers the lowest-cost path from this bridge to the root bridge. It is significant when the bridge is not the root. The default is zero.
- **Root Path Cost—** Displays the cost of the path from this bridge to the root.
- **Topology Changes Counts—** Displays the total amount of STP state changes that have occurred.
- **Last Topology Changes—** Displays the total amount of time since the last topographic change. The time is displayed in day/hour/minute/second format, for example, 0 day 5 hours 10 minutes and 4 seconds.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Spanning Tree -> MSTP Interface Settings

This screen manages MSTP Interface Settings. Use it to assign MSTP settings to specific interfaces.

Figure 13-28. MSTP Interface Settings



Instance Details

Instance ID: 1

Interface: g1

MSTP: Enable

Port State N/A

Type: N/A

Role: N/A

Mode: N/A

Interface Priority: 144

Path Cost: 100 ☑ Use Default

Designated Bridge ID: N/A

Designated Port ID: N/A

Designated Cost: N/A

Forward Transitions: N/A

Remain Hops: N/A

ready Read/Write

The MSTP Interface Setting page contains the following parameters:

- **Instance ID**—Lists the MSTP instances configured on the device. Possible field range is 0-15.

- **Interface**—Assigns either ports or LAGs to the selected MSTP instance.

- **Port State**— Indicates whether the port is enabled or disabled in the specific instance.

- **Type**—Indicates whether MSTP treats the port as a point-to-point port or a port connected to a hub and whether the port is internal to the MST region or a boundary port. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode

- **Role**—Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:

  Root – Provides the lowest cost path to forward packets to root device.

  Designated – Indicates the port or LAG via which the designated device is attached to the LAN.

  Alternate – Provides an alternate path to the root device from the interface.

Backup – Provides a backup path to the designated LAN. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

Disabled – Indicates the port is not participating in the Spanning Tree.

- **Mode**—Defines Mode of the MSTP interface for that specific instance. If the port is connected to a LAN segment outside or inside the region, the Mode is *Boundary*, and if the type of BPDU transmitted by this port is STP the mode will be *STP*. If the STP version is not MSTP, it display *N/A*.

- **Interface Priority**—Defines the interface priority for the specified instance. The priority range is 0-240 in steps of 16.The default value is 128.

- **Path Cost**—Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000. When MSTP is enabled, you can check (or uncheck) *Use Default*. If it is unchecked, the path cost you enter overrides the default.

- **Designated Bridge ID**—ID number of the bridge that connects the link or shared LAN to the root.

- **Designated Port ID** —ID number of the port on the designated bridge that connects the link or the shared LAN to the root.

- **Designated Cost**—Cost of the path from the link or the shared LAN to the root.

- **Forward Transitions**—Number of times the port changed to the forwarding state. (Read Only, not on all device's screens)

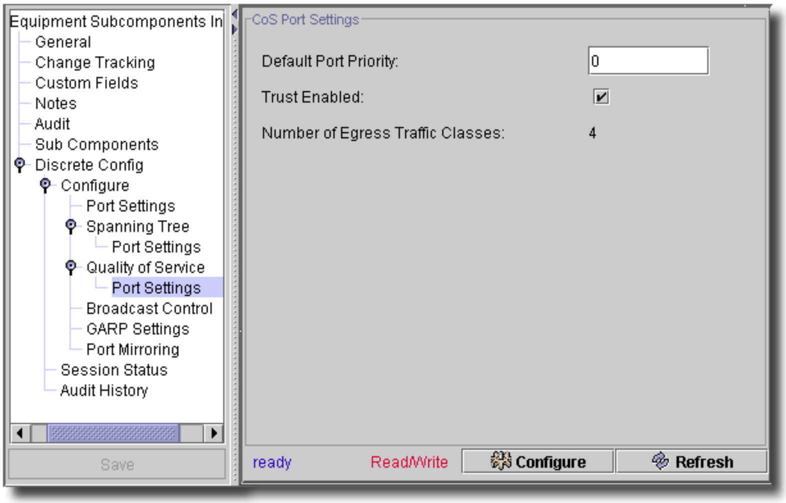
- **Remain Hops**—Indicates the number of hops remaining to the next destination. (Read Only, not on all device's screens)

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Quality of Service -> Port Settings

This screen appears for ports on only selected switch models (53xx and 60xx) and lets you configure QoS port settings.

Figure 13-29. QoS Port Settings



CoS Port Settings

Default Port Priority: 0

Trust Enabled: ☑

Number of Egress Traffic Classes: 4

This screen contains the following fields:

- **Default Port Priority**—Enter a priority (lower numbers are higher priority).

- **Trust Enabled**—Check to enable.

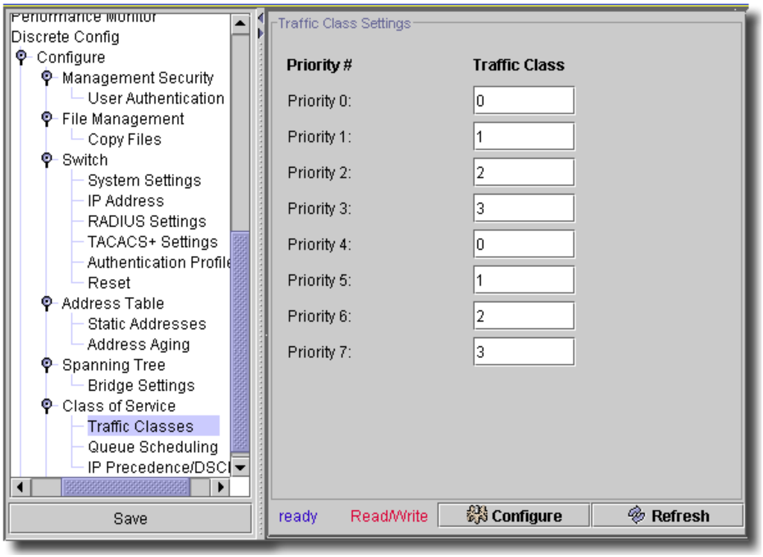
- **Number of Egress Traffic Classes**—A read-only display of how many classes.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Class of Service -> Traffic Classes

You can prioritize classes of traffic on an entire device (not a port) with this screen.

Figure 13-30. Class of Service -> Traffic Classes



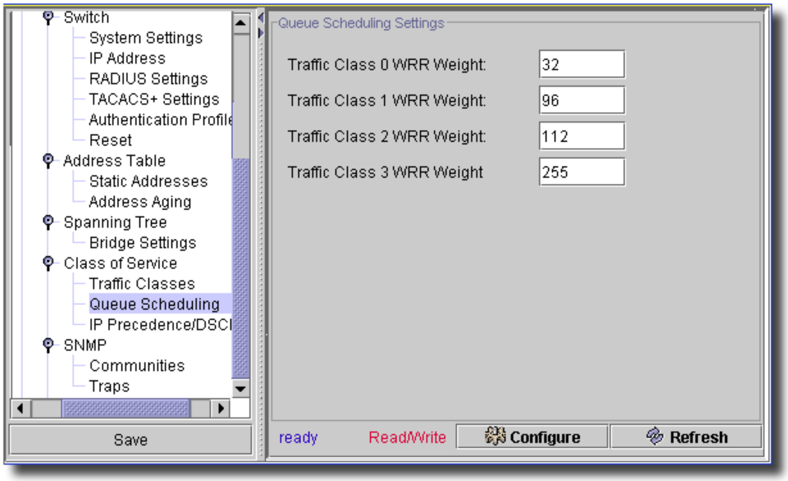
Priority #	Traffic Class
Priority 0:	0
Priority 1:	1
Priority 2:	2
Priority 3:	3
Priority 4:	0
Priority 5:	1
Priority 6:	2
Priority 7:	3

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Class of Service -> Queue Scheduling

Use this screen for queue scheduling on an entire device (not a port).

Figure 13-31. Class of Service -> Queue Scheduling



Queue Scheduling Settings

Traffic Class 0 WRR Weight: 32

Traffic Class 1 WRR Weight: 96

Traffic Class 2 WRR Weight: 112

Traffic Class 3 WRR Weight 255

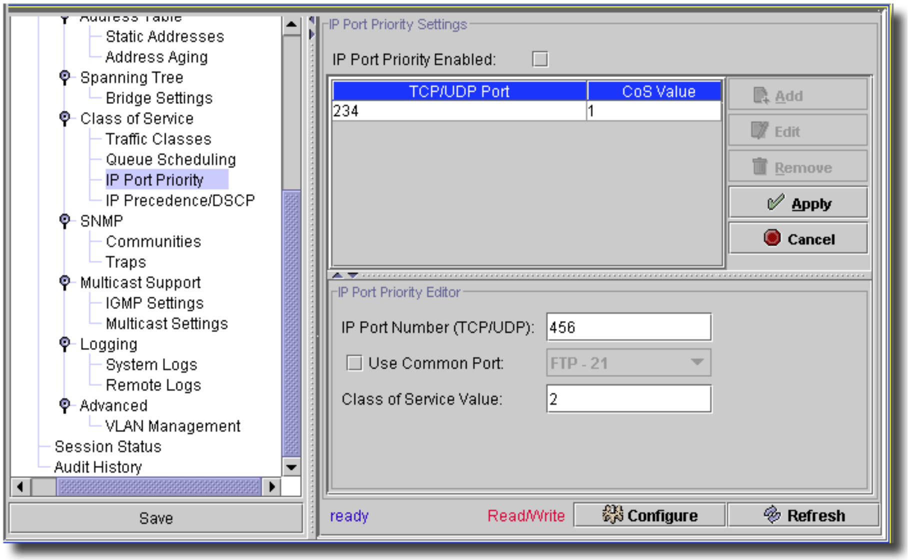
ready Read/Write

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Class of Service -> IP Port Priority

Use this screen to set the IP Port priority for your device.

Figure 13-32. Class of Service -> IP Port Priority



IP Port Priority Enabled: □

TCP/UDP Port	CoS Value
234	1

IP Port Number (TCP/UDP): 456

□ Use Common Port: FTP - 21

Class of Service Value: 2

If you enable IP port priority with the checkbox at the top of this screen, you can add or edit a TCP/UDP port and assign it a class of service priority in this screen. Use the *Add*, *Edit* and *Remove* buttons to manage configured ports in the table. When you select *Add* or *Edit*, the editor appears below the table. It has the following fields:

- **IP Port Number (TCP/UDP)**—Enter the port number

- **Use Common Port**— Check to enable the pick list where you can select a common type of port (*FTP-21*, *HTTP* - 80, and so on).

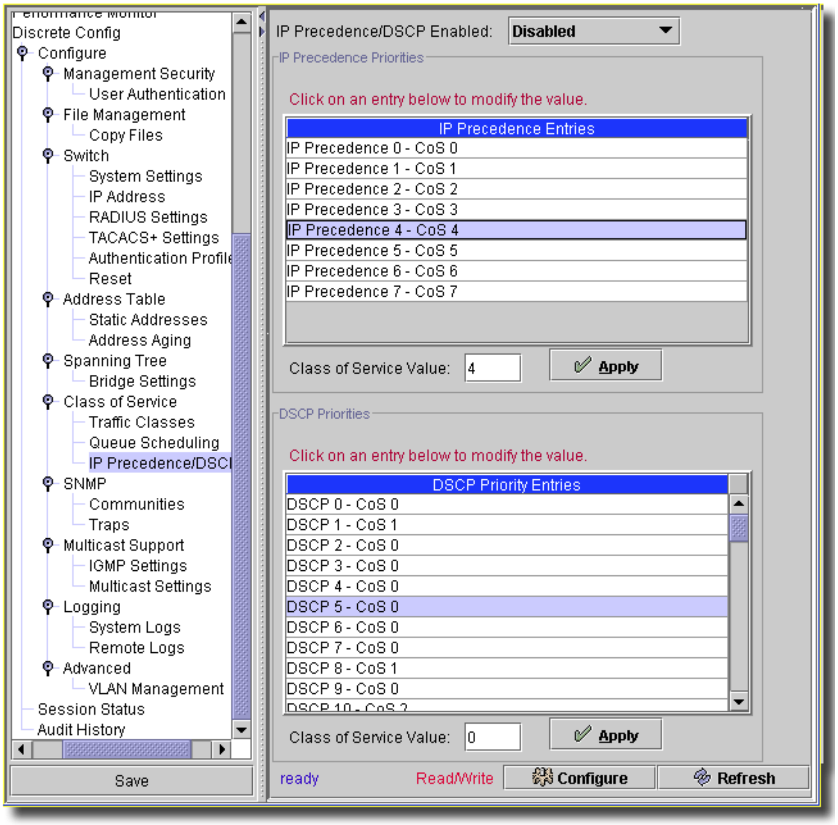
- **Class of Service Value**—Enter a Class of Service number.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Class of Service -> IP Precedence/DSCP

Use this screen to enable/disable (with the checkbox) and manage the IP port precedence for the selected device.

Figure 13-33. Class of Service -> IP Precedence



IP Precedence/DSCP Enabled: Disabled

IP Precedence Priorities

Click on an entry below to modify the value.

IP Precedence Entries
IP Precedence 0 - CoS 0
IP Precedence 1 - CoS 1
IP Precedence 2 - CoS 2
IP Precedence 3 - CoS 3
IP Precedence 4 - CoS 4
IP Precedence 5 - CoS 5
IP Precedence 6 - CoS 6
IP Precedence 7 - CoS 7

Class of Service Value: 4

DSCP Priorities

Click on an entry below to modify the value.

DSCP Priority Entries
DSCP 0 - CoS 0
DSCP 1 - CoS 1
DSCP 2 - CoS 0
DSCP 3 - CoS 0
DSCP 4 - CoS 0
DSCP 5 - CoS 0
DSCP 6 - CoS 0
DSCP 7 - CoS 0
DSCP 8 - CoS 1
DSCP 9 - CoS 0
DSCP 10 - CoS 2

Class of Service Value: 0

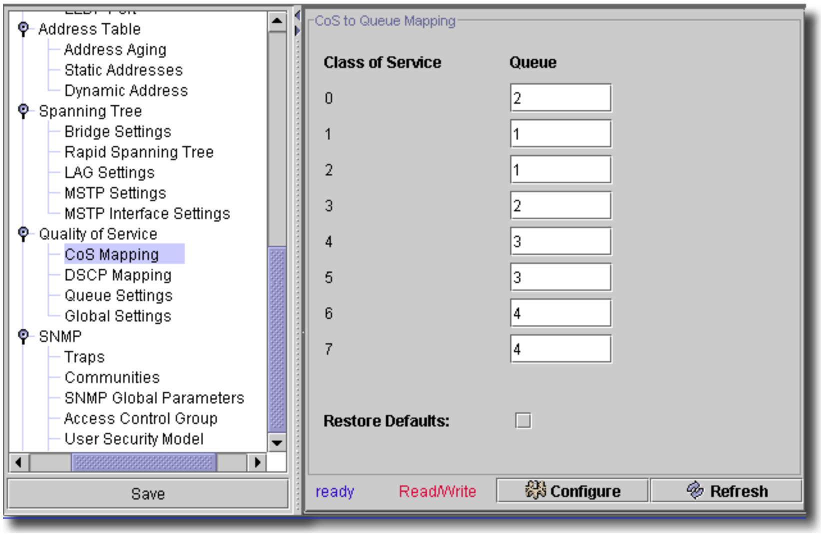
If you check to enable IP precedence, you can select IP Precedence entries (upper table) and DSCP Priorities (lower table). Select an item, and its value appears in the *Class of Service Value* field for the appropriate table. When you change the value, you must click the *Apply* button next to that field.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

QOS -> CoS Mapping

This resembles Class of Service -> Traffic Classes on page 267.

Figure 13-34. QOS -> Class of Service Mappings



CoS to Queue Mapping

Class of Service	Queue
0	2
1	1
2	1
3	2
4	3
5	3
6	4
7	4

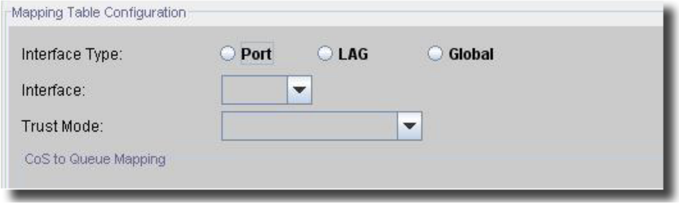
Restore Defaults: ☐

This screen contains the following columns:

- **Class of Service**—Lists Class of Service with queue selection from the drop-down menu.
- **Queue**—Selects a queue for each Class of Service from the drop-down menu. Default queues are displayed initially.
- **Restore Defaults**—Restores default queue values when checked, after you click *Configure*.

Some models precede the Class of Service / Queue mapping with a *Mapping Table Configuration* panel.

Figure 13-35. QOS -> Class of Service Mappings - Mapping Table



Mapping Table Configuration

Interface Type: ○ Port ○ LAG ○ Global

Interface:

Trust Mode:

This includes the following fields:

- **Interface Type**—Select either *Port*, *LAG* or *Global* with the radio buttons. This selects the interface(s) to which the class of service configuration is applied. Global applies the class of configuration to all the interfaces

- **Interface**—Select the interface with the pick list.

- **Trust Mode**—Select with the pick list. This determines which packet fields to use for classifying packets entering the device. When it finds no rules, the device maps traffic containing the predefined packet field (CoS or DSCP) according to the relevant trust modes table, mapping traffic not containing a predefined packet field to best effort. The possible Trust Mode field values are the following:

  Untrusted–Returns to the non-trusted state.

  CoS(802.1P)–The output queue assignment is determined by the IEEE802.1p VLAN priority tag (VPT) or by the default VPT assigned to a port.

  IP DSCP–The output queue assignment is determined by the DSCP field.

NOTE:

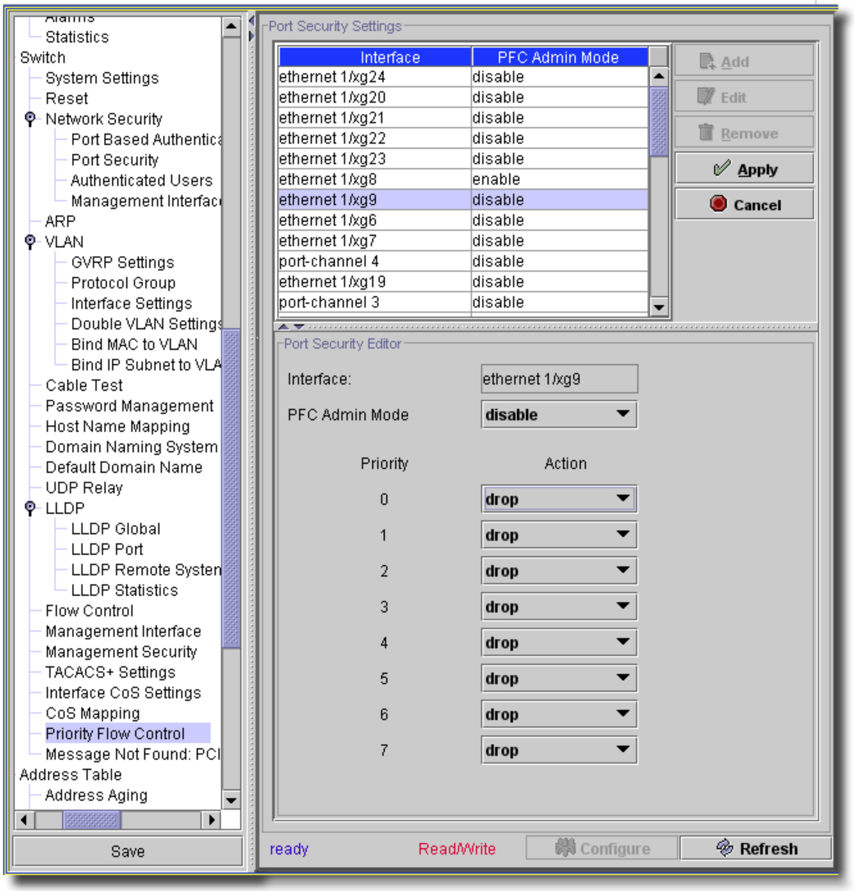
This screen is not available for all equipment.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Priority Flow Control

This screen manages priority flow control (PFC). It specifies ports individually for PFC configuration and applies Priority based Actions to the selected ports.

Figure 13-36. Priority Flow Control



Port Security Settings

Interface	PFC Admin Mode
ethernet 1/xg24	disable
ethernet 1/xg20	disable
ethernet 1/xg21	disable
ethernet 1/xg22	disable
ethernet 1/xg23	disable
ethernet 1/xg8	enable
ethernet 1/xg9	disable
ethernet 1/xg6	disable
ethernet 1/xg7	disable
port-channel 4	disable
ethernet 1/xg19	disable
port-channel 3	disable

Port Security Editor

Interface: ethernet 1/xg9

PFC Admin Mode: disable

Priority	Action
0	drop
1	drop
2	drop
3	drop
4	drop
5	drop
6	drop
7	drop

You can modify the Port Security Settings selected in the upper panel by clicking the *Edit* button to the right of their list. The *Port Security Editor* appears at the bottom of the screen when you do. It contains the following fields:

- **Interface**—The (read only) port designator.

- **PFC Admin Mode**—Select *Enable* or *Disable* to enable or disable PFC on the selected port.

- **Priority**—This displays the priority value for which you can configure an action (*drop/no-drop*) on the selected interface.

NOTE:

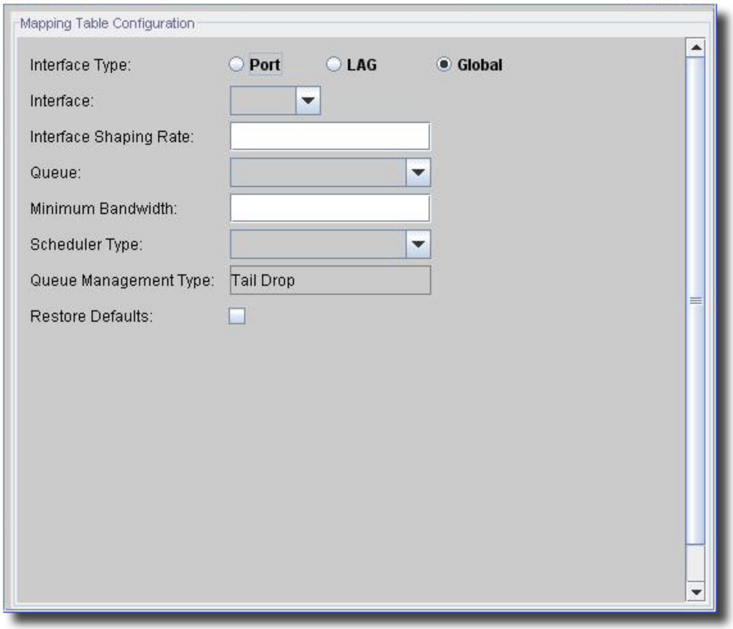
The No Drop policy can only be applied to two Priorities at any time.

Click *Apply* to accept your edits, or *Cancel* to abandon them for the selected port.

QOS -> CoS Interface

This screen lets you configure CoS for interfaces.

Figure 13-37. QOS -> CoS Interface



Mapping Table Configuration

Interface Type: ○ Port ○ LAG ● Global

Interface:

Interface Shaping Rate:

Queue:

Minimum Bandwidth:

Scheduler Type:

Queue Management Type: Tail Drop

Restore Defaults: □

It contains the following fields:

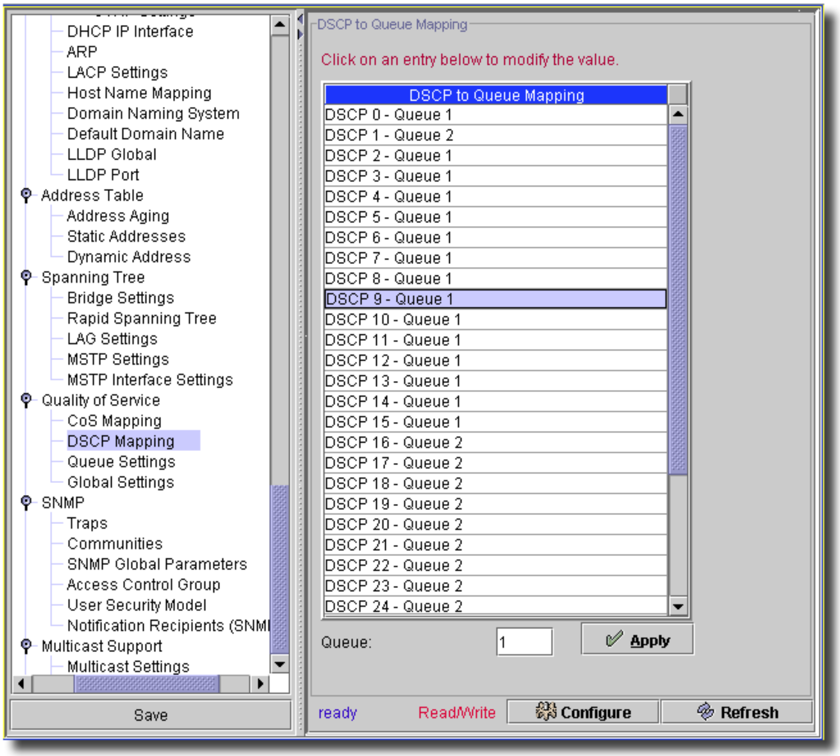
- **Interface Type**—Select either *Port*, *LAG* or *Global* with the radio buttons. This selects the interface(s) to which the class of service configuration is applied. Global applies the class of configuration to all the interfaces
- **Interface**—Select the interface with the pick list. This specifies the Unit/Port, LAG or Global that is being configured.
- **Interface Shaping Rate**—Select the interface with the pick list.
- **Queue**—Select the queue to be configured from the pick list.

- **Minimum Bandwidth**—Enter a percentage of the maximum negotiated bandwidth for the port. Specify a percentage from 0 to 100, in increments of 5.
- **Scheduler Type**—Select the scheduler with the pick list. This selects the type of queue processing. Options are *Weighted* and *Strict*. Defining on a per-queue basis lets you create the desired service characteristics for different types of traffic. *Weighted* round robin associates a weight to each queue. This is the default. *Strict* services traffic with the highest priority on a queue first.
- **Queue Management Type**—Displays the type of packet management used for all packets, which is *Taildrop*. All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped
- **Restore Defaults**—Restores the default interface shaping rate to the selected interfaces when checked.

QOS -> DSCP Mapping

This resembles part of the functions described in Class of Service -> IP Precedence/DSCP on page 270. See that topic for a description of its functions.

Figure 13-38. QOS -> DSCP Mapping



Click on an entry below to modify the value.

DSCP to Queue Mapping
DSCP 0 - Queue 1
DSCP 1 - Queue 2
DSCP 2 - Queue 1
DSCP 3 - Queue 1
DSCP 4 - Queue 1
DSCP 5 - Queue 1
DSCP 6 - Queue 1
DSCP 7 - Queue 1
DSCP 8 - Queue 1
DSCP 9 - Queue 1
DSCP 10 - Queue 1
DSCP 11 - Queue 1
DSCP 12 - Queue 1
DSCP 13 - Queue 1
DSCP 14 - Queue 1
DSCP 15 - Queue 1
DSCP 16 - Queue 2
DSCP 17 - Queue 2
DSCP 18 - Queue 2
DSCP 19 - Queue 2
DSCP 20 - Queue 2
DSCP 21 - Queue 2
DSCP 22 - Queue 2
DSCP 23 - Queue 2
DSCP 24 - Queue 2

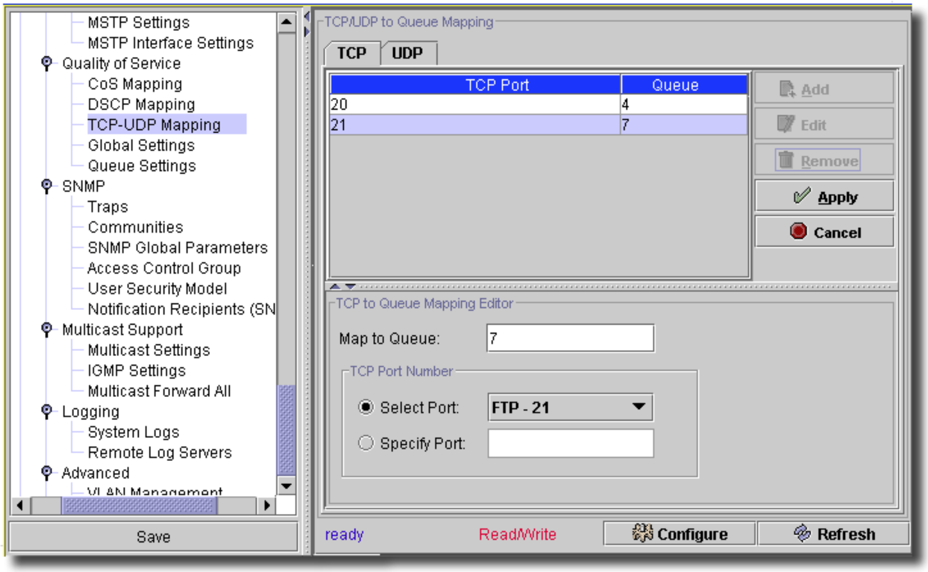
Queue: 1

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

QOS -> TCP/UDP Mapping

This screen handles the TCP and UDP to Queue mapping. Use it as you would other editor screens to manage those mappings.

Figure 13-39. TCP and UDP to Queue Mappings



TCP Port	Queue
20	4
21	7

Map to Queue: 7

● Select Port: FTP - 21

○ Specify Port:

ready Read/Write

When you *Add* or *Edit* a mapping, the editor panel appears in the panel below the *TCP* and *UDP* tabs. Click *Apply* to confirm your edits (*Cancel* to abandon them). Here are the fields that appear in both editors:

- **Map to Queue**—Enter a queue number to map.

- Radio buttons ensure you only select one of the following fields:

- **Select Port** —Select an already discovered port from the pick list.

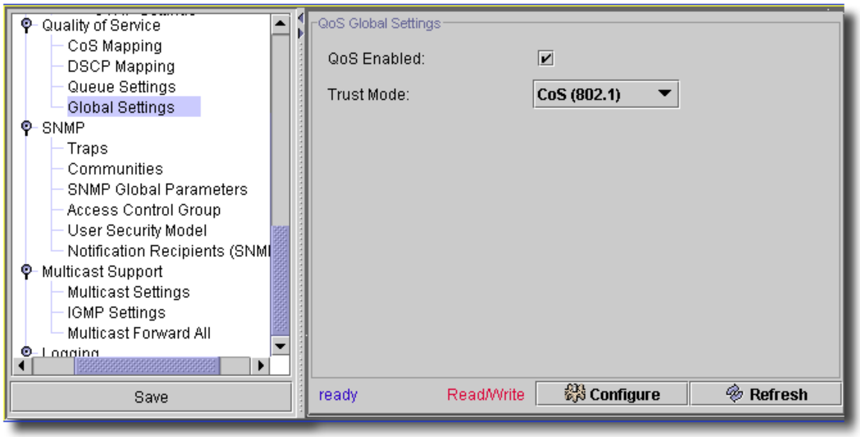
- **Specify Port**—Type in the port number.

Click *Configure* to implement your edits; *Refresh* to re-query the database for them.

QOS -> Global Settings

The Global Settings screen lets you enable/disable QoS management (with the checkbox), and set the *Trust Mode* with a pick list.

Figure 13-40. QOS -> Global Settings



QoS Global Settings

QoS Enabled: ☑

Trust Mode: CoS (802.1)

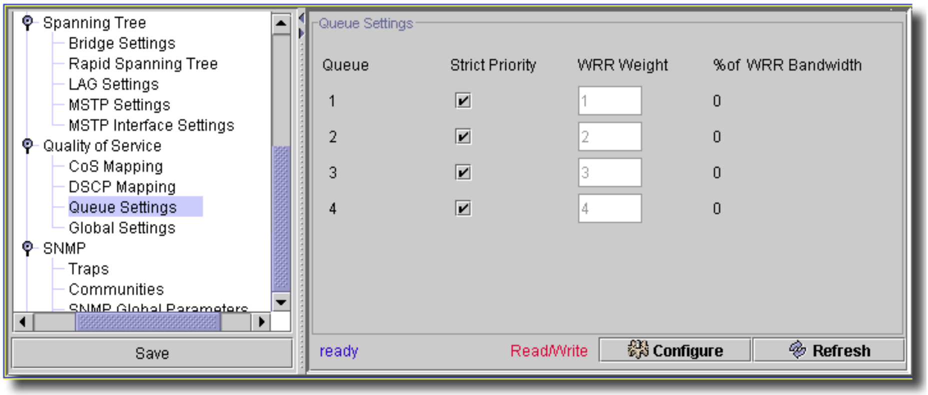
The available choices for *Trust Mode* include *None*, *CoS (802.1)*, *DSCP*, and *TCP/UDP Port*. The *TCP/UPD Port* option is not available in all switches.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

QOS -> Queue Settings

This screen lets you manage queue settings.

Figure 13-41. QOS -> Queue Settings



Queue Settings

Queue	Strict Priority	WRR Weight	%of WRR Bandwidth
1	☑	1	0
2	☑	2	0
3	☑	3	0
4	☑	4	0

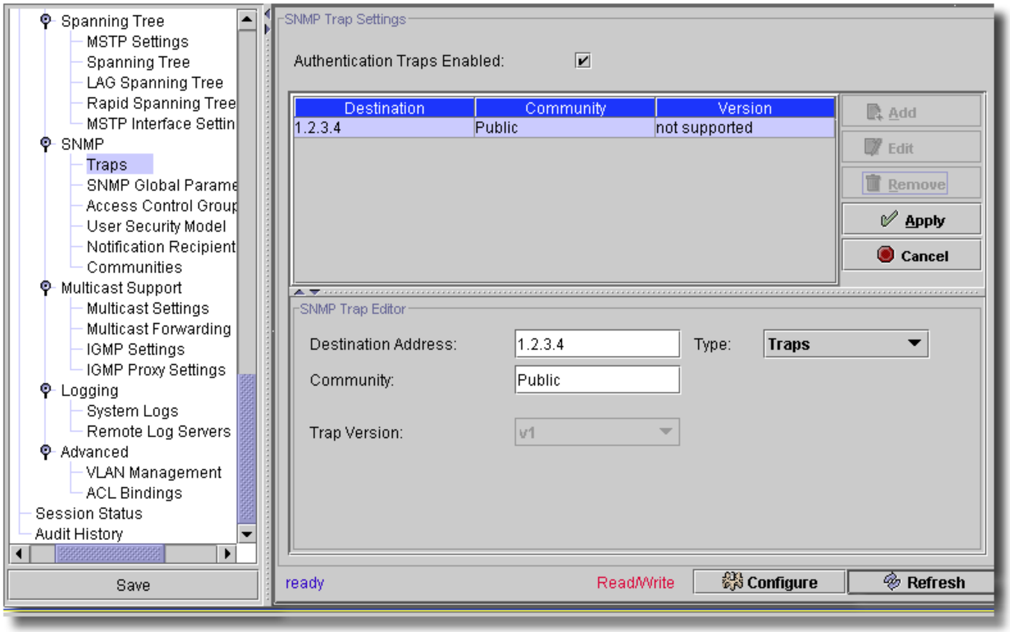
See Class of Service -> Queue Scheduling on page 268 for details about its functions.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

SNMP -> Traps

This screen lets you manage SNMP Trap Settings. Existing SNMP trap settings appear in the SNMP Trap Table showing the following columns: *Destination*, *Community* and *Version*. When you elect to add or edit a row in this table, the lower panel displays an editor.

Figure 13-42. SNMP -> Traps



Authentication Traps Enabled: ☑

Destination	Community	Version
1.2.3.4	Public	not supported

Destination Address: 1.2.3.4

Type: Traps

Community: Public

Trap Version: v1

Click *Apply* to accept your edits, or *Cancel* to abandon them. You can also select a row and delete it by clicking *Remove*. The following are fields on the editor:

- **Destination Address**—An IP address.

Community —The Community String. Text.

- **Trap Version**—Values: [V1, V2c] (grayed out when not supported).

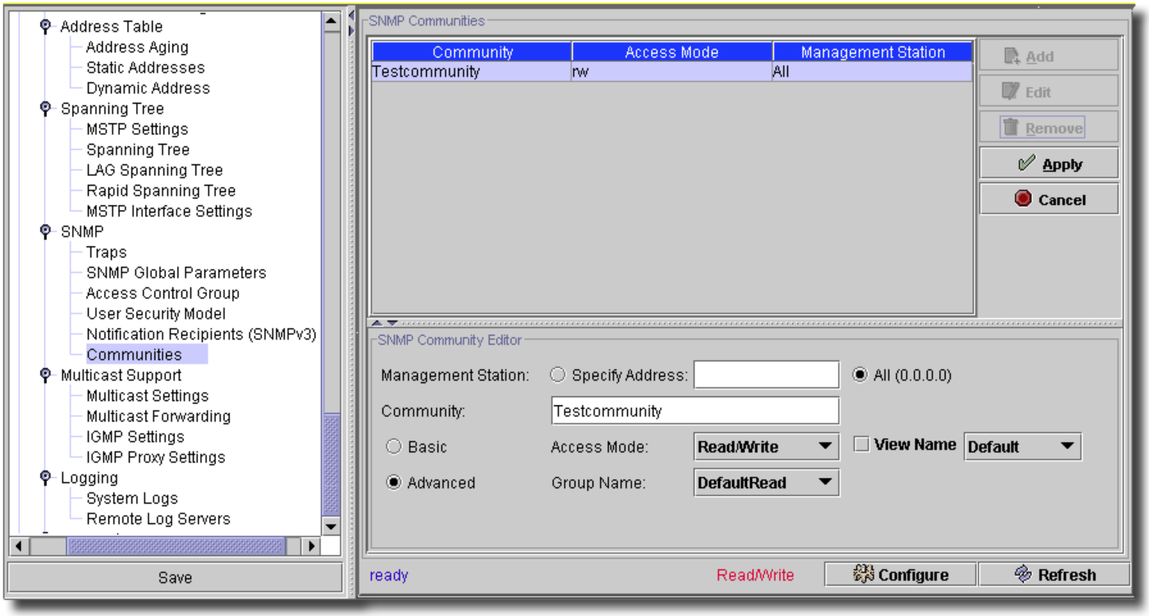
- **Access**—Select from the pick list (*Read Only*, etc.) This lets you specify the community access during creation of a trap destination. This is not necessary for all switches.

You can also enable authentication traps with the *Authentication Traps Enabled* checkbox. When you add or edit values, you must click *Apply* to confirm your edits, or *Cancel* to abandon them. Click *Configure* to apply the values; *Refresh* to re-query the database for them.

SNMP -> Communities

This screen lets you manage SNMP Community Settings. Existing SNMP settings appear listed at the top of this screen. When you elect to add or edit a row in this table the lower panel displays an editor.

Figure 13-43. SNMP -> Communities



Community	Access Mode	Management Station
Testcommunity	rw	All

Management Station: ○ Specify Address: ● All (0.0.0.0)

Community: Testcommunity

○ Basic Access Mode: Read/Write □ View Name Default

● Advanced Group Name: DefaultRead

ready Read/Write

You can also select a row and *Remove* it.The following are fields on this screen. They are mandatory:

Community String—Text for the community string.

- **Access Mode**—Values: *Read-Only, Read-Write, SNMP Admin*. Not all these options appear for all switches.
- **Management Station**—This field appears for some models and represents the IP address of computers that access the switch. A value of 0.0.0.0 means that the community can be used for accessing the switch from all management stations. If you specify a specific IP, then only the specific management station can use the community.

NOTE:

This also supports IPv6 addresses.

Depending on the device you select, another screen may appear.

In addition to the *Community* text, the editor lets you check to select the following (check to *Allow*):

Allow Sets

Allow Gets

Allow Traps

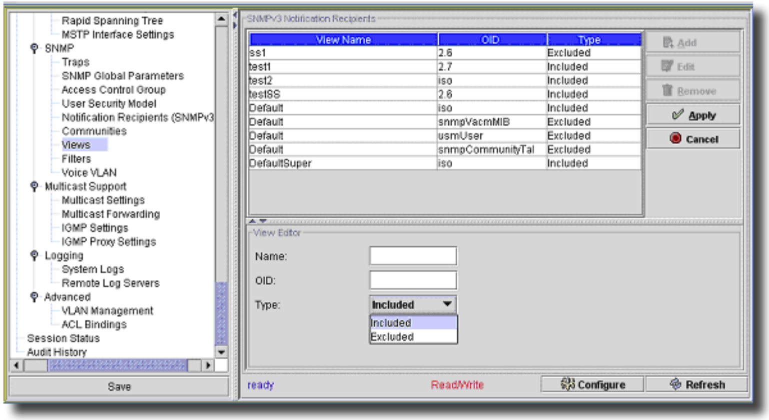
These checkboxes and the *Community* field appear when you elect to *Add* or *Edit* a row in the table.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

SNMP -> Views / Filters

These screens manage SNMP views and filters for the selected device.

Figure 13-44. SNMP -> Views or SNMP -> Filters



View Name	OID	Type
ss1	2.6	Excluded
test1	2.7	Included
test2	iso	Included
testSS	2.6	Included
Default	iso	Included
Default	snmpVacmMIB	Excluded
Default	usmUser	Excluded
Default	snmpCommunityTal	Excluded
DefaultSuper	iso	Included

Name:

OID:

Type: Included

Included
Excluded

The Notification Filter page filters or notifications traps based on OIDs. Each OID is linked to a device feature or a feature aspect.

When you *Add* or *Edit* a mapping, the editor panel appears on the lower panel. Click *Apply* to confirm your edits (*Cancel* to abandon them). Here are the fields that appear in the editor:

- **Name**—Enter an identifier for the SNMP view. A view or filter name can contain a maximum of 30 alphanumeric characters.

- **OID** —Specifies a valid SNMP OID string that can include meta characters like *.

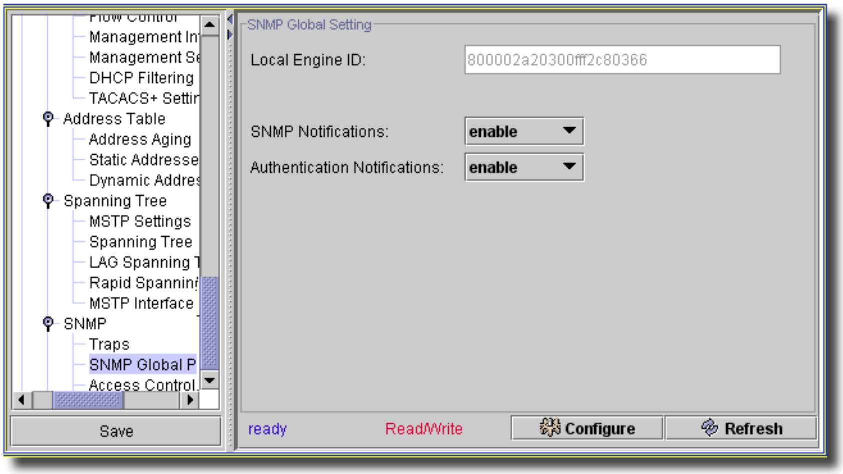
- **Type**—Select whether you want the objectIDs in the view are included or excluded. For filters, this indicates whether trap recipients receive informs or traps regarding the OID.

Click *Configure* to implement your edits; *Refresh* to re-query the database for updates.

SNMP -> SNMP Global Parameters

This screen controls global SNMP parameters for the selected device.

Figure 13-45. SNMP -> SNMP Global Parameters



SNMP Global Setting

Local Engine ID: 800002a20300fff2c80366

SNMP Notifications: enable

Authentication Notifications: enable

ready

Read/Write

This screen has the following fields:

- **Local Engine ID**—Text for the Engine ID (retrieved from the equipment).

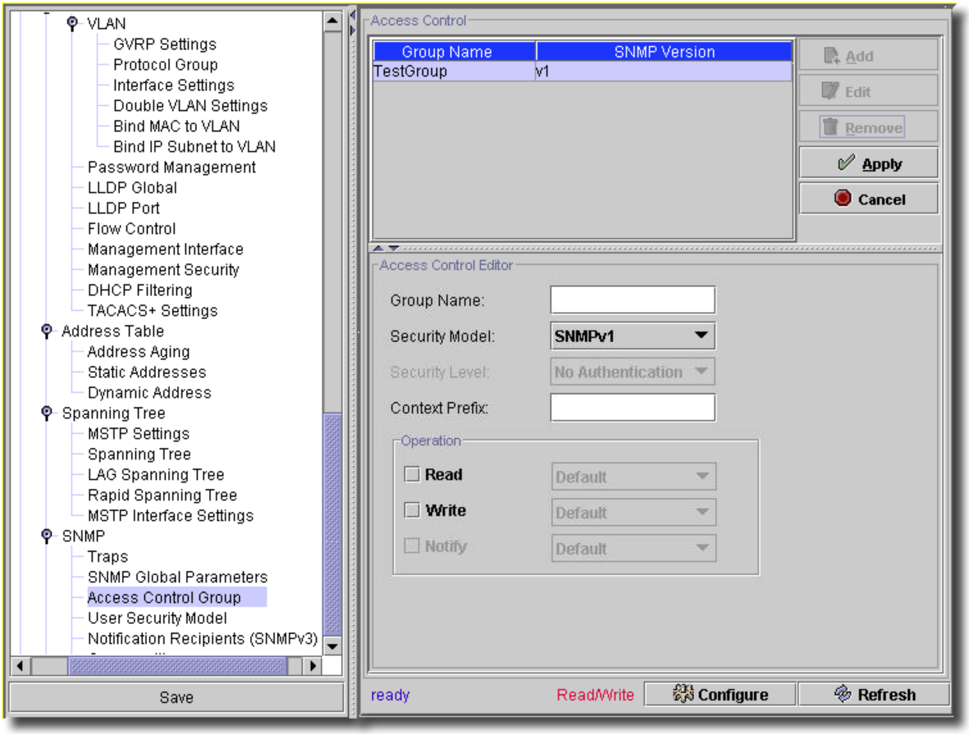
- **SNMP Notifications**—Select from *enable* / *disable*.

- **Authentication Notification**—Select from *enable* / *disable*.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

SNMP -> Access Control Groups

This screen manages the SNMP access control groups for the selected equipment.



Group Name	SNMP Version
TestGroup	v1

Group Name:

Security Model: SNMPv1

Security Level: No Authentication

Context Prefix:

□ Read Default

□ Write Default

□ Notify Default

Figure 13-46. SNMP -> Access Control Groups

When you *Add* or *Edit* a group, the editor panel appears below. Select one and click *Delete* to remove a row. Click *Apply* to confirm your edits (*Cancel* to abandon them). Here are the fields that appear in the editor:

- **Groups Name**—The group identifier. Groups are user-defined lists to which access control rules are applied. A group name can contain a maximum of 30 alphanumeric characters

- **Security Model**—Select the SNMP level to choose a security level for access to the group. The possible field values are:*SNMPv1 SNMPv2*, and *USM* (the SNMPv3 User Security Model [USM] is defined for the group).

- **Security Level**—Select from the pick list. Security levels apply to SNMPv3 groups only. The possible field values include

  No Auth No Priv–Neither Authentication nor Privacy security levels are assigned to the group. Using this option provides no security, confidentiality, or privacy at all. It might be useful for certain applications such as development and debugging to turn security off.

Auth No Priv.–Authenticates SNMP messages without encrypting them.

Auth Priv–Users are authenticated by the SNMPv3 entity before the entity allows the user to access any of the values in the MIB objects on the agent. In addition, all of the requests and responses from the management application to the SNMPv3 entity are encrypted, so that all the data is completely secure.

- **Context Prefix**—(0-30 Characters - does not appear in all device's screens). Specify this to associate the performance information from the MIB objects with that Prefix. The Context EngineID identifies the SNMP entity that should process the request (the physical router) and the Context Prefix (Name) tells the agent in which context it should search for the objects requested by the user or the management application.
- **Operation**—Select from *Default / DefaultSuper* once you check to activate *Read*, *Write* and/or *Notify*. The meaning of these values are:

Read–Select a view that restricts management access to viewing the contents of the agent. If no view is selected, all objects except the community-table, SNMPv3 user and access tables can be viewed.

Write—Select a view that permits management read-write access to the contents of the agent but not to the community.

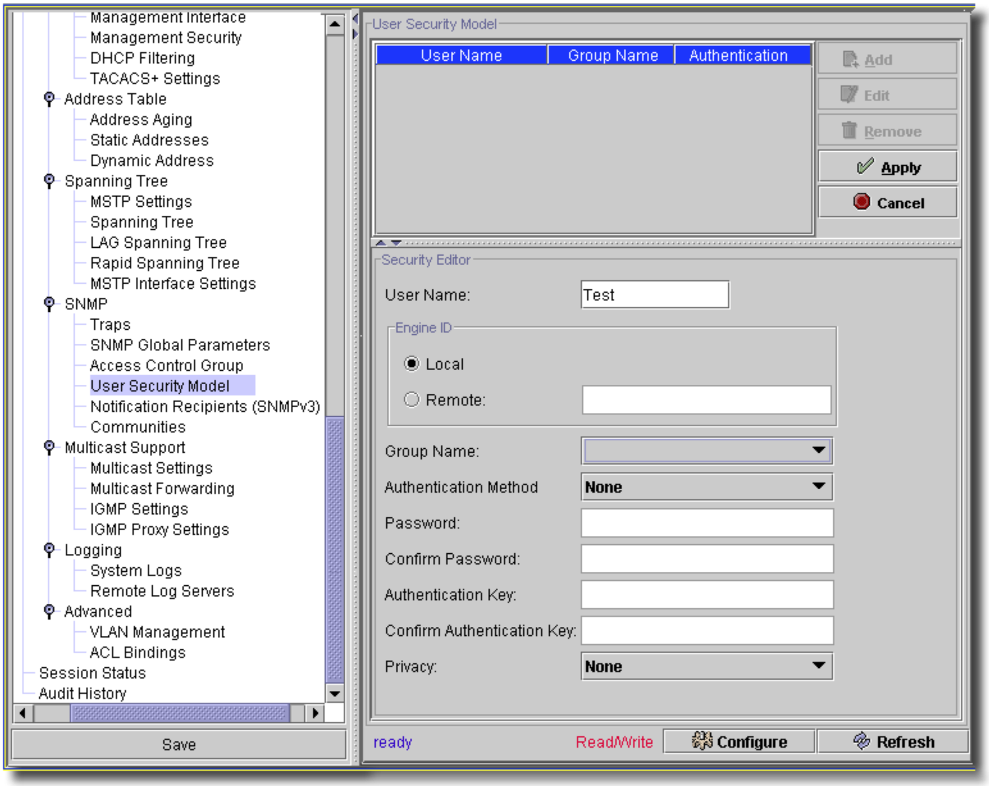
Notify–Select a view that permits sending SNMP traps or informs.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

SNMP -> User Security Model

This screen manages the user security model for the selected equipment.

Figure 13-47. SNMP -> User Security Model



User Name: Test

Engine ID

● Local

○ Remote:

Group Name:

Authentication Method: None

Password:

Confirm Password:

Authentication Key:

Confirm Authentication Key:

Privacy: None

When you *Add* or *Edit* a security model, the editor panel appears below. Select one and click *Delete* to remove a row. Click *Apply* to confirm your edits (*Cancel* to abandon them). Here are the fields that appear in the editor:

- **User Name**—The model identifier.

Engine ID

Select from *Local* or *Remote* with the radio buttons. If you select *Remote*, you must enter the ID in the field to the right of that button.

- **Group Name**—Select the security group from the pick list. You can configure these in the screen described in SNMP -> Access Control Groups on page 282.
- **Authentication Method**—Select from the pick list (*none, MD5 Password, SHA Password, MD5 Key,* or *SHA Key.*)
- **Password/Confirm**—Enter a password.

- **Authentication Key/Confirm**—Enter a key.

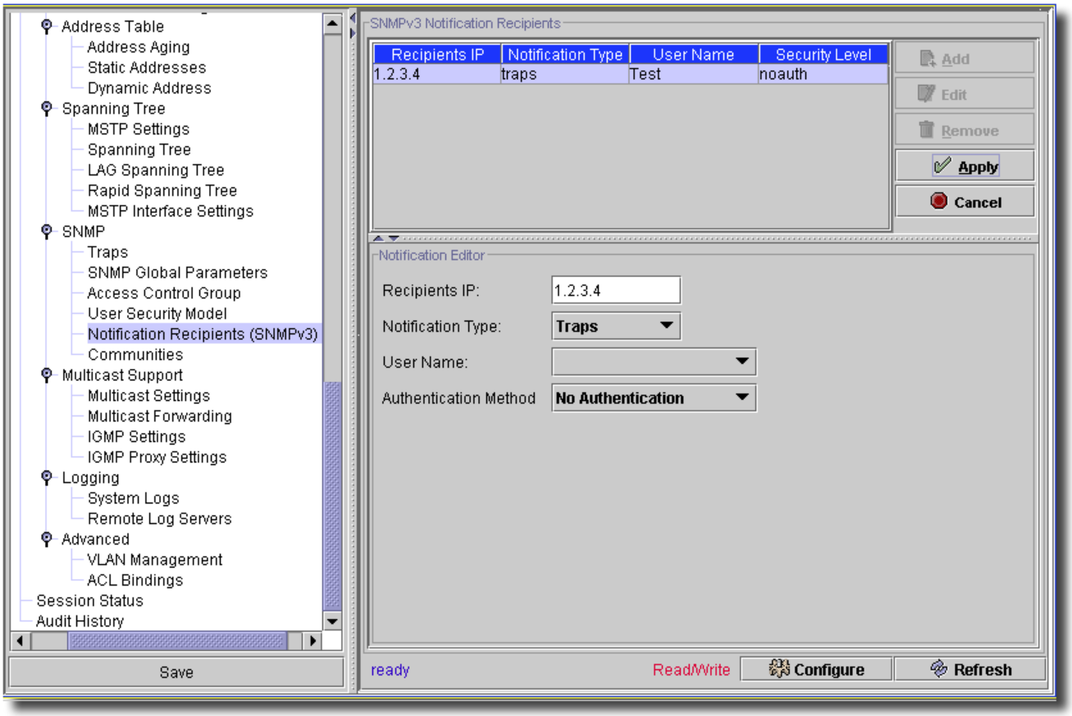
- **Privacy**—Select from the pick list (*None*, *DES*, *DESKey*).

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

SNMP -> Notification Recipients (SNMP v3)

This screen manages the notification recipients for the selected equipment.

Figure 13-48. SNMP -> Notification Recipients (SNMP v3)



SNMPv3 Notification Recipients

Recipients IP	Notification Type	User Name	Security Level
1.2.3.4	traps	Test	noauth

Notification Editor

Recipients IP: 1.2.3.4

Notification Type: Traps

User Name:

Authentication Method No Authentication

When you *Add* or *Edit* a recipient, the editor panel appears below. Select one and click *Delete* to remove a row. Click *Apply* to confirm your edits (*Cancel* to abandon them). Here are the fields that appear in the editor:

- **Recipients IP**—The IP address of the notification recipient.

- **Notification Type**—Select from the pick list (*traps* / *informs*).

- **User Name**—Select a user name from the pick list. user name is now a combo box (derived from the SNMPv3 users in the config).

- **Authentication Method**—Select from the pick list (*No Authentication*, *Authentication* or *Privacy*).

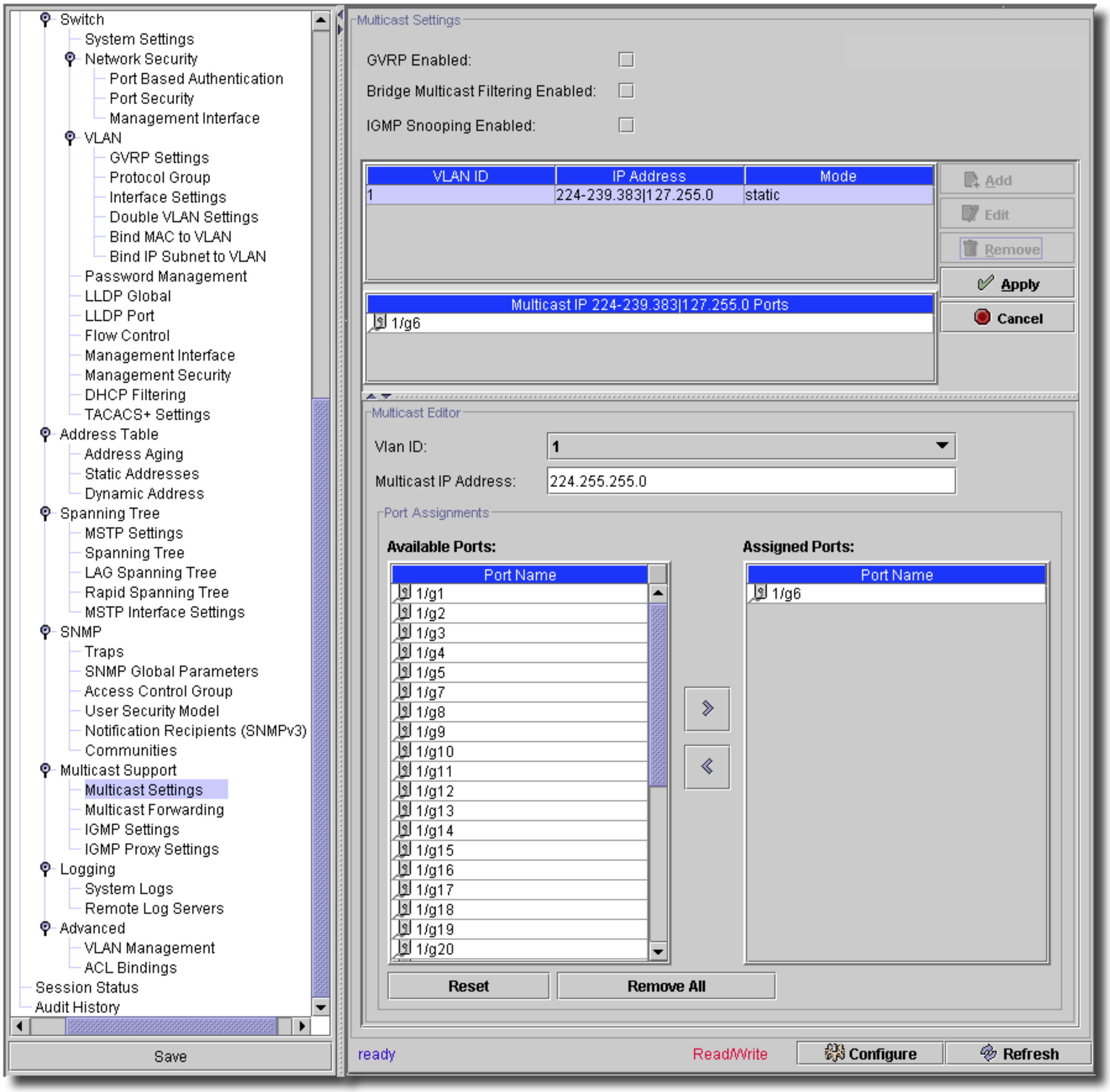
The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Multicast -> Multicast Settings

If you want to assign a multicast IP to a VLAN, you must know the ports associated with the VLAN. When you select a VLAN ID, the Available Ports (left select panel) dynamically changes showing the user the ports currently assigned to this VLAN. This makes it easy to quickly add a multicast address. An intuitive error validation against the multicast IP Address makes a dialog appear showing the acceptable multicast ranges and what addresses are reserved (not allowed to be set on the network equipment).

The following screen is for all supported Dell equipment. The lowest panel is blank, and the A*dd*, *Edit*, *Remove* buttons are active when you select an address. If you click A*dd* or select one and click *Edit*, the editor (lower) panel appears with the fields for the address described below.

Figure 13-49. Assigning a Multicast IP



Multicast Settings

GVRP Enabled: □

Bridge Multicast Filtering Enabled: □

IGMP Snooping Enabled: □

VLAN ID	IP Address	Mode
1	224-239.383|127.255.0	static

Multicast IP 224-239.383|127.255.0 Ports
1/g6

Multicast Editor

Vlan ID: 1

Multicast IP Address: 224.255.255.0

Port Assignments

Available Ports:

Port Name
1/g1
1/g2
1/g3
1/g4
1/g5
1/g7
1/g8
1/g9
1/g10
1/g11
1/g12
1/g13
1/g14
1/g15
1/g16
1/g17
1/g18
1/g19
1/g20

Assigned Ports:

Port Name
1/g6

ready   Read/Write

When you select an address, the multicast ports for that address appear in the middle panel. You can enable the following with checkboxes at the top of this screen:

GVRP Enabled—Checkbox to enable/disable GVRP.

- **Bridge Multicast Filtering Enabled**—Enables or disables bridge Multicast filtering. Disabled is the default value. IGMP Snooping can be enabled only if Bridge Multicast Filtering is enabled. This does not appear on all devices' screens.
- **IGMP Snooping Enabled**—Enables or disables IGMP Snooping on the device. This does not appear on all devices' screens.

  Disabled is the default value. Layer 2 switching forwards Multicast packets to all relevant VLAN ports by default, treating the packet as a Multicast transmission. While this is functional, in the sense that all relevant ports/nodes receive a copy of the frame, it is potentially wasteful as ports/nodes may receive irrelevant frames only needed by a subset of the ports of that VLAN. Multicast forwarding filters enable forwarding of Layer 2 packets to port subsets, defined in the Multicast filter database.

  When you enable IGMP snooping globally, the switching ASIC is programmed to forward all IGMP packets to the CPU. The CPU analyzes the incoming packets and determines which ports are to join which Multicast groups, which ports have Multicast routers generating IGMP queries, and what routing protocols are forwarding packets and Multicast traffic. Ports requesting to join a specific Multicast group issues an IGMP report specifying that Multicast group. This results in the creation of the Multicast filtering database.

The following are fields on the editor in the lowest panel. All are mandatory unless otherwise described.

Multicast Table—A read-only view of all the Multicast Services on the system. Double clicking a service, or selecting one and clicking *Edit* edits the selected Service/VLAN.

VLAN ID—A pick list of all current VLANS. Only mandatory if you enable GVRP.

Multicast IP Address—Text, an IP Address or *None*.

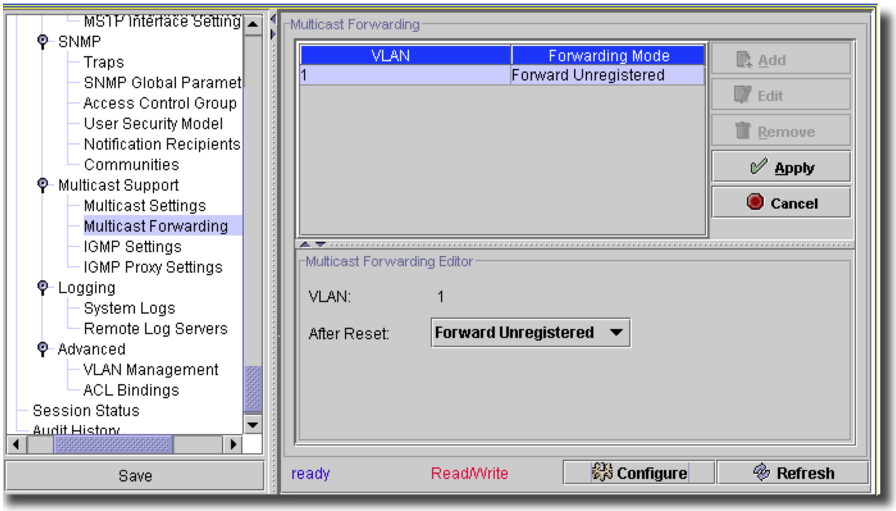
- **Port Assignments**—Click the Right/Left Arrows to assign ports (move from *Available Ports* to *Assigned Ports*) for this multicast. *Reset* restores the original port assignments (from the database), while *Remove All* removes any port assignments you have made.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Multicast -> Multicast Forwarding

This screen manages multicast forwarding for devices that support it.

Figure 13-50. Multicast -> Multicast Forwarding



VLAN	Forwarding Mode
1	Forward Unregistered

VLAN: 1

After Reset: Forward Unregistered

When you *Edit* a forwarding selection, the editor panel appears below. Select one and click *Delete* to remove a row. Click *Apply* to confirm your edits (*Cancel* to abandon them). Here are the fields that appear in the editor:

- **VLAN**—A read-only reminder of the related VLAN.

- **After Reset**—Select from the pick list (*Forward Unregistered*, *Forward All*, *Filter Unregistered*).

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

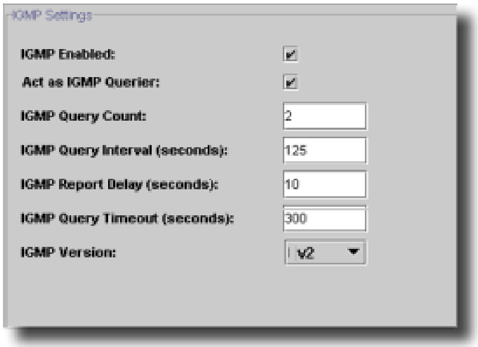
Multicast -> IGMP Settings

This screen lets you manage IGMP. Fields described below do not all appear for all selected devices. Some IGMP screens are as simple as a checkbox (enabling IGMP).

Figure 13-51. IGMP Settings

Possible Screens:

Other Switches ->



IGMP Settings

IGMP Enabled: ☑

Act as IGMP Querier: ☑

IGMP Query Count: 2

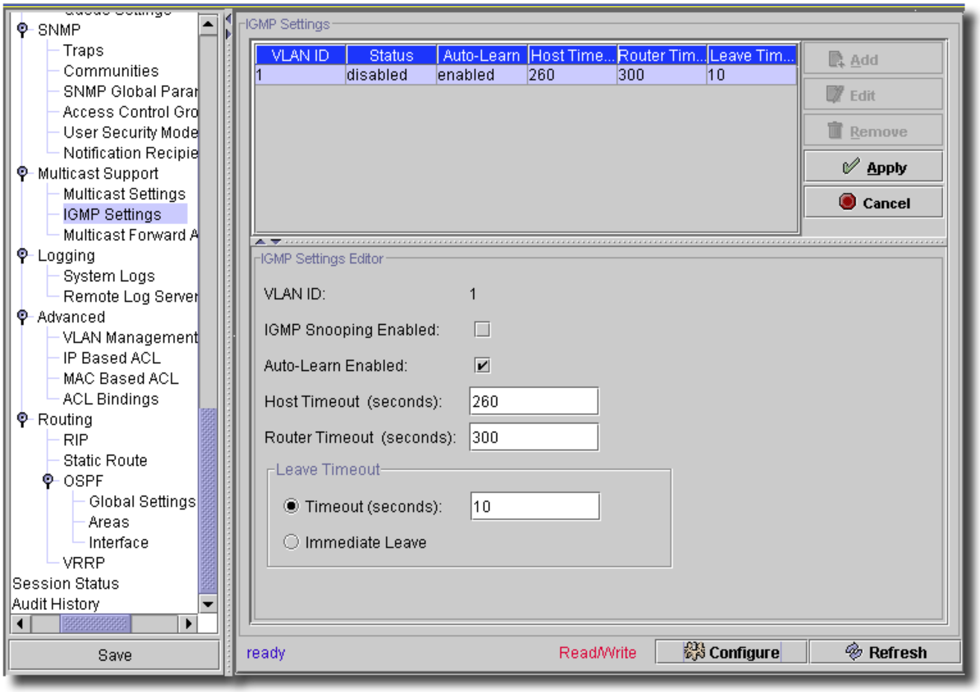
IGMP Query Interval (seconds): 125

IGMP Report Delay (seconds): 10

IGMP Query Timeout (seconds): 300

IGMP Version: v2

5324 / 5316 Switches
|
v



IGMP Settings

VLAN ID	Status	Auto-Learn	Host Time...	Router Tim...	Leave Tim...
1	disabled	enabled	260	300	10

IGMP Settings Editor

VLAN ID: 1

IGMP Snooping Enabled: □

Auto-Learn Enabled: ☑

Host Timeout (seconds): 260

Router Timeout (seconds): 300

Leave Timeout

● Timeout (seconds): 10

○ Immediate Leave

Click *Add* (or *Edit* when you select an address listed) to open the editor on the lower panel. Click *Apply* to enter an listed item you have edited, or *Cancel* to abandon your edits. Not all fields appear for all devices. All fields are mandatory. This screen has settings for the following (described when not self-explanatory):

Fields for switches other than 5324 / 5316

- **IGMP Enabled**—Checkbox.

- **Act as IGMP Querier**—Checkbox.

- **IGMP Query Count**—Valid Values: 2 - 10

- **IGMP Query Interval**—Valid Values: 60 - 125

- **IGMP Report Delay**—Valid Values: 5 - 30

- **IGMP Query Timeout**—Valid Values: 300 - 500

- **IGMP Version**—Select from pick list.

Fields for 5324 / 5316 switches

Click *Remove* to delete a selected, listed setting. Click *Add* (or select an existing setting and click *Edit*) to open the editor in the bottom panel. Click *Apply* to accept your edits (and list the settings in the top of the screen), or *Cancel* to abandon them. The editor has the following fields:

- **VLAN ID**—A read-only field displaying the VLAN ID for the selected item.

- **IGMP Snooping Enabled**—Check to enable.

- **Auto-Learn Enabled**—Check to enable.

- **Host Timeout (seconds)**—Enter a timeout.

- **Multicast Router Timeout (seconds)**—Enter a timeout.

Leave Timeout

- **Timeout (seconds)**—Enter a timeout.

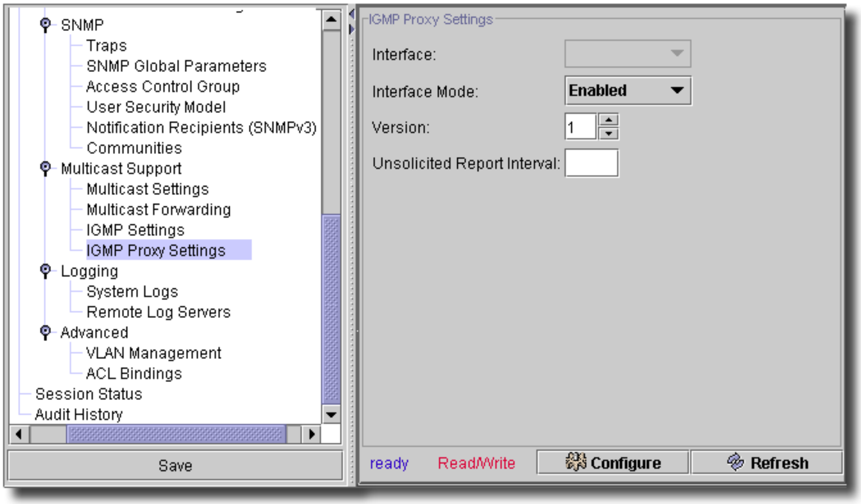
- **Immediate Leave**—Select this radio button for immediate leaving.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Multicast -> IGMP Settings

This screen manages IGMP proxy settings for the selected device.

Figure 13-52. Multicast -> IGMP Proxy Settings



Interface:

Interface Mode: Enabled

Version: 1

Unsolicited Report Interval:

You must have configured at least one router interface before configuring or displaying data for an IGMP proxy interface, and it should not be an IGMP routing interface. This screen has the following fields:

- **Interface**—A read-only reminder of the IGMP proxy interface.

- **Interface Mode**—Select from the pick list (*Enabled / Disabled*). The default is *Disabled*. Routing, IGMP, and Multicast global admin modes should be enabled to enable IGMP Proxy interface mode.

- **Version**—Select an IGMP version from the spinner (valid values: 1,2,3)

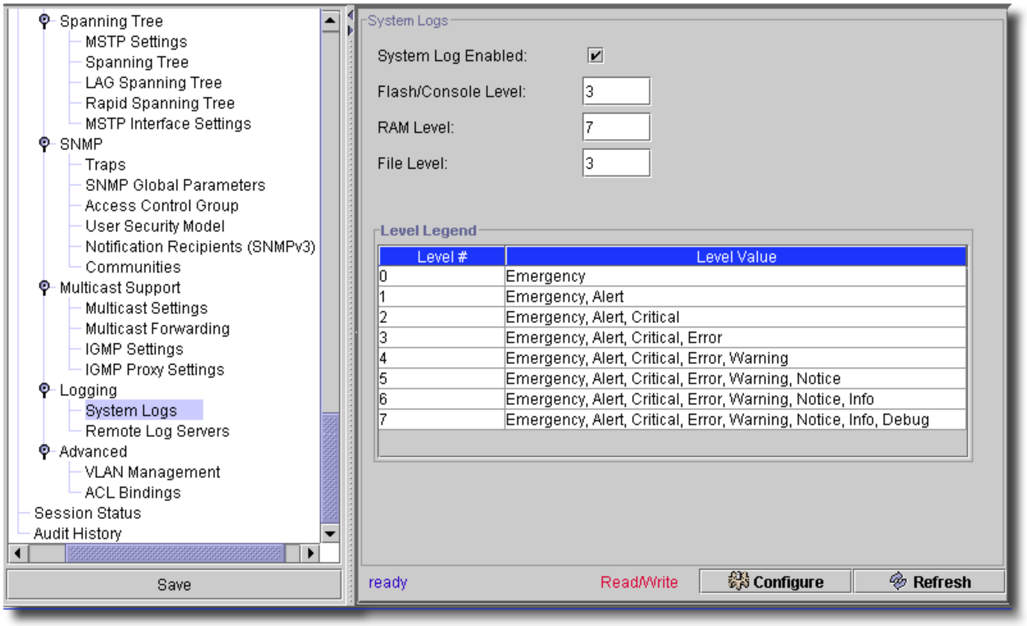
- **Unsolicited Report Interval**—Enter the unsolicited time interval value in seconds. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Valid values are from 1 to 260. The default value is 1.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Logging -> System Logs

This screen lets you manage System Logging.

Figure 13-53. System Logs



System Logs

System Log Enabled: ☑

Flash/Console Level: 3

RAM Level: 7

File Level: 3

Level Legend

Level #	Level Value
0	Emergency
1	Emergency, Alert
2	Emergency, Alert, Critical
3	Emergency, Alert, Critical, Error
4	Emergency, Alert, Critical, Error, Warning
5	Emergency, Alert, Critical, Error, Warning, Notice
6	Emergency, Alert, Critical, Error, Warning, Notice, Info
7	Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug

The following are fields on this screen. They are all mandatory:

- **System Log Enabled**—Checkbox.

- **Flash Level**—Valid Values: 0-7

- **RAM Level**—Valid Values: 0-7

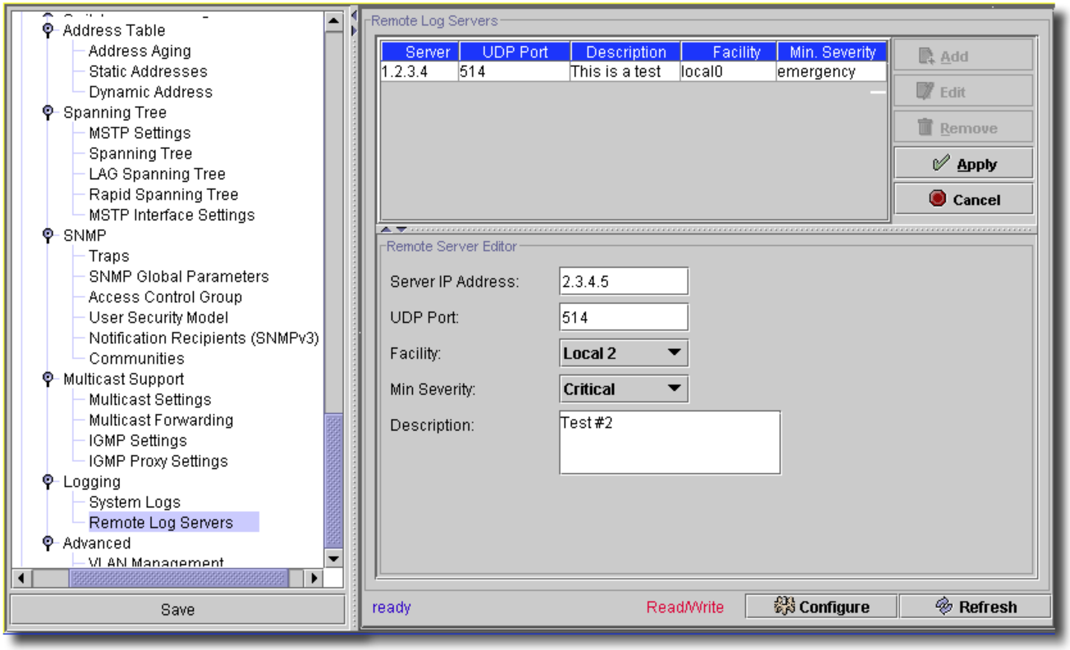
- **File Level**—Appears on some screens.

The *Level Legend* is there to remind you of the values for levels selected above. The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Logging -> Remote Log Servers

This screen lets you manage Remote Logging.

Figure 13-54. Remote Logs



Remote Log Servers

Server	UDP Port	Description	Facility	Min. Severity
1.2.3.4	514	This is a test	local0	emergency

Remote Server Editor

Server IP Address: 2.3.4.5

UDP Port: 514

Facility: Local 2

Min Severity: Critical

Description: Test #2

Click *Add* (or *Edit* when you select a log facility listed) to open the editor on the lower panel. Click *Apply* to enter an listed item you have edited, or *Cancel* to abandon your edits. Not all fields appear for all devices. This screen has settings for the following:

- **Server IP Address/UDP Port**—The IP address and port of the log server.

- **Facility**—Select from the pick list.

- **Min Severity**—Select from the pick list.

- **Description**—A text description of the remote logging facility.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

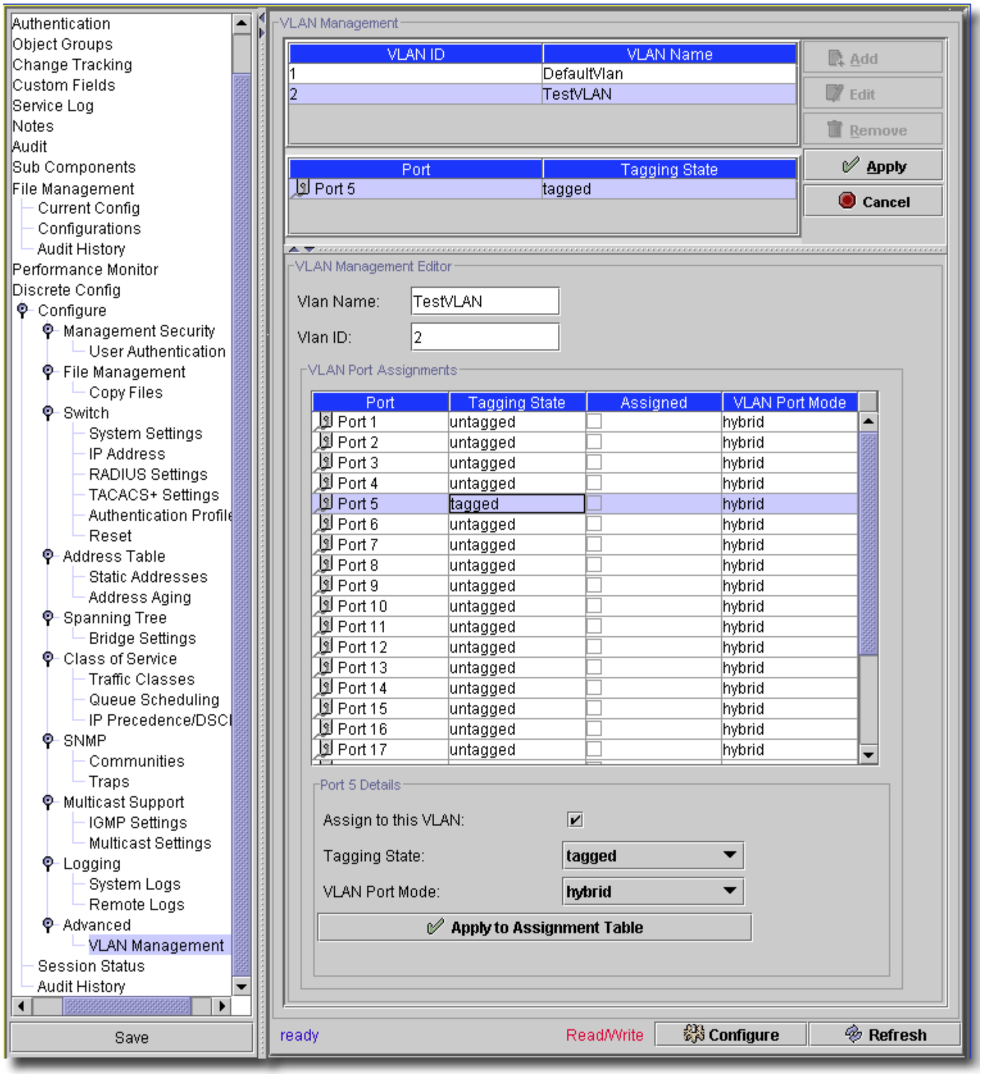
Policy

You can manage policies on your Dell devices with its policy module. Use the *Settings -> Permissions -> Register License* menu item to open a dialog that lets you locate the license file. Select the file, and click Register License in the dialog, and you can use the licensed product. The *Settings -> Permissions -> View License* menu lets you see what is already registered.

Advanced -> VLAN Management

VLAN Management lets you assign an interface to any VLAN except the default interface. This also lets you change the interface VLAN mode—*Trunk* or *Access*—and the Tagging state.

Figure 13-55. Policy: VLAN Management.



VLAN ID	VLAN Name
1	DefaultVlan
2	TestVLAN

Port	Tagging State
Port 5	tagged

Vlan Name: TestVLAN

Vlan ID: 2

Port	Tagging State	Assigned	VLAN Port Mode
Port 1	untagged	□	hybrid
Port 2	untagged	□	hybrid
Port 3	untagged	□	hybrid
Port 4	untagged	□	hybrid
Port 5	tagged	□	hybrid
Port 6	untagged	□	hybrid
Port 7	untagged	□	hybrid
Port 8	untagged	□	hybrid
Port 9	untagged	□	hybrid
Port 10	untagged	□	hybrid
Port 11	untagged	□	hybrid
Port 12	untagged	□	hybrid
Port 13	untagged	□	hybrid
Port 14	untagged	□	hybrid
Port 15	untagged	□	hybrid
Port 16	untagged	□	hybrid
Port 17	untagged	□	hybrid

Port 5 Details

Assign to this VLAN: ☑

Tagging State: tagged

VLAN Port Mode: hybrid

Select a VLAN in the top left panel, then a port in the middle panel and click *Edit* (or simply click *New* without selecting a VLAN). The ports and their tagged state appear in an editor. Click A*pply* to confirm your edits (*Cancel* to abandon them). Click *Configure* to implement your edits; *Refresh* to re-query the database for them. Select a listed VLAN and click *Remove* to delete it from the list.

NOTE:

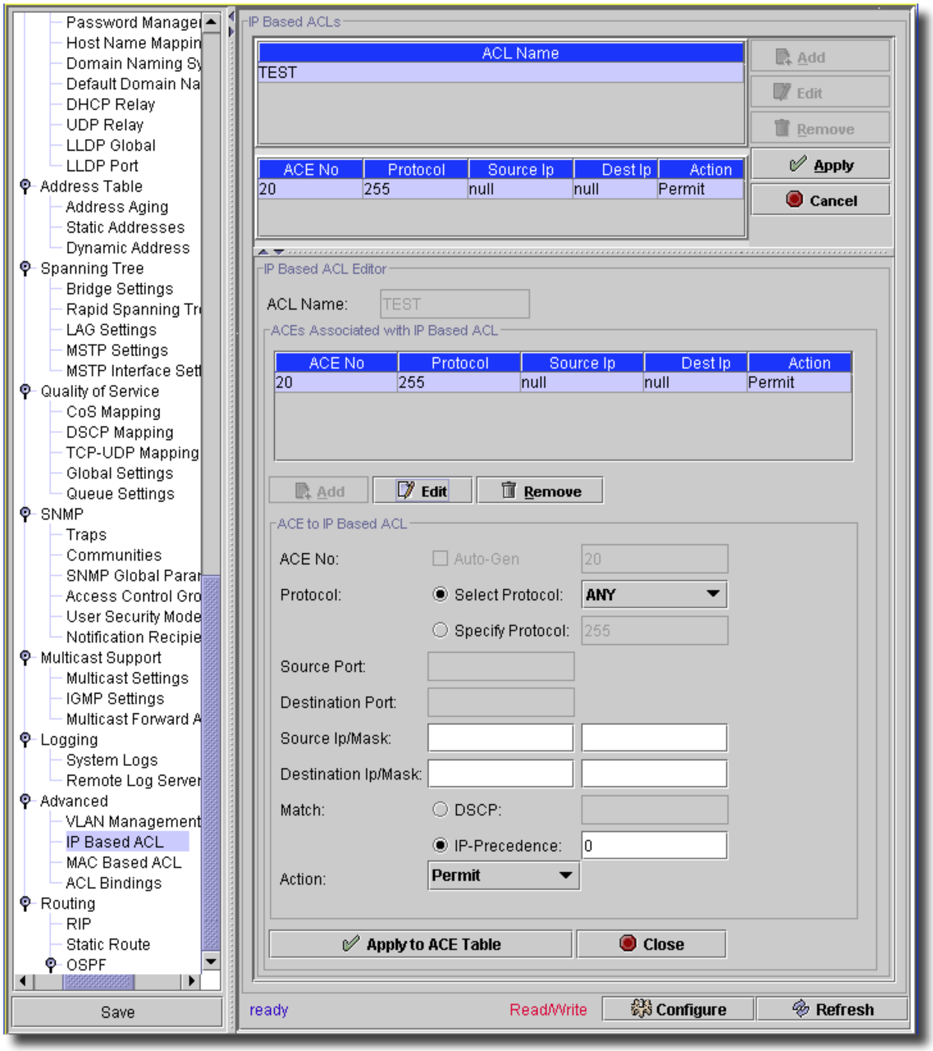
You can modify only the name for the default VLAN

The screens below are not available for all equipment.

Advanced -> IP Based ACL

This screen (not available on all devices) lets you determine access control lists based on IP addresses. Here, you can associate multiple ACEs to the ACL. The source and destination port fields are enabled only when you select TCP or UDP as the protocol.

Figure 13-56. IP Based ACL.



ACL Name
TEST

ACE No	Protocol	Source Ip	Dest Ip	Action
20	255	null	null	Permit

ACL Name: TEST

ACE No	Protocol	Source Ip	Dest Ip	Action
20	255	null	null	Permit

ACE No: □ Auto-Gen 20

Protocol: ● Select Protocol: ANY

○ Specify Protocol: 255

Source Port:

Destination Port:

Source Ip/Mask:

Destination Ip/Mask:

Match: ○ DSCP:

● IP-Precedence: 0

Action: Permit

ready Read/Write

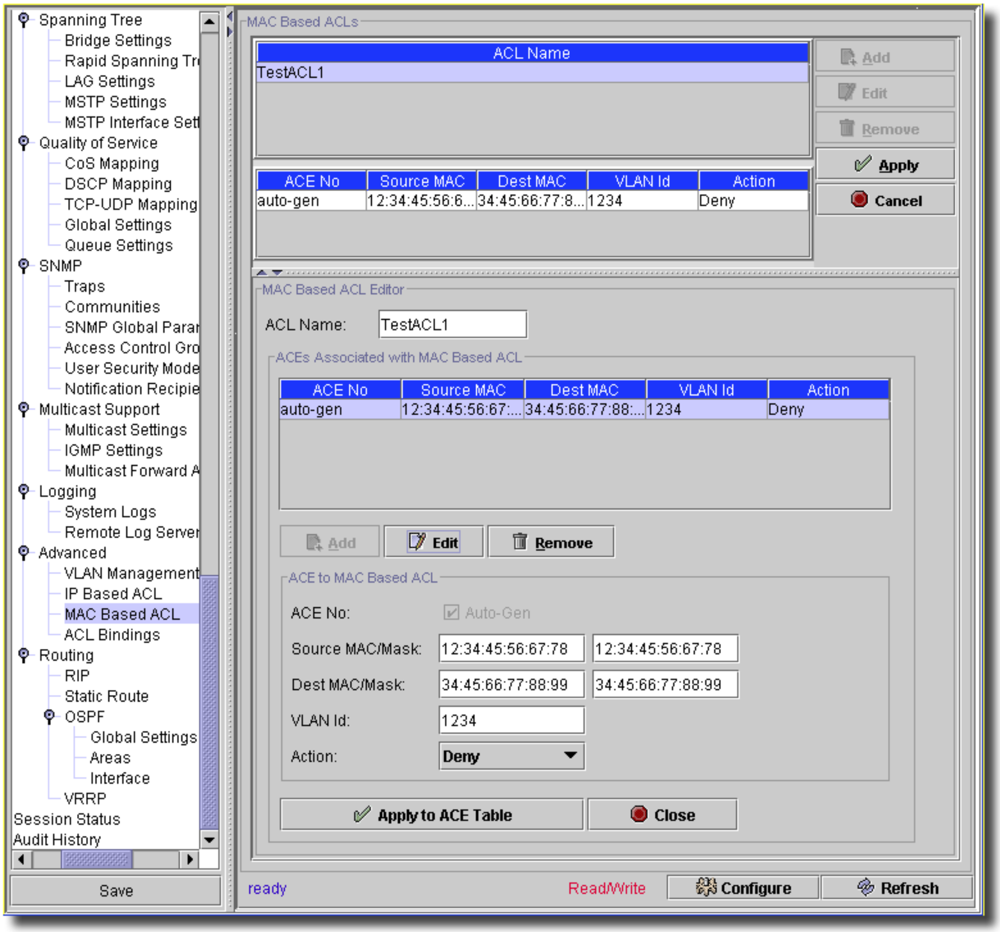
In this screen you can *Add*, *Edit* and *Remove* IP-based ACLs listed in the upper panel. Select the listed properties below these, click *Add* or *Edit*, and an editor appears where you can add or alter the *ACE No*, *Protocol*, *Source IP*, *Destination IP*, and *Action*. *Source Port* and *Destination Port* are enabled when you select *TCP* or *UDP* protocols. Click *Remove* to delete a selected, listed item.

Click *Apply* to confirm your edits (*Cancel* to abandon them). Click *Configure* to implement your edits; *Refresh* to re-query the database for them. This screen appears for some, but not all, devices.

Advanced -> MAC Based ACL

You can use the following screen to manage MAC based access control lists, and associated multiple ACEs.

Figure 13-57. MAC-based Access Control Lists



ACL Name
TestACL1

ACE No	Source MAC	Dest MAC	VLAN Id	Action
auto-gen	12:34:45:56:6...	34:45:66:77:8...	1234	Deny

ACL Name: TestACL1

ACE No	Source MAC	Dest MAC	VLAN Id	Action
auto-gen	12:34:45:56:67:...	34:45:66:77:88:...	1234	Deny

ACE No: ☑ Auto-Gen

Source MAC/Mask: 12:34:45:56:67:78 12:34:45:56:67:78

Dest MAC/Mask: 34:45:66:77:88:99 34:45:66:77:88:99

VLAN Id: 1234

Action: Deny

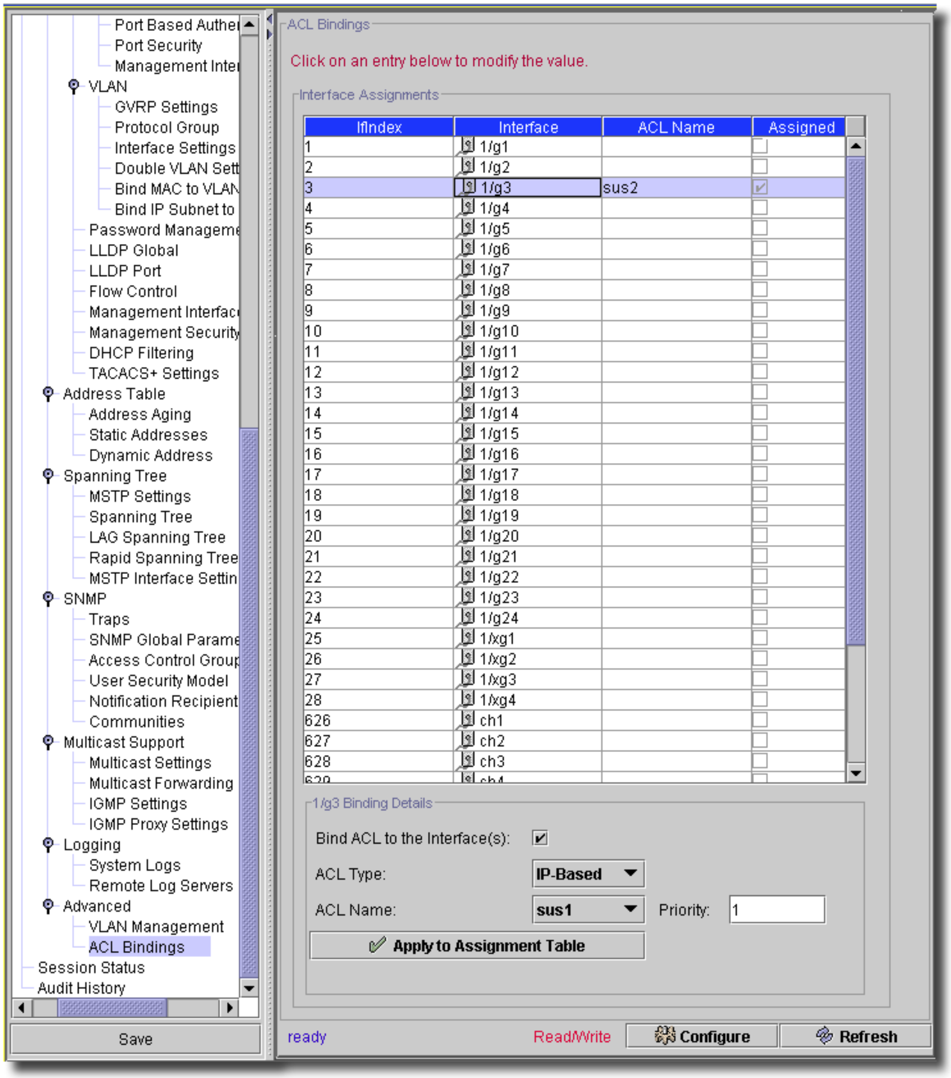
Select a listed ACL in the upper panel, and the listed details in the lower panels. You can *Add*, *Edit*, or *Remove* a listed ACL. When you *Add* or *Edit* a selected ACL, an editor appears where you can enter the *ACL Name*. Click *Add* (or *Edit* for existing ACE/Mac combinations) to enter the *ACE No* (or check *Auto Gen*) and the *Destination MAC*. Click *Apply to ACE Table* to accept the lowest panel's edits. Click *Remove* to delete a selected, listed item.

Click *Apply* to confirm your edits to the ACL (*Cancel* to abandon them). Click *Configure* to implement your edits; *Refresh* to re-query the database for them. This screen appears for some, but not all, devices.

Advanced -> ACL Bindings

This screen lists the bindings for Access Control Lists. You can use this screen to associate IP or MAC-based ACLs to Interfaces (*Port*, *LAG*, *VLAN*), or to unassociate them from the ACL. You can specify either *IP-Based* or *MAC-Based* ACLs with the pick box below the listed bindings.

Figure 13-58. Access Control List Binding



Click on an entry below to modify the value.

IfIndex	Interface	ACL Name	Assigned
1	1/g1		□
2	1/g2		□
3	1/g3	sus2	☑
4	1/g4		□
5	1/g5		□
6	1/g6		□
7	1/g7		□
8	1/g8		□
9	1/g9		□
10	1/g10		□
11	1/g11		□
12	1/g12		□
13	1/g13		□
14	1/g14		□
15	1/g15		□
16	1/g16		□
17	1/g17		□
18	1/g18		□
19	1/g19		□
20	1/g20		□
21	1/g21		□
22	1/g22		□
23	1/g23		□
24	1/g24		□
25	1/xg1		□
26	1/xg2		□
27	1/xg3		□
28	1/xg4		□
626	ch1		□
627	ch2		□
628	ch3		□
629	ch4		□

Bind ACL to the Interface(s): ☑

ACL Type: IP-Based

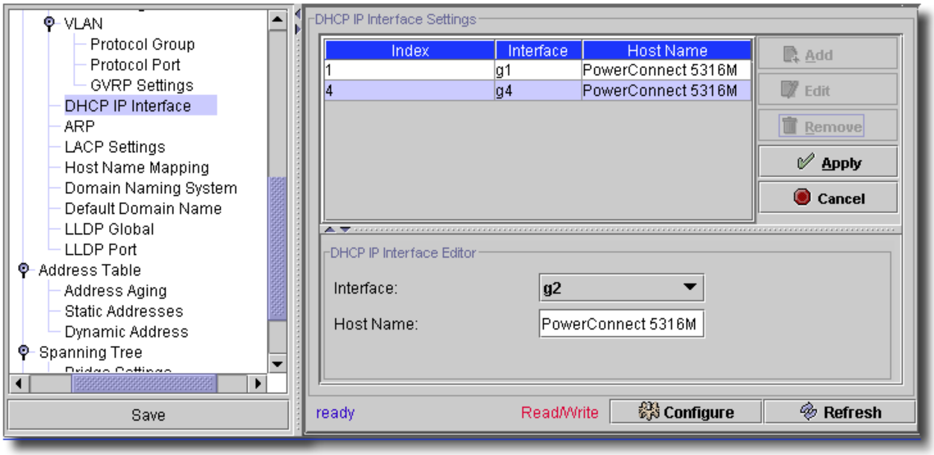
ACL Name: sus1 Priority: 1

This table lists the *IfIndex*, *Interface*, *ACL Name* and whether it is *Assigned*. The *Refresh* button updates the screen. Click *Apply to Assignment Table* to confirm your edits; click *Configure* to deploy them. This screen appears for some, but not all, devices.

DHCP IP Interface Parameters

The DHCP IP Interface screen configures the DHCP clients connected to the 34xx switch module.

Figure 13-59. DHCP IP Parameters



DHCP IP Interface Settings

Index	Interface	Host Name
1	g1	PowerConnect 5316M
4	g4	PowerConnect 5316M

DHCP IP Interface Editor

Interface: g2

Host Name: PowerConnect 5316M

You can *Edit* DHCP IP Interface settings for the selected device in this screen. When you select an existing interface listed in the upper portion of the screen and click *Edit* the Editor opens (the lower portion of the screen) with the following fields:

- **Interface**—Choose the specific interface connected to the switch module -Port, LAG, or VLAN.

- **Host Name**—The system name. This field can contain up to 20 characters.

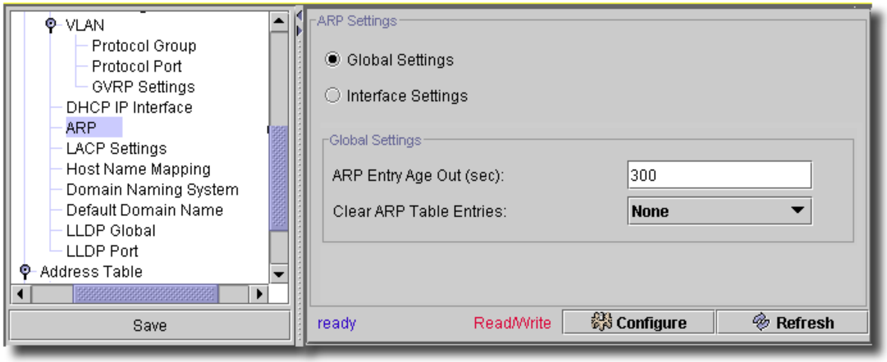
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

ARP

The Address Resolution Protocol (ARP) converts IP addresses into physical addresses, and maps the IP address to a MAC address. ARP allows a host to communicate with other hosts only when the IP address of its neighbors is known.

Figure 13-60. ARP Settings



ARP Settings

● Global Settings

○ Interface Settings

Global Settings

ARP Entry Age Out (sec): 300

Clear ARP Table Entries: None

- The ARP Settings screen contains the following fields:

- **Global Settings/Interface Settings**—Select this option to activate the fields for ARP global settings.

- **ARP Entry Age Out (sec)** (1-40000000)—Before the entry is deleted from the table. The range is 1 - 4000000. Zero indicates that entries are never cleared from the cache. The default value is 60000 seconds.

- **Clear ARP Table Entries**—The type of ARP entries that are cleared on all Ethernet switch module s. The possible values are:

None—ARP entries are not cleared.

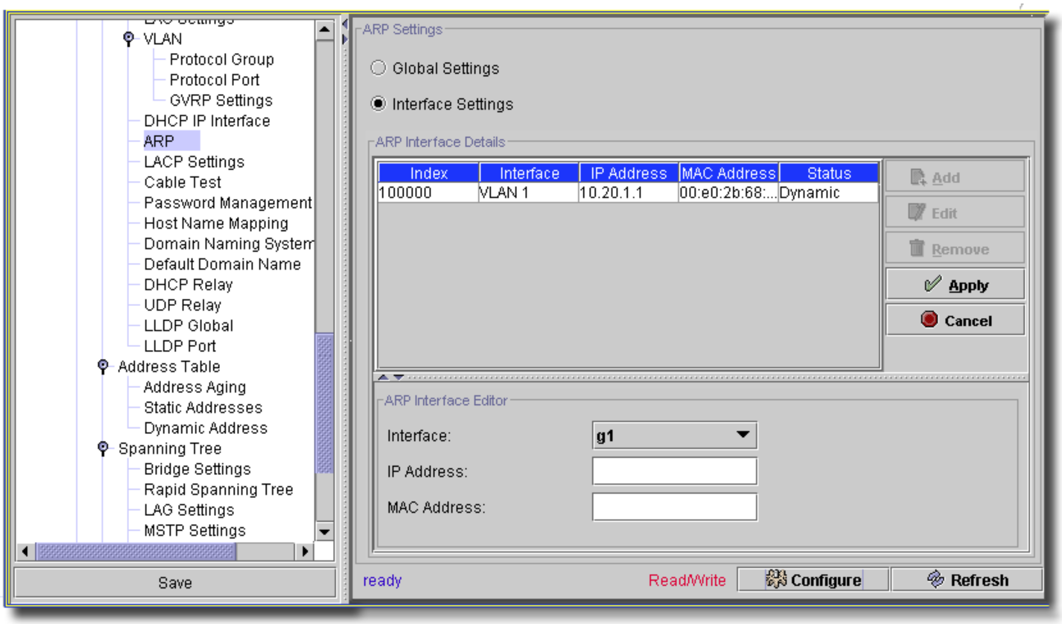
All—All ARP entries are cleared.

Dynamic—Only dynamic ARP entries are cleared.

Static—Only static ARP entries are cleared.

- **Interface Settings**—Select this option to activate the fields for ARP settings on a single Ethernet switch module.

Figure 13-61. ARP Interface Settings



ARP Settings

○ Global Settings

● Interface Settings

ARP Interface Details

Index	Interface	IP Address	MAC Address	Status
100000	VLAN 1	10.20.1.1	00:e0:2b:68:...	Dynamic

ARP Interface Editor

Interface: g1

IP Address:

MAC Address:

ready Read/Write

You can *Edit* ARP Interface settings for the selected device in this screen. Click *Add* to create a new group of settings, or select an existing interface listed in the upper portion of the screen and click *Edit* the editor opens (the lower portion of the screen) with the following fields:

- **Interface**—The interface number of the port, LAG, or VLAN that is connected to the Ethernet switch module.
- **IP Address**—The station IP address, which is associated with the MAC address filled in below.
- **MAC Address**—The station MAC address, which is associated in the ARP table with the IP address.
- **Status**—The ARP Table entry status. (*Static* or *Dynamic*)

NOTE:

This screen is not available for all equipment.

Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

LACP Settings

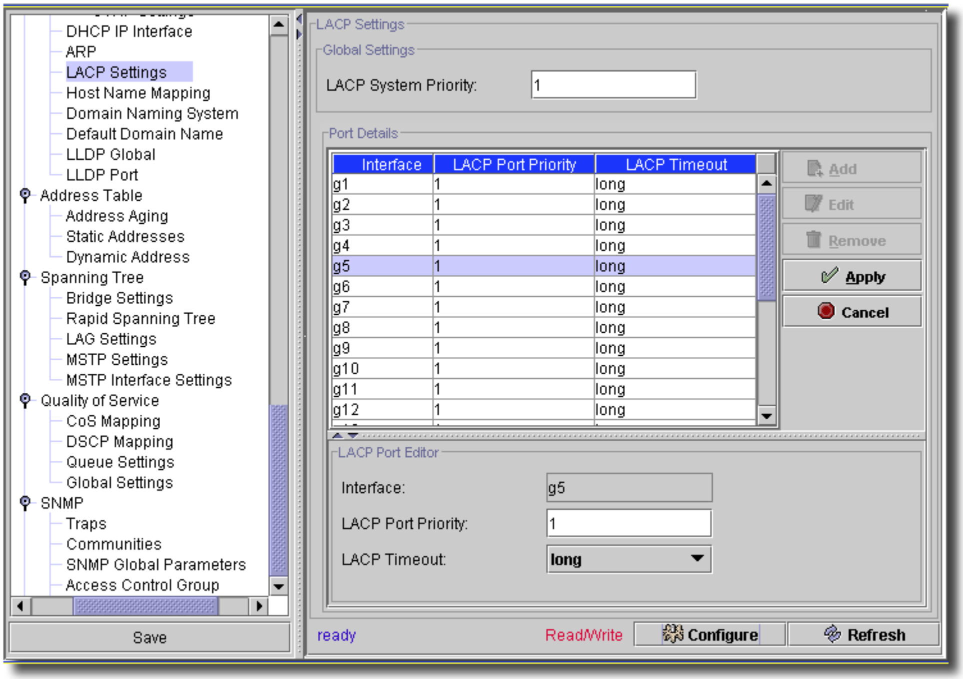
The Link Aggregation Control Protocol (LACP) Settings screen contains information for configuring LACP LAGs. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed.

NOTE:

This setting is applicable only for external ports.

Aggregated Links can be manually setup or automatically established by enabling LACP on the relevant links.

Figure 13-62. LACP Settings



LACP System Priority: 1

Interface	LACP Port Priority	LACP Timeout
g1	1	long
g2	1	long
g3	1	long
g4	1	long
g5	1	long
g6	1	long
g7	1	long
g8	1	long
g9	1	long
g10	1	long
g11	1	long
g12	1	long

Interface: g5

LACP Port Priority: 1

LACP Timeout: long

Click *Remove* to delete a selected, listed item. You can *Edit* LACP settings for the selected device in this screen.

- **LACP System Priority (1-65535)**—The LACP priority value for global settings.

Click *Add* to create a new group of settings, or select an existing interface listed in the upper portion of the screen and click *Edit* the editor opens (the lower portion of the screen) with the following fields:

- **Select a Port**—The port number to which timeout and priority values are assigned. (does not appear for all devices)

- **Interface**—The interface number to which timeout and priority values are assigned. (does not appear for all devices)
- **LACP Port Priority (1-65535)**—LACP priority value for the port.
- **LACP Timeout**—Administrative LACP timeout. (*Short*, *Long*).

NOTE:

This screen is not available for all equipment.

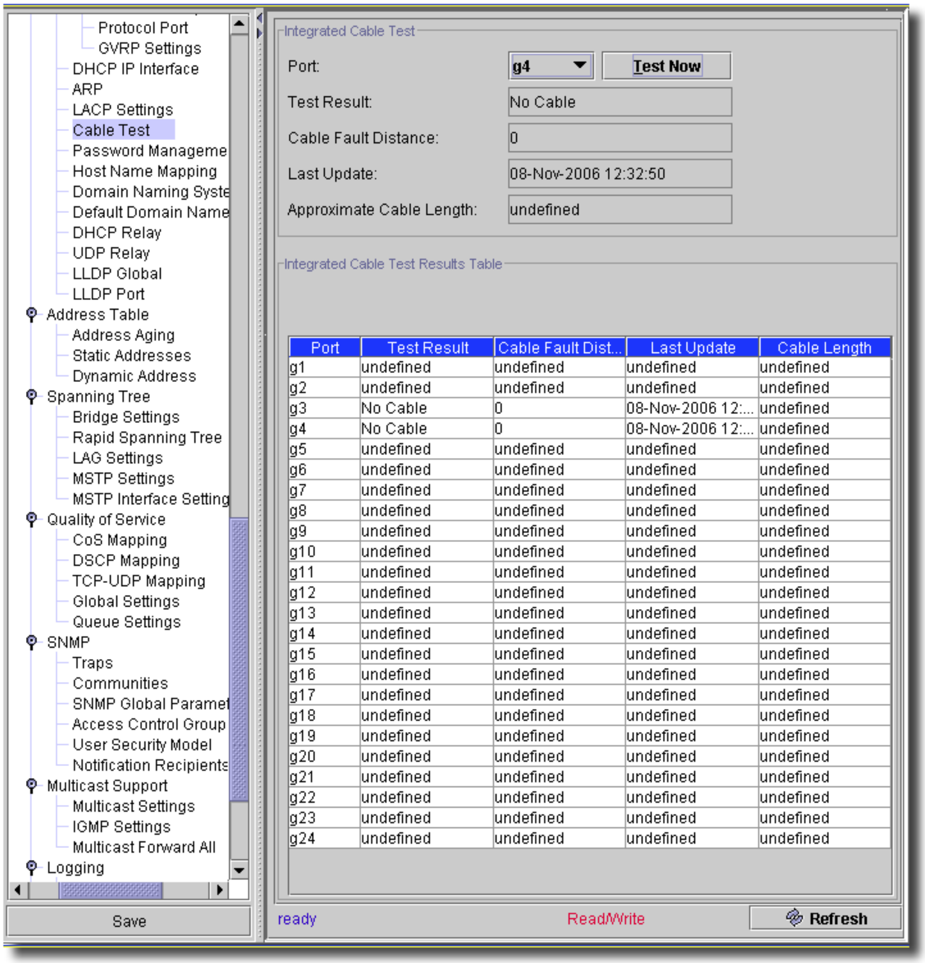
Click A*pply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Cable Test

This screen lets you perform a cable test on ports on the selected equipment.

Figure 13-63. Cable Test



Integrated Cable Test

Port: g4

Test Result: No Cable

Cable Fault Distance: 0

Last Update: 08-Nov-2006 12:32:50

Approximate Cable Length: undefined

Integrated Cable Test Results Table

Port	Test Result	Cable Fault Dist...	Last Update	Cable Length
g1	undefined	undefined	undefined	undefined
g2	undefined	undefined	undefined	undefined
g3	No Cable	0	08-Nov-2006 12:...	undefined
g4	No Cable	0	08-Nov-2006 12:...	undefined
g5	undefined	undefined	undefined	undefined
g6	undefined	undefined	undefined	undefined
g7	undefined	undefined	undefined	undefined
g8	undefined	undefined	undefined	undefined
g9	undefined	undefined	undefined	undefined
g10	undefined	undefined	undefined	undefined
g11	undefined	undefined	undefined	undefined
g12	undefined	undefined	undefined	undefined
g13	undefined	undefined	undefined	undefined
g14	undefined	undefined	undefined	undefined
g15	undefined	undefined	undefined	undefined
g16	undefined	undefined	undefined	undefined
g17	undefined	undefined	undefined	undefined
g18	undefined	undefined	undefined	undefined
g19	undefined	undefined	undefined	undefined
g20	undefined	undefined	undefined	undefined
g21	undefined	undefined	undefined	undefined
g22	undefined	undefined	undefined	undefined
g23	undefined	undefined	undefined	undefined
g24	undefined	undefined	undefined	undefined

ready   Read/Write

Select a *Port* from the pick list and click *Test Now*. This displays the *Test Result*, *Cable Fault Distance*, *Last Update*, and *Approximate Cable Length*. The results of any previous tests appear in the *Integrated Test Results Table*.

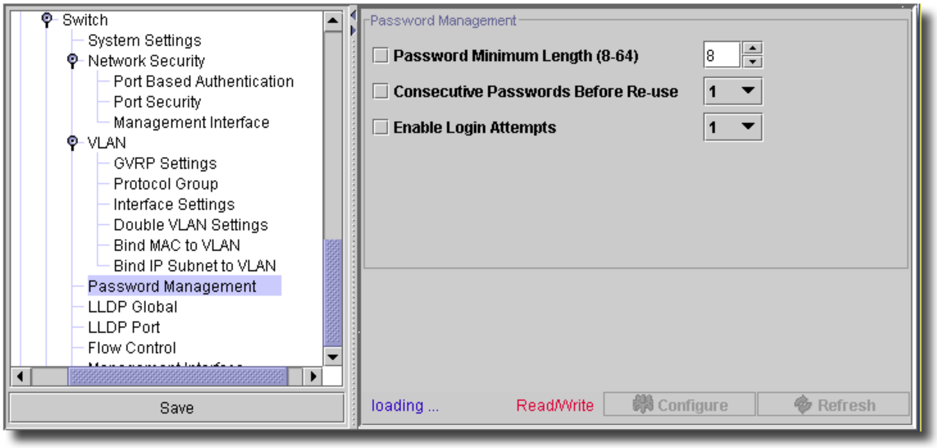
NOTE:

This screen is not available for all equipment.

Password Management

This screen lets you configure password management settings for some devices.

Figure 13-64. Password Management



Password Management

□ **Password Minimum Length (8-64)** 8

□ **Consecutive Passwords Before Re-use** 1

□ **Enable Login Attempts** 1

It has the following fields (checkboxes enable the fields):

- **Password Minimum Length** (8-64)—Enter a number or use the spinners.

- **Consecutive Passwords Before Re-use**—Select a number with the pick list.

- **Enable Login Attempts**—Select a number with the pick list.

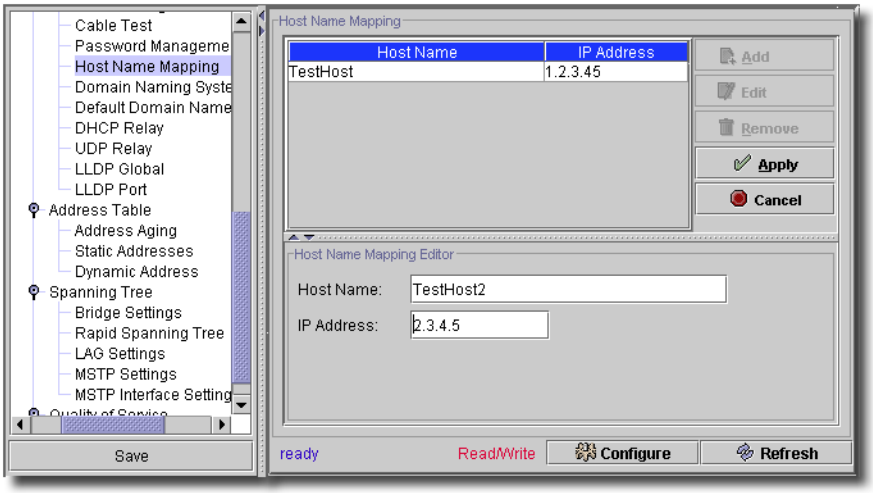
- **Enable Password Aging**—Enter the days until expiration. (Does not appear for all devices.)

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Host Name Mapping

This screen manages host name mapping for some selected devices.

Figure 13-65. Host Name Mapping



Host Name Mapping

Host Name	IP Address
TestHost	1.2.3.45

Host Name Mapping Editor

Host Name: TestHost2

IP Address: 2.3.4.5

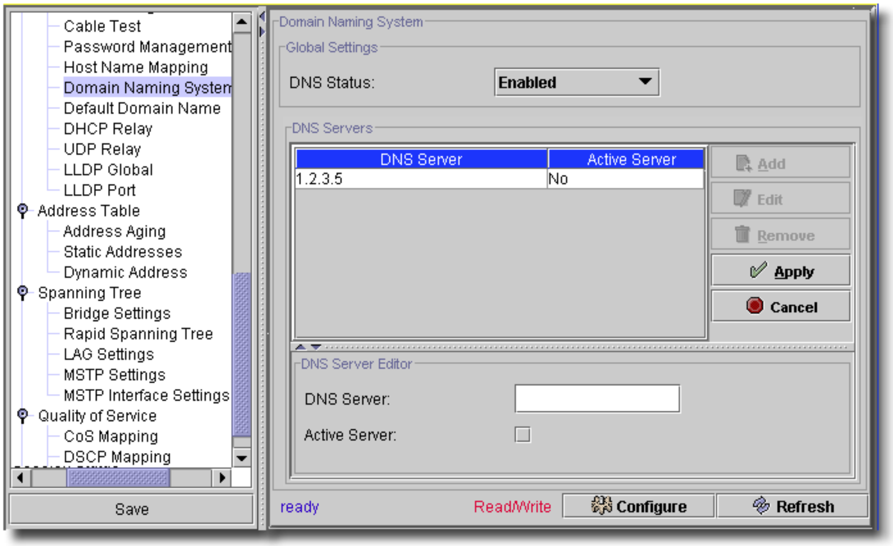
Host Names and their corresponding *IP address* appear in a list at the top of this screen. To add a new hostname/IP pair, click *Add*, or click *Edit* to alter an existing selected pair, and the editor appears at the bottom of the screen with the two fields to create or alter. Click *Remove* to delete a selected, listed item. Click *Apply* to accept your edits, or *Cancel* to abandon them.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Domain Naming System

This screen manages domain naming for some selected devices.

Figure 13-66. Domain Naming System



DNS Status: Enabled

DNS Server	Active Server
1.2.3.5	No

DNS Server:

Active Server: □

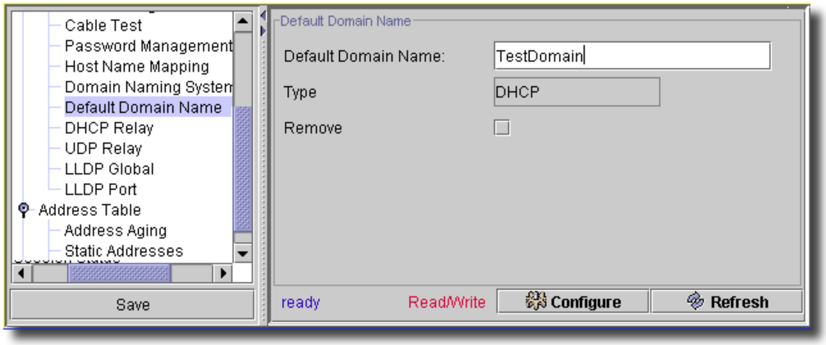
Under *Global Settings* elect whether the *DNS Status* is *Enabled / Disabled*. DNS servers appear listed under this. To create new servers (alter an existing one), click *Add* (or select a listed server and click *Edit*). The *DNS Server Editor* appears with a field where you can enter the *DNS Server* IP address, and, in some screens, a checkbox to check if you want this one to be active. Click *Remove* to delete a selected, listed item. Click *Apply* to confirm your edits, or *Cancel* to abandon them.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Default Domain Name

This screen configures the default domain name for some selected equipment.

Figure 13-67. Default Domain Name



Default Domain Name

Default Domain Name: TestDomain

Type DHCP

Remove ☐

This screen has the following fields:

- **Default Domain Name**—The domain name you want to be the default.

- **Type**—This read-only field displays the type. For example, DHCP.

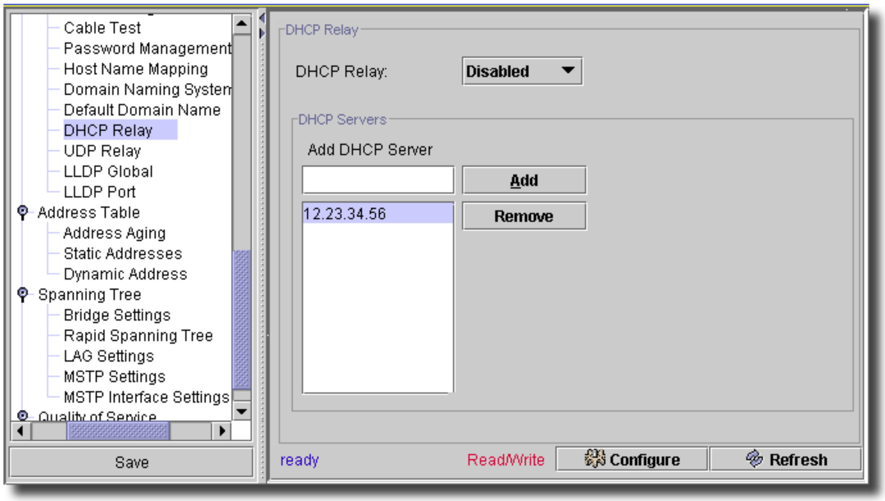
- **Remove**—Check this to remove the domain default.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

DHCP Relay

This screen configures DHCP relay for the selected device.

Figure 13-68. DHCP Relay



DHCP Relay

DHCP Relay: Disabled

DHCP Servers

Add DHCP Server

12.23.34.56

This screen has the following fields:

- **DHCP Relay**—Select from *Enabled / Disabled*.

DCHP Servers

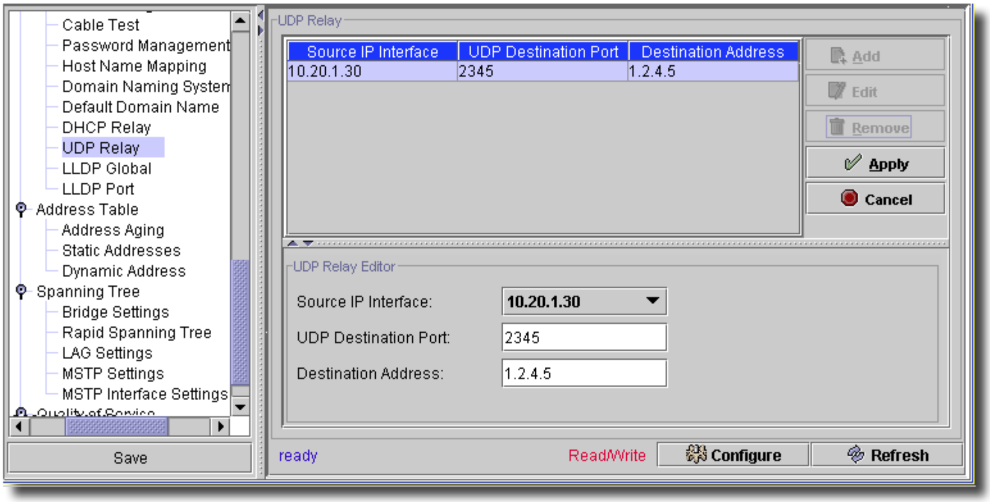
Enter a DHCP server in the blank field next to *Add*, then click that button to list one here. Select a listed server and click *Remove* to delete it from the list.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

UDP Relay

This screen controls UPD relay characteristics for the selected equipment.

Figure 13-69. UDP Relay



Source IP Interface	UDP Destination Port	Destination Address
10.20.1.30	2345	1.2.4.5

Source IP Interface: 10.20.1.30

UDP Destination Port: 2345

Destination Address: 1.2.4.5

To create a new relay, or configure an existing selected one, click *Add*, or *Edit*, respectively. Once you select a listed relay, you can click *Remove* to delete it from the list. When you are adding or editing a relay, the following fields appear in the editor below the list:

- **Source IP Interface**—Select from those on the device in the pick list.

- **UPD Destination Port**—Enter a destination port number (1 - 65535).

- **Destination Address**—Enter the IP address of a permitted destination.

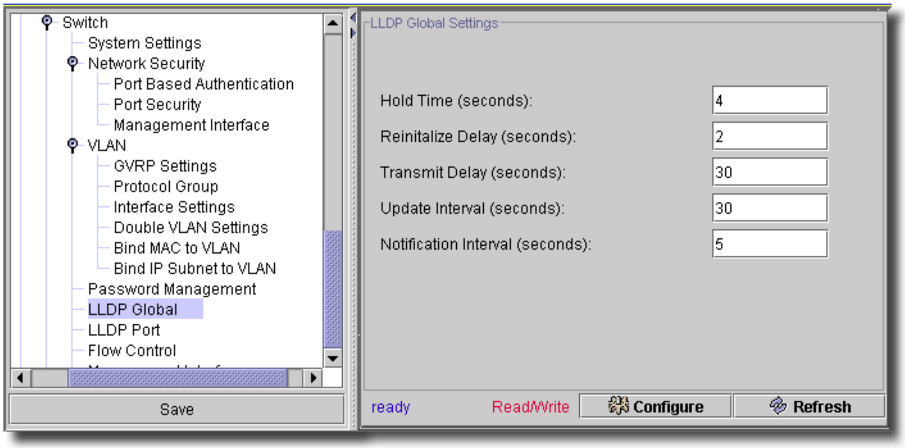
Click *Apply* to accept your edits, or *Cancel* to abandon them. Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

LLDP Global

LLDP (Link Layer Discovery Protocol) discovers network neighbors by standardizing methods for network devices to advertise themselves to other system, and to store discovered information. Device discovery information includes Device Identification, Device Capabilities, and Device Configuration.

The advertising device transmits multiple advertisement message sets in a single LAN packet. The multiple advertisement sets are sent in the packet Type Length Value (TLV) field. LLDP devices must support chassis and port ID advertisement, as well as system name, system ID, system description, and system capability advertisements. This screen configures LLDP global settings for the selected equipment.

Figure 13-70. LLDP Global



Hold Time (seconds): 4

Reinitalize Delay (seconds): 2

Transmit Delay (seconds): 30

Update Interval (seconds): 30

Notification Interval (seconds): 5

This screen has the following fields:

- **LLDP Enabled**—Check to enable LLDP. (Does not appear for all devices)
- **Hold Time (seconds)**—The period that LLDP packets are held before they are discarded. The possible field range is 2 - 10 seconds. The field default is 4 seconds. Does not appear on all devices.
- **Hold Multiplier**—Specifies multiplier on the transmit interval to assign to TTL. Default is 4 seconds (2 - 10). Does not appear on all devices.
- **Reinitialize Delay (seconds)**—The time between disabling LLDP and when reinitializing begins. The possible field range is 1 - 10 seconds. The field default is 2.
- **Transmit Delay (seconds)**—The time between successive LLDP frame transmissions due to changes in the LLDP local systems MIB. The possible field value is 0 - 32768 seconds. The field default is 30 seconds.
- **Update Interval (seconds)**—Indicates that rate at which LLDP advertisement updates are sent. The possible field range is 5 - 3276 seconds. The default value is 30 seconds.

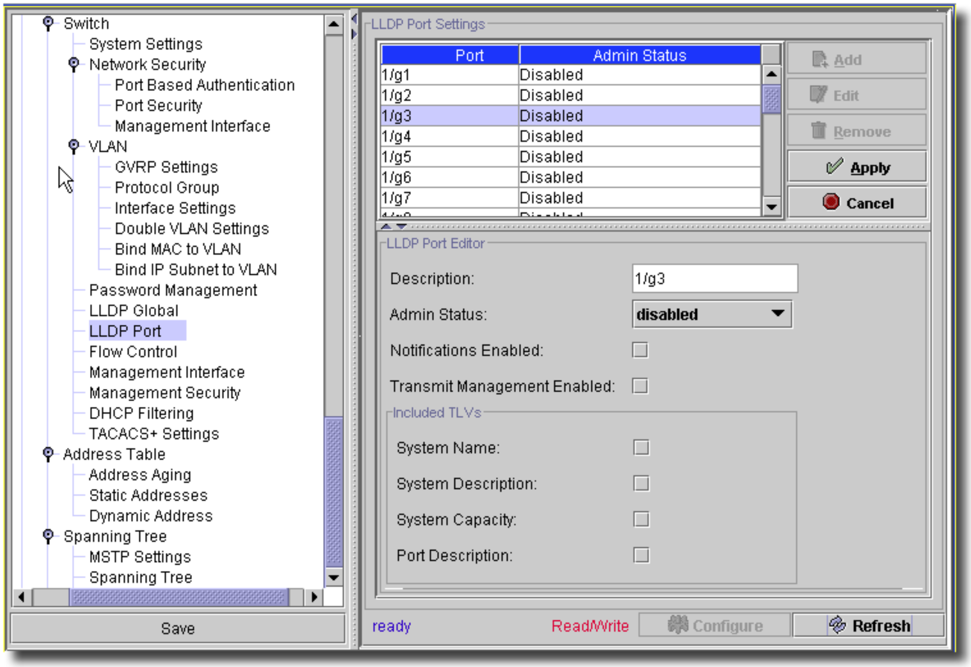
- **Notification Interval (seconds)**—Indicates that rate at which LLDP notifications are sent. The possible field range is 5 - 3600 seconds. The default value is 5 seconds. (Does not appear for all devices)

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

LLDP Port

The LLDP Port Settings let you define port types, states, and the type of information advertised for ports selected.

Figure 13-71. LLDP Port



Port	Admin Status
1/g1	Disabled
1/g2	Disabled
1/g3	Disabled
1/g4	Disabled
1/g5	Disabled
1/g6	Disabled
1/g7	Disabled

Description: 1/g3

Admin Status: disabled

Notifications Enabled: □

Transmit Management Enabled: □

Included TLVs

System Name: □

System Description: □

System Capacity: □

Port Description: □

You can *Edit* port settings for the selected device in this screen. Click *Add* to create a port setting, or select an existing port listed in the upper portion of the screen and click *Edit* the editor opens (the lower portion of the screen) with the following fields:

- **Description**—The port name.

- **Admin Status**— Select the port type on which LLDP is enabled. The possible field values include:

  Tx Only–Enables transmitting LLDP packets only.

  Rx Only–Enables receiving LLDP packets only.

  Tx & Rx–Enables transmitting and receiving LLDP packets. This is the default value.

Disable–Indicates that LLDP is disabled on the port.

Select from the pick list.

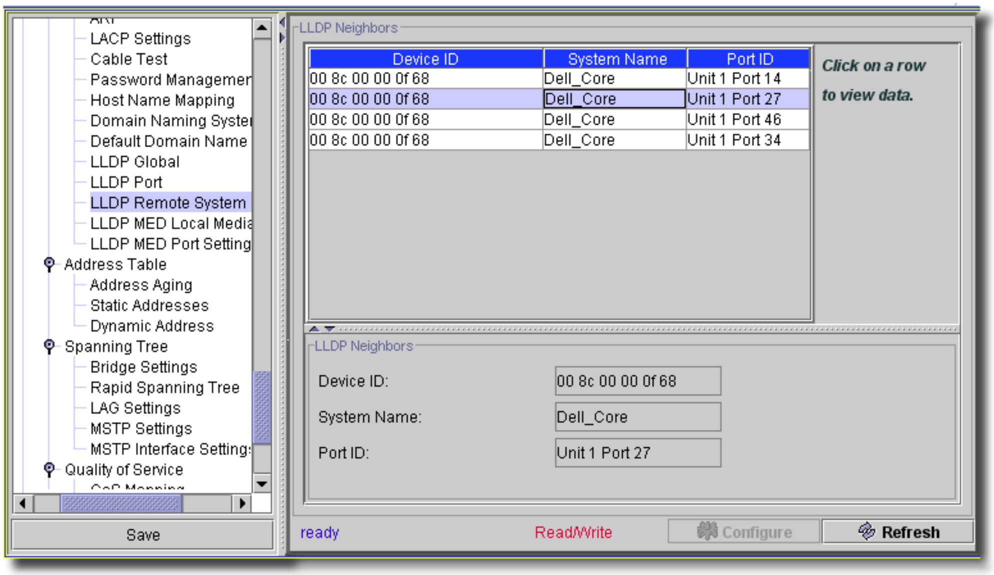
- **Notifications Enabled**—Check to enable. Unchecked indicates that the device LLDP advertisement settings are disabled, and LLDP advertisement settings are user defined. This is the default value.
- **Transmit Management Information**—Check to enables transmission of management address instance.
- **System Name**—Check to enable advertising the system name.
- **System Description**—Check to enable advertising this.
- **System Capacity**—Check to enable advertising this.
- **Port Description**—Check to enable advertising this.

Click *Apply* to accept your edits, or *Cancel* to abandon them. Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

LLDP Remote Settings

This screen displays LLDP remote settings for the selected device.

Figure 13-72. LLDP Remote Settings



LLDP Neighbors

Device ID	System Name	Port ID
00 8c 00 00 0f 68	Dell_Core	Unit 1 Port 14
00 8c 00 00 0f 68	Dell_Core	Unit 1 Port 27
00 8c 00 00 0f 68	Dell_Core	Unit 1 Port 46
00 8c 00 00 0f 68	Dell_Core	Unit 1 Port 34

LLDP Neighbors

Device ID: 00 8c 00 00 0f 68

System Name: Dell_Core

Port ID: Unit 1 Port 27

Select a row displayed at the top of this screen and its data appears below:

- **Device ID**—Displays the neighbor’s Device ID.
- **System Name**—Displays the neighbor’s System Name.

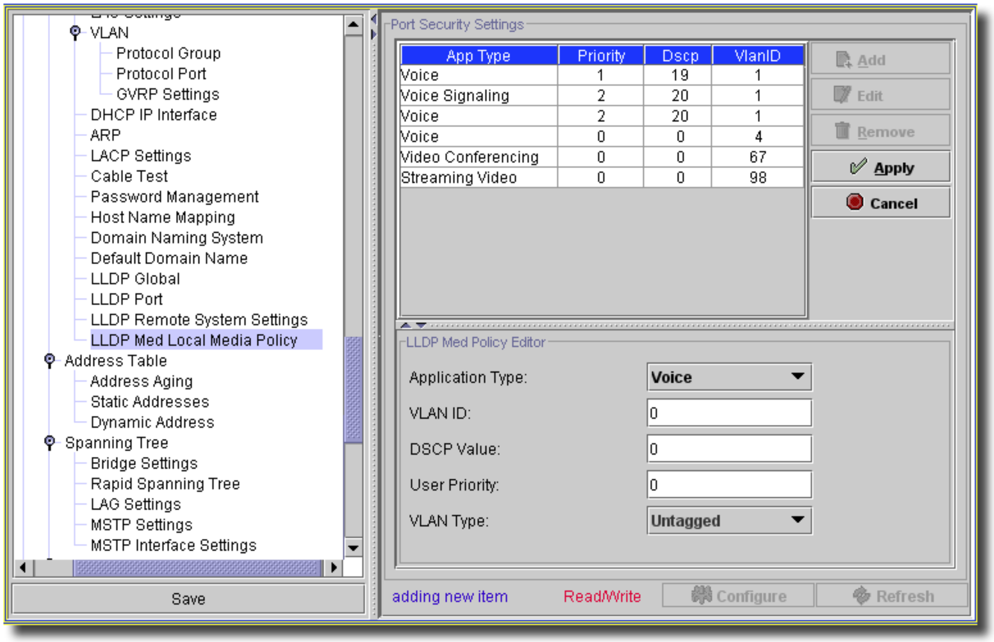
- **Port ID**—Displays the neighbor’s Port ID.

Click *Refresh* to renew the device information on this screen.

LLDP Med Local Media Policy

This screen sets LLDP Med local media policy for the selected device.

Figure 13-73. LLDP Med Local Media Policy



App Type	Priority	Dscp	VlanID
Voice	1	19	1
Voice Signaling	2	20	1
Voice	2	20	1
Voice	0	0	4
Video Conferencing	0	0	67
Streaming Video	0	0	98

Application Type: Voice

VLAN ID: 0

DSCP Value: 0

User Priority: 0

VLAN Type: Untagged

You can *Edit* settings for the selected device in this screen. Click *Add* to create a setting, or select an existing setting listed in the upper portion of the screen and click *Edit* the editor opens (the lower portion of the screen) with the following fields:

- **Application type**—Displays the application for which the network policy is defined. The possible field values are:

  Voice—Indicates that the network policy is defined for a Voice application.

  Voice Signaling—Indicates that the network policy is defined for a Voice Signaling application.

  Guest Voice—Indicates that the network policy is defined for a Guest Voice application.

  Guest Voice Signaling—Indicates that the network policy is defined for a Guest Voice Signaling application.

  Softphone Voice—Indicates that the network policy is defined for a Softphone Voice application.

Video Conferencing—Indicates that the network policy is defined for a Video Conferencing application.

Streaming Video—Indicates that the network policy is defined for a Streaming Video application.

Video Signaling—Indicates that the network policy is defined for a Video Signalling application.

- **VLAN ID**—Displays the VLAN ID for which the network policy is defined.

- **VLAN Type**—Indicates the VLAN type for which the network policy is defined. the possible field values are:

Tagged–Indicates the network policy is defined for tagged VLANs.

Untagged – Indicates the network policy is defined for untagged VLANs.

User Priority –Defines the priority assigned to the network application.

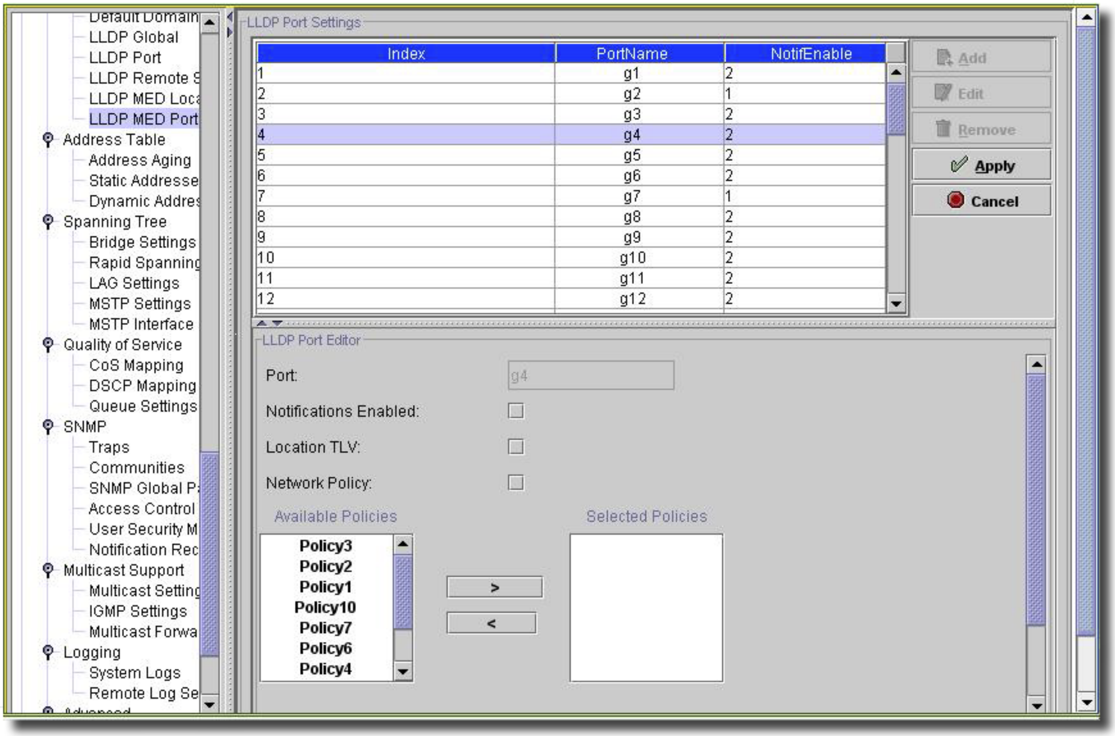
DSCP Value – Defines the DSCP value assigned to the network policy. The possible field value is 1-64.

Click *Apply* to accept your edits, or *Cancel* to abandon them. Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

LLDP MED Port Settings

This screen lets you manage LLDP MED Port settings for the selected device.

Figure 13-74. LLDP MED Port Settings



Index	PortName	NotifEnable
1	g1	2
2	g2	1
3	g3	2
4	g4	2
5	g5	2
6	g6	2
7	g7	1
8	g8	2
9	g9	2
10	g10	2
11	g11	2
12	g12	2

Port: g4

Notifications Enabled: □

Location TLV: □

Network Policy: □

Available Policies

Policy3
Policy2
Policy1
Policy10
Policy7
Policy6
Policy4

Selected Policies

You can *Add* or *Edit* MED Port settings for the selected device in this screen. Select a listed port and click *Remove* to delete it. Select a port listed and click *Edit*, and the editor opens (the lower portion of the screen) with the following fields:

- **Port**—The name of the port. This is read-only when you edit an existing port.

- **Notifications**—Check this to enable notifications

- **Location TLV**—Check to enable location TLV in LLDP frames.

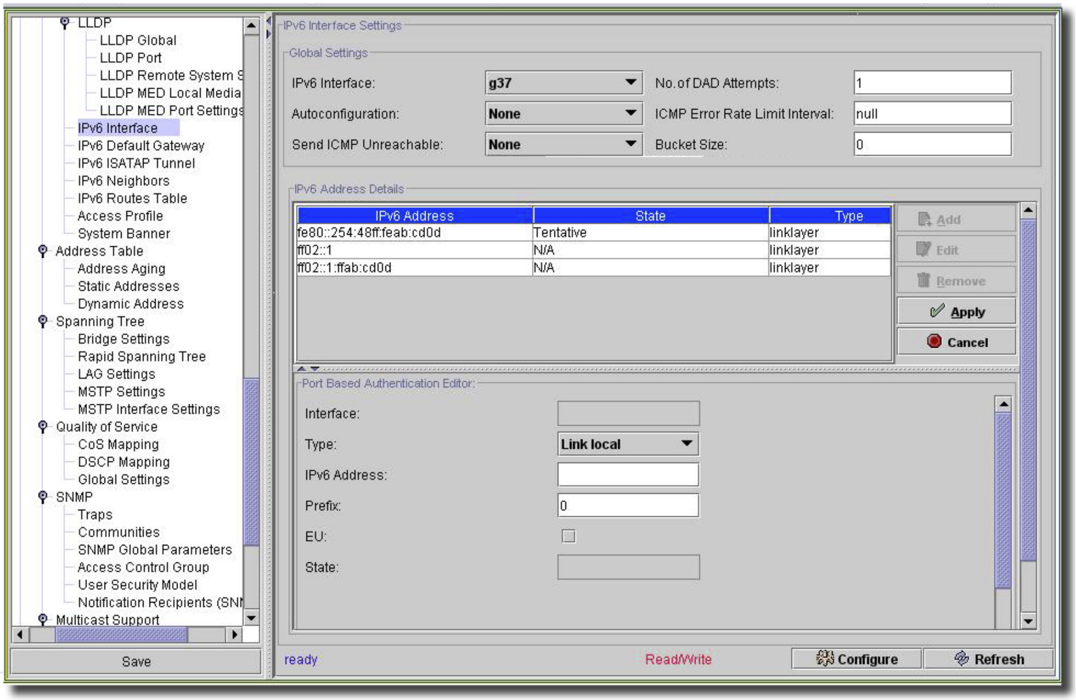
- **Network Policy**—Check to enable transmitting the network policy TLV in LLDP frames. Select from the available policies that appear in the *Available Policies* panel below this field. Click the right arrow to move a policy from *Available* to *Selected.*

Click *Apply* to accept your edits, or *Cancel* to abandon them. Click *Refresh* to renew the device information on this screen.

IPv6 Interface

This screen manages IP v6 interfaces for the selected device.

Figure 13-75. IPv6 Interface



IPv6 Interface Settings

Global Settings

IPv6 Interface: g37

No. of DAD Attempts: 1

Autoconfiguration: None

ICMP Error Rate Limit Interval: null

Send ICMP Unreachable: None

Bucket Size: 0

IPv6 Address Details

IPv6 Address	State	Type
fe80::254:48ff:feab:cd0d	Tentative	linklayer
ff02::1	N/A	linklayer
ff02::1:ffab:cd0d	N/A	linklayer

Port Based Authentication Editor:

Interface:

Type: Link local

IPv6 Address:

Prefix: 0

EU: □

State:

This screen contains the following fields:

Global Settings

- **IPv6 Interface**—The IPv6 interface that has been selected for configuration.

- **No of DAD Attempts**—Defines the number of consecutive neighbor solicitation messages that are sent on an interface while Duplicate Address Detection (DAD) is performed on unicast IPv6 addresses on this interface. New addresses remain in a tentative state while duplicate address detection is performed. A field value of 0, disables duplicate address detection processing on the specified interface. A field value of 1, indicates a single transmission without follow up transmissions. Range is 0-600, default is 1.

- **Autoconfiguration**—Specifies whether IPv6 address assignment on an interface is done by stateless auto configuration. When enabled, the router solicitation ND procedure is initiated (to discover a router in order to assign an IP address to the interface based on prefixes received with RA messages). When autoconfiguration is disabled, the device does no automatic assignment of IPv6 Global Unicast addresses, and it removes existing automatically assigned IPv6 Global Unicast addresses from the interface. Default is *Enabled*.

- **ICMP Error Rate Limit Interval**—The rate-limit interval for ICMPv6 error messages in milliseconds. The value of this parameter together with the Bucket Size parameter (below) determines how many ICMP error messages may be sent per time interval. For example, a rate-limit interval of 100 ms and a bucket size of 10 messages translates to 100 ICMP error messages per second.
- **Send ICMP Unreachable**—Specifies whether transmission of ICMPv6 Address Unreachable messages is enabled. When enabled, unreachable messages are generated for any packet arriving on the interface with unassigned TCP/UDP port. The default is *Enabled*.
- **Bucket Size**—The bucket size for ICMPv6 error messages. The value of this parameter together with the Interval parameter (above) determines how many ICMP error messages may be sent per time interval. For example, a rate-limit interval of 100 ms and a bucket size of 10 messages translates to 100 ICMP error messages per second. Default is 100 ICMP error messages per second; this corresponds to the default interval of 100 ms multiplied by the default bucket size of 10.

IPv6 Address Details

This panel lists the IPv6 addresses available on the selected interface. You can *Add*, or *Edit* addresses for the selected device in this screen. Select a listed interface and click *Remove* to delete it. Click *Add*, or select a listed interface and click *Edit*, and the editor opens (the lower portion of the screen) with the following fields:

Port Based Authentication Editor

- **Interface**—The IPv6 interface that has been selected for configuration.
- **Type**—Specifies the means by which the IP address was added to the interface. The possible field values are:

  Link Local—Indicates the IP address is link local; non-routable and can be used for communication on the same network only. A Link Local address has a prefix of `FE80`.

  Global Unicast—Indicates the IP address is a globally unique IPv6 unicast address; visible and reachable from different subnets.

  Global Anycast—Indicates the IP address is a globally unique IPv6 anycast address; visible and reachable from different subnets.

  Multicast—Indicates the IP address is multicast.

- **IPv6 Address**—Indicates the IPv6 address assigned to the interface. The address must be a valid IPv6 address, specified in hexadecimal using 16-bit values between colons. An example of an IPv6 address is 2031:0:130F:0:0:9C0:876A:130D and the compressed version is represented as 2031::0:9C0:876A:130D. Up to five IPv6 addresses (not including Link Local addresses) can be set per interface, with the limitation of up to 128 addresses per system.

- **Prefix**—Specifies the length of the IPv6 prefix. The length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). The Prefix field is applicable only on a static IPv6 address defined as a Global IPv6 address.
- **EU**—Check to enable transmitting the network policy TLV in LLDP
- **State**—Displays the Duplicate Address Detection (DAD) Status which is the process of verifying and assuring an inserted IPv6 address is unique. This is a read-only parameter with the following possible values:

Tentative—Indicates the system is in process of IPv6 address duplication verification.

Duplicate—Indicates the IPv6 address is being used by an another host on the network. The duplicated IPv6 address is suspended and is not used for sending or receiving any traffic.

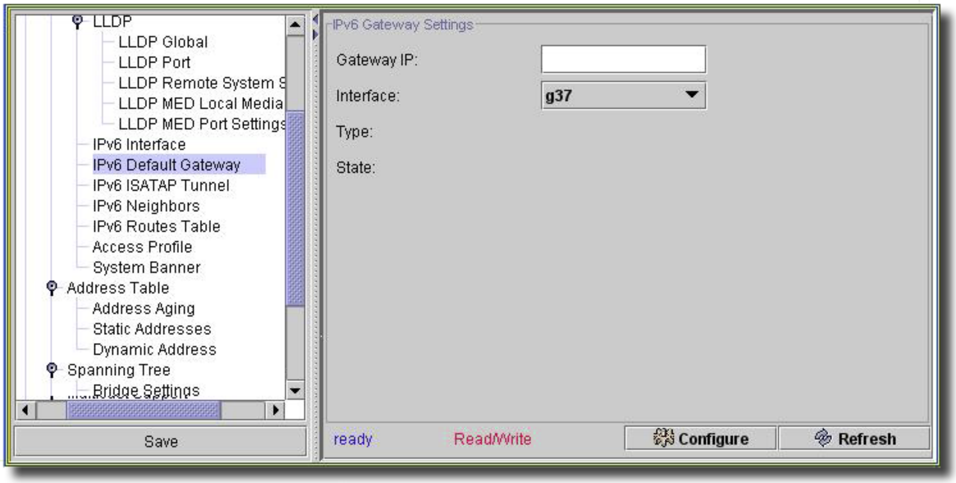
Active—Indicates the IPv6 address is set to active.

Click *Apply* to accept your edits, or *Cancel* to abandon them. Click *Refresh* to renew the device information on this screen or *Configure* to send your edits to the device.

IPv6 Default Gateway

This screen configures the IPv6 default gateway for the selected device.

Figure 13-76. IPv6 Default Gateway



IPv6 Gateway Settings

Gateway IP:

Interface: g37

Type:

State:

This screen lets you manually configure the router of all off-link traffic. The default gateway address is an interface that serves as an access point to another network. For IPv6, the configuration of the default gateway is not mandatory, since hosts can automatically learn of the existence of a router on the local network through the router advertisement procedure.

Unlike IPv4, the IPv6 default gateway can have multiple IPv6 addresses which may include up to one user-defined static address and multiple dynamic addresses learned via router solicitation message. The user-defined default gateway has a higher precedence over an automatically advertised router.

When removing an IP interface, all of its default gateway IP addresses are removed. Dynamic IP addresses cannot be removed. An Alert message appears once a user attempts to insert more than one user-defined address. An Alert message appears when attempting to insert a none Link Local type address.

This editor has the following fields:

- **Gateway IP**—Displays the Link Local IPv6 address of the default gateway.
- **Interface**—Specifies the outgoing interface through which the default gateway can be reached. Interface refers to any Port/LAG/VLAN and/or Tunnel.
- **Type**—Specifies the means by which the default gateway was configured. The possible field values are:

  Static—Indicates the default gateway is user-defined.

  Dynamic—Indicates the default gateway is dynamically configured.
- **State**—Displays the default gateway status. The possible field values are:

  Incomplete—Indicates that address resolution is in progress and the link-layer address of the default gateway has not yet been determined.

  Reachable—Indicates that the default gateway is known to have been reachable recently (within the last tens of seconds).

  Stale—Indicates that the default gateway is no longer known to be reachable but until traffic is sent to the default gateway, no attempt is made to verify its reachability.

  Delay—Indicates that the default gateway is no longer known to be reachable, and traffic has recently been sent to the default gateway. Rather than probe the default gateway immediately, however, there is a delay sending probes for a short while in order to give upper-layer protocols a chance to provide reachability confirmation.

  Probe—Indicates that the default gateway is no longer known to be reachable, and unicast Neighbor Solicitation probes are being sent to verify reachability.

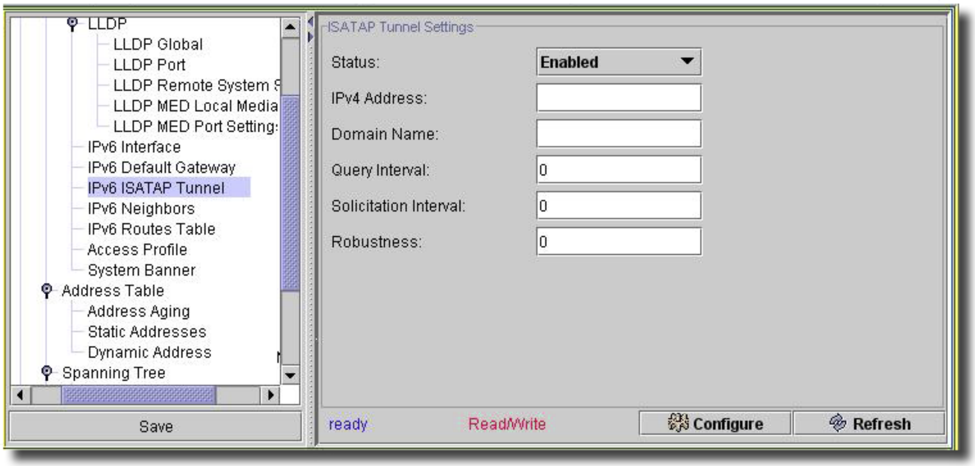
  Unreachable—Indicates that no reachability confirmation was received.

Click *Refresh* to renew the device information on this screen or *Configure* to send your edits to the device.

IPv6 ISATAP Tunnel

This screen manages ISATAP tunnel settings for the selected device.

Figure 13-77. IPv6 ISATAP Tunnel



ISATAP Tunnel Settings

Status:	Enabled
IPv4 Address:	
Domain Name:	
Query Interval:	0
Solicitation Interval:	0
Robustness:	0

ready Read/Write

The IPv6 ISATAP Tunnel Page defines the tunneling process on the device, which encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 network.

The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is an IPv6 transition mechanism which is defined as a tunneling IPv6 interface. It transmits IPv6 packets between dual-stack nodes on top of an IPv4 network.

When enabling ISATAP on a tunnel interface, an explicit IP address is configured as the tunnel source. Alternatively, an automatic mode exists where the lowest IPv4 address is assigned to an IP interface. This source IPv4 sets the tunnel interface identifier according to ISATAP addressing convention. When a tunnel interface is enabled for ISATAP, you must set the tunnel source for the interface for the interface to become active.

You can represent an ISATAP address using the [64-bit prefix]:0:5EFE:w.x.y.z, where 5EFE is the ISATAP identifier and w.x.y.z is a public or private IPv4 address. Thus, a Link Local address appears as FE80::5EFE:w.x.y.z

Once the last IPv4 address is removed from the interface, the ISATAP IP interface state becomes inactive and appears *Down*, however the Admin state remains enabled.

When defining tunneling, note the following:

- An IPv6 Link Local address is assigned to the ISATAP interface. The initial IP address is assigned to the interface, and the interface state becomes Active.
- If an ISATAP interface is active, the ISATAP router IPv4 address resolves through DNS by using ISATAP-to-IPv4 mapping. If the ISATAP DNS record is not resolved, the ISATAP host name-to-address mapping is searched in the host name cache.

- When an ISATAP router IPv4 address is not resolved via DNS process, the status of the ISATAP IP interface remains *Active*. The system does not have a default gateway for ISATAP traffic until the DNS procedure is resolved.
- For an ISATAP Tunnel to work properly over an IPv4 network, you must set up an ISATAP Router.

The editor screen contains the following fields:

- **Status**—Specifies the status of ISATAP on the device. The possible field values are: *Enabled* or *Disabled* (the default value).

- **IPv4 Address**—Specifies the local (source) IPv4 address of a tunnel interface.

- **Domain Name**—Specifies a global string that represents a specific automatic tunnel router domain name. The default value is *ISATAP.*

- **Query Interval**—Specifies the interval between DNS Queries (before the IP address of the ISATAP router is known) for the automatic tunnel router domain name. The range is 10 - 3600 seconds. The default is 10 seconds.

- **Solicitation Interval**—Specifies the interval between router solicitations messages when there is no active router. The range is 10 - 3600 seconds. The default is 10.

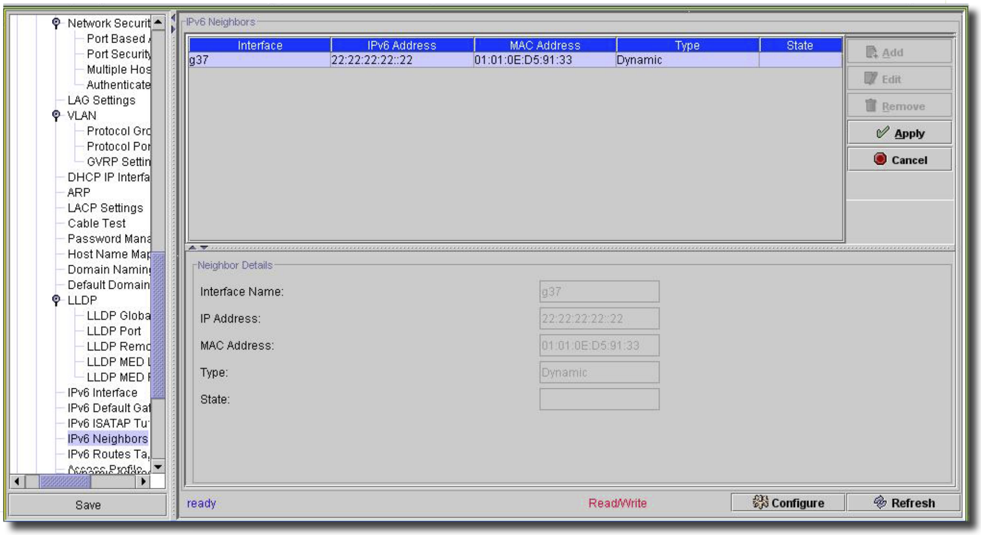
- **Robustness**—Specifies the number of DNS Query/ Router Solicitation refresh messages that the device sends. The range is 1 - 20 seconds. The default is 3.

Click *Refresh* to renew the device information on this screen or *Configure* to send your edits to the device.

IPv6 Neighbors

This screen defines IPv6 Neighbors for the selected equipment.

Figure 13-78. IPv6 Neighbors



Interface	IPv6 Address	MAC Address	Type	State
g37	22:22:22:22::22	01:01:0E:D5:91:33	Dynamic	

Interface Name: g37

IP Address: 22:22:22:22::22

MAC Address: 01:01:0E:D5:91:33

Type: Dynamic

State:

These definitions are like the functionality of the IPv4 Address Resolution Protocol (ARP). IPv6 Neighbors enables detecting Link Local addresses within the same subnet, and includes a database for maintaining reachability information about the active neighbors paths.

These devices typically support a total of up to 256 neighbors obtained either statically or dynamically. When removing an IPv6 interface, all neighbors learned statically and dynamically are removed.

- **Interface** — Displays the interface on which IPv6 Interface is defined. Interfaces include Ports, LAGs, or VLANs.
- **IPv6 Address** — Defines the currently configured neighbor IPv6 address.
- **MAC Address** — Displays the MAC address assigned to the interface.
- **Type** — Displays the type of the neighbor discovery cache information entry. The possible field values are:

  Static — Shows static neighbor discovery cache entries. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—as learned through the IPv6 neighbor discovery process—you can convert the entry to a static entry.

  Dynamic — Shows dynamic neighbor discovery cache entries.

  Remove — When selected, removes the neighbor from the list.

In the IPv6 Neighbors Table, the following additional parameter appears:

State — Displays the IPv6 Neighbor status. The field possible values are:

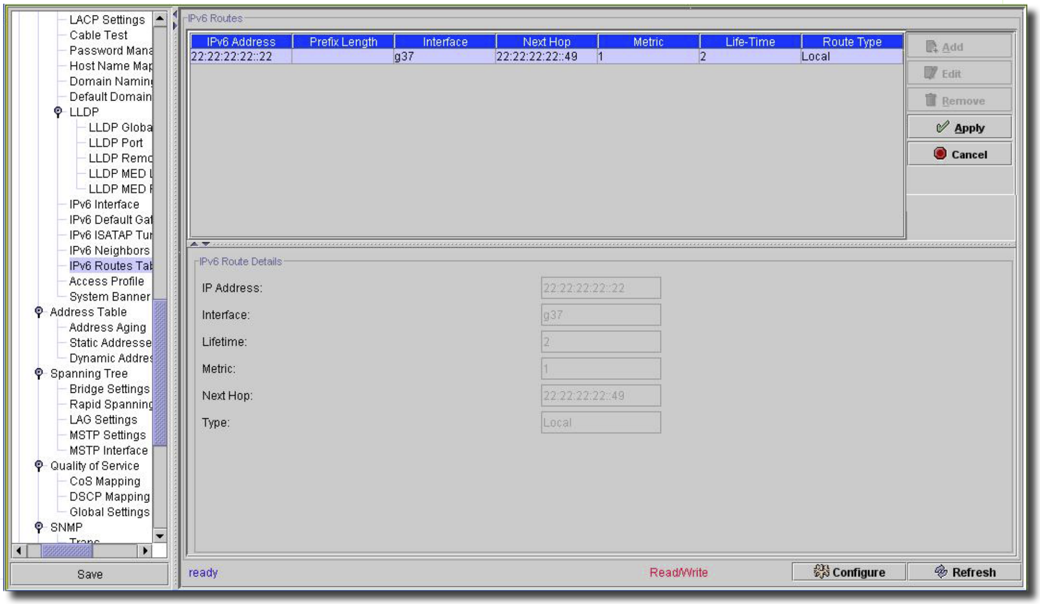
- **Incomplete** — Indicates that an address resolution is in progress and the link-layer address of the neighbor has not yet been determined.
- **Reachable** — Indicates that the neighbor is known to have been reachable recently (within tens of seconds ago).
- **Stale** — Indicates that the neighbor is no longer known to be reachable but until traffic is sent to the neighbor, no attempt is made to verify its reachability.
- **Delay** — Indicates that the neighbor is no longer known to be reachable, and traffic has recently been sent to the neighbor. Rather than probe the neighbor immediately, however, there is a delay sending probes for a short while in order to give upper-layer protocols a chance to provide reachability confirmation.
- **Probe** — Indicates that the neighbor is no longer known to be reachable, and unicast Neighbor Solicitation probes are being sent to verify reachability.

Click *Refresh* to renew the device information on this screen or *Configure* to send your edits to the device.

IPv6 Routes

This screen displays the IPv6 Routes Table

Figure 13-79. IPv6 Routes



IPv6 Routes

IPv6 Address	Prefix Length	Interface	Next Hop	Metric	Life-Time	Route Type
22:22:22:22::22		g37	22:22:22:22::49	1	2	Local

IPv6 Route Details

IP Address: 22:22:22:22::22
Interface: g37
Lifetime: 2
Metric: 1
Next Hop: 22:22:22:22::49
Type: Local

The IPv6 Routes Table stores information about IPv6 destination prefixes and how they are reached, either directly or indirectly. The routing table determines the next-hop address and the interface used for forwarding.

Each dynamic entry also has an associated invalidation timer value (extracted from Router Advertisements) used to delete entries that are no longer advertised.

- **IPv6 Address** — Defines the destination IPv6 address.

- **Prefix Length** — Specifies the length of the IPv6 prefix. The Prefix field is applicable only when the IPv6 Static IP address is defined as a Global IPv6 address. The range is 5 - 128.

- **Interface** — Displays the interface that is used to forward the packet. Interface refers to any Port, LAG or VLAN.

- **Next Hop** — Defines the address to which the packet is forwarded on the route to the Destination address (typically the address of a neighboring router). This can be either a Link Local or Global IPv6 address.

- **Metric** — Indicates the value used for comparing this route to other routes with the same destination in the IPv6 route table. This is an administrative distance with the range of 0-255. The default value is 1.

- **Life-Time** — Indicates the life-time of the route.

- **Route Type** — Displays whether the destination is directly attached and the means by which the entry was learned. The following values are:

- **Local** — Indicates a directly connected route entry.

- **Static** — Indicates the route is learned through the ND process. The entry is automatically converted to a static entry.

- **ICMP** — Indicates the route is learned through ICMP messages.

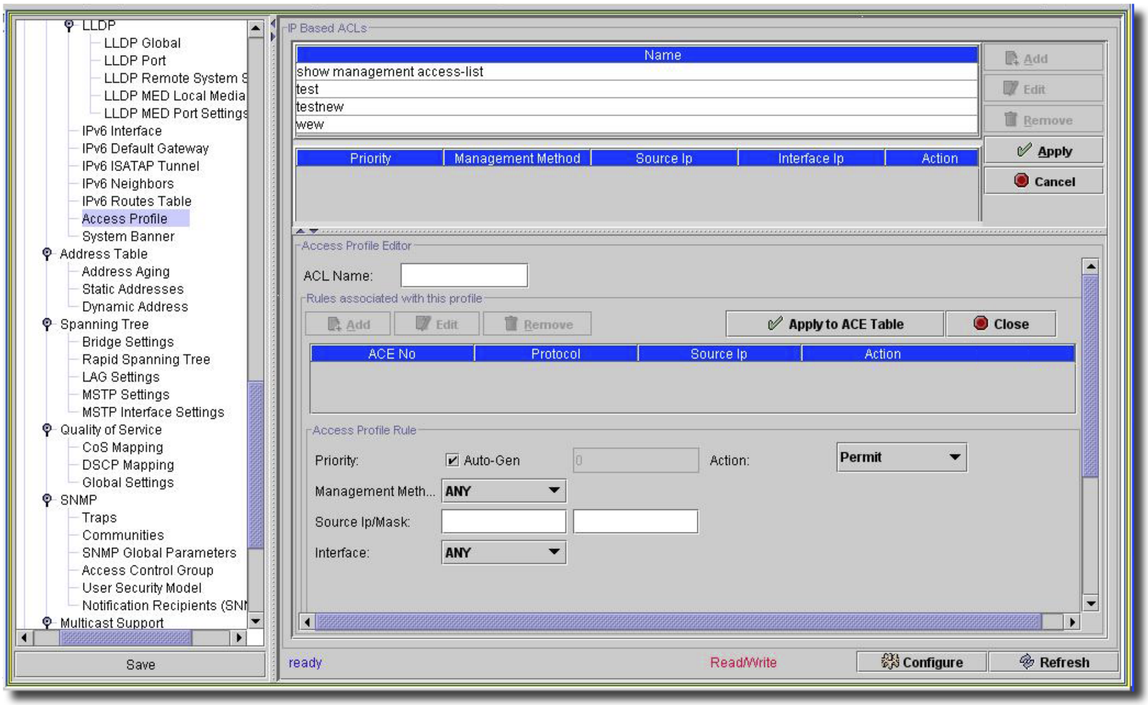
- **ND** — Indicates the route is learned through RA messages.

Click *Refresh* to renew the device information on this screen or *Configure* to send your edits to the device.

Access Profile

This screen manages the access control list (ACL) profiles for the selected device.

Figure 13-80. Access Profile



Name
show management access-list
test
testnew
wew

Priority	Management Method	Source Ip	Interface Ip	Action

ACL Name:

ACE No	Protocol	Source Ip	Action

Priority: ☑ Auto-Gen 0 Action: Permit

Management Meth... ANY

Source Ip/Mask:

Interface: ANY

Access Control Lists (ACL), which consist of Access Control Entries (ACE), allow network managers to define classification actions and rules for specific ingress ports. Packets entering an ingress port, with an active ACL, are either admitted or denied entry and the ingress port is disabled. If they are denied entry, the user can disable the port.

When an ACL is bound to an interface, all the ACE rules that have been defined are applied to the selected interface.Whenever an ACL is assigned on a port or LAG, flows from that ingress interface that do not match the ACL are matched to the default rule, which drops unmatched packets.

For example, a network administrator defines an ACL rule that states, port number 20 can receive TCP packets, however, if it receives a UDP packet, it drops the packet.

ACLs consist of access control entries (ACEs) made of the filters that determine traffic classifications. Each ACE is a rule, and 1,024 rules are available. But rules are not only used for user configuration purposes, they are also used for features like iSCSI and PVE, so not all 1,024 are available for ACEs. At least 600 rules are therefore available.

Access Profile Editor

This panel lists the access profiles available on the selected device. You can *Add*, or *Edit* ACLs for the selected device in this screen. Select a listed ACL and click *Remove* to delete it. Click *Add*, or select a listed interface and click *Edit*, and the editor opens (the lower portion of the screen) with the following fields:

- **ACL Name**—The identifier for the ACL.

Click *Add*, or *Edit* to add rules for an ACL. Click *Apply to ACE Table* to accept your configured rules. Configured rules for the ACL appear listed below the *Add*, *Edit* and *Remove* buttons. screen. When you click *Add*, or select a listed ruleset and click *Edit*, an editor opens (the lower portion of the screen) with the following fields:

Access Profile Rule

- **Prioriity**—Rule priority that determines which ACE is matched to a packet based on a first-match basis. Check *Auto-Gen* to automatically generate the priority. When the packet matches a rule, user groups are either granted or denied device management access. The rule order is set by defining a rule number within the Profile Rules Table. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. (1-65535)
- **Action**—Indicates the ACL forwarding action. The possible field values are:

  Permit—Forwards packets which meet the ACL criteria.

  Deny—Drops packets which meet the ACL criteria.

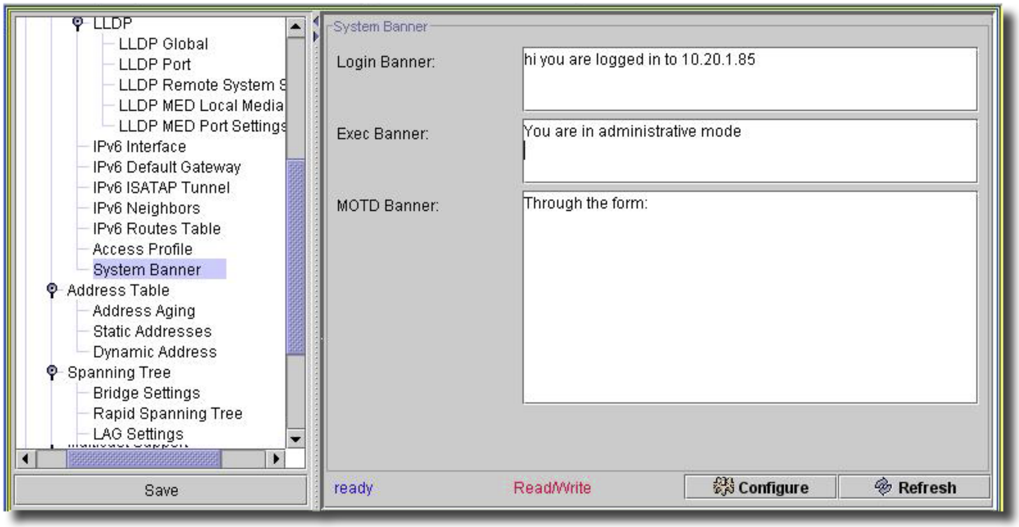
  Shutdown—Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.
- **Management Method**—The management method for which the access profile is defined. Users with this access profile can access the device using the management method selected.
- **Source Ip/Mask**—The source IP and IP address mask for the source to which this rule applies.
- **Interface**—The interface type to which the rule applies. This is an optional field. This rule can apply to a selected port, LAG, or VLAN by selecting the appropriate option and interface. Assigning an access profile to an interface denies access via other interfaces. If you select (*Any*) as an access profile, device access is granted all interfaces.

Click *Apply* to accept your edits, or *Cancel* to abandon them. Click *Refresh* to renew the device information on this screen or *Configure* to send your edits to the device.

System Banner

This screen configures the banner messages for the selected device.

Figure 13-81. System Banner



Login Banner: hi you are logged in to 10.20.1.85

Exec Banner: You are in administrative mode

MOTD Banner: Through the form:

This has the following fields that configure various command shell banners for the selected device.

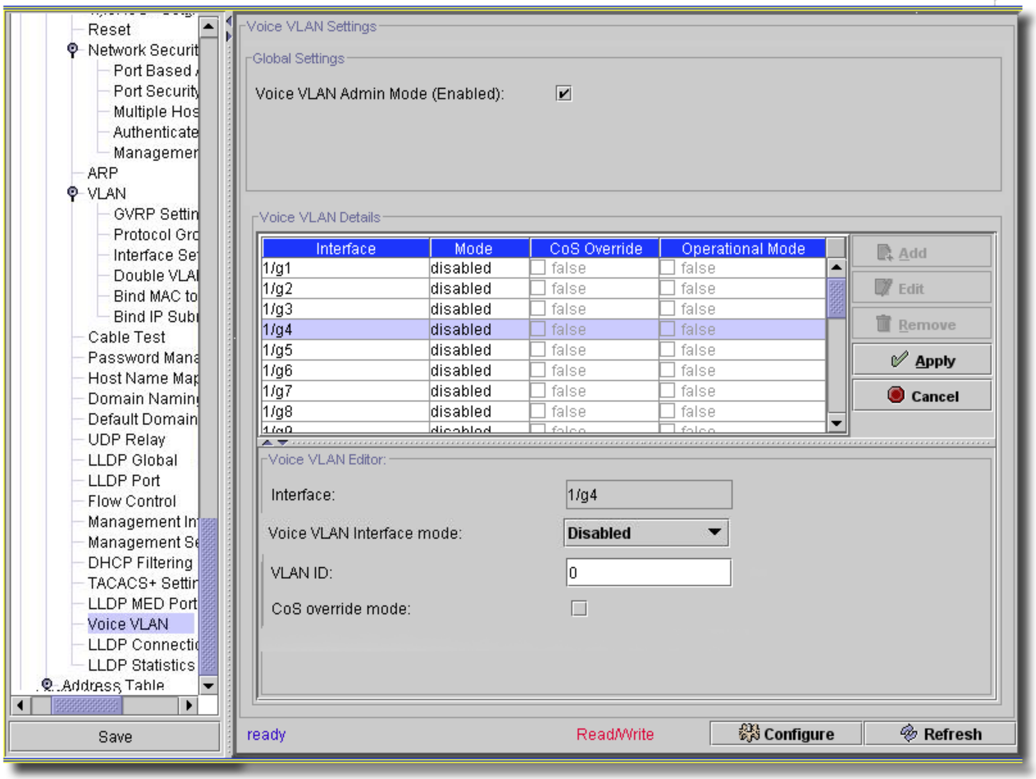
- **MOTD Banner**—The message-of-the-day is the message that appears when you first connect to the device.
- **Login Banner**—The message that appears in a session just before the login prompt.
- **Exec Banner**—The message that appears after you log in.

Click *Refresh* to renew the device information on this screen or *Configure* to send your edits to the device.

Voice VLAN

This screen manages SNMP voice VLAN for the selected device.

Figure 13-82. Voice VLAN



Voice VLAN Settings

Global Settings

Voice VLAN Admin Mode (Enabled): ☑

Voice VLAN Details

Interface	Mode	CoS Override	Operational Mode
1/g1	disabled	□ false	□ false
1/g2	disabled	□ false	□ false
1/g3	disabled	□ false	□ false
1/g4	disabled	□ false	□ false
1/g5	disabled	□ false	□ false
1/g6	disabled	□ false	□ false
1/g7	disabled	□ false	□ false
1/g8	disabled	□ false	□ false
1/g9	disabled	□ false	□ false

Voice VLAN Editor:

Interface: 1/g4

Voice VLAN Interface mode: Disabled

VLAN ID: 0

CoS override mode: □

ready Read/Write

Check the *Voice VLAN Admin Mode (Enabled)* checkbox to enable Voice VLAN administration. Click *Edit* on one of the listed interfaces to edit its settings in the lowest panel. Click *Apply* to accept your edits (or *Cancel* to abandon them). The following fields appear in the settings editor:

- **Interface**—A read-only reminder of the interface you are editing.

- **Voice VLAN Interface mode**—Select the interface mode from the pick list. *Disable* is the default value. *None* allows the IP phone to use its own configuration to send untagged voice traffic. *VLAN ID* means enter the Voice Vlan Id within the range of 1 to 4093. *dot1p* configures Voice Vlan 802.1p priority tagging for voice traffic. Priorities range from 0 to 7. *Untagged* configures the phone to send untagged voice traffic.

- **VLAN ID**—Enter an identifier for the VLAN.

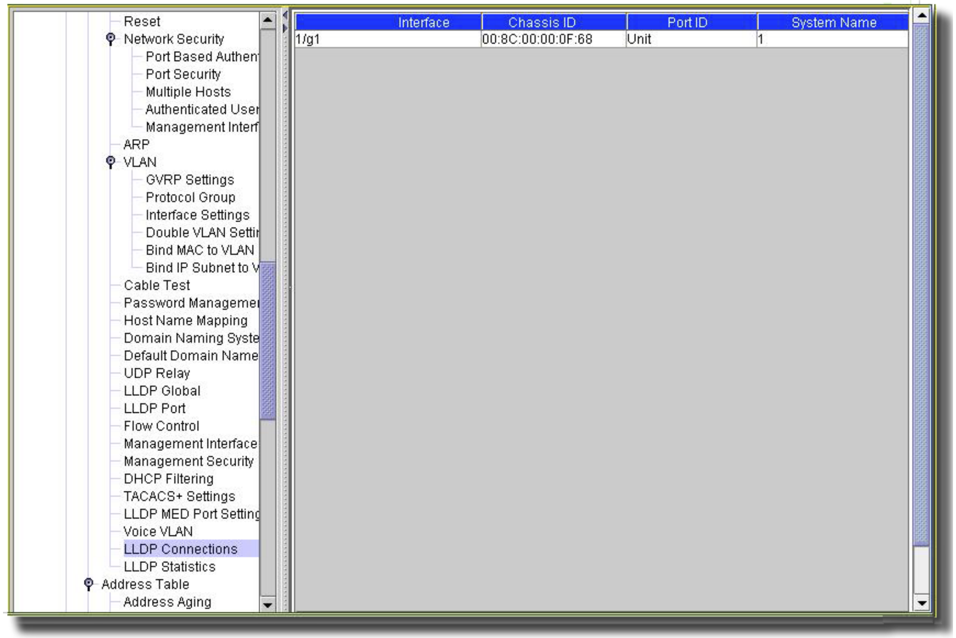
- **CoS override mode**—Check to override CoS settings for this interface.

Click *Configure* to implement your edits; *Refresh* to re-query the database for updates.

LLDP Connections

This screen displays the LLDP connections for the selected device.

Figure 13-83. LLDP Connections



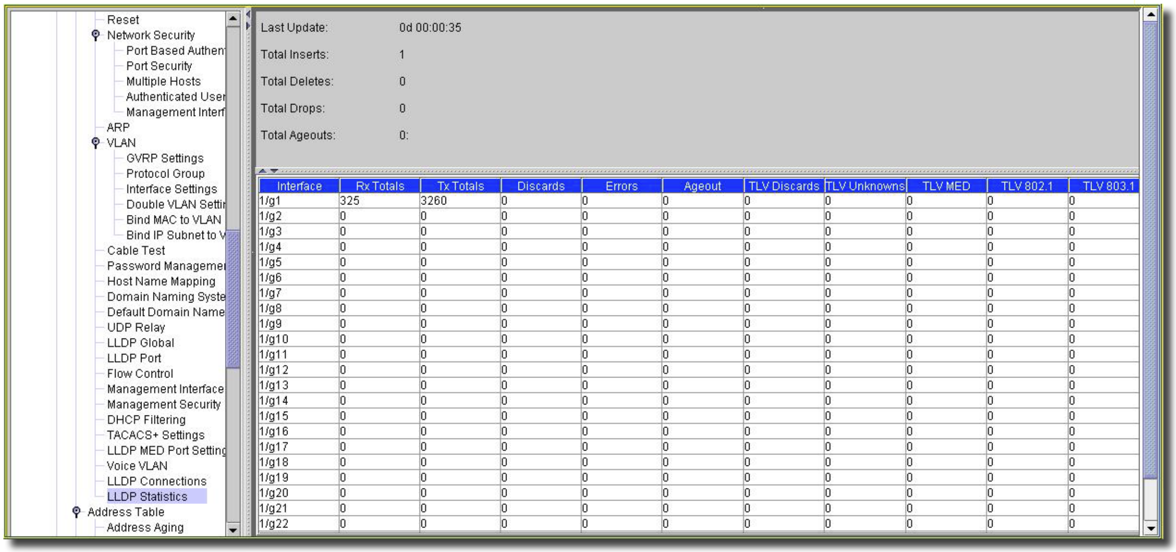
Interface	Chassis ID	Port ID	System Name
1/g1	00:8C:00:00:0F:68	Unit	1

This shows the *Interface*, *Chassis ID*, *Port ID*, and *System* name for LLDP connections detected. Click *Refresh* to re-query the device.

LLDP Statistics

This screen displays the LLDP statistics for the selected device.

Figure 13-84. LLDP Statistics



Last Update: 0d 00:00:35

Total Inserts: 1

Total Deletes: 0

Total Drops: 0

Total Ageouts: 0:

Interface	Rx Totals	Tx Totals	Discards	Errors	Ageout	TLV Discards	TLV Unknowns	TLV MED	TLV 802.1	TLV 803.1
1/g1	325	3260	0	0	0	0	0	0	0	0
1/g2	0	0	0	0	0	0	0	0	0	0
1/g3	0	0	0	0	0	0	0	0	0	0
1/g4	0	0	0	0	0	0	0	0	0	0
1/g5	0	0	0	0	0	0	0	0	0	0
1/g6	0	0	0	0	0	0	0	0	0	0
1/g7	0	0	0	0	0	0	0	0	0	0
1/g8	0	0	0	0	0	0	0	0	0	0
1/g9	0	0	0	0	0	0	0	0	0	0
1/g10	0	0	0	0	0	0	0	0	0	0
1/g11	0	0	0	0	0	0	0	0	0	0
1/g12	0	0	0	0	0	0	0	0	0	0
1/g13	0	0	0	0	0	0	0	0	0	0
1/g14	0	0	0	0	0	0	0	0	0	0
1/g15	0	0	0	0	0	0	0	0	0	0
1/g16	0	0	0	0	0	0	0	0	0	0
1/g17	0	0	0	0	0	0	0	0	0	0
1/g18	0	0	0	0	0	0	0	0	0	0
1/g19	0	0	0	0	0	0	0	0	0	0
1/g20	0	0	0	0	0	0	0	0	0	0
1/g21	0	0	0	0	0	0	0	0	0	0
1/g22	0	0	0	0	0	0	0	0	0	0

The top of the screen displays when this information was last updated (*Last Update*), in addition to *Totals* for *Inserts*, *Deletes*, *Drops* and *Ageouts* for the device (all interfaces) Below, this screen displays the *Interface*, *Rx Totals*, *Tx Totals*, *Discards*, *Errors*, *Ageout*, *TLV discards*, *TLV Unknowns*, *TLV MED*, *TLV 802.1*, and *TLV 803.1* statistics detected for each interface. Click *Refresh* to re-query the device.

Flow Control

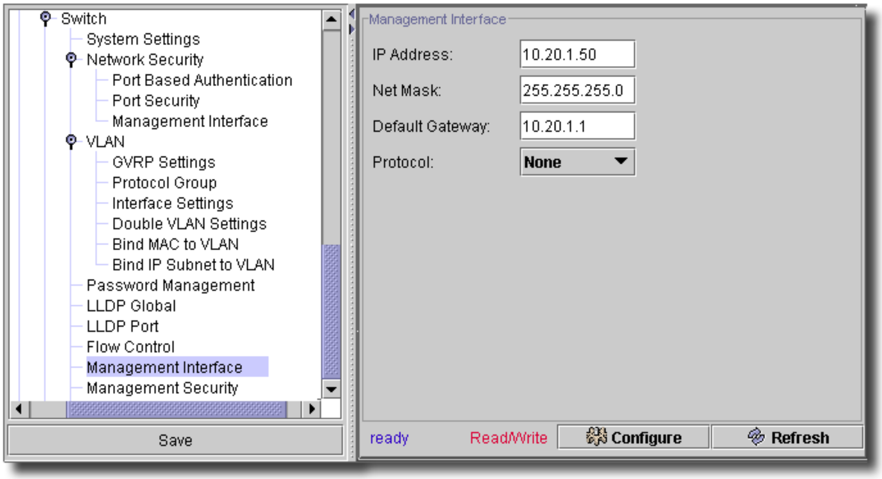
This screen displays a pick list with *Enable* / *Disable* as the options. Select whether you want flow control. *Enabled* turns on the ingress back pressure mechanism of the switch. *Disabled* restores the switch operation to head of line blocking prevention.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Management Interface

This screen sets up the management interface for the device.

Figure 13-85. Management Interface



IP Address: 10.20.1.50

Net Mask: 255.255.255.0

Default Gateway: 10.20.1.1

Protocol: None

This screen has the following fields:

- **IP Address / Net Mask**—The IP address and net mask of the management interface.

- **Default Gateway**—The default gateway for the management interface.

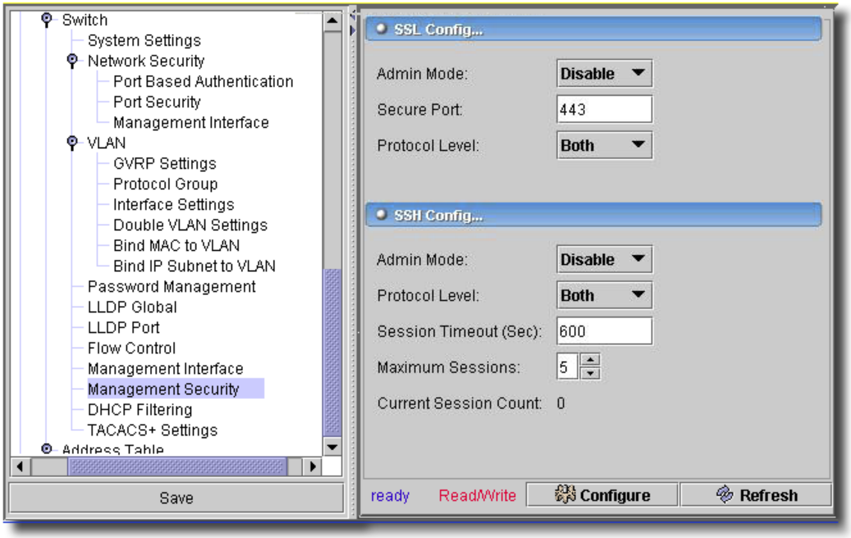
- **Protocol**—The protocol to use. Options can include *none*, *BOOTP*, and *DHCP*.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Management Security

This screen manages security for managing the selected device.

Figure 13-86. Management Security



SSL Config...

Admin Mode: Disable

Secure Port: 443

Protocol Level: Both

SSH Config...

Admin Mode: Disable

Protocol Level: Both

Session Timeout (Sec): 600

Maximum Sessions: 5

Current Session Count: 0

This screen has the following fields:

SSL Config...

- **Admin Mode**—Select *Enable* / *Disable* from the pick list.

- **Secure Port**—Enter the port number.

- **Protocol Level**—Select from the pick list. Options can include *Both*, *SSL30*, or *TLS10*.

SSH Config...

- **Admin Mode**—Select *Enable* / *Disable* from the pick list.

- **Protocol Level**—Select from the pick list. Options can include *Both*, *SSL10*, or *SSL20*.

- **Session Timeout (Sec)**—Enter a maximum timeout for a management session.

- **Maximum Sessions**—Enter a maximum number of management sessions.

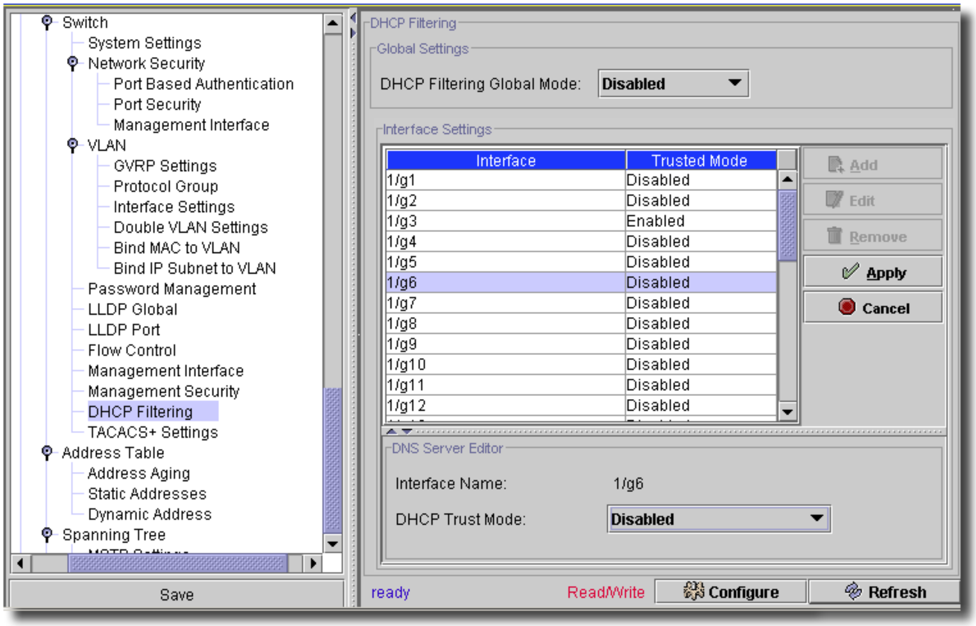
- **Current Session Count**—Displays the number of current sessions.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

DHCP Filtering

This screen lets you manage DHCP filtering for interfaces on the selected device.

Figure 13-87. DHCP Filtering



DHCP Filtering Global Mode: Disabled

Interface	Trusted Mode
1/g1	Disabled
1/g2	Disabled
1/g3	Enabled
1/g4	Disabled
1/g5	Disabled
1/g6	Disabled
1/g7	Disabled
1/g8	Disabled
1/g9	Disabled
1/g10	Disabled
1/g11	Disabled
1/g12	Disabled

Interface Name: 1/g6

DHCP Trust Mode: Disabled

You can *Edit* DHCP interface settings for the selected device in this screen. At the top of the screen, you can *Enable / Disable* the Global DHCP Settings. Select an interface listed and click *Edit*. The editor opens (the lower portion of the screen) with the following fields:

- **Interface Name**—A read-only reminder of the interface name.

- **DHCP Trust Mode**— Select *Enable* or *Disable*.

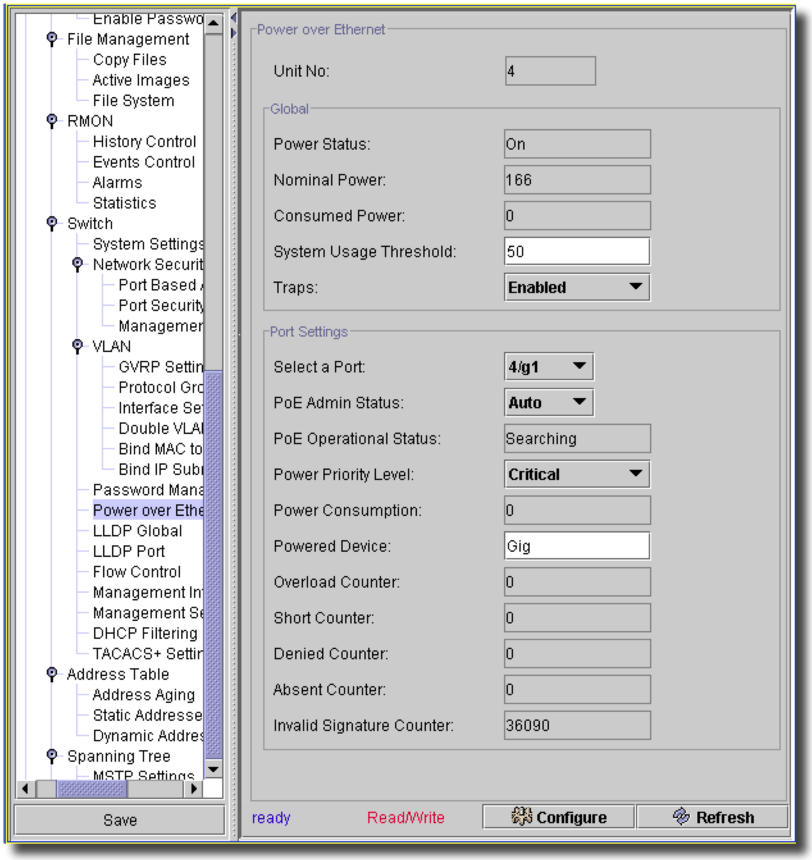
Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

PoE

Power over Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power over Ethernet removes the necessity of placing network devices next to power sources.

PoE Powered Devices receive their power from the PowerConnect power supplies, such as IP phones, security cameras and clocks. Powered Devices are connected to the PowerConnect device via Ethernet ports. PoE technology is available on several Dell PowerConnect switches including 6224P, 6248P, 3524P, 3548P, 3424P, and 3448P.

Figure 13-88. PoE



Power over Ethernet

Unit No: 4

Global

Power Status: On

Nominal Power: 166

Consumed Power: 0

System Usage Threshold: 50

Traps: Enabled

Port Settings

Select a Port: 4/g1

PoE Admin Status: Auto

PoE Operational Status: Searching

Power Priority Level: Critical

Power Consumption: 0

Powered Device: Gig

Overload Counter: 0

Short Counter: 0

Denied Counter: 0

Absent Counter: 0

Invalid Signature Counter: 36090

This screen has the following fields:

- **Unit No:**—Select the unit from the pick list.

Global

- **Power Status**—A read-only display. *On/Off* indicates that the power supply unit is/is not functioning. *Faulty* indicates that the power supply unit is functioning, but an error has occurred. For example, a power overload or a short circuit.

- **Nominal Power**—A read-only display. Indicates the actual amount of power the device can supply. The field value appears in Watts.

- **Consumed Power**—A read-only display. Indicates the amount of the power used by the device. The field value appears in Watts.

- **System Usage Threshold**—Enter the percentage of power consumed before an alarm is generated. The field value is 1-99 percent. The default is 95 percent.

- **Traps**—Enables or Disables receiving PoE device traps. The default is disabled.

Port Settings

- **Select a Port**—Select the port from the pick list. This is the specific interface for which PoE parameters are defined and assigned to the powered interface connected to the selected port.
- **PoE Admin Status**— Select the status from the pick list. This indicates the device's PoE mode. The possible field values are:

  Auto–Enables the Device Discovery protocol, and provides power to the device using the PoE module. The Device Discovery Protocol enables the device to discover Powered Devices attached to the device interfaces, and to learn their classification. This is the default settings.

  Never–Disables the Device Discovery protocol, and stops the power supply to the device using the PoE module.
- **PoE Operational Status**—A read-only display. Indicates if the port is enabled to work on PoE. The possible field values are:

  Delivering Power–The device is delivering power to the interface.

  On–The device is on (and delivering power to the interface).

  Off–The device is not delivering power to the interface.

  Test Fail–The powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device.

  Testing–The powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply.

  Searching–The PowerConnect device is currently searching for a powered device. Searching is the default PoE operational status.

  Fault–The PowerConnect device has detected a fault on the powered device. For example, the powered device memory could not be read.
- **Power Priority Level**—Select from the pick list. Determines the port priority if the power supply is low. The port power priority is used if the power supply is low. The field default is low. For example, if the power supply runs at 99% usage, and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 is prioritized to receive power, and port 3 may be denied power.

  Critical–Assigns the highest power priority level.

  High–Assigns the second highest power priority level.

  Low–Assigns the lowest power priority level.
- **Power Consumption** —A read-only display. Indicates the amount of power assigned to the powered device connected to the selected interface. Devices are classified by the powered device, and the PowerConnect devices use the classification information. The field values are represented in Watts. The possible field values are:

0.44 – 12.95–Indicates that the port is assigned a power consumption level of 0.44 to 12.95 Watts.

0.44 – 3.8–Indicates that the port is assigned a power consumption level of 0.44 to 3.8 Watts.

3.84 – 6.49–Indicates that the port is assigned a power consumption level of 3.84 to 6.49 Watts.

6.49 – 12.95–Indicates that the port is assigned a power consumption level of 6.49 to 12.95 Watts.

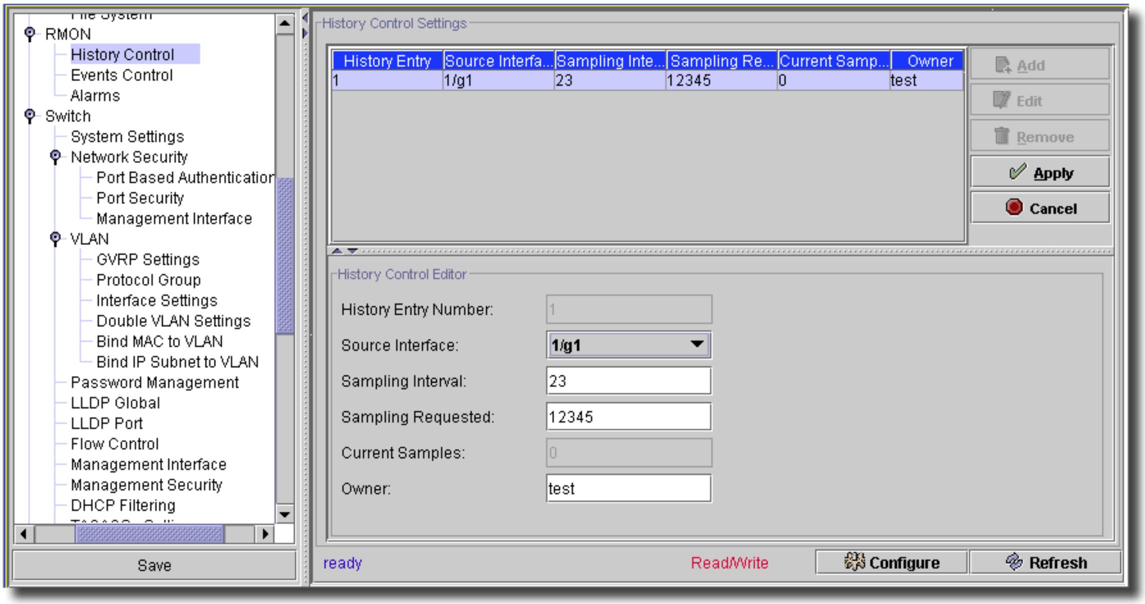
- **Powered Device**—Enter text in the field. Provides a user-defined powered device description. The field can contain up to 24 characters.
- **Overload Counter**—A read-only display. Indicates the total power overload occurrences.
- **Short Counter**—A read-only display. Indicates the total power shortage occurrences.
- **Denied Counter**—A read-only display. Indicates times the powered device was denied power.
- **Absent Counter**—A read-only display. Indicates the times the power supply was stopped to the powered device because the powered device was no longer detected.
- **Invalid Signature Counter**—A read-only display. Indicate the times an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signatures are generated during powered device detection, classification, or maintenance.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

RMON -> History Control

The RMON History Control screen contains information about samples of data taken from ports.

Figure 13-89. RMON History Control



History Entry	Source Interfa...	Sampling Inte...	Sampling Re...	Current Samp...	Owner
1	1/g1	23	12345	0	test

History Entry Number: 1

Source Interface: 1/g1

Sampling Interval: 23

Sampling Requested: 12345

Current Samples: 0

Owner: test

You can *Edit* RMON History Control settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. Click *Add* to create a new group of settings, or select an existing interface listed in the upper portion of the screen and click *Edit* the editor opens (the lower portion of the screen) with the following fields:

- **History Entry Number.**—Entry number for the History Control Table.

- **Source Interface**—Port or LAG from which the history samples were taken.

- **Sampling Interval (1-3600)**—Indicates in seconds the time that samples are taken from the ports. The possible values are 1-3600 seconds.

- **Sampling Requested**—Number of samples to be saved. The default value is 50. ((1-65535)

NOTE:

A change to the number of sample is only effective after a reboot.

- **Current No. of Samples in List**—The current number of samples taken.

- **Owner (0-20 characters)**—RMON station or user that requested the RMON information.

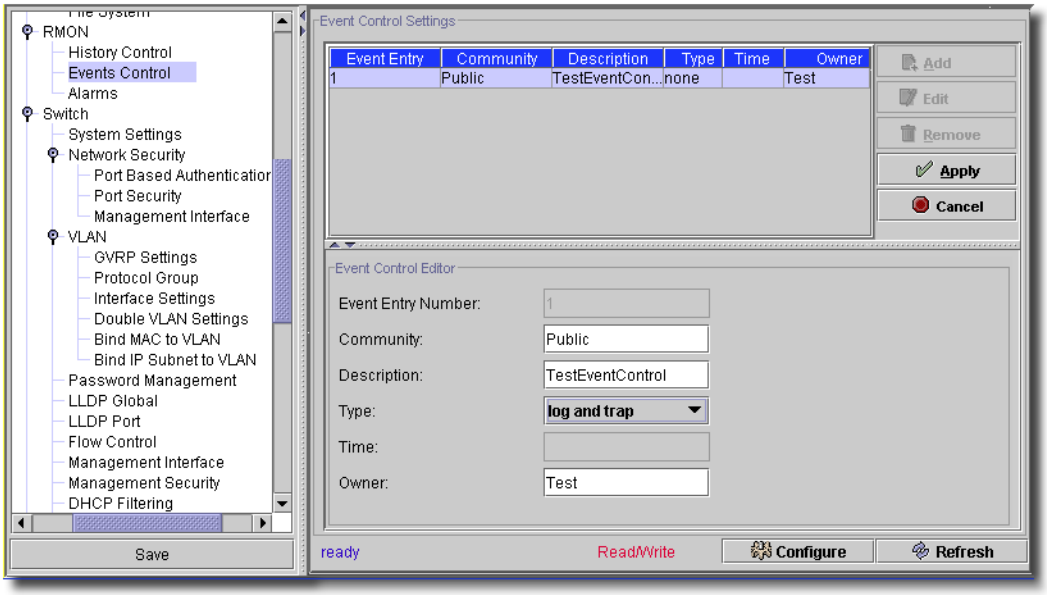
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

RMON -> Events Control

This screen lets you manage the RMON Events.

Figure 13-90. RMON Events Control



Event Entry	Community	Description	Type	Time	Owner
1	Public	TestEventCon...	none		Test

Event Entry Number: 1

Community: Public

Description: TestEventControl

Type: log and trap

Time:

Owner: Test

You can *Edit* RMON Event Control settings for the selected device in this screen. Click *Add* to create a new group of settings, or select an existing interface listed in the upper portion of the screen and click *Edit* the editor opens (the lower portion of the screen) with the following fields:

- **Event Entry Number**—The event.

- **Community**—Community to which the event belongs.

- **Description**—User-defined event description.

- **Type**—Describes the event type. Possible values are:

  Log—Event type is a log entry.

  Trap—Event type is a trap.

  Log and Trap—Event type is both a log entry and a trap.

  None—There is no event.

- **Time**—Time when the event occurred for example 29 March 2004 at 11:00am is displayed as 29/03/2004 11:00:00.

- **Owner**—The Ethernet switch module or user that defined the event.

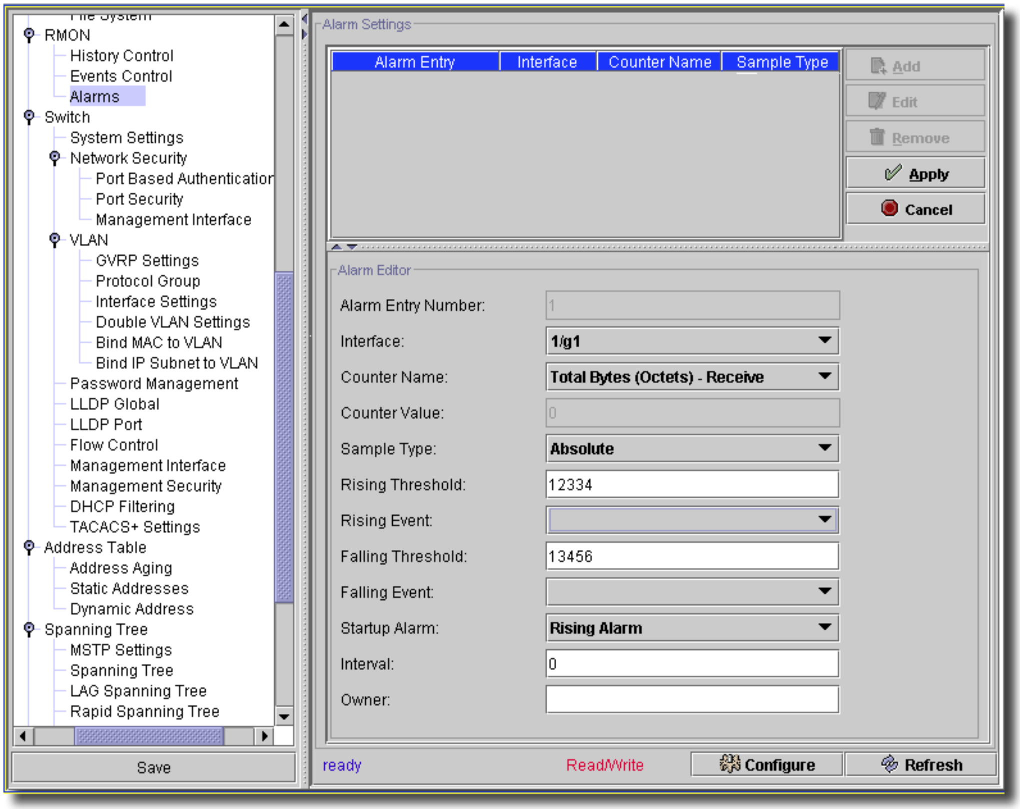
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

RMON -> Alarms

The RMON Alarms screen contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events.

Figure 13-91. RMON Alarm Configuration



Alarm Entry	Interface	Counter Name	Sample Type

Alarm Entry Number: 1

Interface: 1/g1

Counter Name: Total Bytes (Octets) - Receive

Counter Value: 0

Sample Type: Absolute

Rising Threshold: 12334

Rising Event:

Falling Threshold: 13456

Falling Event:

Startup Alarm: Rising Alarm

Interval: 0

Owner:

You can *Edit* RMON Alarm Control settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. Click *Add* to create a new group of settings, or select an existing interface listed in the upper portion of the screen and click *Edit* the editor opens (the lower portion of the screen) with the following fields:

- **Alarm Entry**—Indicates a specific alarm.

- **Interface**—The interface number for which RMON statistics appear.

- **Counter Name**—The selected MIB variable.

- **Counter Value**—The value of the selected MIB variable.

- **Sample Type**—Specifies the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:

  Delta—Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

  Absolute—Compares the values directly with the thresholds at the end of the sampling interval.

- **Rising Threshold**—The rising counter value that triggers the rising threshold alarm.

- **Rising /Falling Event**—Two fields that indicate the mechanism reporting alarms - LOG, TRAP, or a combination of both. When you select LOG, no saving mechanism exists in either the switch module or in the management system. However, if the switch module is not being reset, it remains in the switch module LOG table. If you select TRAP, the trap's general mechanism generates and reports an SNMP trap. You can save the TRAP using the same mechanism.

- **Falling Threshold**—The falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on the bottom of the graph bars

- **Startup Alarm**—The trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.

- **Interval (sec)**—Alarm interval time.

- **Owner**—Switch module or user that defined the alarm.

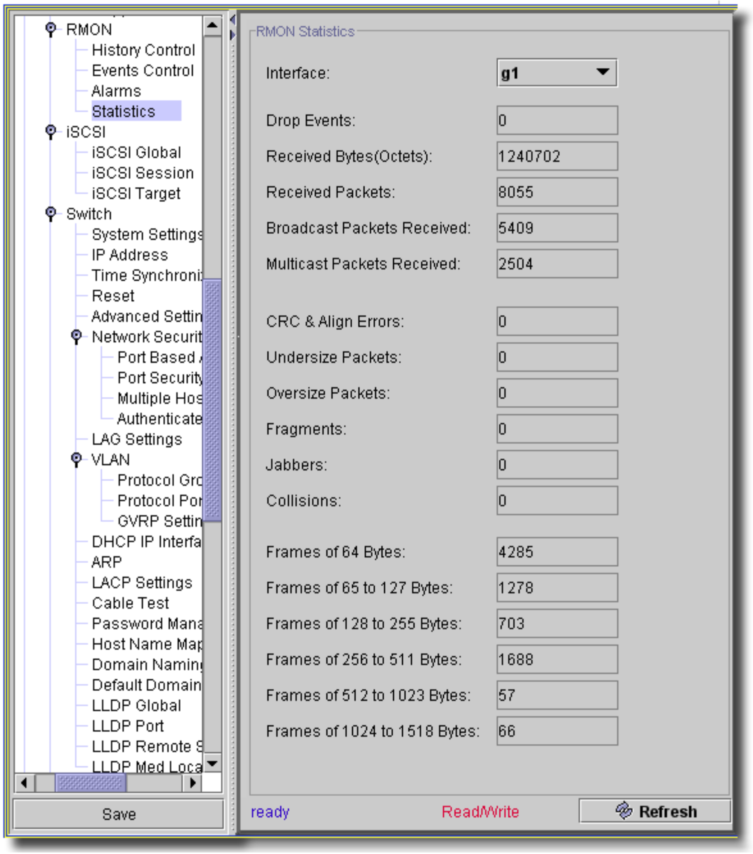
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

RMON -> Statistics

This screen displays the RMON statistics for the selected device.

Figure 13-92. RMON -> Statistics



Interface: g1

Drop Events: 0

Received Bytes(Octets): 1240702

Received Packets: 8055

Broadcast Packets Received: 5409

Multicast Packets Received: 2504

CRC & Align Errors: 0

Undersize Packets: 0

Oversize Packets: 0

Fragments: 0

Jabbers: 0

Collisions: 0

Frames of 64 Bytes: 4285

Frames of 65 to 127 Bytes: 1278

Frames of 128 to 255 Bytes: 703

Frames of 256 to 511 Bytes: 1688

Frames of 512 to 1023 Bytes: 57

Frames of 1024 to 1518 Bytes: 66

These statistics are read-only, but at the top of the screen, you can select from among the discovered interfaces with the *Interface* pick list. Here are the fields:

- **Drop Events**—Number of dropped events that have occurred on the interface since the device was last refreshed.
- **Received Bytes (Octets)**—Number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets**— Number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.
- **Multicast Packets Received**—Number of good Multicast packets received on the interface since the device was last refreshed.

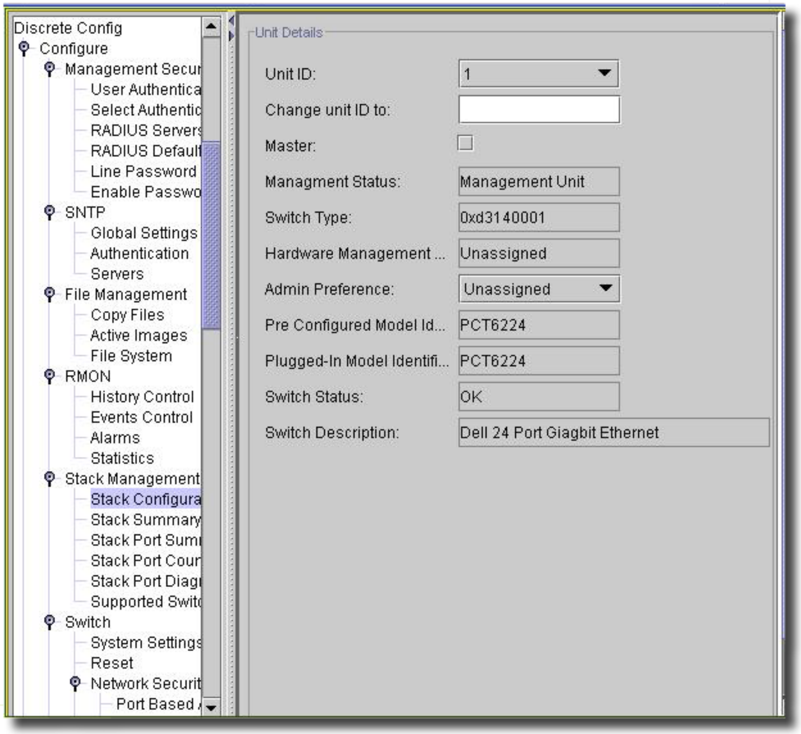
- **Broadcast Packets**—Number of good broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets
- **CRC & Align Errors**— Number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Oversize Packets**—Number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Undersize Packets**—Number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Fragments**—Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
- **Jabbers**—Number of jabbers (packets longer than 1518 octets) received on the interface since the device was last refreshed.
- **Collisions**—Number of collisions received on the interface since the device was last refreshed.
- **Frames of xx Bytes**—Number of xx-byte frames received on the interface since the device was last refreshed.

You do not need to click *Refresh* to update the screen when you change interfaces, but you may want to refresh the screen to get more current data.

Stack Management -> Stack Configuration

This screen configures stack configuration for the selected device. On some devices, it consists of a single checkbox to switch the master from Unit-1 to Unit-2. Check to activate this switch. Other devices have a series of more complex screen.

Figure 13-93. Stack Management -> Stack Configuration



Unit Details

Unit ID: 1

Change unit ID to:

Master: □

Managment Status: Management Unit

Switch Type: 0xd3140001

Hardware Management ... Unassigned

Admin Preference: Unassigned

Pre Configured Model Id... PCT6224

Plugged-In Model Identifi... PCT6224

Switch Status: OK

Switch Description: Dell 24 Port Giagbit Ethernet

This screen has the following fields:

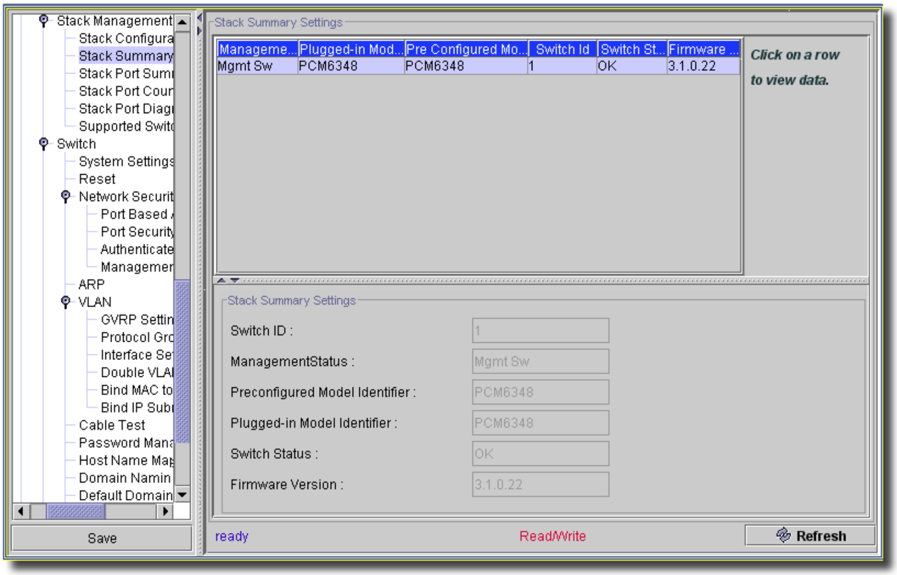
- **Unit ID**—Select the identifier for the unit to be configured.
- **Change unit ID to** —Enter the new identifier for the unit to be configured. Admin users can renumber the switch ID of the selected switch. This field is nonconfigurable for users with read-only access.
- **Master**—Check if you want this unit to be a master (management) unit in preference to another unit. The default value for this setting is Unassigned.
- **Management Status**—Displays whether the selected switch is configured as the Master switch (displays Management Unit) or a normal stacking member (Unassigned). The default value for this setting is Unassigned.
- **Switch Type**—Displays the switch type hardware ID.

- **Hardware Management**—Management preference by hardware configuration to be considered for selection as Management unit.
- **Admin Preference**—Determines whether this unit can become the master switch. Values range from Disable (the unit cannot support Master Switch function) to Preference 12. The higher value means that the unit is more desirable than another unit with lower value for running the management function.
- **Pre Configured Model Identifier**—A 16-byte character string to identify the pre-configured model of the selected unit.
- **Plugged-In Model Identifier**—A 16-byte character string to identify the plugged-in model of the selected unit.
- **Switch Status**—Displays the status of the selected unit. The possible values are: *OK* (The unit is in place and functioning), *Unsupported* (The unit is in place, but can not function as a member of the stack), *Code Mismatch* (The software of the switch does not match the master unit software), *Config Mismatch* (The configuration of the switch does not match the master unit configuration), *Not Present* (The selected unit is not present).
- **Switch Description**—80-byte data field that identifies the device.

Stack Management -> Stack Summary

This screen summarizes stack configuration for the selected device.

Figure 13-94. Stack Management -> Stack Summary



Manageme...	Plugged-in Mod...	Pre Configured Mo...	Switch Id	Switch St...	Firmware ...
Mgmt Sw	PCM6348	PCM6348	1	OK	3.1.0.22

Switch ID : 1

ManagementStatus : Mgmt Sw

Preconfigured Model Identifier : PCM6348

Plugged-in Model Identifier : PCM6348

Switch Status : OK

Firmware Version : 3.1.0.22

Select a unit to display a summary of its stack data. The screen that appears at the bottom of this window has the following fields:

- **Switch ID**—Select the identifier for the unit. The maximum number of units allowed in the stack is 8.

- **Interface**—Identifies the stack interface assigned to the unit.

- **Configured Stack Mode**—Indicates whether or not each unit is able to participate in the stack.

- **Running Stack Mode**—Indicates whether or not each unit is actually participating in the stack.

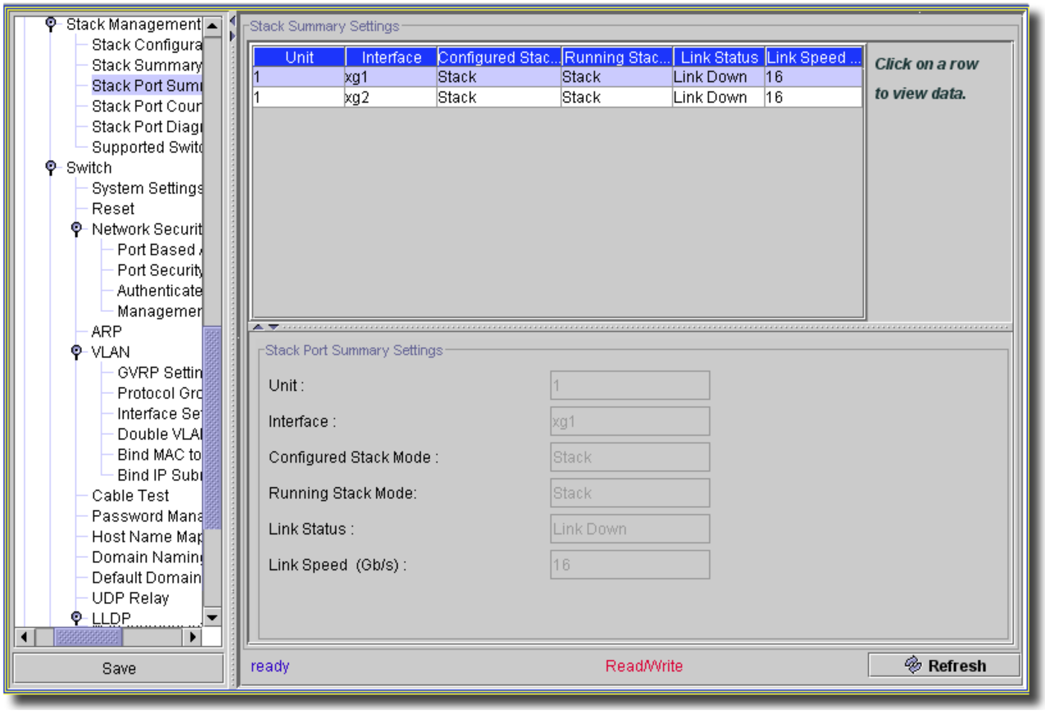
- **Link status**—Indicates whether or not the stack interface for each unit is operating.

- **Link speed (Gb/s)**—Indicates the nominal speed of each unit's link.

Stack Management -> Stack Port Summary

This screen summarizes stack port configuration for the selected device.

Figure 13-95. Stack Management -> Stack Port Summary



Unit	Interface	Configured Stac...	Running Stac...	Link Status	Link Speed ...
1	xg1	Stack	Stack	Link Down	16
1	xg2	Stack	Stack	Link Down	16

Unit : 1

Interface : xg1

Configured Stack Mode : Stack

Running Stack Mode: Stack

Link Status : Link Down

Link Speed (Gb/s) : 16

Select a unit to display a summary of its stack port data. The screen that appears at the bottom of this window has the following fields:

- **Unit**—Select the identifier for the unit.

- **Interface**—Displays whether the selected switch is configured as the Master switch (displays Management Unit) or a normal stacking member (Unassigned). The default value for this setting is Unassigned.

- **Pre Configured Model Identifier**—A 16-byte character string to identify the pre-configured model of the selected unit.

- **Plugged-In Model Identifier**—A 16-byte character string to identify the plugged-in model of the selected unit.

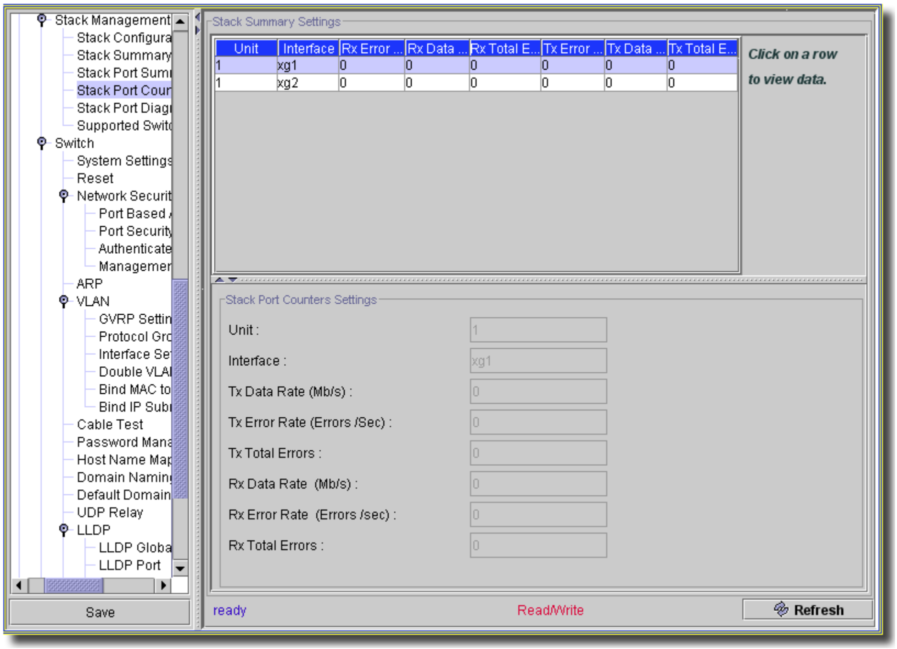
- **Switch Status**—Displays the status of the selected unit. The possible values are: *OK* (The unit is in place and functioning), *Unsupported* (The unit is in place, but can not function as a member of the stack), *Code Mismatch* (The software of the switch does not match the master unit software), *Config Mismatch* (The configuration of the switch does not match the master unit configuration), *Not Present* (The selected unit is not present).

- **Firmware Version**—The version number for the firmware on the selected stack device.

Stack Management -> Stack Port Counters

This screen summarizes stack port counters for the selected device.

Figure 13-96. Stack Management -> Stack Port Counters



Unit	Interface	Rx Error ...	Rx Data ...	Rx Total E...	Tx Error ...	Tx Data ...	Tx Total E...
1	xg1	0	0	0	0	0	0
1	xg2	0	0	0	0	0	0

Unit : 1

Interface : xg1

Tx Data Rate (Mb/s) : 0

Tx Error Rate (Errors /Sec) : 0

Tx Total Errors : 0

Rx Data Rate (Mb/s) : 0

Rx Error Rate (Errors /sec) : 0

Rx Total Errors : 0

Select a unit to display a its stack port counter data. The screen that appears at the bottom of this window has the following fields:

- **Unit**—The subordinate switch being viewed.

- **Interface**—The name of the interface.

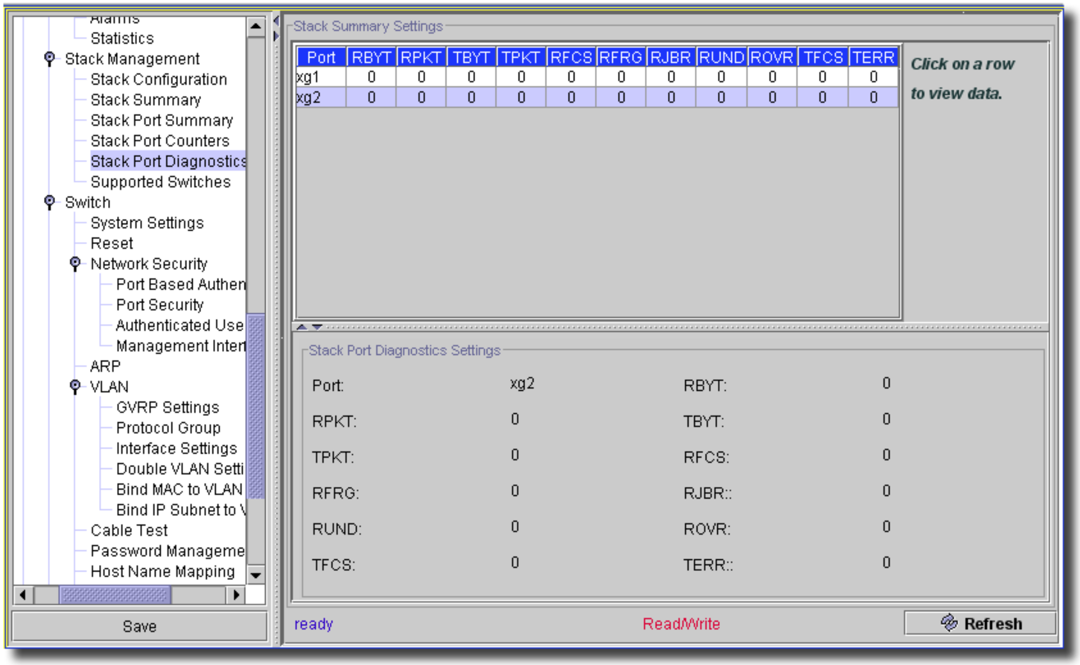
- **Tx Data Rate (Mb/s)**—The speed at which the data is transmitted.

- **Transmit Error Rate (Errors/sec)**— The number of errors transmitted per second.
- **Total Errors**—Total number of errors transmitted.
- **Rx Data Rate (Mb/s)**—Indicates the speed at which the data is received.
- **Receive Error Rate (Errors/sec)**—Indicates the number of errors received per second.
- **Total Errors**—Total number of errors received.

Stack Management -> Stack Port Diagnostics

This screen displays stack port diagnostic settings.

Figure 13-97. Stack Management -> Stack Port Diagnostics



Port	RBYT	RPKT	TBYT	TPKT	RFCS	RFRG	RJBR	RUND	ROVR	TFCS	TERR
xg1	0	0	0	0	0	0	0	0	0	0	0
xg2	0	0	0	0	0	0	0	0	0	0	0

Click on a row to view data.

Port:	xg2	RBYT:	0
RPKT:	0	TBYT:	0
TPKT:	0	RFCS:	0
RFRG:	0	RJBR::	0
RUND:	0	ROVR:	0
TFCS:	0	TERR::	0

This displays the following:

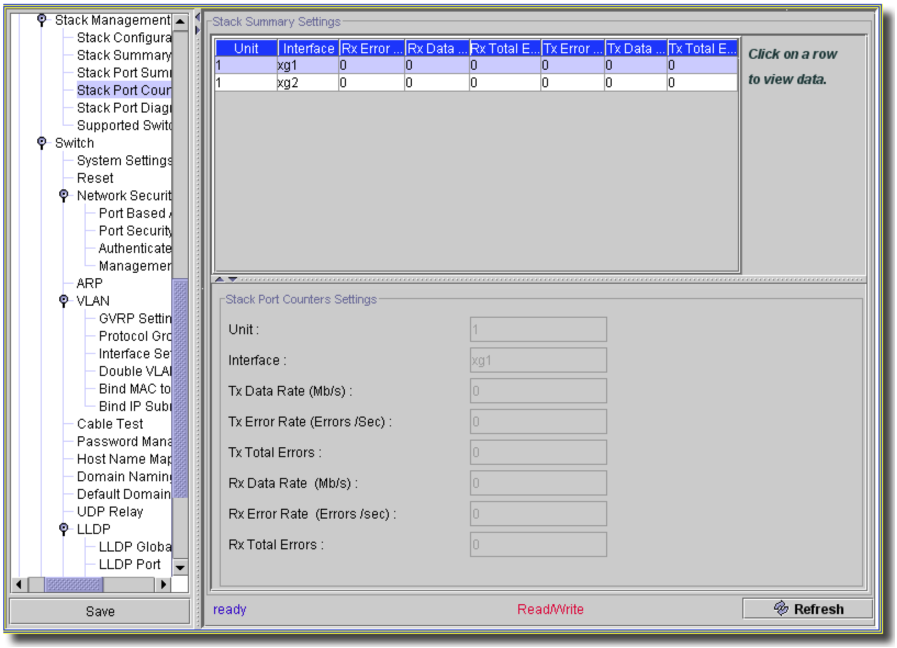
- **Port**—The port selected in the rows at the top of this screen.
- **RPKT**—Received Packets
- **TPKT**—Transmitted Packets
- **RFRG**—Received Fragments
- **RUND**—Received undersized packets
- **TFCS**—Transmitted frame check sequence errors.
- **RBYT**—Received bytes.

- **TBYT**—Transmitted bytes.
- **RFCS**—Received frame check sequence errors.
- **RJBR**—Received jabbers.
- **ROVR**—Received oversized packets.
- **TERR**—Transmit errors.

Stack Management -> Supported Switches

This screen summarizes stack port counters for the selected device.

Figure 13-98. Stack Management -> Stack Port Counters



Unit	Interface	Rx Error ...	Rx Data ...	Rx Total E...	Tx Error ...	Tx Data ...	Tx Total E...
1	xg1	0	0	0	0	0	0
1	xg2	0	0	0	0	0	0

Unit : 1

Interface : xg1

Tx Data Rate (Mb/s) : 0

Tx Error Rate (Errors /Sec) : 0

Tx Total Errors : 0

Rx Data Rate (Mb/s) : 0

Rx Error Rate (Errors /sec) : 0

Rx Total Errors : 0

Select a unit to display a its stack port counter data. The screen that appears at the bottom of this window has the following fields:

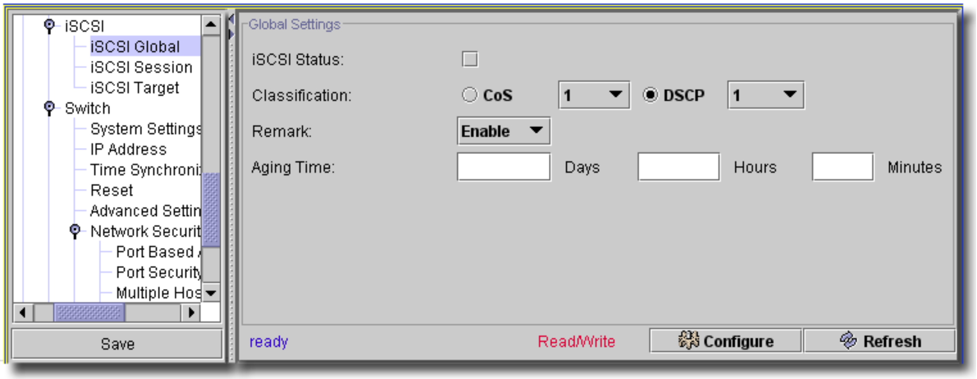
- **Supported Switches**—The pick list lets you select switches supported.
- **Switch Index**—The index assigned to the selected switch type.
- **Switch Type**—Specify the type of switch hardware when creating a new switch.
- **Switch Model ID**—A 16-byte character string to identify the model of the supported switch.
- **Description**—A 256-byte data field used to identify the device.

- **Management Preference**—Determines whether this unit is capable of becoming the master switch. If the value is set to zero then the unit cannot support the Master Switch function. A higher value means that the unit is more desirable than another unit with lower value for running the management function. The device manufacturer sets the initial value of this field.
- **Expected Code Type**—The release number and version number of the code expected.

iSCSI -> Global

This screen configures global settings for iSCSI on the selected device.

Figure 13-99. iSCSI -> Global



Global Settings

iSCSI Status: □

Classification: ○ CoS 1 ● DSCP 1

Remark: Enable

Aging Time: Days Hours Minutes

This screen contains the following fields and checkboxes:

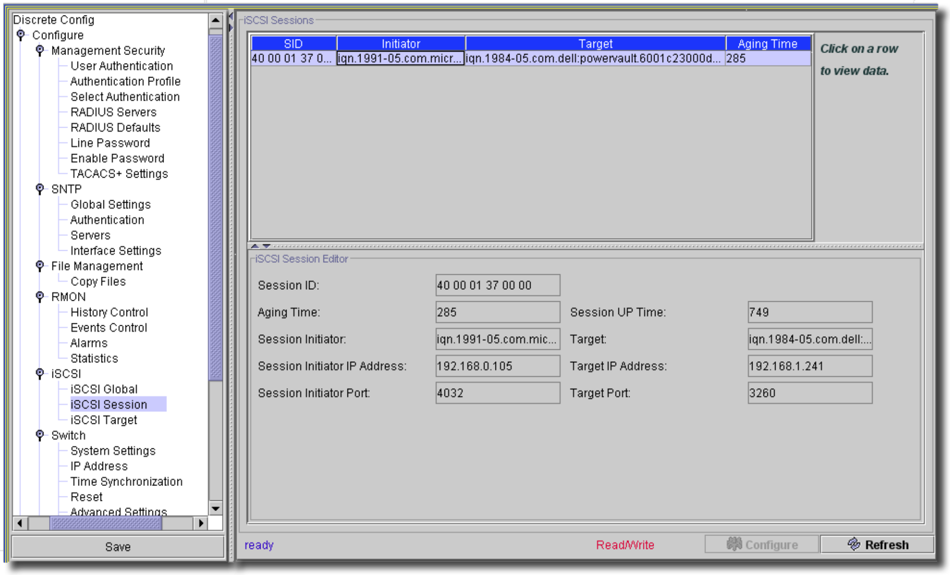
- **iSCSI Status**—Whether iSCSI Optimization is enabled on the device. The default value is enabled.
- **Classification**—Use the radio buttons to select between *CoS* or *DSCP*. Select a number from the pick list to the right of the selected button.
- **Remark**—Whether iSCSI remarks are enabled on the device. (Select from the pick list)
- **Aging Time**—How long the device will wait after the last received frame of an iSCSI session before deleting the session from the list. Enter *Days*, *Hours* and *Minutes*.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

iSCSI -> Session

The iSCSI Targets Table contains information about iSCSI targets in the network.

Figure 13-100. iSCSI -> Session



SID	Initiator	Target	Aging Time
40 00 01 37 0...	iqn.1991-05.com.micr...	iqn.1984-05.com.dell:powervault.6001c23000d...	285

Session ID:	40 00 01 37 00 00		
Aging Time:	285	Session UP Time:	749
Session Initiator:	iqn.1991-05.com.mic...	Target:	iqn.1984-05.com.dell:...
Session Initiator IP Address:	192.168.0.105	Target IP Address:	192.168.1.241
Session Initiator Port:	4032	Target Port:	3260

Click a row to view the configuration of its contents in the lower panel. It contains the following fields:

- **Session ID**—The iSCSI session ID.

- **Aging Time**—The time left until the session ages out and is removed.

- **Target Name**—The name of the target.

- **Session Initiator / IP Address / Port** —The name of the initiator, its address and port.

When you click Details, the following additional information is shown for the session:

- **Session Up Time**—The time since the first frame of the session.

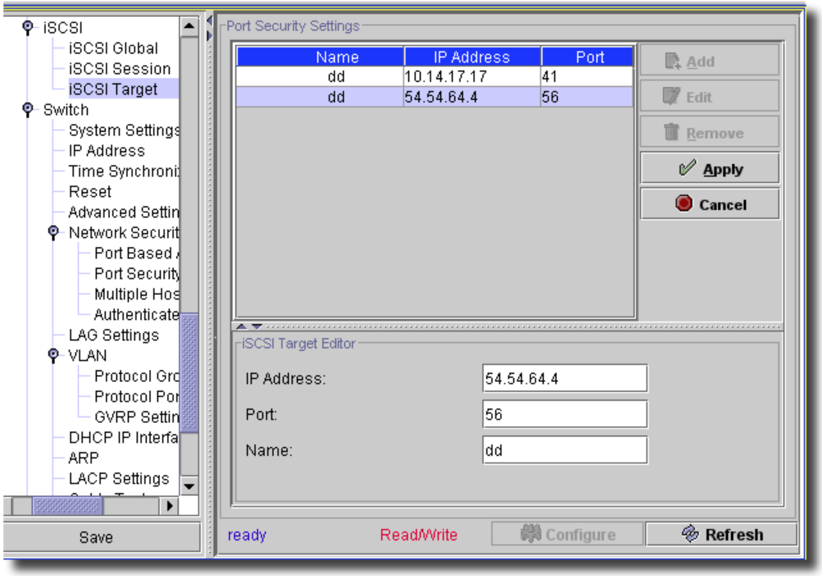
- **Target / IP Address/TCP Port**—The IP address and TCP port used by the target in the session.

Click *Refresh* to renew the device information on this screen.

iSCSI -> Target

This screen displays the iSCSI target settings for the selected device.

Figure 13-101. iSCSI -> Target



Name	IP Address	Port
dd	10.14.17.17	41
dd	54.54.64.4	56

IP Address: 54.54.64.4

Port: 56

Name: dd

Click *Remove* to delete a selected, listed item. You can *Edit* target settings for the selected device in this screen. Click *Add* to create a new setting, or select an existing setting listed in the upper portion of the screen and click *Edit* the editor opens (the lower portion of the screen) with the following fields:

- **IP Address**—The address of the iSCSI target. The IP address 0.0.0.0 is Any IP Address.

- **Port**—The TCP port of the iSCSI target.

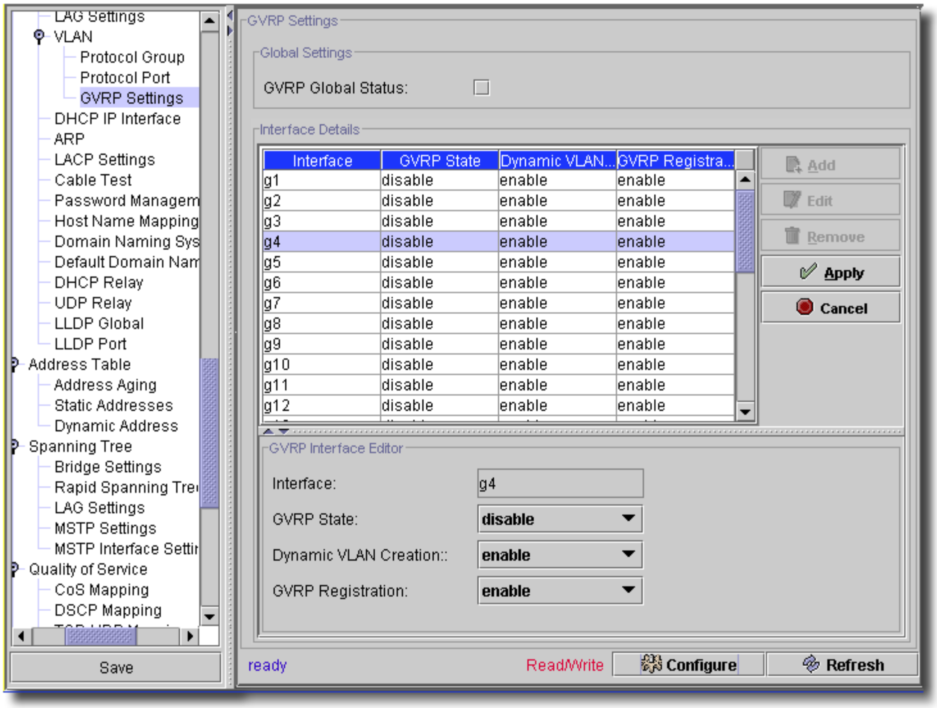
- **Name**—The name of the iSCSI target.

Click *Apply* to accept your edits, or *Cancel* to abandon them. Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

VLAN -> GVRP Global Parameters

GARP VLAN Registration Protocol (GVRP) is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge and register VLAN membership.

Figure 13-102. GRVP Global Parameters



GVRP Global Status: □

Interface	GVRP State	Dynamic VLAN...	GVRP Registra...
g1	disable	enable	enable
g2	disable	enable	enable
g3	disable	enable	enable
g4	disable	enable	enable
g5	disable	enable	enable
g6	disable	enable	enable
g7	disable	enable	enable
g8	disable	enable	enable
g9	disable	enable	enable
g10	disable	enable	enable
g11	disable	enable	enable
g12	disable	enable	enable

Interface: g4

GVRP State: disable

Dynamic VLAN Creation:: enable

GVRP Registration: enable

The GVRP Global Parameters screen enables GVRP globally. GVRP can also be enabled on a per-interface basis. Click *Remove* to delete a selected, listed item. You can *Edit* GVRP settings for the selected device in this screen. Click *Add* to create a new group of settings, or select an existing interface listed in the upper portion of the screen and click *Edit* the editor opens (the lower portion of the screen) with the following fields:

- **GVRP Global Status**—Enables or disables GVRP on the switch module. GVRP is disabled by default.
- **Interface**—The port or LAG for which GVRP is enabled.
- **GVRP State**—Enables or disables GVRP on an interface.
- **Dynamic VLAN Creation**—Enables or disables VLAN creation through GVRP.
- **GVRP Registration**—The GVRP Registration status.

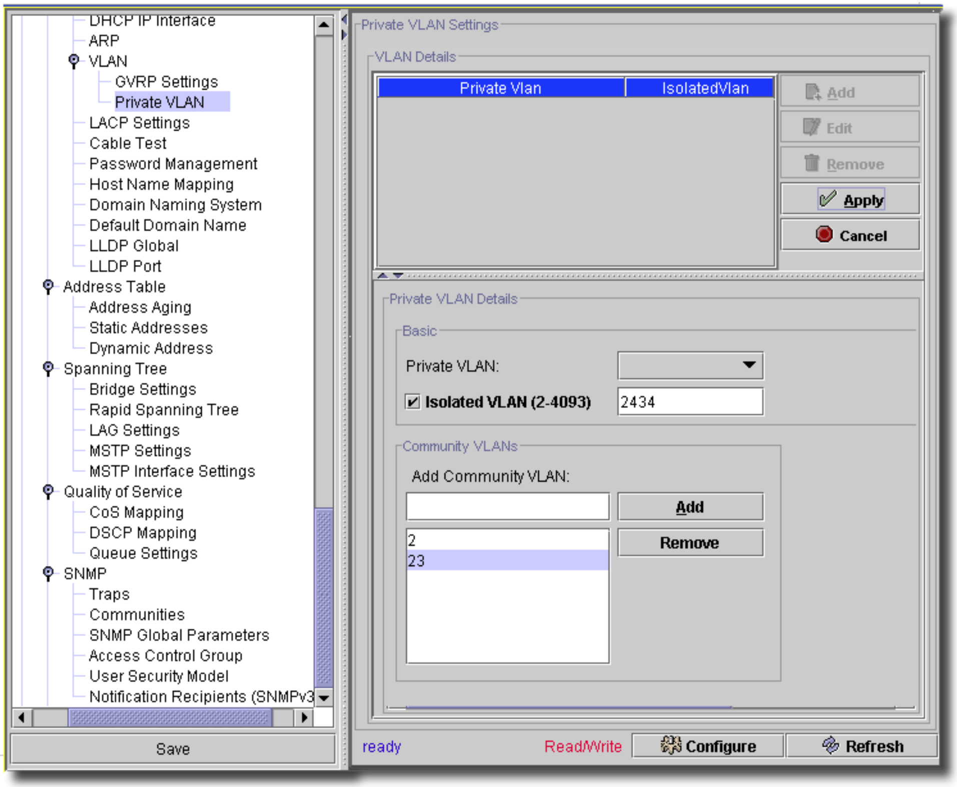
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

VLAN -> Private VLAN

This screen configures Private VLANs on the selected device.

Figure 13-103. VLAN -> Private VLAN



Private Vlan	IsolatedVlan

Private VLAN:

☑ Isolated VLAN (2-4093) 2434

Add Community VLAN:

2
23

Click *Remove* to delete a selected, listed item. Click *Add* to create a new private VLAN, or *Edit* to alter a selected existing one, listed at the top of this screen, and the *Private VLAN Details* editor opens at the bottom of the screen. Click *Accept* to enter your edits in those private VLANs listed (or *Cancel*) to abandon them. This editor has the following fields:

Basic

- **Private VLAN**—Select a number from the pick list.

- **Isolated VLAN (2 - 4093)**—Check to enable, and if enabled, enter a number.

Community VLANs

Enter a community VLAN number in the field under *Add Community VLAN*, then click *Add* to list one here. You can also select a listed VLAN and click *Remove* to delete it from the list.

NOTE:

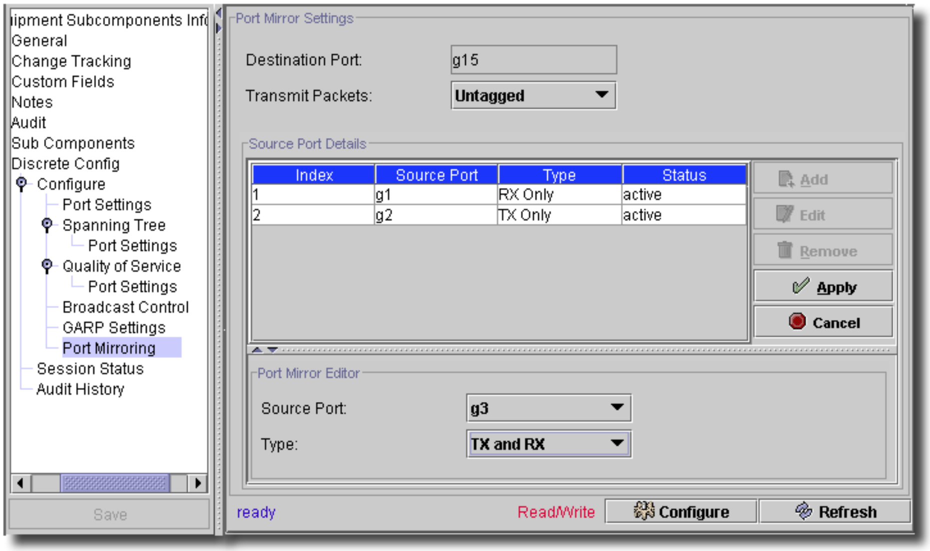
Private VLANs only appear on some devices.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Port Mirroring

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from monitored port to a monitoring port. Port Mirroring settings are found at the Port level within the Reference Tree.

Figure 13-104. Port Mirroring



Destination Port: g15

Transmit Packets: Untagged

Index	Source Port	Type	Status
1	g1	RX Only	active
2	g2	TX Only	active

Source Port: g3

Type: TX and RX

Port mirroring is configured by selecting a specific port to copy all packets, and different ports from which the packets copied. Click *Remove* to delete a selected, listed item. The following rules apply:

Before configuring Port Mirroring, note the following:

- Monitored port cannot operate faster than the monitoring port.
- All the RX/TX packets should be monitored to the same port.
- The Destination port cannot be configured as a source port.
- Source Ports cannot be configured as a destination port.
- Destination port cannot be a LAG member.
- Source Ports cannot be a LAG member.

- IP interfaces are not configured on the Destination (or Monitoring).
- GVRP is not enabled on the Destination (or Monitoring).
- The Destination (or Monitoring) port is not a VLAN member.
- Only one Destination (or Monitoring) port can be defined.
- A maximum of 4 ports can be monitored (both Rx and Tx).
- All packets are transmitted tagged from the destination port.
- Monitored all RX/TX packets to the same port.

NOTE:

Internal ports may be effected by enabling Port Mirroring. When a port is set to be a target port for a port-mirroring session, all normal operations on it are suspended. This includes Spanning Tree and LACP.

General Port Mirror Settings consist of the following:

- **Destination Port**—The port number to which port traffic is copied. Also known as the monitoring port.

- **Transmit Packets**—Select whether packets transmitted are *Tagged*, or *Untagged*. This field may not be visible for all switches.

You can *Edit* Port Mirroring settings for a source port in the table below these two fields. Click A*dd* to create a new group of settings, or select an existing interface listed in the upper portion of the screen and click *Edit* the editor opens (the lower portion of the screen) with the following fields:

- **Source Port**—Defines the port number from which port traffic is mirrored. Also known as the monitored ports.

- **Type**—Indicates if the source port is RX, TX, or both RX and TX.

Click A*pply* to accept the edits you have configured and add it to the list. C*ancel* abandons your edits.

Click C*onfigure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Routing Protocols

The following screens appear in Dell devices that support these routing protocols. Click C*onfigure* to apply your edits to the device and/or database. Click *Refresh* to update the screen with the latest device information.

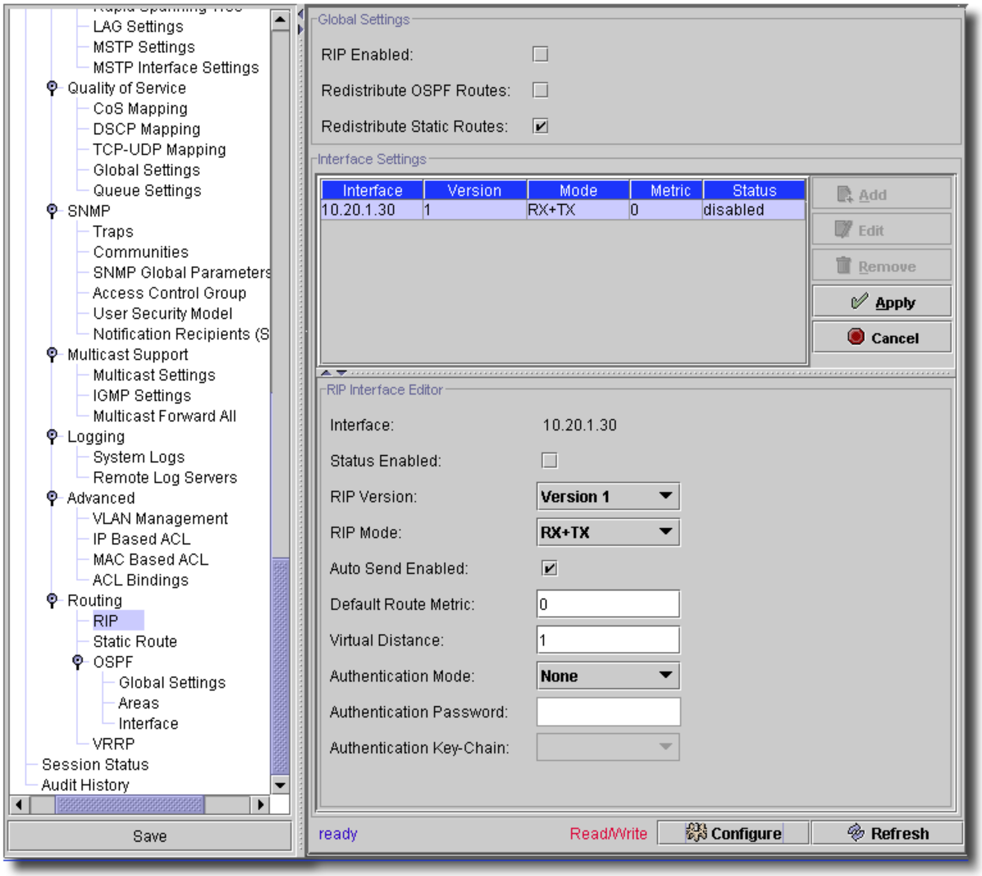
RIP

Routing Information Protocol (RIP) is the most commonly used Internet standard for interior gateway protocols. The protocol broadcasts routing information to determine the quickest route to the next destination. RIP is a distance vector routing protocol that is best used in small networks. Routes are determined through the smallest hop count. Routing updates contain pairs of values consisting of an IP address and the distance to the node. RIP version 2 does the following:

- Supports subnet masks.

- Provides authentication methods.
- Supports routing protocols.
- Provides larger distribution and smaller bandwidth overhead requirements.

Figure 13-105. Routing: RIP



Global Settings

RIP Enabled: □

Redistribute OSPF Routes: □

Redistribute Static Routes: ☑

Interface Settings

Interface	Version	Mode	Metric	Status
10.20.1.30	1	RX+TX	0	disabled

RIP Interface Editor

Interface: 10.20.1.30

Status Enabled: □

RIP Version: Version 1

RIP Mode: RX+TX

Auto Send Enabled: ☑

Default Route Metric: 0

Virtual Distance: 1

Authentication Mode: None

Authentication Password:

Authentication Key-Chain:

ready Read/Write

The application's RIP screen includes the following fields.

Global Settings

- **RIP Enabled**—Enables or disables RIP on the device.

- **Redistribute OSPF Routes**—When enabled, redistributes routes from OSPF to RIP. Redistribution of routes involves importing foreign routing interfaces to the OSPF protocol.

- **Redistribute Static Routes**—When enabled, redistributes routes from static

- routes to RIP.

RIP Interface Editor

When you Edit an interface, you can alter the following fields (displayed in the Interface Settings table):

- **Interface**—A read-only reminder of the current interface.

- **Status Enabled**—Check to enable.

- **RIP Version**—The type of RIP being broadcast. Possible values are:

  Version 1–Broadcasts RIP updates compliant with RFC 1058.

  Version 2–Indicates the device is broadcasting RIP 2 updates.

- **RIP Mode**—The type of RIP operation. Possible values are:

  RX–The device can receive RIP receive broadcasts.

  RX & TX–The device can receive RIP receive and transmit broadcasts.

- **Auto Send Enabled**—Check to enable. When enabled, the device can advertise RIP messages in the default metric only, so stations can learn the default router address. This prevents the router from sending excessive RIP updates on links where no routers exist to receive them. While Auto Send is active, the router sends a short-form RIP update, which allows stations listening for RIP to do router discovery, and so on, and to send an RIP update to routers added to the network later. If an interface receives a RIP update, Auto Send is disabled on that interface, and full RIP updates are sent. If the device detects another RIP message, Auto Send is disabled.

- **Default Route Metric**—The default route entry metric in RIP updates originating on this interface. Zero indicates that no default route is originated.

- **Virtual Distance**—Virtual number of hops assigned to the interface. This fine-tunes the RIP routing algorithm.

- **Authentication Mode**—The interface authentication type, Password or MD5, that authenticates RIP version 2 messages.

- **Authentication Password**—The authentication password.

- **Authentication Key-Chain**—The authentication key chain.

- Click *Apply* to accept your edits, or *Cancel* to abandon them.

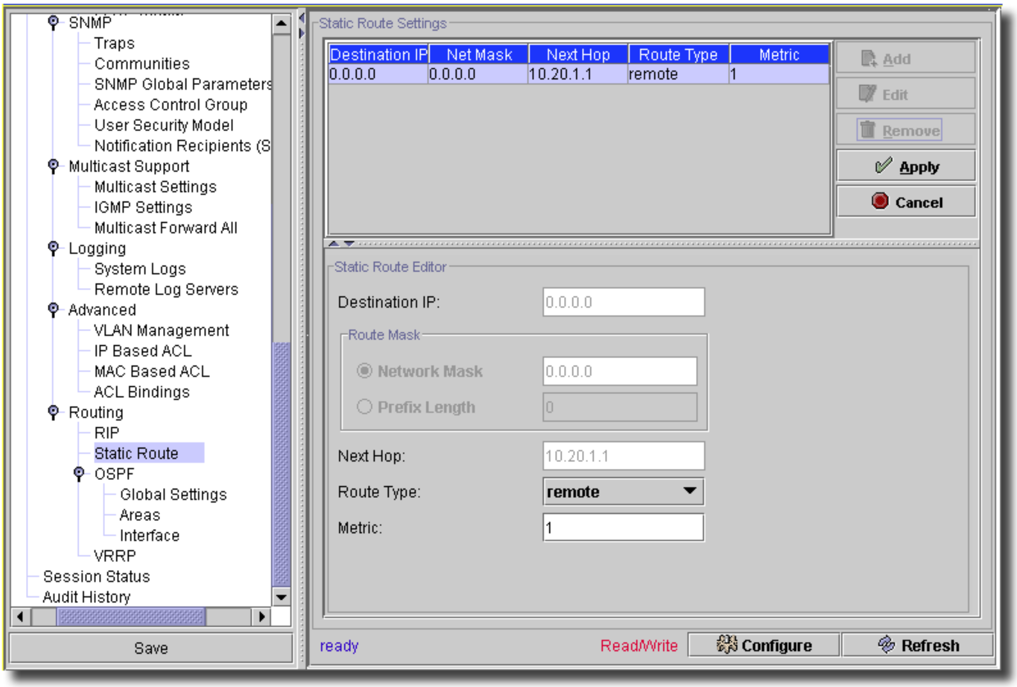
NOTE:

This screen is not available for all equipment.

Static Routes

Use this screen to define static routes.

Figure 13-106. Routing: Static Routes



Destination IP	Net Mask	Next Hop	Route Type	Metric
0.0.0.0	0.0.0.0	10.20.1.1	remote	1

Destination IP: 0.0.0.0

○ Network Mask 0.0.0.0

○ Prefix Length 0

Next Hop: 10.20.1.1

Route Type: remote

Metric: 1

You can *Edit* listed settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. Click *Add* to create a new group of settings, or select an existing interface listed in the upper portion of the screen and click *Edit* the editor opens with the following fields:

- **Destination IP**—Static route’s destination IP network.

Route Mask

- **Network Mask**—The destination network mask for this route.

- **Prefix Length**—The number of bits that comprise the destination IP address pre-fix. The length is between 1-32 bits.

- **Next Hop**—The next system address on the route.

- **Route Type**—Specifies how remote routing is handled. The possible field values are:

  Remote–Forward the packet.

  Reject–Drop the packet.

  Local–Send packet to a local network.

- **Metric**—Number of hops to the destination network.

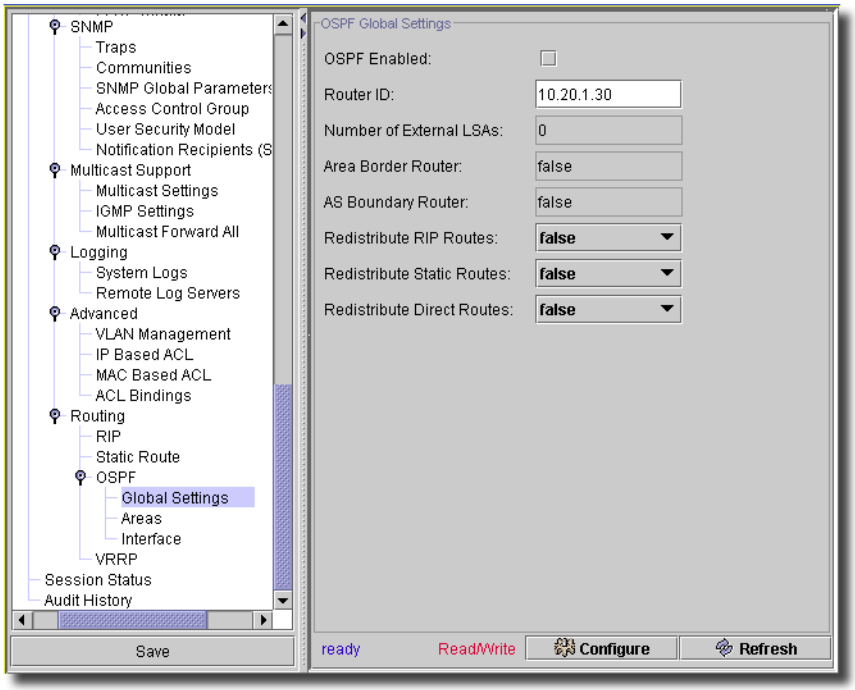
OSPF -> Global Settings

The Open Shortest Path First (OSPF) internal gateway protocol enables routers to exchange link state messages by gathering network information and determining the best routing path based on node distance. (OSPF discovers the best routing path based on node distance.)

OSPF is a link state protocol rather than a distance vector protocol and, therefore, needs less bandwidth than RIP. OSPF is enabled and defined by:

- Configuring OSPF Parameters
- Configuring OSPF Areas
- Configuring the OSPF Virtual Links
- Viewing the Link State Table
- Viewing the External Link State Table
- Viewing the OSPF Neighbor Table

Figure 13-107. Routing OSPF Global Settings



OSPF Global Settings

OSPF Enabled: □

Router ID: 10.20.1.30

Number of External LSAs: 0

Area Border Router: false

AS Boundary Router: false

Redistribute RIP Routes: false

Redistribute Static Routes: false

Redistribute Direct Routes: false

ready Read/Write

The OSPF Global Settings screen contains the following fields:

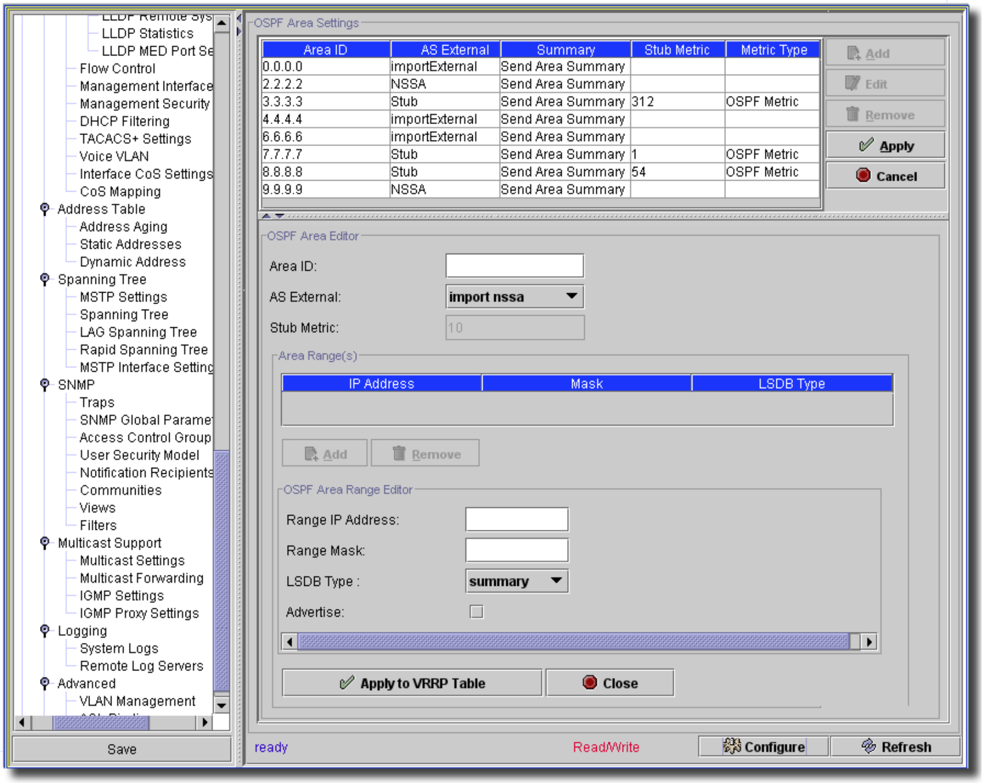
- **OSPF Enabled**—Enables OSPF on at least one interface. When selected, disables OSPF for all interfaces.

- **Router ID**—The router ID number. By default, this is an IP address on the device. Router ID is an optional field, with a default value of the smallest device IP interface.
- **Number of External LSAs**—The number of external link-state advertisements (LSAs) in the link-state database.
- **Area Border Router**—Indicates whether the device is an area border router. If the device is configured as an ABR, the device is connected to two or more areas. One area is the backbone area.
- **AS Boundary Router**—Indicates whether the device is configured as an ASBR (Autonomous System Boundary Router). If the device is configured as an ASBR, the device imports routing data from non-OSPF routing protocols. Redistribute RIP Routes—Checking this enables the redistribution of routes inserted into the IP routing table by the RIP protocol to advertise OSPF as external routes.
- **Redistribute RIP Routes**—Lets you advertise all external routes to RIP as external routes. This enables/disables redistribution of external direct routes.
- **Redistribute Static Routes**—Lets you advertise all statically configured routes as OSPF external routes. This enables/disables redistribution of static routes.
- **Redistribute Direct Routes**—Lets you advertise all external routes to OSPF as external routes. This enables/disables redistribution of external direct routes.

OSPF -> Areas

The Areas screen contains information for defining and maintaining OSPF areas within which interfaces and virtual links are defined. Once you create an OSPF area, OSPF is automatically enabled on all IP interfaces.

Figure 13-108. Routing OSPF Areas



OSPF Area Settings

Area ID	AS External	Summary	Stub Metric	Metric Type
0.0.0.0	importExternal	Send Area Summary		
2.2.2.2	NSSA	Send Area Summary		
3.3.3.3	Stub	Send Area Summary	312	OSPF Metric
4.4.4.4	importExternal	Send Area Summary		
6.6.6.6	importExternal	Send Area Summary		
7.7.7.7	Stub	Send Area Summary	1	OSPF Metric
8.8.8.8	Stub	Send Area Summary	54	OSPF Metric
9.9.9.9	NSSA	Send Area Summary		

OSPF Area Editor

Area ID:

AS External: import nssa

Stub Metric: 10

Area Range(s)

IP Address	Mask	LSDB Type

OSPF Area Range Editor

Range IP Address:

Range Mask:

LSDB Type : summary

Advertise: □

ready

Read/Write

You can *Edit* listed settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. Click *Add* to create a new group of settings, or select an existing interface listed in the upper portion of the screen and click *Edit* the editor opens with the following fields:

- **Area ID**—The area ID. The format is an IP address.

- **AS External**—Indicates whether this is a stub area. If it cannot import external LSAs, the area is a stub area. Otherwise, the area allows importing autonomous system (AS) external link state advertisements (LSA). Selectable options include *nssa*, *external*, *stub*.

- **Stub Metric**—(0-16777215) The metric of the default route created for the stub area. Stub areas do not import external AS. Therefore, a default route is created by the area border router for the stub area.

Area Range(s)

Click *Add* to add OSPF area ranges to those listed here, or select one and click *Remove* to delete it. When you add a range, the *OSPF Area Range Editor* opens at the bottom of the screen. This editor has the following fields:

- **Range IP Address / Mask**—The range IP address and mask of the OSPF area.

- **LSDB Type**—The link state database type. Select from *nssa*, or *summary*.

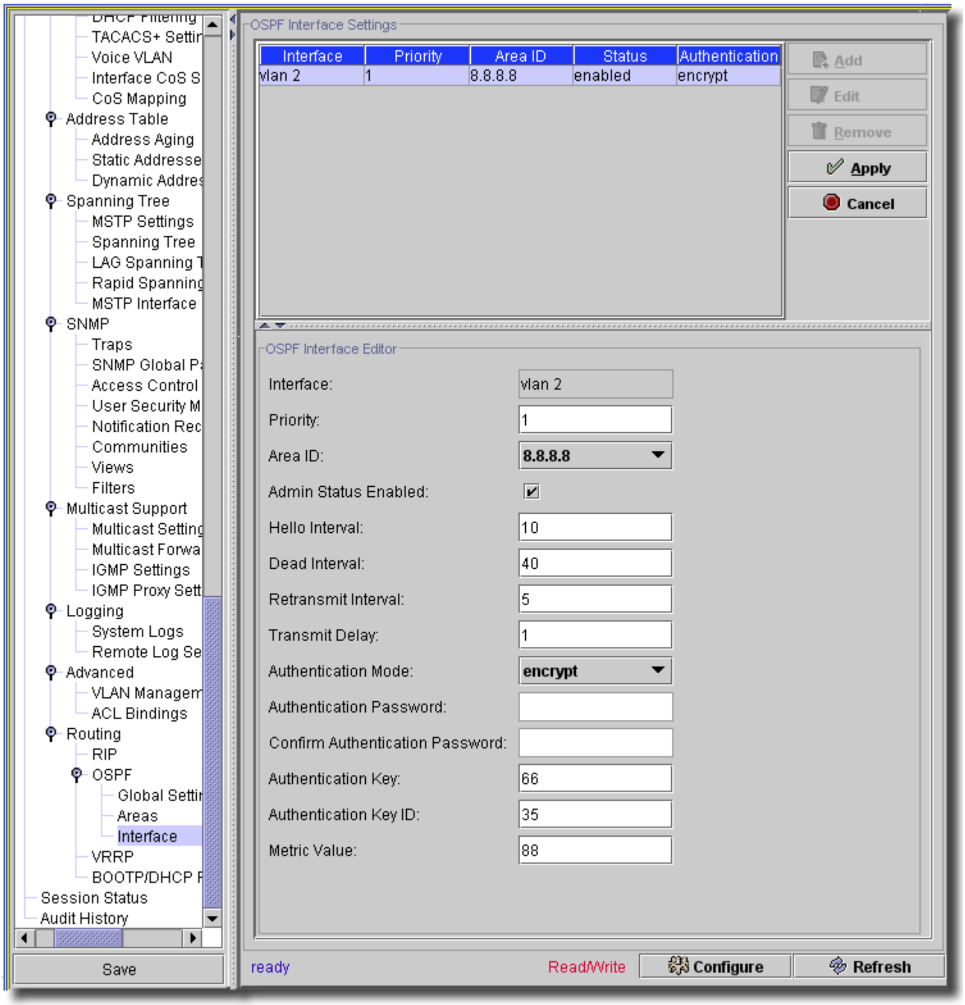
- **Advertise**—Check to advertise this range.

Click *Apply to VRRP Table* to accept your edits, or *Cancel* to abandon them. After you have finished editing the OSPF area, then click *Apply* to accept your edits (or *Cancel* to abandon them).

OSPF -> Interface

After OSPF global parameters and areas are defined, you can configure OSPF on each interface. The OSPF Interface table enables IP routing using OSPF-specific information.

Figure 13-109. Routing OSPF Interface



Interface	Priority	Area ID	Status	Authentication
vlan 2	1	8.8.8.8	enabled	encrypt

Interface:	vlan 2
Priority:	1
Area ID:	8.8.8.8
Admin Status Enabled:	☑
Hello Interval:	10
Dead Interval:	40
Retransmit Interval:	5
Transmit Delay:	1
Authentication Mode:	encrypt
Authentication Password:	
Confirm Authentication Password:	
Authentication Key:	66
Authentication Key ID:	35
Metric Value:	88

You can *Edit* listed settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. Click *Add* to create a new group of settings, or select an existing interface listed in the upper portion of the screen and click *Edit* the editor opens with the following fields:

- **Interface**—IP address of the OSPF interface.

- **Priority**—(0-255) The interface priority. The value 0 indicates that you cannot define the device as the designated device on the current network. If more than one device has the same priority, the router ID is used. The default is 1.
- **Area ID**—The OSPF interface area ID.
- **Admin Status Enabled**—Enables or disables the OSPF process.
- **Hello Interval**—(1-65535) Time (seconds) between Hello packets. All devices attached to a common network must have the same Hello interval. The default is 10 seconds.
- **Dead Interval**—(1-65535 or 2147483647, depending on the device type) Time (seconds) router Hello packets have not been detected, and the router times out. The value must be a multiple of the Hello Interval. All routers attached to a common network must have a value specified for this parameter. The default is 60 seconds.
- **Retransmit Interval**—(1-3600) Time (seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The value must be greater than the expected round-trip delay between any two routers on the attached network. The default is five seconds.
- **Transmit Delay**—(1-3600) Estimated time (seconds) required to send a link-state update packet on the interface. LSAs in the update packet have their age incremented by this amount before transmission. The default value is one second.
- **Authentication Mode**—The interface authentication type, Password or MD5, used to authenticate OSPF link state messages.
- **Authentication Password / Confirm Authentication Password**—The password (eight characters or less) that authenticates OSPF link state messages.
- **Authentication Key / Authentication Key ID**—The MD5 key and its ID that authenticates OSPF link sate messages. The key field is empty if none exists, however you can select the authentication as Message Digest-5 (MD5) with a blank key. You can still create key values with the HTTP cut thru to the device's web interface. MD5 authentication functions even while the key value combination is blank
- **Metric Value**—(1-65535)—The metric for this type of service on the interface.

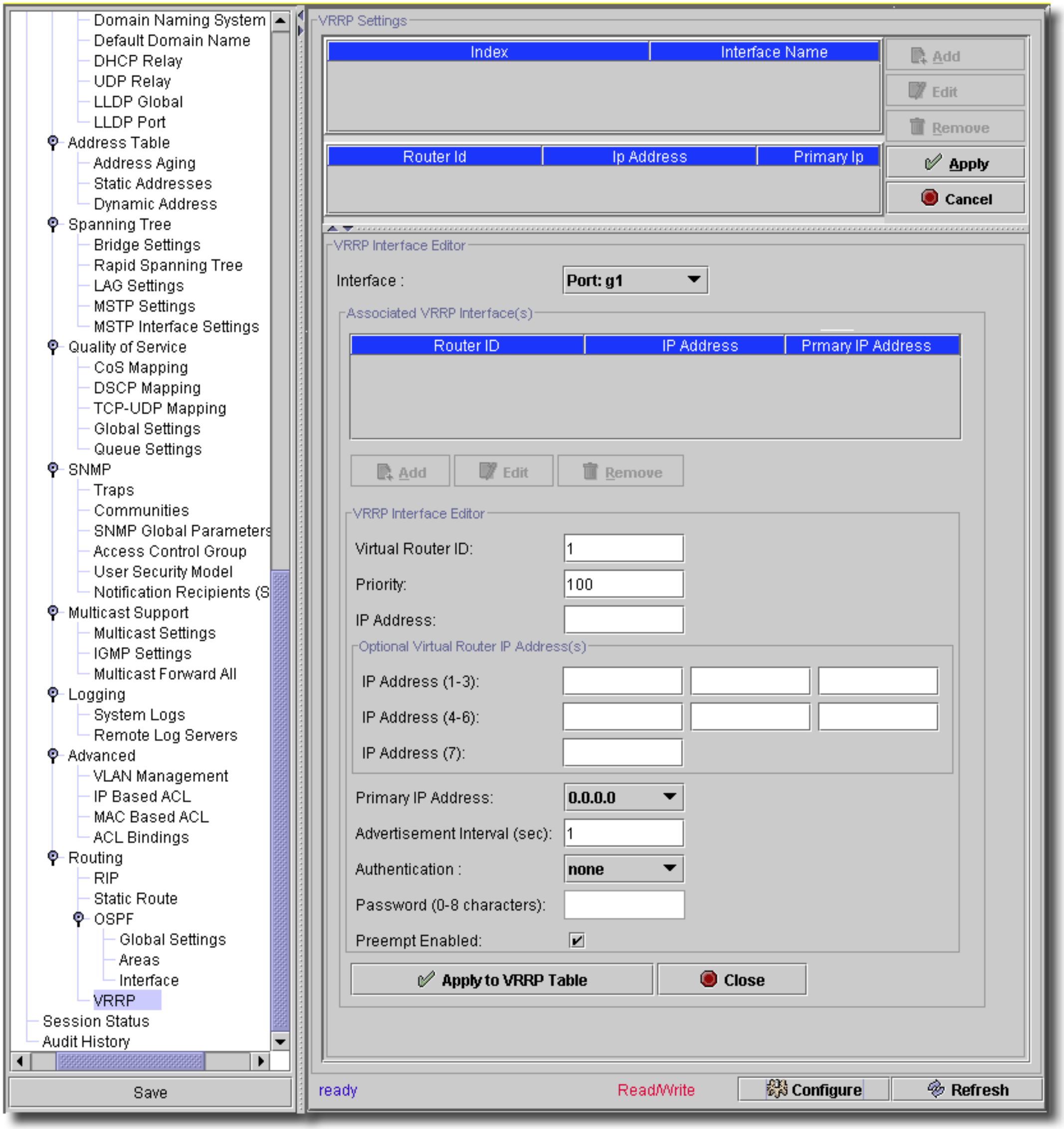
NOTE:

This screen is not available for all equipment.

VRRP

Virtual Router Redundancy Protocol (VRRP) specifies an elector protocol that dynamically assigns routing responsibility to one of the VRRP routers on the LAN (the master router). The election process enables dynamic failover of routing responsibility in case the master router becomes unavailable. The advantage of VRRP is that it eliminates the single-point-failure phenomenon inherent to the routing environment by providing a higher availability default path, while eliminating the need for configuration of dynamic routing or router discovery protocols on every end-host. The Virtual Router Redundancy Protocol (VRRP) page sets the switch's VRRP routing parameters.

Figure 13-110. Routing VRRP



Interface : Port: g1

Virtual Router ID: 1

Priority: 100

IP Address:

IP Address (1-3):

IP Address (4-6):

IP Address (7):

Primary IP Address: 0.0.0.0

Advertisement Interval (sec): 1

Authentication : none

Password (0-8 characters):

Preempt Enabled: ☑

ready ReadWrite

You can *Edit* listed settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. Click A*dd* to create a new group of settings, or select an existing interface listed in the upper portion of the screen7 and click *Edit* the editor opens. The VRRP screen contains the following fields:

VRRP Interface Editor

- **Interface**—Interface type and number attached to the VRRP router. Select from the pick list.

When you click Add, or select a listed VRRP interface, and select *Edit*, the associated editor lets you configure the following:

- **VRRP Router ID**—Virtual router identifier (1-255).
- **Priority—**Router priority used for the virtual router election process. The range is 1-255. The value may determine if a higher priority VRRP router overrides a lower priority VRRP router.
- **IP Address**—The VRRP router that is currently master for this virtual router.

Associated VRRP Interfaces

Use the Add, Edit or Remove buttons below the listed, associated interfaces to manage the list of interfaces associated with this virtual router. This table also repeats at the bottom left of the screen, displaying associated interfaces when you select a listed index and interface name.

Optional Virtual Router IP Addresses

- **IP Address (1-3)**—Use this field and the two following fields to enter optional virtual router IP addresses.
- **IP Address (4-6)**—Use this field and the one following field to enter optional virtual router IP addresses.
- **IP Address (7)** —Use this field to enter optional virtual router IP addresses.
- **Primary IP Address**—Virtual IP address identified with the virtual router. The primary IP Address is selected from actual interface addresses configured on a VRRP router.
- **Advertisement Interval (sec)**—Indicates the rate at which advertisements are sent when the router is the master.
- **Authentication**—Specifies whether no authentication process occurs, or pass-words the authenticate VRRP protocol exchanges.
- **Password (0-8 characters)** —The password used to authenticate VRRP protocol exchanges.
- **Preempt Enabled**—When checked, allows higher priority VRRP routers to over-ride lower priority routers.

To accept your changes, click A*pply to* VRRP. To cancel, click *Close*.

VRRF Settings

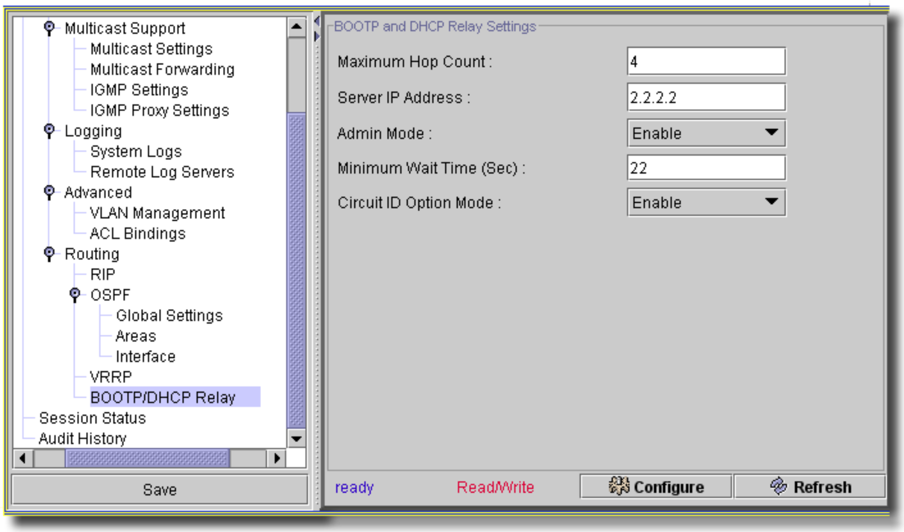
- **Index**—the ifIndex (assigned by the device) of the interface (port/LAG/VLAN) selected to associate a virtual router.

- **Interface Name**—A unique identifier for the particular interfaces.

BOOTP / DHCP Relay

This screen manages Bootp and DHCP relay settings for the selected device.

Figure 13-111. BOOTP / DHCP Relay



BOOTP and DHCP Relay Settings

Maximum Hop Count : 4

Server IP Address : 2.2.2.2

Admin Mode : Enable

Minimum Wait Time (Sec) : 22

Circuit ID Option Mode : Enable

This screen has the following fields:

- **Maximum Hop Count**—Enter the maximum number of hops. This is the maximum number of hops a client request can take before being discarded. It can be an integer from 1 to 16. The default value is 4.

- **Server IP Address**—Enter either the IP address of the BOOTP/DHCP server or the IP address of the next BOOTP/DHCP Relay Agent.

- **Admin Mode**—Select *Enable* or *Disable* from the pick list. Selecting *Enable* forwards BOOTP/DHCP requests to the IP address entered in the *Server IP Address* field.

- **Minimum Wait Time (Sec)**—Enter a time in seconds. This value is compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets are only forwarded when the time stamp exceeds the minimum wait time.

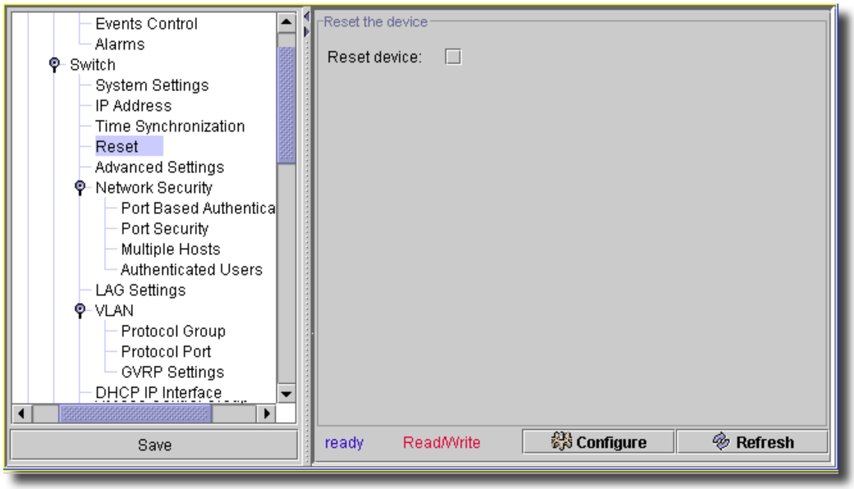
- **Circuit ID Option Mode**—Select *Enable* or *Disable* from the pick list. If you select *Enable*, the relay agent adds Option 82 header packets to the DHCP Request packets before forwarding them to the server, and strips them off while forwarding the responses to the client.

Click *Configure* to send your entries to the device, or *Refresh* to re-query the device to update this screen.

Reset

Check the checkbox on this screen to reset the device.

Figure 13-112. Reset Device



Reset device: □

Click *Configure* to send your reset request to the device.

Dell Default Screens

Depending on the model, all or a subset of the following screens may appear.

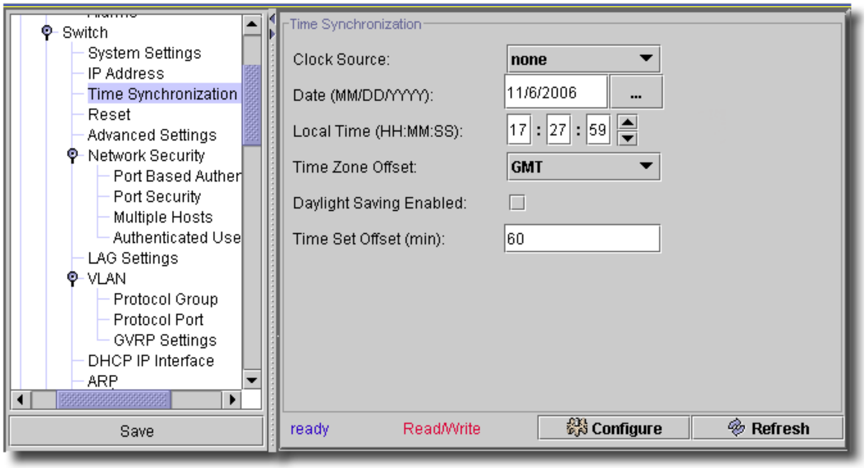
- Time Synchronization
- Advanced Settings
- Port Based Authentication
- Port Security
- Multiple Hosts
- Authenticated Users
- SNTP -> Global Settings
- SNTP -> Authentication
- SNTP -> Servers
- SNTP -> Interface Settings
- Copy Files
- LAG Settings
- VLAN -> Protocol Group
- VLAN -> Protocol Port

- VLAN -> Interface Settings
- VLAN -> Double VLAN Settings
- VLAN -> Bind MAC to VLAN
- VLAN -> Bind IP Subnet to VLAN
- Multicast Forward All

Time Synchronization

This screen lets you set the time synchronization for this switch.

Figure 13-113. Time Synchronization



Time Synchronization

Clock Source: none

Date (MM/DD/YYYY): 11/6/2006

Local Time (HH:MM:SS): 17 : 27 : 59

Time Zone Offset: GMT

Daylight Saving Enabled: □

Time Set Offset (min): 60

It has the following fields:

- **Clock Source**—Select from the pick list (*SNTP, none*).

- **Date (MM/DD/YY)**—Enter a date, or select from the calendar that appears when you click the command button (...).

- **Local Time (HH:MM:SS)**—Enter the time in 24-hour format.

- **Time Zone Offset**—Select the local time zone offset (the difference between Greenwich Mean Time or GMT and local time) from the pick list. For example, the Time Zone Offset for Paris is GMT +1, while the local time in New York is GTM –5.

- **Daylight Saving Enabled**—Check to enable daylight saving time, and select a country for the type of daylight savings.

USA—The device switches to DST at 2 a.m. on the first Sunday of April, and reverts to standard time at 2 a.m. on the last Sunday of October.

European—The device switches to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. The European option applies to EU members, and other European countries using the EU standard.

Other—The DST definitions are user-defined based on the device locality. If Other is selected, you must define the *From* and *To* fields that appear with this selection. For example, DST begins on the 25th October 2007 5:00 am, the two *From* fields will be 25Oct07 and 5:00.

Recurring Enabled—Check this to enable a recurring daylight savings time. Use the pick lists to configure the *Date* fields that appear above the *Time* fields.

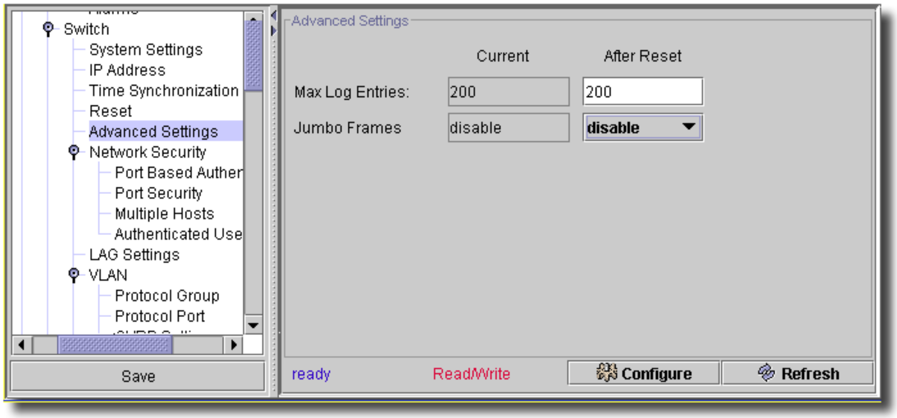
- **Time Set Offset (min)**—(1-1440) For non USA and European countries, the amount of time for DST can be set in minutes. The default time is 60 minutes.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Advanced Settings

The the Advanced Settings page contains a link for configuring global advanced settings. This screen varies slightly, depending on the device.

Figure 13-114. Advanced Settings



Advanced Settings

	Current	After Reset
Max Log Entries:	200	200
Jumbo Frames	disable	disable

ready ReadWrite

The page includes the following fields:

- **Max Log Entries** (20-400)—The maximum number of RAM Log entries. When the Log entries are full, the log is cleared and the Log file restarts.
- **Jumbo Frames**—Enables or disables the Jumbo Frames feature. Jumbo Frames allow identical data transport data in fewer frames. This ensures less overhead, lower processing time, and fewer interrupts.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

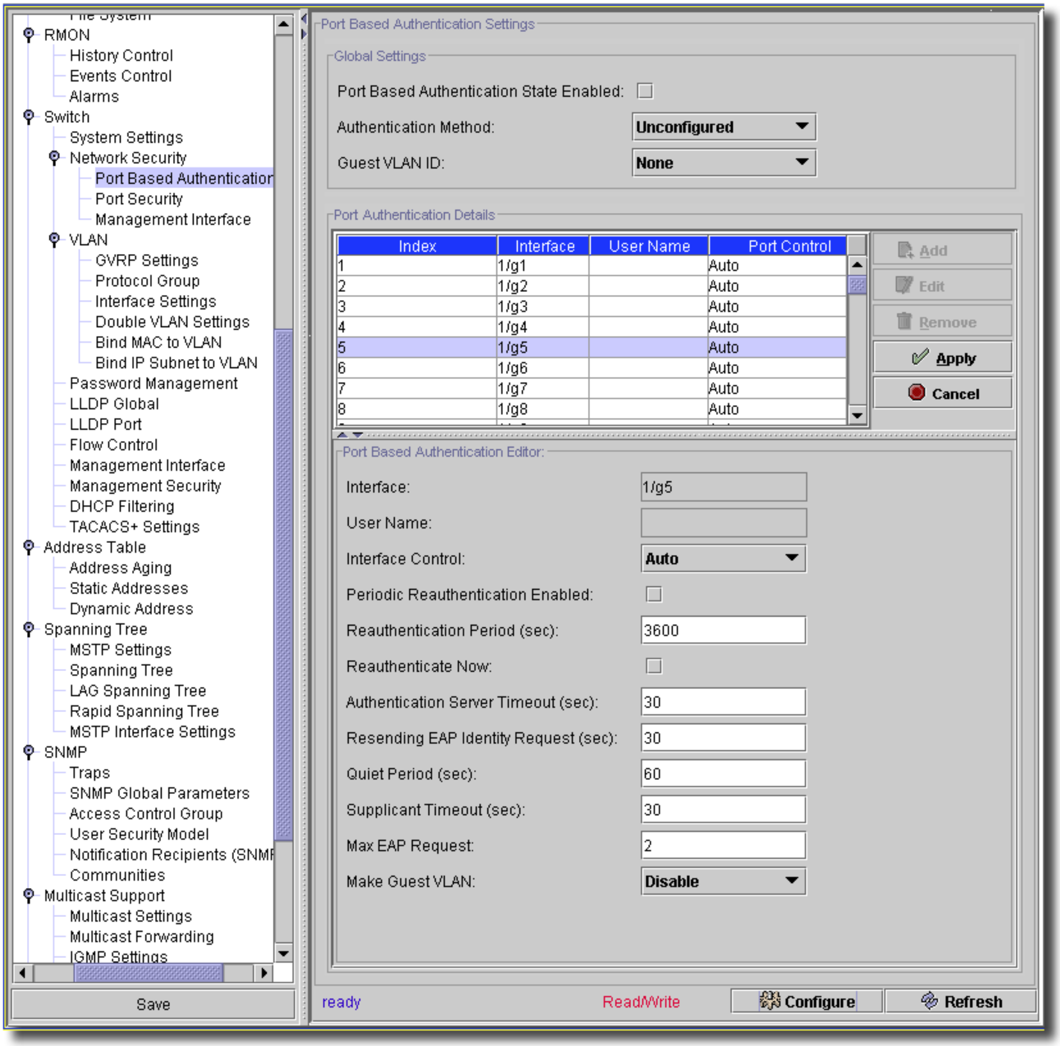
NOTE:

The changes to these attributes are applied only after the device is reset.

Port Based Authentication

The Port Based Authentication screen for switches contains fields for configuring port-based authentication.

Figure 13-115. Port Based Authentication



Port Based Authentication Settings

Global Settings

Port Based Authentication State Enabled: □

Authentication Method: Unconfigured

Guest VLAN ID: None

Port Authentication Details

Index	Interface	User Name	Port Control
1	1/g1		Auto
2	1/g2		Auto
3	1/g3		Auto
4	1/g4		Auto
5	1/g5		Auto
6	1/g6		Auto
7	1/g7		Auto
8	1/g8		Auto

Port Based Authentication Editor:

Interface: 1/g5

User Name:

Interface Control: Auto

Periodic Reauthentication Enabled: □

Reauthentication Period (sec): 3600

Reauthenticate Now: □

Authentication Server Timeout (sec): 30

Resending EAP Identity Request (sec): 30

Quiet Period (sec): 60

Supplicant Timeout (sec): 30

Max EAP Request: 2

Make Guest VLAN: Disable

You can *Edit* listed settings for the selected device in this screen (*Add* and *Remove* are disabled). Select an existing port authentication configuration listed in the upper portion of the screen and click *Edit*; the editor opens. This screen contains the following fields:

- **Port Based Authentication State Enabled**— When checked, enables port based authentication on the device.

- **Authentication Method**—The Authentication method used. The pick list values include:

  None—No authentication method is used to authenticate the port.

  RADIUS—The RADIUS servers does port authentication.

  RADIUS, None—The RADIUS server first does port authentication. If the port is not authenticated, then no authentication method is used, and the session is permitted.

Click *Remove* to delete a selected, listed item. You can *Add, Edit* or *Remove* port authentications for the selected device in this screen. When you click *Add* (or select an existing authentication listed in the *Port Authentication Details* portion of the screen and click *Edit*) the *Port Based Authentication Editor* opens (the lower portion of the screen) with the following fields:

Guest VLAN ID—Select from the pick list.

Port Authentication Details

- **Interface**—Contains an interface list.

User Name—The user name as configured in the RADIUS server.

- **Interface Control**—Defines the port authorization state. The possible field values include:

  Authorized—Set the interface state to authorized (permit traffic).

  Unauthorized—Set the interface state to unauthorized (deny traffic).

  Auto—Authorize state is set by the authorization method.

- **Periodic Reauthentication Enabled**—Reauthenticates the selected port periodically, when enabled. The reauthentication period is defined in the *Reauthentication Period (300-4294967295)* field.

- **Reauthentication Period** (300-4294967295)—Indicate the period for the selected port to be reauthenticated. The field value is in seconds. The field default is 3600 seconds.

- **Reauthenticate Now**—Permits immediate port reauthentication, when selected.

- **Authentication Server Timeout** (1-65535)—Defines the period that lapses before the device resends a request to the authentication server. The field value is in seconds. The field default is 30 seconds.

- **Resending EAP Identity Request** (1-65535)—Defines the period that lapses before EAP request are resent. The field default is 30 seconds.

Quiet Period (0-65535)—The number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.

- **Supplicant Timeout** (1-65535)—The amount of time that lapses before EAP requests are resent to the user. The field value is in seconds. The field default is 30 seconds.

- **Max EAP Requests** (1-10)—The total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries

- **Make Guest VLAN**—Select *Enable* or *Disable*.

Port Security

You can increase network security by limiting access on a specific port only to users with specific MAC addresses. Locked ports limit access to users with specific MAC addresses. You can either manually define these addresses on the port, or configure the ports to lean them until it is locked.

NOTE:

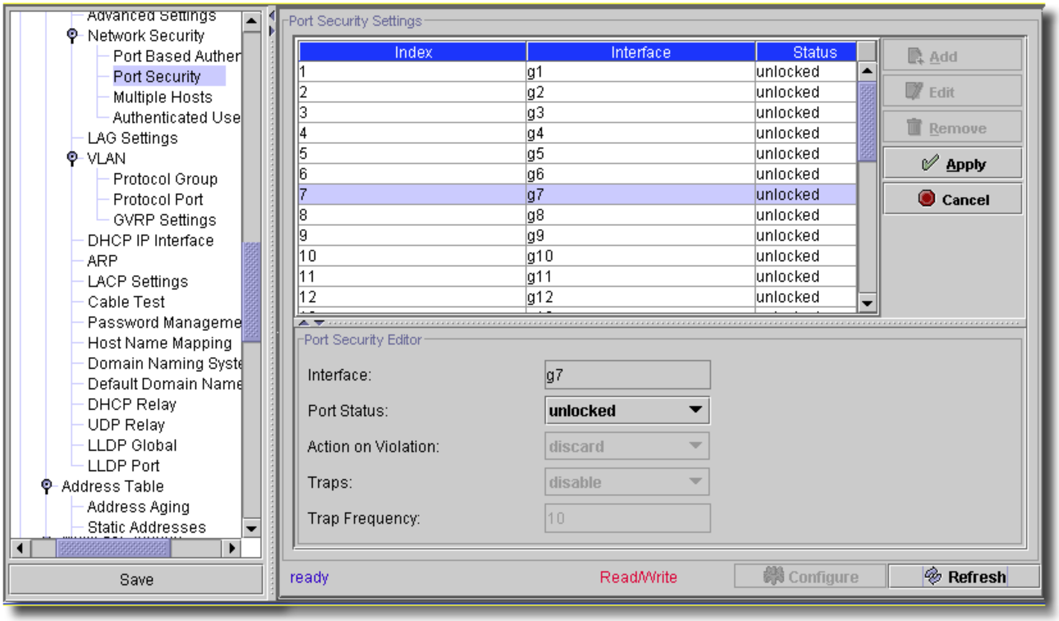
This screen appears only for switches that support it.

When a locked port receives a packet, and the packet's source MAC address is not tied to that port (either it was learned on a different port, or is unknown to the system), the device invokes the protection mechanism, and can provide various options. Unauthorized packets arriving to a locked port are either:

- Forwarded
- Discarded with no trap
- Discarded with a trap
- The ingress port is disabled

Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset.

Figure 13-116. Port Security



Index	Interface	Status
1	g1	unlocked
2	g2	unlocked
3	g3	unlocked
4	g4	unlocked
5	g5	unlocked
6	g6	unlocked
7	g7	unlocked
8	g8	unlocked
9	g9	unlocked
10	g10	unlocked
11	g11	unlocked
12	g12	unlocked

Interface: g7

Port Status: unlocked

Action on Violation: discard

Traps: disable

Trap Frequency: 10

Click *Remove* to delete a selected, listed item. You can *Add*, *Edit* or *Remove* ports for the selected device in this screen. When you click *Add* (or select an existing port listed in the *Port Security Settings* portion of the screen and click *Edit*) the *Port Security Editor* opens (the lower portion of the screen) with the following fields:

The page includes the following fields:

Interface—The (read only) port designator

- **Port Status**—This pick list sets the currently configured Port status. The port is either locked or unlocked. A port set to locked must have multiple hosts enabled. See Multiple Hosts on page 377.

- **Action on Violation**—The action to be applied to packets arriving on a locked port. The possible field values are:

  Forward—Forwards the packets from an unknown source, however, the MAC address is not learned.

  Discard—Discards the packets from any unlearned source. This is the default value.

  Shutdown—Discards the packet from any unlearned source and locks the port. Port remained locked until they are activated, or the device is reset.

- **Traps**—Enables/disables sending traps when a packet is received on a locked port.

Trap Frequency (1-1000000)—The period (in seconds) between traps. This field only applies to Locked ports. The default value is 10 seconds.

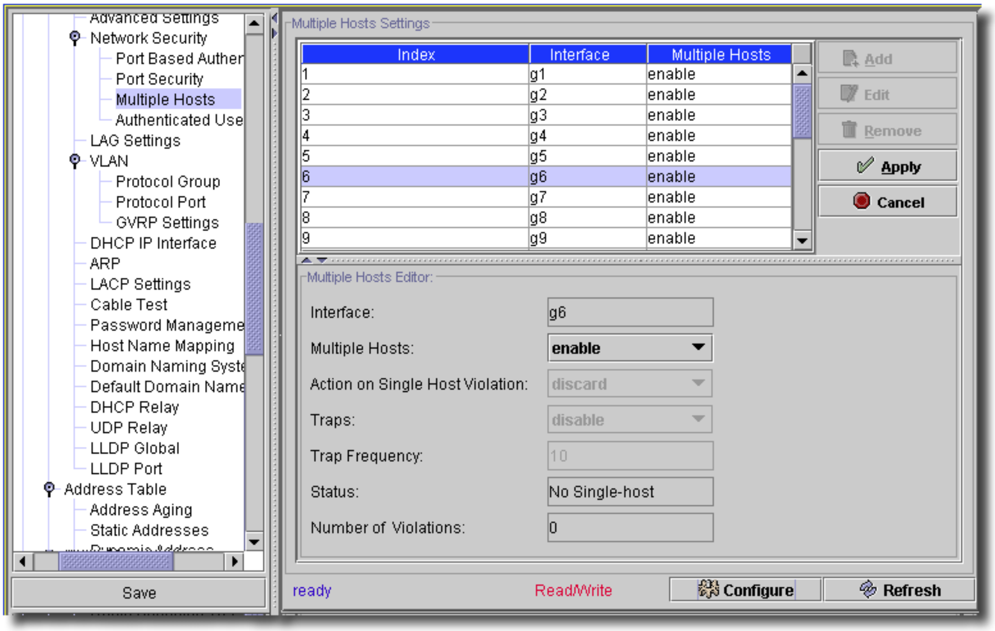
Max Learned Addresses—The maximum number of addresses learned of this port. (Does not appear in all screens)

Click *Apply* to accept the port settings you have configured and add it to the list. *Cancel* abandons your edits. Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Multiple Hosts

The Multiple Hosts screen provides information for defining advanced port-based authentication settings for specific ports.

Figure 13-117. Multiple Hosts



Index	Interface	Multiple Hosts
1	g1	enable
2	g2	enable
3	g3	enable
4	g4	enable
5	g5	enable
6	g6	enable
7	g7	enable
8	g8	enable
9	g9	enable

Interface: g6

Multiple Hosts: enable

Action on Single Host Violation: discard

Traps: disable

Trap Frequency: 10

Status: No Single-host

Number of Violations: 0

Click *Remove* to delete a selected, listed item. You can *Add, Edit* or *Remove* ports for the selected device in this screen. When you click *Add* (or select an existing port listed in the *Multiple Hosts Settings* portion of the screen and click *Edit*) the *Multiple Hosts Editor* opens (the lower portion of the screen) with the following fields:

NOTE:

A port set to locked in Port Security on page 375 must have multiple hosts enabled.

The *Index* column in the *Multiple Hosts Settings* is simply for reference. You configure the other fields in the *Multiple Hosts Editor* panel. The screen includes the following fields:

- **Interface**—The interface for which Advanced Port Based Authentication is enabled.

- **Multiple Hosts**—Enables or disables a single host to authorize multiple hosts for system access. This setting must be enabled in order to either disable the ingress-filter, or to use port-lock security on the selected port.

- **Action on Single Host Violation**—Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address. You can define this field only if you select *disable* in the *Multiple Hosts* pick list. The possible field values here are:

  Permit—Forwards the packets from an unknown source, however, the MAC address is not learned.

  Deny—Discards the packets from any unlearned source. This is the default value.

  Shutdown—Discards the packet from any unlearned source and locks the port. Ports remain locked until they are activated, or the device is reset.

- **Traps**—Enables or disables sending traps to the host if a violation occurs.

- **Trap Frequency** (1-1000000) (Sec)—Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if the Multiple Hosts field is defined as Disable. The default is 10 seconds.

- **Status**—The host status. The possible field values are:

  Unauthorized—Clients (supplicants) have full port access.

  Authorized—Clients (supplicants) have limited port access.

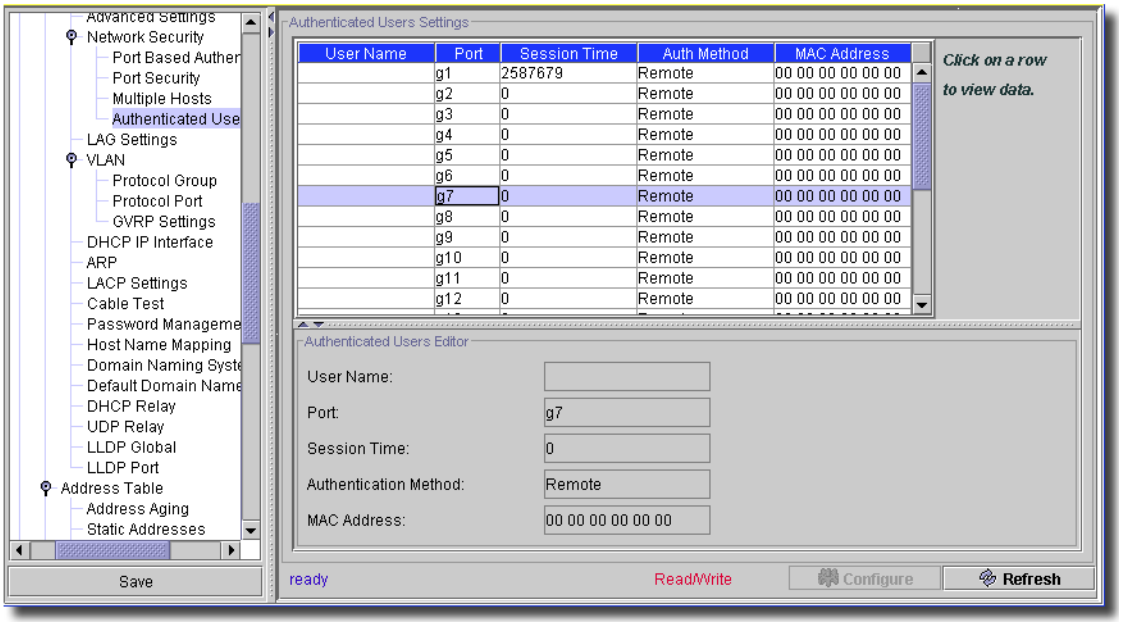
  No single-host—Multiple Hosts is enabled.

- **Number of Violations**—The number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address.

Authenticated Users

The *Authenticated Users* screen displays user port access lists.

Figure 13-118. Authenticated Users



Authenticated Users Settings

User Name	Port	Session Time	Auth Method	MAC Address
	g1	2587679	Remote	00 00 00 00 00 00
	g2	0	Remote	00 00 00 00 00 00
	g3	0	Remote	00 00 00 00 00 00
	g4	0	Remote	00 00 00 00 00 00
	g5	0	Remote	00 00 00 00 00 00
	g6	0	Remote	00 00 00 00 00 00
	g7	0	Remote	00 00 00 00 00 00
	g8	0	Remote	00 00 00 00 00 00
	g9	0	Remote	00 00 00 00 00 00
	g10	0	Remote	00 00 00 00 00 00
	g11	0	Remote	00 00 00 00 00 00
	g12	0	Remote	00 00 00 00 00 00

Authenticated Users Editor

User Name:	
Port:	g7
Session Time:	0
Authentication Method:	Remote
MAC Address:	00 00 00 00 00 00

Click on a row displayed in the *Authenticated Users Settings* table to see the row in the *Authenticated Users Editor* in the lower portion of this screen. The screen includes the following fields:

- **User Name**—List of users authorized via the RADIUS Server.

- **Port**—The port number(s) used for authentication - per user name.

- **Session Time**—The period during which the user was logged on to the device.

- **Authentication Method**—The method by which the last session was authenticated. The possible field values are:

  Remote—The user was authenticated from a remote server.

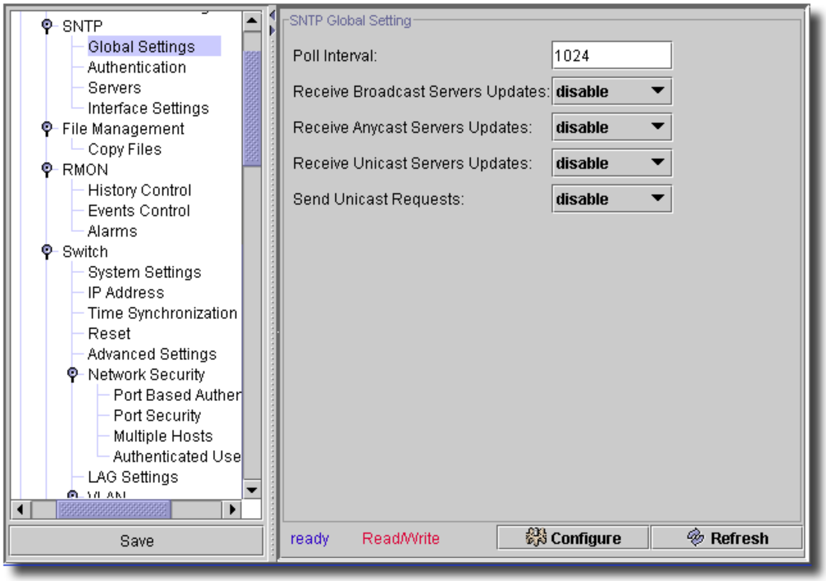
  None—The user was not authenticated.

- **MAC Address**—The client (supplicant) MAC address.

SNTP -> Global Settings

This screen lets you set global SNTP for the selected device.

Figure 13-119. Global SNTP Settings



SNTP Global Setting

Poll Interval: 1024

Receive Broadcast Servers Updates: disable

Receive Anycast Servers Updates: disable

Receive Unicast Servers Updates: disable

Send Unicast Requests: disable

Configure SNTP with the following fields and selections:

- **Poll Interval**—The seconds between polling (60 - 86400)

- **Receive Broadcast Server Updates**—Select *Enable* or *Disable*.

- **Receive Anycast Server Updates**—Select *Enable* or *Disable*.

- **Receive Unicast Server Updates**—Select *Enable* or *Disable*.

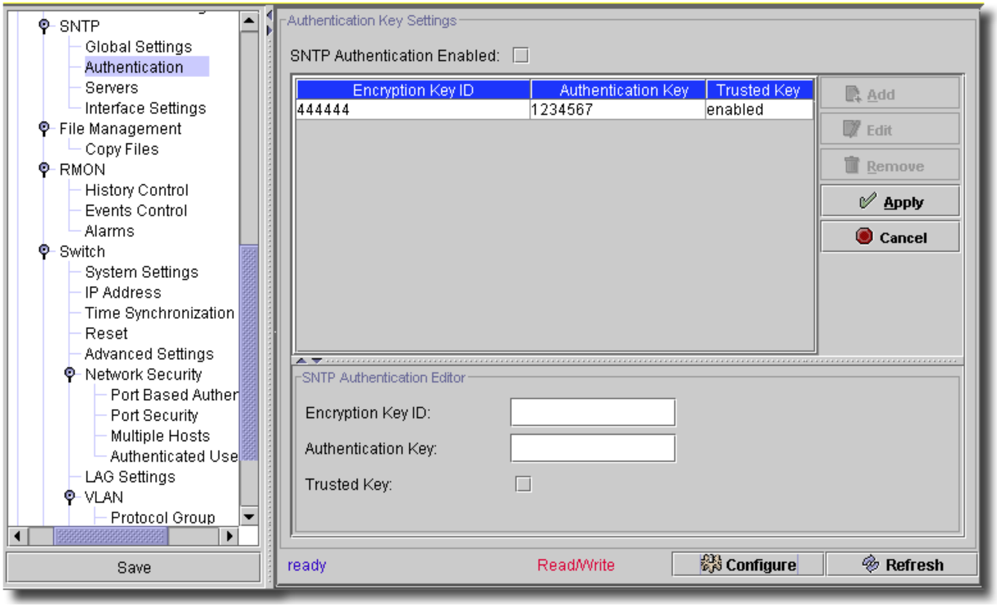
- **Send Unicast Requests**—Select *Enable* or *Disable*.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

SNTP -> Authentication

This screen lets you create authentications for SNTP.

Figure 13-120. SNTP Authentication



Authentication Key Settings

SNTP Authentication Enabled: □

Encryption Key ID	Authentication Key	Trusted Key
444444	1234567	enabled

SNTP Authentication Editor

Encryption Key ID:

Authentication Key:

Trusted Key: □

ready

Read/Write

- **SNTP Authentication**—When checked, this enables authenticating an SNTP session between the device and an SNTP server.

Click *Remove* to delete a selected, listed item. You can *Add*, *Edit* or *Remove* SNTP authentications for the selected device in this screen. When you click *Add* (or select an existing authentication listed in the *Authentication Key Settings* portion of the screen and click *Edit*) the *SNTP Authentication Editor* opens (the lower portion of the screen) with the following fields:

- **Encryption Key ID**—This defines the Key Identification that authenticates the SNTP server and device. The field value is up-to 4294967295characters.

- **Authentication Key** (1-8 Characters)—The key for authentication.

- **Trusted Key**—Checked, indicates this is the Encryption Key that authenticates the SNTP server.

Click *Apply* to accept the authentication you have configured and add it to the list. *Cancel* abandons your edits.

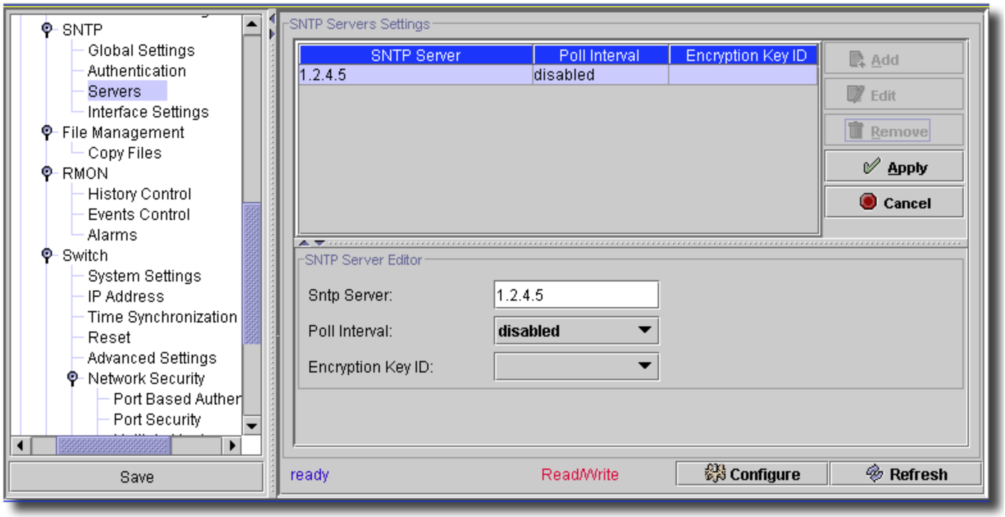
CAUTION:
Duplicate Authentication Key entries are not allowed.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

SNTP -> Servers

With this screen, you can configure (adding or enabling) the SNTP servers. The SNTP Servers page enables the device to request and accept SNTP traffic from a server.

Figure 13-121. SNTP Servers



SNTP Server	Poll Interval	Encryption Key ID
1.2.4.5	disabled	

Sntp Server: 1.2.4.5

Poll Interval: disabled

Encryption Key ID:

Click *Remove* to delete a selected, listed item. When you click *Add* (or select an existing server listed in the *SNTP Servers Settings* portion of the screen and click *Edit*) the *SNTP Server Editor* opens (the lower portion of the screen) with the following fields:

- **SNTP Server**—Enter a user-defined SNTP server IP addresses or hostname. Up to eight SNTP servers can be defined. This field can contain 1 - 158 characters. It is read-only when you edit listed servers.

- **Poll Interval**—Enables polling the selected SNTP Server for system time information, when enabled.

- **Encryption Key ID**—Specifies the Key Identification for communication between the SNTP server and device. The range is 1 - 4294967295.

SNTP Server Details (Read-only)

This section appears only when you edit an existing server setup.

- **Preference**—The SNTP server providing SNTP system time information. The possible field values are:

  Primary—The primary server provides SNTP information.

  Secondary—The backup server provides SNTP information.

- **Status**—The operating SNTP server status The possible field values are:

Up—The SNTP server is currently operating normally.

Down—The SNTP server is currently not operating normally.

Unknown—The SNTP server status is currently unknown.

- **Last Response**—The last time a response was received from the SNTP server.

- **Offset**—Timestamp difference between the device local clock and the acquired time from the SNTP server.

- **Delay**—The amount of time it takes to reach the SNTP server.

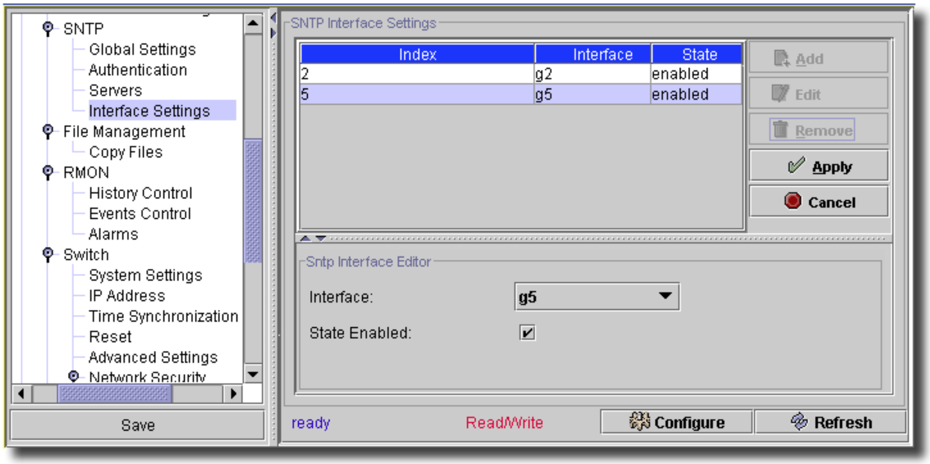
Click *Apply* to accept the server you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

SNTP -> Interface Settings

The SNTP Interface settings screen contains fields for setting SNTP on different interfaces.

Figure 13-122. SNTP Interfaces



Index	Interface	State
2	g2	enabled
5	g5	enabled

Interface: g5

State Enabled: ☑

You can *Add*, *Edit* or *Remove* SNTP interfaces for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you click *Add* (or select an existing interface listed in the *SNTP Interface Settings* portion of the screen and click *Edit*) the *SNTP Interface Editor* opens (the lower portion of the screen) with the following fields:

The screen includes the following fields:

- **Interface**—Contains an interface list on which SNTP can be enabled.

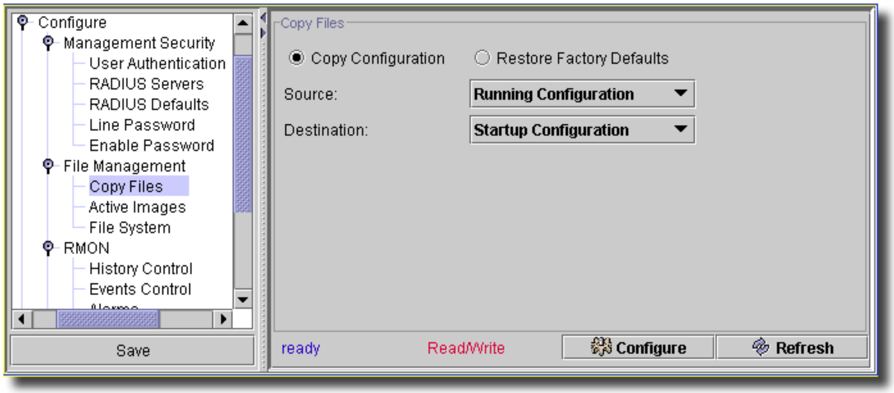
- **State Enabled**—Check this box to enable the interface.

Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits. Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Copy Files

You can copy and delete files from the Copy Files screen.

Figure 13-123. Copy Files



Copy Files

● Copy Configuration ○ Restore Factory Defaults

Source: Running Configuration

Destination: Startup Configuration

After a configuration change use this screen to copy running to startup config. The screen includes the following fields:

- **Copy Configuration**—When selected, copies either the *Running Configuration*, *Startup Configuration* or *Backup Configuration* files. Select possible values in the pick lists below (disabled if you select *Restore Configuration Factory Defaults*):

  Source—Copies either the *Running Configuration*, *Startup Configuration* or *Backup Configuration* files.

  Destination—The file to which the *Startup Configuration* or *Backup Configuration* file is copied.

- **Restore Configuration Factory Defaults**—When selected, specifies that the factory configuration default files should be reset. When unselected, maintains the current configuration settings.

- **New File Name**—On some (34xx) switch models, this checkbox and field appears. Check to activate and then fill in the new file name.

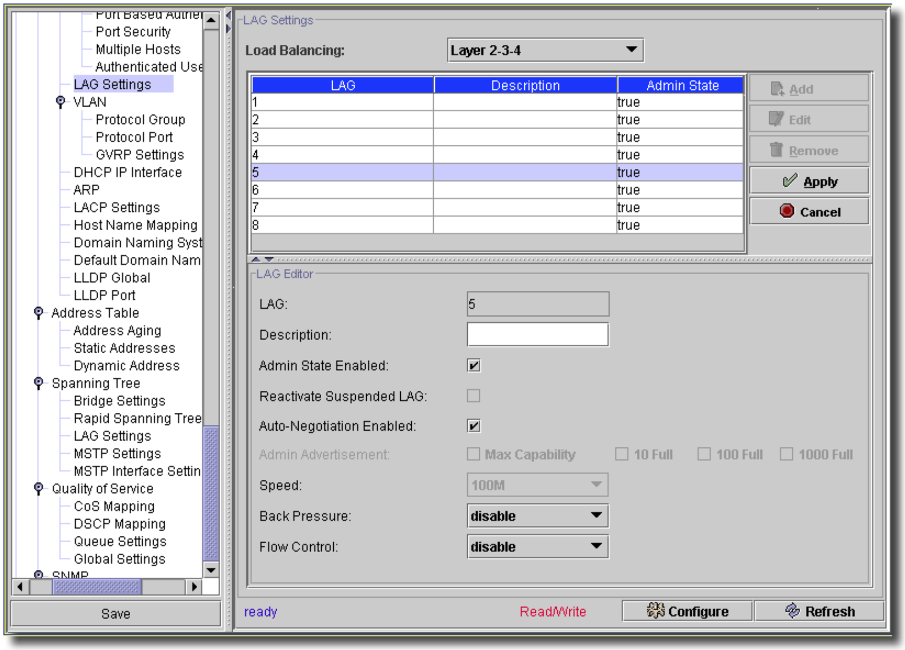
LAG Settings

The Switch -> LAG Settings screen contains fields for configuring parameters for configured LAGs. The device supports up to eight ports per LAG, and eight LAGs per system.

NOTE:

If you modify port configuration while the port is a LAG member, the configuration change is only effective after the port is removed from the LAG.

Figure 13-124. LAG Settings



Load Balancing: Layer 2-3-4

LAG	Description	Admin State
1		true
2		true
3		true
4		true
5		true
6		true
7		true
8		true

LAG: 5

Description:

Admin State Enabled: ☑

Reactivate Suspended LAG: □

Auto-Negotiation Enabled: ☑

Admin Advertisement: □ Max Capability □ 10 Full □ 100 Full □ 1000 Full

Speed: 100M

Back Pressure: disable

Flow Control: disable

You can *Edit* LAG settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you select an existing interface listed in the *LAG Settings* portion of the screen and click *Edit* the *LAG Editor* opens (the lower portion of the screen) with the following fields:

- **LAG**—The LAG number.

- **Description** (0-64 Characters)—Provides a user-defined description of the configured LAG.

- **Admin State Enabled**— When checked, enables traffic forwarding through the selected LAG.

Reactivate Suspended LAG—When checked, reactivates a suspended LAG.

- **Auto Negotiation Enabled**— When checked, enables the currently configured Auto Negotiation setting. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission rate, duplex mode and flow control (the flow control default is disabled) abilities to its partner.

Admin Advertisement— When enabled, check *Max Capability*, *10 Full*, *100 Full* or *1000 Full*.

Speed—The speed at which the LAG is operating.

- **Back Pressure**—*Enable/Disable* Back Pressure mode on the LAG. Back Pressure mode is effective on the ports operating in Half Duplex in the LAG.

- **Flow Control**—*Enable/Disable/Auto Negotiation*. Flow Control mode is effective on the ports operating in Full Duplex in the LAG.

Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

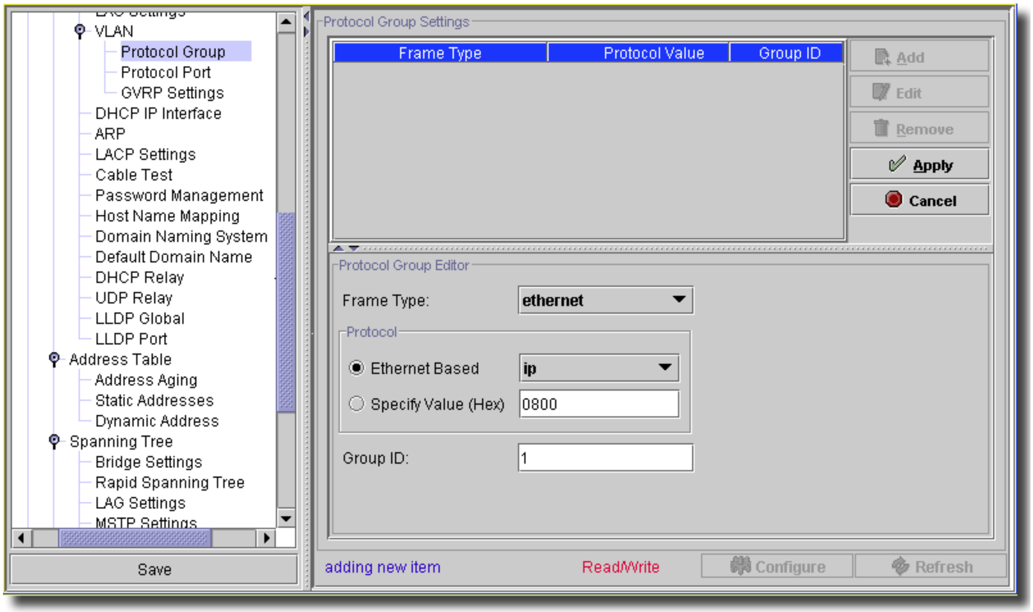
Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

VLAN -> Protocol Group

The Protocol Group page provides parameters for grouping protocols for filtering, configuring frame types to specific protocol groups. Protocol filtering prevents certain protocol traffic from being forwarded out switch ports. This filters broadcast and unicast traffic based on the membership of ports in different protocol groups. This filtering is in addition to the filtering provided by port-VLAN membership.

Protocol filtering identifies ports based on protocol. A port can be a member of one or more of the protocol groups. The device forwards flood traffic for each protocol group out a port only if that port belongs to the appropriate protocol group. Layer 2 protocols, like Spanning Tree Protocol (STP), are not affected by protocol filtering.

Figure 13-125.   VLAN ->Protocol Group



Frame Type: ethernet

Protocol

● Ethernet Based ip

○ Specify Value (Hex) 0800

Group ID: 1

adding new item   Read/Write

You can *Add*, *Edit* or *Remove* Protocol Group settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you click *Add* (or select an existing interface listed in the *Protocol Group Settings* portion of the screen and click *Edit*) the *Protocol Group Editor* opens (the lower portion of the screen) with the following fields:

- **Frame Type**—The packet type. Possible field values are *Ethernet*, *RFC1042*, and *LLC Other*.

Protocol

- **Ethernet-Based**—The Ethernet protocol group type. The possible field values are *IP, IPX* and *IPV6*.

- **Specify Value (Hex)**—A user-defined value to identify the protocol group.The value has to be even number of hex digits(0-9,a-f)

- **Group ID**— The VLAN Group ID number.

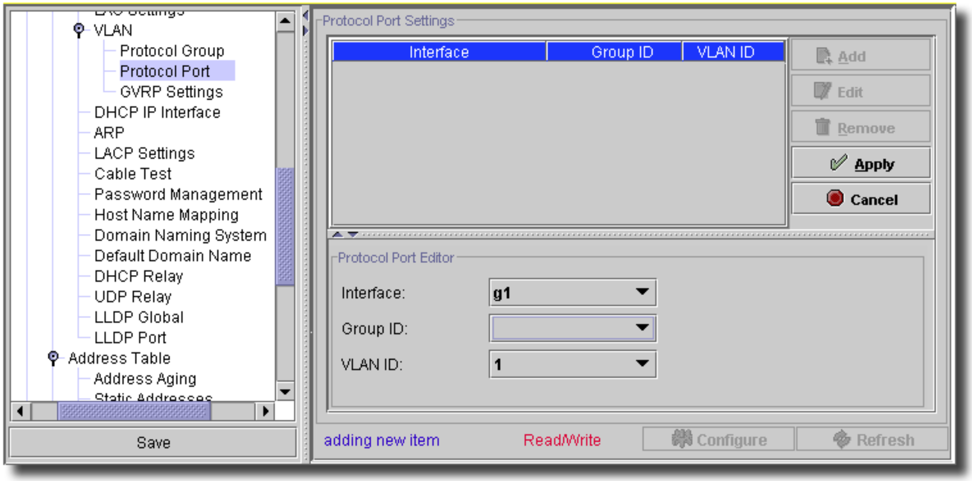
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

VLAN -> Protocol Port

The Protocol Port page adds interfaces to Protocol groups. For more information about protocol filtering, see VLAN -> Protocol Group on page 386.

Figure 13-126. VLAN Protocol Port



Interface: g1

Group ID:

VLAN ID: 1

adding new item

Read/Write

You can *Add*, *Edit* or *Remove* Protocol Port settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you click *Add* (or select an existing interface listed in the *Protocol Port Settings* portion of the screen and click *Edit*) the *Protocol Port Editor* opens (the lower portion of the screen) with the following fields:

- **Interface**—Port or LAG number added to a protocol group.
- **Group ID**—Protocol group ID to which the interface is added. Protocol group IDs are defined in the VLAN -> Protocol Group screen.
- **VLAN ID** (1-4095)—Attaches the interface to a user-defined VLAN ID. Protocol ports can either be attached to a VLAN ID.

NOTE:

VLAN 4095 is the discard VLAN. **Also**: You can define Protocol ports only on ports that are defined as General in the screen described in Advanced -> VLAN Management on page 295. If you do not see that option then you must register the license file for this feature to appear.

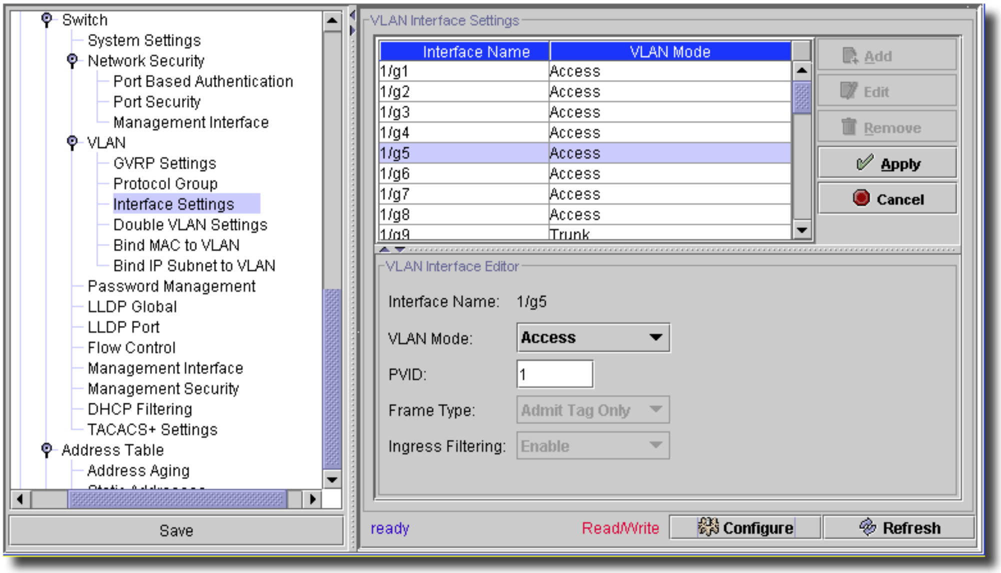
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

VLAN -> Interface Settings

This screen manages VLAN interface settings if the selected device support them.

Figure 13-127. VLAN -> Interface Settings



Interface Name	VLAN Mode
1/g1	Access
1/g2	Access
1/g3	Access
1/g4	Access
1/g5	Access
1/g6	Access
1/g7	Access
1/g8	Access
1/g9	Trunk

Interface Name: 1/g5

VLAN Mode: Access

PVID: 1

Frame Type: Admit Tag Only

Ingress Filtering: Enable

You can *Edit* VLAN interface settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you select an existing interface listed in the *VLAN Interface Settings* portion of the screen and click *Edit*, the *VLAN Interface Editor* opens (the lower portion of the screen) with the following fields:

- **Interface Name**—A read-only reminder of which interface you are editing.
- **VLAN Mode**—Select the mode from the pick list. Possible values are: *General*, *Access* and *Trunk*.
- **PVID**—(1-4093) | 4095. Assigns a VLAN ID to untagged packets. The possible values are 1-4093 | 4095.
- **Frame Type**—Specifies frame type accepted on the port. Default is *Admit Tag Only*. Possible values are: *Admit Tag only* and *Admit All*.
- **Ingress Filtering**—Enables or disables Ingress filtering on the port. Ingress filtering discards frames where the VLAN tag does not match the port VLAN membership.

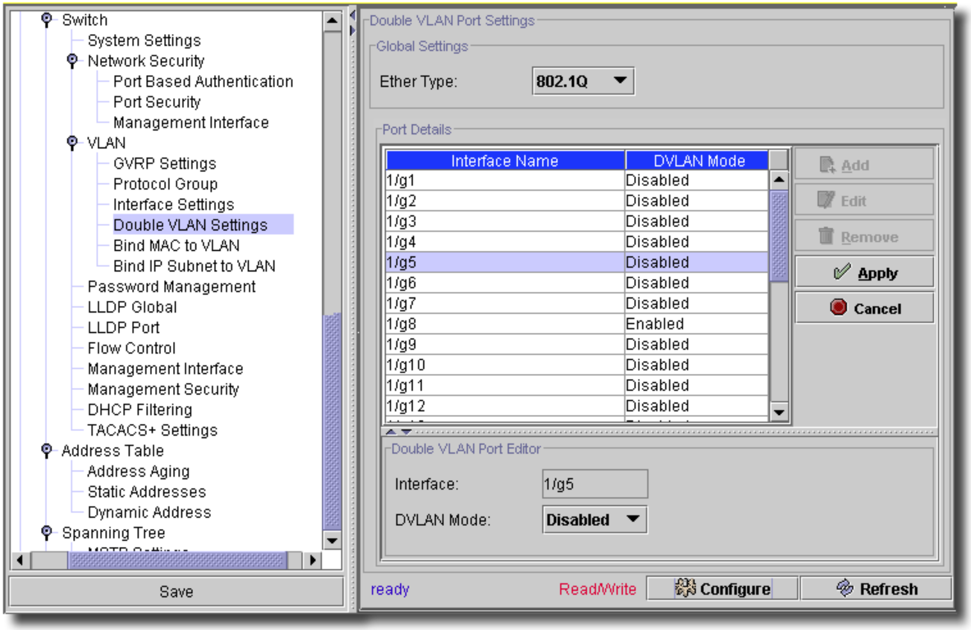
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

VLAN -> Double VLAN Settings

This screen lets you set double VLAN settings if the selected device supports them.

Figure 13-128. VLAN -> Double VLAN Settings



Ether Type: 802.1Q

Interface Name	DVLAN Mode
1/g1	Disabled
1/g2	Disabled
1/g3	Disabled
1/g4	Disabled
1/g5	Disabled
1/g6	Disabled
1/g7	Disabled
1/g8	Enabled
1/g9	Disabled
1/g10	Disabled
1/g11	Disabled
1/g12	Disabled

Interface: 1/g5

DVLAN Mode: Disabled

ready

Read/Write

You can *Edit* double VLAN port settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you select an existing port listed in the *Double VLAN Port Settings* portion of the screen and click *Edit*, the *Double VLAN Port Editor* opens (the lower portion of the screen) with the following fields:

- **Interface** —A read-only reminder of which interface you are editing.

- **DVLAN Mode**—Select the mode from the pick list. Possible values are: *Enabled / Disabled*.

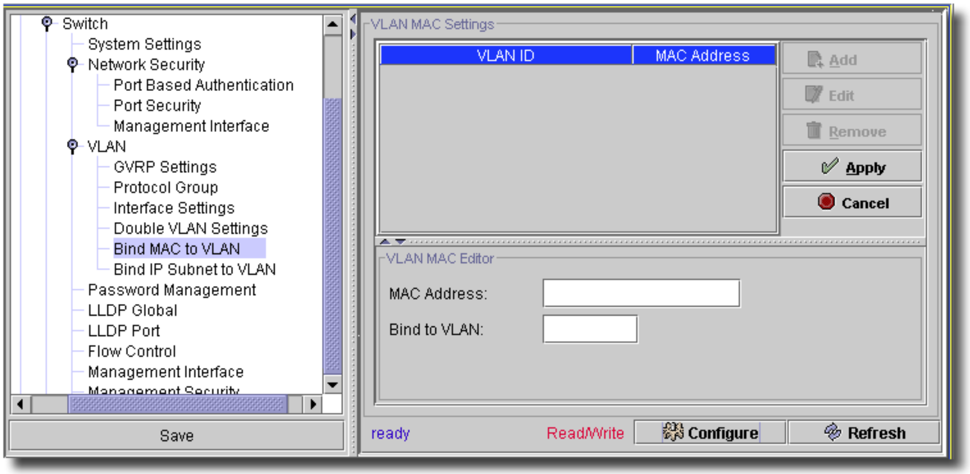
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

VLAN -> Bind MAC to VLAN

This screen lets you map a MAC entry to the VLAN table. After you specify the source MAC address and the VLAN ID, the MAC to VLAN configurations are shared across all ports of the switch. The MAC to VLAN table supports up to 128 entries.

Figure 13-129. VLAN -> Bind MAC to VLAN



You can *Add*, *Edit* or *Remove* MAC/VLAN pairs for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you click *Add* (or select an existing interface listed in the *VLAN MAC Settings* portion of the screen and click *Edit*) the *VLAN MAC Editor* opens (the lower portion of the screen) with the following fields:

- **MAC Address**—The MAC address to map to the selected VLAN.

- **Bind to VLAN**—The VLAN number (1 - 4093) to which this MAC is bound.

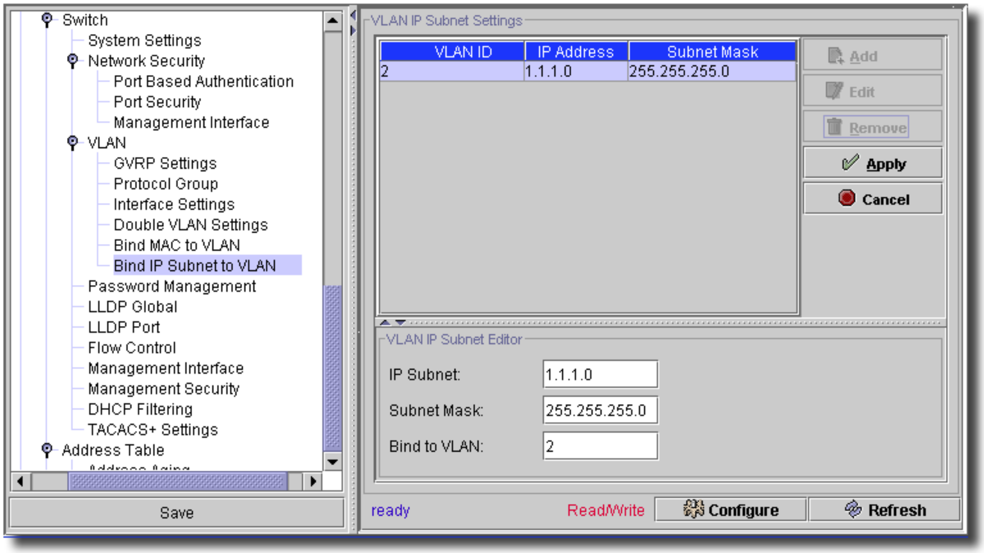
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

VLAN -> Bind IP Subnet to VLAN

The Bind IP Subnet to VLAN page lets you assign an IP Subnet to a VLAN.

Figure 13-130. VLAN -> Bind IP Subnet to VLAN



VLAN ID	IP Address	Subnet Mask
2	1.1.1.0	255.255.255.0

IP Subnet: 1.1.1.0

Subnet Mask: 255.255.255.0

Bind to VLAN: 2

You can *Add*, *Edit* or *Remove* IP Subnet/VLAN pairs for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you click *Add* (or select an existing interface listed in the *VLAN IP Subnet Settings* portion of the screen and click *Edit*) the *VLAN IP Subnet Editor* opens (the lower portion of the screen) with the following fields:

- **IP Address**—The packet source IP address.

- **Subnet Mask**—The packet source IP subnet mask address.

- **Bind to VLAN**—The VLAN number (1 - 4093) to which this IP address is assigned.

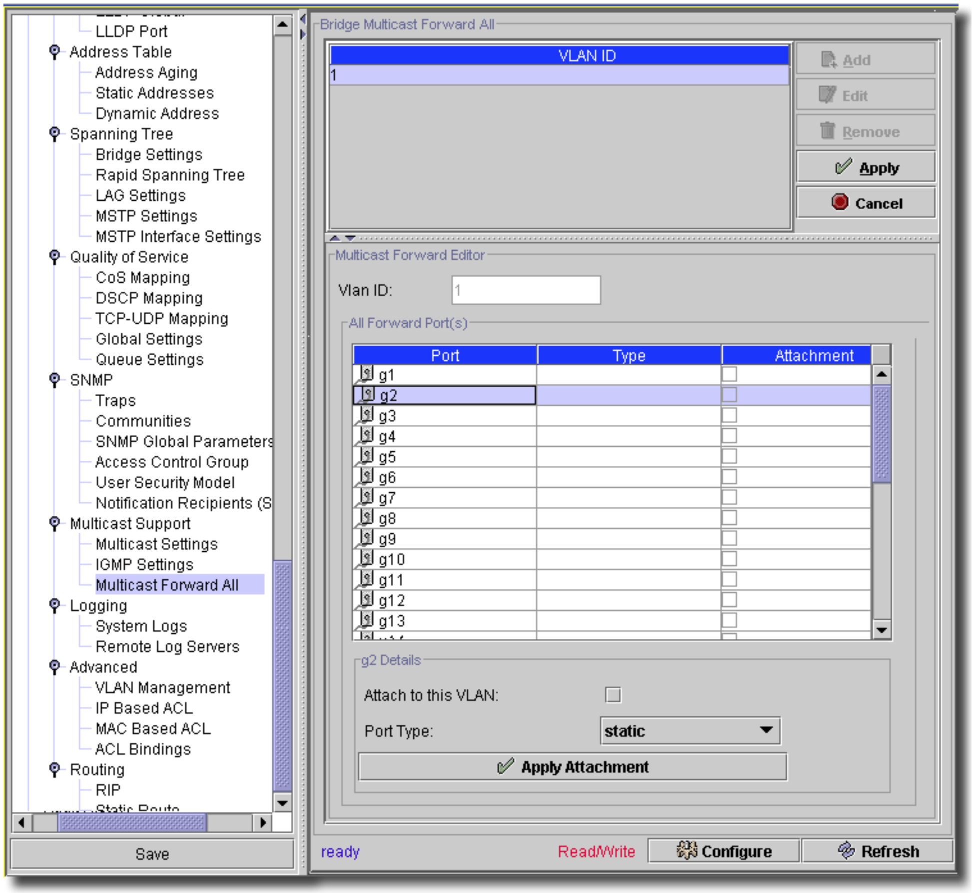
Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Multicast Forward All

The Bridge Multicast Forward All page contains fields for attaching ports or LAGs to a device attached to a neighboring Multicast router/switch. Once you enable IGMP Snooping, Multicast packets are forwarded to the appropriate port or VLAN.

Figure 13-131. Multicast Forward All



VLAN ID
1

Vlan ID: 1

Port	Type	Attachment
g1		□
g2		□
g3		□
g4		□
g5		□
g6		□
g7		□
g8		□
g9		□
g10		□
g11		□
g12		□
g13		□

Attach to this VLAN: □

Port Type: static

You can *Edit* Bridge Multicast Forwarding settings for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you select an existing interface listed in the *Bridge Multicast Forward All* portion of the screen and click *Edit* the *Multicast Forward Editor* opens (the lower portion of the screen) with the following fields:

VLAN ID—Identifies a VLAN.

Ports—Ports that can be added to a Multicast service.

LAGs—LAGs that can be added to a Multicast service.

The table in the lower portion of this screen contains the settings for managing router and port settings. Port *Type* can be any of the following:

Static—Attaches the port to the Multicast router or switch as a static port.

Forbidden—Forbidden.

If the port is not attached to a Multicast router or switch, this is handled by the *Associated with VLAN* check box in the application.

Do the following in the *Multicast Forward Editor* panel to attach a Port or LAG to a Multicast Router or Switch:

1 If you are not editing an existing VLAN, define the VLAN ID (for existing VLANs, it is read-only).

2 Select a port or LAG in the *All Forwarded Ports* table in the lowest panel, and assign it a *Type* and check *Attach to this VLAN* if you want that enabled.

3 Click *Apply Attachment*. (This button applies changes to *All Forwarded Ports* rather than to the list in the top panel.)

The port or LAG is then attached to the Multicast router or switch.

Click *Apply* to accept the edits you have configured and add it to the list. *Cancel* abandons your edits. Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Additional Dell Screens

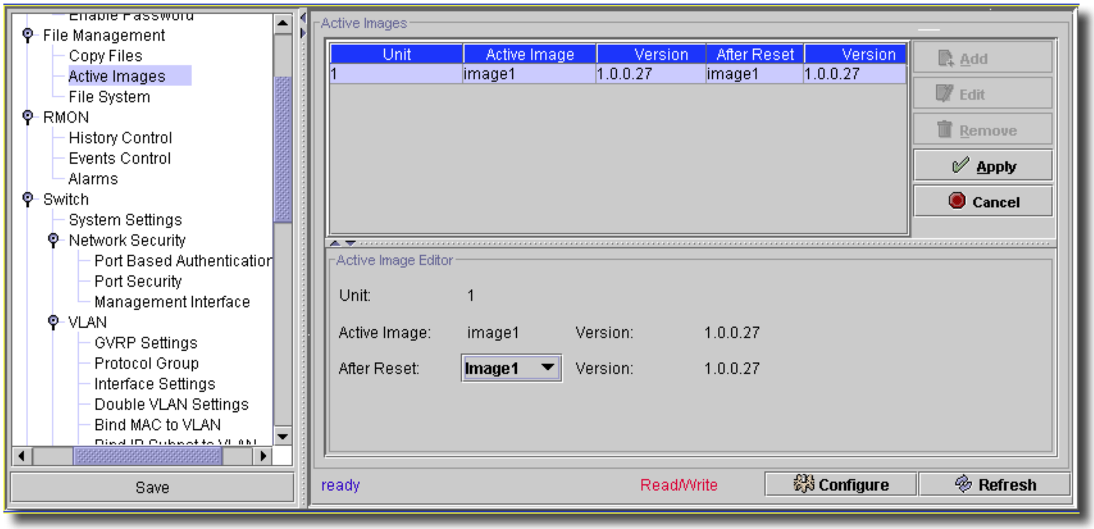
The screens described in the following sections appear on certain Dell equipment like the 6000 and 8000 series switches.

- File Management -> Active Images
- File Management -> File System
- Management Interface
- VLAN -> Protocol Group

File Management -> Active Images

This screen configures active images on the selected device.

Figure 13-132. File Management -> Active Images



Active Images

Unit	Active Image	Version	After Reset	Version
1	image1	1.0.0.27	image1	1.0.0.27

Active Image Editor

Unit: 1

Active Image: image1 Version: 1.0.0.27

After Reset: Image1 Version: 1.0.0.27

ready Read/Write

Click *Edit* to modify a listed image, and the *Active Image Editor* panel appears below the list of such images. Click *Apply* to accept any changes you make to the edited image, or *Cancel* to abandon those changes. The editor includes the following fields:

- **Unit**—A read-only display of the unit for the active image.

- **Active Image**—The read-only name and version of the image.

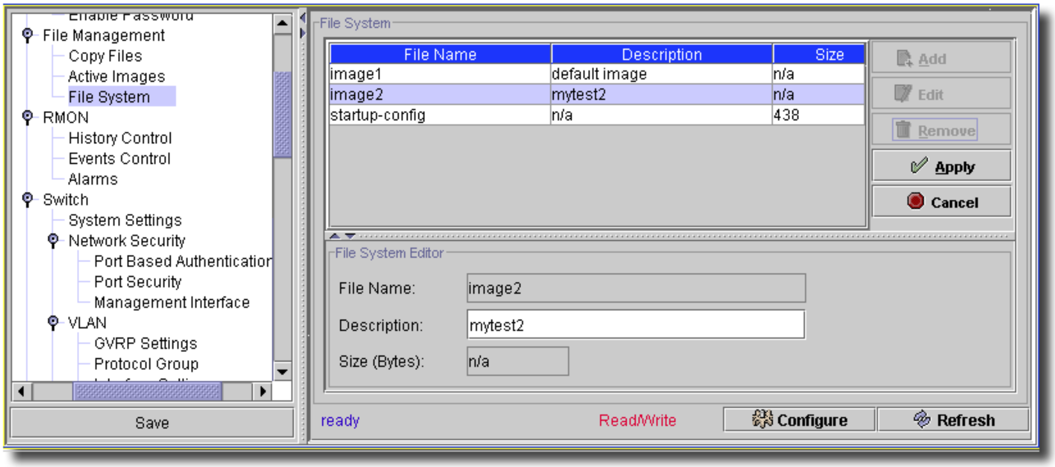
- **After Reset**—Select the image to use from the pick list.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

File Management -> File System

This screen lets you configure the description of images available on the file system

Figure 13-133. File Management -> File System.



File Name	Description	Size
image1	default image	n/a
image2	mytest2	n/a
startup-config	n/a	438

File Name: image2

Description: mytest2

Size (Bytes): n/a

This screen lets you *Edit* selected images when you click that button after selecting them. Click *Apply* to accept any changes you make to the edited image, or *Cancel* to abandon those changes. The editor includes the following fields:

- **File Name**—A read-only display of the file name.

- **Description**—A text description of the file.

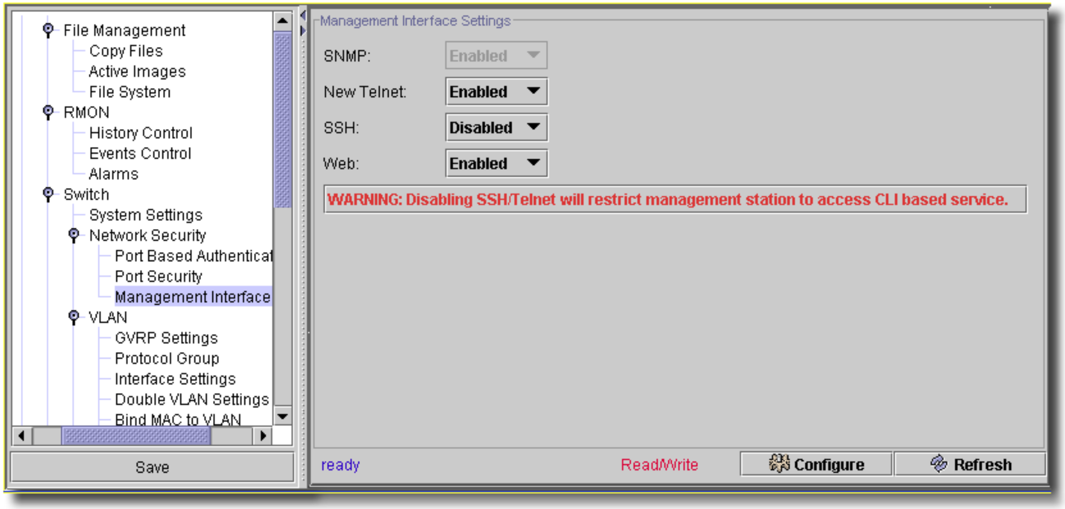
- **Size (Bytes)**—The read-only size of the file.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Management Interface

This screen sets up the management interface for the device.

Figure 13-134. Management Interface



SNMP: Enabled

New Telnet: Enabled

SSH: Disabled

Web: Enabled

WARNING: Disabling SSH/Telnet will restrict management station to access CLI based service.

- This screen has fields that let you Enable/Disable *SNMP*, *Telnet*, *SSH*, and *Web*.

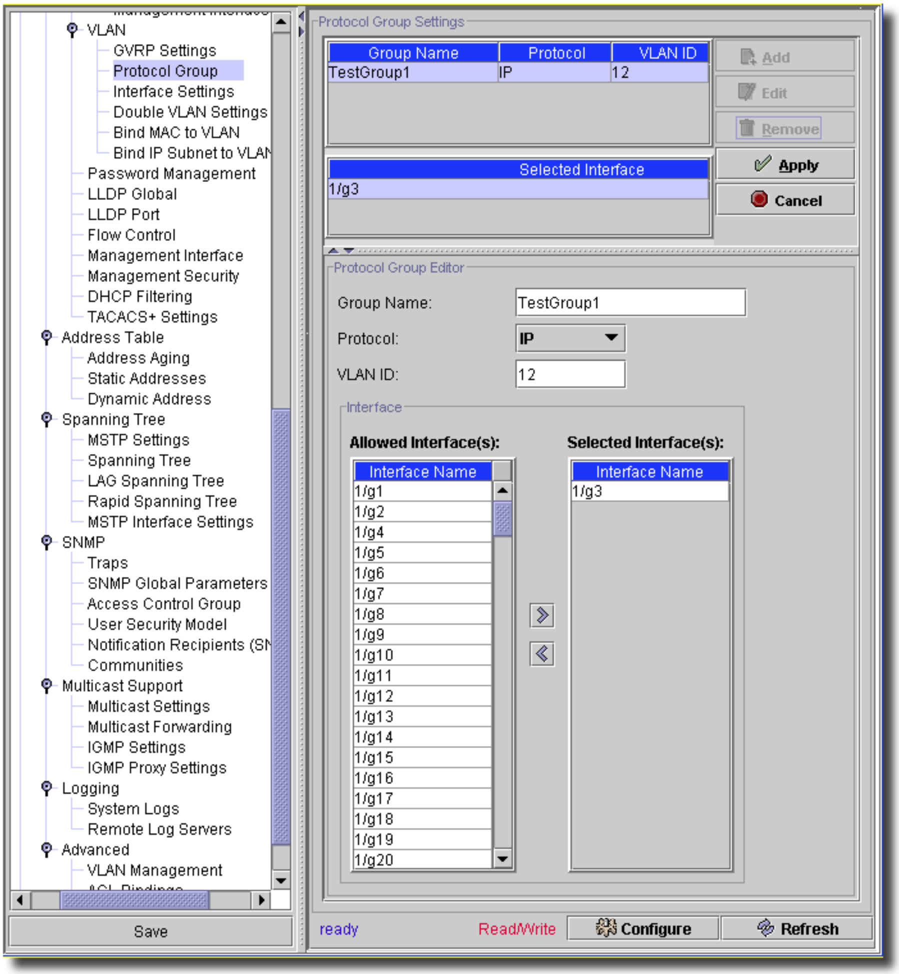
A warning appears on this screen to remind you that disabling SSH/Telnet will restrict command-line interface access.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

VLAN -> Protocol Group

This screen sets up the VLAN protocol group(s) for the device.

Figure 13-135. VLAN -> Protocol Group



Protocol Group Settings

Group Name	Protocol	VLAN ID
TestGroup1	IP	12

Selected Interface
1/g3

Protocol Group Editor

Group Name: TestGroup1

Protocol: IP

VLAN ID: 12

Interface

Allowed Interface(s):

Interface Name
1/g1
1/g2
1/g4
1/g5
1/g6
1/g7
1/g8
1/g9
1/g10
1/g11
1/g12
1/g13
1/g14
1/g15
1/g16
1/g17
1/g18
1/g19
1/g20

Selected Interface(s):

Interface Name
1/g3

ready Read/Write

You can *Add*, *Edit* or *Remove* VLAN protocol configurations for the selected device in this screen. Click *Remove* to delete a selected, listed item. When you click *Add* (or select an existing interface listed in the *Protocol Group Settings* portion of the screen and click *Edit*) the *Protocol Group Editor* opens (the lower portion of the screen) with the following fields:

- **Group Name**—The name of the protocol group

- **Protocol**—Select the protocol from the pick list

- **VLAN ID**—The number of the assigned VLAN

- **Interface**—Click the arrows to move *Allowed* interfaces to *Selected* interfaces.

Click *Configure* to send any altered configuration to the device. Click *Refresh* to renew the device information on this screen.

Dell PowerConnect B-Series Device Driver

This driver lets you discover and manage Dell PowerConnect B-Series devices on your network.

Supported Powerconnect B-series systems include the following models: B-MLXe-4, B-MLXe-8, B-MLXe-16, B-MLXe-16, B-DCX4S-24, B-FCX624 I/E, B-FCX648 I/E, B-FCX6xx-S, B-TurboIron, B-RX4, B-RX8, B-RX16, B-8000/8000e, and B-DCX4. Systems also include 3800, 3850, 3900, 200E, 2014, 2016, 2040, 2024, 4100, 4900, 5000, 76000, 12000, 24000, 48000, DCX 8000e, 8000, BigIron RX4, RX8. (See Help > About for the details of supported firmware.)

NOTE:

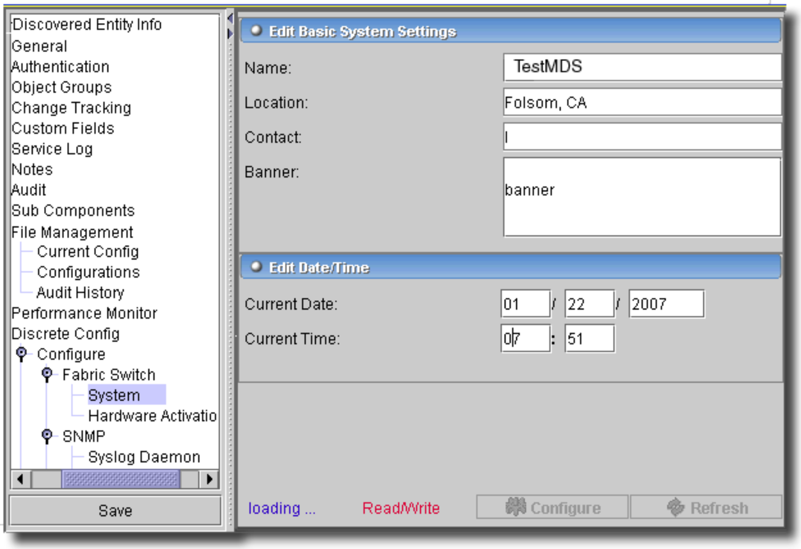
OpenManage Network Manager will not telnet connect to some devices if they use the factory default password. You must set the password to something other than that default. OpenManage Network Manager does not recognize the additional prompt asking that default password be changed each time log in occurs.

This driver has the screens described in the following sections.

Fabric -> System

This screen manages the system portion of the selected equipment's fabric.

Figure 13-1. Fabric -> System



Name: TestMDS

Location: Folsom, CA

Contact:

Banner: banner

Current Date: 01 / 22 / 2007

Current Time: 07 : 51

This screen has the following fields:

- **Name**—The name of the system.

- **Location**—The location of the system.

- **Contact**—The system's contact.

- **Banner**—The system’s banner.

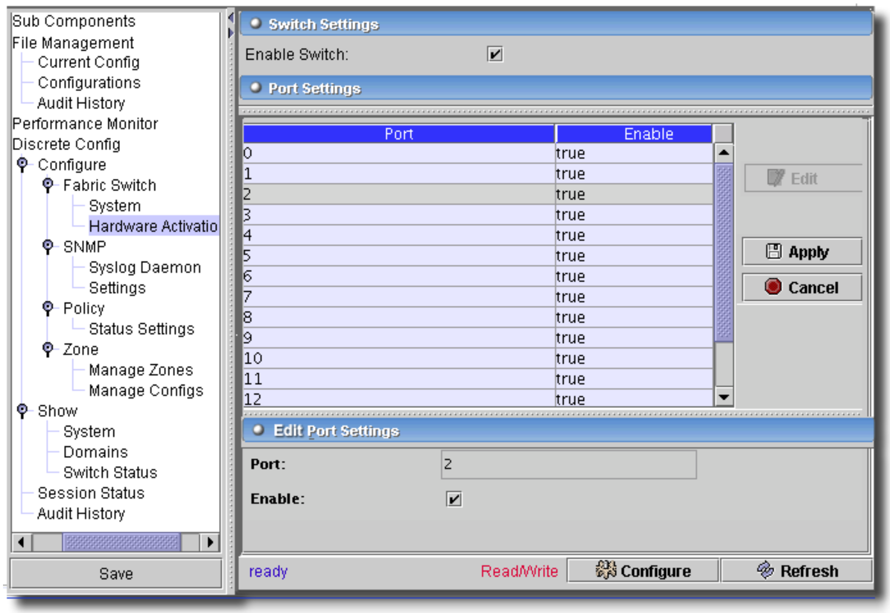
- **Current Date / Time**—The system’s date and time.

Click *Configure* to send this configuration to the device, or *Refresh* to update the information.

Fabric -> Hardware Activation

This screen lets you activate the switch and/or individual ports on the selected equipment.

Figure 13-2. Fabric -> Hardware Activation



Enable Switch: ☑

Port	Enable
0	true
1	true
2	true
3	true
4	true
5	true
6	true
7	true
8	true
9	true
10	true
11	true
12	true

Port: 2

Enable: ☑

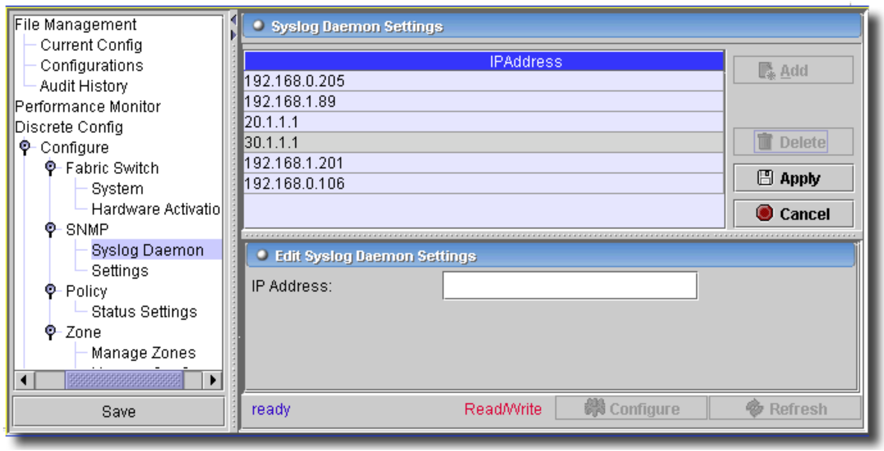
Check the *Enable Switch* checkbox to activate the entire switch. Select a listed port and click *Edit* to enable/disable the individual port in the lowest panel with the *Enable* checkbox. Click *Apply* to accept your edits, or *Cancel* to abandon them.

Click *Configure* to send this configuration to the device, or *Refresh* to update the information.

SNMP -> Syslog Daemon

This screen configures the syslog daemon for the selected equipment.

Figure 13-3. SNMP -> Syslog Daemon



IPAddress
192.168.0.205
192.168.1.89
20.1.1.1
30.1.1.1
192.168.1.201
192.168.0.106

IP Address:

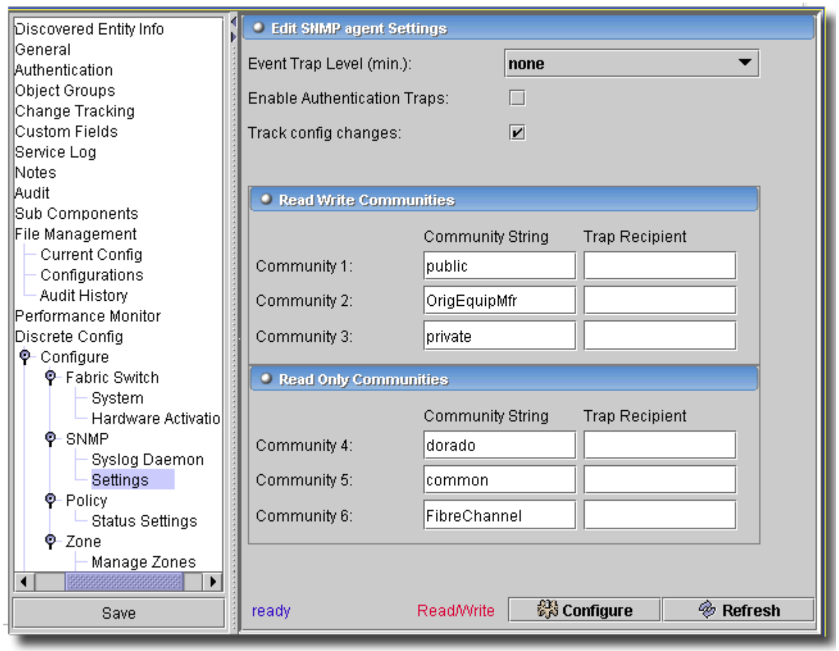
Click *Add* to enter a new IP address for syslog daemon. Select a listed IP address and click *Delete* to remove it. Once you have entered an IP address, click *Apply* to list it, or click *Cancel* to abandon your edits.

Click *Configure* to send this configuration to the device, or *Refresh* to update the information.

SNMP -> Settings

This screen manages SNMP settings for the selected equipment.

Figure 13-4. SNMP -> Settings



Edit SNMP agent Settings

Event Trap Level (min.): none

Enable Authentication Traps: □

Track config changes: ☑

Read Write Communities

	Community String	Trap Recipient
Community 1:	public	
Community 2:	OrigEquipMfr	
Community 3:	private	

Read Only Communities

	Community String	Trap Recipient
Community 4:	dorado	
Community 5:	common	
Community 6:	FibreChannel	

This screen has the following fields and settings:

Edit SNMP agent Settings

- **Event Trap Level (min)**—Select the minimum trap level from the pick list. The equipment sends traps of this level or higher.
- **Enable Authentication Traps**—Check to enable.
- **Track config changes**—Check to enable.

Read Write Communities

This panel lists three trap community string settings and the trap recipient IP Address.

Read Only Communities

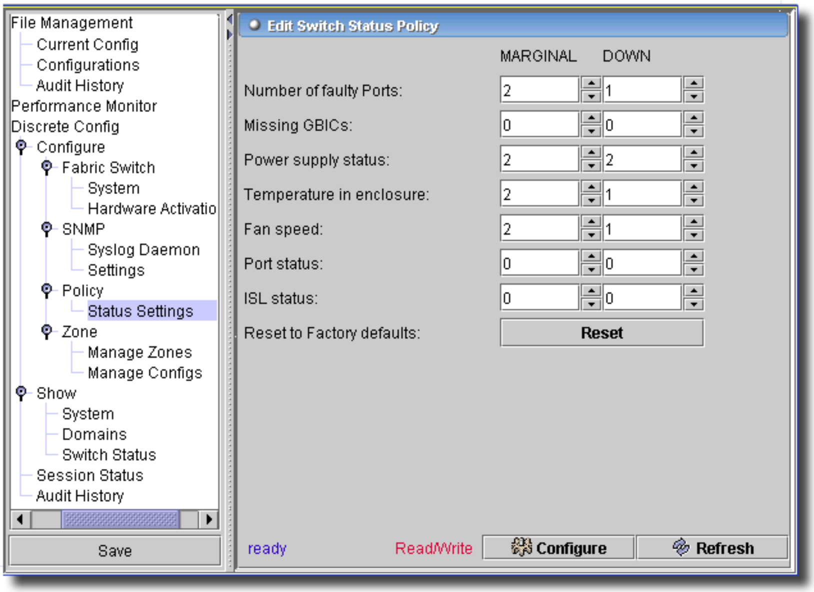
This panel lists three trap community string settings and the trap recipient IP Address.

Click *Configure* to send this configuration to the device, or *Refresh* to update the information.

Policy -> Status Settings

This screen configures policy status settings for the selected equipment.

Figure 13-5. Policy -> Status Settings



	MARGINAL	DOWN
Number of faulty Ports:	2	1
Missing GBICs:	0	0
Power supply status:	2	2
Temperature in enclosure:	2	1
Fan speed:	2	1
Port status:	0	0
ISL status:	0	0
Reset to Factory defaults:	Reset	

This has the following fields where you can set policy for permitting *Marginal* or *Down* elements of the equipment.

- **Number of faulty Ports**—The faulty ports permitted.

- **Missing GBICs**—Missing GBICs.

- **Power supply status**—The status of the equipment’s power supplies.

- **Temperature in enclosure**—The enclosure’s temperature permitted.

- **Fan speed**—The fan speed.

- **Port status**—The port status.

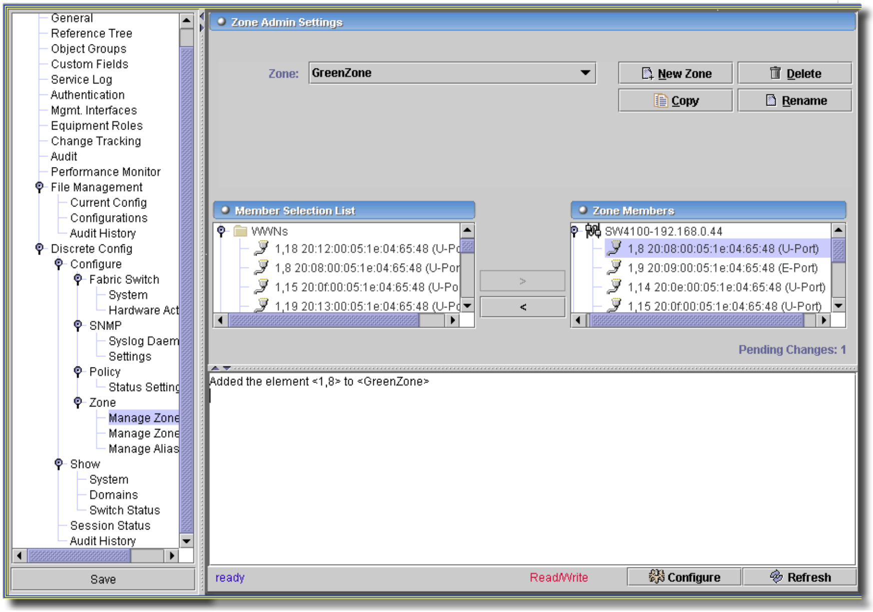
- **ISL Status**—The system’s interlink switch (ISL) status. ISLs connect switches with E-ports.

- **Reset to Factory defaults**—Clicking this button resets the device to the original factory settings.

Zone -> Manage Zone

This screen manages ports in zones for the selected equipment.

Figure 13-6. Zone -> Manage Zone



Zone: GreenZone

Member Selection List:

```
WWNs
  1,18 20:12:00:05:1e:04:65:48 (U-Po
  1,8 20:08:00:05:1e:04:65:48 (U-Por
  1,15 20:0f:00:05:1e:04:65:48 (U-Po
  1,19 20:13:00:05:1e:04:65:48 (U-Po
```

Zone Members:

```
SW4100-192.168.0.44
  1,8 20:08:00:05:1e:04:65:48 (U-Port)
  1,9 20:09:00:05:1e:04:65:48 (E-Port)
  1,14 20:0e:00:05:1e:04:65:48 (U-Port)
  1,15 20:0f:00:05:1e:04:65:48 (U-Port)
```

Pending Changes: 1

```
Added the element <1,8> to <GreenZone>
```

A Zone is a region within the fabric, where switches and devices can communicate. A device can only communicate with other devices connected to the fabric within its specified zone. The members of a zone are determined using the following methods:

- Alias names
- Switch domain and port area number pair.
- WWN

Click *New Zone* to add a zone to the pick list at the top of this screen. Select one on the list to modify an existing zone. Select a zone and click *Delete* to remove a listed zone, or click *Copy* or *Rename* to perform those functions on the selected zone.

Actions configured in this screen, reconfiguring, adding or deleting members, appear listed in the *Pending Changes* panel at the bottom of this screen (you may have to click and drag the divider to see this panel). They do not take effect until you Click *Configure*.

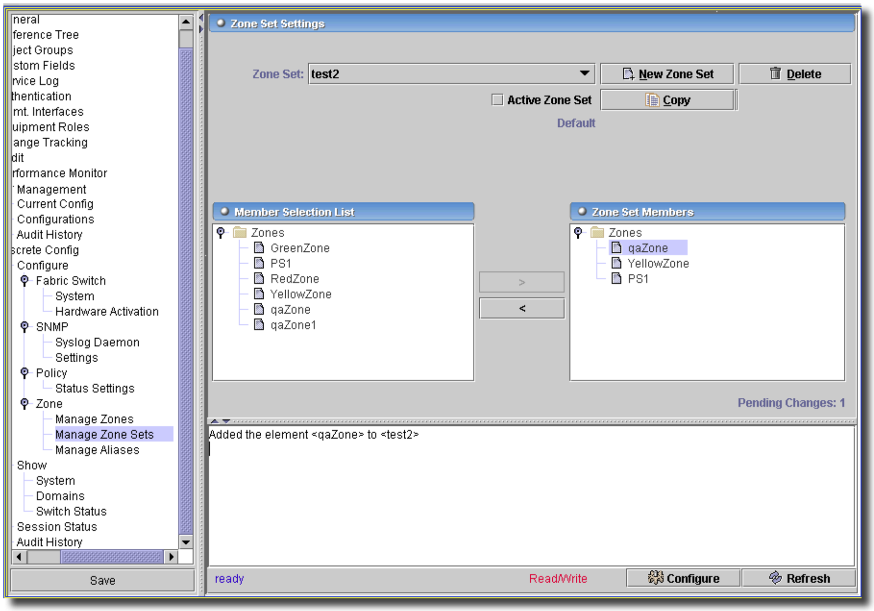
Member Selection List / Zone Members

Click the right arrow to send selected Ports to Ports in the zone (those on the right). Click *Configure* to send this configuration to the device, or *Refresh* to update the information.

Zone -> Manage Zone Sets

This screen manages zone configurations for the selected device. The maximum number of items that can be stored in the zoning configuration depends on the switches in the fabric.

Figure 13-7. Zone -> Manage Configs



Zone Set: test2

☐ Active Zone Set

Added the element <qaZone> to <test2>

Pending Changes: 1

Click *New Zone Set* to add a configuration to the pick list at the top of this screen, or select a member of that list to modify an existing Zone Set. Select a configuration and click *Delete* or *Copy* to remove or copy a listed configuration. Click *Configure* to send this configuration to the device, or *Refresh* to update the information.

Check *Effective Zone Set* to make the selected Zone Set the one in effect. A read-only reminder of which is the effective Zone Set appears in the upper right corner of this screen.

Member Selection List / Zone Set Members

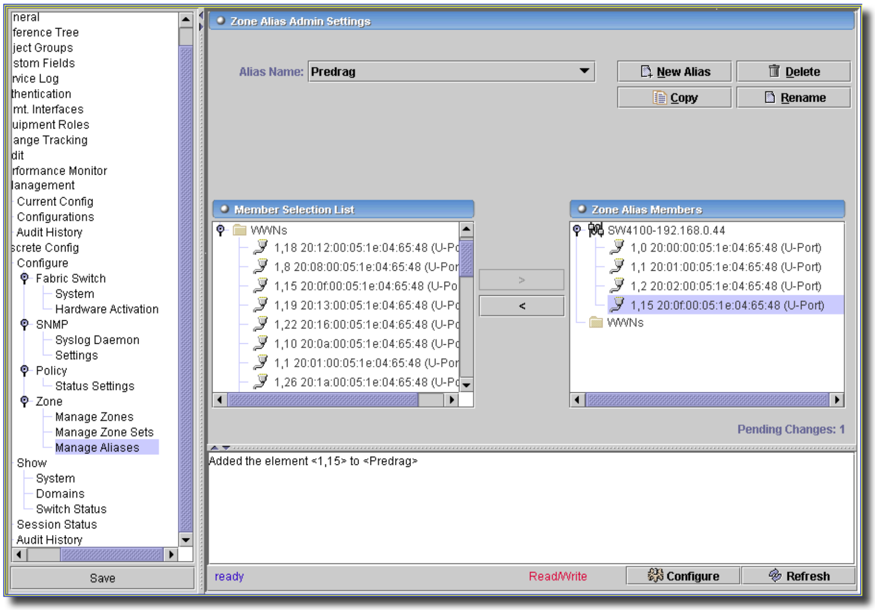
Click the right arrow to send selected Zone to the selected set (those on the right). Actions configured in this screen, reconfiguring, adding or deleting members, appear listed in the *Pending Changes* panel at the bottom of this screen (you may have to click and drag the divider to see this panel). They do not take effect until you Click *Configure*.

Click *Configure* to send this configuration to the device, or *Refresh* to update the information.

Zone -> Manage Aliases

This screen manages aliases for zones for the selected device.

Figure 13-8. Zone -> Manage Aliases



Alias Name: Predrag

Member Selection List:

WWNs
- 1,18 20:12:00:05:1e:04:65:48 (U-Po
- 1,8 20:08:00:05:1e:04:65:48 (U-Por
- 1,15 20:0f:00:05:1e:04:65:48 (U-Po
- 1,19 20:13:00:05:1e:04:65:48 (U-Po
- 1,22 20:16:00:05:1e:04:65:48 (U-Po
- 1,10 20:0a:00:05:1e:04:65:48 (U-Po
- 1,1 20:01:00:05:1e:04:65:48 (U-Por
- 1,26 20:1a:00:05:1e:04:65:48 (U-Po

Zone Alias Members:

SW4100-192.168.0.44
- 1,0 20:00:00:05:1e:04:65:48 (U-Port)
- 1,1 20:01:00:05:1e:04:65:48 (U-Port)
- 1,2 20:02:00:05:1e:04:65:48 (U-Port)
- 1,15 20:0f:00:05:1e:04:65:48 (U-Port)

WWNs

Pending Changes: 1

```
Added the element <1,15> to <Predrag>
```

ready Read/Write

Click *New Alias* to add a configuration to the pick list at the top of this screen, or select a member of that list to modify an existing Alias. Select a configuration and click *Delete* or *Copy* to remove or copy a listed Alias. Click *Configure* to send this configuration to the device, or *Refresh* to update the information.

Member Selection List / Alias Members

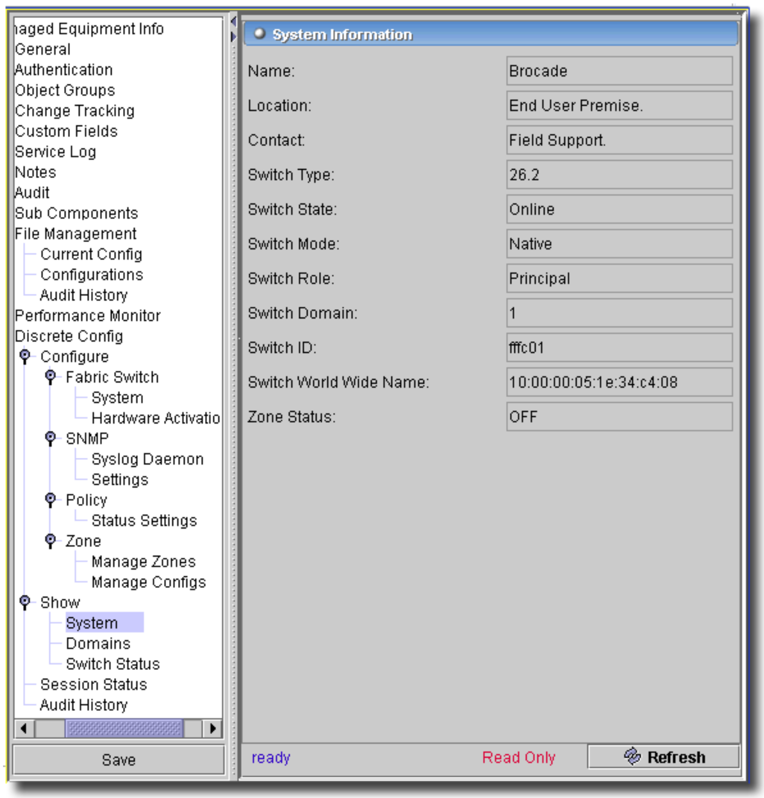
Click the right arrow to send selected members to the selected Alias (those on the right). Actions configured in this screen, reconfiguring, adding or deleting members, appear listed in the *Pending Changes* panel at the bottom of this screen (you may have to click and drag the divider to see this panel). They do not take effect until you Click *Configure*.

Click *Configure* to send this configuration to the device, or *Refresh* to update the information.

Show -> System

This screen displays system settings for the selected device.

Figure 13-9. Show -> System



System Information

Name: Brocade
Location: End User Premise.
Contact: Field Support.
Switch Type: 26.2
Switch State: Online
Switch Mode: Native
Switch Role: Principal
Switch Domain: 1
Switch ID: fffc01
Switch World Wide Name: 10:00:00:05:1e:34:c4:08
Zone Status: OFF

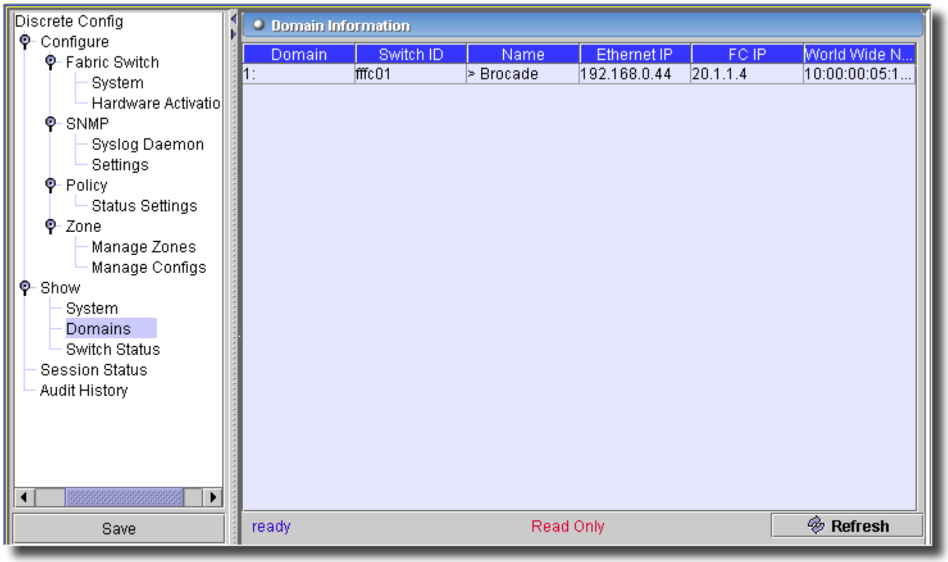
ready Read Only

Click *Refresh* to update the information.

Show -> Domains

This screen displays system settings for the selected device.

Figure 13-10. Show -> Domains



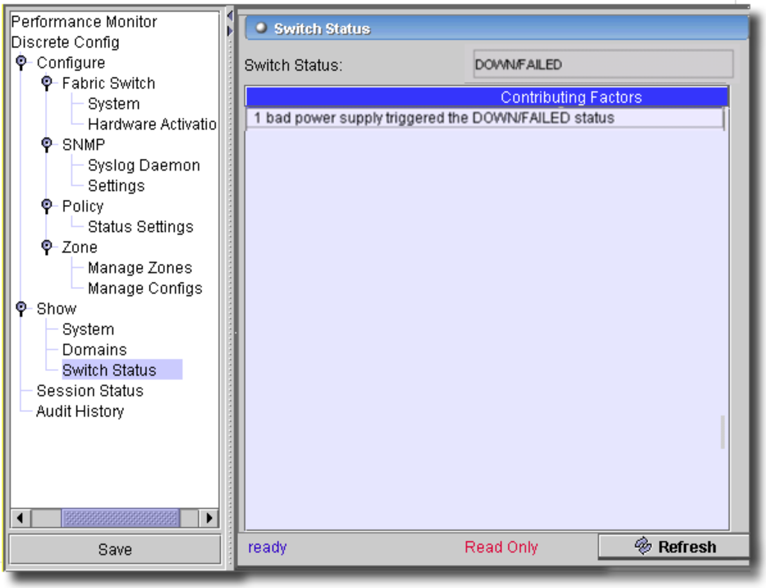
Domain	Switch ID	Name	Ethernet IP	FC IP	World Wide N...
1:	fffc01	> Brocade	192.168.0.44	20.1.1.4	10:00:00:05:1...

Click *Refresh* to update the information.

Show -> Switch Status

This screen displays system settings for the selected device.

Figure 13-11. Show -> Switch Status



Switch Status: DOWN/FAILED

Contributing Factors

1 bad power supply triggered the DOWN/FAILED status

Click *Refresh* to update the information.

Dell PowerConnect J-series Device Driver

The following sections discuss the J-series Device Driver-related device driver panels, and how this device driver changes Equipment Editor and other aspects of OpenManage Network Manager's operation.The IRM (Internet Router Module) is used with the Lucent CBX device.

NOTE:

If a J-series device has multiple management IP addresses, discovery by subnet, CIDR or IP range saves only the last IP address configured in the list of management interfaces.

To get firmware images for updates, go to www.juniper.com, and deploy as you would other firmware updates in OpenManage Network Manager.

Pre-Configuring the Hardware

You must set up your J-series equipment to respond correctly to this application. For example: J-series users require users assigned to the superuser class for some operations. Consult the hardware's manuals and/or the *Administration Section* for specifics. Configuration for these devices is based on XML transmitted over SSH/Telnet. File transfer (backup/restore) is done with FTP/SFTP (FTP over SSH). Here are examples of pre-configuration commands for this equipment:

Community String

Enable a community string on the J-series router to enable the RNS management system to access the router via snmp to enable high level discovery.

```
community dorado {
    authorization read-only;
}
```

Trap Group

Enable a trap group specifying the application's IP address.

```
trap-group dorado {
    targets {
        192.168.0.98;
    }
```

Telnet

You must enable telnet service to enable deep discovery.

```
services {
    telnet {
        connection-limit 50;
        rate-limit 50;
        }
    }
```

Radius Server

You must either define a user or provice user access with a radius server, as follows.

```
    login {
        user superguy {
            class super-user;
            authentication {
                encrypted-password "$1$iX9M87qC$rBJubIgZ.8cjJyuxnn5cG/"; #
    SECRET-DATA
            }
        }
    }
```

MTU Configuration for L3 VPNs

Provisioning L3 VPNs one customer site at a time works well, but trying to provision two sites or more at the same time, may fail, leaving stray configurations on the router that may cause more problems.

The root issue is an MTU problem in the WAN cloud between the OpenManage Network Manager server and the J-series routers. OpenManage Network Manager provisions using JUNOScript over telnet/ssh, and sends large packet sizes (default MTU on Solaris server is 1500) that somehow get fragmented and fail. The workaround is to configure the MTU size on the Ethernet NIC on the Solaris host to a lower value (say, 1300 or 1400).

Preserving Configlet Files for Debugging

You can preserve restored configlet files on the device, for debugging. Go to the menu item *Settings* -> *Configuration* -> *Control Settings*, and, in the properties tab of the screen this produces, find `redcell.devicedriver.juniper.netrestore.delete_tmp_files`. By default, this is true, and deletes the files in temporary storage. change this to false to preserve the files.

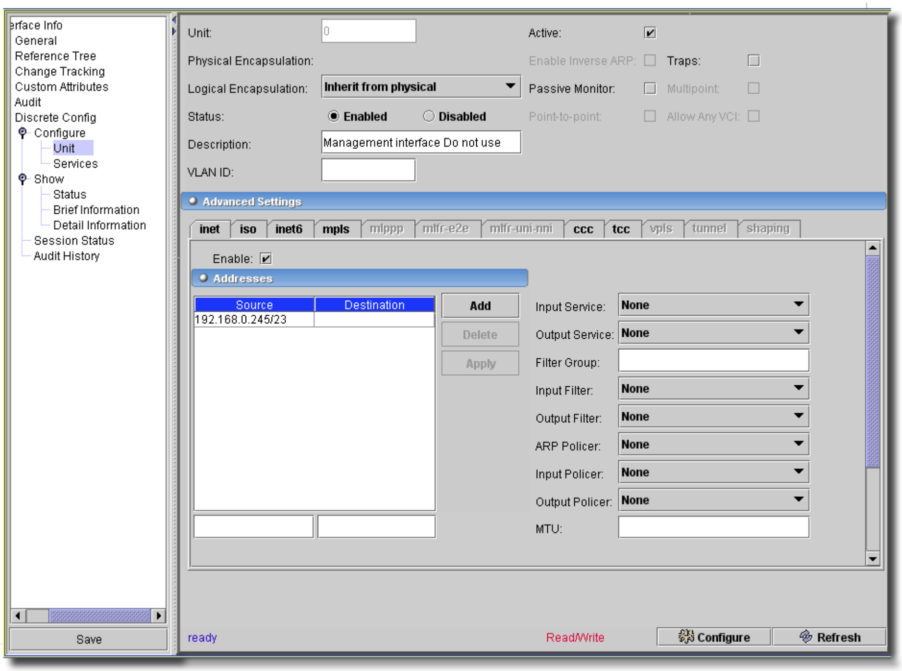
You can see the preserved temporary files by logging into the device that was configured. Once logged in, type `start shell` to get into the shell command mode. Display the temporary directory typing `cd /tmp`. The temporary configlet files are stored here. Type `cat 'filename.conf'` to see the file contents. Find the filename restored from the user interface by looking at the details of the Audit Log for that restore action.

Making a Link

This describes the process of making and verifying an ISIS link between two J-series devices:

1 After you discover two J-series devices (we'll call them "A" and "B") right-click an interface (fe 0/0/0) and select *Open*.

2 In Configure -> Units, select the iso tab, click *Enable*, and enter `49.0001.0245.0245.0245.00` as the ISO Network Address.



Unit: 0

Active: ☑

Physical Encapsulation:

Enable Inverse ARP: □ Traps: □

Logical Encapsulation: Inherit from physical

Passive Monitor: □ Multipoint: □

Status: ● Enabled ○ Disabled

Point-to-point: □ Allow Any VCI: □

Description: Management interface Do not use

VLAN ID:

Advanced Settings

Enable: ☑

Addresses

Source	Destination
192.168.0.245/23	

Input Service: None

Output Service: None

Filter Group:

Input Filter: None

Output Filter: None

ARP Policer: None

Input Policer: None

Output Policer: None

MTU:

ready

Read/Write

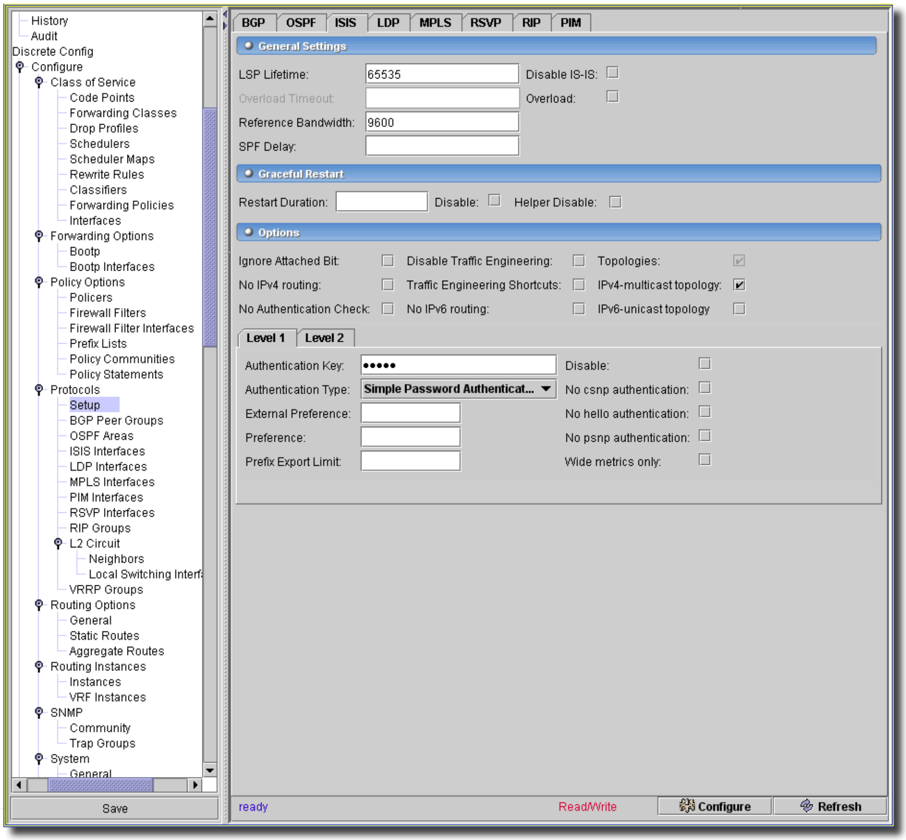
An ISO address—for example, `49.0001.0118.0118.0118.00`–is 16 bytes. Reading from right-to-left, the last `00` is the NSAP selector and is always `00`. The `0118.0118.0118` is the system ID, which should be unique on your network. The `49.0001` is the Area address. Finally, `49` indicates that the ISO address is private.

3 Click *Apply* and *Configure*

4 Edit the entire managed resource where you just configured the interface above.

5 Click to open *Discrete Config* -> *Configure* -> *Protocols* -> *Setup*, and select the *ISIS* tab.

6 Select the *Level 1* tab



General Settings

LSP Lifetime: 65535 Disable IS-IS: □

Overload Timeout: Overload: □

Reference Bandwidth: 9600

SPF Delay:

Graceful Restart

Restart Duration: Disable: □ Helper Disable: □

Options

Ignore Attached Bit: □ Disable Traffic Engineering: □ Topologies: ☑

No IPv4 routing: □ Traffic Engineering Shortcuts: □ IPv4-multicast topology: ☑

No Authentication Check: □ No IPv6 routing: □ IPv6-unicast topology □

Level 1 | Level 2

Authentication Key: ••••• Disable: □

Authentication Type: Simple Password Authenticat... No csnp authentication: □

External Preference: No hello authentication: □

Preference: No psnp authentication: □

Prefix Export Limit: Wide metrics only: □

7 Enter an Authentication Key, for example, *MyKey*

8 Select authentication type. For example, *Simple Password Authentication*

9 Click *Configure*

10 Open Discrete Config -> configure -> Protocols -> ISIS interfaces

11 Click *Add*

12 Enter Name: *all*

13 Check *Active*

14 Select the *Level 1* tab

15 Enter the *Hello Auth Key*: MyKey, and *Hello Auth type*: Simple Password Authentication

16 Click *Apply* and *Configure*

17 For the “B” equipment, perform the same steps as above described with different data

18 Set 49.0001.0118.0118.0118.00 as its iso address under fxp0.0

Check if ISIS adjacency formed

19 You can check for ISIS adjacency manually with the command `show isis adjacency` after you telnet to either / both hosts.

20 Alternatively, you can discover the ISIS Peer Link using OpenManage Network Manager

21 Open the Link manager (*Inventory* -> *Links*)

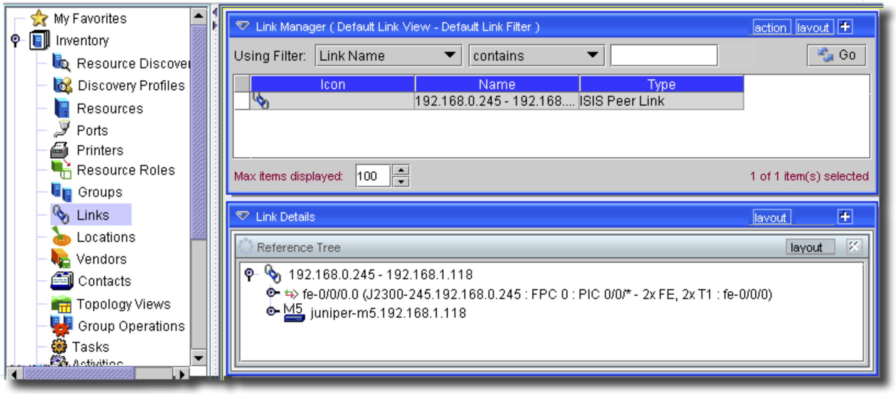
22 Select *action* -> *Discover Links* from that menu.

23 Click *Add* and ctrl+click both resources (A and B) as places to do discovery, then click the *Select* button.

24 Click *Next*

25 Select the *ISIS Peer Link* type.

26 Click Next, and you should see at least one ISIS Peer Link discovered.



Using Filter: Link Name contains

Icon	Name	Type
	192.168.0.245 - 192.168....	ISIS Peer Link

Max items displayed: 100

1 of 1 item(s) selected

192.168.0.245 - 192.168.1.118
fe-0/0/0.0 (J2300-245.192.168.0.245 : FPC 0 : PIC 0/0/* - 2x FE, 2x T1 : fe-0/0/0)
M5 juniper-m5.192.168.1.118

Group Operations

This device driver now supports Batch/Global Group Operations for the following:

Batch and Global Group Operations

- Adaptive Services—IDS Rules on page 436, IP-Security Policies on page 431, Network Address Translation (NAT) on page 426, and Stateful Firewall Rules on page 423.
- System Authentication—System Authentication -> Authentication Order on page 569, System Authentication -> Login Class on page 571, System Authentication -> Login User on page 570 and System Authentication -> Radius / TACACs on page 569.
- Setting SNMP Trap & Community—See SNMP -> Trap Groups on page 555 and SNMP -> Community on page 554.
- System Date and Time, Services—System -> Date and Time on page 559 and System -> Services on page 561

Batch Group Operations

- Protocols— See Protocols -> ISIS Interfaces on page 516, Protocols -> LDP Interfaces on page 519, Protocols -> MPLS Interfaces on page 520, Protocols -> OSPF Areas on page 510, Protocols -> RIP Groups on page 525 and Protocols -> RSVP Interfaces on page 523.
- Bootp and Bootp Interfaces in Forwarding Options -> Bootp on page 464 and Forwarding Options -> Bootp Interfaces on page 465.
- Channelized PICs on page 610
- System—System -> General on page 557, and System -> Loopback on page 561
- Routing Options -> Static Routes on page 534

Global Group Operations

- System—System -> Location on page 560, System -> Syslog Files on page 564, System -> Syslog Hosts on page 566, System -> Syslog Settings on page 562, and System -> Syslog Users on page 568.
- Channelized Options—including CH AU-4, CH E1, CH OC-1, CH OC12, CH T1, CH, T3, DSO, E1, E1 QPP, E3, STM-1, Sonet, T1, T1 QPP, and T3. See Channelized PICs on page 610 for more information.

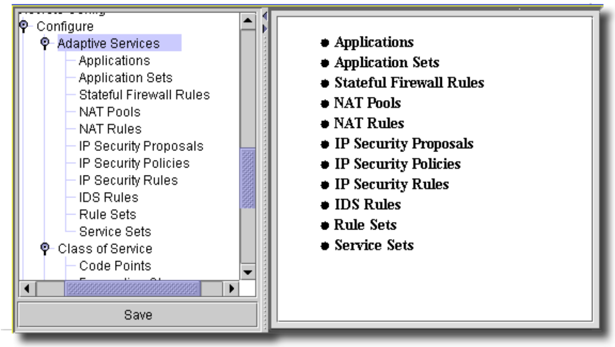
NOTE:

Class of Service, and Adaptive services require a license. Contact your sales representative for more information.

Adaptive Services PIC

The following screens are available to manage Adaptive Services PICs. Such PICs let you provide multiple services on a single PIC by configuring a set of services and applications.

Figure 13-1. Adaptive Services PIC



- Applications
- Application Sets
- Stateful Firewall Rules
- NAT Pools
- NAT Rules
- IP Security Proposals
- IP Security Policies
- IP Security Rules
- IDS Rules
- Rule Sets
- Service Sets

NOTE:

Adaptive services require a license. Contact your sales representative for more information. If you have a license, use the Settings -> Permissions -> Register License menu item to open a dialog that lets you locate the license file. Select the file, and click Register License in the dialog, and you can use the licensed product.

You can install the ASP PIC on any M Series Router but the M7i and M10i includes an integrated version.

The following are services configured within a Service Set:

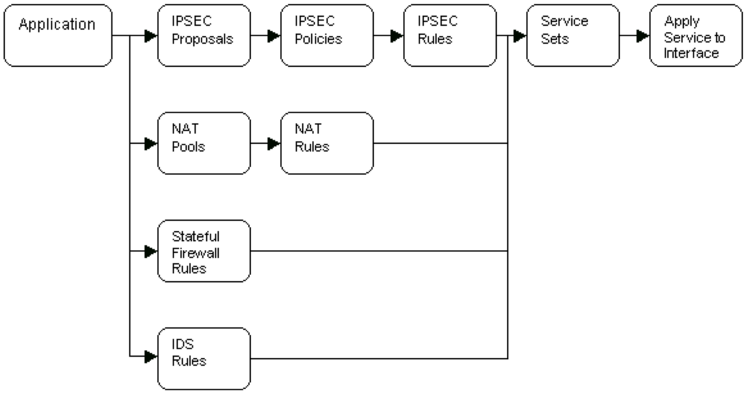
- Stateful firewall
- Network Address Translation (NAT)
- Intrusion detection services (IDS)
- Internet Protocol Security (IPSec)

Each service follows the structure of a firewall filter:

- Match Criteria which compares traffic.
- Actions to be taken if the match conditions are met

The ASP Services configuration flow appears here in the order you typically configure Adaptive Services on a device for the first time.

Figure 13-2. Adaptive Services Flow

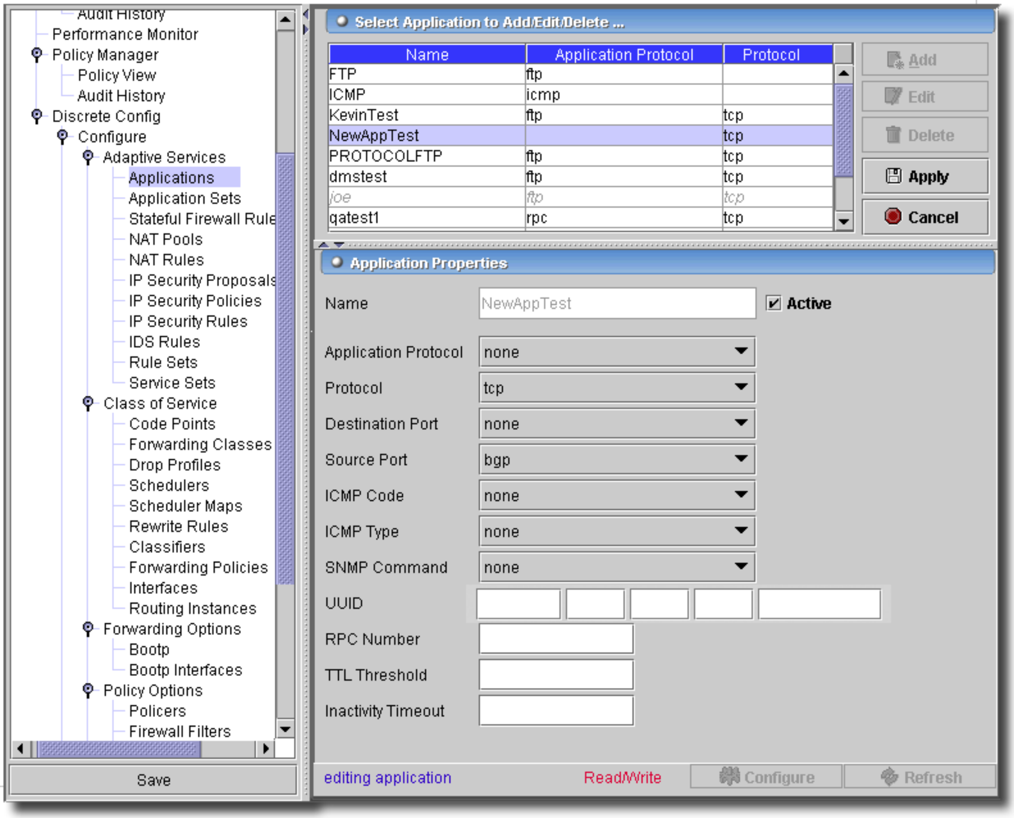


- Applications
- IPSEC Proposals, Policies, and Rules.
- Stateful Firewalls
  - Stateful Firewall Rules
- Network-Address-Translation (NAT)
  - NAT Pools
  - NAT Rules
- IDS Rules
- Service-Sets
- Apply Service-Sets to Interfaces

Applications

An application protocol defines application parameters using information from network Layer 3 and above. In this screen, you can select the properties of applications.

Figure 13-3. Adaptive Services Applications



Name	Application Protocol	Protocol
FTP	ftp	
ICMP	icmp	
KevinTest	ftp	tcp
NewAppTest		tcp
PROTOCOLFTP	ftp	tcp
dmstest	ftp	tcp
joe	ftp	tcp
qatest1	rpc	tcp

Name: NewAppTest ☑ Active

Application Protocol: none

Protocol: tcp

Destination Port: none

Source Port: bgp

ICMP Code: none

ICMP Type: none

SNMP Command: none

UUID:

RPC Number:

TTL Threshold:

Inactivity Timeout:

editing application Read/Write

Add, *Edit* or *Delete* selected applications. Click *Export* to save a description of these listed items to a file. When you *Add* or *Edit* a selected application set, the following fields appear:

- **Name**—An identifier for the application.

- **Application Protocol**—Select the protocol from the pick list. Options include *none, bootp, dce-rpc, dce-rpc-portmap, dns, exec, ftp, h323, icmp, iiop, login, netbios, netwho, readaudio, rpc, rpc-portmap, rtsp, shell, snmp, sqlnet, tftp, tracerout, winframe.*

- **Protocol**—Select the protocol from the pick list. Options include *none, ah, egp, esp, gre, icmp, igmp, ipip, ospf, pim, rsvp, sctp, tcp, udp.*

- **Destination Port**—Select the destination from the pick list. Options include *Enter port # / range, afs, bgp, biff, bootpc, bootps, cmd, cvspserver, dhcp, domain, eklogin, ekshell, exec, finger, ftp, ftp-data, http, https, ident, imap, kerberos-sec, klogin, kpasswd, krb-prop, krbupdate, kshell, ldap, ldp, login, mobileip-agent, mobilip-mn, msdp, netbios-dgm, netbios-ns, netbios-ssn, nfsd, nntp, ntalk, ntp, pop3, pptp, printer, radacct, radius, rip, rkinit, smtp, snmp, socks, ssh, sunrpc, syslog, tacacs, talk, telnet, tftp, timed, who, xdmcp.*

- **Source Port**—Select the source from the pick list (see *Destination Port* for available options.

- **ICMP Code**—Select the ICMP Code from the pick list. Options include *none*, *communication-prohibited-by-filtering*, *destination-host-prohibited*, *destination-host-unknown*, *destination-network-prohibited*, *destination-network-unknown*, *fragmentation-needed*, *host-precedence-violation*, *host-unreachable*, *host-unreachable-for-tos*, *ip-header-bad*, *network-unreachable*, *port-unreachable*, *precedence-cutoff-in-effect*, *protocol-unreachable*, *redirect-for-host*, *redirect-for-network*, *redirect-for-tos-and-host*, *redirect-for-tos-and-network*, *required-option-missing*, *source-host-isolated*, *source-route-failed*, *ttl-eq-zero-during-reassembly*, *ttl-eq-zero-during-transit*.

- **ICMP Type**—Select the ICMP Type from the pick list. Options include *none*, *echo-reply*, *echo-request*, *info-reply*, *info-request*, *mask-reply*, *mask-request*, *parameter-problem*, *redirect*, *router-advertisement*, *router-solicit*, *source-quench*, *time-exceeded*, *timestamp*, *timestamp-reply*, *unreachable*.

- **SNMP Command**—Select the SNMP command from the pick list. Options include *none*, *get*, *get-next*, *get-response*, *set*, *trap*.

- **UUID**—Match universal unique identifier for DCE RPC objects.

- **RPC Number**—Match range of RPC program numbers.

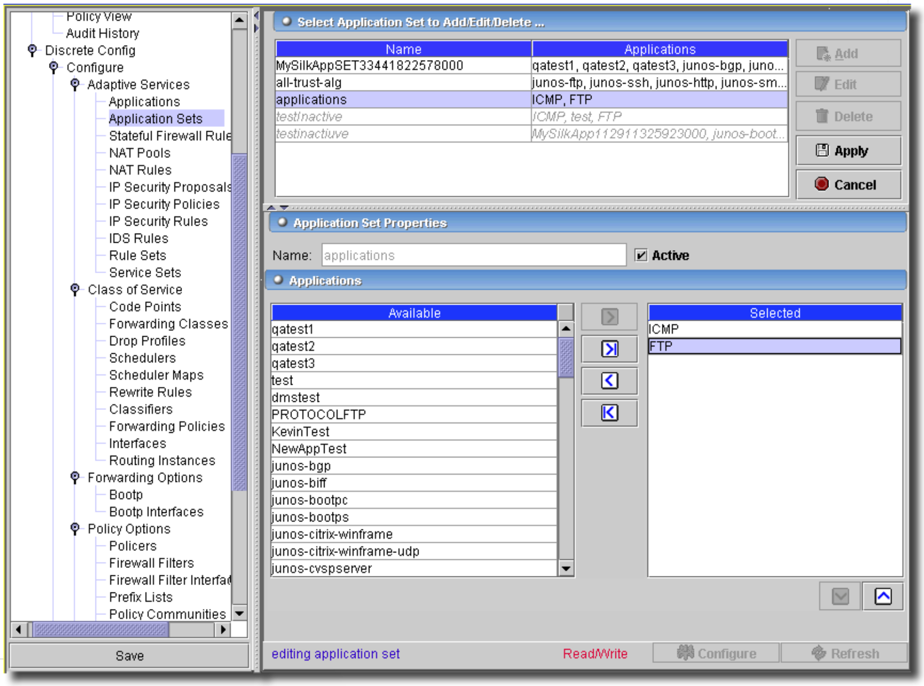
- **TTL Threshold**—Traceroute TTL threshold (0 - 255).

- **Inactivity Timeout**—Application-specific inactivity timeout (4 - 86400 seconds).

Application Sets

An application protocol defines application parameters using information from network Layer 3 and above.

Figure 13-4. Adaptive Services—Application



Name	Applications
MySilkAppSET33441822578000	qatest1, qatest2, qatest3, junos-bgp, juno...
all-trust-alg	junos-ftp, junos-ssh, junos-http, junos-sm...
applications	ICMP, FTP
testInactive	ICMP, test, FTP
testinactiuve	MySilkApp11291132592300, junos-boot...

Name: applications ☑ Active

Available
qatest1
qatest2
qatest3
test
dmstest
PROTOCOLFTP
KevinTest
NewAppTest
junos-bgp
junos-biff
junos-bootpc
junos-bootps
junos-citrix-winframe
junos-citrix-winframe-udp
junos-cvspserver

Selected
ICMP
FTP

editing application set ReadWrite

Add, *Edit* or *Delete* selected application sets from those selected at the bottom of this screen. Click *Export* to save a description of the listed items to a file. When you *Add* or *Edit* a selected application set, the selection panel appears. Use the arrows to move applications from the *Available* to the *Selected* panel (and back).

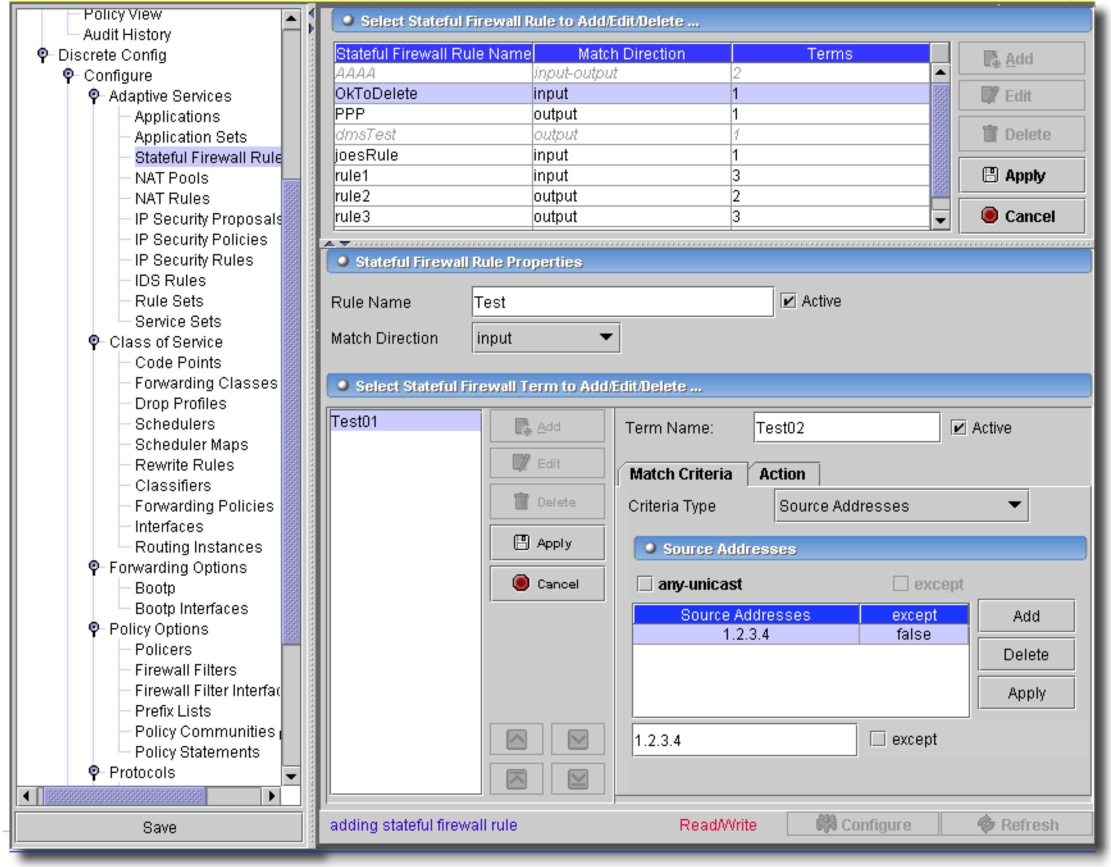
Stateful Firewall Rules

Contrasted with a stateless firewall that inspects packets in isolation, a stateful firewall provides an extra layer of security by using state information derived from past communications and other applications to make dynamic control decisions for new communication attempts.

By inspecting the application protocol data, the AS PIC firewall can intelligently enforce security policies and allow only the minimal required packet traffic to flow through the firewall.

This driver also lets you configure firewall services with group operations. Consult the following sections for field definitions on the group operations screen. This configures Stateful Firewall rules.

Figure 13-5. Adaptive Services—Stateful Firewall Rules



Policy View
Audit History
Discrete Config
Configure
Adaptive Services
Applications
Application Sets
Stateful Firewall Rule
NAT Pools
NAT Rules
IP Security Proposals
IP Security Policies
IP Security Rules
IDS Rules
Rule Sets
Service Sets
Class of Service
Code Points
Forwarding Classes
Drop Profiles
Schedulers
Scheduler Maps
Rewrite Rules
Classifiers
Forwarding Policies
Interfaces
Routing Instances
Forwarding Options
Bootp
Bootp Interfaces
Policy Options
Policers
Firewall Filters
Firewall Filter Interfac
Prefix Lists
Policy Communities
Policy Statements
Protocols

Select Stateful Firewall Rule to Add/Edit/Delete ...

Stateful Firewall Rule Name	Match Direction	Terms
AAAA	*input-output*	*2*
OkToDelete	input	1
PPP	output	1
dmsTest	*output*	*1*
joesRule	input	1
rule1	input	3
rule2	output	2
rule3	output	3

Stateful Firewall Rule Properties

Rule Name	Test ☑ Active
Match Direction	input

Select Stateful Firewall Term to Add/Edit/Delete ...

Test01

Term Name:	Test02 ☑ Active
Criteria Type	Source Addresses

Source Addresses

□ any-unicast □ except

Source Addresses	except
1.2.3.4	false

1.2.3.4 □ except

adding stateful firewall rule ReadWrite

Click *Add* (or select an existing rule and click *Edit*) to open the firewall rules editor. You can also click *Delete* to remove a selected firewall rule at the top of this screen. Click *Export* to save a description of the listed items to a file. Once you have edited a rule, click *Apply* to accept your edits for the list, or click *Cancel* to abandon them. The editor has the following fields:

- **Rule Name**—An identifier for the stateful firewall ruleset.

- **Active**—Check this to activate the rule.

- **Match Direction**—*input/output*. These specify the side of the interface where the rule applies.

Select a Stateful Firewall term to Add/Edit:

The firewall rule terms appear listed on the left. Use the *Add/Edit/Delete/Export* buttons in this portion of the screen to manage them. The editor for terms appears in the right panel. Here are the fields you can configure in this screen:

- **Term Name**—The identifier for the term.

- **Active**—Check this to enable the term.

Firewall filters consist of one or more terms that specify the filtering criteria and the action to take if a match occurs. Some handy definitions:

- Match Criteria tab —Specifies values or fields that the packet must contain including the IP destination address or the TCP protocol.

- Action tab—Specifies what to do if a packet matches the match conditions. Actions include accepting, discarding, or rejecting a packet, then going to the next term.

The order of the terms within a firewall filter is also significant. The application tests packets against each term in the listed order. When it finds the first matching conditions, it applies the action associated with that term to the packet and the evaluation of the firewall filter ends.

After all terms are evaluated, if a packet matches no terms in a filter, the application silently discards the packet. IPv4 is the supported packet type.

Match Criteria tab

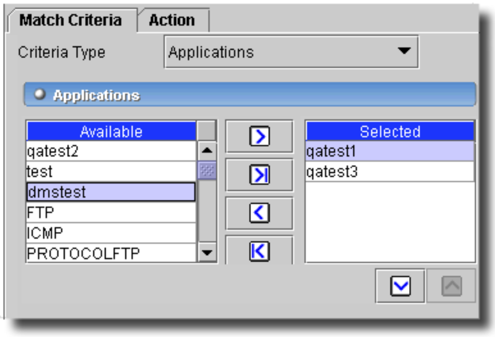
This tab lets you configure match criteria for a rule term.

- **Criteria**—Select criteria from the pick list. Criteria include *Source Address*, *Destination Address*, *Application*, *Application Sets*.

- **Address**—If you select one of the *Address* terms, the editor panel lets you enter IP addresses for source or destination. You can also check *any-unicast* as an address. Click *Add* to add the address you type in the field below the list. Check *Except* if you want to exclude this address from the criteria.

- **Application/Application Sets**—When you select one of the *Application* or *Application Set* terms, the editor panel lets you select from available applications or application sets (see Applications on page 420 and Application Sets on page 422 for the source of this information).

Figure 13-6. Firewall Rule Term Match Criteria



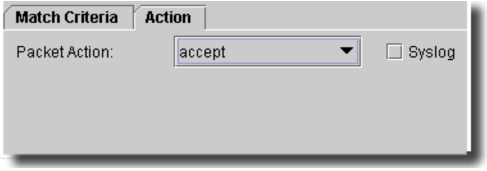
Criteria Type: Applications

Click one of the *Available* applications or application sets, and click the right arrow (>) to move it to the *Selected* panel. You can also use the up/down arrows below the *Selected* panel to reorder selected items.

Action tab

This tab lets you configure an action once this term's match criteria are met.

Figure 13-7. Firewall Rule Term Actions.



Packet Action: accept

□ Syslog

- Potential actions on the pick list in this tab include the following:

- **Accept**—Packet is accepted and sent to its destination

- **Discard**—Packet is not accepted and is not processed further.

- **Reject**—Packet is not accepted, and a rejection message returns.

- **Syslog**—Check this if you want to log the property's action.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Network Address Translation (NAT)

Network Address Translation (NAT) is a mechanism for concealing a set of host addresses on a private network behind a pool of public addresses. This can be a security measure to protect the host addresses from direct targeting in network attacks. Network address port translation (NAPT) is supported for source addresses.

This device driver also supports NAT as a group operation. Consult NAT Rules on page 427 for a description of the fields in the group operations screen.

The AS PIC interfaces support the following types of NAT processing:

- **Static-source** NAT hides a private network without using NAPT.

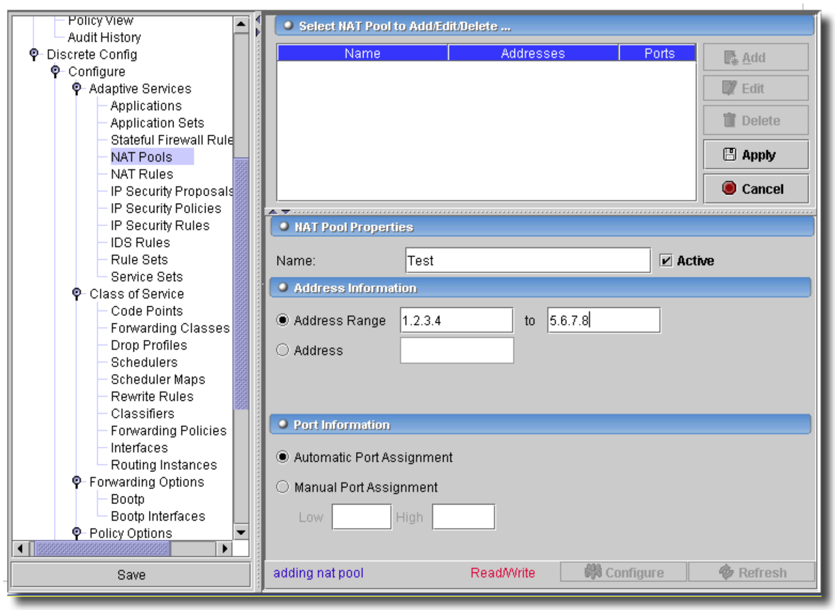
- **Dynamic-source** NAT hides a private network using NAPT.

- **Static-destination** NAT makes selected private servers accessible.

NAT Pools

NAT Pools define the address(es) and port(s) used for network address translation.

Figure 13-8. Adaptive Services—NAT Pool Properties



Name: Test ☑ Active

● Address Range 1.2.3.4 to 5.6.7.8

○ Address

● Automatic Port Assignment

○ Manual Port Assignment

Low High

adding nat pool Read/Write

Click *Add*, *Edit*, *Delete* or *Export* to manage the listed pools at the top of this screen. Click *Export* to save a description of the listed items to a file. When you *Add* or *Edit*, you can specify either a single specific address, a prefix, or an address range. For example:

```
Pool: My-New-Pool
    address-range low 192.168.8.3 high 192.168.8.31;
    port automatic;
```

Click *Apply* to accept your edits, or *Cancel* to abandon them.

Fields to configure:

- **Name**—Identifier for the NAT pool.

- **Address / Address Range**—IP address(es). These are limited to a maximum of 32 addresses.

- **Port Information**—You can elect automatic port assignment, or a manually-assigned range of ports.

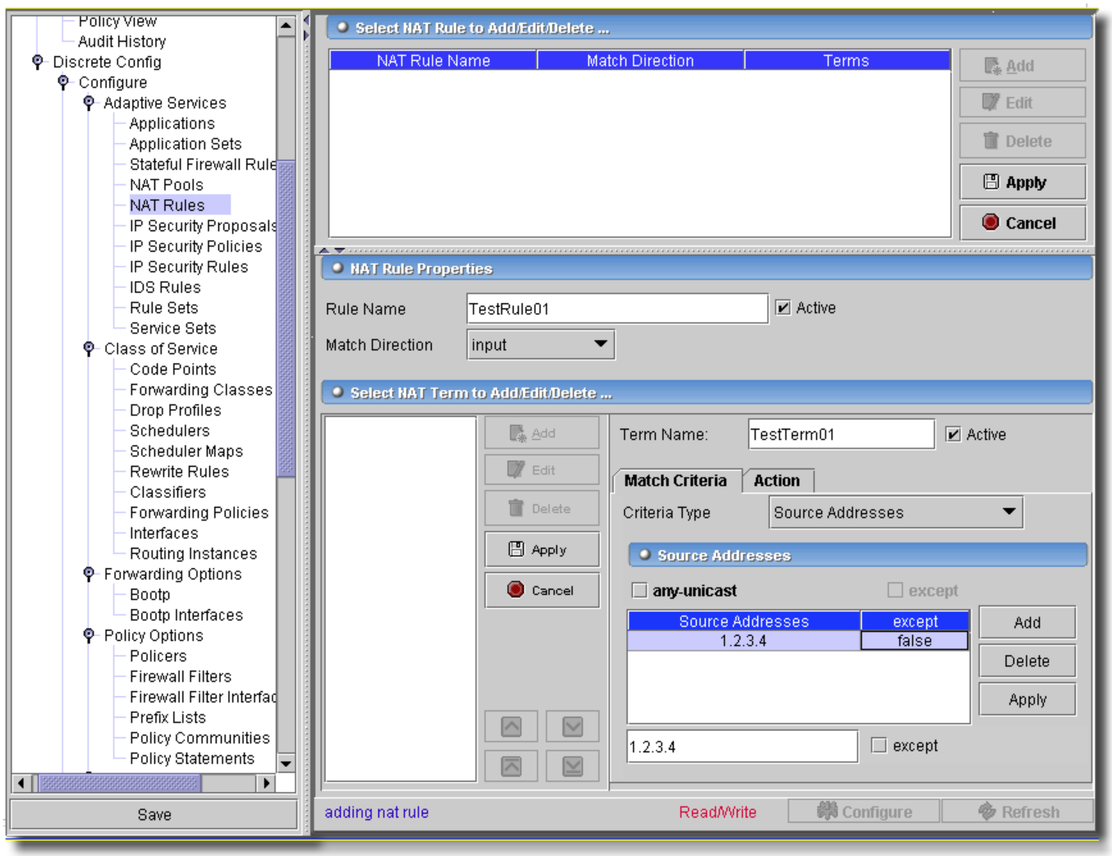
- Click *Apply* to finish configuring the NAT Pool.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

NAT Rules

This application also offers a screen configure NAT rules

Figure 13-9. Adaptive Services—NAT Rules



NAT Rule Name	Match Direction	Terms

Rule Name: TestRule01 ☑ Active

Match Direction: input

Term Name: TestTerm01 ☑ Active

Criteria Type: Source Addresses

□ any-unicast □ except

Source Addresses	except
1.2.3.4	false

1.2.3.4 □ except

adding nat rule

Read/Write

In the first screen, select the *Name*, *Direction* (only *input/output* here), and *Rule Set*. Click *Export* to save a description of the listed items to a file. Click *Add* (or select an existing rule and click *Edit*) to open the NAT rules editor. You can also click *Delete* to remove a selected rule at the top of this screen. Click *Export* to save a description of the listed items to a file. Once you have edited a rule, click *Apply* to accept your edits for the list, or click *Cancel* to abandon them. The editor has the following fields:

- **Rule Name**—An identifier for the stateful firewall ruleset.

- **Active**—Check this to activate the rule.

- **Match Direction**—*input/output*. These specify the side of the interface where the rule applies.

Select a Stateful Firewall term to Add/Edit:

The firewall rule terms appear listed on the left. Use the *Add/Edit/Delete/Export* buttons in this portion of the screen to manage them. The editor for terms appears in the right panel. Here are the fields you can configure in this screen:

This screen also describes how to configure the rule's Match Criteria. These include Destination and Source Addresses and defined Applications or Application Sets (see Match Criteria tab on page 425). NAT rule actions are configured when you *Add*, or *Edit* an Action on this tab. In this tab, you can configure the following:

Action tab

- **Source Pool**—Select from the available pools in the pick list. This is the source address pool for translated traffic.
- **Destination Pool**—Select from the available pools in the pick list. This is the destination address pool for translated traffic.
- **Translation Type**—Possible types:

Static-source NAT hides a private network without using NAPT.

Dynamic-source NAT hides a private network using NAPT.

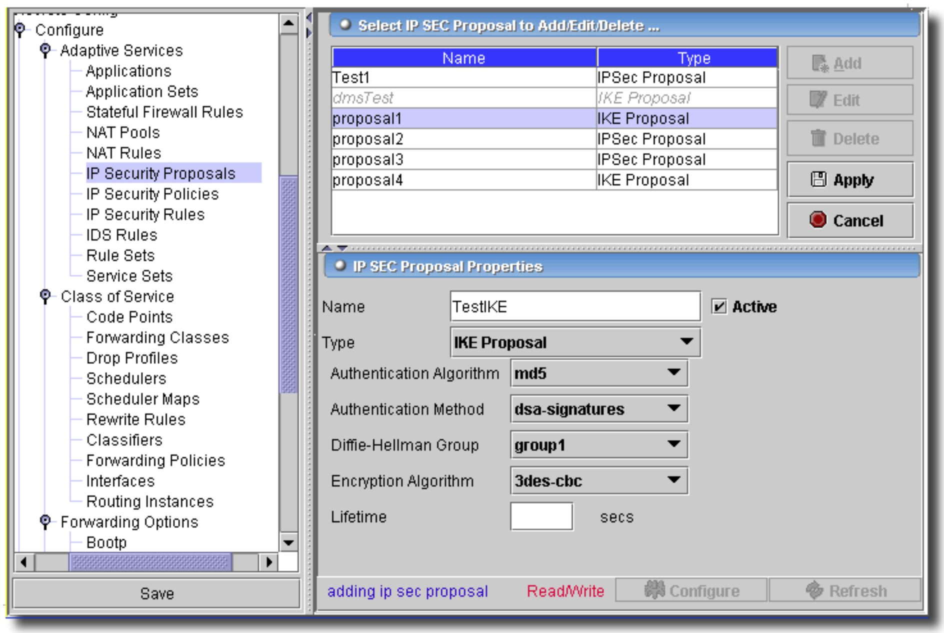
Static-destination NAT makes selected private servers accessible.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

IP Security–IKE Proposal

You can create IPSec or IKE Proposals for dynamic security associations. An IKE E proposal is a list of IKE attributes to protect the IKE connection between the IKE host and its peer. (This is the first phase and protects the initial validation of peer). An IPSec proposal lists protocols and algorithms (security services) to be negotiated with the remote IPSec peer. (This is the second phase, its protects the data after establishing a connection).

Figure 13-10. Adaptive Services—IP Sec IKE Proposal



Select IP SEC Proposal to Add/Edit/Delete ...

Name	Type
Test1	IPSec Proposal
dmsTest	IKE Proposal
proposal1	IKE Proposal
proposal2	IPSec Proposal
proposal3	IPSec Proposal
proposal4	IKE Proposal

IP SEC Proposal Properties

Name: TestIKE ☑ Active

Type: IKE Proposal

Authentication Algorithm: md5

Authentication Method: dsa-signatures

Diffie-Hellman Group: group1

Encryption Algorithm: 3des-cbc

Lifetime: secs

adding ip sec proposal Read/Write

Use the *Add*, *Edit*, *Delete*, and *Export* buttons to manage the security proposals listed in the table at the top of this screen. Like other screens, the *Name* field is a unique identifier for the configured proposal. The *Type* selection determines what fields appear below it. Here, we selected IPSec Proposal. The fields:

- **Authentication Algorithm**—Either *md5* (128 bit) or *sha1* (160 bit)

- **Authentication Method**—Either *dsa-signatures* (Digital Signature Algorithm), *preshared keys*, or *rsa signature*.

- **Diffie-Hellman Group**—Select from the pick list. This public cryptographic scheme allows two parties to establish a shared secret. Types:

group 1—768 bit.

group 2— 1024 bit (provides more security, but processing requires more time)

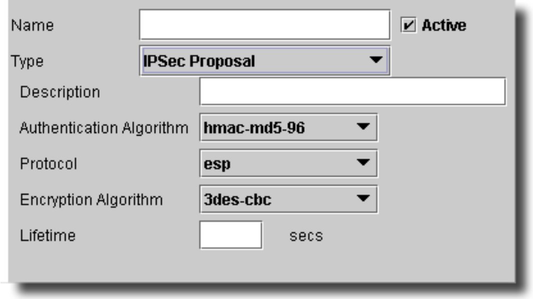
Encryption Algorithm—Select from the pick list: 3*des-cbc*, *des-cbc*.

- **Lifetime**—The lifetime of an IKE SA. Can be from 180 - 86400 seconds. The default is 3600 seconds.

IP Security–IP Sec Proposal

Choosing IP Sec proposal *Type* changes the fields at the bottom of the screen.

Figure 13-11. Adaptive Services—IP Sec Proposal



Name

☑ Active

Type: IPSec Proposal

Description

Authentication Algorithm: hmac-md5-96

Protocol: esp

Encryption Algorithm: 3des-cbc

Lifetime secs

The fields:

- **Description**—A text description of the proposal.
- **Authentication Algorithm**—Select from the pick list: *hmac-md5-96* (128 bit) or *hmac-sha1-96* (160 bit).
- **Authentication Method**—Select from the pick list alternatives: *dsa-signatures*, *rsa-signatures*, or *pre-shared key*.
- **Diffie Hellman Group**—Select from the pick list:
- **Encryption Algorithm**—Select from the pick list: *3des-cbc* (1192 bits), or *dec-cbc* (48 bits)
- **Lifetime**—The lifetime of an IPSec SA. Can be from 180 - 86400 seconds. The default is 28,800 seconds.

The *Configure* button at the bottom of the screen executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

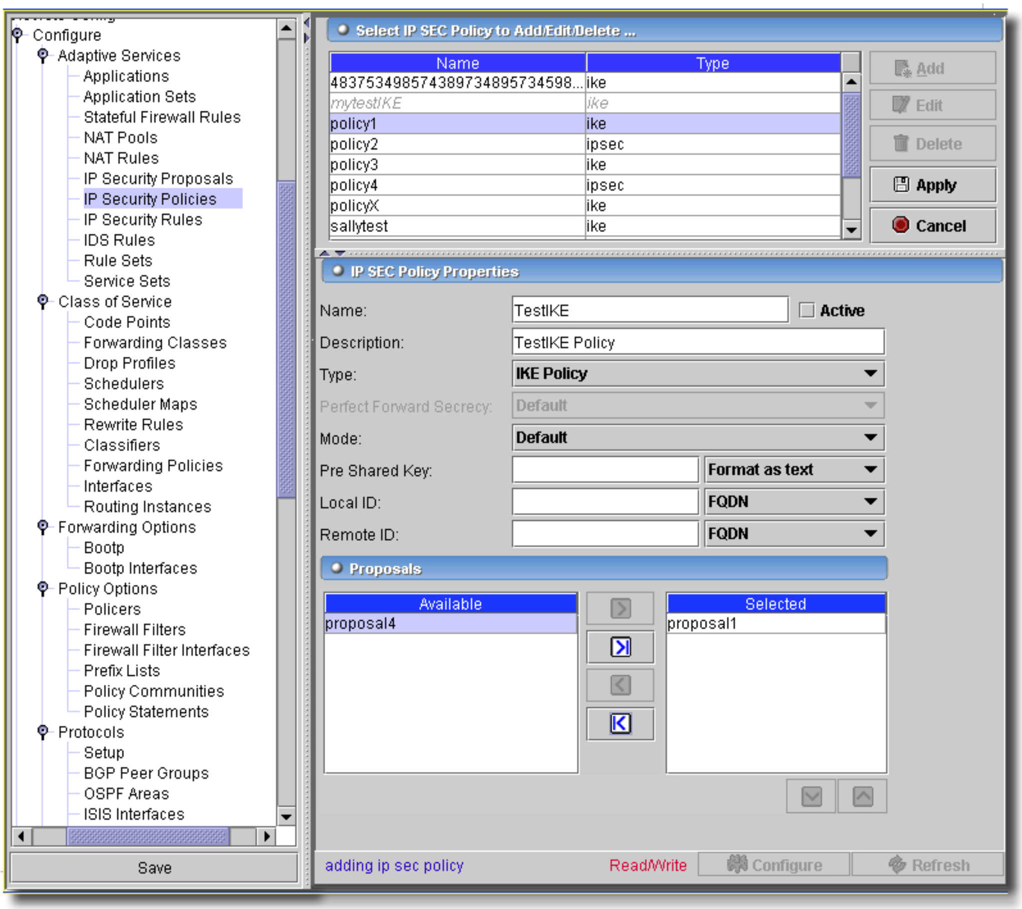
IP-Security Policies

These policies define a combination of security parameters (IPSec/IKE proposals) used during IPSec/IKE negotiation. The application seeks a proposal that is the same on both peers. It makes a match when both policies from the two peers have a proposal that contains the same configured attributes

This device driver also supports configuring IP Security Policies as a group operation.

Consult the following sections for the field definitions in the group operations screen.

Figure 13-12. Adaptive Services—IP Security Policies (IKE Edit).



Name	Type
483753498574389734895734598...	ike
mytestIKE	ike
policy1	ike
policy2	ipsec
policy3	ike
policy4	ipsec
policyX	ike
sallytest	ike

Name: TestIKE □ Active

Description: TestIKE Policy

Type: IKE Policy

Perfect Forward Secrecy: Default

Mode: Default

Pre Shared Key: Format as text

Local ID: FQDN

Remote ID: FQDN

Available	Selected
proposal4	proposal1

adding ip sec policy

Read/Write

You can create multiple, prioritized IKE/IPSec policies at each peer to ensure that at least one proposal matches a remote peer's proposal. When you *Add* or *Edit* (after selecting one in the table at the top of the screen) a policy, the policy editor appears at the bottom of the screen. The *Name* and *Description* fields are similar whether the policy is IP Sec or IKE (a unique identifier, and a text description, respectively). The fields below this change, depending on the *Type* selection.

IKE Policy

When you select IKE Policy from the *Type* pick list, you can edit the following:

Pre-shared Key

- Mode—Select a mode from the pick list. For example, *aggressive* mode increases the negotiation speed without some of the safety features.

- **Pre Shared Key**—A text field appears for a new encryption key. Select *Format as text* or *Hexadecimal*. This authenticates peers. It must match its peer's key. By default, the format is alphanumeric, but, with the pick list, you can specify hexadecimal formatting.
- **Local-ID Value**—Select from a pick list, and fill in the field, if necessary. This specifies local parameters for IKE Phase 1 Negotiation.
- **Remote-ID Value**—Select from a pick list, and fill in the field, if necessary. This defines the remote-authentication values for which the IKE Policy applies.

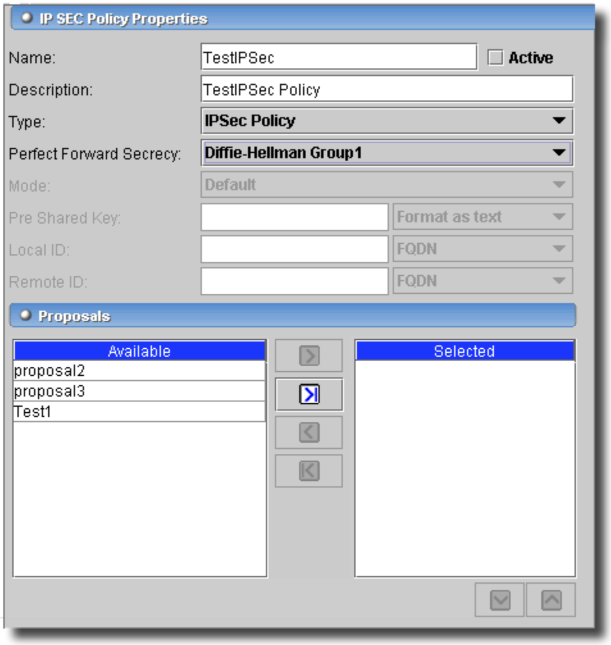
Proposals

Use this section *Add*, *Delete* or order (with the up/down arrows) the IKE Proposals selected in the pick list and connected to this policy. (See IP Security–IKE Proposal on page 429 and IP Security–IP Sec Proposal on page 430)

IP Sec Policy

- If you select IP Sec Policy as the *Type*, some different fields appear.

Figure 13-13. Adaptive Services—IP Security Policies (IP Sec Edit)



IP SEC Policy Properties

Name: TestIPSec ☐ Active

Description: TestIPSec Policy

Type: IPSec Policy

Perfect Forward Secrecy: Diffie-Hellman Group1

Mode: Default

Pre Shared Key: Format as text

Local ID: FQDN

Remote ID: FQDN

Proposals

Available	Selected
proposal2	
proposal3	
Test1	

Here are the additional fields:

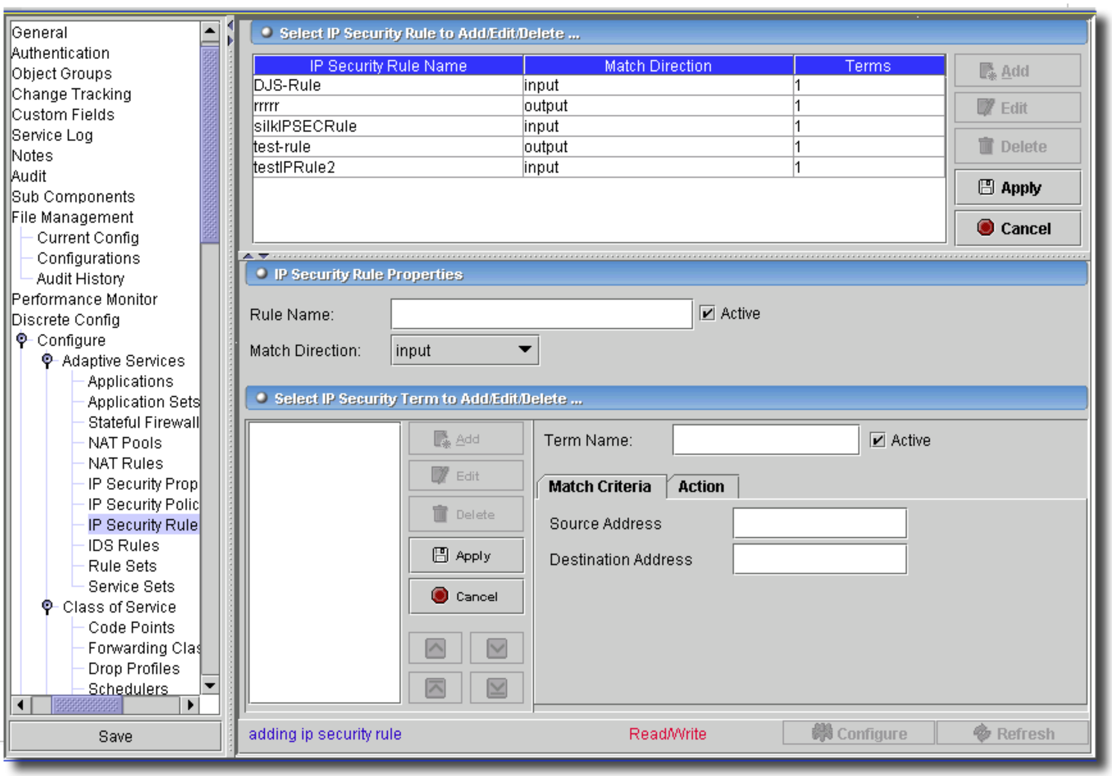
- **Perfect-Forward-Secrecy**—Select from the pick list. This provides additional security

- **Proposal**—Select from the *Available* list and move proposals to the *Selected* panel with the arrows. These originate with proposals created in IP Security–IP Sec Proposal on page 430. The up/down arrows determine in which order the application applies proposals.

IP Security Rules

This screen lets you configure IP Security rules.

Figure 13-14. IP Security Rules



IP Security Rule Name	Match Direction	Terms
DJS-Rule	input	1
rrrrr	output	1
silkIPSECRule	input	1
test-rule	output	1
testIPRule2	input	1

Rule Name: ☑ Active

Match Direction: input

Term Name: ☑ Active

Source Address

Destination Address

adding ip security rule

Read/Write

Click *Add* (or select an existing rule and click *Edit*) to open the rules editor. You can also click *Delete* to remove a selected rule at the top of this screen. Click *Export* to save a description of the listed items to a file. Once you have edited a rule, click *Apply* to accept your edits for the list, or click *Cancel* to abandon them. The editor has the following fields:

- **Rule Name**—An identifier for the stateful firewall ruleset.

- **Active**—Check this to activate the rule.

- **Match Direction**—*input/output*. These specify the side of the interface where the rule applies.

Editing / Creating an IP Security Term

The rule terms appear listed on the left. Use the *Add/Edit/Delete/Export* buttons in this portion of the screen to manage them. The editor for terms appears in the right panel. Configure the match criteria tab as in Match Criteria tab on page 425. In the *Action* tab, here are the fields you can configure:

- **Remote Gateway**—Enter the IP address of the remote gateway.
- **Syslog**—Check if you want to syslog information about the packet.
- **SA Configuration**—Select from *manual* or *dynamic*. If you select *manual* the lowest panel in the editor becomes active.
- **Clear - Do not** —Clear the do-not-fragment bit
- **IKE Policy**—Select from the pick list. See IKE Policy on page 432 for more about configuring the contents of that list.
- **No-Anti-Replay**—Disable the anti-replay check.
- **IPSec Policy**—Select from the pick list. See IP Sec Policy on page 433 for more about configuring the contents of that list.
- **Direction**—Select either *bidirectional* or *inbound-outbound*. If you select the latter, the *Outbound Parameters* tab in the lowest panel becomes active.

Inbound / Outbound Parameters

These tabs let you configure parameters for inbound and outbound traffic. You only need to configure one tab (labelled simply *Parameters*) if the direction selected is *bidirectional*. Here are the fields in these tabs:

- **Protocol**—Select from the pick list. Options include *ah* (authentication header), *esp* (encapsulated security payload), and *bundle* (a combination of *ah* and *esp*).
- **SPI—**Define the Security Parameter Index (256 - 16639)
- **Auxiliary SPI**—The ESP Security Parameter Index for IP Sec SA bundle.
- **Encryption**—Select the encryption algorithm from the pick list (*none, des-cbc,* and 3*dec-cbc*), and, if necessary its key in the field to the right of the pick list (check the right-hand checkbox if the key is in *Hexadecimal*)
- **Authentication**—Select the authentication algorithm from the pick list (*none, des-cbc,* and 3*dec-cbc*), and, if necessary its key in the field to the right of the pick list (check the right-hand checkbox if the key is in *Hexadecimal*)

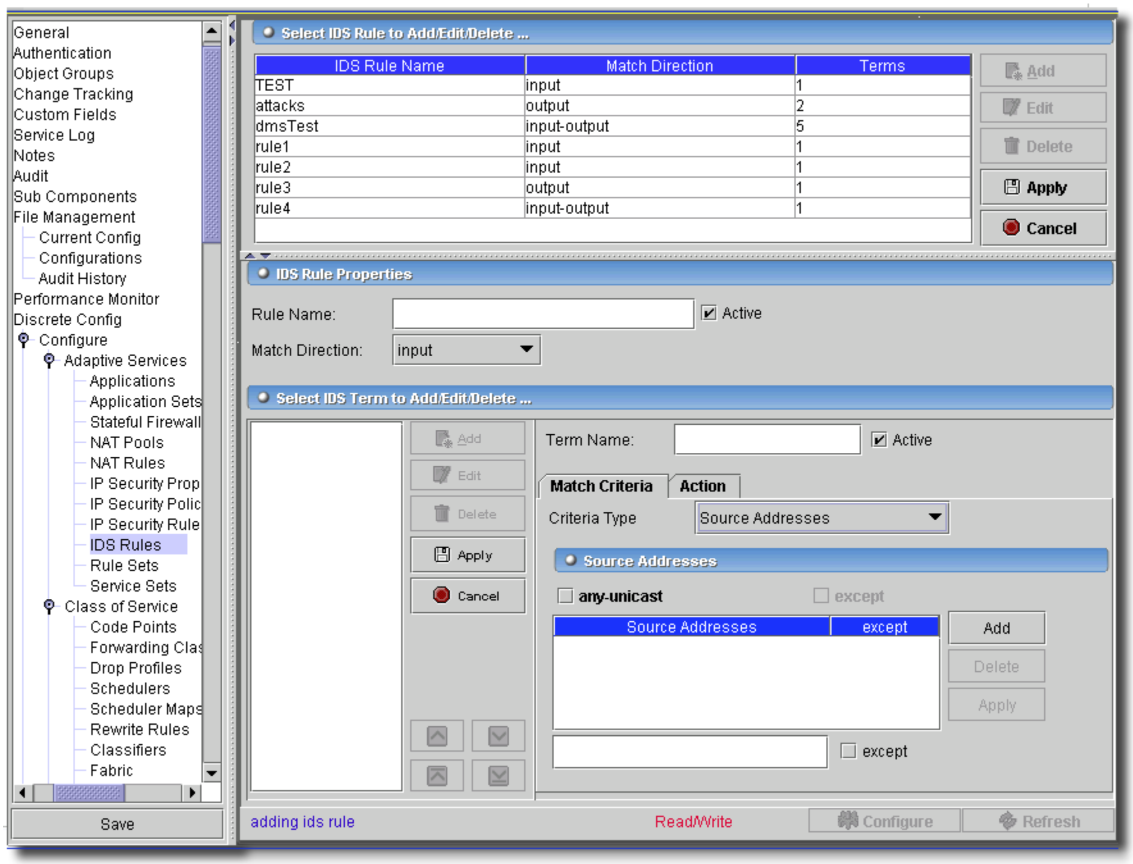
The *Configure* button at the bottom of the screen executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

IDS Rules

The Adaptive Services PIC (AS PIC) supports a limited set of intrusion detection services (IDS) to perform attack detection. It detects various types of denial of service (DoS) and directed denial of service (DDoS) attacks. It also detect attempts at network scanning and probing. Finally, it detects anomalies in traffic pattern, such as sudden bursts or decline in bandwidth. It redirects attack traffic to a collector for analysis.

This driver also supports IDS as a group operation. Consult the following for descriptions of fields in the group operations screen.

Figure 13-15. IDS Rules



IDS Rule Name	Match Direction	Terms
TEST	input	1
attacks	output	2
dmsTest	input-output	5
rule1	input	1
rule2	input	1
rule3	output	1
rule4	input-output	1

Rule Name: ☑ Active

Match Direction: input

Term Name: ☑ Active

Criteria Type: Source Addresses

☐ any-unicast ☐ except

Source Addresses	except

☐ except

adding ids rule

Read/Write

Click *Add* (or select an existing rule and click *Edit*) to open the rules editor. You can also click *Delete* to remove a selected rule at the top of this screen. Click *Export* to save a description of the listed items to a file. Once you have edited a rule, click *Apply* to accept your edits for the list, or click *Cancel* to abandon them. The editor has the following fields:

- **Rule Name**—An identifier for the stateful firewall ruleset.

- **Active**—Check this to activate the rule.

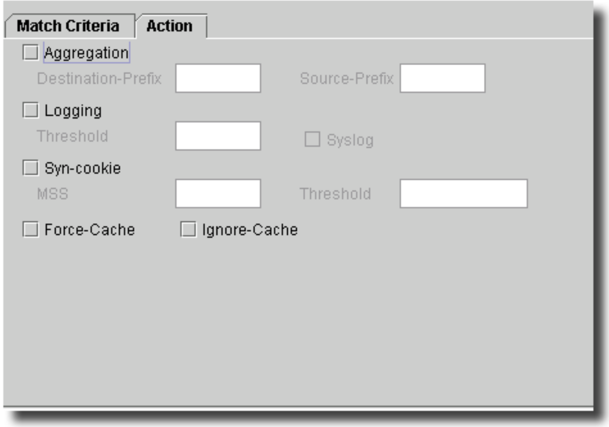
- **Match Direction**—*input/output*. These specify the side of the interface where the rule applies.

Editing / Creating an IDS Rule

The rule terms appear listed on the left. Use the *Add/Edit/Delete/Export* buttons in this portion of the screen to manage them. The editor for terms appears in the right panel. Configure the match criteria tab as in Match Criteria tab on page 425. In the *Action* tab, here are the fields you can configure:

The *Action* tab in the term editor.

Figure 13-16. IDS Rule Action Editor



Here are the fields you can alter:

- **Aggregation**—When checked, aggregates traffic labelled with a specific source or destination prefix before passing the event to IDS processing.

  Destination Prefix: 1-32— the prefix value for the destination IP aggregates.

  Source Prefix: 1-32— the prefix value for the source IP aggregates.

- **Logging**—When enabled (checked), this lets you set the number of events per second (in the *Threshold* field) that have to appear before logging occurs.

- **Syslog**—Makes syslogging occur when events are logged.

- **Syn-cookie**—When enabled, this allows Syn-cookie defensive mechanisms.

  MSS—Maximum Sequence Selection value used in TCP delayed binding. Range: 128-8192. Default: 1500

  Threshold—Syn-cookie defence, the number of SYN attacks per second.

- **Force-Cache**—Check to enable.

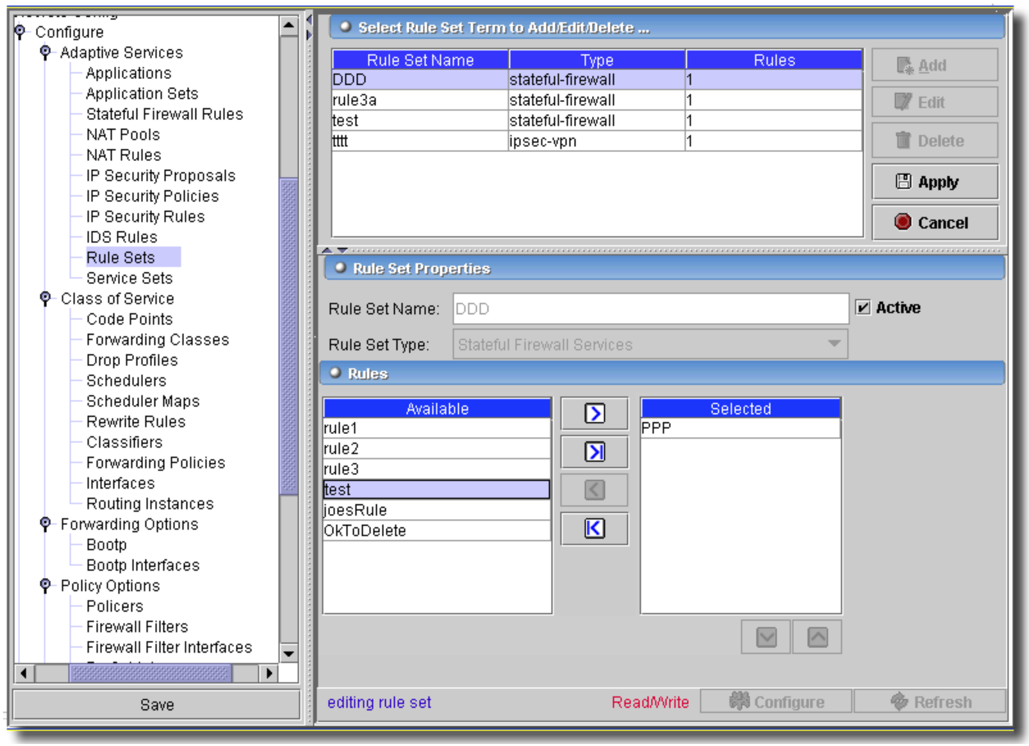
- **Ignore Cache**—Check to enable.

The *Configure* button at the bottom of the screen executes the desired configuration on the selected equipment. Click the *Refresh* button to re-query for these items.

Rule Sets

This screen lets you configure Adaptive Services rule sets.

Figure 13-17. Adaptive Services Rule Sets



Rule Set Name	Type	Rules
DDD	stateful-firewall	1
rule3a	stateful-firewall	1
test	stateful-firewall	1
tttt	ipsec-vpn	1

Rule Set Name: DDD ☑ Active

Rule Set Type: Stateful Firewall Services

Available	Selected
rule1	PPP
rule2	
rule3	
test	
joesRule	
OkToDelete	

editing rule set Read/Write

Click *Add* (or select an existing rule set and click *Edit*) to open the rules sets editor. You can also click *Delete* to remove a selected rule set at the top of this screen. Click *Export* to save a description of the listed items to a file. Once you have edited a rule set, click *Apply* to accept your edits for the list, or click *Cancel* to abandon them. The editor has the following fields:

- **Rule Set Name**—An identifier for the rule set.

- **Active**—Check this to activate the rule set.

- **Rule Set Type**—Select from the pick list. Options can include: *Network Address Translation, Intrusion Detection System, Stateful Firewall Services* and *IPSec VPN Service*.

Rules

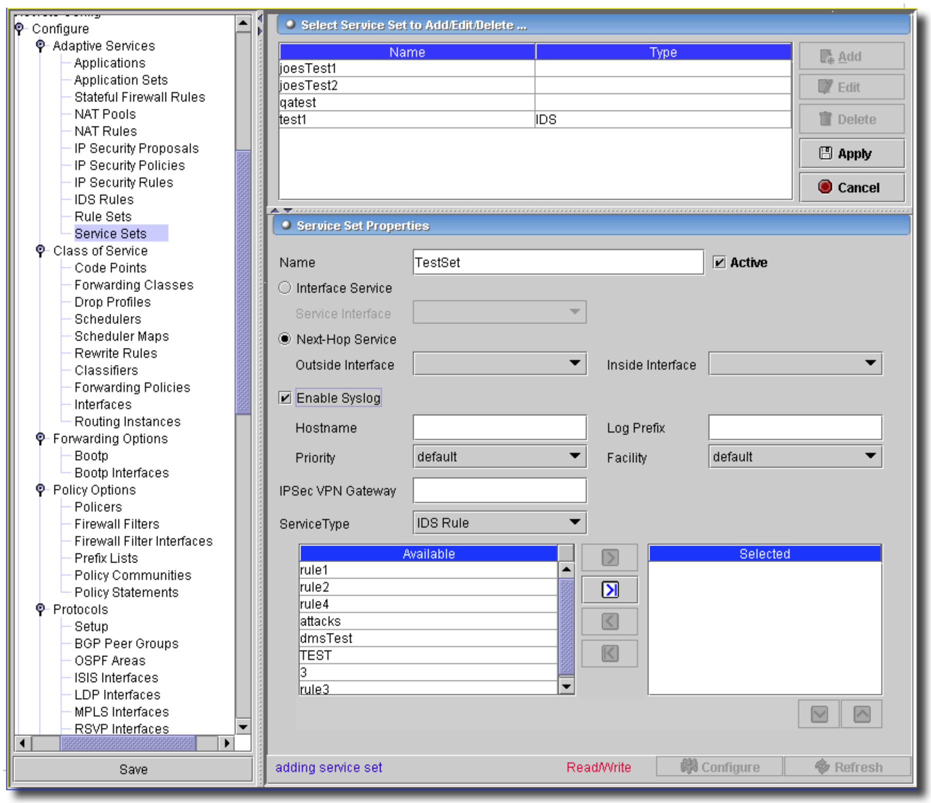
In the lowest panel, rules for the selected type appear in the *Available* panel. Use the left/right arrows to move the rules you want as part of a set to the *Selected* panel. The up/down arrows below this panel arrange the order to apply these rules.

The *Configure* button at the bottom of the screen executes the desired configuration on the selected equipment. Click the *Refresh* button to re-query for these items.

Service Sets

Once you specify all services (NAT, Stateful Firewall, and so on), you can assemble them as Service Sets.

Figure 13-18. Service Sets



Name	Type
joesTest1	
joesTest2	
qatest	
test1	IDS

Name: TestSet ☑ Active

○ Interface Service

Service Interface:

● Next-Hop Service

Outside Interface: Inside Interface:

☑ Enable Syslog

Hostname: Log Prefix:

Priority: default Facility: default

IPSec VPN Gateway:

ServiceType: IDS Rule

Available
rule1
rule2
rule4
attacks
dmsTest
TEST
3
rule3

Selected

adding service set ReadWrite

Click *Export* to save a description of the listed service sets. Use *Add*, *Edit*, and *Delete* to manage these service sets. Click *Export* to save a description of the listed items to a file. With the *Service Set* radio buttons, you can select from two types of service sets:

- **Interface service**—The service set retains the input-interface information even after services are applied, so that functions like filter-class forwarding that depend on input-interface information continue to work. You must specify a *Service Interface* if you select this option.
- **Next-Hop service**—The service set is a forwarding next hop. Useful when services need to apply to an entire VRF or when routing decisions determine that services need to occur. You must specify an *Outside Interface* and an *Inside Interface* if you select this option.

Syslog

Check the *Enable Syslog* box to activate this. Here, you can also configure system log messages generated for the service-set.

- **Hostname**—Name a target logging host.
- **Log Prefix**—The address prefix for all logging to the system log host.
- **Priority**—The level for system log messages (*alert*, and so on) and a Facility (authorization, and so on).
- **Facility**—Override the logging to a particular facility. Types: *authorization*, *daemon*, *ftp*, *kernel*, *user*, *local* 0 - *local* 9.

Service Set Information

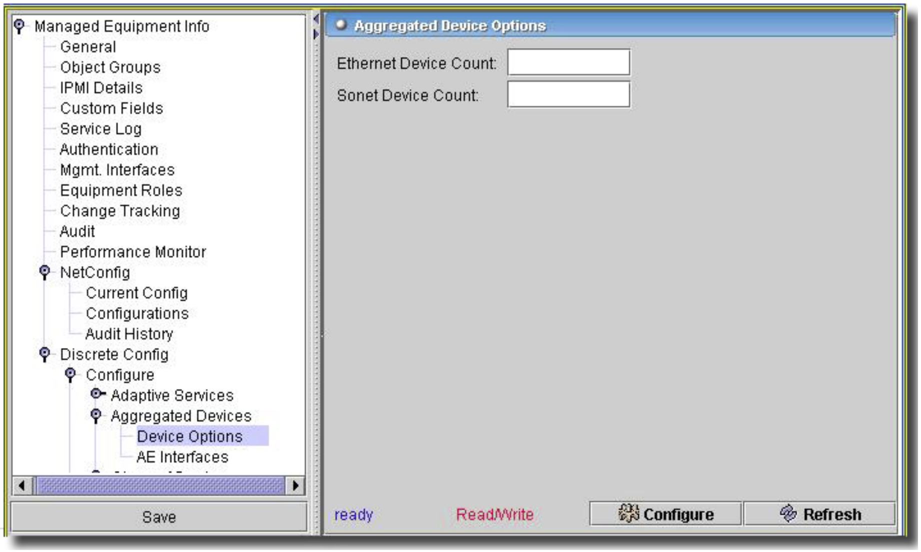
You can *Add* or *Remove* these with the button on the right. Select a *Type* (*IDS Rule*, *Stateful Firewall,* and so on), and further specify (*IDSRule2*, *FirewallRule1*, and so on), if necessary. This specifies the rules and rule sets that constitute the service set. See Unit Services on page 607 for more about services.

Click *Apply* to accept your edits, and *Cancel* to abandon them. The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Aggregated Devices -> Device Options

The IEEE 802.3ad standard defines link aggregation of Ethernet interfaces. The JUNOS implementation of 802.3AD balances traffic across the member links within an aggregated Ethernet bundle based on the Layer 3 information carried in the packet. This implementation uses the same load balancing algorithm used for per-packet load balancing The *Device Options* screen controls device options for Aggregated Devices.

Figure 13-19. Aggregated Devices -> Device Options



Aggregated Device Options

Ethernet Device Count:

Sonet Device Count:

This screen has the following fields:

- **Ethernet Device Count**—The number of ethernet devices aggregated.

- **Sonet Device Count**—The number of Sonet devices aggregated.

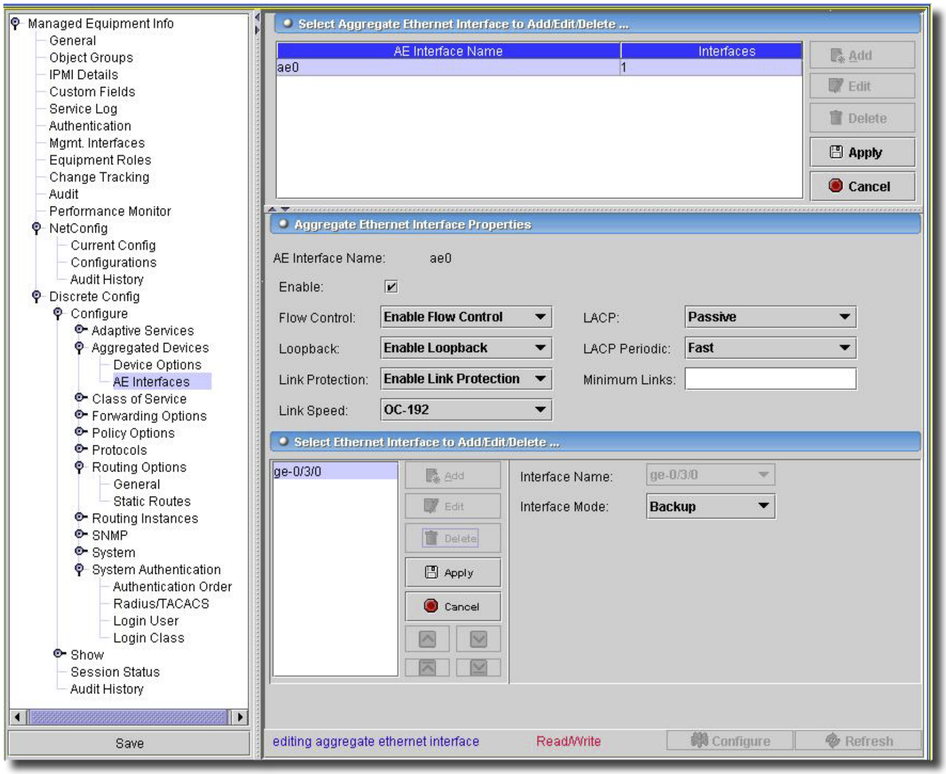
- The maximum number of aggregated devices you can configure is 128.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Aggregated Devices -> AE Interfaces

This screen manages the aggregate ethernet (AE) interfaces for aggregated devices.

Figure 13-20. Aggregated Devices -> AE Interfaces



Select Aggregate Ethernet Interface to Add/Edit/Delete ...

AE Interface Name	Interfaces
ae0	1

Aggregate Ethernet Interface Properties

AE Interface Name: ae0

Enable: ☑

Flow Control: Enable Flow Control

Loopback: Enable Loopback

Link Protection: Enable Link Protection

Link Speed: OC-192

LACP: Passive

LACP Periodic: Fast

Minimum Links:

Select Ethernet Interface to Add/Edit/Delete ...

ge-0/3/0

Interface Name: ge-0/3/0

Interface Mode: Backup

editing aggregate ethernet interface   Read/Write

You configure an aggregated Ethernet virtual link by specifying the link number as a physical device and then associating a set of ports that have the same speed and are in full-duplex mode. The physical interfaces can be either Fast Ethernet, Gigabit Ethernet, Gigabit Ethernet IQ, or 10-Gigabit Ethernet devices. Generally, you cannot use a combination of these interfaces within the same aggregated link; however, you can combine Gigabit Ethernet and Gigabit Ethernet IQ interfaces in a single aggregated Ethernet bundle.

On the aggregated bundle, no IQ-specific capabilities such as MAC accounting, VLAN rewrites, and VLAN queuing are available.

Click *Add* (or select an existing aggregate ethernet interface and click *Edit*) to open the editor. You can also click *Delete* to remove a selected interface at the top of this screen. Click *Export* to save a description of the listed items to a file. Once you have edited an interface, click *Apply* to accept your edits for the list, or click *Cancel* to abandon them. The editor has the following fields:

Aggregate Ethernet Interface Properties

- **AE Interface Name**—An identifier for the interface.

- **Enable**—Check this to activate the interface.

- **Flow Control**—By default, flow control regulates the amount of traffic sent out a Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interface. This is useful if the remote side of the connection is a Fast Ethernet or Gigabit Ethernet switch. You can disable flow control if you want the routing platform to permit unrestricted traffic.

- **Loopback**—By default, local aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces connect to a remote system, however you can enable loopback with the pick list here.

- **Link Protection**—Elect to *Enable* / *Disable* link protection.

- **Link Speed**—Select from the pick list. On aggregated Ethernet interfaces, you can set the required link speed for all interfaces included in the bundle. All interfaces that make up a bundle must be the same speed. For aggregated Ethernet links, you can specify speed in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).

  Aggregated SONET/SDH links can have one of the following speed values.

  - oc3—Links are OC-3c or STM-1c.
  - oc12—Links are OC-12c or STM-4c.
  - oc48—Links are OC-48c or STM-16c.
  - oc192—Links are OC-192c or STM-64c.

- **LACP**—Select from the pick list. The LACP mode can be *Active* or *Passive*. If the actor and partner are both in passive mode, they do not exchange LACP packets, which results in the aggregated Ethernet links not coming up. If either the actor or partner is active, they do exchange LACP packets. By default, LACP is in passive mode on aggregated Ethernet interfaces. To initiate transmission of LACP packets and response to LACP packets, you must enable LACP *Active* mode.

- **LACP Periodic**—By default, the actor and partner send LACP packets every second. You can configure the interval at which the interfaces send LACP packets in this field.

- **Minimum Links**—Enter the minimum number of links. On aggregated Ethernet interfaces, you can configure the minimum number of links that must be *up* for the bundle as a whole to be labeled *up*. By default, only one link must be up for the bundle to be labeled up.

Select Ethernet Interfaces to Add / Edit / Delete

In this portion of the screen *Add* / *Edit* / *Delete* as you do above, but for individual interfaces to aggregate. Change the order of aggregation by selecting a listed interface and clicking the up/down arrows. Aggregated interfaces are numbered from ae0 through ae127. The fields in the editor are these:

- **Interface name**—The name of the selected interface.

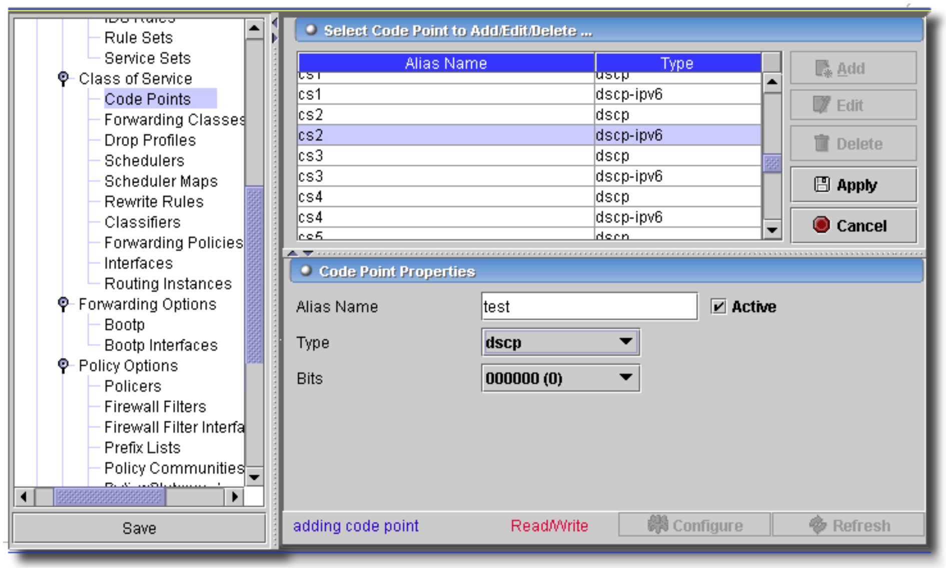
Interface mode—Select the mode (*Primary*, *Backup*) from the pick list.

Click *Apply* to accept your edits, and *Cancel* to abandon them. The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Class of Service -> Code Points

This panel displays the available code points defined on the device. It also lets you create new code points.

Figure 13-21. Code Points



Alias Name	Type
cs1	dscp
cs1	dscp-ipv6
cs2	dscp
cs2	dscp-ipv6
cs3	dscp
cs3	dscp-ipv6
cs4	dscp
cs4	dscp-ipv6
cs5	dscp

Alias Name: test ☑ Active

Type: dscp

Bits: 000000 (0)

adding code point Read/Write

Click *Add* to create a new code point, or select one from those listed and select *Edit*. Click *Delete* to delete selected code points. Click *Export* to save a description of the listed items to a file. Click *Apply* to accept your edits, or *Cancel* to abandon them. The *Code Point Properties* panel has the following fields:

Code Point Properties

- **Alias Name**—A code-point alias is a name you assign to a set of DiffServ code point and DSCP IPv6 bits. When you configure classes and define classifiers, you can refer to the code points by these alias names. You can configure user-defined classifiers in terms of alias names. If the value of an alias changes, it alters the behavior of any classifier that references that alias.

You use code-point aliases to do the following:

- Define an alias for bits that currently have no alias
- Define multiple aliases for the same bits
- Redefine an alias name to mean a different set of bits than the default

- **Type**—Code point type being created (Select from the pick list).

- **Bits**—Using the code-point alias means using these bits.

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

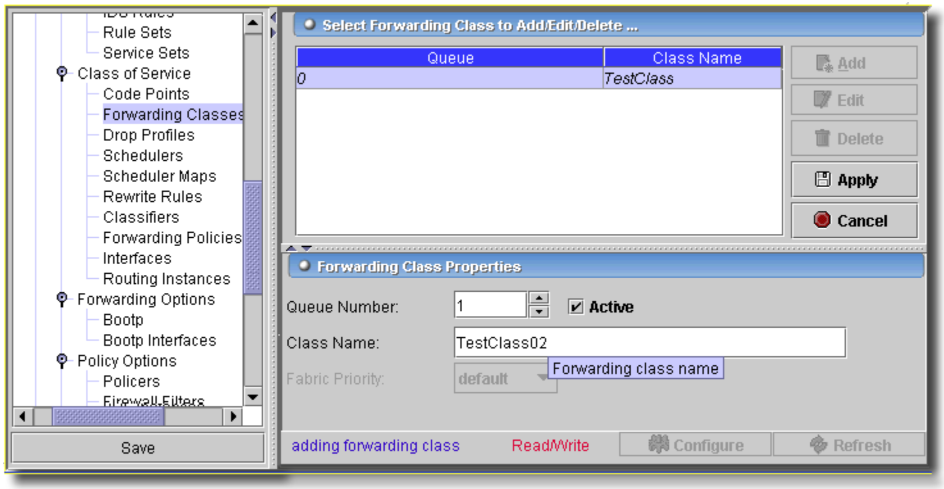
Class of Service -> Forwarding Classes

This Panel manages COS forwarding classes—also known as ordered aggregates in the IETF's DiffServ architecture. These affect the forwarding, scheduling, and marking policies applied to packets as they transit a router. Select a supported class from the pick list. The forwarding class plus the loss priority define the per-hop behavior.

The following rules govern queue assignment:

- If classifiers fail to classify a packet, the packet always receives the default classification to the class associated with queue 0.
- The number of queues is dependent on the hardware plugged into the chassis. CoS configurations are inherently contingent on the number of queues on the system. Only two classes, best-effort and network-control, are actually referenced in the default configuration. The default configuration works on any platform.
- CoS configurations that specify more queues than the platform can support are not accepted. The commit fails with a detailed message that states the total number of queues available.
- All default CoS configuration is based on queue number. The name of the forwarding class that shows up when the default configuration is displayed is the forwarding class currently associated with that queue.

Figure 13-22. COS Forwarding Classes Panel



Queue	Class Name
0	*TestClass*

Queue Number: 1 ☑ Active

Class Name: TestClass02

Fabric Priority: default

Forwarding class name

adding forwarding class Read/Write

Click *Add* to create a new property, or select one from those listed and select *Edit*. Click *Delete* to remove selected properties. Click *Export* to save a description of the listed items to a file. Click *Apply* to accept your edits, or *Cancel* to abandon them. The *Forwarding Class Properties* panel has the following fields:

Forwarding Class Properties

- **Queue Number**—0 - 3

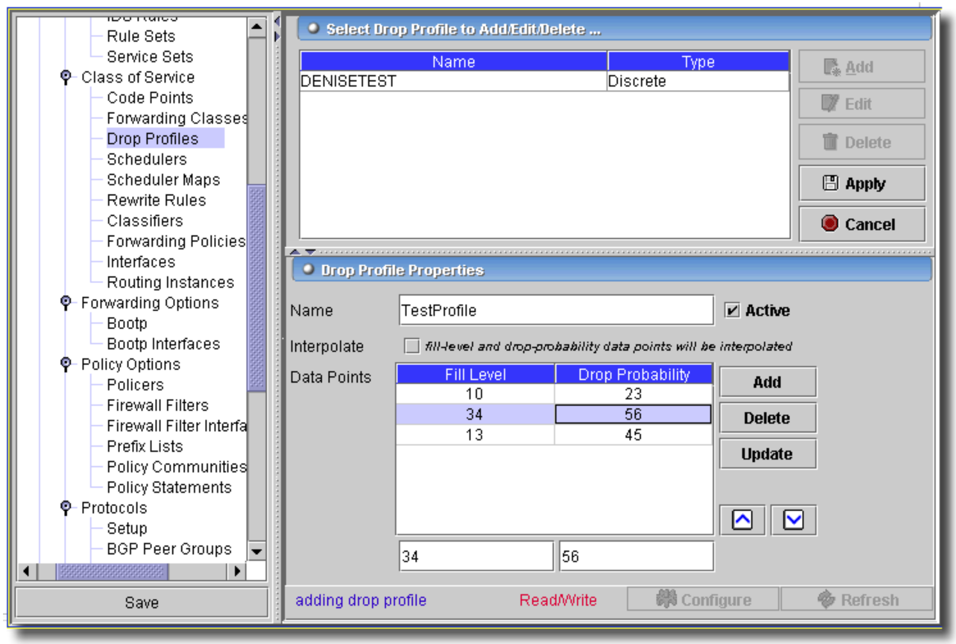
- **Class Name**—Each queue can have only one unique name.

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Class of Service -> Drop Profiles

This panel manages COS drop profiles. Dropped packets must match the drop profile. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet.

Figure 13-23. Drop Profiles



Name	Type
DENISETEST	Discrete

Name: TestProfile ☑ Active

Interpolate ☐ *fill-level and drop-probability data points will be interpolated*

Data Points

Fill Level	Drop Probability
10	23
34	56
13	45

34 56

adding drop profile Read/Write

Drop Profiles are associated with the forwarding classes and loss priorities from the scheduler-map you configured on the interface. (see Class of Service -> Scheduler Maps on page 449). In this configuration, you can select either the discrete or interpolated. If you do not check *Interpolate*, you, in effect, select *Discrete*. There, specify the fill-level and drop-probability percentage values. If you select *Interpolate*, you can configure each drop probability up to 64 *Fill-level/ Drop-probability* pairs, or a profile represented as a series of line segments

Click *Add* to create a new drop profile, or select one from those listed and select *Edit*. Click *Delete* to remove selected profile. Click *Export* to save a description of the listed items to a file. Click *Apply* to accept your edits, or *Cancel* to abandon them. The *Drop Profile Properties* panel has the following fields:

- **Name**—Up to 64 characters describing the Drop-Profile.
- **Interpolate**—(check box) When the drop-profile is interpolated, for *Fill-Levels* and *Drop-Probabilities*, you can specify 1-64 values ranging from 0-100. Multiple values are added/ removed by using the *Add/Delete* buttons for the *Fill-Level* and *Drop-Probabilities* lists.

Enter the following two fields below the table of pairs at the bottom of the screen. Click *Add* to enter your values, and *Update* to edit an existing pair. *Delete* removes the selected pair from the list. Note also that you can use the up/down arrows to the right of this table to re-order these pairs.

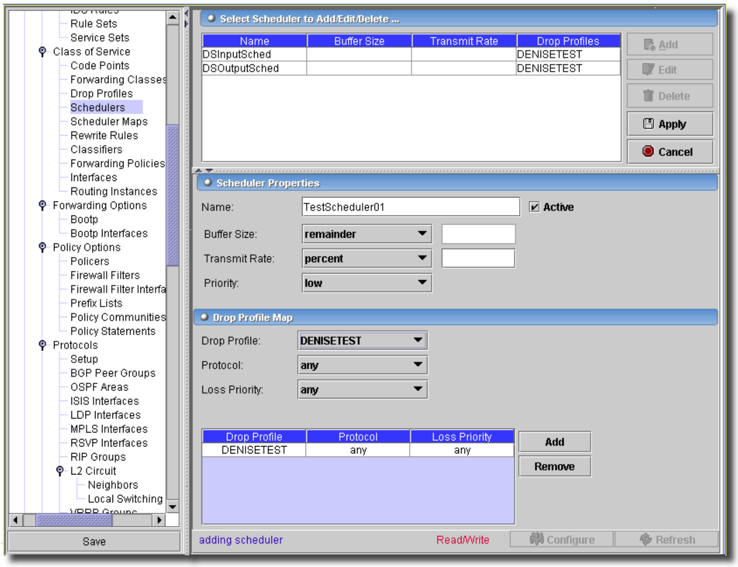
- **Fill-Level**—If the drop-profile is not interpolated then this value represents queue full percentage. For interpolated profiles, it represents the data points for queue full percentage.
- **Drop-Probability**—If the drop-profile is not interpolated then this value represents packet drop probability. For interpolated profiles it represents the data points for packet drop probability.

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Class of Service -> Schedulers

This manages the scheduler for COS to let you define the priority, bandwidth, delay buffer size, rate control status, and RED drop profiles to be applied to a particular forwarding class for packet transmission.

Figure 13-24. COS Scheduler Panel



Select Scheduler to Add/Edit/Delete ...

Name	Buffer Size	Transmit Rate	Drop Profiles
DSInputSched			DENISETEST
DSOutputSched			DENISETEST

Scheduler Properties

Name: TestScheduler01 ☑ Active

Buffer Size: remainder

Transmit Rate: percent

Priority: low

Drop Profile Map

Drop Profile: DENISETEST

Protocol: any

Loss Priority: any

Drop Profile	Protocol	Loss Priority
DENISETEST	any	any

Add

Remove

adding scheduler Read/Write

Use the *Add*, *Edit* and *Remove* buttons to manage rows here. Click *Apply* to accept your edits, or *Cancel* to abandon them. When you *Add* or *Edit* a selected schedule, the fields appearing in the lower panel are the following:

- **Name**—Any valid name up to 64 characters.

- **Transmit Rate**—0 to 100 percent.

- **Buffer Size**—Remainder (no value needed), percent (0-100) or temporal (1-200000)

- **Transmit Rate**—*rate* (1-32000000000), *percent* (0-100), *remainder* (no value needed) or *exact* (enforce the exact transmission rate). Under sustained congestion, a rate-controlled queue that goes into negative credit fills up and eventually drops packets.

- **Priority**—*Low, medium-high, medium-low, strict-high* or *high*.

- **Drop-Profile**—Drop profile defined in Drop-Profiles Screen. (See Class of Service -> Drop Profiles on page 446).

- **Protocol**—*any, non-tcp* or *tcp*.

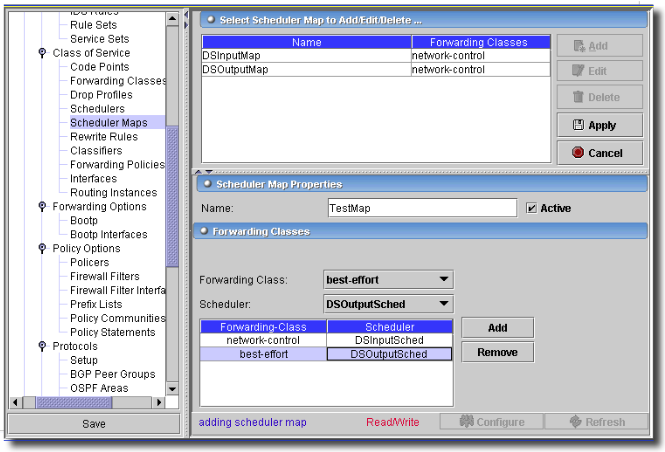
- **Loss Priority**—*any, low* or *high*.

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Class of Service -> Scheduler Maps

This screen manages scheduler maps for COS. This lets you associate the schedulers with forwarding classes and scheduler maps. You can then associate each scheduler map with an interface, thereby configuring the hardware queues, packet schedulers, and RED processes that operate according to this mapping.

Figure 13-25. COS Scheduler Map



Name	Forwarding Classes
DSInputMap	network-control
DSOutputMap	network-control

Name: TestMap ☑ Active

Forwarding Class: best-effort

Scheduler: DSOutputSched

Forwarding-Class	Scheduler
network-control	DSInputSched
best-effort	DSOutputSched

adding scheduler map Read/Write

Use the *Add*, *Edit* and *Remove* buttons to manage rows here. Click *Apply* to accept your edits, or *Cancel* to abandon them. When you *Add* or *Edit* a selected scheduler map, the fields appearing in the lower panel are the following:

Scheduler Map Properties

- **Name**—Any valid name up to 64 characters.

- **Forwarding Class**—A forwarding class defined in the *Forwarding Class* (see Class of Service -> Forwarding Classes on page 445).

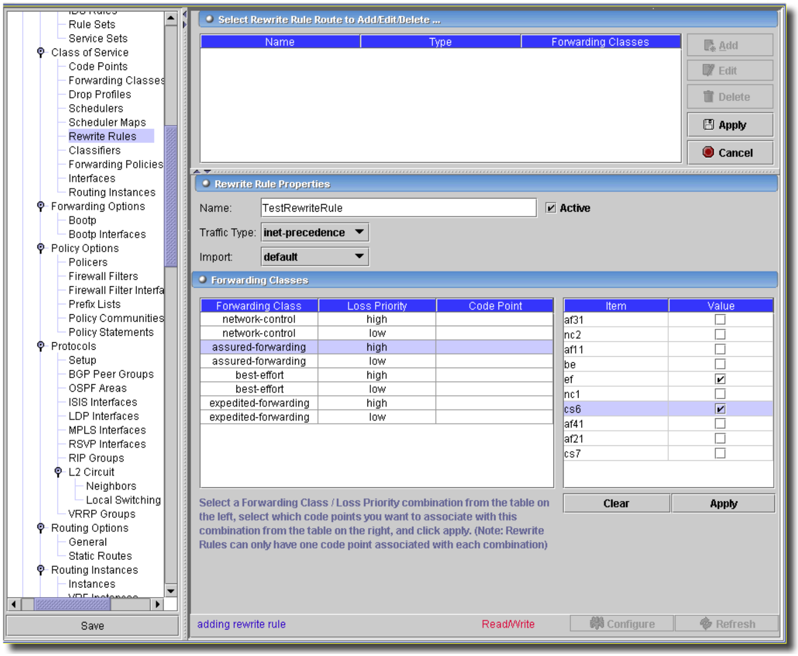
- **Schedule**—Defined Schedule in Scheduler panel (see Class of Service -> Schedulers on page 447).

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Class of Service -> Rewrite Rules

This screen manages COS rewrite rules. These let you redefine the code-point value of outgoing packets. Rewriting or marking outbound packets is useful when the router is at the border of a network and must alter the code points to meet the policies of the targeted peer.

Figure 13-26. COS Rewrite Rules Panel



Name	Type	Forwarding Classes

Name: TestRewriteRule ☑ Active

Traffic Type: inet-precedence

Import: default

Forwarding Class	Loss Priority	Code Point
network-control	high	
network-control	low	
assured-forwarding	high	
assured-forwarding	low	
best-effort	high	
best-effort	low	
expedited-forwarding	high	
expedited-forwarding	low	

Item	Value
af31	☐
nc2	☐
af11	☐
be	☐
ef	☑
nc1	☐
cs6	☑
af41	☐
af21	☐
cs7	☐

Select a Forwarding Class / Loss Priority combination from the table on the left, select which code points you want to associate with this combination from the table on the right, and click apply. (Note: Rewrite Rules can only have one code point associated with each combination)

adding rewrite rule   Read/Write

Use the *Add*, *Edit* and *Remove* buttons to manage rows in these tables. When you *Add* or *Edit* a selected rewrite rule, the lower panel lets you edit that rule's properties. Click *Apply* to accept your edits and make the rewrite rule part of the table in the upper part of the screen. Click *Cancel* to abandon your edits. The editor portion of the screen has the following fields:

Rewrite Rule Properties

Name—Any name length 64 characters or less.

Traffic Type—*dscp*, *exp*, *ieee-802.1*, *inet-precedence* or *dscp-ipv6*.

Forwarding Class

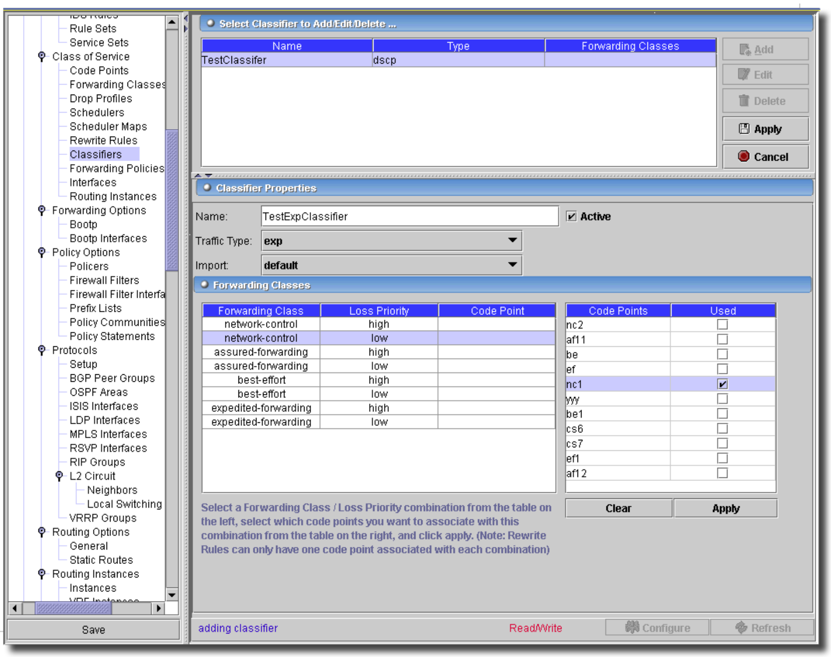
These classes are class defined in Class of Service -> Forwarding Classes on page 445. Select a class/ loss priority combination from those listed on the left, then check the matching code point (the list changes depending on the *Traffic Type* you select. Rewrite rules can have only one code point associated with each combination. Code points are defined and retrieved from the screen described in Class of Service -> Code Points on page 444.

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Class of Service -> Classifiers

These let you associate incoming packets with a forwarding class and loss priority and, based on the associated forwarding class, let you assign packets to output queues. This application supports behavior aggregate (BA) or code point traffic classifiers. Code points determine each packet's forwarding class and loss priority. BA classifiers let you set the forwarding class and loss priority of a packet based on DiffServ code point (DSCP) bits, IP precedence bits, MPLS EXP bits, and IEEE 802.1p bits. The default classifier is based on IP precedence bits.

Figure 13-27. COS Classifiers



Name	Type	Forwarding Classes
TestClassifer	dscp	

Name: TestExpClassifier ☑ Active

Traffic Type: exp

Import: default

Forwarding Class	Loss Priority	Code Point
network-control	high	
network-control	low	
assured-forwarding	high	
assured-forwarding	low	
best-effort	high	
best-effort	low	
expedited-forwarding	high	
expedited-forwarding	low	

Code Points	Used
nc2	☐
af11	☐
be	☐
ef	☐
nc1	☑
yyy	☐
be1	☐
cs6	☐
cs7	☐
ef1	☐
af12	☐

Select a Forwarding Class / Loss Priority combination from the table on the left, select which code points you want to associate with this combination from the table on the right, and click apply. (Note: Rewrite Rules can only have one code point associated with each combination)

adding classifier ReadWrite

Use the *Add*, *Edit* and *Remove* buttons to manage rows here. Click *Apply* to accept your edits, or *Cancel* to abandon them. When you *Add* or *Edit* a selected property, the fields appearing in the lower panel are the following:

Classifier Properties

- **Name**—Any name length 64 characters or less

- **Traffic Type**—*dscp*, *exp*, *ieee-802.1* or *inet-precedence*.

Forwarding Class

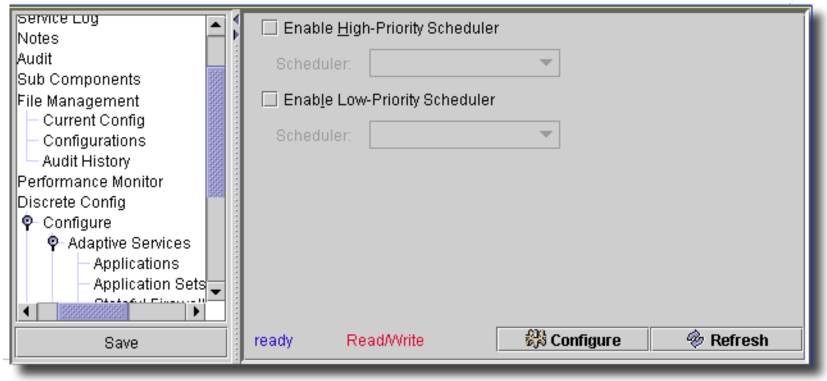
These classes are class defined in Class of Service -> Forwarding Classes on page 445. Select a class/ loss priority combination from those listed on the left, then check the matching code point (the list changes depending on the *Traffic Type* you select. Rewrite rules can have only one code point associated with each combination. Code points are defined and retrieved from the screen described in Class of Service -> Code Points on page 444.

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Class of Service -> Fabric

This screen manages Fabric settings for devices that support it.

Figure 13-28. Class of Service -> Fabric



☐ Enable High-Priority Scheduler

Scheduler:

☐ Enable Low-Priority Scheduler

Scheduler:

ready ReadWrite

On M320 and T-series platforms only, you can associate a scheduler with a class of traffic that has a specific priority while transiting the fabric. Traffic transiting the fabric can have two priority values: low or high. To associate a scheduler with a fabric priority, include the priority and scheduler statements at the [edit class-of-service fabric scheduler-map] hierarchy level.

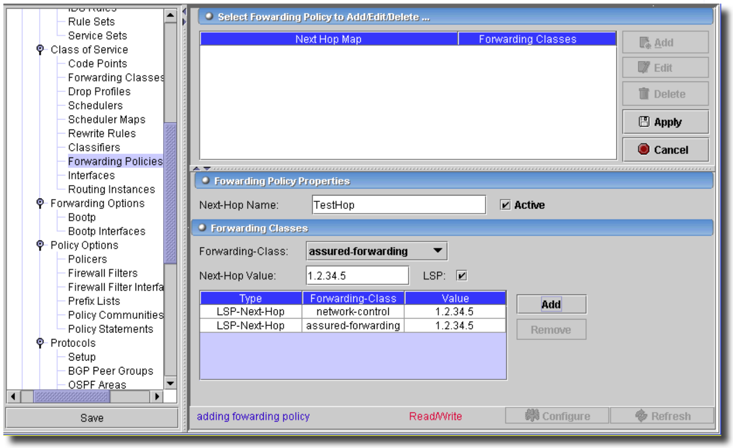
Click the checkbox to *Enable High-Priority Scheduler,* and select a scheduler from the drop down list. Select low priority schedulers similarly.

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Class of Service -> Forwarding Policies

This screen manages COS forwarding policies. These let you associate forwarding classes with next hops. Forwarding policies also let you create classification overrides, which assign forwarding classes to sets of prefixes.

Figure 13-29. COS Forwarding Policy Panel



Next Hop Map	Forwarding Classes

Next-Hop Name: TestHop ☑ Active

Forwarding-Class: assured-forwarding

Next-Hop Value: 1.2.34.5 LSP: ☑

Type	Forwarding-Class	Value
LSP-Next-Hop	network-control	1.2.34.5
LSP-Next-Hop	assured-forwarding	1.2.34.5

adding fowarding policy Read/Write

Use the *Add*, *Edit* and *Remove* buttons to manage rows in these tables. Click *Apply* to accept your edits, or *Cancel* to abandon them. The portion of the screen that appears when you click *Add* or *Edit* has the following fields:

Forwarding Policy Properties

- **Next-Hop Name**—Any name up to 64 characters.

Forwarding Classes

This area displays a table of *Forwarding Class* and *Next-Hope Value* fields. *Add* or *Remove* in this lower panel to enter or remove rows

- **ForwardingClass**—A class defined in Class of Service -> Forwarding Classes on page 445 (a drop down if a list is defined).
- **NextHop IP/Interface**—A valid interface name or IP.

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

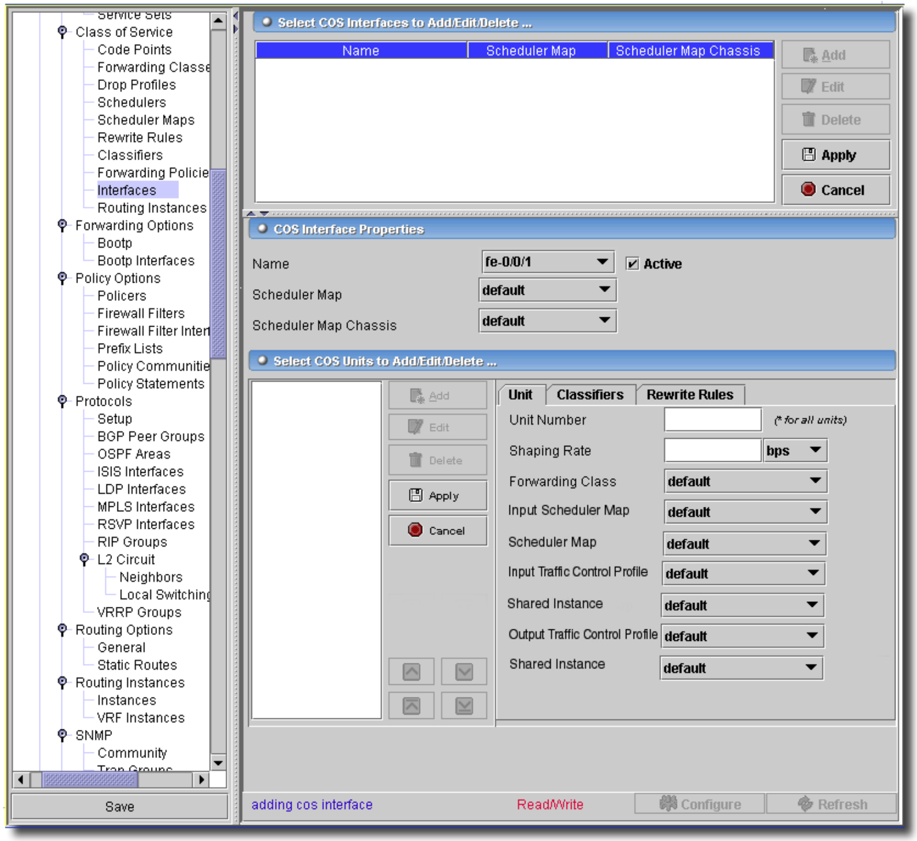
Class of Service -> Interfaces

This panel displays *Class-of-Service* (COS) settings for interfaces that currently have a COS configuration.

NOTE:

Class of Service functionality requires a license. Contact your sales representative for more information. use the Settings -> Permissions -> Register License menu item to open a dialog that lets you locate the license file. Select the file, and click Register License in the dialog, and you can use the licensed product.

Figure 13-30. Class of Service -> Interfaces



Name	Scheduler Map	Scheduler Map Chassis

Name: fe-0/0/1 ☑ Active

Scheduler Map: default

Scheduler Map Chassis: default

Unit Number: (* for all units)

Shaping Rate: bps

Forwarding Class: default

Input Scheduler Map: default

Scheduler Map: default

Input Traffic Control Profile: default

Shared Instance: default

Output Traffic Control Profile: default

Shared Instance: default

adding cos interface   Read/Write

The *Add* button lets you configure additional interfaces (click *Edit* to alter an existing, selected interface). Click *Apply* to add your edits to the list, or *Cancel* to abandon those edits. When you add or edit an interface, you can configure the following:

- **Name**—Interface name, wildcards accepted

- **Scheduler Map**—Scheduler map applied to this physical interface. This pick list comes from the configuration done in Class of Service -> Scheduler Maps on page 449.

- **Scheduler Map Chassis**—Scheduler map applied to chassis queues (separate scheduler-map will apply to queues on the pic)

Unit Tab

You can *Add*, *Edit* and *Remove* the items in the *COS Units* list to the lower left of this screen, as you can in the upper screen. Click *Apply* to add your edits to the list, or *Cancel* to abandon those edits. Here are *Unit* fields you can configure:

- **Unit Number**—Enter a wild card (* signifies all logical units for this interface), or a logical unit number.

- **Shaping rate** (6.4 & above)—Bandwidth rate for this interface (1000 - 32000000000 bits per second).

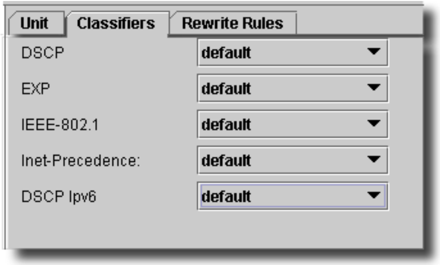
- **Forwarding class**—Select a forwarding class assigned to incoming packets from the pick list. These are defined and created in Class of Service -> Forwarding Classes on page 445.

- **Scheduler Map**—Select the scheduler map applied to this logical interface from the pick list. See Class of Service -> Scheduler Maps on page 449.

Classifiers Tab

This tab configures classifiers applied to incoming packets for the selected interface.

Figure 13-31. Class of Service -> Interfaces -> Classifiers Tab



DSCP: default
EXP: default
IEEE-802.1: default
Inet-Precedence: default
DSCP Ipv6: default

- Configure the following on this screen by selecting from the pick lists:

- **DSCP**—Differentiated Services code point (DSCP) classifier.

- **EXP**—EXP classifier.

- **IEEE-802.1**—IEEE-802.1 classifier.

- **Inet-Precedence**—IPv4 precedence classifier.

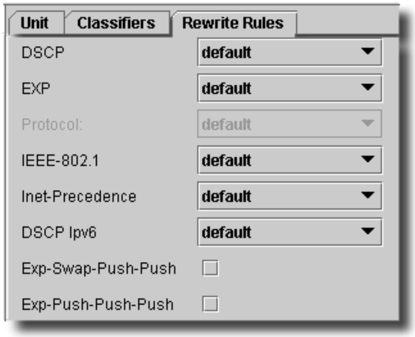
- **DSCP Ipv6**—Differentiated Services code point (DSCP) classifier IPv6 (Junos 6.3 & above).

This panel contains drop-down options defined and created in Class of Service -> Classifiers on page 451.

Rewrite Rules Tab

This tab configures Rewrite Rules applied to incoming packets for the selected interface.

Figure 13-32. Class of Service -> Interfaces -> Rewrite Rules Tab



DSCP default

EXP default

Protocol: default

IEEE-802.1 default

Inet-Precedence default

DSCP Ipv6 default

Exp-Swap-Push-Push □

Exp-Push-Push-Push □

Here, you can configure the following with pick lists, or checkboxes:

- **DSCP**—Differentiated Services code point (DSCP) rewrite rule.

- **EXP**—EXP rewrite rule.

- **Protocol**—Specify protocol matching criteria.

  mpls-any—Apply to MPLS packets, write MPLS header only.

  mpls-inet-both—Apply to IPv4 MPLS packets, write MPLS and IPv4 header.

  mpls-inet-both-non-vpn—Apply to IPv4 MPLS packets, write MPLS and IPv4 header for only non VPN traffic.

- **IEEE-802.1**—IEEE-802.1 rewrite rule.

- **Inet-Precedence**—IPv4 precedence rewrite rule.

- **DSCP Ipv6**—Differentiated Services code point rewrite rule IPv6 (Junos 6.3 & above).

- **Exp-Swap-Push-Push**—Check to copy incoming EXP into all swap-push-push labels.

- **Exp-Push-Push-Push**—Check to enable top-label EXP rewrite rule for push-push-push operation.

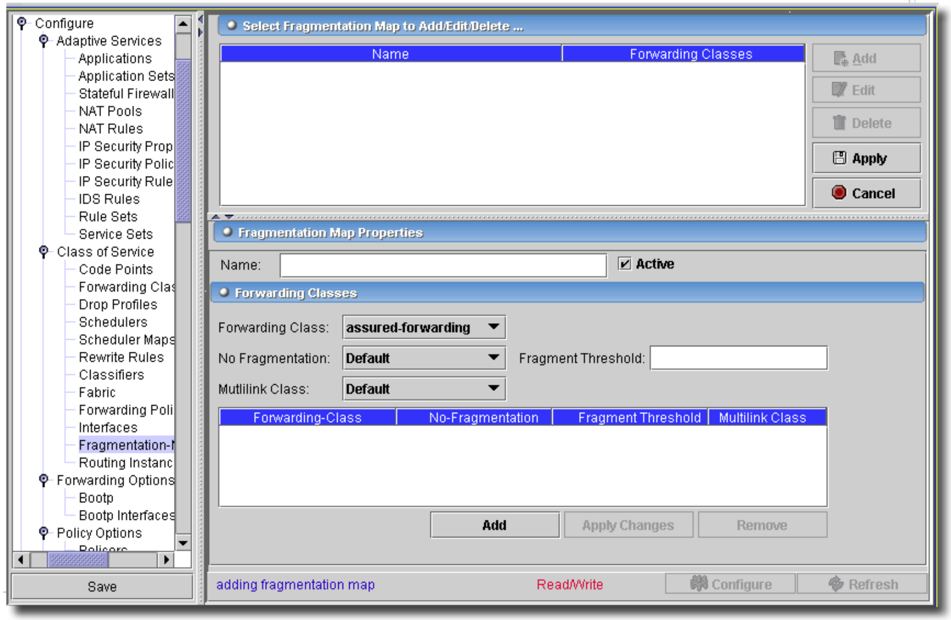
This panel contains drop-down options defined and created in Class of Service -> Rewrite Rules on page 449

The *Configure* button at the bottom of the screen sends the selected configuration to the device. The *Refresh* button queries the device and retrieves the active COS configuration for this unit.

Class of Service -> Fragmentation Map

This screen configures fragmentation maps for the selected device.

Figure 13-33. Class of Service -> Fragmentation Map



Name:

☑ Active

Forwarding Class: assured-forwarding

No Fragmentation: Default

Fragment Threshold:

Mutlilink Class: Default

adding fragmentation map

Read/Write

Use the *Add*, *Edit* and *Remove* buttons to manage rows here. Click *Apply* to accept your edits, or *Cancel* to abandon them. Click *Export* to save a file describing the listed items. When you *Add* or *Edit* a selected property, the fields appearing in the lower panel are the following:

Name—A unique identifier for the fragmentation map.

Active—Check to make this fragmentation map active.

Select the other options that you wish to apply to that forwarding class. Some of the options are mutually exclusive, so the form prevents selecting those. For example, if you enable *no fragmentation* for a forwarding class, you cannot set a fragment threshold or a multilink class. Click the *Add* button to add the Forwarding Class you have configured to the table.

After you add a forwarding class to the fragmentation map, you can also edit it by selecting it from either the *Fowarding Class* combo box or from the table, and then changing its properties. After you are done making the changes to the forwarding class, click *Apply Changes*. Select a listed row and click *Remove* to delete it.

Forwarding Class—Select the first forwarding class that you will be using (select one from the combo-box.

- **No Fragmentation**—When selected, this disables both Fragmentation Threshold and Multilink class. Enter a *Fragmentation Threshold*, when applicable.

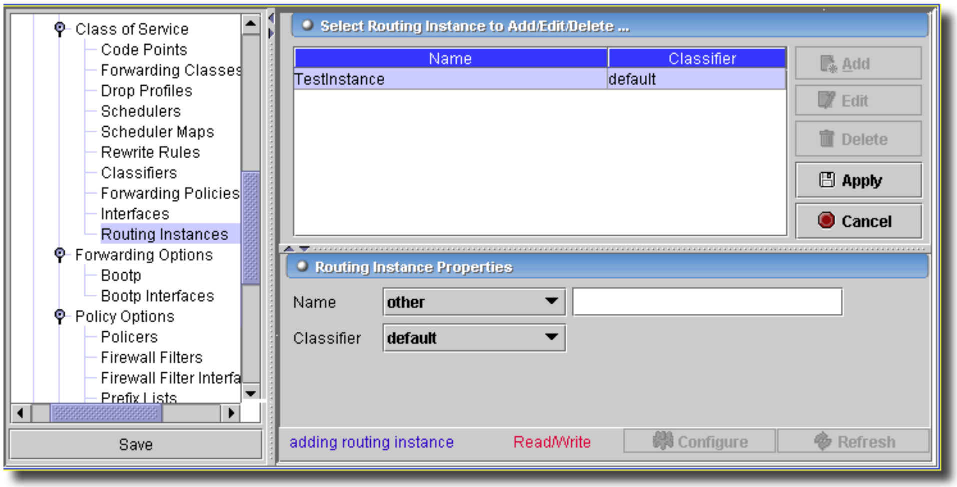
- **Multilink Class**—Select the class to accompany this fragmentation map.

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Class of Service -> Routing Instance

This configures a routing instance on the selected device, letting you associate EXP classifiers with routing-instances.

Figure 13-34. Class of Service -> Routing Instances



Name	Classifier
TestInstance	default

Name: other

Classifier: default

adding routing instance   Read/Write

NOTE:

Available only on routers with JunOS 7.3+

Use the *Add*, *Edit* and *Remove* buttons to manage rows in these tables. Click *Apply* to accept your edits, or *Cancel* to abandon them. The portion of the screen that appears when you *Add* or *Edit* lets you add or alter a Routing-Instance. This screen has the following fields:

- **Name**—You can either enter a name for the instance manually (select *other* from the drop down list, then enter the name in the text box that appears), or select the name of an existing routing-instance

CAUTION:

If you select an existing the routing-instance, it must already have a vrf-table-label configured.

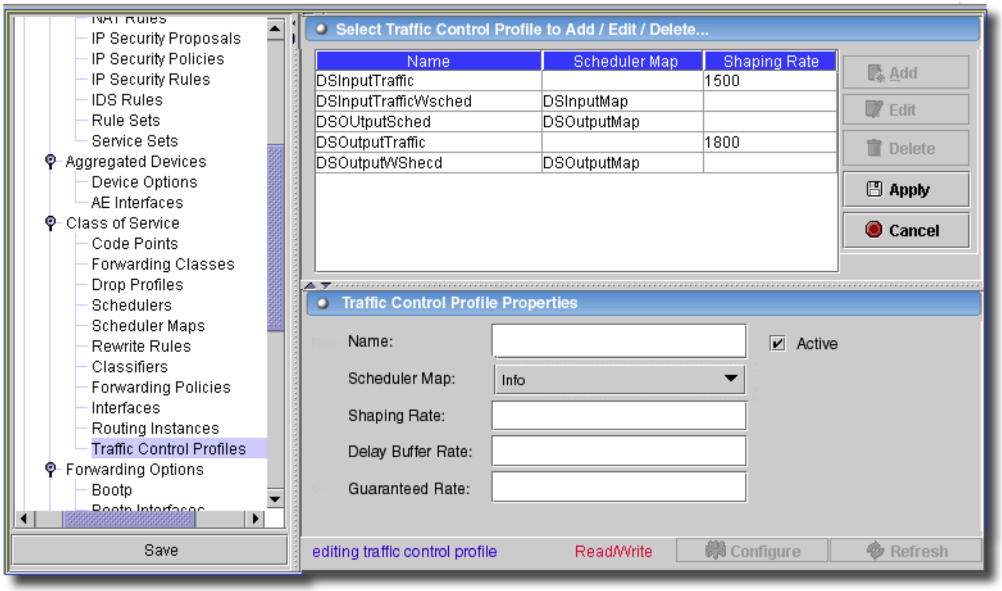
- **Classifier**—Select one of these from the pick list. Configurable user-defined EXP classifiers replace default classifiers. See Class of Service -> Classifiers on page 451 for more information about these.

The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Class of Service -> Traffic Control Profiles

Enter traffic control profiles for the selected device in this screen.

Figure 13-35. Class of Service -> Traffic Control Profiles



Name	Scheduler Map	Shaping Rate
DSInputTraffic		1500
DSInputTrafficWsched	DSInputMap	
DSOUtputSched	DSOutputMap	
DSOutputTraffic		1800
DSOutputWShecd	DSOutputMap	

Name:

☑ Active

Scheduler Map: Info

Shaping Rate:

Delay Buffer Rate:

Guaranteed Rate:

Use the *Add*, *Edit* and *Remove* buttons to manage rows here. Click *Export* to save a file describing the listed items. When you *Add* or *Edit* a selected property, the fields appearing in the lower panel are the following:

- **Name**—A unique identifier for the control profile.

- **Active**—Check to make this profile active.

- **Scheduler Map**—Select from the pick list. See Class of Service -> Scheduler Maps on page 449 for the source of this list.

- **Shaping Rate**—Enter a rate.

- **Delay Buffer Rate**—Enter a rate.

- **Guaranteed Rate**—Enter a rate.

NOTE:

This screen is only available for OS versions 7.6 and above.

Click *Apply* to accept your edits, or *Cancel* to abandon them. The *Configure* button executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Redundant Routing Engine (RE) Support

This driver offers Redundant Routing-Engine Support. For routers with redundant Routing Engines (RE), you can configure a master and backup RE. By default, the RE in slot RE0 is the master, and the RE in slot RE1 is the backup. The backup RE ill assume mastership once a loss signal is detected from the master. See Configure -> Redundancy on page 462 for more information.

Graceful Restart Engine Switchover allows the change from one RE to a fail over routing engine by keeping the forwarding data on both routing engines. This allows in-service software upgrades. You can also enable automatic synchronization of the two configurations.

Following Router Models support Redundant Routing-Engines: M10i, M20, M40

M160E, T320, T640. JunOS version 5.5 or greater supports redundancy.

Failover Sequence

The following describes the routing engine failover sequence:

1. After keepalive loss for a specified period, the driver logs a message.
2. After keepalive loss for a specified period seconds, the backup RE attempts to become master. Whenever the backup RE is active the application generates an alarm, and the display updates with the current status.
3. Once the backup RE becomes master, it continues to function as master even after the originally configured master RE has successfully resumed operation. You must manually restore it to its previous backup status. However, if at any time one of the REs is not present, the other RE becomes master automatically, regardless of how redundancy is configured.

The driver is listening for the following notification from the router:

```
1.3.6.1.4.1.2636.4.1.4
```

The jnxRedundancySwitchover defined in min JUNIPER-MIB.

When received, the driver attempts to determine which routing engine (RE) is the current master based on var bind content. The management interfaces are updated based on the configured IP address for that RE which would have been recorded in the database on the last resync.

You can view what the recorded IP is for each RE from the Routing Engine screen under Discrete Config in the redundancy view. (See Configuring Routing Engines on page 463.)

For this to work the router needs to be configured to send this application a v2 notification of the above mentioned OID. In testing, the following configuration under SNMP receives this notification:

```
trap-group redcell {
    version v2;
        categories {
            chassis;
    }
    targets {
        192.168.0.64;
            }
}
```

The groups section of the config attempts to find the configured IP addresses for the REs. There should be a section for each RE as shown in the example below:

```
groups {
    re0 {
        system {
            host-name morgan-re0;
        }
        interfaces {
                    fxp0 {
                        description "10/100 Management Interface";
                        unit 0 {
                            family inet {
                                address 10.255.10.103/24;
                                        }
                                }
                            }
                    }
        }
re1 {
    system {
        host-name morgan-re1;
            }
            interfaces {
                fxp0 {
                    description "10/100 Management Interface";
                    unit 0 {
                        family inet {
                            address 10.255.10.153/24;
                                    }
                            }
                        }
                    }
                }
            }
```

Updating IP Addresses on Routing Engines

The following property helps those who manage the router with a loopback address or port other than the management port and (for some reason) need to configure the IP on the routing engines (REs).

```
com.dorado.devicedriver.juniper.updatemanagement=true
```

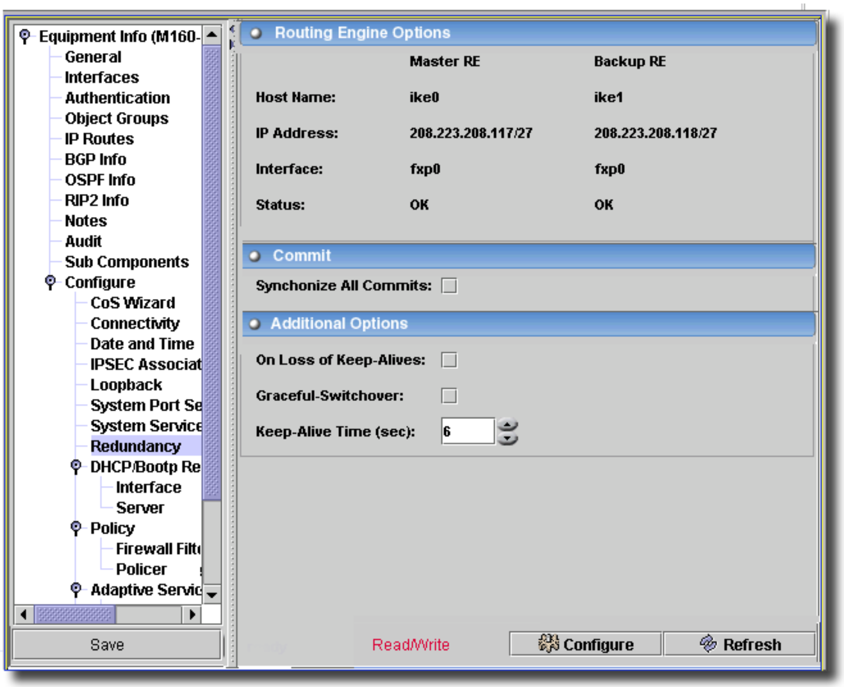
If set to true (the default), this always updates the management interfaces after a failover between REs. In some cases, you may not want to update these -- if you use loopback interfaces for routing purposes, for example.

Configure the IP on the REs when there are dual routing engines in the Groups section of the config with two groups with special names, re0 and re1. Which ever RE is the master is the config that is in play, at the time of the switchover the other is used.

Configure -> Redundancy

With this device driver, you can configure or view the master or backup RE.

Figure 13-36. Configuring Redundancy



Routing Engine Options

	Master RE	Backup RE
Host Name:	ike0	ike1
IP Address:	208.223.208.117/27	208.223.208.118/27
Interface:	fxp0	fxp0
Status:	OK	OK

Commit

Synchonize All Commits: □

Additional Options

On Loss of Keep-Alives: □

Graceful-Switchover: □

Keep-Alive Time (sec): 6

You can view current status of the REs. You can view the *Host Name*, *IP Address*, *Interface*, and *Status* for both REs.

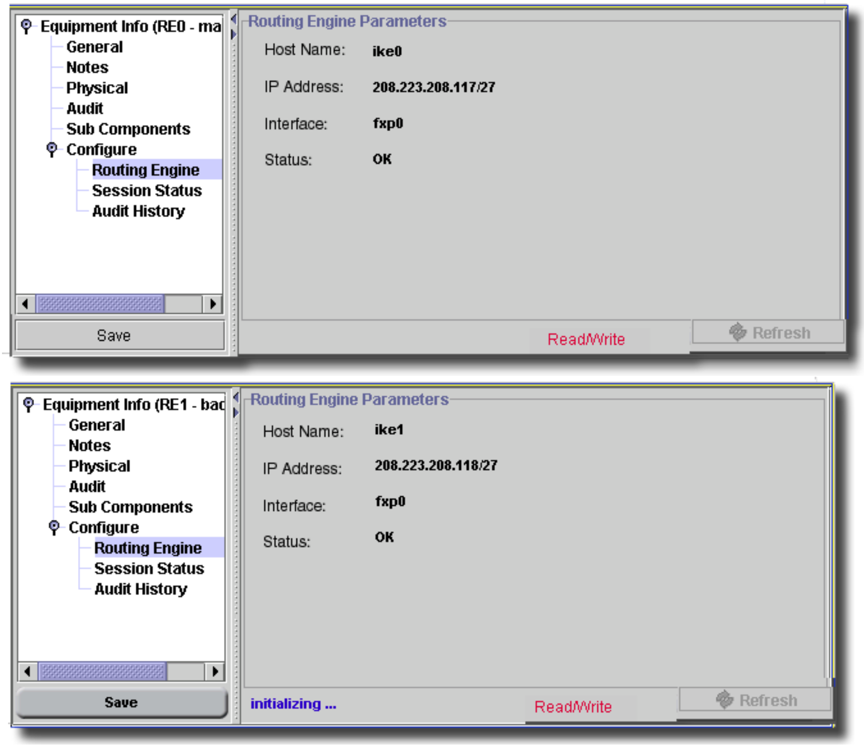
Configurable redundancy options include:

- **Synchronize All Commits**—Enables automatically committing synchronization between REs.
- **Keep Alive Time**—Seconds to wait before switching to backup.
- **On Loss of Keep-Alives**—When checked, enables switching when keep-alives are lost.
- **Graceful switchover**—Enables graceful switchover when failure occurs.

Configuring Routing Engines

You can also view current status of the REs.

Figure 13-37. Configuring Routing Engines



Host Name: ike0

IP Address: 208.223.208.117/27

Interface: fxp0

Status: OK

Host Name: ike1

IP Address: 208.223.208.118/27

Interface: fxp0

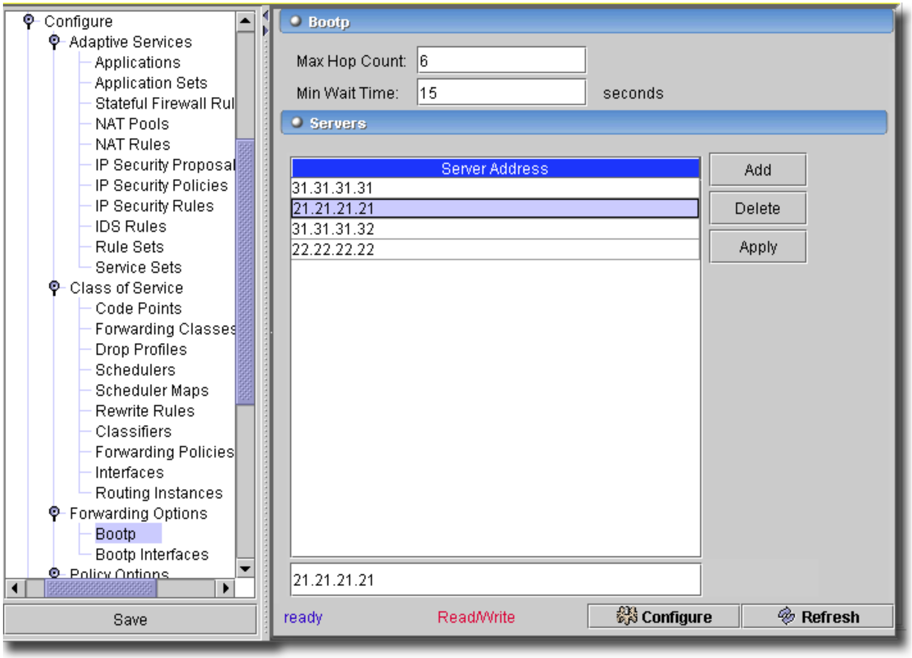
Status: OK

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Forwarding Options -> Bootp

This screen manages DHCP / Bootp Relay server settings.

Figure 13-38. DHCP / Bootp Relay Servers



Max Hop Count: 6

Min Wait Time: 15 seconds

Server Address
31.31.31.31
21.21.21.21
31.31.31.32
22.22.22.22

21.21.21.21

Use the *Add* or *Remove* buttons to manage rows in this table.

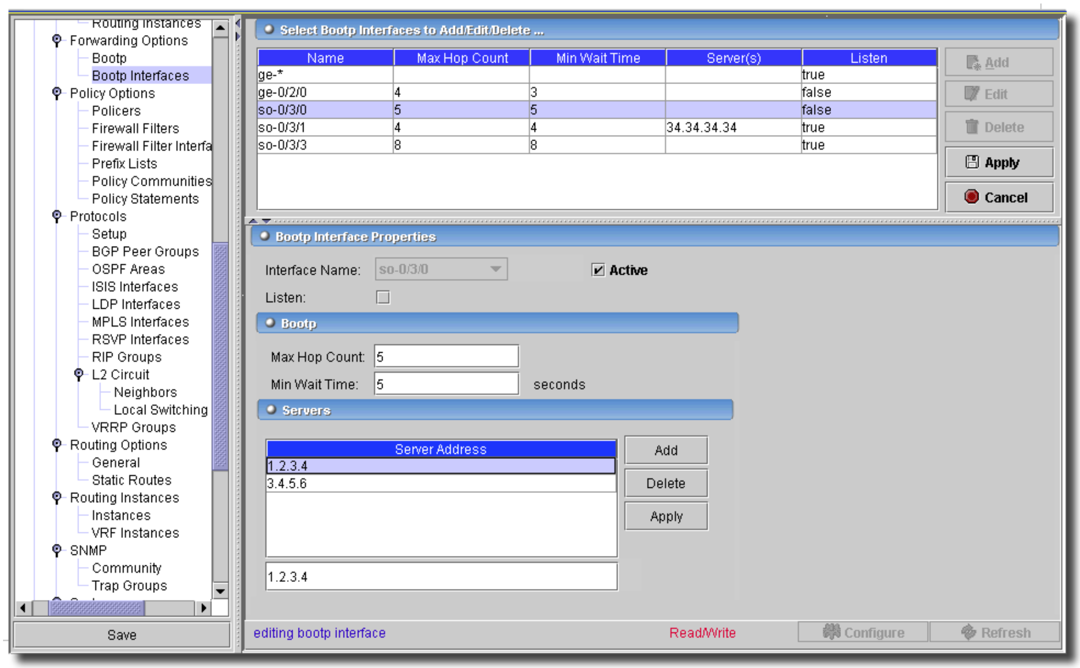
- **Max Hop Count**—The max hop count for the selected interface. Range: 1-16
- **Min Wait Time**—The minimum wait time. Range: 0 - 30000 seconds. (If you leave this blank, the equipment assumes the default remains unchanged.)
- **Servers**—This table lists IP addresses of DHCP / Bootp Relay servers. Enter an address, and click *Add* to list one in the table. Select one and click *Delete* to remove it from the list. Click *Apply* to accept your selections.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Forwarding Options -> Bootp Interfaces

This screen manages DHCP / Bootp Relay interface settings.

Figure 13-39. DHCP / Bootp Relay Interface



Select Bootp Interfaces to Add/Edit/Delete ...

Name	Max Hop Count	Min Wait Time	Server(s)	Listen
ge-*				true
ge-0/2/0	4	3		false
so-0/3/0	5	5		false
so-0/3/1	4	4	34.34.34.34	true
so-0/3/3	8	8		true

Bootp Interface Properties

Interface Name: so-0/3/0 ☑ Active

Listen: □

Bootp

Max Hop Count: 5

Min Wait Time: 5 seconds

Servers

Server Address
1.2.3.4
3.4.5.6

Add Delete Apply

1.2.3.4

editing bootp interface Read/Write

Use the *Add* or *Delete* buttons to manage rows in this table of interfaces. Click *Export* to save a description of the listed items to a file. Here are the columns you can edit within the rows here:

- **Interface Name**—The interface name. (Add / Remove)

- **Listen**—A checkbox to set whether this interface is listening.

- **Max Hop Count**—The max hop count for the selected interface. Range: 1-16

- **Min Wait Time**—The minimum wait time. Range: 0 - 30000 seconds. (If you leave this blank, the equipment assumes the default remains unchanged.)

- **Server(s)**—The IP Address(es) of servers associated with this interface. Click *Add* after you enter a server name in the lowest field. You can also select a listed server and click *Delete* to remove it from the list. Click *Apply* to confirm your selections.

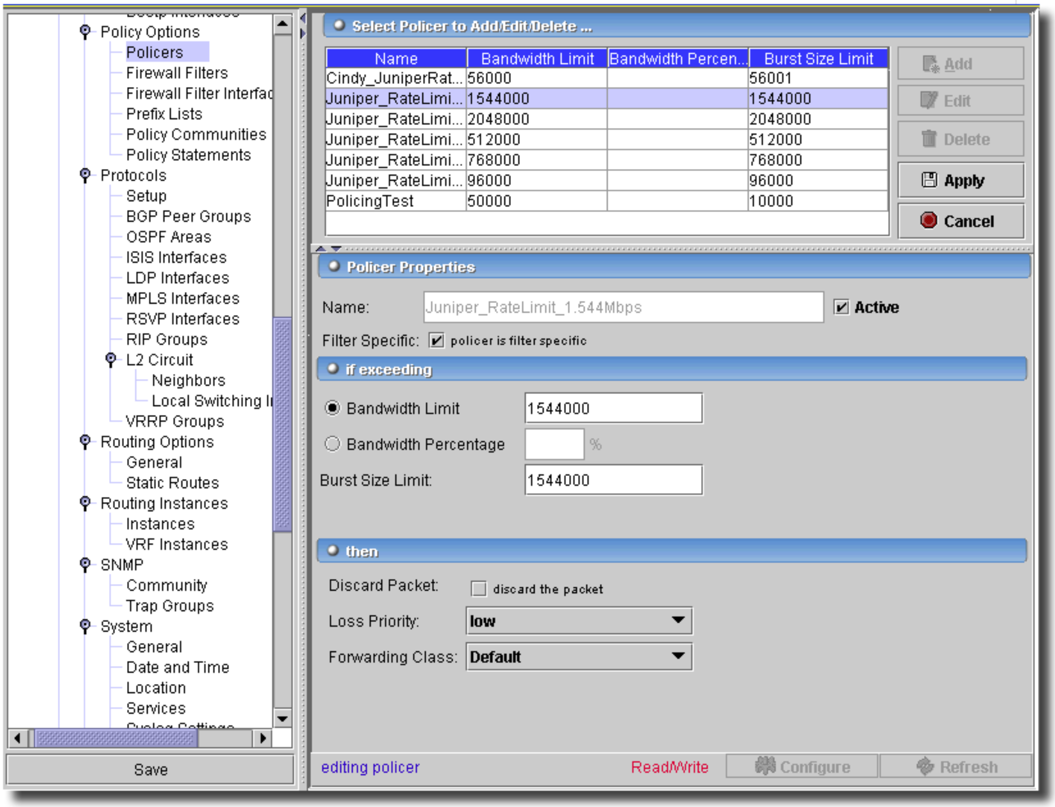
The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Policy Options -> Policers

Policing, or rate limiting, lets you limit the amount of traffic that passes into or out of an interface. It is an essential component of firewall filters that thwart denial-of-service (DoS) attacks. You can define specific classes of traffic on an interface and apply a set of rate limits to each. You can use a policer in one of two ways: as part of a filter configuration or as an individual policer statement that applies to each family on an interface. After you have defined and named a policer, the application stores it as a template. You can later use the same policer name to provide the same policer configuration each time you use it. This eliminates the need to define the same policer values more than once.

To make a policer, click the *Policer* node in Equipment Editor after you have selected the appropriate device. The subsequent screen lets you configure the policer:

Figure 13-40. Policer Manager



Select Policer to Add/Edit/Delete ...

Name	Bandwidth Limit	Bandwidth Percen...	Burst Size Limit
Cindy_JuniperRat...	56000		56001
Juniper_RateLimi...	1544000		1544000
Juniper_RateLimi...	2048000		2048000
Juniper_RateLimi...	512000		512000
Juniper_RateLimi...	768000		768000
Juniper_RateLimi...	96000		96000
PolicingTest	50000		10000

Policer Properties

Name: Juniper_RateLimit_1.544Mbps ☑ Active

Filter Specific: ☑ policer is filter specific

if exceeding

● Bandwidth Limit 1544000

○ Bandwidth Percentage %

Burst Size Limit: 1544000

then

Discard Packet: □ discard the packet

Loss Priority: low

Forwarding Class: Default

editing policer ReadWrite

Click *Export* to save a description of the listed items. Click *Add* or select an existing Policer and click *Edit*. The *Policer Properties* and *Policer Actions* portions of the screen let you set policies and actions for this policer. Here are the fields that appear:

Policer Properties

- **Name**—A unique identifier for the Policer
- **Bandwidth-Limit**—The average number of bits per second permitted. Units can be bits, kilobits (kbps) megabits (mbps) or gigabits (gbps).
- **Bandwidth-Rate**—Rate-limit based upon port speed. You must specify the percentage as a complete decimal number between 1 and 100.
- **Burst-Rate-Limit**—The maximum size permitted for bursts of data that exceed the given bandwidth limit. Units can be bits, kilobits (kbps) megabits (mbps) or gigabits (gbps).
- **Filter-Specific**—Lets you configure policers and counters for a specific filter name.

Policer Actions

- **Discard**—Discards a packet that exceeds the rate limits.
- **Loss-Priority**—Sets the loss priority level to low or high.
- **Forwarding-Class**—Specifies the forwarding class to any class name already configured for the forwarding class.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

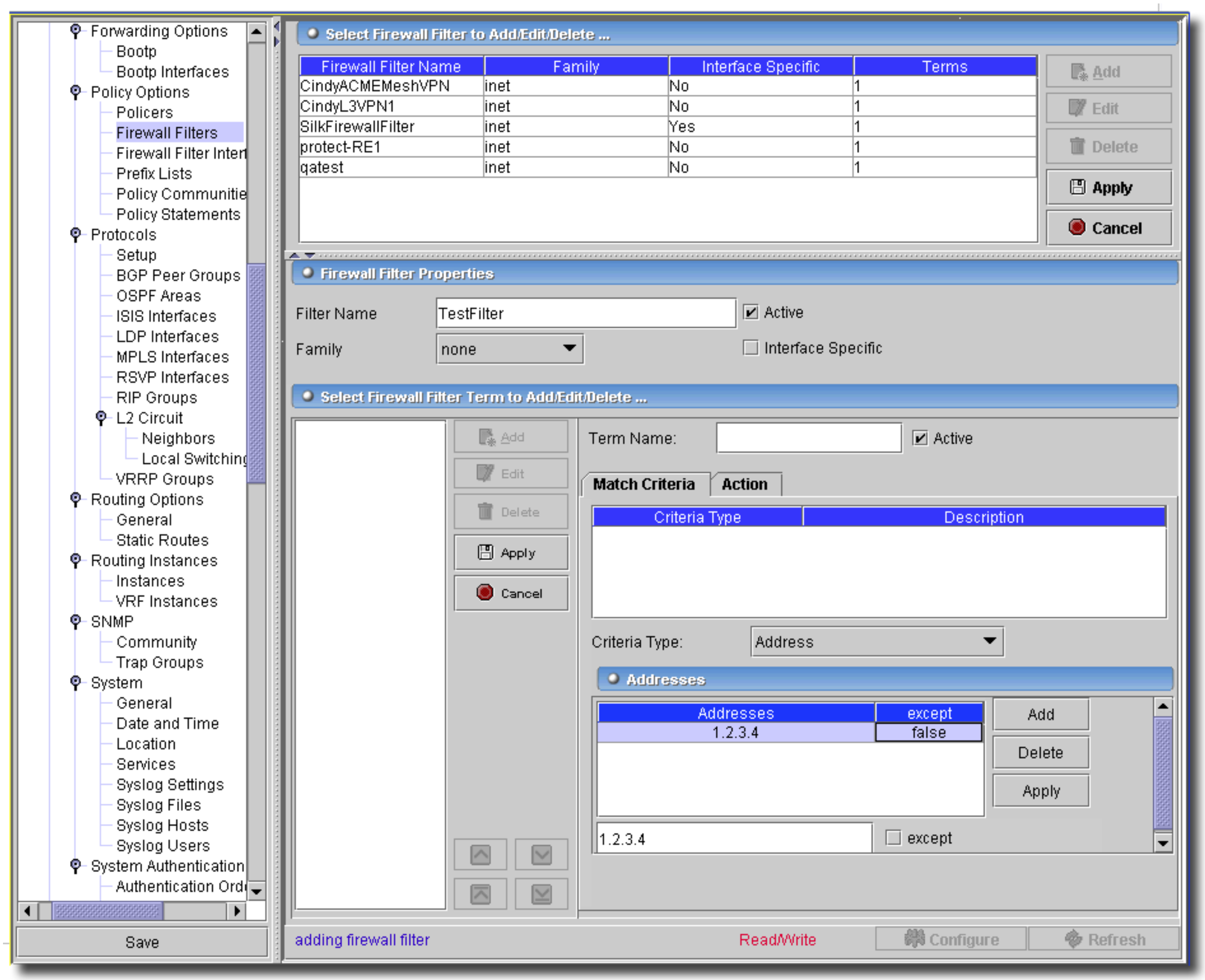
Policy Options -> Firewall Filters

irewall Filter Policies control traffic at the interface level. Firewall filters let you filter packets based on their components and act on packets that match the filter.

These filters can restrict the local packets that pass from the router's physical interfaces to the Routing Engine. Input filters affect only inbound traffic destined for the Routing Engine, and output filters affect only outbound traffic sent from the Routing Engine. Policing, or rate limiting provides a finer level of control over local packets destined for the Routing Engine. (See Policy Options -> Policers on page 467.)

For each interface, you can apply a firewall filter to incoming or outgoing traffic, or both, and can use the same filter for both. Type of traffic supported includes IPv4 and MPLS.

Figure 13-41. Policy Options -> Firewall Filters



Firewall Filter Name	Family	Interface Specific	Terms
CindyACMEMeshVPN	inet	No	1
CindyL3VPN1	inet	No	1
SilkFirewallFilter	inet	Yes	1
protect-RE1	inet	No	1
qatest	inet	No	1

Filter Name: TestFilter ☑ Active

Family: none □ Interface Specific

Term Name: ☑ Active

Criteria Type	Description

Criteria Type: Address

Addresses	except
1.2.3.4	false

1.2.3.4 □ except

adding firewall filter

Read/Write

This screen filters traffic according to Match condition(s) which can include addresses, ports and other criteria. It can also apply various administrative functions to the Firewall Policy like policers, accounting filters and logging. Click *Export* to save a description of the listed items to a file. Click *Add* (or select an existing rule and click *Edit*) to open the rules editor. You can also click *Delete* to remove a selected rule at the top of this screen. Click *Export* to save a description of the listed items to a file. Once you have edited a rule, click *Apply* to accept your edits for the list, or click *Cancel* to abandon them. The editor has the following fields:

- **Filter Name**—An identifier for the stateful firewall ruleset.

- **Family**—For future functionality.

- **Active**—Check this to activate the rule.

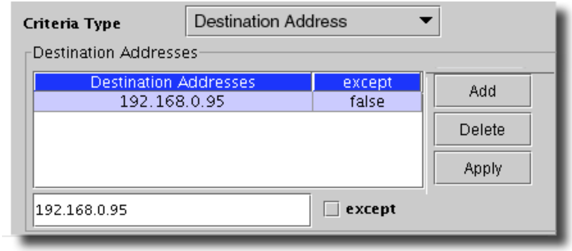
- **Interface Specific**—Check to make this filter specific to an interface.

Match Criteria Tab

You can specify multiple match conditions in a filter, effectively chaining together a series of match action operations to apply to the packets on an interface. If multiple match conditions exist you can also select and reorder them (indicating the order they apply) using the *Up* and *Down* buttons.

Select the *Advanced Type*, enter the fields for that type and then click *Add* to add the criteria. Select a criteria and select *Delete* to remove it from the match-condition.

Figure 13-42. Advanced Firewall Filter Match Conditions



Criteria Type: Destination Address

Destination Addresses

Destination Addresses	except
192.168.0.95	false

192.168.0.95 □ except

Address filter conditions match prefix values in a packet. Types include the following:

- **Source / Destination / Address**—If you select one of the *Address* terms (*Source*, *Destination* or blank, which means *Either*), the editor panel lets you enter IP addresses for source or destination. Click *Add* to add the address you type in the field below the list. Check *Except* if you want to exclude this address from the criteria.
- **Single prefix**—Either source-address, destination-address or both where the format can be 192.168.0.1 or 192.168.1.0/24.

Multiple prefix—A set of source-addresses, destination-addresses or both.

- **Source / Destination / Prefix-lists**—These define a list of IP address prefixes under a prefix-list alias for frequent reference. Select *SecondVPN*, or *ThirdVPN* from the pick list.
- **Source / Destination / Port**—Select from the pick list. Options include *afs*, *bgp*, *biff*, *bootpc*, *bootps*, *cmd*, *cvspserver*, *dhcp*, *domain*, *eklogin*, *ekshell*, *exec*, *finger*, *ftp*, *ftp-data*, *http*, *https*, *ident*, *imap*, *kerberos-sec*, *klogin*, *kpasswd*, *krb-prop*, *krbupdate*, *kshell*, *ldap*, *ldp*, *login*, *mobileip-agent*, *mobileip-mn*, *msdp*, *nebios-dgm*, *netbios-ns*, *netbios-ssn*, *nfsd*, *nntp*, *ntalk*, *ntp*, *pop3*, *pptp*, *printer*, *radacct*, *radius*, *rip*, *rkinit*, *smtp*, *snmp*, *snmptrapp*, *snpp*, *socks*, *ssh*, *sunrpc*, *syslog*, *tacacs*, *talk*, *telnet*, *ttfp*, *timed*, *who*, *xdmcp*.
- **IP options**—These include *any*, *loose-source-route*, *route-record*, *route-alert*, *security*, *stream-id*, *strict-source-route*, *timestamp*.
- **Ah Spi**—Enter a value under the table and click *Add*.
- **Esp Spi**—Enter a value under the table and click *Add*.
- **DSCP**—Select a value from the pick list and click *Add*. Values include *af11 - af43*, *be*, *cs1 - cs7*, *ef*.

- **Fragment Offset**—Enter a value under the table and click *Add*.

- **Icmp code**—Select a value from the pick list and click *Add*. Values include *communication-prohibited-by-filter, destination-host-prohibited, destination-host-unknown, destination-network-prohibited, destination-.network-unknown, host-precedence violation, host-unreachable, host-unreachable-for-tos, ip-header-bad, network-unreachable, network-unreachable-for-tos, port-unreachable, precedence-cutoff-in-effect, protocol unreachable, redirect-for-host, redirect-for-network, redirect-for-tos-and-host, redirect-for-tos-and-net, required-option-missing, source-host-isolated, source-route-failed, tti-eq-zero-during-reassembly, tti-eq-zero-during-transit.*

- **Icmp type**—Select a value from the pick list and click *Add*. Values include *echo-reply, echo-request, info-reply, info-request, mask-request, mask-reply, parameter-problem, redirect, router-advertisement, router-solicit, source-quench, time-exceeded, timestamp, timestamp-reply, unreachable.*

- **Packet length**—Enter a value under the table and click *Add*.

- **Precedence**—Select a value from the pick list and click *Add*. Values include *critical-ecp, flash, flash-override, immediate, internet-control, net-control, priority, routine.*

- **Protocol**—Select a value from the pick list and click *Add*. Values include *ah, dstopts, egp, esp, fragment, gre, hop-by-hop, icmp, icmpv6, igmp, ipip, ipv6, no-next-header, ospf, pim, routing, rsvp, sctp, tcp, udp, vrrp.*

- **Forwarding-class**—Select a value in the pick list under the table and click *Add*. See Class of Service -> Forwarding Classes on page 445 for the origin of this list.

- **Except**—When checked, means “Match anything but this criterion.”

- **TCP Flag**—Bit-field filter conditions match packet fields if particular bits in those fields are or are not set. You can match the IP options, TCP flags, and IP fragmentation fields. For bit-field filter match conditions, you specify a keyword that identifies the field and tests to determine that the option is present in the field. See the table Bit-Field Firewall Filter Match Conditions on page 472

  NOTE:

  NOTE: This software does not automatically check the first fragment bit when matching TCP flags.

  To specify the bit-field value to match, enter it in the *TCP Flags* field. For example, a match occurs if the RST bit in the TCP flags field is set: `rst`

  Generally, specify the bits being tested using keywords. Bit-field match keywords always map to a single bit value. You also can specify bit fields as hexadecimal or decimal numbers. To negate a match, precede the value with an exclamation point. For example, a match occurs only if the RST bit in the TCP flags field is not set: `!rst`

To match multiple bit-field values, use the logical operators listed below. The operators are listed in order, from highest precedence to lowest precedence. Operations are left-associative.

Logical Operator	**Description**
(...)	Grouping
!	Negation
& or +	Logical AND
| or	Logical OR

As an example of a logical AND operation, in the following, a match occurs if the packet is the initial packet on a TCP session: `syn & !ack`

As an example of a logical OR operation, in the following, a match occurs if the packet is not the initial packet on a TCP session: `!syn | ack`

As an example of grouping, in the following, a match occurs for any packet that is either a TCP reset or is not the initial packet in the session: `!(syn & !ack) | rst`

When you specify a numeric value that has more than one bit set, the value is treated as a logical AND of the set bits. For example, the following two values are the same and a match occurs only if either bit 0x01 or 0x02 is not set: `!0x3`

`!(0x01 & 0x02)`

(enter both in the table)

You can use text synonyms to specify some common bit-field matches. You specify these matches as a single keyword. For example: `-established`

TCP flags

Normally, you specify this match in conjunction with the protocol match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): ack (0x10), fin (0x01), push (0x08), rst (0x04), syn (0x02), or urgent (0x20).

Match Condition	**Description**
Conditions with Variables	
fragment-flags number	IP fragmentation flags. In place of the numeric field value, you can specify one of the following keywords (the field values are also listed): dont-fragment (0x4000), more-fragments (0x2000), or reserved (0x8000).

Table 13-1. Bit-Field Firewall Filter Match Conditions

Match Condition	**Description**
ip-options number	IP options. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): loose-source-route (131), record-route (7), router-alert (148), strict-source-route (137), or timestamp (68).
tcp-flags number	TCP flags. Normally, you specify this match in conjunction with the protocol match statement to determine which protocol is being used on the port. For more details, see How Firewall Filters Test a Packet's Protocol. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): ack (0x10), fin (0x01), push (0x08), rst (0x04), syn (0x02), or urgent (0x20).
Text Synonyms	
first-fragment	First fragment of a fragmented packet. This condition does not match unfragmented packets.
is-fragment	This condition matches if the packet is a trailing fragment; it does not match the first fragment of a fragmented packet. To match both first and trailing fragments, you can use two terms.
tcp-established	TCP packets other than the first packet of a connection. This is a synonym for "(ack | rst)". This condition does not implicitly check that the protocol is TCP. To check this, specify the protocol tcp match condition.
tcp-initial	First TCP packet of a connection. This is a synonym for "(syn & !ack)".

Table 13-1. Bit-Field Firewall Filter Match Conditions

This condition does not implicitly check that the protocol is TCP. To check this, specify the protocol tcp match condition.

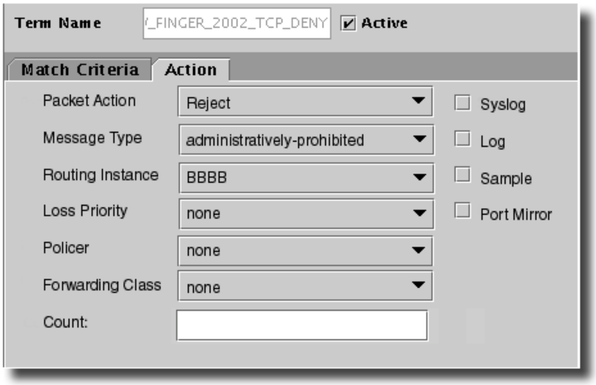
- **TCP established**—TCP packets other than the first packet of a connection. This is a synonym for "(ack | rst)".

In some screens you can select *Advanced* to bring up additional match condition parameters.

Action Tab

This tab configures the firewall response for data that meets the matching criteria.

Figure 13-43. Action Tab



Term Name _FINGER_2002_TCP_DENY ☑ Active

Packet Action: Reject

Message Type: administratively-prohibited

Routing Instance: BBBB

Loss Priority: none

Policer: none

Forwarding Class: none

Count:

□ Syslog

□ Log

□ Sample

□ Port Mirror

The following describes this screen's fields.

- **Packet Action**—The following actions are valid:

  No-Action–Does nothing.

  Accept–Accepts the packet sends it to its destination.

  Discard–Discards the packet and does not process it further. You cannot log or sample discarded packets.

  Reject–Rejects the packet and returns a rejection message. You *can* log or sample Rejected packets. This activates the *Message Type* pick list below.

  Next Term–Evaluate the next term in the firewall filter.

  Routing Instance—Lets you select the *Routing Instance* from that pick list, activated below.

- **Message Type—**When you use the reject action you can specify sending one of the following message-types: *administratively-prohibited (default)*, *bad-host-tos*, *bad-network-tos*, *host-prohibited*, *host-unknown*, *host-unreachable*, *network-prohibited*, *network-unknown*, *network-unreachable*, *port-unreachable*, *precedence-cutoff*, *precedence-violation*, *protocol-unreachable*, *source-host-isolated*, *source-route-failed*, or *tcp-reset*.

- **Routing Instance**—Select from the pick list if this is activated.

- **Loss Priority—**Configure *None*, *High*, or *Low*.

Policer—Apply rate-limiting procedures to the traffic.

Forwarding Class—Specify the packet forwarding class name.

Count—Count the packet in the named counter.

Check the following to enable them:

SysLog—Log an alert for the packet.

Log—Store the packet's header information on the Routing Engine.

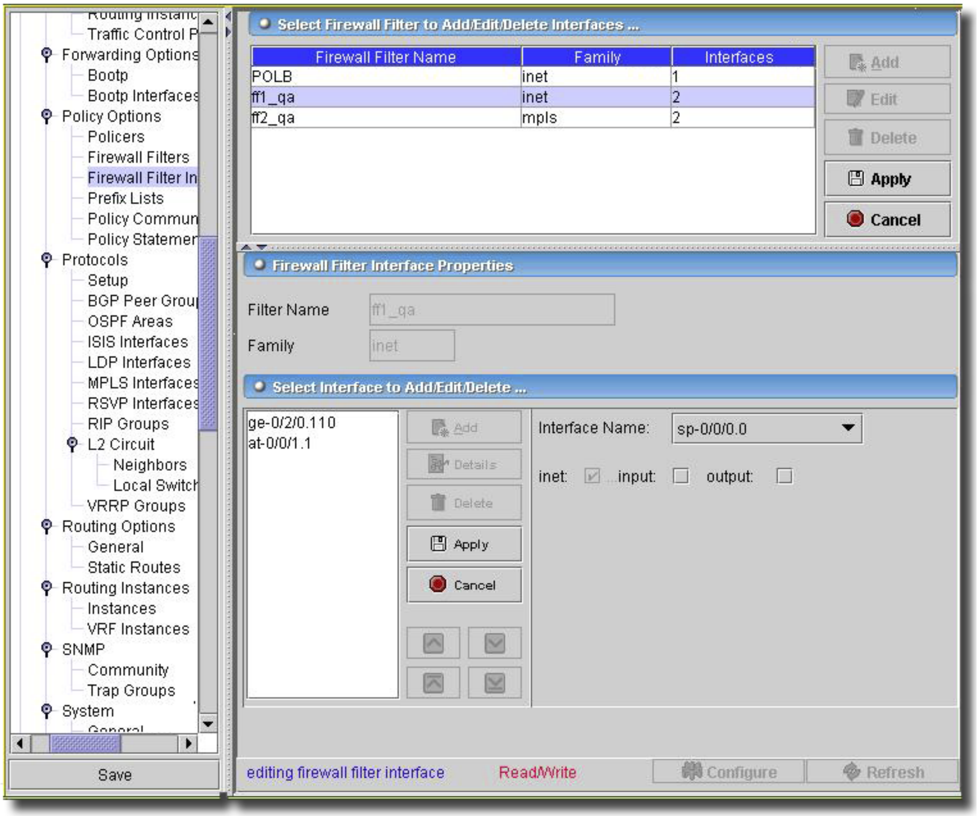
Sample—Sample the packet traffic.

Port Mirror—Port mirrored traffic is copied and sent to another interface.

Policy Options -> Firewall Filter Interfaces

This screen manages firewall filter interfaces associated with firewall filters.

Figure 13-44. Policy Options -> Firewall Filter Interfaces



Firewall Filter Name	Family	Interfaces
POLB	inet	1
ff1_qa	inet	2
ff2_qa	mpls	2

Filter Name ff1_qa

Family inet

ge-0/2/0.110
at-0/0/1.1

Interface Name: sp-0/0/0.0

inet: ☑ input: ☐ output: ☐

editing firewall filter interface Read/Write

For a description of how to configure filters, see Policy Options -> Firewall Filters on page 468. Click *Export* to save a description of the listed items to a file. Click *Add* (or select an existing filter and click *Edit*) to open the interfaces editor. You can also click *Delete* to remove a selected filter at the top of this screen. Click *Export* to save a description of the listed items to a file. Once you have edited an interface configuration, click *Apply* to accept your edits for the list, or click *Cancel* to abandon them. The editor has the following fields:

Firewall Filter Interfaces Properties

- **Filter Name**—An identifier for the stateful firewall ruleset.

- **Family**—For future functionality.

Select Interface to Add / Details / Delete

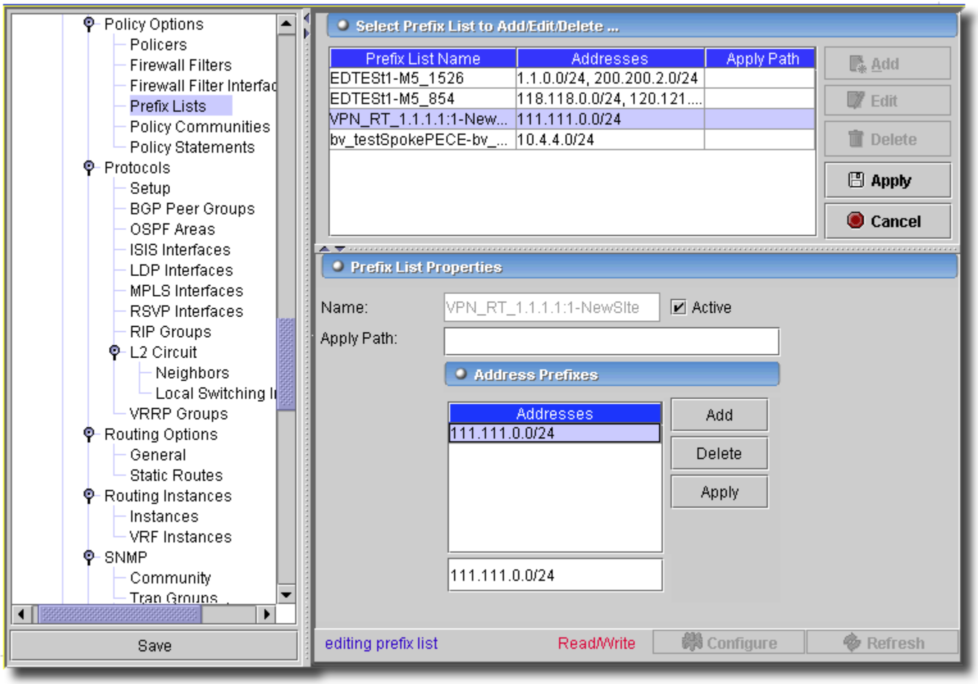
Click *Add / Details* to add or edit the interface configuration, or click *Delete* to delete a selected, listed interface. Select an interface from the pick list and check *inet*, *input*, *output* as appropriate for that interface. Click *Apply* to accept your edits and list the interface. Notice that you can use the up/down arrows to re-order selected interfaces. Interfaces at the top of the list have priority over those at the bottom.

Click *Apply* to accept your edits, or *Cancel* to abandon them. Clicking *Configure* sends these items as configured to the selected equipment. *Refresh* re-queries for field values on this screen.

Policy Options -> Prefix Lists

Use this screen to define a list of IPv4 or IPv6 address prefixes for use in a routing policy statement or firewall filter statement.

Figure 13-45. Policy Options -> Prefix Lists



Prefix List Name	Addresses	Apply Path
EDTESt1-M5_1526	1.1.0.0/24, 200.200.2.0/24	
EDTESt1-M5_854	118.118.0.0/24, 120.121....	
VPN_RT_1.1.1.1:1-New...	111.111.0.0/24	
bv_testSpokePECE-bv_...	10.4.4.0/24	

Name: VPN_RT_1.1.1.1:1-NewSite ☑ Active

Apply Path:

Addresses
111.111.0.0/24

111.111.0.0/24

editing prefix list

Read/Write

NOTE:

You must license this service.

Click *Export* to save a description of the listed items to a file. To remove a prefix list, select it and click *Delete*. Click *Add* or *Edit* to create a new, or modify an existing, selected item. When you are adding or editing, the following fields appear:

- **Name**—Name that identifies the list of IPv4 or IPv6 address prefixes.

- **Active**—Mark this item active or inactive in the configuration.

- **Apply Path**—Expand a prefix-list to include all prefixes implied by a defined path. These paths are strings of elements composed of identifiers or configuration keywords that point to a set of prefixes. You can include wildcards (enclosed in angle brackets) to match more than one identifier.

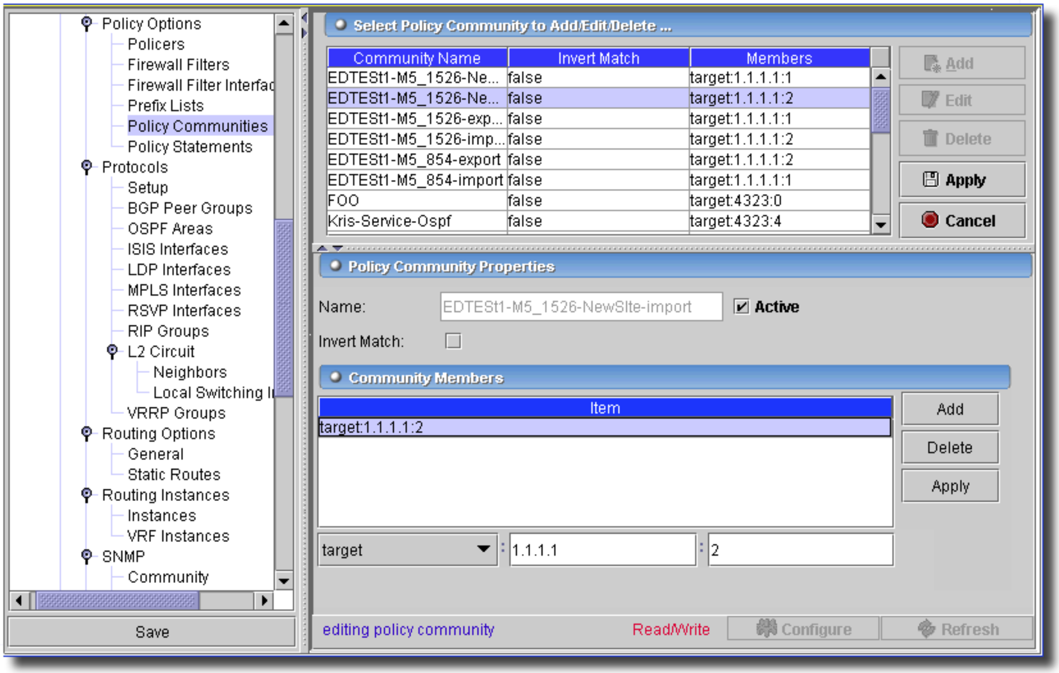
- **Addresses**—List of IPv4 or IPv6 address prefixes, one IP address per line in the configuration.

Click *Apply* to accept your edits, or *Cancel* to abandon them. Clicking *Configure* sends these items as configured to the selected equipment. *Refresh* re-queries for field values on this screen.

Policy Options -> Policy Communities

Use this screen to define communities or extended communities for use in a routing policy match conditions.

Figure 13-46. Policy Options -> Policy Communities



Community Name	Invert Match	Members
EDTESt1-M5_1526-Ne...	false	target:1.1.1.1:1
EDTESt1-M5_1526-Ne...	false	target:1.1.1.1:2
EDTESt1-M5_1526-exp...	false	target:1.1.1.1:1
EDTESt1-M5_1526-imp...	false	target:1.1.1.1:2
EDTESt1-M5_854-export	false	target:1.1.1.1:2
EDTESt1-M5_854-import	false	target:1.1.1.1:1
FOO	false	target:4323:0
Kris-Service-Ospf	false	target:4323:4

Name: EDTESt1-M5_1526-NewSIte-import ☑ Active

Invert Match: □

Item
target:1.1.1.1:2

target : 1.1.1.1 : 2

editing policy community   Read/Write

NOTE:

You must license this service.

To remove a community, select it and click *Delete*. Click A*dd* or *Edit* to create a new, or modify an existing, selected item. Click *Export* to save a description of the listed items to a file. When you are adding or editing, the following fields appear:

- **Name**—Name that identifies the regular expression. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters.
- **Active**—Check this to make the community active in the configuration.
- **Invert Match**—Invert the results of the community expression matching.

Community Members

These community-ids define one or more members of the community. They consist of two components, which you specify in the following format:

```
as-number:community-value
```

as-number–AS number of the community member. It can be a value from 1 through 65,534. You can specify the AS number in one of the following ways:

- AS number.
- Asterisk (*)–A wildcard character that matches all AS numbers. (In the definition of the community attribute, the asterisk also functions as described in Table 1.)
- Period (.)–A wildcard character that matches any single digit in an AS number.
- Group of AS numbers–A single AS number or a group of AS numbers enclosed in parentheses. Grouping the numbers in this way allows you to perform a common operation on the group as a whole and to give the group precedence. The grouped numbers can themselves include regular expression operators. For more information about the community regular expressions, see Configuring the Community Attribute Using UNIX Regular Expressions (See Using UNIX Regular Expressions on page 480 and Examples of Defining Community Attribute Regular Expressions on page 481).

community-value–Identifier of the community member. It can be a number from 0 through 65,535. You can specify the community value in one of the following ways:

- Community value number.
- Asterisk (*)–A wildcard character that matches all community values. (In the definition of the community attribute, the asterisk also functions as described in Table 1.)
- Period (.)–A wildcard character that matches any single digit in a community value number.
- Group of community value numbers–A single community value number or a group of community value numbers enclosed in parentheses. Grouping the regular expression in this way allows you to perform a common operation on

the group as a whole and to give the group precedence. The grouped path can itself include regular expression operators.

Pre-defined Community Names

You also can specify community-id as one of the following well-known community names, which are defined in RFC 1997, BGP Communities Attribute:

- **no-advertise**—Routes in this community name must not be advertised to other BGP peers.

- **no-export**—Routes in this community must not be advertised outside a BGP confederation boundary.

- **no-export-subconfed**—Routes in this community must not be advertised to external BGP peers, including peers in other members' ASs inside a BGP confederation.

Defining Community by Type

community-ids also identifies the type of extended community in the following format:

```
type:administrator:assigned-number
```

- *type*—The type of extended community. This can be either a *bandwidth*, *target*, *origin*, or *domain-id* community. The bandwidth community sets up the bandwidth extended community. The target community identifies the destination to which the route is going. The origin community identifies where the route originated. The domain-id community identifies the Open Shortest Path First (OSPF) domain from which the route originated.

administrator is the administrator. It is either an AS number or an IP version 4 (IPv4) address prefix, depending on the type of extended community.

assigned-number identifies the local provider.

NOTE:

Regular expressions are not supported for extended communities

See Configuring the Extended Communities Attribute (Examples) for examples.

Click A*pply* to accept your edits, or *Cancel* to abandon them. Clicking *Configure* sends these items as configured to the selected equipment. *Refresh* re-queries for field values on this screen.

Configuring the Extended Communities Attribute (Examples)

The following are JunOS representations of example extended community configurations. They display the extended community expressions described above.

- A target community with an administrative field of 10458 and an assigned number of 20:
  ```
  target:10458:20
  ```
- A target community with an administrative field of 1.1.1.1 and an assigned number of 20:
  ```
  target:1.1.1.1:20
  ```
- An origin community with an administrative field of 1.1.1.1 and an assigned number of 20:
  ```
  origin:1.1.1.1:20
  ```

Using UNIX Regular Expressions

When specifying community-ids, you can use UNIX-style regular expressions to specify the AS number and the member identifier. A regular expression consists of two components, which you specify in the following format:

```
term<operator>
```

- *term*—identifies the string to match.

- *operator*—specifies how the term must match. The following table lists the regular expression operators supported for the community attribute. You place an operator immediately after term with no intervening space, except for the pipe (|) and dash (-) operators, which you place between two terms, and parentheses, with which you enclose terms. The second table shows examples of how to define community-ids using community regular expressions. The operator is optional.

  Community regular expressions are identical to the UNIX regular expressions. Both implement the extended (or modern) regular expressions as defined in POSIX 1003.2.

NOTE:

Community regular expressions evaluate the string specified in term on a character-by-character basis. For example, if you specify 1234:5678 as term, the regular expressions see nine discrete characters, including the colon (:), instead of two sets of numbers (1234 and 5678) separated by a colon.

Supported Regular Expressions

Operator	Match...
{m, n}	At least m and at most n repetitions of term. Both m and n must be positive integers, and m must be smaller than n.
{m}	Exactly m repetitions of term. m must be a positive integer.
{m,}	m or more repetitions of term. m must be a positive integer.
*	Zero or more repetitions of term. This is equivalent to {0,}.
+	One or more repetitions of term. This is equivalent to {1,}.
?	Zero or one repetition of term. This is equivalent to {0,1}.
|	One of the two terms on either side of the pipe.
-	Between a starting and ending range, inclusive.
^	Character at the beginning of a community attribute regular expression. We recommend the use of this operator for the clearest interpretation of your community attribute regular expression. If you do not use this operator, the regular expression `123:456` could also match a route tagged with `5123:456`.
$	Character at the end of a community attribute regular expression. We recommend the use of this operator for the clearest interpretation of your community attribute regular expression. If you do not use this operator, the regular expression `123:456` could also match a route tagged with `123:4563`.

[ ]	Set of characters. One character from the set can match. To specify the start and end of a range, use a hyphen (-). To specify a set of characters that do not match, use the caret (^) as the first character after the opening square bracket ([).
( )	A group of terms that are enclosed in the parentheses. If enclosed in quotation marks with no intervening space ("()"), indicates a null. Intervening space between the parentheses and the terms is ignored.

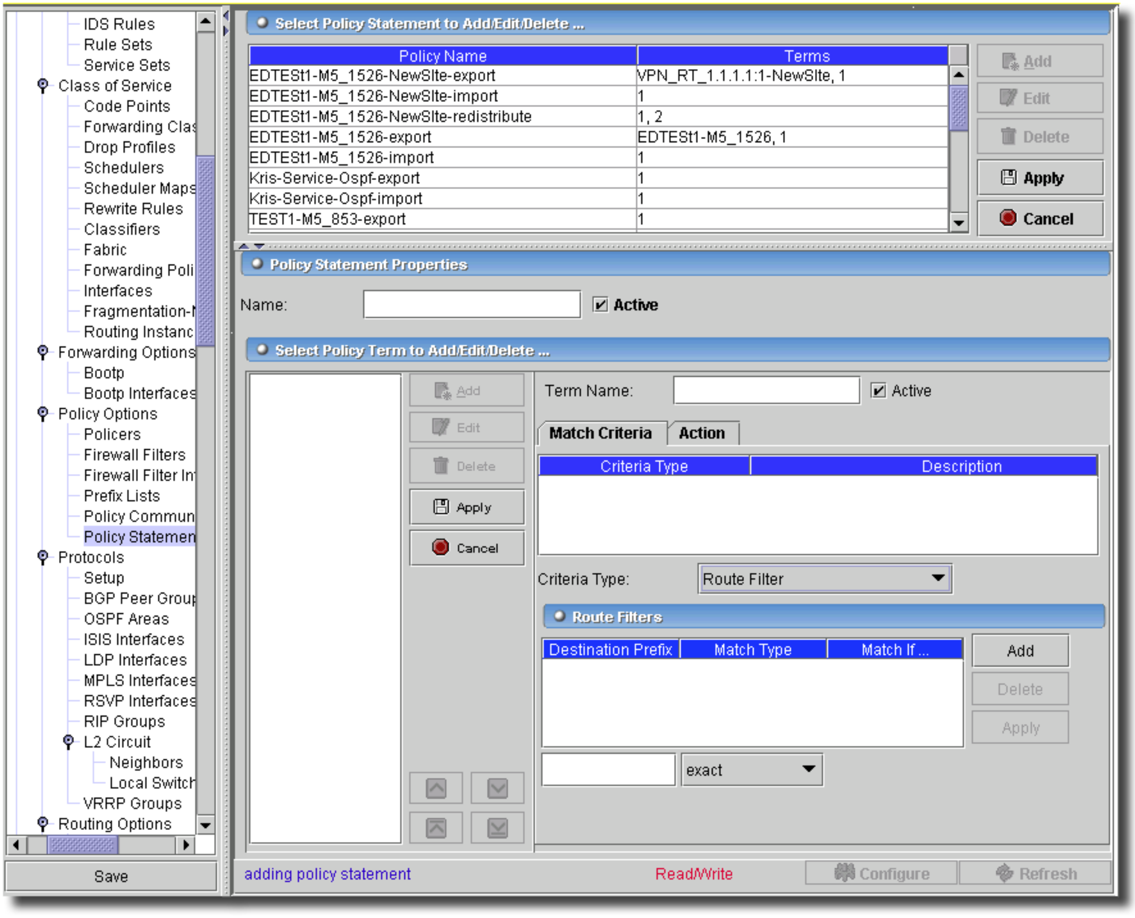
Examples of Defining Community Attribute Regular Expressions

Community Attribute to Match	Regular Expression	Example Matches
AS number is 56 or 78. Community value is any number.	^((56) | (78)):(.*)$	56:1000 78:65000
AS number is 56. Community value is any number that starts with 2.	^56:(2.*)$	56:2 56:222 56:234
AS number is any number. Community value is any number that ends with 5, 7, or 9.	^(.*):(.*[579])$	1234:5 78:2357 34:65009
AS number is 56 or 78. Community value is any number that starts with 2 and ends with 2 through 8.	^((56) | (78)):(2.*[2-8])$	56:22 56:21197 78:2678

Policy Options -> Policy Statements

This screen defines a routing policy, including subroutine policies.

Figure 13-47. Policy Options -> Policy Statements



Policy Name	Terms
EDTESt1-M5_1526-NewSlte-export	VPN_RT_1.1.1.1:1-NewSlte, 1
EDTESt1-M5_1526-NewSlte-import	1
EDTESt1-M5_1526-NewSlte-redistribute	1, 2
EDTESt1-M5_1526-export	EDTESt1-M5_1526, 1
EDTESt1-M5_1526-import	1
Kris-Service-Ospf-export	1
Kris-Service-Ospf-import	1
TEST1-M5_853-export	1

Name: ☑ Active

Term Name: ☑ Active

Criteria Type	Description

Criteria Type: Route Filter

Destination Prefix	Match Type	Match If ...

exact

adding policy statement

Read/Write

NOTE:

You must license this service.

To remove a community, select it and click *Delete*. Click *Export* to save a description of the listed items to a file. Click *Add* or *Edit* to create a new, or modify an existing, selected item. When you are adding or editing, the following fields appear:

- **Name**—Name that identifies the policy. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long.

- **Active**—Mark this item active or inactive in the configuration.

You can *Add* or *Edit* a policy statement term (with an accompanying *Match Criteria* and *Action*) with those buttons on the left side of the lower screen. Select a term and click *Delete* to remove it from those listed. Select a policy and use the up/down arrows to re-arrange (re-prioritize) those listed. Click *Apply* to accept your term edits, or *Cancel* to abandon them.

Common to the two tabs are these fields:

- **Term Name**—An identifier of the terms within the policy. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long.

- **Active**—Mark this item active or inactive in the configuration.

The following tabs let you configure the remaining information:

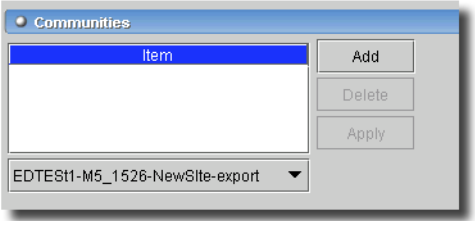
- Match Criteria
- Action

Match Criteria

The list below the policy name is a list of terms configured for this routing policy. Each term can contain Match Criteria and Actions. This portion of the screen changes, depending on the *Criteria Type* selected in the pick list.

- **Community**—BGP Communities can be selected that were created in Policy Options -> Policy Communities on page 477. Select a community with the pick list below the listed terms, and click *Add* to amend the list. Click *Delete* to remove a listed term, or *Apply* to apply any edits you make to an already selected term.

Figure 13-48. Community



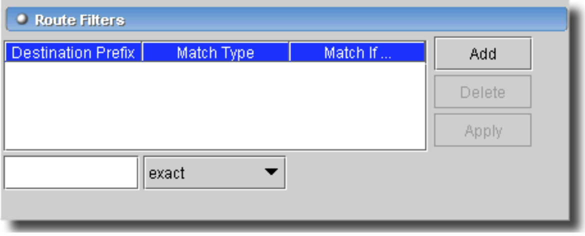
EDTESt1-M5_1526-NewSIte-export

- **Prefix List**—Similar to Community, this allows you to select list of IPv4 or IPv6 prefix lists created in Policy Options -> Prefix Lists on page 476. Manage these as you would the community selection described previously.

- **Protocols**—Select from the list of protocols in the pick list. The following values are available options: *aggregate*, *bgp*, *direct*, *isis*, *ldp*, *local*, *ospf*, *rip*, *ripng*, *rsvp* and *static*. Manage these as you would the community selection described previously.

- **Route Filter**—List of routes on which to perform an immediate match. Manage these as you would the community selection described previously. Destination Prefix is the IPv4 or IPv6 route prefix to match, Match Type is the type of match (see table below).

Figure 13-49. Route Filter

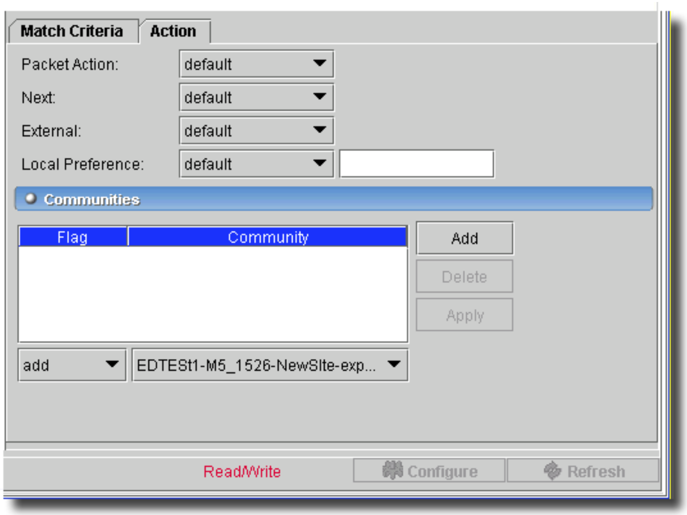


A match occurs if it meets the *Match If…* condition described in the table below. The appearance of *Match If* fields to the right of the *Match Type* selection varies depending on which *Match Type* you select.

Match Type	**Match If ...**
exact	The route shares the same most-significant bits (described by *prefix-length*), and *prefix-length* is equal to the route's prefix length.
longer	The route shares the same most-significant bits (described by *prefix-length*), and *prefix-length* is greater than the route's prefix length.
orlonger	The route shares the same most-significant bits (described by *prefix-length*), and *prefix-length* is equal to or greater than the route's prefix length.
prefix-length-range prefix-length2- prefix-length3	The route shares the same most-significant bits (described by *prefix-length*), and the route's prefix length falls between *prefix-length2* and *prefix-length3*, inclusive.
through destination-prefix	All the following are true: –The route shares the same most-significant bits (described by *prefix-length*) of the first destination prefix. –The route shares the same most-significant bits (described by *prefix-length*) of the second destination prefix for the number of bits in the prefix length. –The number of bits in the route's prefix length is less than or equal to the number of bits in the second prefix.
up to prefix-length2	The route shares the same most-significant bits (described by *prefix-length*) and the route's prefix length falls between *prefix-length* and *prefix-length2*.

- **Tag**—Configure a list of tag values (0 - 4294967295). Manage these as you would the community selection described previously.

Action



Packet Action: default

Next: default

External: default

Local Preference: default

Flag	Community

add

EDTESt1-M5_1526-NewSIte-exp...

Policy Actions can contain the following attributes:

- **Packet Action**—Choose to accept the route and propagate it (or reject it) here. After accepting a route, no other terms in the routing policy and no other routing policies are evaluated. After you reject a route, no other terms in the routing policy and no other routing policies are evaluated.

- **Next**—Select next *Policy* to skip to and evaluate the next routing policy. Any accept or reject action specified in the *then* statement is skipped. Any actions in the *then* statement that manipulate route characteristics then apply to the route. Next *Policy* is the default control action if a match occurs, if you do not specify a flow control action, and there are no further terms in the current routing policy. You can select the next *Term* to skip to and evaluate the next term in the same routing policy. Any accept or reject action specified in the *then* statement is skipped. Any actions in the *then* statement that manipulate route characteristics are applied to the route.

- **Local Preference**—(BGP only) Set the BGP local preference (LOCAL_PREF) attribute. The preference value can be a number in the range from 0 through 4,294,967,295 (232 -1).

  When you use *add/subtract* instead of default, you can change the local preference value by the specified amount. If an addition operation results in a value that is greater than 4,294,967,295 (232 - 1), the application sets the value to 232 - 1. If a subtraction operation results in a value less than zero (0), the application sets the value to zero. If an attribute value is not already set at the time of the addition or subtraction operation, the attribute value defaults to a value of zero (0) regardless of the amount specified. If you perform an addition to an attribute with a value of zero, the number you add becomes the resulting attribute value.

For BGP, if the attribute value is not known, it is initialized to 100 before the routing policy is applied.

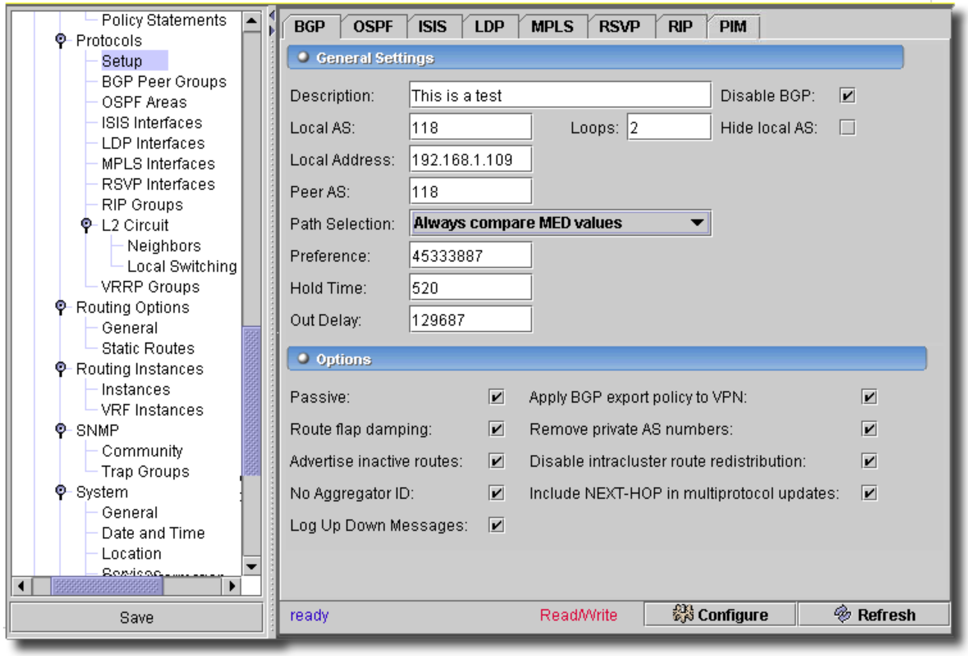
- **Communities**—(BGP only) Add the specified communities to the set of communities in the route. Manage these as you would the community selection described previously in the Match Criteria tab.

Click *Apply* to accept your edits, or *Cancel* to abandon them. Clicking *Configure* sends these items as configured to the selected equipment. *Refresh* re-queries for field values on this screen.

Protocols -> Setup

This screen contains tabs to set up the various protocols on the selected device. Use the tabs at the top of this screen to select a type of protocol.

Figure 13-50. Protocols -> Setup (BGP)



General Settings

Description: This is a test
Disable BGP: ☑
Local AS: 118
Loops: 2
Hide local AS: ☐
Local Address: 192.168.1.109
Peer AS: 118
Path Selection: Always compare MED values
Preference: 45333887
Hold Time: 520
Out Delay: 129687

Options

Passive: ☑
Apply BGP export policy to VPN: ☑
Route flap damping: ☑
Remove private AS numbers: ☑
Advertise inactive routes: ☑
Disable intracluster route redistribution: ☑
No Aggregator ID: ☑
Include NEXT-HOP in multiprotocol updates: ☑
Log Up Down Messages: ☑

ready
Read/Write

For the definition of the fields configurable on this screen's tabs, see the following sections:

- BGP
- OSPF
- ISIS
- LDP
- MPLS

- RSVP
- RIP
- PIM

BGP

This tab lets you control the basic BGP settings. It has the following fields:

General Settings

- **Description**—A Text Description for BGP. Check *Disable BGP* to reserve these settings without applying them.

- **Local AS**—Local autonomous system number

- **Loops**—Maximum number of times this AS can be in an AS path (1 - 10).

- **Local Address**—Address of local end of BGP session

- **Peer AS**—Peer autonomous system number (1 - 65,535),

- **Authentication Key**—MD5 authentication key.

Checkbox Options:

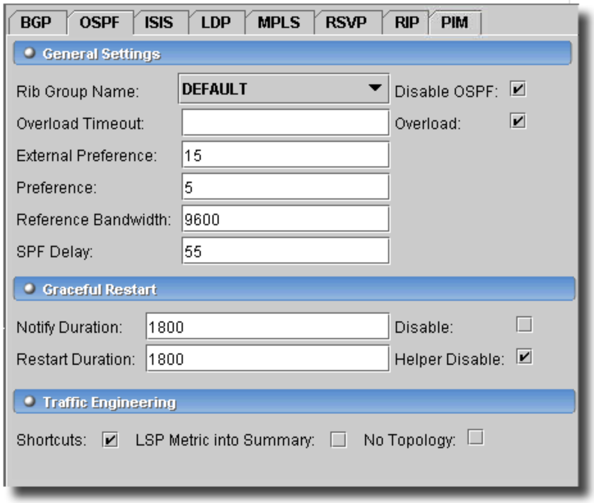
Check any of the following to enable them:

- Enable route flap damping.
- Include Next Hop multi protocol updates.
- Log a message for peer state transitions.
- Allow load sharing among multiple BGP paths.
- Set router ID in aggregator path attribute to 0 (No Aggregator ID).
- Hide this local AS in paths learned from this peering.
- Do not send open messages to a peer.
- Remove well-known private AS numbers.

OSPF

This screen manages OSPF Protocol settings.

Figure 13-51. Routing Protocols -> Setup: OSPF General



General Settings

Rib Group Name: DEFAULT

Disable OSPF: ☑

Overload Timeout:

Overload: ☑

External Preference: 15

Preference: 5

Reference Bandwidth: 9600

SPF Delay: 55

Graceful Restart

Notify Duration: 1800

Disable: □

Restart Duration: 1800

Helper Disable: ☑

Traffic Engineering

Shortcuts: ☑ LSP Metric into Summary: □ No Topology: □

- This screen has the following fields:

General Settings

- **Rib Group Name**—Routing table group for importing OSPF routes.
- **Disable OSPF**—Disables OSPF Protocols on this device.
- **Overload Timeout** (available only if overload is selected)—Time after which overload mode is reset (60 - 1800 seconds)
- **Overload**—Set the overload mode (repel transit traffic)
- **External Preference**—Preference of external routes.
- **Preference**—Preference of internal routes.
- **Reference Bandwidth**—Bandwidth for calculating metric defaults (9600 - 1000000000000
- **SPF Delay**—Time to wait before running an SPF (50 - 1000 milliseconds)

Graceful Restart

- **Notify Duration**—Time to send all max-aged grace LSAs (1 - 3600 seconds)
- **Restart Duration**—Time for all neighbors to become full (1 - 3600 seconds)
- **Disable**—Disable OSPF graceful restart capability
- **Helper Disable**—Disable graceful restart helper capability

Traffic Engineering

- **Shortcuts**—Use label-switched paths as next hops, if possible

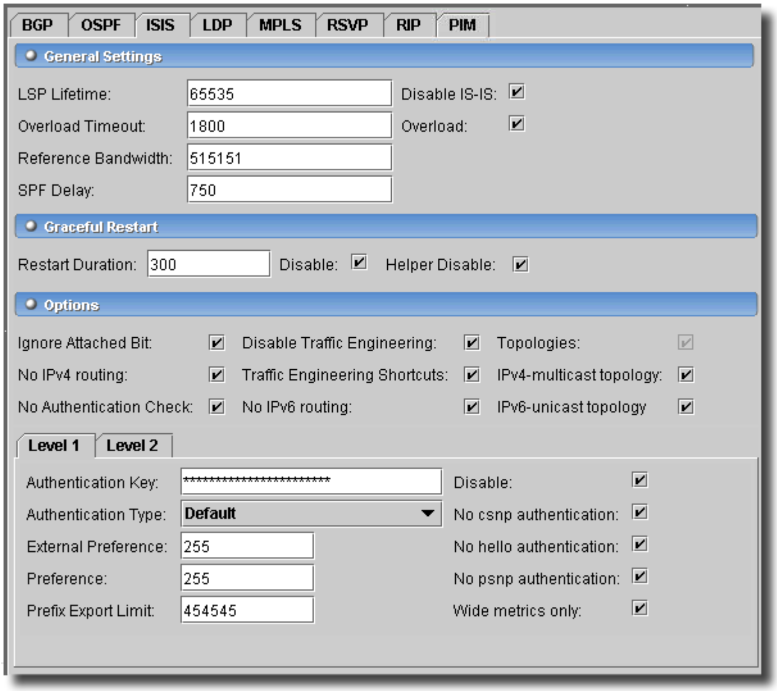
- **LSP Metric into Summary** (only available if Shortcuts is selected)—Advertise LSP metric into summary LSAs
- **No Topology**—Disable dissemination of TE link-state topology information

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

ISIS

This tab lets you control ISIS settings for the selected device.

Figure 13-52. Routing Protocols -> Setup: ISIS



General Settings

LSP Lifetime: 65535 — Disable IS-IS: ☑
Overload Timeout: 1800 — Overload: ☑
Reference Bandwidth: 515151
SPF Delay: 750

Graceful Restart

Restart Duration: 300 — Disable: ☑ — Helper Disable: ☑

Options

Ignore Attached Bit: ☑ — Disable Traffic Engineering: ☑ — Topologies: ☑
No IPv4 routing: ☑ — Traffic Engineering Shortcuts: ☑ — IPv4-multicast topology: ☑
No Authentication Check: ☑ — No IPv6 routing: ☑ — IPv6-unicast topology ☑

Authentication Key: ************************ — Disable: ☑
Authentication Type: Default — No csnp authentication: ☑
External Preference: 255 — No hello authentication: ☑
Preference: 255 — No psnp authentication: ☑
Prefix Export Limit: 454545 — Wide metrics only: ☑

This screen has the following fields:

General Settings

LSP Lifetime—Lifetime of LSPs (350 - 65535 seconds). How long an LSP originating from the router should persist in the network. The router sends LSPs often enough so that the LSP lifetime never expires. Default: 1200 seconds

Disable ISIS—Do not enable this configuration

- **Overload Timeout**—Time after which overload bit is reset (60 - 1800 seconds)
- **Overload**—(checkbox) Set the overload bit (no transit traffic).

- **Reference Bandwidth**—Bandwidth for calculating metric defaults. Set the reference bandwidth used in calculating the default interface cost. The cost is calculated using the following formula: cost = reference-bandwidth/bandwidth. Default: 10 Mbps. Range: 9600 through 1,000,000,000,000 Mbps
- **SPF Delay**—Time to wait before running an SPF (milliseconds). This configures the shortest-path-first (SPF) delay milliseconds (the number of milliseconds between the detection of a topology change and when the SPF algorithm runs). Range: 50 through 1000 milliseconds. Default: 200 milliseconds

Graceful Restart

Restart duration—Maximum time for graceful restart to finish (seconds). Range: 30 through 300 seconds. Default: 90 seconds

Disable—Disable graceful restart.

Helper Disable—Disable graceful restart helper capability.

Options

The following checkboxes further configure ISIS.

- **Ignore Attached Bit**—Ignore the attached bit in Level 1 LSPs. Ignore the attached bit on ISIS Level 1 routers. Configuring this statement allows the router to ignore the attached bit on incoming Level 1 LSPs. If the attached bit is ignored, no default route, which points to the router which has set the attached bit, will be installed.
- **No Authentication Check**—Disable authentication checking. Generate authenticated packets, check the authentication on received packets, but do not reject packets that cannot be authenticated.
- **No IPv4-routing**—Disable IPv4 routing

Disable Traffic Engineering—Disable traffic engineering

- **Traffic Engineering Shortcuts**—Use label-switched paths as next hops, if possible.
- **No IPv6 routing**—Disable IPv6 routing.
- **Topologies**—Enable topologies.
- **IPv4-multicast**—Enable IPv4-multicast topology

IPv6-unicast—Enable IPv6-unicast topology

Levels 1 & 2

These tabs configure global level attributes

- **Authentication Key**—Authentication key (password). Neighboring routers use the password to verify the authenticity of packets sent from this interface. For the key to work, you also must include the authentication-type statement. All routers must use the same password. If you are using the JUNOS ISIS software with another implementation of ISIS, the other implementation must be configured to use the same password for the domain, the area, and all interfaces adjacent to the router.

- **Authentication Type**— Enable authentication and specify the authentication scheme for IS-IS. If you enable authentication, you must specify a password by including the authentication-key statement. Possible completions include

  md5 – (MD5 authentication) Simple password authentication

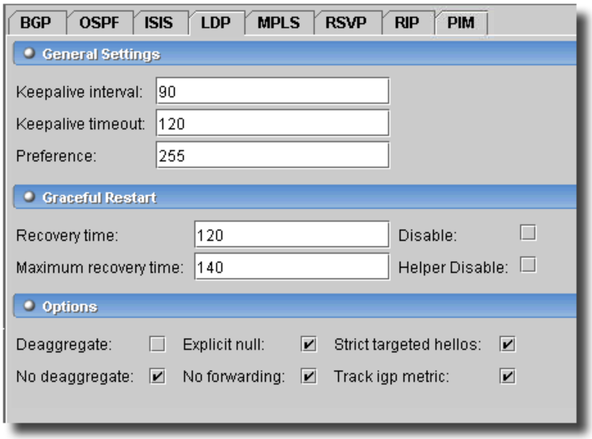
  disable–Disable IS-IS on this level

- **External Preference**–Preference of external routes. Range: 0 through 255 Default: 15 (for Level 1 internal routes), 18 (for Level 2 internal routes), 160 (for Level 1 external routes), 165 (for Level 2 external routes).
- **Preference**—Preference of internal routes. Range: 0 through 255 Default: 15 (for Level 1 internal routes), 18 (for Level 2 internal routes), 160 (for Level 1 external routes), 165 (for Level 2 external routes).
- **Prefix Export Limit**—Maximum number of external prefixes that can be exported (0 - 4294967295)
- **No csnp authentication**—Disable authentication for complete sequence number packets
- **No hello authentication**—Disable authentication for hello packets.
- **No psnp authentication**—Disable authentication for partial sequence number packets
- **Wide metrics only**—Generate wide metrics only. This configures ISIS to generate metric values greater than 63 on a per ISIS level basis.

LDP

This tab lets you manage LDP attributes for the selected equipment.

Figure 13-53. Protocols -> Setup: LDP



General Settings

Keepalive interval: 90

Keepalive timeout: 120

Preference: 255

Graceful Restart

Recovery time: 120 Disable: ☐

Maximum recovery time: 140 Helper Disable: ☐

Options

Deaggregate: ☐ Explicit null: ☑ Strict targeted hellos: ☑

No deaggregate: ☑ No forwarding: ☑ Track igp metric: ☑

Here are the fields on this screen:

General Settings

- **Keepalive interval**—(1 - 65535 seconds).
- **Keepalive timeout**—(1 - 65535 seconds)
- **Preference**—Set the route preference level for LDP routes. (0 - 255)

Graceful Restart

Configure graceful restart attributes. Enable LDP graceful restart on the LDP master protocol instance.

- **Recovery time**—Time required for recovery (120 - 1800 seconds) Specifies the amount of time a router waits for LDP to restart gracefully. Configure the recovery time, in seconds. Range: 120 through 1800 seconds. Default: 140 seconds
- **Maximum recovery time**—Maximum time stale mappings are maintained (seconds). Specify the maximum period (in seconds) to wait before giving up an attempt to gracefully restart. Range: 140 through 1900 seconds. Default: 140 seconds
- **Disable**—Disable graceful restart. Explicitly disable LDP on an interface, or explicitly disable LDP graceful restart.
- **Helper Disable**—Disable the graceful restart helper capability. Disables helper mode for LDP graceful restart. When helper mode is disabled, a router cannot help a neighboring router that is attempting to restart LDP. Helper mode is enabled by default on all routing protocols (including LDP) that support graceful restart.

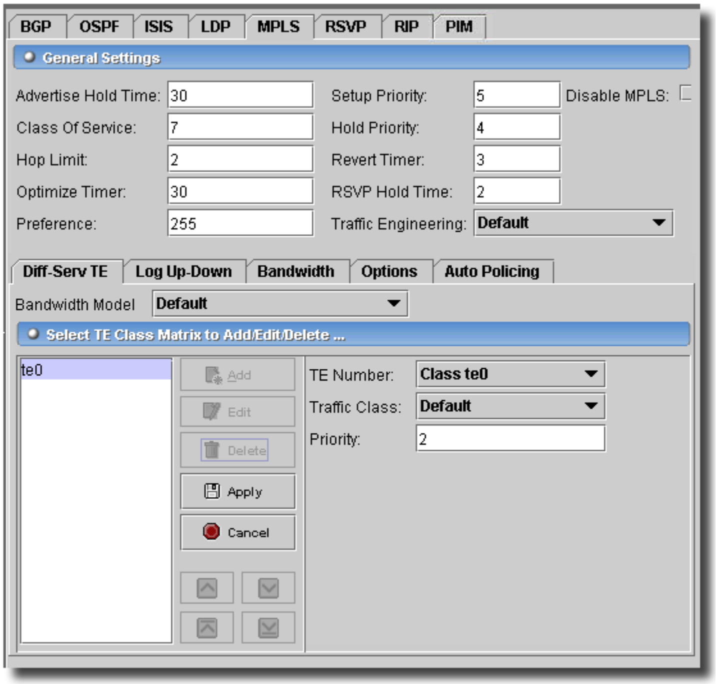
Options

- **Deaggregate**—Deaggregate FECs into separate labels. Control forwarding equivalence class (FEC) deaggregation on the router. Deaggregation is disabled on the router by default.
- **No deaggregate**—Don't deaggregate FECs into separate labels, aggregate FECs.
- **Explicit null**—Advertise the EXPLICIT_NULL label for egress FECs. Advertise label 0 to the egress router of a label-switched path (LSP). If you do not include the explicit-null statement in the Multiprotocol Label Switching (MPLS) configuration, label 3 (implicit null) is advertised.
- **No forwarding**—Do not use LDP ingress routes for forwarding. Do not add ingress routes to the inet.0 routing table even if traffic-engineering bgp-igp (configured at the [edit protocols mpls] hierarchy level) is enabled.
- **Strict targeted hellos**—Do not send targeted hellos to unconfigured neighbors
- **Track igp metric**—Track the IGP metric. Use the IGP route metric for the LDP routes instead of the default LDP route metric (the default LDP route metric is 1).

MPLS

This tab configures the top level MPLS protocol options.

Figure 13-54. Protocols -> Setup: MPLS (Diff-Serv TF)



Advertise Hold Time: 30
Class Of Service: 7
Hop Limit: 2
Optimize Timer: 30
Preference: 255
Setup Priority: 5
Hold Priority: 4
Revert Timer: 3
RSVP Hold Time: 2
Traffic Engineering: Default
Disable MPLS: □

Bandwidth Model: Default

te0

TE Number: Class te0
Traffic Class: Default
Priority: 2

This tab has the following fields:

- **Advertise Hold Time**—Do not advertise when the LSP goes from up to down, for a certain period of time known as hold time. Enter number of seconds.
- **Class of Service**—(CoS) value given to all packets in the LSP. The CoS value might affect the scheduling or queuing algorithm of traffic traveling along an LSP. A higher value typically corresponds to a higher level of service. Range—0 through 7. If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value.
- **Hop Limit**—For an LSP, the maximum number of routers that the LSP can traverse, including the ingress and egress routers. For fast reroute, how many more routers a detour is allowed to traverse compared with the LSP itself. For example, if an LSP traverses 4 routers, any detour for the LSP can be no more than 10 router hops, including the ingress and egress routers. Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute) Default: 255 (for an LSP); 6 (for fast reroute).
- **Optimize Timer**—Enable periodic reoptimization of an LSP that is already set up. If topology changes occur, an existing path might become suboptimal, and a subsequent recomputation might be able to determine a better path. This option is useful only on LSPs for which

constrained-path computation is enabled; that is, for which the no-cspf statement is not configured. To avoid extensive resource consumption that might result because of frequent path recomputations, or to avoid destabilizing the network as a result of constantly changing LSPs, best practice is either to leave the timer value sufficiently large or to disable the timer value. By default, the optimize timer is disabled.

- **Preference**—Preference for the route. You can optionally configure multiple LSPs between the same pair of ingress and egress routers. This is useful for balancing the load among the LSPs because all LSPs, by default, have the same preference level. To prefer one LSP over another, set different preference levels for individual LSPs. The device uses the LSP with the lowest preference value. The default preference for LSPs is lower (more preferred) than all learned routes except direct interface routes. Range: 1 through 255. Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs
- **Setup Priority**—If, at session setup time, insufficient link bandwidth is encountered during session establishment, the setup priority is compared with existing established sessions on the link to determine whether some of them should be preempted to accommodate the new session. The session with the lower hold priority is preempted. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority. Default: 7 (The session cannot preempt any existing sessions.).
- **Hold Priority**—Hold priority, used to keep a reservation after it has been set up. A smaller number has a higher priority. The priority must be greater than or equal to the setup priority to prevent preemption loops. Range: 0 through 7, where 0 is the highest and 7 is the lowest priority. Default: 0 (Once the session is set up, no other session can preempt it.).
- **Revert Timer**—Specify the amount of time (in seconds) that an LSP must wait before it can revert traffic back onto a primary path. If during this time the primary path experiences any connectivity problem or stability problem, the timer is restarted. If you have configured a value of 0 seconds for the revert-timer statement and traffic is switched to the secondary path, the traffic remains on that path indefinitely. It is never switched back to the primary path unless you intervene. Range: 0 through 65,535 seconds. Default: 60 seconds.
- **RSVP Hold Time**—Amount of time MPLS retains RSVP PathErr messages and considers them for CSPF computations. The more time you configure, the more time a source node (ingress of the RSVP LSPs) can have to learn about the failures of its LSP by monitoring PathErr messages transmitted from downstream nodes. Information from the PathErr messages is incorporated into subsequent LSP computations, which can improve the accuracy and speed of LSP setup. Some PathErr messages are also used to update traffic engineering database (TED) bandwidth information, reducing inconsistencies between the TED and the network. Range: 0 through 240 seconds. Default: 25 seconds.
- **Traffic Engineering**—Select whether MPLS performs traffic engineering on BGP destinations only or on both BGP and IGP destinations. Affects only LSPs originating from this router, not transit or egress LSPs. Options:

BGP destinations only—Ingress routes are installed in the inet.3 routing table.

BGP and IGP destinations—Ingress routes are installed in the inet.0 routing table. If IGP shortcuts are enabled, the shortcut routes are automatically installed in the inet.0 routing table.

BGP and IGP destinations with routes—Ingress routes are installed in the inet.0 and inet.3 routing tables. This option is used to support VPNs.

Use MPLS Routes—On both BGP and IGP destinations. Use ingress routes for forwarding only, not for routing.

The following are tabs that further manage MPLS settings:

Diff-Serv TE

This tab configures Differentiated-Services-Aware Traffic Engineering. It has the following fields:

- **Bandwidth Model**—Configure the bandwidth model for differentiated services. Note that you cannot configure both bandwidth models at the same time. Options:

MAM with Support for E-LSPs—The extended maximum allocation model (MAM) is a bandwidth model based on MAM.

Maximum Allocation Model—The MAM is defined in Internet draft *draft-ietf-tewg-diff-te-mam-03.txt*, Maximum Allocation Bandwidth Constraints Model for Diff-Serv-Aware MPLS Traffic Engineering.

Russian Dolls Model—The Russian dolls bandwidth allocation model (RDM) is defined in Internet draft *draft-ietf-tewg-diff-te-russian-05.txt*, Russian Dolls Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering. RDM makes efficient use of bandwidth by allowing the class types to share bandwidth.

- **TE Class Matrix**—Here, you specify the traffic engineering class matrix for a multiclass LSP or a differentiated-services-aware traffic engineering LSP. Click *Add* to create a new TE class matrix item, or *Edit* to modify an existing, selected item. *Delete* removes listed items. When you click *Add* or *Edit*, the following fields appear to the right of the list:

TE Number—Specify the number of the traffic engineering class. It can be one of eight values: te0, te1, te2, te3, te4, te5, te6, te7. You must configure the traffic engineering classes in order, starting with te0.

Traffic Class—Specify the traffic class for the traffic engineering class (0 - 3).

Priority—Specify the priority of the class type. It can be one of eight values from 0 through 7.

Use the *Up/Down/Top/Bottom* areas below the listed items to re-order them.

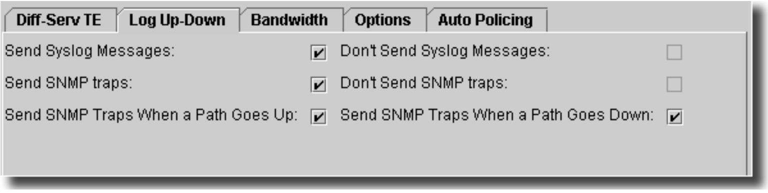
You are not required to configure the traffic engineering classes. The following table shows the default values for everything in the traffic engineering class matrix. The default mapping is expressed in terms of the default forwarding classes defined in the CoS configuration.

Traffic Engineering Class	Class Type	Queue	Priority
te0	ct0	0	7
te1	ct1	1	7
te2	ct2	2	7
te3	ct3	3	7
te4	ct0	0	0
te5	ct1	1	0
te6	ct2	2	0
te7	ct3	3	0

Log Up-Down

This tab manages SNMP and Syslog messaging for MPLS.

Figure 13-55. Protocols -> Setup:MPLS (Log Up-Down)



Send Syslog Messages: ☑ Don't Send Syslog Messages: □
Send SNMP traps: ☑ Don't Send SNMP traps: □
Send SNMP Traps When a Path Goes Up: ☑ Send SNMP Traps When a Path Goes Down: ☑

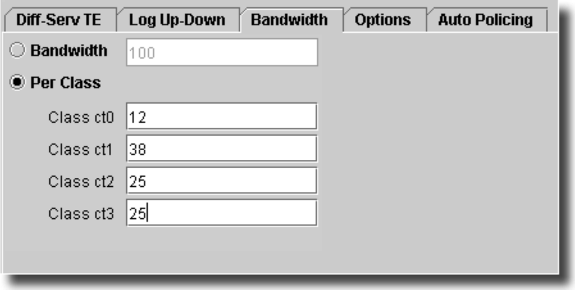
These log a message or send a Simple Network Management Protocol (SNMP) trap whenever an LSP makes a transition from up to down, or vice versa, and whenever an LSP switches from one active path to another. Only the ingress router performs these operations. This tab has the following checkbox pairs:

- Send/Don’t send Syslog Messages
- Send/Don’t send SNMP traps
- Send SNMP Traps When a Path goes up/down.

Bandwidth

This screen lets you set MPLS bandwidth two ways.

Figure 13-56. Protocols -> Setup:MPLS (Bandwidth)



○ Bandwidth 100

● Per Class

Class ct0 12

Class ct1 38

Class ct2 25

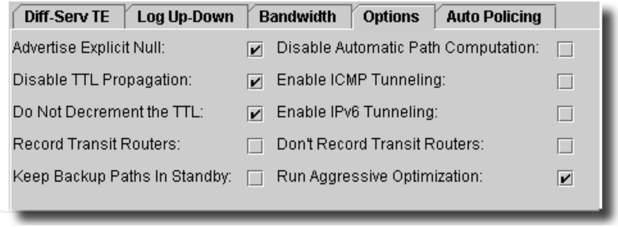
Class ct3 25

You can either set it generally (with the *Bandwidth* radio button and the field to its right), or *Per Class* (similarly).

Options

This screen lets you configure MPLS options.

Figure 13-57. Protocols -> Setup:MPLS (Options)



Advertise Explicit Null:	☑	Disable Automatic Path Computation:	□
Disable TTL Propagation:	☑	Enable ICMP Tunneling:	□
Do Not Decrement the TTL:	☑	Enable IPv6 Tunneling:	□
Record Transit Routers:	□	Don't Record Transit Routers:	□
Keep Backup Paths In Standby:	□	Run Aggressive Optimization:	☑

It has the following checkboxes:

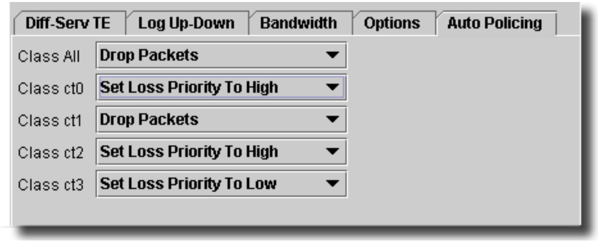
- **Advertise explicit Null**—Advertise label 0 to the egress router of an LSP.
- **Disable TTL Propagation**—Enter number of seconds.
- **Do Not Decrement the TTL**—Disable normal TTL decrementing, which decrements the TTL field in the IP header by 1. This statement decrements the IP TTL by 1 before encapsulating the IP packet within an MPLS packet. When the penultimate router pops off the top label, it does not use the standard write-back procedure of writing the MPLS TTL into the IP TTL field. Therefore, the IP packet is decremented by 1. The ultimate router then decrements the packet by one more for a total cloud appearance of 2, thus hiding the network topology.
- **Record Transit Routers**—Check to enable.
- **Keep Backup Paths in Standby**—Check to enable.
- **Disable Automatic Path Computation**—Check to enable.
- **Enable ICMP Tunneling**—Enables ICMP tunneling, which can be used for debugging and tracing purposes.

- **Enable IPv6 Tunneling**—Allow IPv6 routes to be resolved over an MPLS network by converting all routes stored in the inet.3 routing table to IPv4-compatible IPv6 addresses and then copying them into the inet6.3 routing table. This routing table can be used to resolve next hops for inet6 and inet6-vpn routes.
- **Don't Record Transit Routers**—Check to enable.
- **Run Aggressive Optimization**—If enabled, the LSP reoptimization is based solely on the IGP metric. The reoptimization process ignores the available bandwidth ratio calculations, the least-fill 10 percent congestion improvement rule, and the hop-counts rule. This statement makes reoptimization more aggressive than the default.

Auto Policing

This tab lets you pick auto-policing options.

Figure 13-58. Protocols -> Setup:MPLS (Auto Policing)



Class All Drop Packets
Class ct0 Set Loss Priority To High
Class ct1 Drop Packets
Class ct2 Set Loss Priority To High
Class ct3 Set Loss Priority To Low

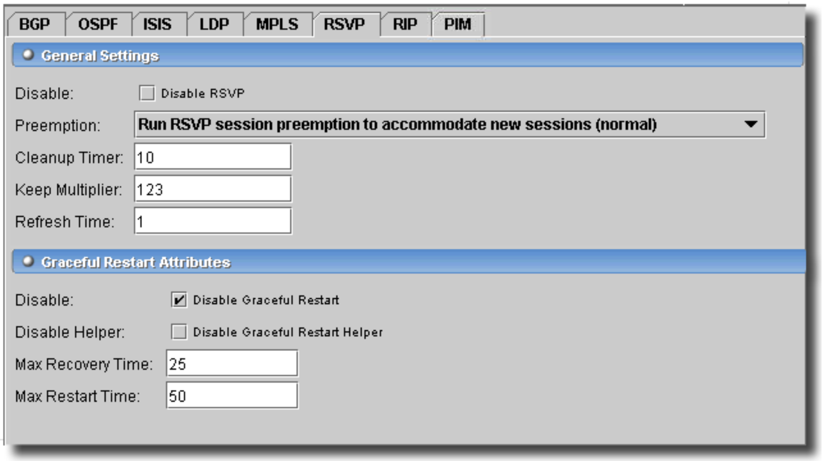
Here, you can select policing options for MPLS for all classes (*Class All*) or for individual classes (*Class ct0*, *Class ct1*, *Class ct2*, *Class ct3*). You can specify the following policer actions by selecting them from the pick list:

- **Default**—no action
- **Drop Packets**—Drop all packets.
- **Set Loss Priority to High**—Set the packet loss priority (PLP) to high.
- **Set Loss Priority to Low**—Set the packet loss priority (PLP) to low.

RSVP

This tab manages RSVP.

Figure 13-59. Protocols -> Setup: RSVP



General Settings

Disable: □ Disable RSVP

Preemption: Run RSVP session preemption to accommodate new sessions (normal)

Cleanup Timer: 10

Keep Multiplier: 123

Refresh Time: 1

Graceful Restart Attributes

Disable: ☑ Disable Graceful Restart

Disable Helper: □ Disable Graceful Restart Helper

Max Recovery Time: 25

Max Restart Time: 50

This tab has the following fields:

General Settings

- **Disable**—Check to disable RSVP
- **Preemption**—Select from the pick list. Available options:

  Run RSVP session preemption to accommodate new sessions (normal)–(the default) Preempt RSVP sessions to accommodate new higher-priority sessions when bandwidth is insufficient to handle all sessions.

  Run RSVP session preemption whenever necessary (aggressive)–Preempt RSVP sessions whenever bandwidth is insufficient to handle all sessions. A session is preempted whenever bandwidth is lowered or a new higher-priority session is established.

  No RSVP session preemption (disabled)–Do not preempt RSVP sessions.

- **Cleanup Timer**—Soft preemption attempts to establish a new path for a preempted LSP before tearing it down. A value of 0 disables soft preemption. Range: 0 through 180 seconds. Default: 30 seconds
- **Keep Multiplier**—Set the keep multiplier value. Range: 1 through 255, Default: 3
- **Refresh Time**—Set the refresh time. Range: 1 through 65,535 (seconds). Default: 30 seconds

Graceful Restart Attributes

- **Disable**—Check to disable Graceful Restart.
- **Disable Helper**—Check to disable Graceful Restart Helper. Helper mode is enabled by default.

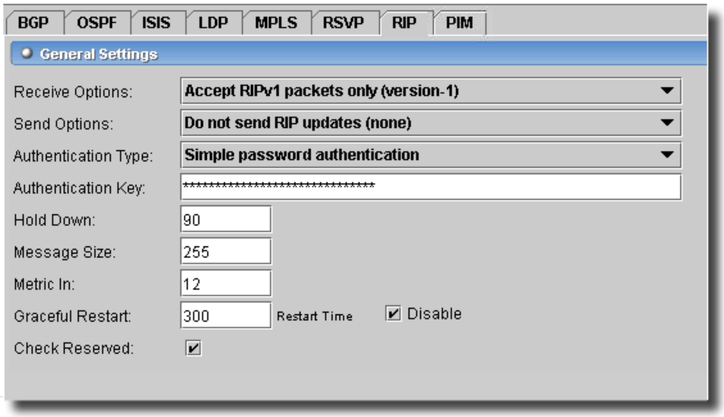
- **Max Recovery Time**—The maximum amount of time the router stores the state of neighboring routers when they undergo a graceful restart. The value applies to all neighboring routers, so it should be based on the time that the slowest RSVP neighbor requires for restart. Default: 180 seconds. Range: 1 through 3600 seconds

- **Maximum Restart Time**—The maximum amount of time the router waits between when it discovers that a neighboring router has gone down and when it declares the neighbor down. This value is applied to all neighboring routers, so it should be based on the time that the slowest RSVP neighbor requires for restart. Default: 20 seconds. Range: 1 through 1800 seconds.

RIP

This tab manages RIP settings.

Figure 13-60. Protocols -> Setup: RIP



Receive Options: Accept RIPv1 packets only (version-1)
Send Options: Do not send RIP updates (none)
Authentication Type: Simple password authentication
Authentication Key: ********************************
Hold Down: 90
Message Size: 255
Metric In: 12
Graceful Restart: 300 Restart Time ☑ Disable
Check Reserved: ☑

- It has the following fields:

General Settings

- **Receive Options**—Configure RIP receive options. Options:

  Do not receive RIP packets (none)—Do not receive RIP packets.

  Accept RIPv1 and RIPv2 packets (both)—Accept both RIP version 1 and version 2 packets. (The default.)

  Accept RIPv1 packets only (version-1)—Accept only RIP version 1 packets.

  Accept RIPv2 packets (version-2)—Accept only RIP version 2 packets.

- **Send Options**—Configure RIP send options. Options available:

  Broadcast RIPv2 and RIPv1 compatible packets (broadcast)—Broadcast RIP version 2 packets (RIP version 1 compatible).

Multicast RIPv2 packets (multicast)—Multicast RIP version 2 packets. This is the default.

Do not send RIP updates (none)—Do not send RIP updates.

Broadcast RIPv1 packets (version-1)—Broadcast RIP version 1 packets.

- **Authentication Type**—Options include the following:

None–No authentication

Simple password authentication—Uses a text password that is included in the transmitted packet. The receiving router uses an authentication key (password) to verify the packet.

MD5 authentication (md5)—Creates an encoded checksum that is included in the transmitted packet. The receiving router uses an authentication key (password) to verify the packet's MD5 checksum.

- **Authentication Key**—Authentication password. If the password does not match, the packet is rejected. The password can be from 1 through 16 contiguous characters long and can include any ASCII strings.
- **Hold Down**—Seconds.
- **Message Size**—Number of route entries to be included in every RIP update message. To ensure interoperability with other vendors' equipment, use the standard of 25 route entries per message. Range: 25 through 255 entries. Default: 25 entries.
- **Metric In**—Metric to add to incoming routes when advertising into RIP routes that were learned from other protocols. Use this statement to configure the router to prefer RIP routes learned through a specific neighbor. Range: 1 through 16. Default: 1
- **Graceful Restart/Time/Disable**—Enter the time, or check disable.
- **Check Reserved**—Check to enable checking RIP reserved fields. Some of the reserved fields in RIP version 1 packets must be zero, while in RIP version 2 packets most of these reserved fields can contain nonzero values. By default, RIP discards version 1 packets that have nonzero values in the reserved fields and version 2 packets that have nonzero values in the fields that must be zero. This default behavior implements the RIP version 1 and version 2 specifications.

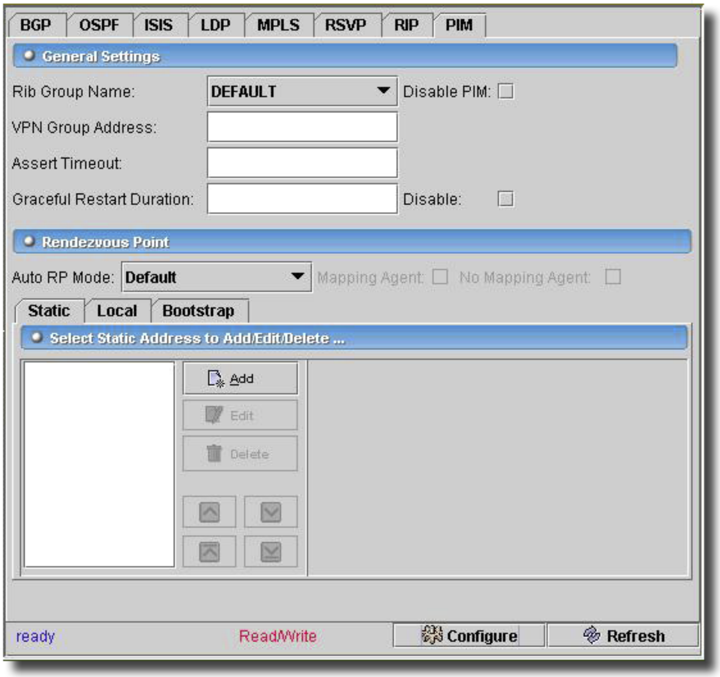
  If you find that you are receiving RIP version 1 packets with nonzero values in the reserved fields or RIP version 2 packets with nonzero values in the fields that must be zero, you can disable checking to receive these packets in spite of the fact that they are being sent in violation of the specifications in RFC 1058 and RFC 2453.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

PIM

This tab is the way to set up PIM interfaces.

Figure 13-61. Protocols -> Setup: PIM



General Settings

Rib Group Name: DEFAULT

Disable PIM: □

VPN Group Address:

Assert Timeout:

Graceful Restart Duration:

Disable: □

Rendezvous Point

Auto RP Mode: Default

Mapping Agent: □ No Mapping Agent: □

Select Static Address to Add/Edit/Delete ...

ready

Read/Write

This screen has the following fields:

- **Rib Group Name**—The name of the routing table group. The name must be one that you previously defined with the rib-group statement when editing/adding routing-options in the command line interface.
- **VPN Group Address**—The IP address of the VPN group.
- **Assert Timeout**—Enter the time. Multicast routers running PIM sparse mode often forward the same stream of multicast packets onto the same LAN through the rendezvous-point tree (RPT) and shortest-path tree (SPT). PIM assert messages help routers determine which router forwards the traffic and prunes the RPT for this group. By default, routers enter an assert cycle every 210 seconds. You can configure this assert timeout between 5 and 210 seconds.
- **Graceful Restart Duration**—Enter the time, or check disable. This is the time the routing platform waits to complete PIM sparse mode graceful restart.

Rendezvous Point

- **Auto RP Mode**—Configure automatic Rendezvous Point (RP) announcement and discovery. You can configure a mode-dynamic way of assigning RPs in a multicast network by means of auto-RP. When you configure auto-RP for a router, the router learns the address of the RP in the network automatically. Auto-RP operates in PIM version 1 and version 2.

NOTE:

If the router receives auto-RP announcements split across multiple messages, the router loses the information in the previous part of the message as soon as the next part of the message is received.

Options include

announce–Listen only for mapping packets. Also configures the router to advertise itself if it is an RP.

discovery–Listen only for mapping packets.

mapping–Router announce, listens for and generates mapping packets, and announces that the router is eligible to be an RP.

Mapping Agent and *No Mapping Agent* checkboxes also appear in this portion of the screen. Auto-RP specifications state that mapping agents should not send mapping messages if they receive messages from a mapping agent with a higher IP address. This process is called mapping agent election. However, some vendors' mapping agents continue to announce mappings, even in the presence of higher-addressed mapping agents. In other words, some mapping agents will always send mapping messages.

For compatibility, you can suppress mapping messages with the checkboxes. When *Mapping Agent* is unchecked, the mapping agent stops sending mapping messages if it receives messages from a mapping agent with a higher IP address.

Checking *No Mapping Agent* suppresses mapping messages. This means that the mapping agent always sends mapping messages even in the presence of higher-addressed mapping agents.

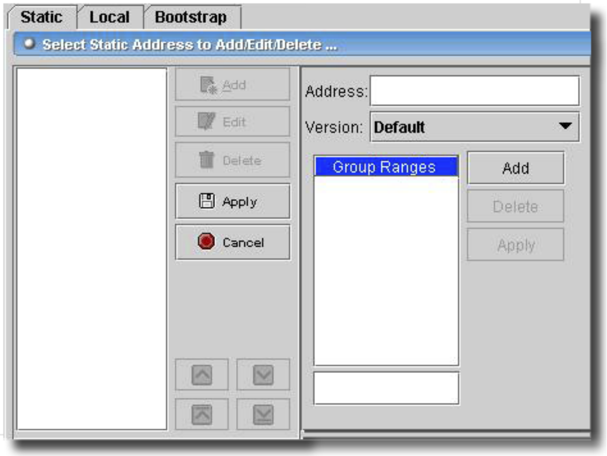
This panel also has three tabs:

- Static
- Local
- Bootstrap

Static

Select Static addresses to *Add / Edit / Delete* with those buttons on this tab. Use the up/down arrows to reorder them in the list on the left.

Figure 13-62. Protocols -> Setup: PIM (Static)



Address:

Version: Default

When you *Add* or *Edit*, the editor on the right appears with these fields:

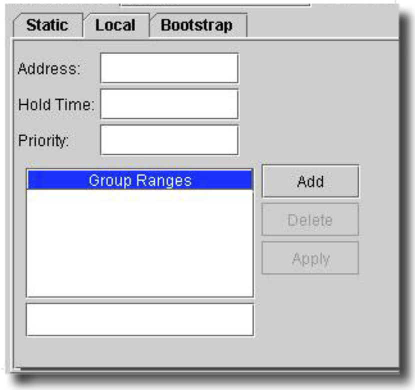
- **Address**—Configure the anycast rendezvous point (RP) addresses in the RP set. You can contribute multiple addresses in an RP set.
- **Version**—Select the PIM version. Default: 2.
- **Group Ranges**—Enter local group range of addresses (enter an address below the list and click *Add*. To change an existing address in the range, select a listed address, and change its characteristics in that lowest field, then click *Apply*. To remove an address, select it, then click *Delete*.

  This configures the address ranges of the multicast groups for which this router can be an RP. By default, the router is eligible to be the RP for all IPv4 or IPv6 groups (224.0.0.0/4 or FF70::/12 to FFF0::/12).

Local

This tab configures local parameters.

Figure 13-63.   Protocols -> Setup: PIM (Static)



It has the following fields:

- **Address**—Enter local address. This configures the router's local address for anycast rendezvous point (RP). If this statement is omitted, the application uses the router ID as this address.

- **Hold Time**—Enter local hold time in seconds. This specifies how long a neighbor should consider the sending router (this router) to be operative (up). Range: 0 through 255.

- **Priority**—Enter local priority. This configures the router's likelihood to be elected as the bootstrap router. A higher value corresponds to a higher priority. Range: 0 through a 32-bit number 0 (The router has the least likelihood of becoming the bootstrap router and sends packets with a priority of 0.)

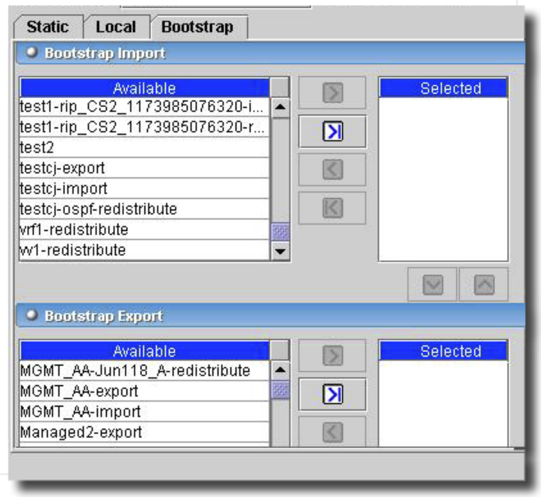
- **Group Ranges**—Enter local group range of addresses (enter an address below the list and click *Add*. To change an existing address in the range, select a listed address, and change its characteristics in that lowest field, then click *Apply*. To remove an address, select it, then click *Delete*.

  This configures the address ranges of the multicast groups for which this router can be an RP. By default, the router is eligible to be the RP for all IPv4 or IPv6 groups (224.0.0.0/4 or FF70::/12 to FFF0::/12).

Bootstrap

This tab configures parameters to control bootstrap routers and messages.

Figure 13-64. Protocols -> Setup: PIM (Static)



Bootstrap Import

Available	Selected
test1-rip_CS2_1173985076320-i...	
test1-rip_CS2_1173985076320-r...	
test2	
testcj-export	
testcj-import	
testcj-ospf-redistribute	
vrf1-redistribute	
w1-redistribute	

Bootstrap Export

Available	Selected
MGMT_AA-Jun118_A-redistribute	
MGMT_AA-export	
MGMT_AA-import	
Managed2-export	

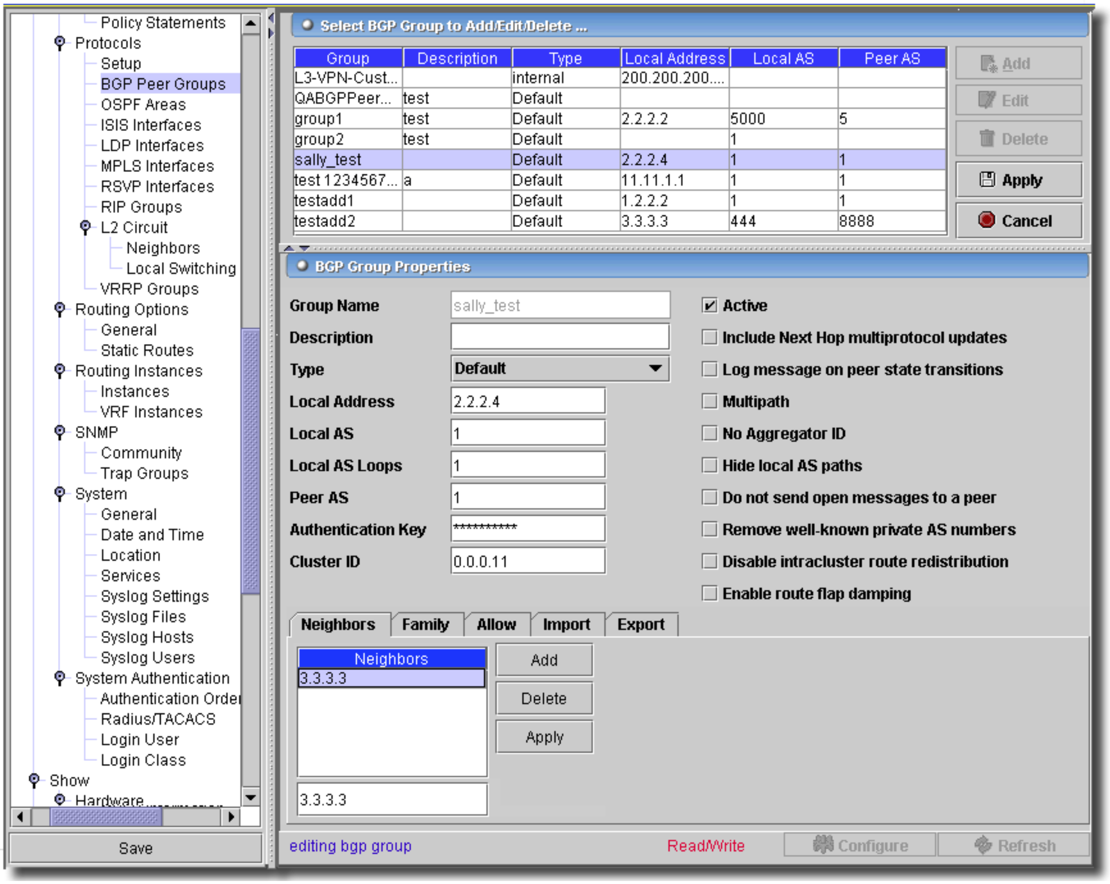
Click to select *Available* import / export bootstrap policies, and click the arrows to move the desired policies to the *Selected* side of this tab. Use the up/down arrows below the *Selected* policies to re-order their application. These control incoming and outgoing PIM bootstrap messages.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Protocols -> BGP Peer Groups

This panel manages BGP Peer Group settings.

Figure 13-65. Routing Protocols: BGP Peer Groups—Neighbors



Select BGP Group to Add/Edit/Delete ...

Group	Description	Type	Local Address	Local AS	Peer AS
L3-VPN-Cust...		internal	200.200.200....		
QABGPPeer...	test	Default			
group1	test	Default	2.2.2.2	5000	5
group2	test	Default		1	
sally_test		Default	2.2.2.4	1	1
test 1234567...	a	Default	11.11.1.1	1	1
testadd1		Default	1.2.2.2	1	1
testadd2		Default	3.3.3.3	444	8888

BGP Group Properties

Group Name	sally_test
Description	
Type	Default
Local Address	2.2.2.4
Local AS	1
Local AS Loops	1
Peer AS	1
Authentication Key	**********
Cluster ID	0.0.0.11

☑ Active
☐ Include Next Hop multiprotocol updates
☐ Log message on peer state transitions
☐ Multipath
☐ No Aggregator ID
☐ Hide local AS paths
☐ Do not send open messages to a peer
☐ Remove well-known private AS numbers
☐ Disable intracluster route redistribution
☐ Enable route flap damping

Neighbors | Family | Allow | Import | Export

Neighbors
3.3.3.3

Add
Delete
Apply

3.3.3.3

editing bgp group
Read/Write

Use the *Add*, *Edit* or *Delete* buttons to manage rows in the table at the top of this screen. Click *Export* to save a description of the listed items to a file. When you select a group to *Edit* or *Add* a new one, the editor panel in the lower part of the screen opens. Use *Export* to save these groups in a file. Click *Apply* in the top right of the screen to accept your edits, or *Cancel* to abandon them. The following are the editor's fields and checkboxes:

- **Group Name**—Name/Identifier for the group

- **Description**—A Text Description for the group

- **Type**—Type of peer group (internal/external)

- **Local Address**—Address of local end of BGP session

- **Local AS**—Local autonomous system number

- **Local AS Loops**—Maximum number of times this AS can be in an AS path (1 - 10).

- **Peer AS**—Peer autonomous system number (1 - 65,535),

- **Authentication Key**—MD5 authentication key.

- **Cluster ID**—An identifier for the peer group cluster.

Checkbox Options:

Check any of the following to enable them:

- Active—Mark this item as active.
- Include Next Hop multi protocol updates.
- Log message for peer state transitions.
- Mulitipath—Allow load sharing among multiple BGP paths.
- No Aggregator ID—Set router ID in aggregator path attribute to 0.
- Hide local AS paths—Hide this local AS in paths learned from this peering.
- Do not send open messages to a peer.
- Remove well-known private AS numbers.
- Disable intracluster route redistribution.
- Enable route flap damping.

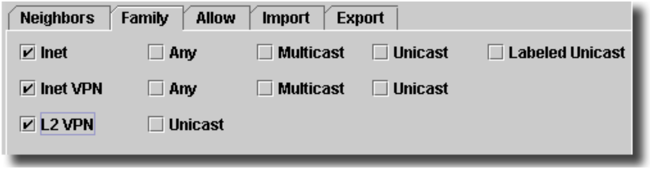
Neighbors

This tab lets you configure the list of neighbors for this group. Enter an IP address in the lowest field on the screen, and click A*dd* to list a neighbor, or select an existing IP address and click *Delete* to remove it from the list. Click A*pply* to accept the list as configured.

Family

This tab lets you configure the family for the selected BGP Peer Group.

Figure 13-66. Routing Protocols: BGP Peer Groups—Family



☑ Inet ☐ Any ☐ Multicast ☐ Unicast ☐ Labeled Unicast

☑ Inet VPN ☐ Any ☐ Multicast ☐ Unicast

☑ L2 VPN ☐ Unicast

You can select from among the following checkboxes. Check to activate these properties and configure protocol family attributes for NLRIs in updates.

- **Inet**—Options; Any, Multicast, Unicast, Labeled Unicast.

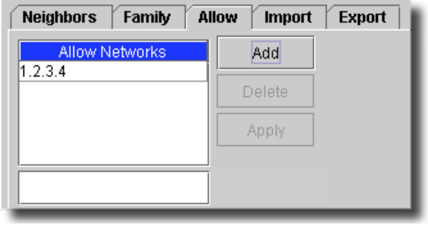
- **Inet VPN**—Options; Any, Multicast, Unicast.

- **L2 VPN**—Options; Unicast.

Allow

This tab lets you configure peer connections for specific networks.

Figure 13-67. Routing Protocols: BGP Peer Groups—Allow



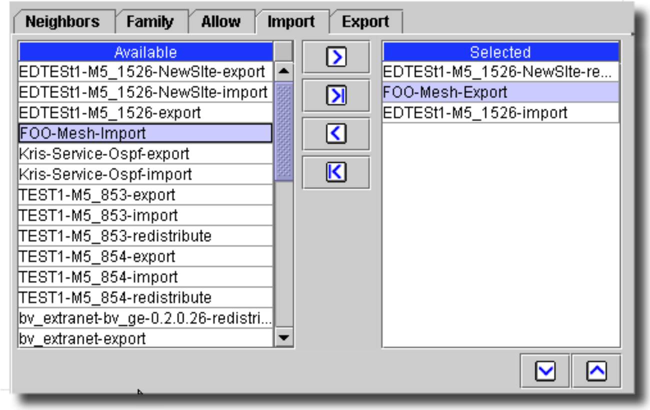
Allow Networks
1.2.3.4

Configure peer connection networks as you did in the Neighbors section, above.

Import

Here, you can configure an ordered list of import policies.

Figure 13-68. Routing Protocols: BGP Peer Groups—Import



Available
EDTESt1-M5_1526-NewSlte-export
EDTESt1-M5_1526-NewSlte-import
EDTESt1-M5_1526-export
FOO-Mesh-Import
Kris-Service-Ospf-export
Kris-Service-Ospf-import
TEST1-M5_853-export
TEST1-M5_853-import
TEST1-M5_853-redistribute
TEST1-M5_854-export
TEST1-M5_854-import
TEST1-M5_854-redistribute
bv_extranet-bv_ge-0.2.0.26-redistri...
bv_extranet-export

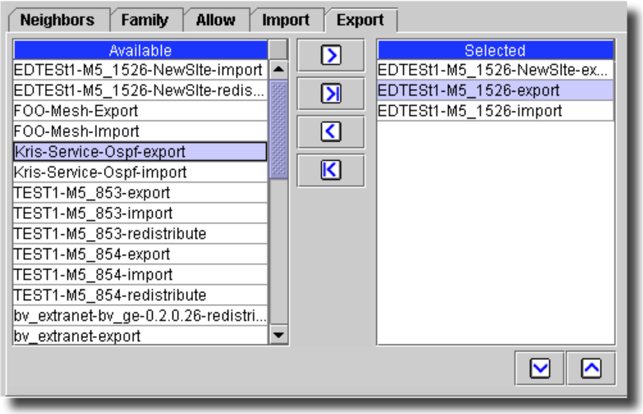
Selected
EDTESt1-M5_1526-NewSlte-re...
FOO-Mesh-Export
EDTESt1-M5_1526-import

Click an *Available* import policy, then click the arrows between *Available* and *Selected* to move that policy to the *Selected Column*. You can use the arrows below the *Selected* column to re-arrange selected policies.

Export

Here, you can configure an ordered list of export policies.

Figure 13-69. Routing Protocols: BGP Peer Groups—Export



Available
EDTESt1-M5_1526-NewSlte-import
EDTESt1-M5_1526-NewSlte-redis...
FOO-Mesh-Export
FOO-Mesh-Import
Kris-Service-Ospf-export
Kris-Service-Ospf-import
TEST1-M5_853-export
TEST1-M5_853-import
TEST1-M5_853-redistribute
TEST1-M5_854-export
TEST1-M5_854-import
TEST1-M5_854-redistribute
bv_extranet-bv_ge-0.2.0.26-redistri...
bv_extranet-export

Selected
EDTESt1-M5_1526-NewSlte-ex...
EDTESt1-M5_1526-export
EDTESt1-M5_1526-import

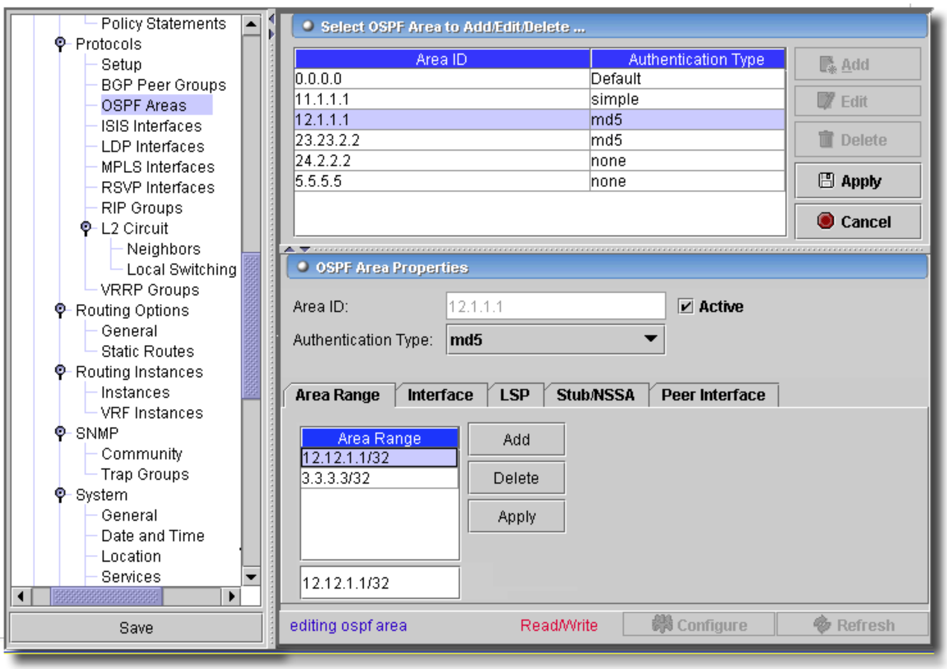
Click an *Available* export policy, then click the arrows between *Available* and *Selected* to move that policy to the *Selected Column*. You can use the arrows below the *Selected* column to re-arrange selected policies.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Protocols -> OSPF Areas

This screen manages OSPF Area settings.

Figure 13-70. Routing Protocols: BGP Peer Groups—Export



Area ID	Authentication Type
0.0.0.0	Default
11.1.1.1	simple
12.1.1.1	md5
23.23.2.2	md5
24.2.2.2	none
5.5.5.5	none

Area ID: 12.1.1.1 ☑ Active

Authentication Type: md5

Area Range
12.12.1.1/32
3.3.3.3/32

12.12.1.1/32

editing ospf area Read/Write

To *Add* or *Edit* existing OSPF areas to the table at the top of this screen, click those buttons. Click *Export* to save a description of the listed items to a file. Select a row and click *Delete* to remove it from the table. When you add or edit a row, the editor appears in the bottom of this screen. Click *Apply* to accept your edits, or *Cancel* to abandon them. The following are items you can configure for areas:

- **Area ID**—A unique identifier for an area (read-only when editing). Specify the area identifier for this router to use when participating in OSPF routing.

- **Authentication type**—Enable authentication and specify the authentication scheme for the backbone or area. Select from the pick list. Options include:

  none - Disable authentication.

  simple - Use a simple password. The password is included in the transmitted packet, making this method of authentication relatively insecure.

  md5 - Use the MD5 algorithm to create an encoded checksum of the packet. The encoded checksum is included in the transmitted packet. The receiving router uses the authentication key to verify the packet, discarding it if the digest does not match. This algorithm provides a more secure authentication scheme.

The bottom of the editor screen contains the following tabs for additional configuration:

- Area Range

- Interface
- LSP
- Stub/NSSA
- Peer Interface

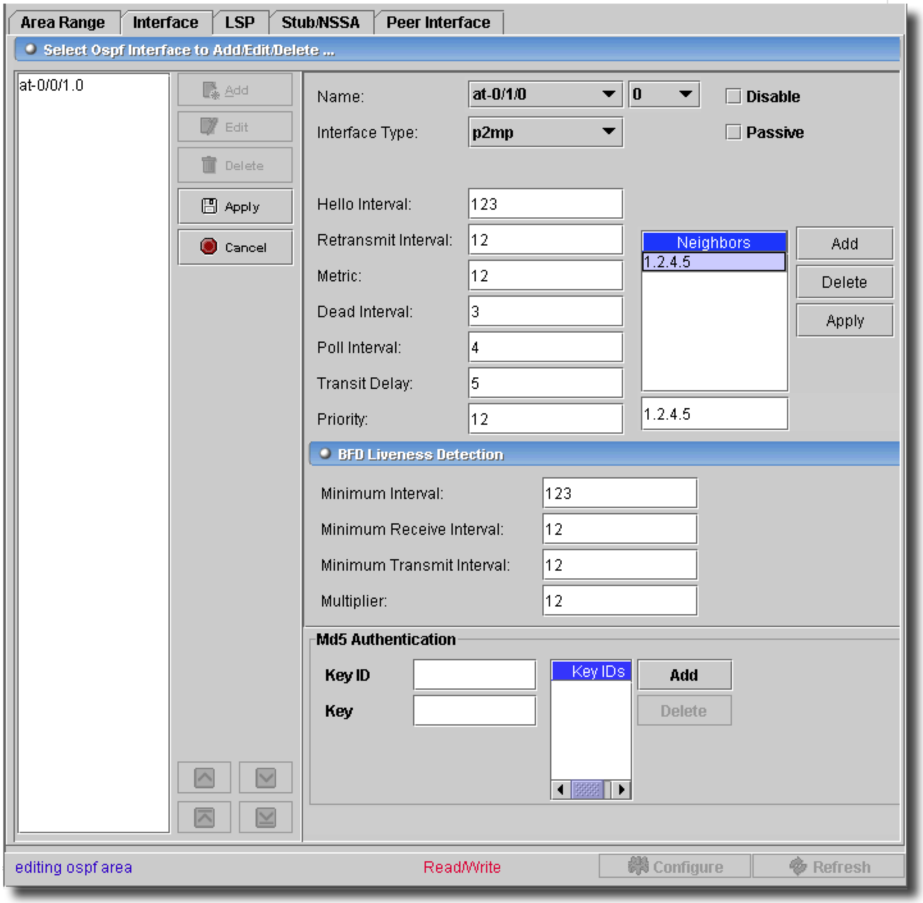
Area Range

- **Area Range**—Configure area ranges (network/mask-length). Enter an area range at the bottom of this table and click *Add* to enter it among those listed. Select a listed item and click *Delete* to remove it from the list. Click *Apply* to accept the entire list.

Interface

This tab lets you configure interfaces.

Figure 13-71. Routing Protocols: OSPF Interface



at-0/0/1.0

Name: at-0/1/0 0
□ Disable
Interface Type: p2mp
□ Passive

Hello Interval: 123
Retransmit Interval: 12
Metric: 12
Dead Interval: 3
Poll Interval: 4
Transit Delay: 5
Priority: 12

Neighbors
1.2.4.5

1.2.4.5

Minimum Interval: 123
Minimum Receive Interval: 12
Minimum Transmit Interval: 12
Multiplier: 12

Key ID
Key

editing ospf area
Read/Write

Click *Add* (or select an interface and click *Edit*) in the lower right portion of the screen, and the right screen becomes an editor for the interface. Click *Delete* to remove a selected interface from those listed. This editor has the following to configure:

- **Name**—Select an interface to configure.

- **Interface Type**—Select type of interface

- **Disable**—Disable OSPF on this interface.

- **Passive**—Do not run OSPF, but advertise it

- **Simple Password**—Enter an authentication key, if you chose *Simple* as the authentication type above this tab. This field does not appear if you select something else.

- **Hello Interval**—1 - 255 seconds. Here, you can specify how often the router sends hello packets out the interface. The hello interval must be the same for all routers on a shared logical IP network.

- **Retransmit Interval**—1 - 65535 seconds. This specifies how long the router waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements to an interface's neighbors.

- **Metric**—1 - 65535. Cost of an OSPF interface. The cost is a routing metric that is used in the link-state calculation.

- **Dead Interval**—1 - 65535 seconds. This specifies how long OSPF waits before declaring that a neighboring router is unavailable. This is an interval during which the router receives no hello packets from the neighbor.

- **Poll Interval**—1 - 65535. For non broadcast interfaces only, specify how often the router sends hello packets out of the interface before it establishes adjacency with a neighbor.

- **Transit Delay**—1 - 65535 seconds. This sets the estimated time required to transmit a link-state update on the interface. When calculating this time, you should account for transmission and propagation delays.

- **Priority**—Designated router priority (0 - 255).

BFD Liveness Detection

- **Minimum Interval**— Minimum transmit and receive interval (1 - 255000 milliseconds).

- **Minimum Receive Interval**— 1 - 255000 milliseconds.

- **Minimum Transmit Interval**—1 - 255000 milliseconds.

- **Multiplier**— Detection time multiplier (1 - 255).

- **Neighbors**—NBMA neighbor. Enter a neighbor in the bottom field, then click *Add* to add it to those listed (or click *Delete* to remove one from the list). Click *Apply* to accept the list.

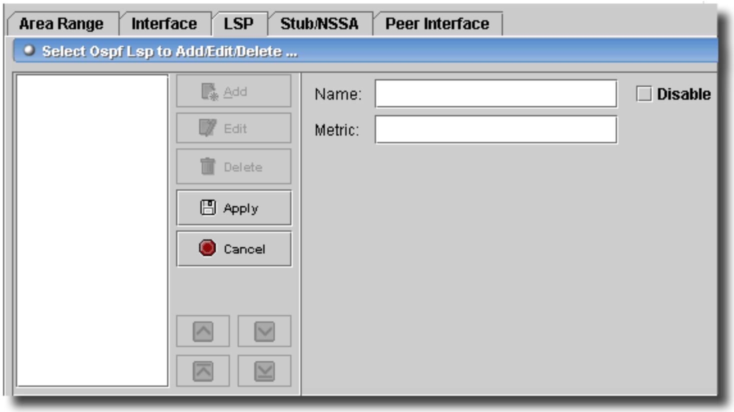
Md5 Panel

If applicable, enter a *Key ID* and *Key* in the provided fields, then click *Add* to include these in the Key IDs listed. You can also select a listed key, and click *Delete* to remove it.

LSP

This tab lets you configure LSPs for the selected OSPF interface.

Figure 13-72. Routing Protocols: OSPF LSP

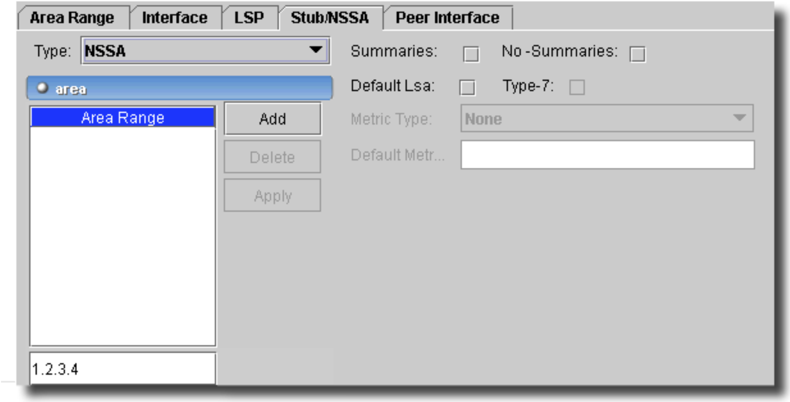


This panel lets you enter the *Name* of label-switched path to be advertised, and the Interface metric (1 - 65535). click *Add* to add an LSP to those listed (or click *Edit* to alter an existing, selected LSP, or *Delete* to remove one from the list) then enter a *Name* and *Metric*. Click *Apply* to accept your edits, or *Cancel* to abandon them. Click the checkbox in the *Enable* column to enable the LSP.

Stub/NSSA

This tab lets you configure Stub/NSSA for the selected OSPF interface.

Figure 13-73. Routing Protocols: OSPF Stub/NSSA



Type: NSSA

Summaries: □ No -Summaries: □

Default Lsa: □ Type-7: □

Metric Type: None

Default Metr...

1.2.3.4

Configure the following with this tab:

- **Type**—Select from the pick list:

  Stub - Configure a stub area

  NSSA - Configure a not-so-stubby area

- **Summaries/No-Summaries**—Check to activate. (These are mutually exclusive, but you can also activate neither). Summaries flood summary LSAs into this stub/nssa area.

- **Default Lsa**—Check to activate.

- **Type-7**—Flood type 7 default LSA if no-summaries is configured. Check to activate.

- **Area Range**—Configure NSSA area ranges. Enter a range below the list panel, then click *Add* (click *Edit* to alter a selected range, or *Delete* to remove it).

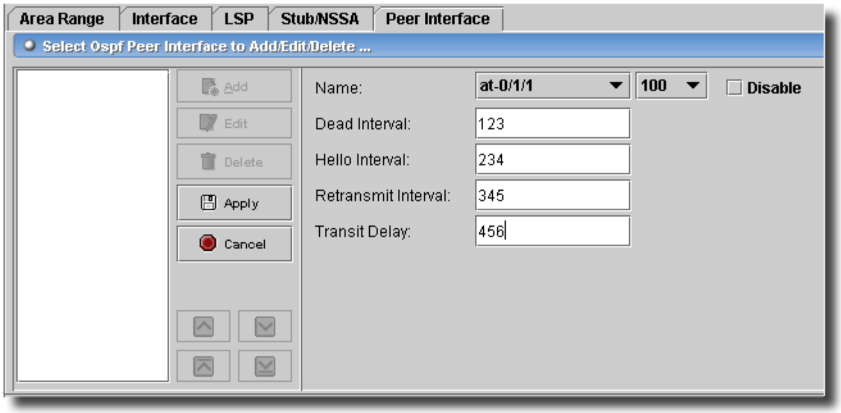
- **Metric Type**—External metric type for the default type 7 LSA (1 - 2). Select from the pick list.

- **Default Metric**—Metric for the default route in this stub/nssa area (1 - 16777215). Enter a default in the field.

Peer Interface

This tab lets you configure peer interfaces for the selected OSPF interface.

Figure 13-74. Routing Protocols: OSPF Peer Interface



Name: at-0/1/1 100 □ Disable

Dead Interval: 123

Hello Interval: 234

Retransmit Interval: 345

Transit Delay: 456

Click *Add* (or select an interface listed on the left and click *Edit*) to open the editor in the right panel. Select an interface and click *Delete* to remove it from the list. Click *Apply* to accept your edits; *Cancel* abandons them. Configure the following with this tab:

- **Name**—Use the pick lists to locate an available interface.

- **Disable**—Check to disable OSPF on this interface.

- **Dead Interval**—1 - 65535 seconds. This specifies how long OSPF waits before declaring that a neighboring router is unavailable. This is an interval during which the router receives no hello packets from the neighbor.

- **Hello Interval**—1 - 255 seconds. This specifies how often the router sends hello packets out the interface. The hello interval must be the same for all routers on a shared logical IP network.

- **Retransmit Interval**—1 - 65535 seconds. This specifies how long the router waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements to an interface's neighbors.

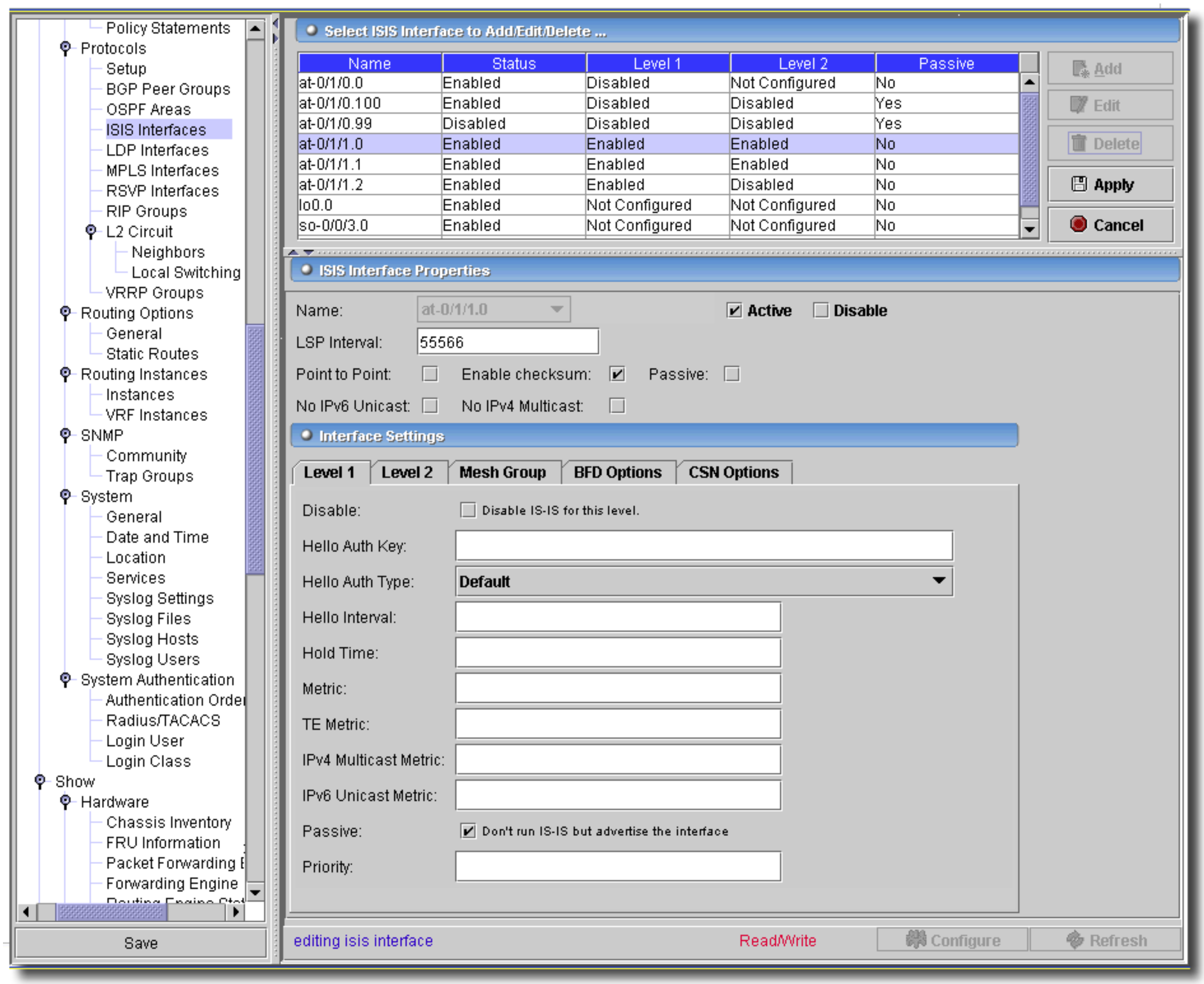
- **Transit Delay**—1 - 65535 seconds. This sets the estimated time required to transmit a link-state update on the interface. When calculating this time, you should account for transmission and propagation delays.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Protocols -> ISIS Interfaces

This screen manages ISIS Interface settings.

Figure 13-75. Routing Protocols: ISIS Levels 1 & 2



Select ISIS Interface to Add/Edit/Delete ...

Name	Status	Level 1	Level 2	Passive
at-0/1/0.0	Enabled	Disabled	Not Configured	No
at-0/1/0.100	Enabled	Disabled	Disabled	Yes
at-0/1/0.99	Disabled	Disabled	Disabled	Yes
at-0/1/1.0	Enabled	Enabled	Enabled	No
at-0/1/1.1	Enabled	Enabled	Enabled	No
at-0/1/1.2	Enabled	Enabled	Disabled	No
lo0.0	Enabled	Not Configured	Not Configured	No
so-0/0/3.0	Enabled	Not Configured	Not Configured	No

ISIS Interface Properties

Name: at-0/1/1.0 ☑ Active □ Disable

LSP Interval: 55566

Point to Point: □ Enable checksum: ☑ Passive: □

No IPv6 Unicast: □ No IPv4 Multicast: □

Interface Settings

Level 1 | Level 2 | Mesh Group | BFD Options | CSN Options

Disable: □ Disable IS-IS for this level.

Hello Auth Key:

Hello Auth Type: Default

Hello Interval:

Hold Time:

Metric:

TE Metric:

IPv4 Multicast Metric:

IPv6 Unicast Metric:

Passive: ☑ Don't run IS-IS but advertise the interface

Priority:

editing isis interface Read/Write

Use the *Add Edit* and *Remove* buttons to manage rows in this table. Click *Apply* to accept your edits and *Cancel* to abandon them. When you add or edit an interface listed, an editor appears in the lower portion of the screen. The following are its fields:

- **Name**—Interface or Unit to which settings apply.

LSP Interval— Interval between LSP transmissions (milliseconds)

The following are checkbox options. Check to activate them:

- **Disable ISIS**—For the named interface/unit (disable)

- **Passive**—Do not run IS-IS, but advertise it (passive)

- **Enable checksum**—For packets on this interface (checksum)

- **No IPv4 Multicast**—Do not include this interface in the IPv4 multicast topology
- **No IPv6 Multicast**—Do not include this interface in the IPv6 unicast topology
- **Point to Point**—Treat interface as point to point

The following tabs let you do additional configuration for ISIS interfaces:

Level 1 and 2

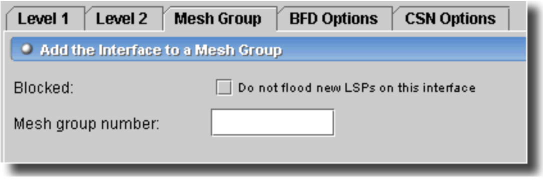
These tabs have the following fields:

- **Disable**—Disable IS-IS for given level.
- **Hello Auth Key**—Authentication key (password) for hello packets.
- **Hello Auth Type**—Authentication type for hello packets (*MD5/Simple*).
- **Hello Interval**—Interval between hello packet transmissions (1 - 21,845 seconds).
- **Hold Time**—Time after which neighbors think the interface is down (1. 65,535 seconds).
- **Metric**—Metric for this level (0 - 16,777,215).
- **TE Metric**—Traffic engineering metric (0 - 16,777,215).
- **Ipv4 Multicast Metric**—IPv4 multicast metric for this level (0 - 16,777,215).
- **Ipv6 Unicast Metric**—IPv6 unicast metric for this level (0 - 16,777,215).
- **Passive**—Don't run IS-IS at this level, but advertise the interface.
- **Priority**—The priority for this interface.

Mesh Group

This tab lets you add the interface to a mesh group.

Figure 13-76. Routing Protocols: ISIS Mesh Group



● Add the Interface to a Mesh Group

Blocked: □ Do not flood new LSPs on this interface

Mesh group number:

This tab has the following you can configure:

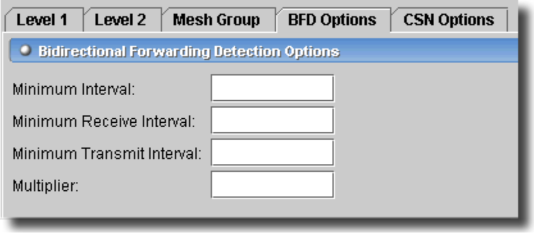
Blocked—Do not flood new LSPs on this interface (when checked).

Group Number—Mesh group number for this interface.

BFD Options

This tab configures Bidirectional Forwarding Detection (BFD) options.

Figure 13-77. Routing Protocols: ISIS BFD Options



Bidirectional Forwarding Detection Options

Minimum Interval:

Minimum Receive Interval:

Minimum Transmit Interval:

Multiplier:

This screen has the following fields:

- **Minimum Interval**—Minimum transmit and receive interval (1 - 255,000 milliseconds).

- **Min Receive Interval**—Minimum receive interval (1 - 255,000 milliseconds).

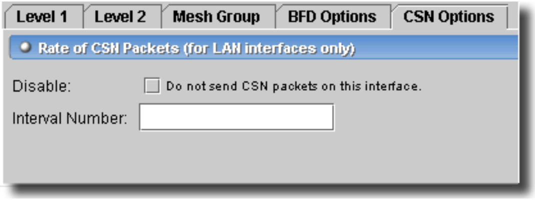
- **Min Transmit Interval**—Minimum transmit interval (1 - 255,000 milliseconds).

- **Multiplier**—Detection time multiplier (1 - 255).

CSN Options

This tab configures the rate of complete sequence number (CSN) packets (for LAN interfaces only).

Figure 13-78. Routing Protocols: ISIS BFD Options



Rate of CSN Packets (for LAN interfaces only)

Disable: □ Do not send CSN packets on this interface.

Interval Number:

This screen has the following fields:

Disable—Do not send CSN packets on this interface.

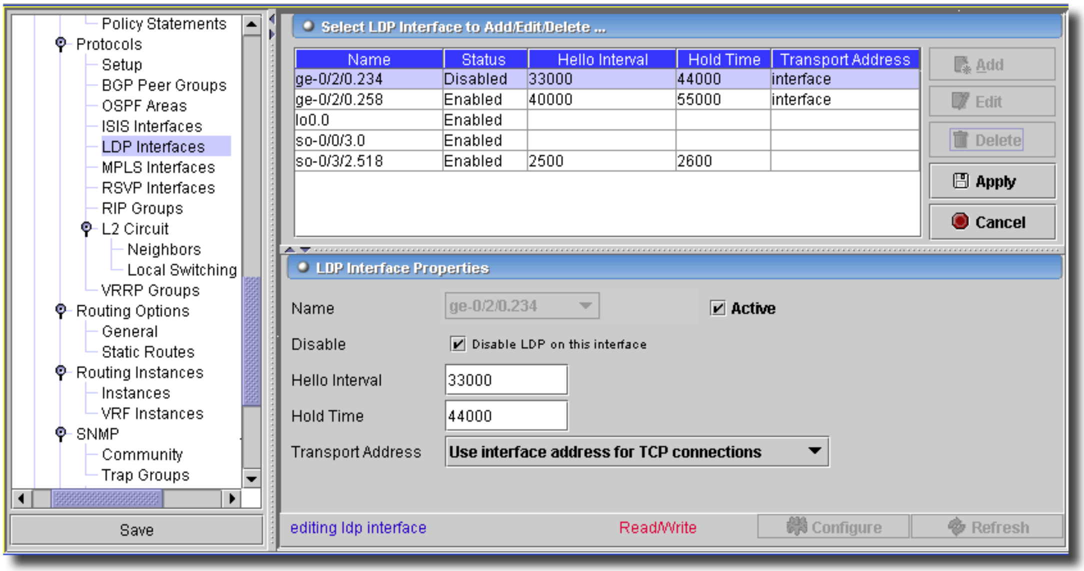
Interval Number—Interval between CSN packets (1 - 65,535 seconds).

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Protocols -> LDP Interfaces

This screen manages LDP settings.

Figure 13-79. Routing Protocols: LDP



Name	Status	Hello Interval	Hold Time	Transport Address
ge-0/2/0.234	Disabled	33000	44000	interface
ge-0/2/0.258	Enabled	40000	55000	interface
lo0.0	Enabled			
so-0/0/3.0	Enabled			
so-0/3/2.518	Enabled	2500	2600	

Name: ge-0/2/0.234 ☑ Active

Disable: ☑ Disable LDP on this interface

Hello Interval: 33000

Hold Time: 44000

Transport Address: Use interface address for TCP connections

editing ldp interface Read/Write

Use the *Add*, *Edit*, *Delete*, or *Export* buttons to manage rows in this table. The following are the fields you can alter for the selected row:

- **Name**—Interface or Unit to which settings apply.

- **Disable**—Check to disable IDP for the named interface/unit.

- **Hello Interval**—Hello interval (1 - 65,535 seconds).

- **Hold Time**—Hello hold time (1 - 65,535 seconds).

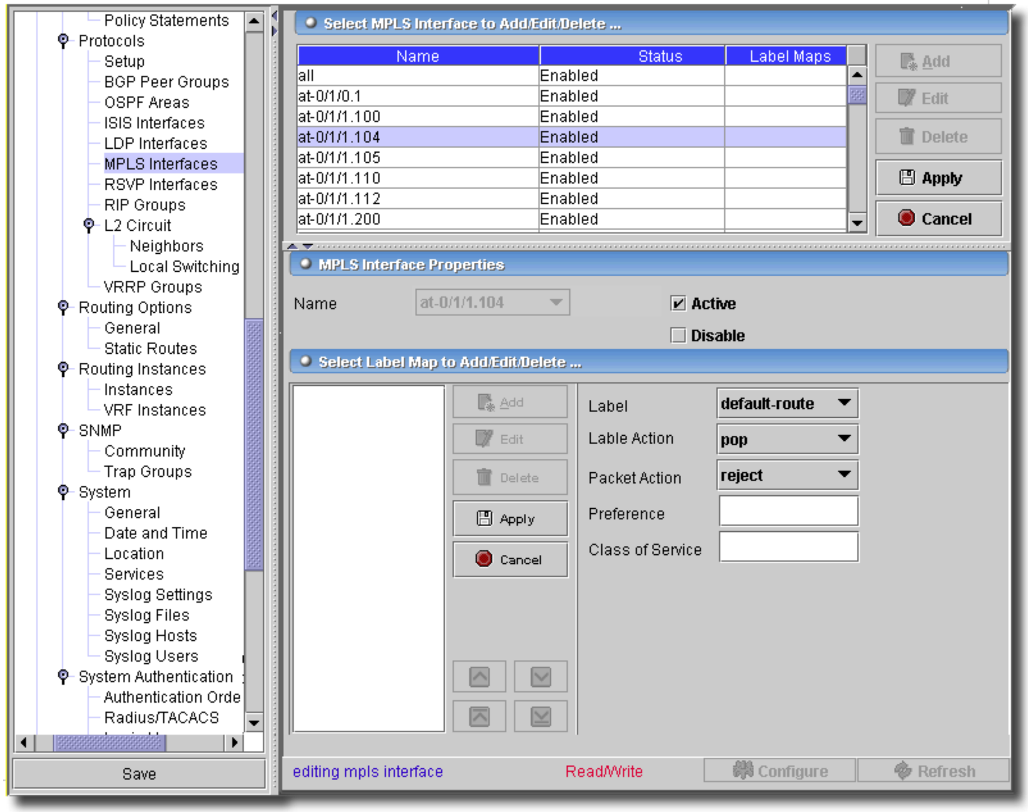
- **Transport Address**—Address used for TCP sessions (*Use interface address for TCP connections* or *Use router ID for TCP connections*)

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Protocols -> MPLS Interfaces

This screen manages MPLS settings.

Figure 13-80.   Routing Protocols: MPLS



Name	Status	Label Maps
all	Enabled	
at-0/1/0.1	Enabled	
at-0/1/1.100	Enabled	
at-0/1/1.104	Enabled	
at-0/1/1.105	Enabled	
at-0/1/1.110	Enabled	
at-0/1/1.112	Enabled	
at-0/1/1.200	Enabled	

Name at-0/1/1.104

☑ Active

□ Disable

Label default-route

Lable Action pop

Packet Action reject

Preference

Class of Service

editing mpls interface   Read/Write

Use the *Add*, *Edit*, *Delete*, or *Export* buttons to manage rows in the *Select MPLS Interface to Add/Edit/Delete* table. The following are fields you can alter in the selected interface:

- **Name**—Interface or Unit to which settings apply. Select from a pick list.

- **Disable**—Check to disable IDP for the named interface/unit.

Select Label Map to Add / Edit / Delete

Use the *Add* or *Remove* buttons to manage Label Map rows in the table. The following are fields you can alter in the selected Label Map:

- **Label**—Select from a pick list (read-only when editing existing)

- **Label Action**—Select from the pick list (*pop*, *swap*, *swap-push*—and when you select *Swap* or *Swap-Push*, additional fields appear to configure those).

- **Packet Action**—Select from the pick list (*reject*, *discard*, or *next hop*).

- **Preference**—Enter an integer. (0 - 4,294,967,295).

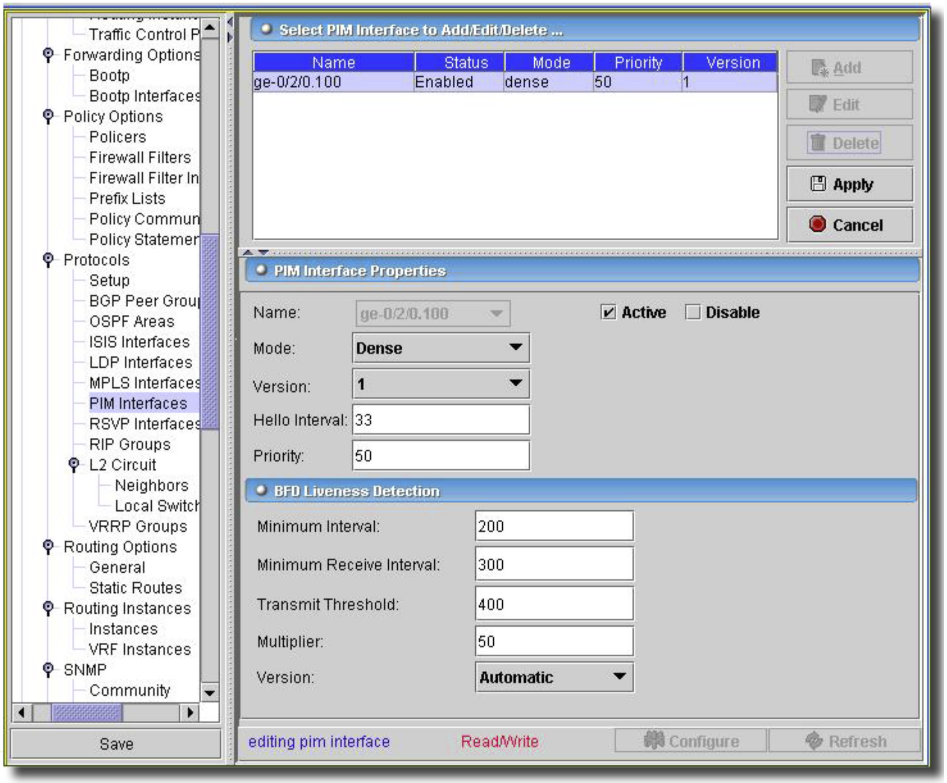
- **Class of Service**—Enter an integer (0 - 7).

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Protocols -> PIM Interfaces

This screen manages PIM interfaces for the selected device.

Figure 13-81. Protocols -> PIM Interfaces



Select PIM Interface to Add/Edit/Delete ...

Name	Status	Mode	Priority	Version
ge-0/2/0.100	Enabled	dense	50	1

PIM Interface Properties

Name: ge-0/2/0.100 ☑ Active □ Disable

Mode: Dense

Version: 1

Hello Interval: 33

Priority: 50

BFD Liveness Detection

Minimum Interval: 200

Minimum Receive Interval: 300

Transmit Threshold: 400

Multiplier: 50

Version: Automatic

editing pim interface ReadWrite

Click *Add* to configure a new interface, or *Edit* to modify a selected, existing interface. If you want to remove a listed interface, select it and click *Delete*. Click *Export* to save a file describing items listed here. When you *Add* or *Edit*, the editor appears with these fields:

PIM Interface Properties

- **Name**—The interface's identifier. Click *Active* or *Disable* to activate or disable this interface.
- **Mode**—Select from the pick list to configure PIM to operate in *sparse*, *dense*, or *sparse-dense* mode.
- **Version**— Select a PIM version from the pick list.

- **Hello Interval**—Enter the number of seconds to designate how often the router sends PIM hello packets out of an interface. Range: 0 through 255
- **Priority**—Enter the router's likelihood to be elected as the bootstrap router. A higher value corresponds to a higher priority. Range: 0 through a 32-bit number. Default: 0. (The router has the least likelihood of becoming the bootstrap router and sends packets with a priority of 0.)

BFD Liveness Detection

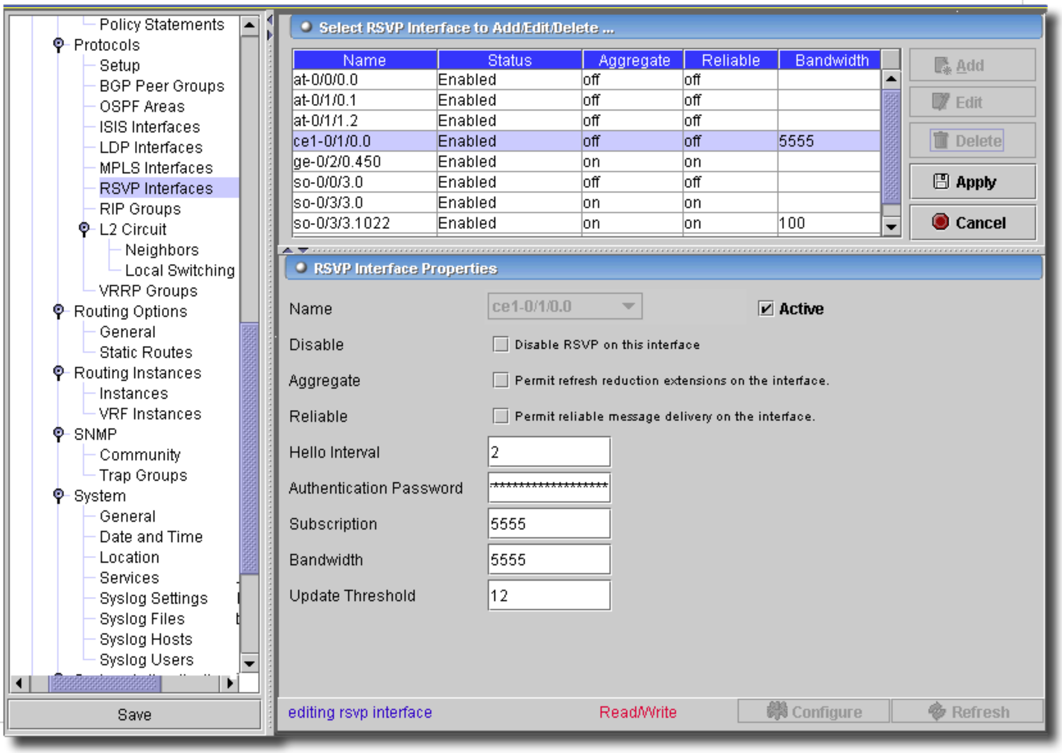
- **Minimum Interval**—The bidirectional forwarding detection (BFD) minimum interval timer. This timer specifies the same value for both the minimum transmit interval and minimum receive interval for the bfd-liveness-detection statement. This specifies the minimum transmit and receive interval. Range: 1 through 255,000 milliseconds
- **Minimum Receive Interval**—The BFD minimum receive interval timer. This timer specifies only the minimum receive interval for the bfd-liveness-detection statement. Range: 1 through 255,000 milliseconds
- **Transmit Threshold**—Specifies only the minimum transmit interval for the bfd-liveness-detection statement. Range: 1 through 255,000 milliseconds
- **Multiplier**—The multiplier for BFD timers; the detection time multiplier. Range: 1 through 255
- **Version**—The PIM version (*0, 1, Automatic*).

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Protocols -> RSVP Interfaces

This screen manages RSVP interface settings.

Figure 13-82. Routing Protocols: RSVP Interfaces



Name	Status	Aggregate	Reliable	Bandwidth
at-0/0/0.0	Enabled	off	off	
at-0/1/0.1	Enabled	off	off	
at-0/1/1.2	Enabled	off	off	
ce1-0/1/0.0	Enabled	off	off	5555
ge-0/2/0.450	Enabled	on	on	
so-0/0/3.0	Enabled	off	off	
so-0/3/3.0	Enabled	on	on	
so-0/3/3.1022	Enabled	on	on	100

Name ce1-0/1/0.0 ☑ Active

Disable ☐ Disable RSVP on this interface

Aggregate ☐ Permit refresh reduction extensions on the interface.

Reliable ☐ Permit reliable message delivery on the interface.

Hello Interval 2

Authentication Password ********************

Subscription 5555

Bandwidth 5555

Update Threshold 12

editing rsvp interface Read/Write

Use the *Add*, *Edit*, *Delete*, *Export* buttons to manage the list of interfaces in the table at the top of this screen. Click *Export* to save a file describing items listed here. When you are done adding or editing, click *Apply* to accept your edits, or *Cancel* to abandon them. When you add or edit, the editor at the bottom of this screen opens, letting you modify the following:

- **Name**—Interface or Unit to which settings apply.

- **Disable**—Check to disable RSVP for the named interface/unit.

- **Aggregate**—Check to permit refresh reduction extensions on the interface.

- **Reliable**—Check to permit reliable message delivery on the interface.

- **Hello Interval**—Hello interval (0 - 60 seconds).

- **Authentication Password**—Authentication key.

- **Subscription**—Link bandwidth percentage for RSVP reservation (0 - 65000).

- **Bandwidth**—Available bandwidth (bps) for the interface.

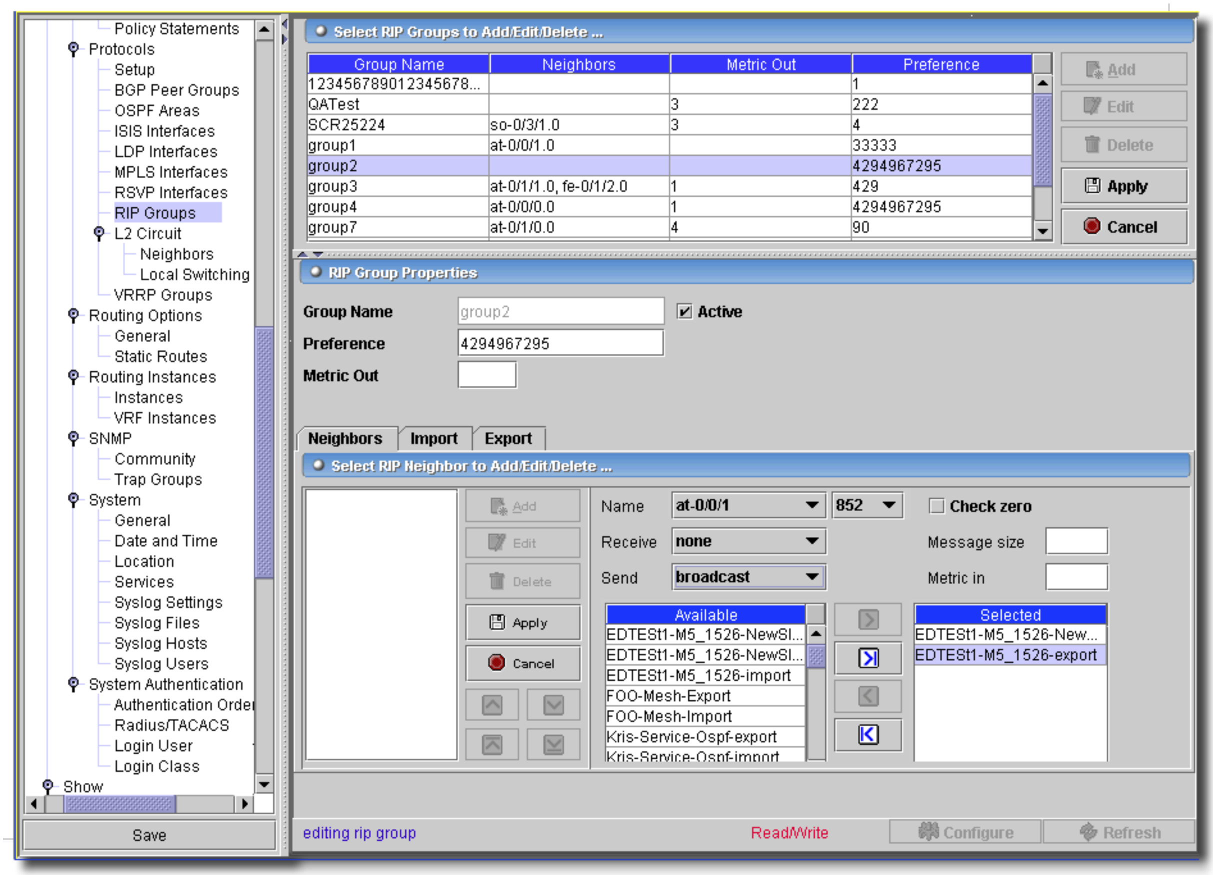
- **Update Threshold**—Percent change in reserved bandwidth to trigger IGP update (1 - 20).

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Protocols -> RIP Groups

This screen controls RIP groups.

Figure 13-83. Protocols -> RIP Groups



Group Name	Neighbors	Metric Out	Preference
123456789012345678...			1
QATest		3	222
SCR25224	so-0/3/1.0	3	4
group1	at-0/0/1.0		33333
group2			4294967295
group3	at-0/1/1.0, fe-0/1/2.0	1	429
group4	at-0/0/0.0	1	4294967295
group7	at-0/1/0.0	4	90

Group Name group2 ☑ Active

Preference 4294967295

Metric Out

Name at-0/0/1 852 □ Check zero

Receive none Message size

Send broadcast Metric in

Available	Selected
EDTESt1-M5_1526-NewSl...	EDTESt1-M5_1526-New...
EDTESt1-M5_1526-NewSl...	EDTESt1-M5_1526-export
EDTESt1-M5_1526-import	
FOO-Mesh-Export	
FOO-Mesh-Import	
Kris-Service-Ospf-export	
Kris-Service-Ospf-import	

editing rip group Read/Write

Click *Add* or *Edit* a selected row to open the editor in the bottom panel. Click *Apply* to accept your edits, or *Cancel* to abandon them. Use *Export* to save these items in a file. The editor has the following fields:

Group Name—Name of the RIP Group to configure.

Preference—Preference of routes learned by this group.

Metric Out—Default metric of exported routes (1 - 15).

Neighbors Tab

Neighbor configuration has the following fields, with a similar *Add* policy to the upper screen:

- **Name**—Interface name

- **Receive**—Configure RIP receive options:

  both - Accept both RIPv1 and RIPv2 packets

  none - Do not receive RIP packets

  version-1 - Accept RIPv1 packets only

  version-2 - Accept only RIPv2 packets

- **Send**—Configure RIP send options:

  broadcast - Broadcast RIPv2 packets (RIPv1 compatible)

  multicast - Multicast RIPv2 packets

  none - Do not send RIP updates

  version-1 - Broadcast RIPv1 packets

Check zero—Check reserved fields on incoming RIPv1 packets

Message Size—Number of route entries per update message (25 - 255)

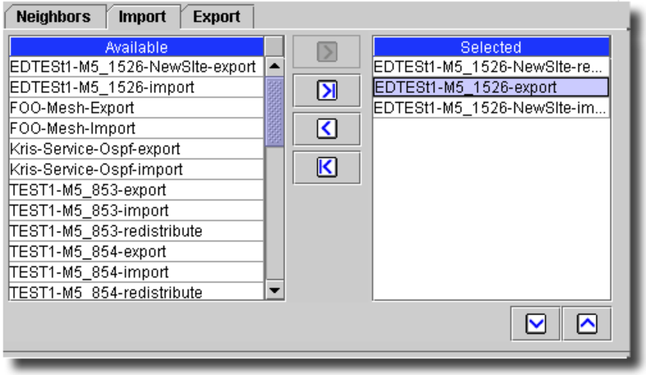
Metric In—Metric value to add to incoming routes (1 - 15)

Note that you can re-order items with the arrows below or to the right of where they are listed.

Import Tab - Import policy

Use this tab to select policies to import.

Figure 13-84. RIP Policy Import



Available

EDTESt1-M5_1526-NewSIte-export
EDTESt1-M5_1526-import
FOO-Mesh-Export
FOO-Mesh-Import
Kris-Service-Ospf-export
Kris-Service-Ospf-import
TEST1-M5_853-export
TEST1-M5_853-import
TEST1-M5_853-redistribute
TEST1-M5_854-export
TEST1-M5_854-import
TEST1-M5_854-redistribute

Selected

EDTESt1-M5_1526-NewSIte-re...
EDTESt1-M5_1526-export
EDTESt1-M5_1526-NewSIte-im...

Notice that, in addition to the arrows moving policies from the *Available* to the *Selected* areas, the arrows below and to the right reorder the listed selected policies.

Export Tab - Export policy

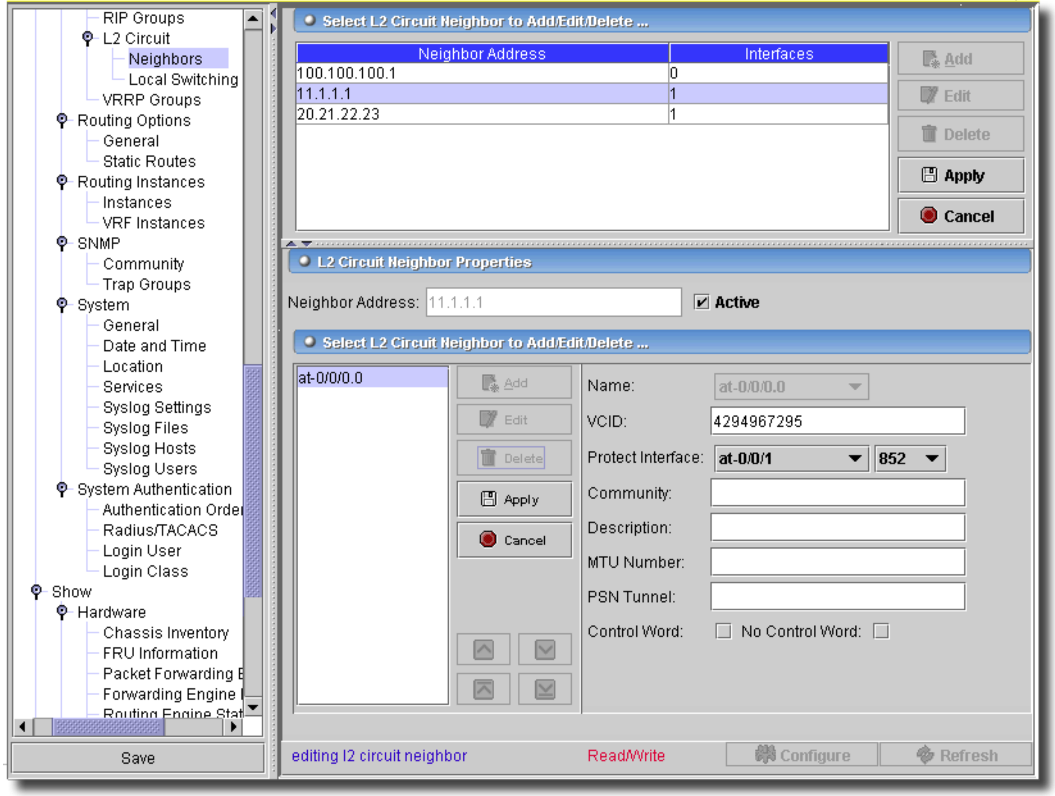
This tab is similar to the *Import* tab.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information appears.

L2 Circuit -> Neighbors

This screen manages Layer 2 Circuit neighbors.

Figure 13-85. L2 Circuit -> Neighbors



Neighbor Address	Interfaces
100.100.100.1	0
11.1.1.1	1
20.21.22.23	1

Neighbor Address: 11.1.1.1 ☑ Active

at-0/0/0.0

Name: at-0/0/0.0

VCID: 4294967295

Protect Interface: at-0/0/1 852

Community:

Description:

MTU Number:

PSN Tunnel:

Control Word: □ No Control Word: □

editing l2 circuit neighbor Read/Write

The top of this screen lists Layer 2 circuit neighbors. Click *Add* (or select a row and click *Edit*) to see the editor in the lowest panel. Select a row and click *Delete* to remove it. Use *Export* to save a description of these items in a file. Click *Apply* to accept your edits, or *Cancel* to accept them. The editor has the following fields:

- **Neighbor Address**—The IP address of the neighbor.

- **Active**—Check this to activate the neighbor.

Edit L2 Circuit Interfaces

Like the top panel, this list of L2 Circuit neighbor (on the left) lets you *Add* or *Edit* (selected) circuit interfaces (and *Delete* them). The editor appears on the right, with the following fields.

- **Interface Name**—Interface forming the Layer 2 circuit.

- **VCID**—An identifier for this Layer 2 circuit (1 - 4294967295). This is mandatory.

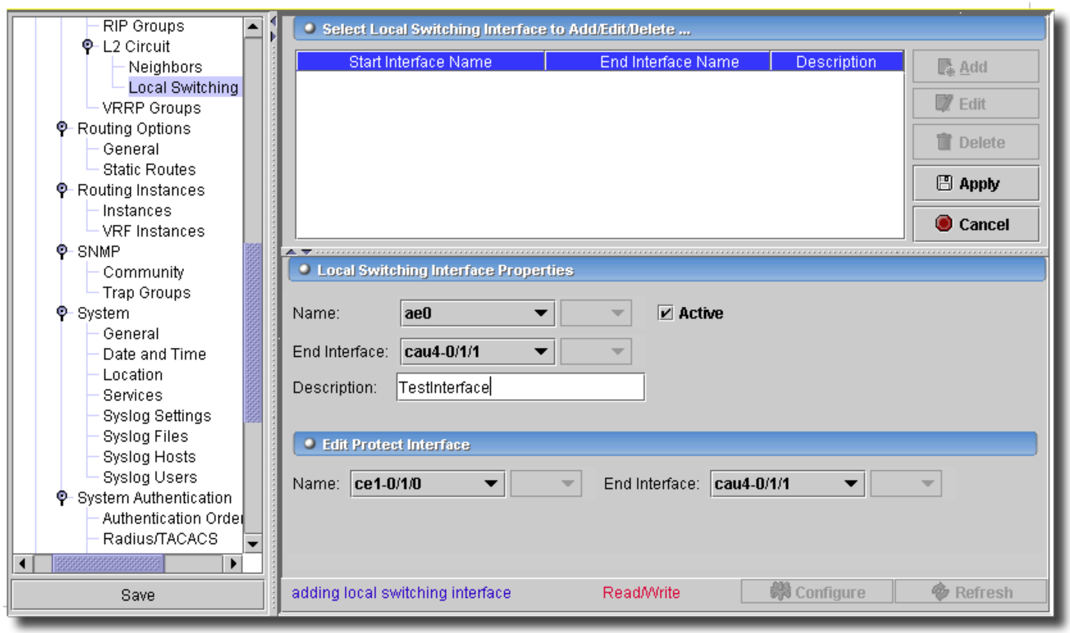
- **Protect Interface**—Name of the protect interface.
- **Community Name**—Community associated with this Layer 2 circuit.
- **Description**—Text description of the Layer 2 circuit.
- **MTU Number**—MTU to be advertised for this Layer 2 circuit (512 - 65535).
- **PSN Tunnel**—Endpoint of the transport tunnel on the remote PE.
- **Control Word / No Control Word**—Check *Control Word* to enable the use of control word. Check *No Control Word* to disable control word.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

L2 Circuit -> Local Switching

This screen configures local switching interfaces for the selected equipment.

Figure 13-86. L2 Circuit -> Local Switching



Name: ae0 ☑ Active

End Interface: cau4-0/1/1

Description: TestInterface

Edit Protect Interface

Name: ce1-0/1/0 End Interface: cau4-0/1/1

adding local switching interface Read/Write

The top of this screen lists Layer 2 local switching interfaces. Click *Add* (or select a row and click *Edit*) to see the editor in the lowest panel. Select a row and click *Delete* to remove it. Click *Export* to save a description of these items in a file. Click *Apply* to accept your edits, or *Cancel* to accept them. The editor has the following fields:

- **Interface Name**—Interface name. Cannot edit once configured. Click the *Active* checkbox to activate this interface.

- **End Interface Name**—Interface name of the other end point.

- **Description**—A text description of the Layer 2 circuit.

- **Protect Interface**—Name of protect interface.

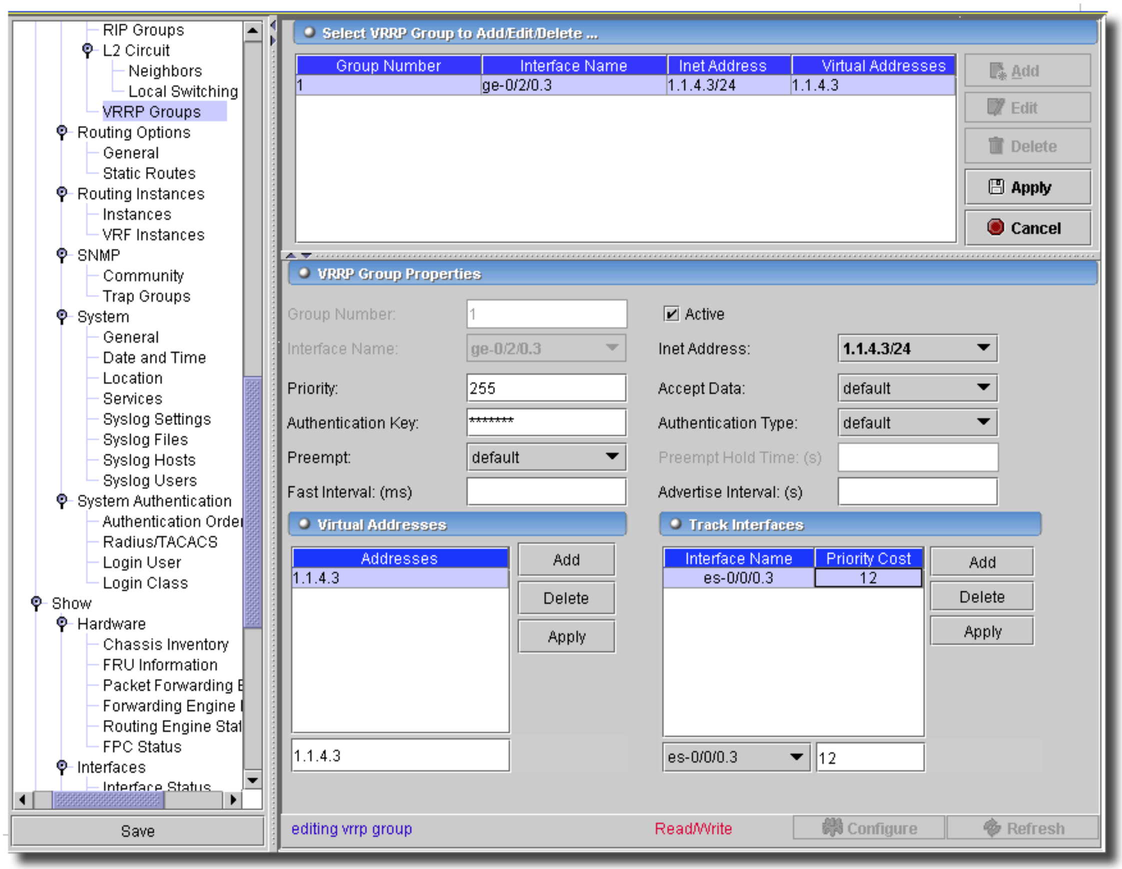
- **End Protect Interface**—Interface name of the other end point.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Protocols -> VRRP Groups

For Fast Ethernet and Gigabit Ethernet interfaces only, use this screen to configure VRRP groups.

Figure 13-87. Protocols -> VRRP Groups



Select VRRP Group to Add/Edit/Delete ...

Group Number	Interface Name	Inet Address	Virtual Addresses
1	ge-0/2/0.3	1.1.4.3/24	1.1.4.3

VRRP Group Properties

Group Number:	1	☑ Active	
Interface Name:	ge-0/2/0.3	Inet Address:	1.1.4.3/24
Priority:	255	Accept Data:	default
Authentication Key:	*******	Authentication Type:	default
Preempt:	default	Preempt Hold Time: (s)	
Fast Interval: (ms)		Advertise Interval: (s)	

Virtual Addresses

Addresses
1.1.4.3

1.1.4.3

Track Interfaces

Interface Name	Priority Cost
es-0/0/0.3	12

es-0/0/0.3 12

editing vrrp group Read/Write

Click *Add* or *Edit* a selected row to open the editor in the bottom panel. Click *Apply* to accept your edits, or *Cancel* to abandon them. The editor has the following fields:

- **Group Number**—VRRP group identifier (0 - 255).

- **Active**—Mark this item active or inactive in the configuration.

- **Interface Name**—Fast Ethernet or Gigabit Ethernet interface to configure this VRRP Group.

- **Inet Address**—Inet Address to configure this VRRP Group. If no Inet address set exists, you can enter one with a text field.

- **Priority**—Router's priority for being elected to be the master router in the VRRP group. A larger value indicates a higher priority for being elected (1 - 255) Default is 100 (for backup routers)

- **Accept Data**—Select from the pick list.

- **Authentication Key**—The authentication password. For simple authentication, it can be 1 through 8 characters long. For Message Digest 5 (MD5) authentication, it can be 1 through 16 characters long.

- **Authentication Type**—On Fast Ethernet or Gigabit Ethernet interfaces only, enable VRRP authentication and specify the authentication scheme for the VRRP group. If you enable authentication, you must specify a password by specifying an authentication key.

  default–Disable authentication.

  simple–Use a simple password. The password is included in the transmitted packet, making this method of authentication relatively insecure.

  md5–Use the MD5 algorithm to create an encoded checksum of the packet. The encoded checksum is included in the transmitted packet. The receiving routing platform uses the authentication key to verify the packet, discarding it if the digest does not match. This algorithm provides a more secure authentication scheme.

- **Preempt**—When configuring VRRP on Fast Ethernet and Gigabit Ethernet interfaces, configure whether a backup router can preempt a master router:

  Preempt–Allow the master router to be preempted.

  No Preempt–Prohibit the preemption of the master router.

  default–If you omit this statement, the backup router can preempt a master router.

- **Preempt Hold Time**—Hold-time before a higher-priority backup router preempts the master router. This field is only enabled if you select *Preempt*. (0 - 3600 seconds).

- **Fast Interval**—On Fast Ethernet and Gigabit Ethernet interfaces only, configure the interval, in milliseconds, between VRRP advertisement packets. All routers in the VRRP group must use the same advertisement interval. (100 - 999 milliseconds).

- **Advertisement Interval**—On Fast Ethernet and Gigabit Ethernet interfaces only, configure the interval between VRRP advertisement packets. All routers in the VRRP group must use the same advertisement interval. (1 - 255 seconds).

NOTE:

Fast Interval and Advertisement Interval are mutually exclusive. Only one of these values can be configured at one time. The user interface warns if you try to configure both values.

- **Virtual Addresses**—When you are configuring VRRP on Fast Ethernet and Gigabit Ethernet interfaces only, configure the addresses of the virtual routers in a VRRP group. You can configure up to eight addresses. Addresses of one or more virtual routers. Do not include a prefix length. If the address is the same as the interface's physical address, the interface becomes the master virtual router for the group.
- **Track Interfaces**—On Fast Ethernet and Gigabit Ethernet interfaces only, enable logical interface tracking for a VRRP group. Up to 10 interfaces can be tracked. For each tracked interface, you must configure a Priority Cost.

NOTE:

When they are available, you can now select IRB ports in this screen. See Integrated Bridging -> Bridge Domain on page 573 for more.

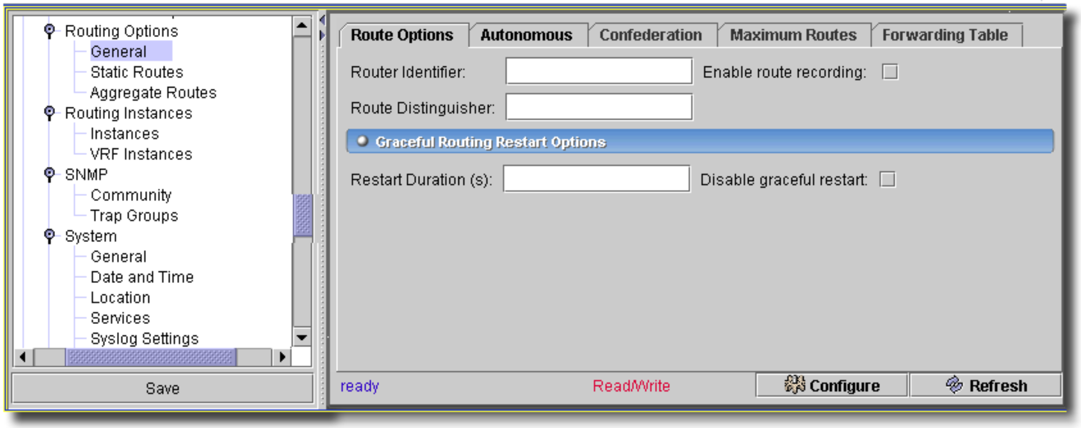
- **Priority Cost**—The value subtracted from the configured VRRP priority when the tracked interface is down, forcing a new master router election. The sum of all the costs for all interfaces or routes that are tracked must be less than or equal to the configured priority of the VRRP group. (1 - 254).

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Routing Options -> General

This screen manages general routing options.

Figure 13-88. Routing Options -> General -> Route Options



Router Identifier:
Enable route recording: □
Route Distinguisher:
Restart Duration (s):
Disable graceful restart: □

It contains the following tabs:

- Route Options
- Autonomous
- Confederation
- Maximum Routes

- Forwarding Table

Route Options

- **Router Identifier**—Specify the router's IP address.

- **Route Distinguisher**—Identifier used in route distinguishers for routing instances.

- **Enable Route Recording**—Enable route recording.

Graceful or hitless routing restart options.

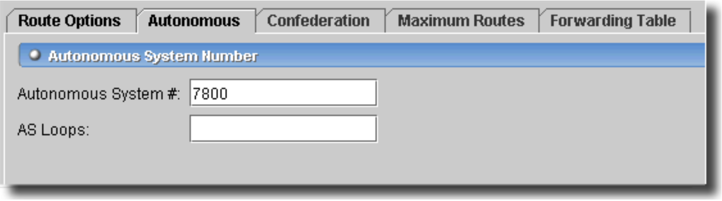
- **Disable graceful restart** - disables graceful restart

- **Restart Duration**—Maximum time for which router is in graceful restart (120 - 900)

Autonomous

This tab describes Autonomous System numbers.

Figure 13-89. Routing Options -> General -> Autonomous



Autonomous System #: 7800

AS Loops:

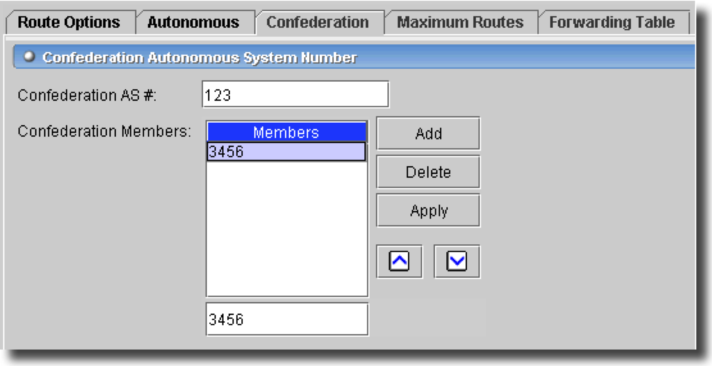
- **Autonomous System #**—Specify the router's AS number.

- **AS Loops**—Maximum number of times this AS can be in an AS path (1 - 10).

Confederation

This tab describes Confederation Autonomous System numbers.

Figure 13-90. Routing Options -> General -> Confederation



Confederation AS #: 123

Confederation Members:

Members
3456

3456

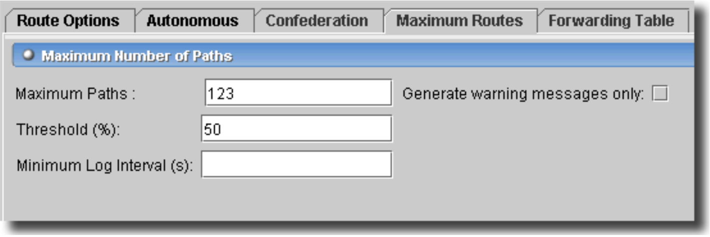
- **Confederation AS #**—Confederation autonomous system number (1 - 65535).

- **Confederation Members**—Autonomous system numbers of confederation members (1 - 65535).

Maximum Routes

This tab describes maximum routes and warning messages.

Figure 13-91. Routing Options -> General -> Maximum Routes



Maximum Number of Paths

Maximum Paths : 123

Generate warning messages only: □

Threshold (%): 50

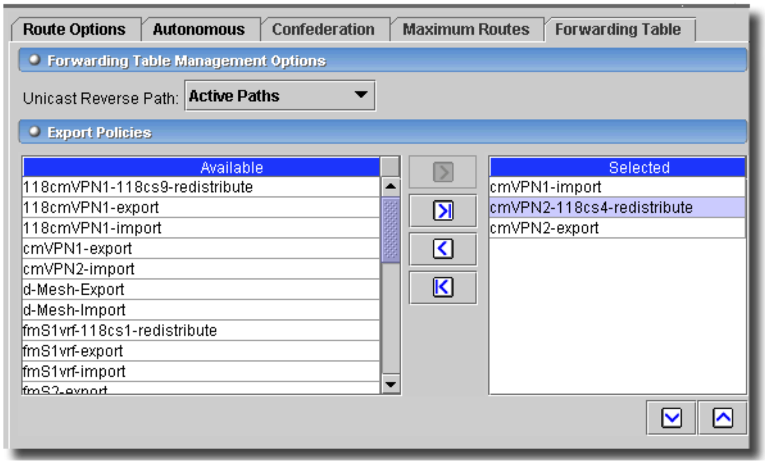
Minimum Log Interval (s):

- **Maximum Paths**—Maximum number of paths (1 - 4294967295). Configure an upper limit for the number of routes installed in a routing table.
- **Threshold** % (can only configure if max routes is set)—Percentage of limit to start warnings (1 - 100).
- **Minimum Log Intervals**—The minimum interval between log messages (5 - 86400 seconds).
- **Generate warning messages only**—Sets the route limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected.

Forwarding Table

This table manages export policies.

Figure 13-92. Routing Options -> General -> Forwarding Table



Forwarding Table Management Options

Unicast Reverse Path: Active Paths

Export Policies

Available
118cmVPN1-118cs9-redistribute
118cmVPN1-export
118cmVPN1-import
cmVPN1-export
cmVPN2-import
d-Mesh-Export
d-Mesh-Import
fmS1vrf-118cs1-redistribute
fmS1vrf-export
fmS1vrf-import
fmS2-export

Selected
cmVPN1-import
cmVPN2-118cs4-redistribute
cmVPN2-export

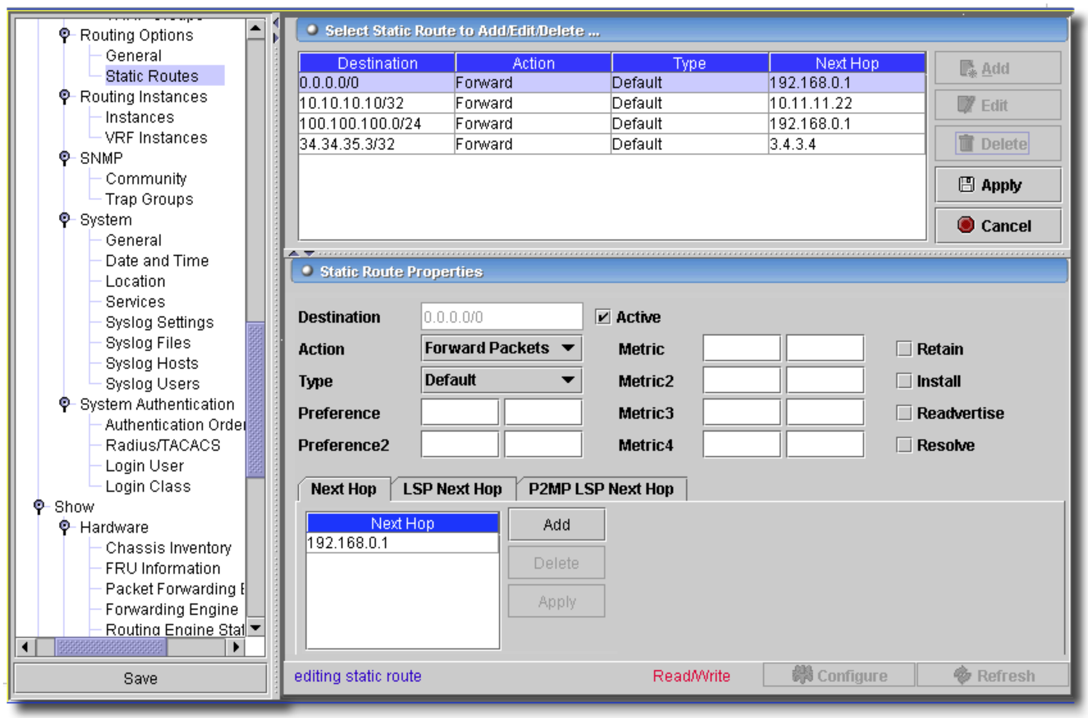
- **Unicast Reverse Path**—Select from the pick list. Options include *Default*, *Active Paths*, *Feasible Paths*.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Routing Options -> Static Routes

This screen manages routing options for static routes.

Figure 13-93. Routing Options -> Static Routes



Select Static Route to Add/Edit/Delete ...

Destination	Action	Type	Next Hop
0.0.0.0/0	Forward	Default	192.168.0.1
10.10.10.10/32	Forward	Default	10.11.11.22
100.100.100.0/24	Forward	Default	192.168.0.1
34.34.35.3/32	Forward	Default	3.4.3.4

Static Route Properties

Destination: 0.0.0.0/0 ☑ Active

Action: Forward Packets

Type: Default

Preference

Preference2

Metric

Metric2

Metric3

Metric4

□ Retain

□ Install

□ Readvertise

□ Resolve

Next Hop
192.168.0.1

editing static route

Read/Write

The table at the top of this screen displays configured static routes showing destination address, action, type and next hop address. *Add* or *Edit* a selected route with those buttons. Click *Export* to save a description of the listed routes. Click *Apply* to accept your edits for the table, *Cancel* to abandon them. Select a row and click *Delete* to remove it. If you add or edit a row, the editor at the bottom of the screen appears with the following fields and checkboxes:

- **Destination**—Destination of the generated route.

- **Action**—Must select one of the following from the pick list:

  Forward Packets—Reach the next-hop router by specifying an IP address or an interface name.

  Reject Packets—Drop packets to destination; send ICMP unreachables.

Discard Packets—Drop packets to destination; send no ICMP unreachables.

Receive Packets—Install a receive route for the destination

- **Type**— Select from the pick list:

Default - Do not configure.

Active—Remove inactive route from forwarding table.

Passive—Retain inactive route in forwarding table.

You can specify up to four metric values, starting with metric (for the first metric value) and continuing with metric2, metric3, and metric4. You also can specify a secondary preference value (preference2).

Metric—Enter an LSP metric value (1 - 65,535).

Preference—Enter an LSP preference value (1 - 255).

- The following are the *Next Hop* checkboxes:

- **Retain**—Always keep route in forwarding table.

- **Install**—Install route into forwarding table.

- **Readvertise**—Mark route as eligible to be readvertised.

- **Resolve**—Allow resolution of indirectly connected next hops.

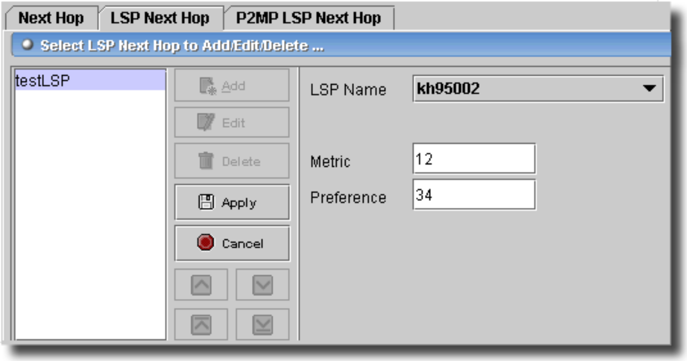
Next Hop

You can only configure the Next Hop List, LSP Next Hop list and the P2MP Next Hop when you select *Forward Packets* as the Action. *Add* the address entered below the list, or *Delete* a selected entry to manage the next hop list. The application will inform you with an error message if you try to configure with a different action.

LSP Next Hop

In this tab you can configure LSP next hops. You can configure multiple LSP next hops using the list manager. Add a new entry or Edit an existing entry in the list. Click Apply to apply the LSP attributes for that entry in the LSP Next Hop list.

Figure 13-94. LSP Next Hop



testLSP

LSP Name: kh95002

Metric: 12

Preference: 34

This screen has the following fields:

- **LSP Name**—Select an existing LSP from the pick list or select *Specify LSP* from the pick list and type in an LSP that has not been created on the field below the list.

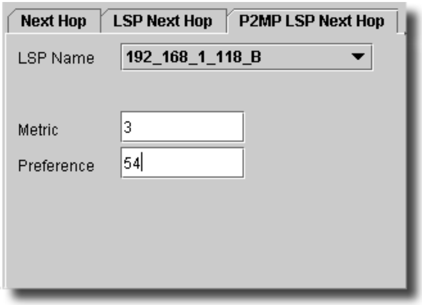
Metric—Enter an LSP metric value (1 - 65,535).

Preference—Enter an LSP preference value (1 - 255).

P2MP LSP Next Hop

This tab configures Point-to-Multipoint (P2MP) LSPs.

Figure 13-95. Point-to-Multipoint (P2MP) LSPs



LSP Name: 192_168_1_118_B

Metric: 3

Preference: 54

It has the following fields:

LSP Name—Select an existing LSP from the pick list or select *Specify LSP* from the pick list and type in an LSP that has not been created on the field that appears below the list.

Metric—Enter an LSP metric value (1 - 65,535).

Preference—Enter an LSP preference value (1 - 255).

NOTE:

The LSP Name blank field does not appear in the screen in Figure 13-95 because the pick list is not set to Specify LSP.

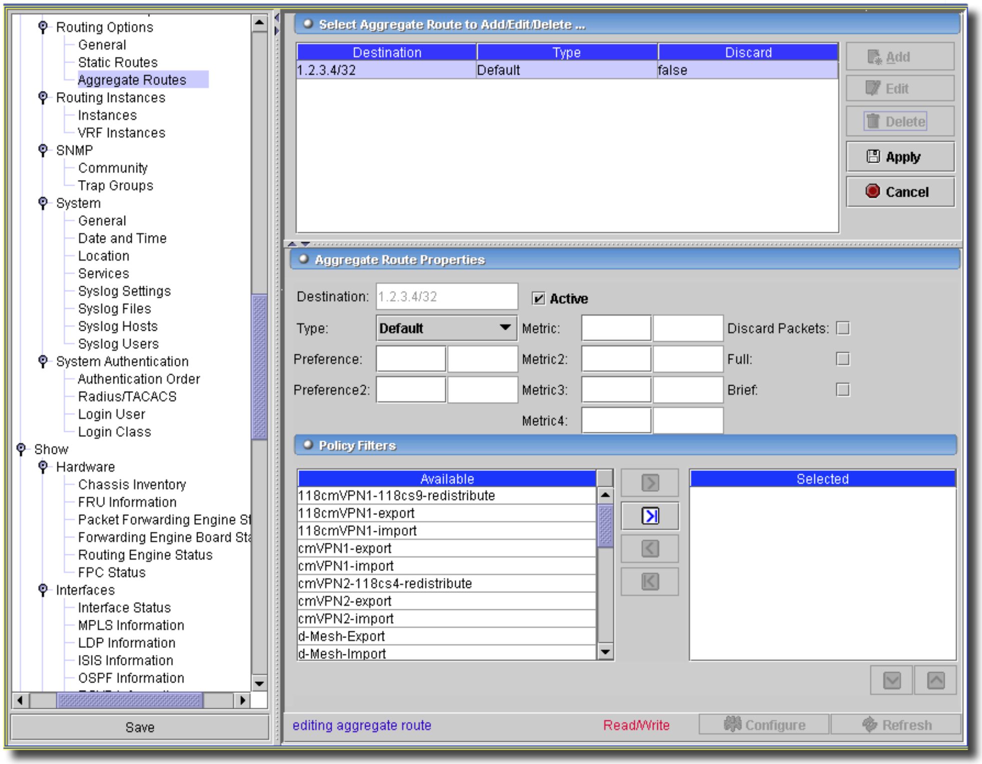
The device only allows one P2MP to be configured. You can configure multiple next hop LSP values.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Routing Options -> Aggregate Routes

This screen manages aggregate routes for the selected device.

Figure 13-96. Routing Options -> Aggregate Routes



Destination	Type	Discard
1.2.3.4/32	Default	false

Destination: 1.2.3.4/32 ☑ Active

Type: Default

Metric:

Discard Packets: □

Preference:

Metric2:

Full: □

Preference2:

Metric3:

Brief: □

Metric4:

Available
118cmVPN1-118cs9-redistribute
118cmVPN1-export
118cmVPN1-import
cmVPN1-export
cmVPN1-import
cmVPN2-118cs4-redistribute
cmVPN2-export
cmVPN2-import
d-Mesh-Export
d-Mesh-Import

Selected

editing aggregate route

Read/Write

The table at the top of this screen displays configured aggregate route instances. *Add* or *Edit* a selected instance with those buttons to the right. Select a row and click *Delete* to remove it. Click *Export* to save a description of these items in a file. If you add or edit a row, the editor at the bottom of the screen appears with the following fields and checkboxes:

Aggregate Route Properties

- **Destination**—Destination address or network.

- **Active**—Check to activate this route.

- **Type**—Select from the pick list. Options include *Default*, *Active* and *Passive*.

- **Preference / Preference2**—Enter a preference value. A lower number indicates a more preferred route (1-255). The second field on these lines indicates the type of route (1-16).

- **Metric / Metric2/ Metric3 / Metric4** —Enter a metric (1-65,535). The second field on these lines indicates the type of metric (1-16).

- **Discard Packets**—Check to drop packets to destination and send no ICMP unreachable messages.

- **Full**—Check to include all AS numbers from all contributing paths.

- **Brief**—Check to include the longest common sequences from contributing paths.

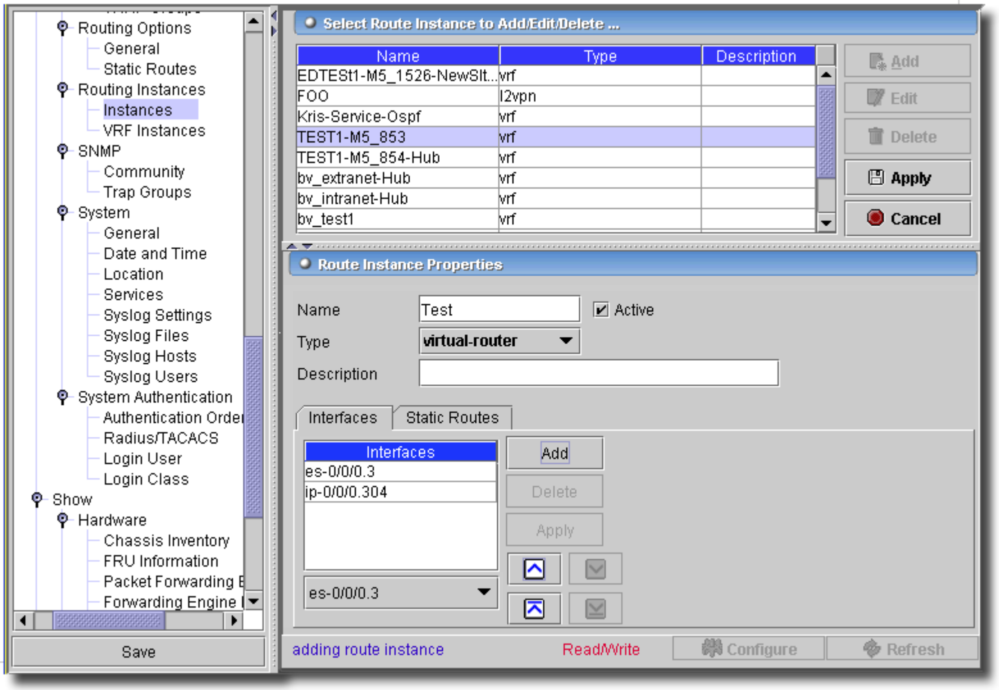
Policy Filters

Select from the *Available* policy filters that appear on the left by clicking the arrows between *Available* and *Selected* panels in this portion of the screen. Use the up/down arrows below the right panel to re-order selected policies. Click *Apply* to accept your edits for the table, *Cancel* to abandon them.

Routing Instances -> Instances

This screen manages Routing Instances (interfaces and static routes).

Figure 13-97. Routing Instances -> Instances



Name	Type	Description
EDTESt1-M5_1526-NewSlt...	vrf	
FOO	l2vpn	
Kris-Service-Ospf	vrf	
TEST1-M5_853	vrf	
TEST1-M5_854-Hub	vrf	
bv_extranet-Hub	vrf	
bv_intranet-Hub	vrf	
bv_test1	vrf	

Name: Test ☑ Active

Type: virtual-router

Description:

Interfaces
es-0/0/0.3
ip-0/0/0.304

es-0/0/0.3

adding route instance Read/Write

The table at the top of this screen displays configured instances. *Add* or *Edit* a selected instance with those buttons to the right. Click *Apply* to accept your edits for the table, *Cancel* to abandon them. Select a row and click *Delete* to remove it. Click *Export* to save a description of these items in a file. If you add or edit a row, the editor at the bottom of the screen appears with the following fields and checkboxes:

- **Name**—A unique identifier for the instance.

- **Type**—Select from the pick list. Only *virtual router* instances are editable.

- **Description**—A text description of the instance.

Interfaces Tab

Type an interface in the lowest field and click *Add* to add it to those listed. You can also select an interface listed and remove it with the *Delete* button. Click *Apply* to accept the list.

Static Routes Tab

You can *Add*, *Apply* and *Delete* Static Routes to the list under *Select State Route*. Click *Apply* above to accept your edits, or *Cancel* to abandon them. Select an interface to *Add* with the pick list at the bottom of the list, or select an existing, listed interface, and click *Apply* to change it. Rearrange the routes by selecting them and clicking the arrows to the right of the list.

Next Hop To Destination

The next hop can be an IP address, hostname or an interface. Choose the corresponding radio button depending on which you want to configure.

- **Destination**—Enter a valid IP address or hostname into the text field

- **IPHost Destination**—Enter a valid IP address or hostname into the text field

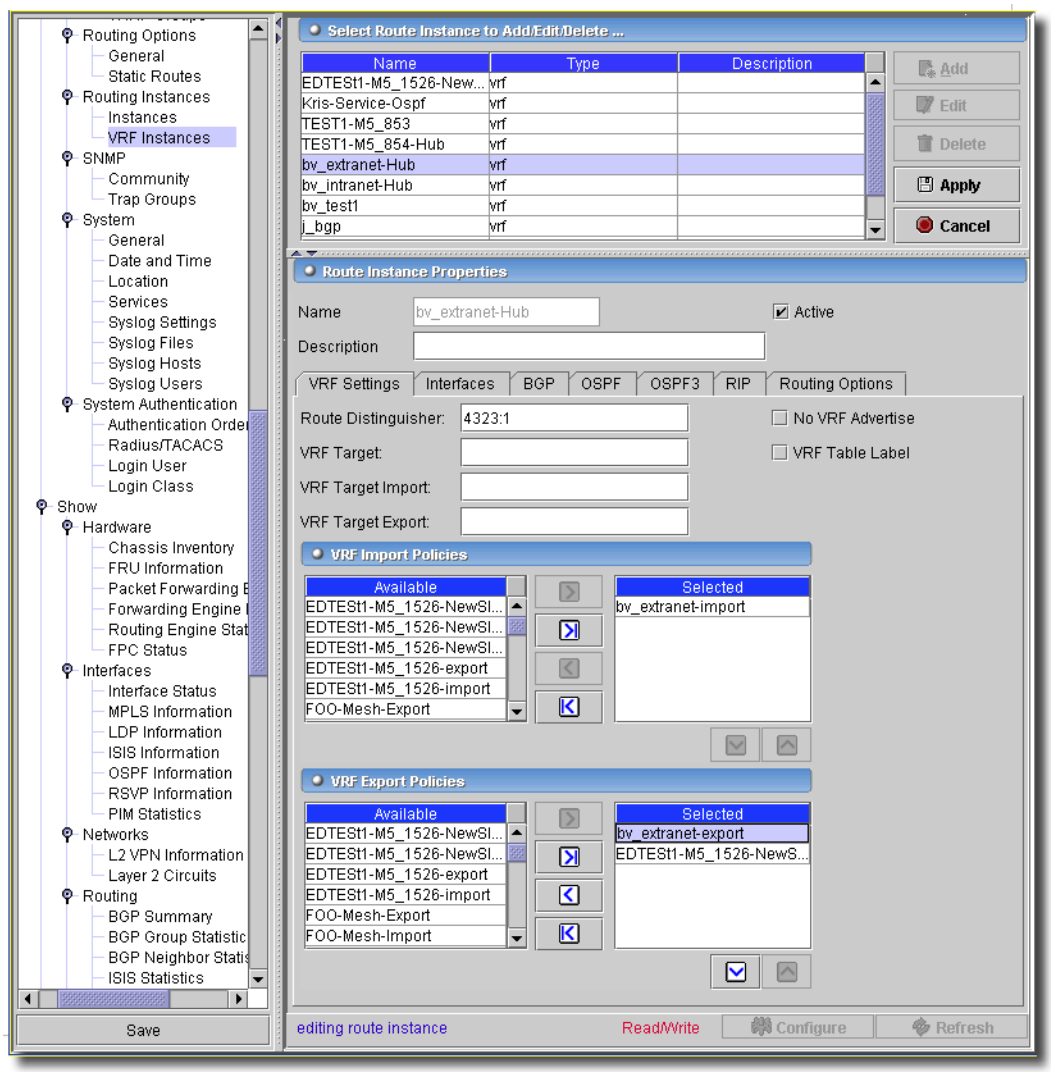
- **Interface Destination**—Select an interface and number from the pick lists. A (read only) label at the bottom indicates the current configured value.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Routing Instances -> VRF Instances

This screen configures VRF Instances on the selected equipment.

Figure 13-98. Routing Instances -> VRF Instances - VRF Settings



Select Route Instance to Add/Edit/Delete ...

Name	Type	Description
EDTESt1-M5_1526-New...	vrf	
Kris-Service-Ospf	vrf	
TEST1-M5_853	vrf	
TEST1-M5_854-Hub	vrf	
bv_extranet-Hub	vrf	
bv_intranet-Hub	vrf	
bv_test1	vrf	
j_bgp	vrf	

Route Instance Properties

Name: bv_extranet-Hub ☑ Active

Description:

Route Distinguisher: 4323:1 ☐ No VRF Advertise

VRF Target: ☐ VRF Table Label

VRF Target Import:

VRF Target Export:

VRF Import Policies

Available	Selected
EDTESt1-M5_1526-NewSl...	bv_extranet-import
EDTESt1-M5_1526-NewSl...	
EDTESt1-M5_1526-NewSl...	
EDTESt1-M5_1526-export	
EDTESt1-M5_1526-import	
FOO-Mesh-Export	

VRF Export Policies

Available	Selected
EDTESt1-M5_1526-NewSl...	bv_extranet-export
EDTESt1-M5_1526-NewSl...	EDTESt1-M5_1526-NewS...
EDTESt1-M5_1526-export	
EDTESt1-M5_1526-import	
FOO-Mesh-Export	
FOO-Mesh-Import	

editing route instance Read/Write

NOTE:

This service requires a license.

The tabs on this screen have the following fields in common:

- **Name**—An identifier for the routing instance. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long.

- **Active**—Check to make this active in the configuration.

- **Description**—A text description of the VPN or VPLS routing instance. Any descriptive text you include appears in the output of the show route instance detail command and has no effect on operation.

The following tabs appear below these fields:

- VRF Settings
- Interfaces
- BGP
- OSPF (and OSPF3)
- RIP
- Routing Options

VRF Settings

- **Route Distinguisher**—An identifier attached to a route that indicates to which VPN or VPLS routing instance it belongs. Each routing instance must have a unique distinguisher associated with it. Each route distinguisher is a 6-byte value. These are the two different values that can be used for the Route Distinguisher:

  as-number:id—*as-number* is your assigned autonomous system (AS) number (a 2-byte value) and *id* is any 4-byte value. The AS number can be in the range from 1 through 65,535.

  ip-address:id—*ip-address* is an IP address in your assigned prefix range (a 4-byte value) and *id* is any 2-byte value. The IP address can be any globally unique unicast address.

- **VRF Target**—If you configure the community only, default VRF import and export policies are generated that accept and tag routes with the specified target community, helping to simplify the VPN configuration process.

  You can also explicitly configure VRF import and export policies using the import and export options. You can configure the following for VRF Target:

  community—Community name.

  import community-name—The allowed communities to accept from neighbors.

  export community-name—The allowed communities to send to neighbors.

- **No VRF Advertise**—Select this option so that this VRF does not advertise this instance to remote PEs.

- **VRF Table Label**—Check this option to map the inner label of a packet to a specific VPN routing and forwarding (VRF) table. This allows the examination of the encapsulated IP header.

VRF Import Policies

Specify how routes are imported into the local PE router's VRF table (routing-instance-name.inet.0) from the remote PE router. You can configure multiple import policies on the PE router.

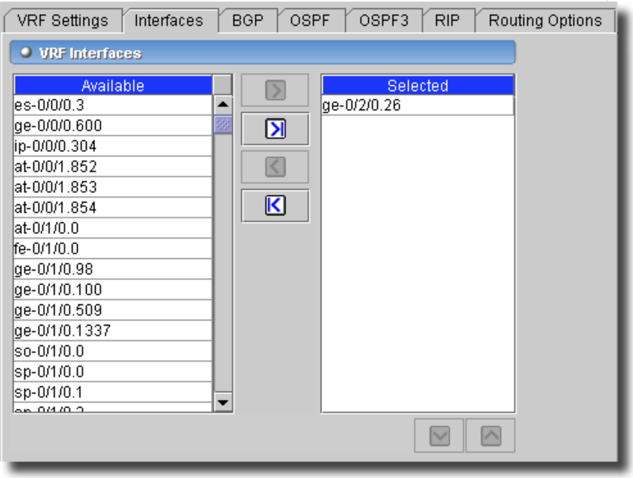
VRF Export Policies

Specify how routes are exported from the local PE router's VRF table (routing-instance-name.inet.0) to the remote PE router. You can configure multiple export policies on the PE router.

Interfaces

This screen configures interfaces over which the VPN traffic travels between the PE router and customer edge (CE) router.

Figure 13-99. Routing Instances -> VRF Instances - Interfaces



Available
- es-0/0/0.3
- ge-0/0/0.600
- ip-0/0/0.304
- at-0/0/1.852
- at-0/0/1.853
- at-0/0/1.854
- at-0/1/0.0
- fe-0/1/0.0
- ge-0/1/0.98
- ge-0/1/0.100
- ge-0/1/0.509
- ge-0/1/0.1337
- so-0/1/0.0
- sp-0/1/0.0
- sp-0/1/0.1

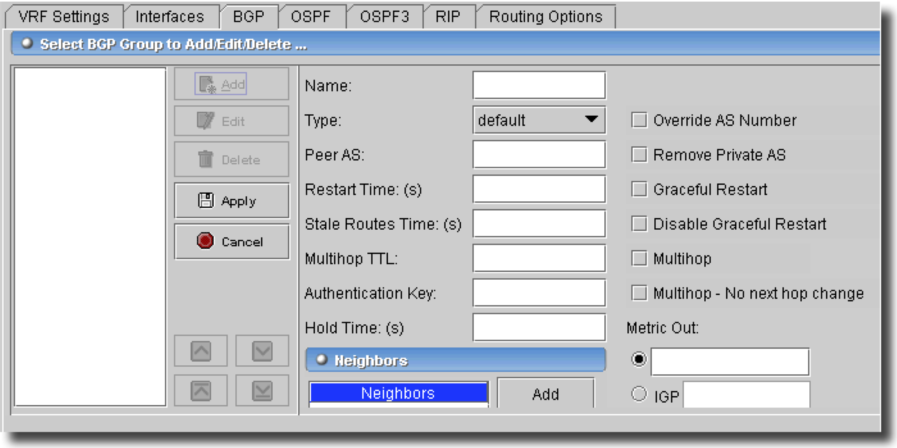
Selected
- ge-0/2/0.26

Configure the interfaces on the PE router by clicking the arrows to move those listed as *Available* to *Selected* (or back).

BGP

This screen configures BGP options for the VRF instance.

Figure 13-100. Routing Instances -> VRF Instances - BGP



Type: default

This screen has the following fields:

- **Name**—This identifies this BGP Group within this routing instance. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long.
- **Type**—Specify the type of BGP peer group, *Internal* or *External*.
- **Override AS Number**—Compare the AS path of an incoming advertised route with the AS number of the BGP peer under the group and replace all occurrences of the peer AS number in the AS path with its own AS number before advertising the route to the peer.

  Enabling the AS override feature allows routes originating from an AS to be accepted by a router residing in the same AS. Without AS override enabled, the router refuses the route advertisement once the AS path shows that the route originated from its own AS. This is done by default to prevent route loops. The as-override statement overrides this default behavior.

CAUTION:
Enabling the AS override feature may result in routing loops. Use this feature only for specific applications that require this type of behavior, and in situations with strict network control. One application is the IGP protocol between the provider edge router and the customer edge router in a virtual private network. For more information, see the *JUNOS MPLS Applications Configuration Guide*.

- **Peer AS**—Specify the neighbor (peer) AS number.
- **Graceful Restart**—Configure graceful restart for BGP.
- **Restart Time**—Time period when the restart is expected to be complete. Range: 1 through 600 seconds
- **Stale Routes Time**—Maximum time that stale routes are kept during restart. Range: 1 through 600 seconds
- **Disable Graceful Restart**—Disables graceful restart for BGP.

- **Multihop**—Configure an EBGP multihop session. External confederation peering is a special case that allows unconnected third-party next hops. You do not need to configure multihop sessions explicitly in this particular case; multihop behavior is implied.

  If you have confederation external BGP peer-to-loopback addresses, you still need the multihop configuration.

  If you omit this statement, all EBGP peers are assumed to be directly connected (that is, you are establishing a nonmultihop, or "regular", BGP session), and the default time-to-live (TTL) value is 1.

- **Multihop TTL**—Configure the maximum TTL value for the TTL in the IP header of BGP packets.   Range: 1 through 255   Default: 64 (for multihop EBGP sessions, confederations, and internal BGP sessions)

- **Multihop - No next hop change**—Specify not to change the TTL value; for next-hop-to-self route advertisements, specify the no-nexthop-self option.

- **Authentication Key**—Configure an MD5 authentication key (password). Neighboring routers use the same password to verify the authenticity of BGP packets sent from this system. It can be up to 126 characters.

- **Hold Time**—Value to use when negotiating a connection with the peer. The hold-time value is advertised in open packets and indicates to the peer the length of time that it should consider the sender valid. If the peer does not receive a keepalive, update, or notification message within the specified hold time, the application closes the BGP connection to the peer and routers through that peer become unavailable.

  The hold time is three times the interval at which keepalive messages are sent. Range: 6 through 65,535 seconds Default: 90 seconds

- **Metric Out**—Metric for all routes sent using the multiple exit discriminator (MED, or MULTI_EXIT_DISC) path attribute in update messages. This path attribute discriminates among multiple exit points to a neighboring AS. If all other factors are equal, the exit point with the lowest metric is preferred.

  You can specify a constant metric value by selecting the first radio button option. For configurations in which a BGP peer sends third-party next hops that require the local system to perform next-hop resolution-IBGP configurations, configurations within confederation peers, or EBGP configurations that include the multihop command-you can specify a variable metric by selecting the second or third radio buttons for the IGP or Min IGP option.

  You can increase or decrease the variable metric calculated from the IGP metric (either from the igp or igp-minimum statement) by specifying a value for <*offset*>. You can specify this offset by entering a value into the text fields next to the *IGP* or *Min IGP* options. The metric increases when you specify a positive value for <*offset*>, and decreases when you specify a negative value for <*offset*>.

  igp—Set the metric to the most recent metric value calculated in the IGP to get to the BGP next hop.

metric—Primary metric on all routes sent to peers. Range: 0 through 4,294,967,295 (232 -1) Default: No metric is sent.

minimum-igp—Set the metric to the minimum metric value calculated in the IGP to get to the BGP next hop. If a newly calculated metric is greater than the minimum metric value, the metric value remains unchanged. If a newly calculated metric is lower, the metric value is lowered to that value.

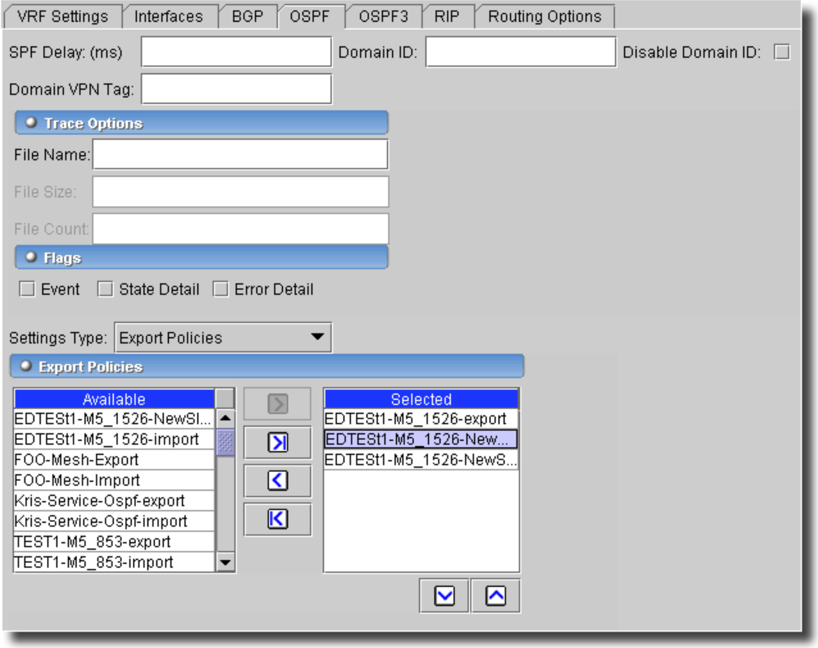
offset—(Optional) Increases or decreases the metric by this value. Range: -231 through 231 -1 (No default).

- **Neighbors**—Explicitly configure a neighbor (peer). To configure multiple BGP peers, include multiple neighbor statements. Specify an IPv6 or IPv4 address for each peer.
- **Export Policies**—Click the arrows to move *Available* to *Selected* policies (or vice-versa). Apply one or more policies to routes being exported from the routing table into BGP. Noticed that you can also re-order policies with the up/down arrows below the *Selected* panel.

OSPF (and OSPF3)

OSPF & OSPF3 settings have identical forms.

Figure 13-101. Routing Instances -> VRF Instances - OSPF and OSPF3 (Export policies)



Settings Type: Export Policies

Available	Selected
EDTESt1-M5_1526-NewSl...	EDTESt1-M5_1526-export
EDTESt1-M5_1526-import	EDTESt1-M5_1526-New...
FOO-Mesh-Export	EDTESt1-M5_1526-NewS...
FOO-Mesh-Import	
Kris-Service-Ospf-export	
Kris-Service-Ospf-import	
TEST1-M5_853-export	
TEST1-M5_853-import	

The following attribute descriptions apply to both tabs

- **SPF Delay**—Configure the shortest path first (SPF) delay. The field lets you specify the number of milliseconds between the detection of a topology change and when the SPF algorithm runs. Range: 50 through 1000 milliseconds Default: 200 milliseconds
- **Domain ID**—Specify a domain ID for a route. The domain ID identifies the OSPFv2 domain from which the route originated. Default: If the router ID is not configured in the routing instance, the router ID is derived from an interface address belonging to the routing instance.
- **Disable Domain ID**—Disable domain ID. If this is selected, a Domain ID value cannot be entered in the previous field.
- **Domain VPN Tag**—Set a virtual private network (VPN) tag for OSPFv2 external routes generated by the provider edge (PE) router.

Trace Options

- **File Name**—The filename that receives the output of the tracing operation. All files are in the directory `/var/log`. Best practice typically is to put OSPF tracing output in the file `ospf-log`.
- **File Size**—Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, `kmd`) reaches this size, it is renamed, `kmd.0`, then `kmd.1` and so on, until the maximum number of trace files is reached—then device overwrites the oldest trace file. Default: 1024 KB
- **File Count**—The maximum number of trace files. When a trace file (for example, `kmd`) reaches this size, it is renamed, `kmd.0`, then `kmd.1` and so on, until the maximum number of trace files is reached—then device overwrites the oldest trace file. If you specify a maximum number of files, you must also specify a maximum file size with the size option. Range: 2 through 1000 files Default: 10 files.

Flags

The following checkboxes set flags:

- **Event**—OSPF and OSPFv3 state transitions.
- **State Detail**—Provide detailed trace information for State transitions.
- **Error Detail**—Provide detailed trace information for OSPF and OSPFv3 error packets.
- **Settings Type**—Select Export Policies, Area or Interface. The remaining screen's appearance depends on your selection here.

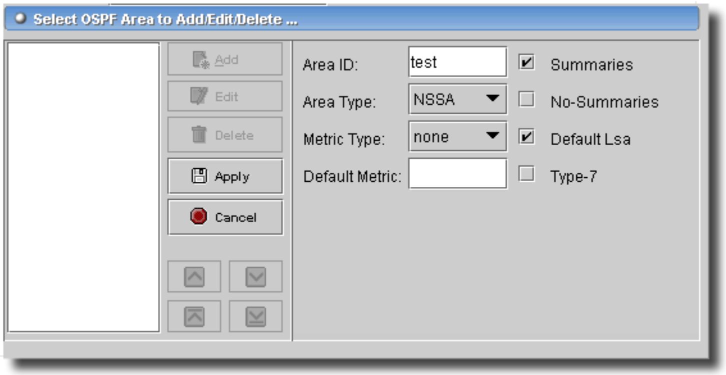
Export Policies

Apply one or more export policies to routes being exported from the routing table into OSPF by using the arrows to move policies from *Available* to *Selected*. Notice that you can also use the up/ down arrows below those *Selected* to re-order the list of policies in force.

Area

If you select the *Area* option, the remainder of the screen has these fields (rather than those in Export Policies or Interface):

Figure 13-102. Routing Instances -> VRF Instances - OSPF and OSPF3 (Area)



Area ID: test

Area Type: NSSA

Metric Type: none

Default Metric:

☑ Summaries

□ No-Summaries

☑ Default Lsa

□ Type-7

- **Area ID**—Specify the area identifier for this router to use when participating in OSPF routing. All routers in an area must use the same area identifier to establish adjacencies.

  Specify multiple area statements to configure the router as an area border router. An area border router does not automatically summarize routes between areas; use the area-range statement to configure route summarization. By definition, an area border router must be connected to the backbone area through either a physical or virtual link.

  To specify that the router is directly connected to the OSPF and OSPFv3 backbone, include the area 0.0.0.0 statement.

- **Area Type**—Select NSSA or *Stub* as the area type.

  An *NSSA* area allows external routes to be flooded within the area. These routes are then leaked into other areas.

  Select *Stub* to indicate that this area should not be flooded with AS external link-state advertisements. You must include the stub statement when configuring all routers that are in the stub area. The backbone cannot be configured as a stub area.

NOTE:

You cannot configure an area as being both a stub area and an NSSA.

- **Metric Type**—External metric type for the default LSA. Select *1* or 2. Enabled for Area Type NSSA only.
- **Default Metric**—On area border routers only, for a stub area, inject a default route with a specified metric value into the area. The default route matches any destination not explicitly reachable from within the area.

- **Summaries**—Configure whether area border routers advertise summary routes into an NSSA. When enabled, this floods summary LSAs into the NSSA.

- **No-Summaries**—Configure whether area border routers advertise summary routes into an NSSA. When checked, this prevents area border routers from advertising summaries into an NSSA. If default-metric is configured for an NSSA, a Type 3 LSA is injected into the area by default.

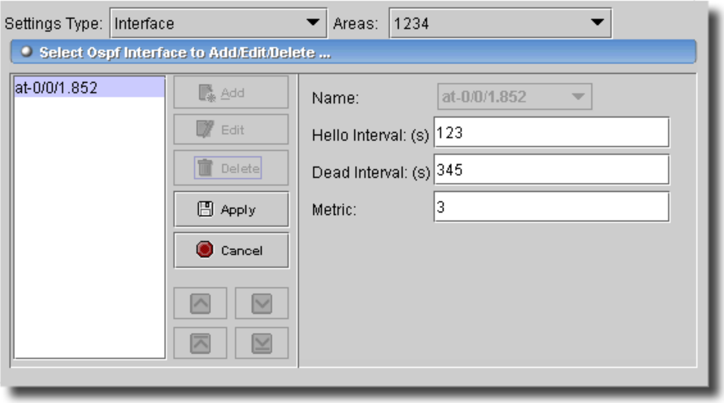
- **Default Lsa**—Enabled for Area Type NSSA only.

- **Type-7**—Enabled for Area Type NSSA only.

Interface

This portion of the screen lets you select an OSPF interface (or delete one).

Figure 13-103. Routing Instances -> VRF Instances - OSPF and OSPF3 (Interface)



Settings Type: Interface
Areas: 1234
Select Ospf Interface to Add/Edit/Delete ...
at-0/0/1.852
Name: at-0/0/1.852
Hello Interval: (s) 123
Dead Interval: (s) 345
Metric: 3

You must select an existing area to add/edit/delete interfaces for a given area with this portion of the screen. When you *Add* or *Edit*, the following fields appear:

- **Name**—Name of the interface. To configure all interfaces, you can specify *all*. Enable OSPF routing on a router interface. You must include at least one interface statement in the configuration to enable OSPF on the router.

- **Hello Interval**—Specify how often the router sends hello packets out the interface. The hello interval must be the same for all routers on a shared logical IP network. Time between hello packets, in seconds. Range: 1 through 255 seconds Default: 10 seconds; 120 seconds (nonbroadcast networks)

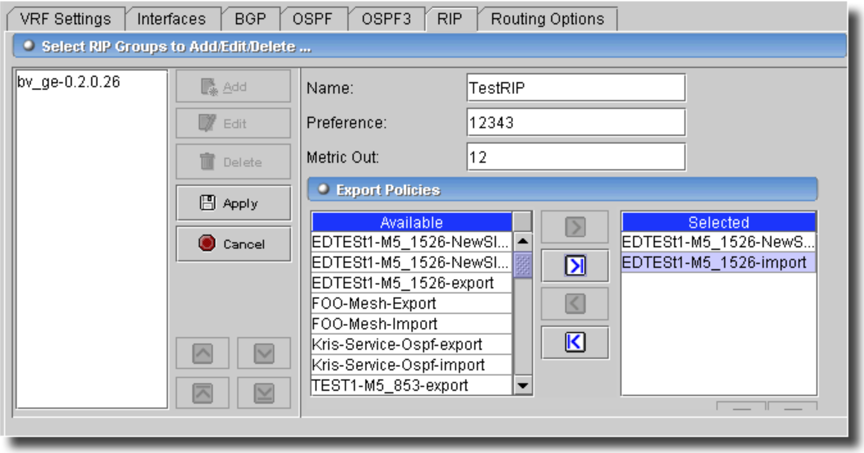
- **Dead Interval**—Specify how long OSPF waits before declaring that a neighboring router is unavailable. This is an interval during which the router receives no hello packets from the neighbor. Range: 1 through 65,535 seconds Default: 40 seconds (four times the hello interval)

- **Metric**—Cost of an OSPF interface route. The cost is a routing metric that is used in the link-state calculation. Range: 1 through 65,535 Default: 1

RIP

This screen configures the RIP portion of the VRF.

Figure 13-104. Routing Instances -> VRF Instances - RIP



bv_ge-0.2.0.26

Name: TestRIP

Preference: 12343

Metric Out: 12

Available	Selected
EDTESt1-M5_1526-NewSl...	EDTESt1-M5_1526-NewS...
EDTESt1-M5_1526-NewSl...	EDTESt1-M5_1526-import
EDTESt1-M5_1526-export	
FOO-Mesh-Export	
FOO-Mesh-Import	
Kris-Service-Ospf-export	
Kris-Service-Ospf-import	
TEST1-M5_853-export	

Rip Groups Configure a set of RIP neighbors that share an export policy and metric. The export policy and metric govern what routes to advertise to neighbors in a given group. This screen has the following fields:

- **Name**—Name of a group, up to 16 characters long.
- **Preference**—Preference of external routes learned by RIP as compared to those learned from other routing protocols. A lower value indicates a more preferred route. Range: 0 through 4,294,967,295 (232 -1) Default: 100
- **Metric Out**—Metric value to add to routes transmitted to the neighbor. Use this statement to control how other routers prefer RIP routes sent from this neighbor. Range: 1 through 16 Default: 1

Export Policies

Apply a policy to routes being exported to the neighbors by using the arrows to move listed policies from *Available* to *Selected*. Name one or more policies.

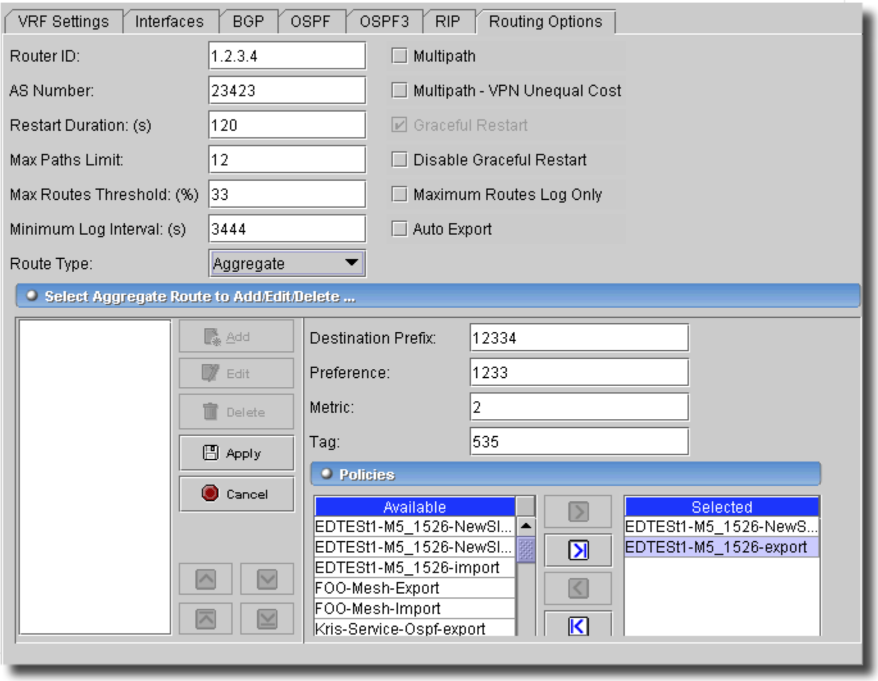
Neighbors

Similar to Export Policies, select the name of interfaces over which a router communicates to its neighbors.

Routing Options

This screen configures routing options for the VRF.

Figure 13-105. Routing Instances -> VRF Instances - Routing Options



Router ID: 1.2.3.4

AS Number: 23423

Restart Duration: (s) 120

Max Paths Limit: 12

Max Routes Threshold: (%) 33

Minimum Log Interval: (s) 3444

Route Type: Aggregate

□ Multipath

□ Multipath - VPN Unequal Cost

☑ Graceful Restart

□ Disable Graceful Restart

□ Maximum Routes Log Only

□ Auto Export

Destination Prefix: 12334

Preference: 1233

Metric: 2

Tag: 535

Available
EDTESt1-M5_1526-NewSl...
EDTESt1-M5_1526-NewSl...
EDTESt1-M5_1526-import
FOO-Mesh-Export
FOO-Mesh-Import
Kris-Service-Ospf-export

Selected
EDTESt1-M5_1526-NewS...
EDTESt1-M5_1526-export

It has the following fields:

- **Router ID**—BGP and OSPF (Open Shortest Path First) uses the router identifier to identify the router from which a packet originated. The router identifier usually is the IP address of the local router. If you do not configure a router identifier, the VRF uses the IP address of the first interface to come online. This is usually the loopback interface. Otherwise, it uses the first hardware interface with an IP address.

- **AS Number**—An autonomous system (AS) is a set of routers that are under a single technical administration and that generally use a single interior gateway protocol (IGP) and metrics to propagate routing information within the set of routers. An AS appears to other Autonomous Systems to have a single, coherent interior routing plan and presents a consistent picture of what destinations are reachable through it.

  A number assigned by the Network Information Center (NIC) in the United States (from 1 through 65,535) identifies Autonomous Systems.

  If you are using the Border Gateway Protocol (BGP) on the router, you must configure an AS number.

- **Multipath**—Enable protocol-independent load balancing for Layer 3 VPNs. This allows the forwarding next hops for both the active route and alternative paths to be used for load balancing.

- **Multipath - VPN Unequal Cost**—Apply protocol-independent load balancing to VPN routes that are equal until their interior gateway protocol (IGP) metrics with regard to route selection. If you do not configure the vpn-unequal-cost statement, protocol-independent load balancing is applied to VPN routes that are equal until their router identifiers with regard to route selection.

- **Graceful Restart**—Configure graceful restart.

- **Restart Duration**—The restart-duration option sets the period of time the router waits for a graceful restart to complete. You can configure a time between 1 through 600 seconds. The default value is 300 seconds. At the end of the configured time period, the router performs a standard restart without recovering state from the neighboring routers. This disrupts VPN services, but is probably necessary if the router is not functioning normally.

- **Disable Graceful Restart**—Disable graceful restart at this level.

- **Max Routes Limit**—Set the route limit. If the device reaches this limit, a warning occurs and the device rejects any additional routes. Range: 1 through 4,294,967,295 Default: Not set

- **Max Routes Threshold**—Threshold value for the mandatory limit that triggers a warning. Range: 1 through 100

- **Maximum Routes Log Only**—Sets the route limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected.

- **Route Types**—This pick list sets the appearance of the lowest part of the screen. Available options include the following:

  - Aggregate Routes
  - Static

Aggregate Routes

Use the *Add*, *Edit* or *Delete* buttons to the left to manage these listed routes. Click *Apply* to accept your edits, or *Cancel* to abandon them. When you *Add* or *Edit*, the following fields appear in an editor:

- **Destination Prefix**—Configure aggregate routes. Network portion of the IP address, and prefix-length is the destination prefix length.

- **Preference**—Preference value for a static, aggregated, or generated route. lower number indicates a more preferred route. Range: 1 through 255 Default: 5 (for static routes), 130 (for aggregate and generated routes)

- **Metric**—Metric value for an aggregate, generated, or static route. Range: 1 through 65,535

- **Tag**—Associate an OSPF tag with a static, aggregate, or generated route

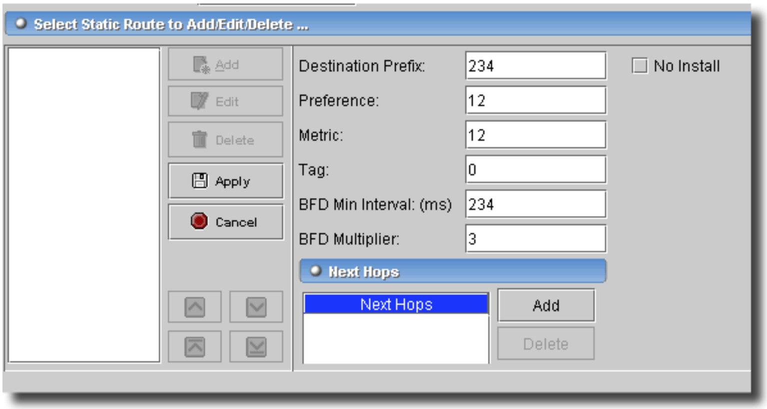
Policies

Associate a routing policy when configuring an aggregate or generated route's destination prefix in the routes part of the aggregate or generate statement. This provides the equivalent of an import routing policy filter for the destination prefix. That is, each potential contributor to an aggregate route, along with any aggregate options, passes through the policy filter. The policy then can accept or reject the route as a contributor to the aggregate route and, if the contributor is accepted, the policy can modify the default preferences. The contributor with the numerically smallest prefix becomes the most preferred, or primary, contributor. A rejected contributor still can contribute to a less specific aggregate route. If you do not specify a policy filter, all candidate routes contribute to an aggregate route. Move policies from *Available* to *Selected* with the arrows between those panels. You can also reorder the *Selected* policies with the up/down arrows below that panel.

Static

Use the *Add*, *Edit* or *Delete* buttons to the left to manage these listed routes.

Figure 13-106. Routing Instances -> VRF Instances - Static



Destination Prefix: 234

Preference: 12

Metric: 12

Tag: 0

BFD Min Interval: (ms) 234

BFD Multiplier: 3

□ No Install

Click *Apply* to accept your edits, or *Cancel* to abandon them. When you *Add* or *Edit*, the following fields appear in an editor:

- **Destination Prefix**—Network portion of the IP address, and prefix-length is the destination prefix length.
- **No Install**—Configure whether the JUNOS software installs all static routes into the forwarding table. Even if you configure a route so it is not installed in the forwarding table, the route is still eligible to be exported from the routing table to other protocols. Do not install the route into the forwarding table, even if it is the route with the lowest preference.
- **Preference**—This is a value for a static, aggregated, or generated route. A lower number indicates a more preferred route. Range: 1 through 255 Default: 5 (for static routes), 130 (for aggregate and generated routes)
- **Metric**—Metric value for an aggregate, generated, or static route. Range: 1 through 65,535.

- **Tag**—Associate an OSPF tag with a static, aggregate, or generated route.

The Bidirectional Forwarding Detection (BFD) protocol is a simple hello mechanism that detects failures in a network. BFD works with a wide variety of network environments and topologies. The failure detection timers for BFD have shorter time limits than the failure detection mechanisms of OSPF, providing faster detection. These timers are also adaptive and can be adjusted to be more or less aggressive.

- **BFD Min Interval**—Minimum transmit and receive interval for failure detection.

CAUTION:

Specifying an interval smaller than 300ms can cause undesired BFD flapping.

Range: (1...255000 milliseconds

- **BFD Multiplier**—Detection time multiplier for failure detection.

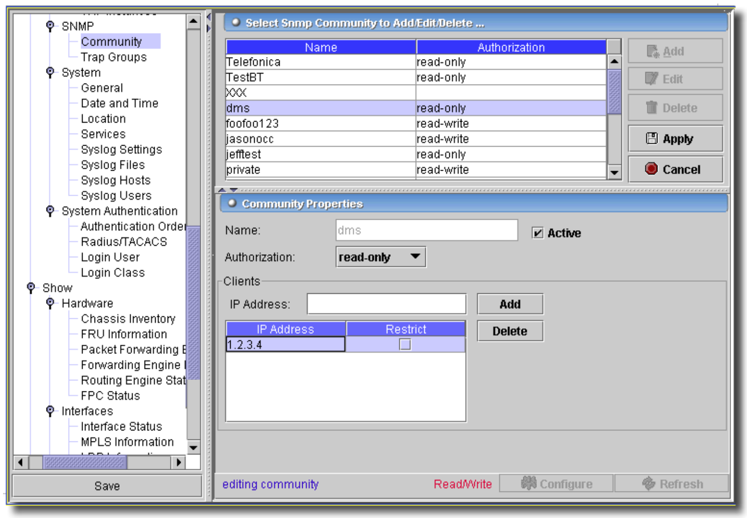
Next Hops

This specifies the device is to reach the next-hop router by specifying IP addresses. Enter an address below the list space and click *Add* to list it there. Click *Delete* to remove one, or *Apply* to change a selected one.

SNMP -> Community

This panel manages the SNMP community permissions for the selected device.

Figure 13-107. SNMP: Community



Select Snmp Community to Add/Edit/Delete ...

Name	Authorization
Telefonica	read-only
TestBT	read-only
XXX	
dms	read-only
foofoo123	read-write
jasonocc	read-write
jefftest	read-only
private	read-write

Community Properties

Name: dms ☑ Active

Authorization: read-only

Clients

IP Address: Add Delete

IP Address	Restrict
1.2.3.4	□

editing community Read/Write

The following are columns from the upper portion of the table. You can configure these when you click *Add* or select an item and click *Edit* in the upper panel. Click *Delete* to remove a selected item. Click *Export* to save a description of the listed communities as a file.

- **Name**—The SNMP community name.

- **Authorization**—The community authentication level (*read only*/*read-write*). Select from a pick list.

In the lower table, use the *Add* or *Remove* buttons to manage rows. Enter text directly in the row, once you add it. These are the columns:

- **Client IP Address**—The community's client.

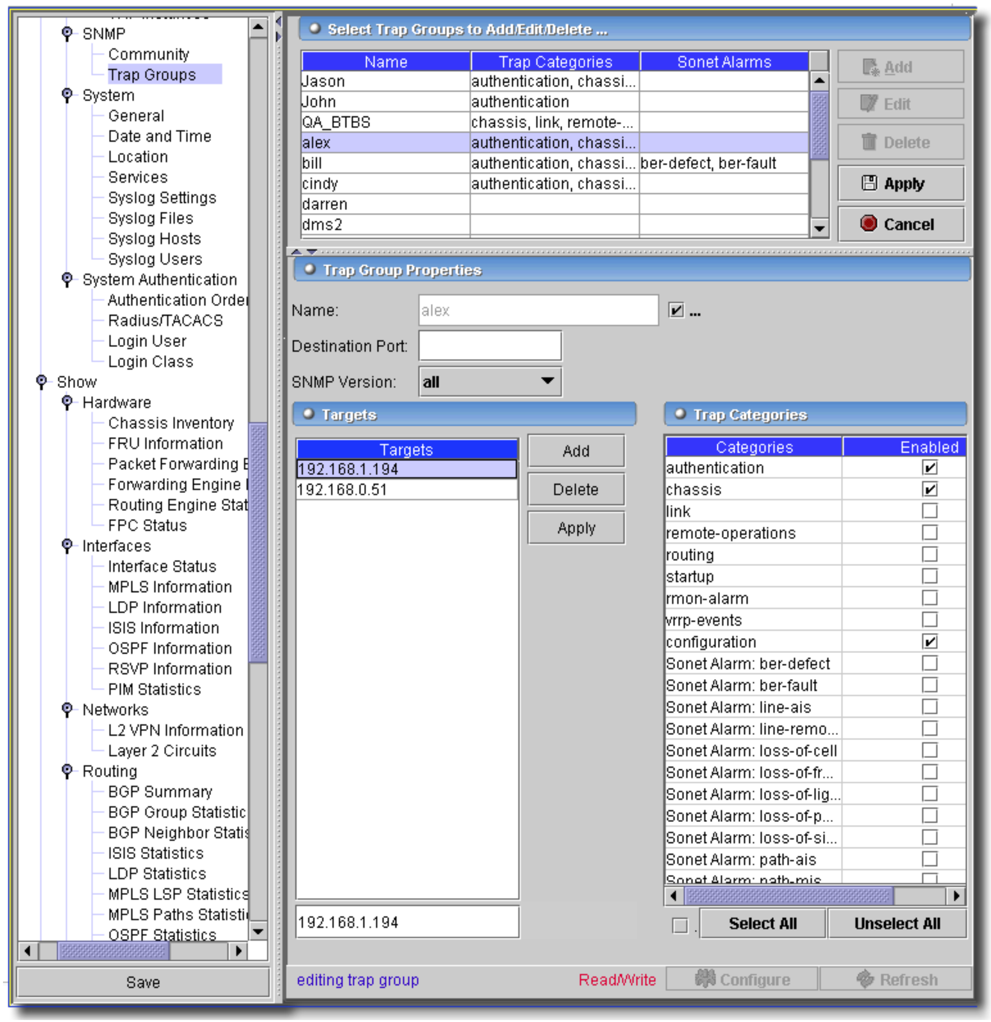
- **Restrict**—Check this to restrict the selected item.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

SNMP -> Trap Groups

This panel manages the SNMP Traps for the selected device.

Figure 13-108. SNMP: Traps



Name	Trap Categories	Sonet Alarms
Jason	authentication, chassi...	
John	authentication	
QA_BTBS	chassis, link, remote-...	
alex	authentication, chassi...	
bill	authentication, chassi...	ber-defect, ber-fault
cindy	authentication, chassi...	
darren		
dms2		

Name: alex ☑ ...

Destination Port:

SNMP Version: all

Targets
192.168.1.194
192.168.0.51

192.168.1.194

Categories	Enabled
authentication	☑
chassis	☑
link	☐
remote-operations	☐
routing	☐
startup	☐
rmon-alarm	☐
vrrp-events	☐
configuration	☑
Sonet Alarm: ber-defect	☐
Sonet Alarm: ber-fault	☐
Sonet Alarm: line-ais	☐
Sonet Alarm: line-remo...	☐
Sonet Alarm: loss-of-cell	☐
Sonet Alarm: loss-of-fr...	☐
Sonet Alarm: loss-of-lig...	☐
Sonet Alarm: loss-of-p...	☐
Sonet Alarm: loss-of-si...	☐
Sonet Alarm: path-ais	☐
Sonet Alarm: path-mis	☐

☐ .

editing trap group   Read/Write

Use the *Add*, *Edit* or *Remove* buttons to manage rows in this table. Click *Export* to save a description of the listed trap groups as a file. Only the *Name* and *Trap Categories* appear in the list of trap groups. The following are the configurable items:

Trap-Group Properties

- **Name**—The trap group name.

- **Destination-Port**—The number of the destination port.

- **SNMP Version**—Select from the supported versions in the pick list (options include *v1*, *v2*, and *all*).

Targets

These are the IP addresses to receive traps. Enter the IP address of the target in the field above the table, then click *Add* to enter a target IP in the list. Select a listed target and click *Delete* to remove it.

Trap Categories

Check the categories of traps you want to receive (*Authentication*, *Chassis*, *Configuration*, *Link*, *Remote-Operations*, *Rmon-Alarm*, *Routing*, *Startup*, *Vrrp-Events*, and *Sonet Alarms*).

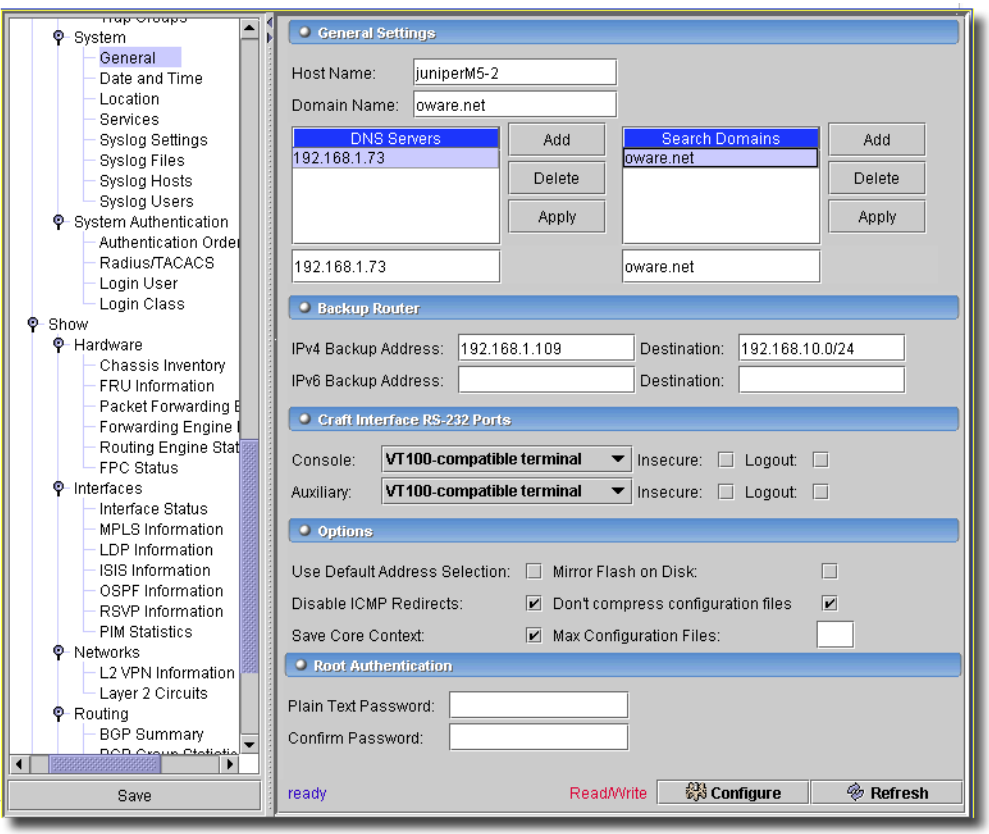
- **Receive all traps**—Check all categories.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

System -> General

This screen configures a variety of general settings for the selected device.

Figure 13-109. System -> General



General Settings

Host Name: juniperM5-2

Domain Name: oware.net

DNS Servers
192.168.1.73

192.168.1.73

Search Domains
oware.net

oware.net

Backup Router

IPv4 Backup Address: 192.168.1.109 Destination: 192.168.10.0/24

IPv6 Backup Address: Destination:

Craft Interface RS-232 Ports

Console: VT100-compatible terminal Insecure: □ Logout: □

Auxiliary: VT100-compatible terminal Insecure: □ Logout: □

Options

Use Default Address Selection: □ Mirror Flash on Disk: □

Disable ICMP Redirects: ☑ Don't compress configuration files ☑

Save Core Context: ☑ Max Configuration Files:

Root Authentication

Plain Text Password:

Confirm Password:

ready ReadWrite

This screen has the following fields:

Host Name—Hostname for this router.

Domain Name—Domain name for this router.

The following two tables let you enter an IP address or domain in the field under the table. Click A*dd* to add this list to the table. Select an item and click *Delete* to remove a listed item. Click A*pply* to accept the list. Here are the listed items:

DNS Servers—An ordered list of DNS servers.

Search Domains—An ordered list of search domains.

Backup Routers

These fields define backup Ipv4 and Ipv6 routers to use while booting

IPv4 Backup Address—IPv4 router to use while booting

Destination (optional)—Destination network reachable through the router

Ipv6 Backup Address—IPv6 router to use while booting

Destination (optional)—Destination network reachable through the router

Craft Interface RS-232 ports

Configure console ports on the router in this portion of the screen.

Console—Define Terminal type.

A*nsi*—ANSI-compatible terminal

small-xterm—Small (24-line) xterm window

vt100—VT100-compatible terminal

xterm—Large (65-line) xterm window

- **Auxiliary**—Define Terminal type. Here are the options:

A*nsi*—ANSI-compatible terminal.

small-xterm—Small (24-line) xterm window.

vt100—VT100-compatible terminal.

xterm—Large (65-line) xterm window.

Checkbox options:

Insecure—Disallow superuser access

Logout—Log out the console session when cable is unplugged

Options

Configure the selected devices with the following checkboxes:

- *Use default address* (for locally originated traffic).

- *Disable ICMP redirects*
- *Save core context*
- *Mirror flash on disk*
- *Compress configuration files* (JUNOS 6.4 and below only)
- *Don't compress configuration files* (JUNOS 7.0 and above only)
- *Max Configuration files to store on flash* [0 - 49] (JUNOS 7.0 and above only)

Root Authentication

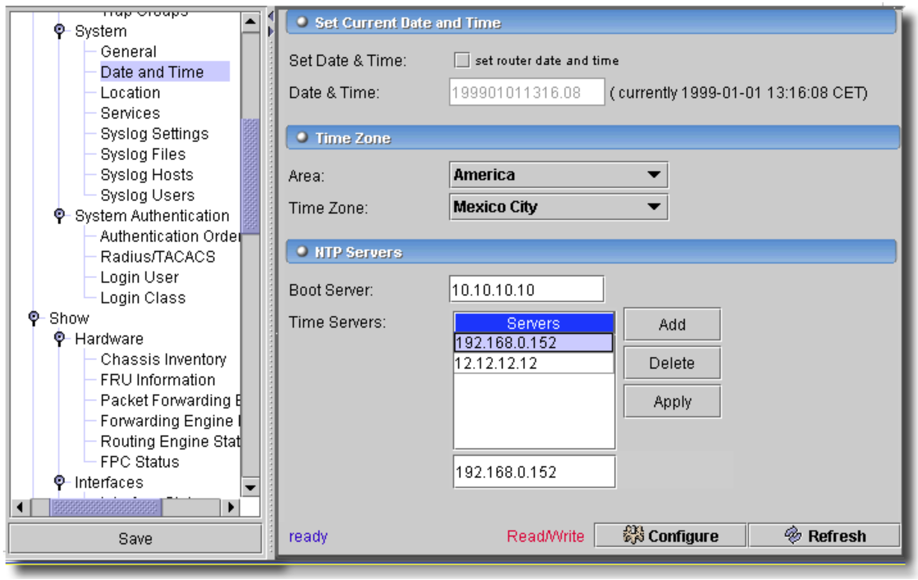
- **Plain Text Password / Confirm Password**—Root authentication password.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

System -> Date and Time

This panel manages time operations.

Figure 13-110. Date and Time



Set Current Date and Time

Set Date & Time: □ set router date and time

Date & Time: 199901011316.08 (currently 1999-01-01 13:16:08 CET)

Time Zone

Area: America

Time Zone: Mexico City

NTP Servers

Boot Server: 10.10.10.10

Time Servers:

Servers
192.168.0.152
12.12.12.12

192.168.0.152

ready ReadWrite

Use the *Add* and *Remove* buttons to manage rows in these tables.

- **Set Date & Time**—Check here to *set router date and time*.

- **Date & Time**—The date and time selected.

- **Time Zone**—The *Area* and *Time Zone* for this router. (Select from a pick list.)

NTP Servers

- **Boot Server**—The time server to associate as the boot time server. (Change)

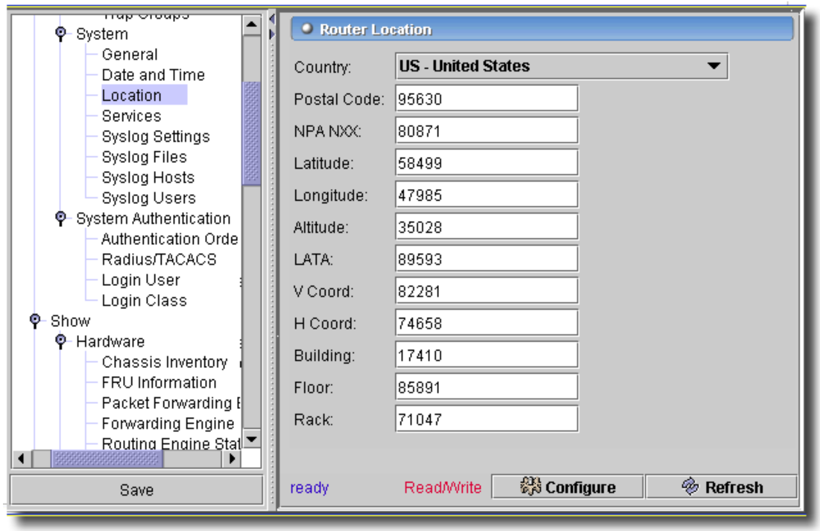
- **Time Servers**—The time server IP address(es). Click *Add* to create a new row in this table. Write directly to that row to add the IP address of an NTP time server. Use the *Remove* button to delete a selected row.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

System -> Location

This screen manages the device's location.

Figure 13-111. System -> Location



Country: US - United States
Postal Code: 95630
NPA NXX: 80871
Latitude: 58499
Longitude: 47985
Altitude: 35028
LATA: 89593
V Coord: 82281
H Coord: 74658
Building: 17410
Floor: 85891
Rack: 71047

This screens contains the following settings where you can manage a device's location:

Country—Two-letter country code.

Postal Code—Zip code or postal code.

NPA NXX—First six digits of phone number (area code plus exchange).

Latitude—Latitude in degree format.

Longitude—Longitude in degree format.

Altitude—Feet above (or below) sea level.

LATA—Long-distance service area.

V Coord—Bellcore vertical coordinate.

H Coord—Bellcore horizontal coordinate.

For devices that support JUNOS 7.0 and above, the following additional fields are available:

Building—Building name.

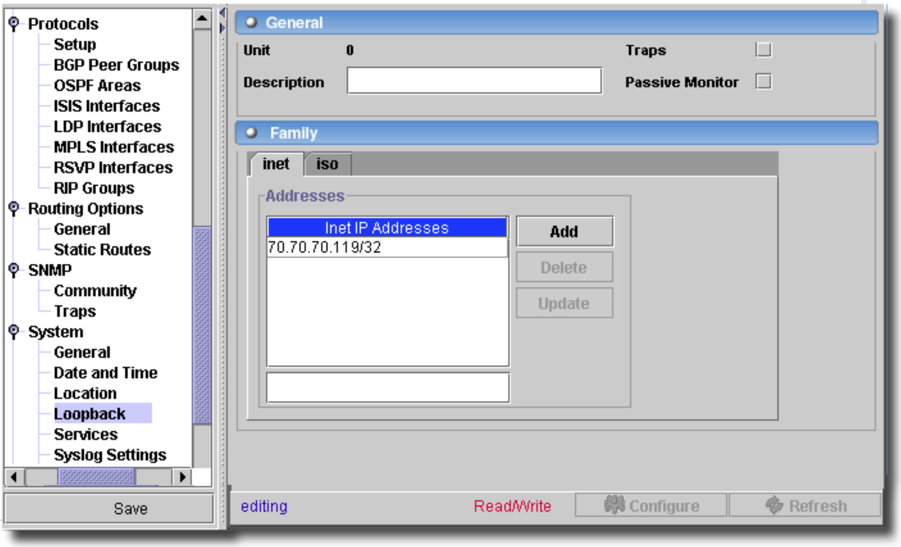
Floor—Floor number.

Rack—Rack number.

System -> Loopback

This screen manages loopback settings.

Figure 13-112. Loopback



Unit 0

Traps □

Description

Passive Monitor □

Inet IP Addresses
70.70.70.119/32

Here are the fields on this panel:

- **Unit**—Unit number is always 0. (read only)

- **Traps**—Check to enable traps.

- **Passive Monitor**—Check to enable.

- **Description**—A text description.

Family

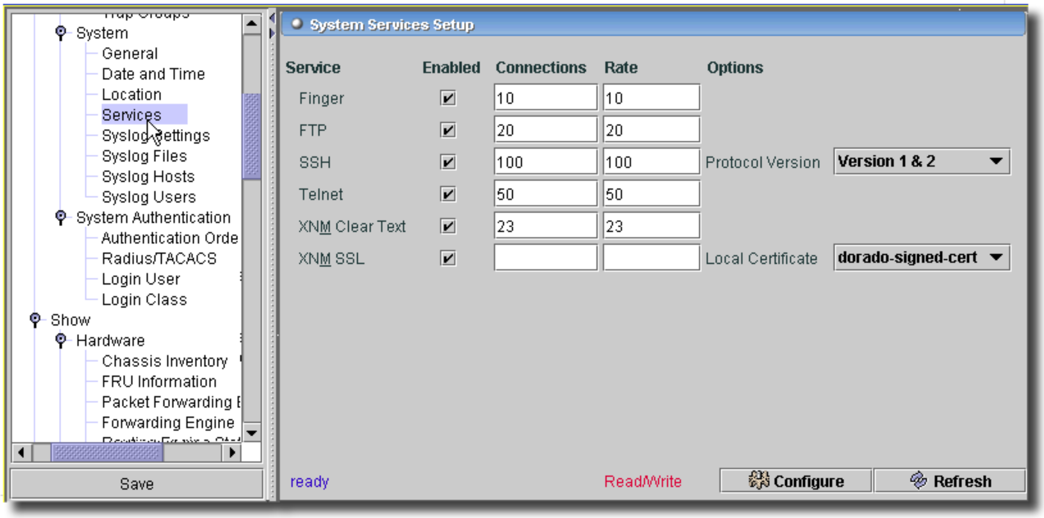
Use *Add* (adds the address entered below the table) and *Delete* to manage rows in the *inet* and *iso* tabs. These are the loopback inet and iso IP addresses.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

System -> Services

This screen manages system services settings.

Figure 13-113. System Services



Service	Enabled	Connections	Rate	Options	
Finger	☑	10	10		
FTP	☑	20	20		
SSH	☑	100	100	Protocol Version	Version 1 & 2
Telnet	☑	50	50		
XNM Clear Text	☑	23	23		
XNM SSL	☑			Local Certificate	dorado-signed-cert

Each section has a checkbox. Check those if the configuration in that section applies. This screen configures *Finger, FTP, SSH, Telnet, XNM Clear Text* and *XNM SSL*, and has the following fields:

- **Connections**—The maximum connections allowed on the finger service. Range: 1-250

- **Rate**—The maximum connections allowed per minute on the finger service. Range: 1-250

- **Protocol Version**—Select from the pick list

- **Authentication Certificate**—Name of local X.509 certificate to use.

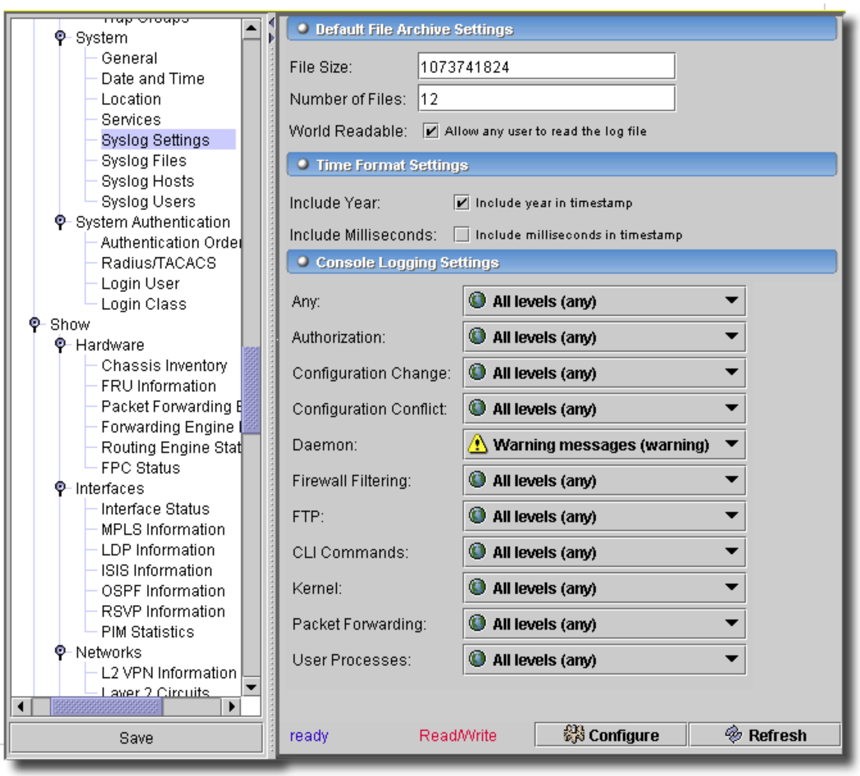
- **Local Certificate**—Select the local X.509 certificate to use for XNM SSL.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

System -> Syslog Settings

This panel manages system log file archive settings.

Figure 13-114.   System Log File



Default File Archive Settings

File Size: 1073741824

Number of Files: 12

World Readable: ☑ Allow any user to read the log file

Time Format Settings

Include Year: ☑ Include year in timestamp

Include Milliseconds: □ Include milliseconds in timestamp

Console Logging Settings

Any: All levels (any)

Authorization: All levels (any)

Configuration Change: All levels (any)

Configuration Conflict: All levels (any)

Daemon: Warning messages (warning)

Firewall Filtering: All levels (any)

FTP: All levels (any)

CLI Commands: All levels (any)

Kernel: All levels (any)

Packet Forwarding: All levels (any)

User Processes: All levels (any)

ready   Read/Write

This has the following items to configure:

Default File Archive Settings:

- **File Size**—The size of the Log file.

- **Number of Files**—The number of files logged (1-1000); one for each chosen period.

- **World Readable**—Check to allow any user to read the log file.

Time Format Settings

Check the following to enable them:

Include year—Include year in timestamp

Include milliseconds—Include milliseconds in timestamp

Console Logging Settings:

These logging settings let you define what messages are logged by setting the priority for each facility. See Priority Levels on page 564 for a list of those. The facilities that generate messages or the levels are the following:

- **Any**—All facilities.

- **Authorization**—Authorization system.

- **Configuration Change**—Configuration change log.

- **Configuration Conflict**—Configuration conflict log.

- **Daemon**—Various system processes.

- **Firewall Filtering**—Firewall filtering system.

- **FTP**—File Transfer Protocol process.

- **CLI Commands**—Commands executed by the user interface.

- **Kernel**—Kernel

- Packet Forwarding

- User processes

Priority Levels

The priority levels you can select for facilities are the following:

- **Default**—Defaults to anything configured at a higher level or no messages if nothing else is defined.

- **Alert**—Conditions that should be corrected immediately.

- **Any**—All levels.

- **Critical**—Critical conditions.

- **Emergency**—Panic conditions.

- **Error**—Error conditions.

- **Info**—Informational messages.

- **None**—No messages

- **Notice**—Conditions that should be handled specially

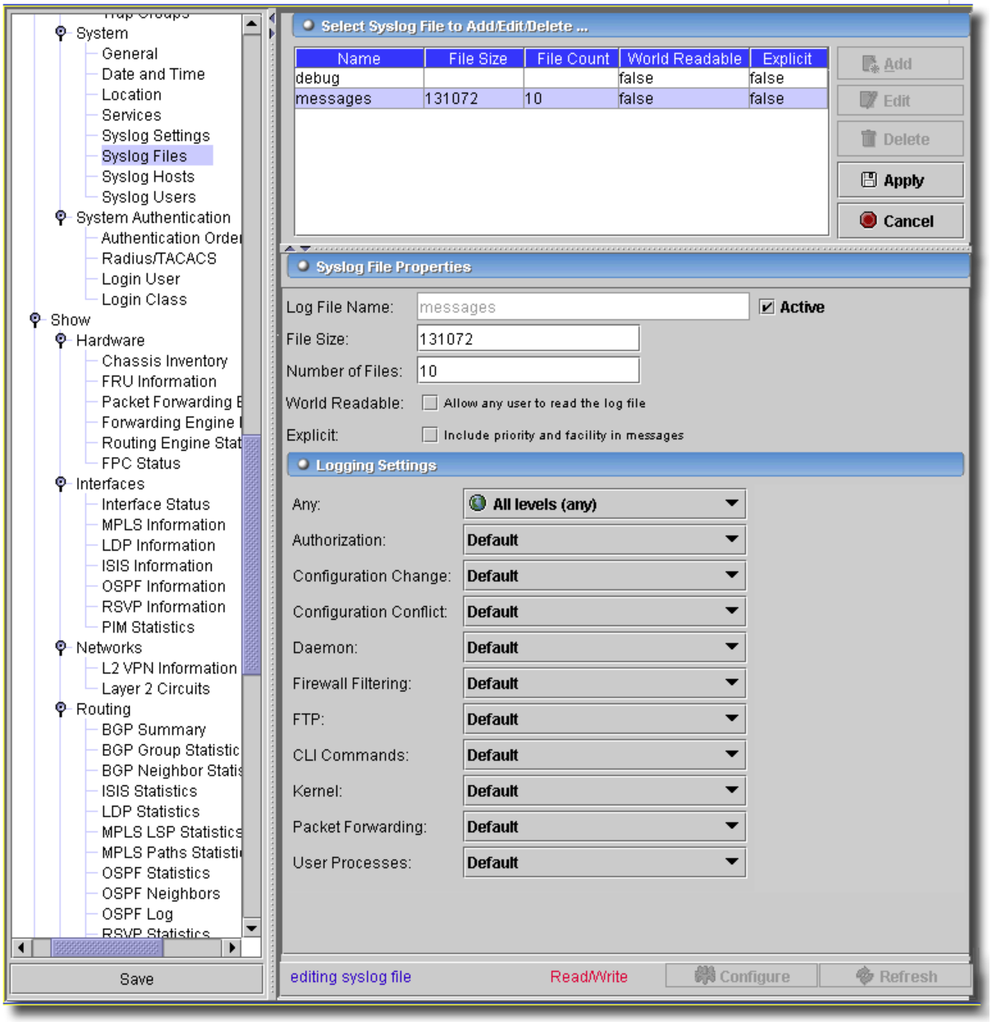
- **Warning**—Warning messages

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

System -> Syslog Files

Configure one or more log files and define what messages will be written to them. Log files are stored on the router in `/var/log`.

Figure 13-115. System -> Syslog Files



Select Syslog File to Add/Edit/Delete ...

Name	File Size	File Count	World Readable	Explicit
debug			false	false
messages	131072	10	false	false

Syslog File Properties

Log File Name: messages ☑ Active

File Size: 131072

Number of Files: 10

World Readable: □ Allow any user to read the log file

Explicit: □ Include priority and facility in messages

Logging Settings

Any: All levels (any)

Authorization: Default

Configuration Change: Default

Configuration Conflict: Default

Daemon: Default

Firewall Filtering: Default

FTP: Default

CLI Commands: Default

Kernel: Default

Packet Forwarding: Default

User Processes: Default

editing syslog file Read/Write

Use the *Add*, *Edit*, and *Delete* buttons to manage rows of Syslog files in this table. Click *Export* to save a description of the listed items. When you *Add* or *Edit* a selected row, the editor panel at the bottom of the screen appears. Click *Apply* to accept your edits, or *Cancel* to abandon them. This screen has the following fields:

Log File Name—The name of log file.

File Size—Size of files to be archived (65536 - 1073741824 bytes)

Number of Files—Number of files to be archived (1 - 1000).

World Readable—Allow any user to read the log file.

Explicit—Include priority and facility in messages.

Logging Settings

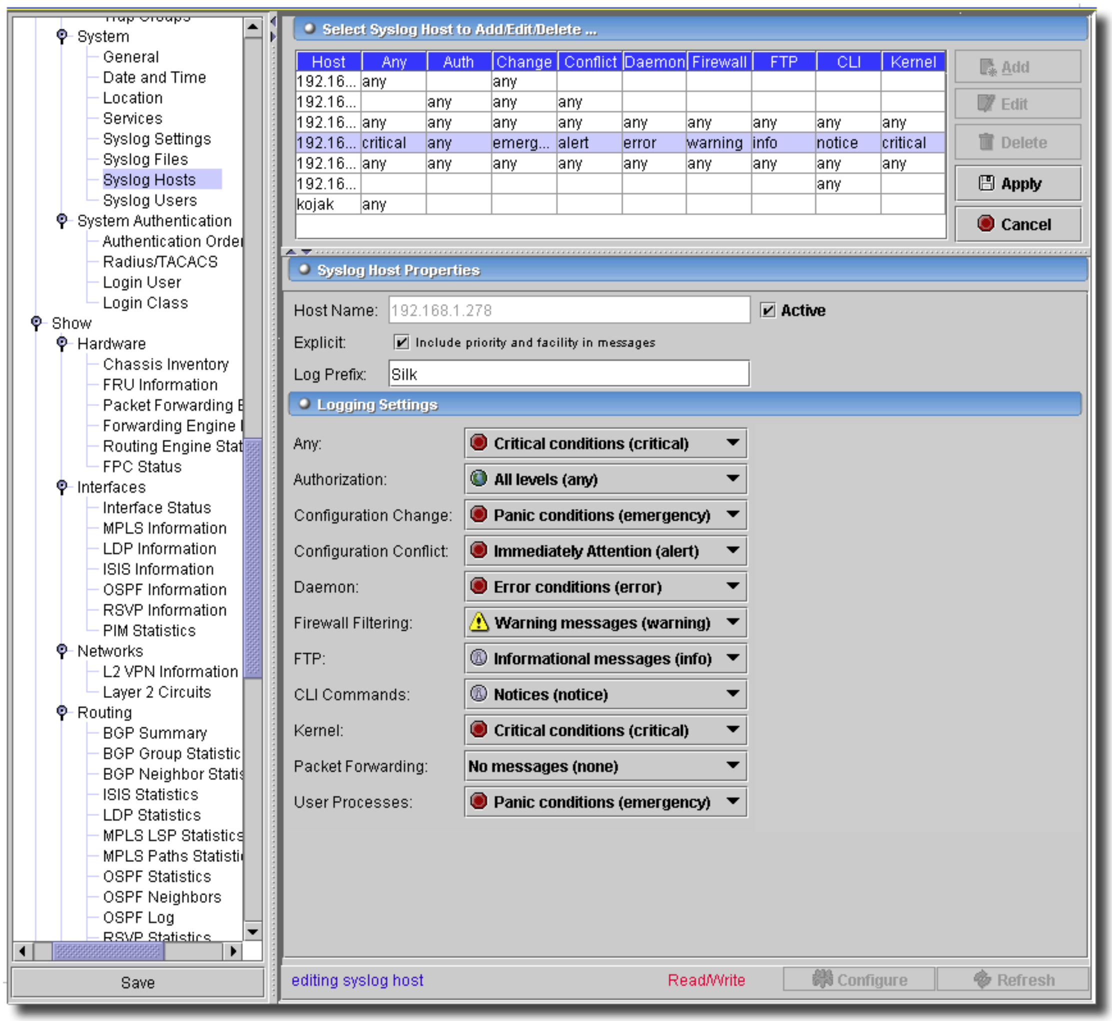
Configure the Facilities and Priorities to log on the console. See Console Logging Settings: on page 564 for a description.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

System -> Syslog Hosts

Configure one or more hosts to send syslog messages.

Figure 13-116. System -> Syslog Hosts



Select Syslog Host to Add/Edit/Delete ...

Host	Any	Auth	Change	Conflict	Daemon	Firewall	FTP	CLI	Kernel
192.16...	any		any						
192.16...		any	any	any					
192.16...	any	any	any	any	any	any	any	any	any
192.16...	critical	any	emerg...	alert	error	warning	info	notice	critical
192.16...	any	any	any	any	any	any	any	any	any
192.16...								any	
kojak	any								

Syslog Host Properties

Host Name: 192.168.1.278 ☑ Active

Explicit: ☑ Include priority and facility in messages

Log Prefix: Silk

Logging Settings

Any:	Critical conditions (critical)
Authorization:	All levels (any)
Configuration Change:	Panic conditions (emergency)
Configuration Conflict:	Immediately Attention (alert)
Daemon:	Error conditions (error)
Firewall Filtering:	Warning messages (warning)
FTP:	Informational messages (info)
CLI Commands:	Notices (notice)
Kernel:	Critical conditions (critical)
Packet Forwarding:	No messages (none)
User Processes:	Panic conditions (emergency)

editing syslog host   Read/Write

Use the *Add*, *Edit*, and *Delete* buttons to manage rows of Syslog files in this table. When you *Add* or *Edit* a selected row, the editor panel at the bottom of the screen appears. Click *Export* to save a description of the listed items. Click *Apply* to accept your edits, or *Cancel* to abandon them. This screen has the following fields:

- **Host Name**—The hostname or IP address to which to log messages.

- **Explicit**—Include priority and facility in messages.

- **Log Prefix**—Prefix for all logging to this host.

Logging Settings

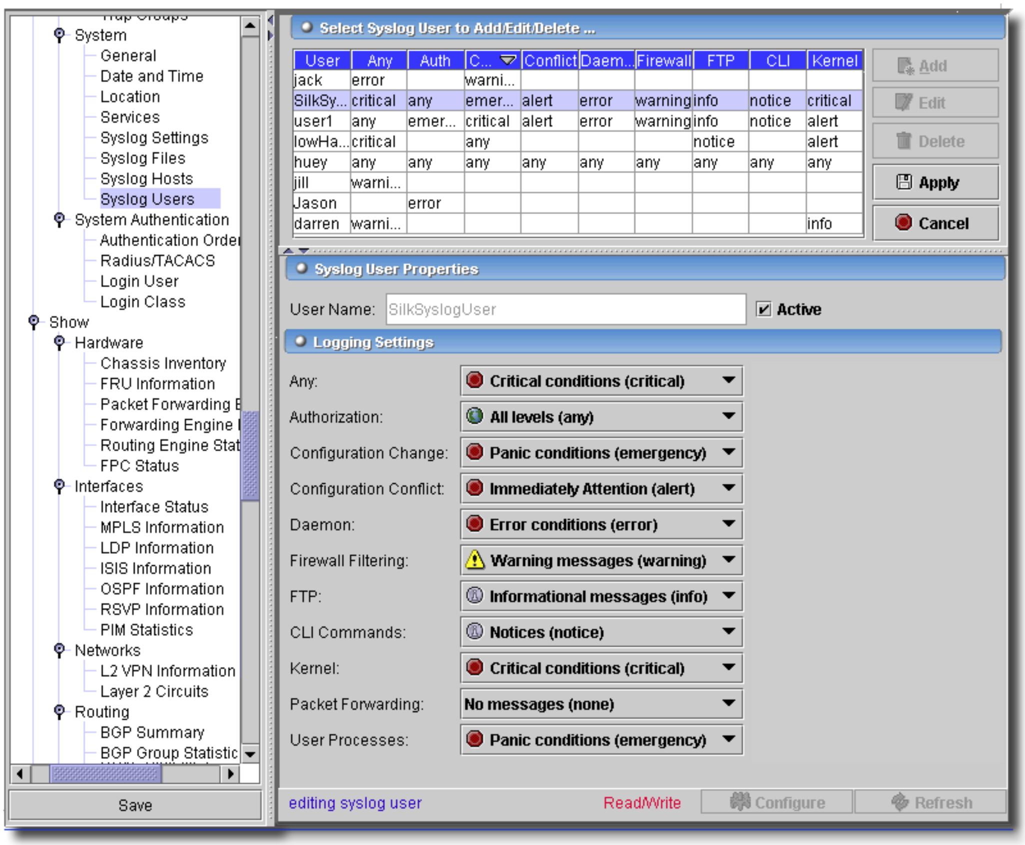
Configure the Facilities and Priorities to log on the console. See Console Logging Settings: on page 564 for a description.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

System -> Syslog Users

This screen configures syslog settings for system users.

Figure 13-117. System -> Syslog Users



Select Syslog User to Add/Edit/Delete ...

User	Any	Auth	C...	Conflict	Daem...	Firewall	FTP	CLI	Kernel
jack	error		warni...						
SilkSy...	critical	any	emer...	alert	error	warning	info	notice	critical
user1	any	emer...	critical	alert	error	warning	info	notice	alert
lowHa...	critical		any				notice		alert
huey	any	any	any	any	any	any	any	any	any
jill	warni...								
Jason		error							
darren	warni...								info

Syslog User Properties

User Name: SilkSyslogUser ☑ Active

Logging Settings

Any:	Critical conditions (critical)
Authorization:	All levels (any)
Configuration Change:	Panic conditions (emergency)
Configuration Conflict:	Immediately Attention (alert)
Daemon:	Error conditions (error)
Firewall Filtering:	Warning messages (warning)
FTP:	Informational messages (info)
CLI Commands:	Notices (notice)
Kernel:	Critical conditions (critical)
Packet Forwarding:	No messages (none)
User Processes:	Panic conditions (emergency)

editing syslog user ReadWrite

Use the *Add*, *Edit*, and *Delete* buttons to manage rows of Syslog files in this table. Click *Export* to save a description of the listed items. When you *Add* or *Edit* a selected row, the editor panel at the bottom of the screen appears. Click *Apply* to accept your edits, or *Cancel* to abandon them. This screen has the following fields:

User Name—A valid system user name

Logging Settings

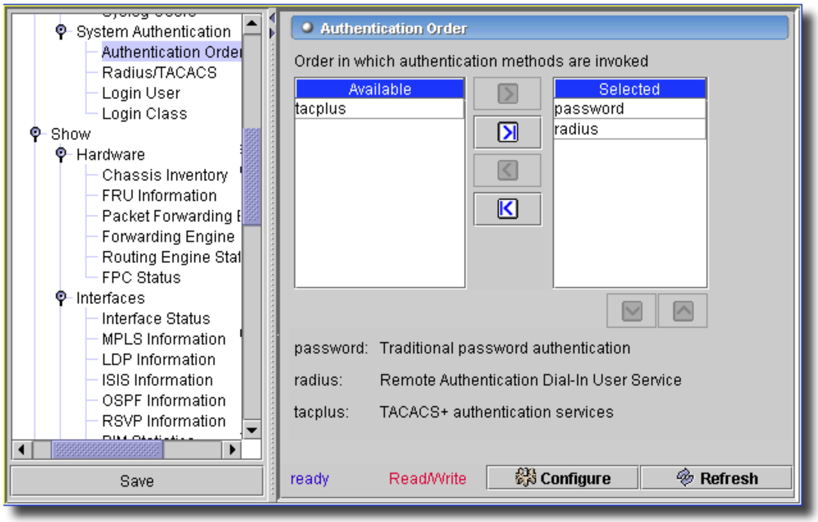
Configure the Facilities and Priorities to log on the console. See Console Logging Settings: on page 564 for a description.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

System Authentication -> Authentication Order

This screen manages the order in which authentication occurs.

Figure 13-118. Authentication Order



Order in which authentication methods are invoked

Available	Selected
tacplus	password
	radius

password: Traditional password authentication

radius: Remote Authentication Dial-In User Service

tacplus: TACACS+ authentication services

ready Read/Write

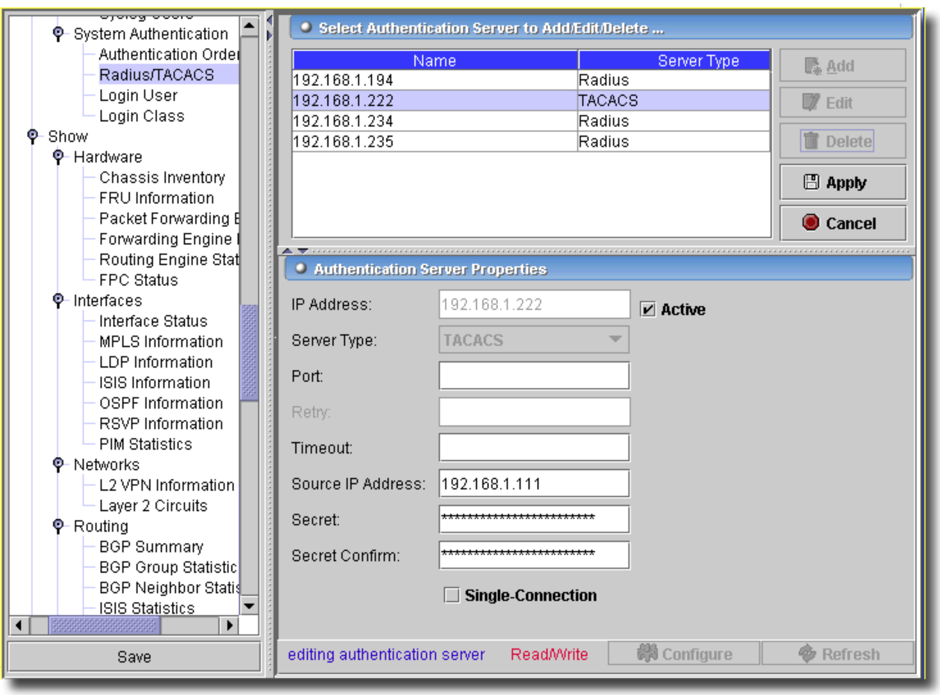
The available authentication types appear here in the *Available* panel. To override the default order, use the arrows (>) to move the authentication types to the right, *Selected* panel. Select and move them to the order you want authentication to occur with the up/down arrows.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

System Authentication -> Radius / TACACs

You can configure the router to use Radius or TACACS+ authentication. You can also specify multiple servers for each type. This authentication supports the following specific attributes: *Allow-commands*, *Deny-commands*, *Allow-configuration*, *Deny-configuration*.

Figure 13-119. Radius Authentication



Name	Server Type
192.168.1.194	Radius
192.168.1.222	TACACS
192.168.1.234	Radius
192.168.1.235	Radius

IP Address: 192.168.1.222 ☑ Active

Server Type: TACACS

Port:

Retry:

Timeout:

Source IP Address: 192.168.1.111

Secret: ************************

Secret Confirm: ************************

☐ Single-Connection

editing authentication server Read/Write

Click *Export* to save a description of the listed items. Use the *Add* or *Remove* buttons to manage rows in this table. Enter text directly in the row, once you add it. The following are its columns:

- **IP Address**—The IP address of the authentication server for this router to use.

- **Server Type**—Select *Radius* or *TACACs+*

- **Port**—The authentication port.

- **Retry**—The number of times to retry authentication (disabled for TACACs+).

- **Timeout**—The timeout, in seconds, for authentication tries.

- **Source IP Address**—The source IP for authentication.

- **Secret / Secret Confirm**—The password for the server selected.

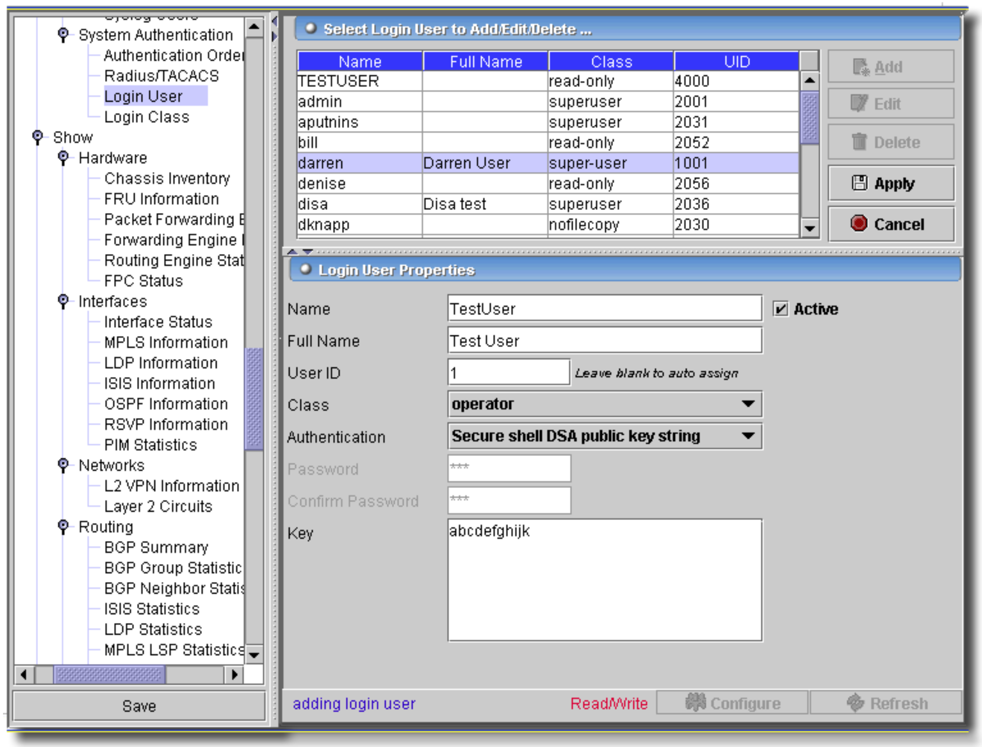
- **Single Connection**—Optimize TCP connection attempts (disabled for Radius).

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

System Authentication -> Login User

This screen lists the users who can have access to the selected device.

Figure 13-120. System Authentication: Users (Telnet & SSH)



Select Login User to Add/Edit/Delete ...

Name	Full Name	Class	UID
TESTUSER		read-only	4000
admin		superuser	2001
aputnins		superuser	2031
bill		read-only	2052
darren	Darren User	super-user	1001
denise		read-only	2056
disa	Disa test	superuser	2036
dknapp		nofilecopy	2030

Login User Properties

Name: TestUser ☑ Active

Full Name: Test User

User ID: 1 *Leave blank to auto assign*

Class: **operator**

Authentication: **Secure shell DSA public key string**

Password: ***

Confirm Password: ***

Key: abcdefghijk

adding login user Read/Write

Click *Export* to save a description of the listed items. Click *Add* or *Edit* a selected row to open the editor in the bottom panel. The editor has the following fields:

- **Name**—A short name for the user.

- **Full Name**—A text description of the user.

- **User ID**—A unique identifier for the user. The *Auto-assign* checkbox automates creating this from the previous fields.

- **Class**—User Permission level.

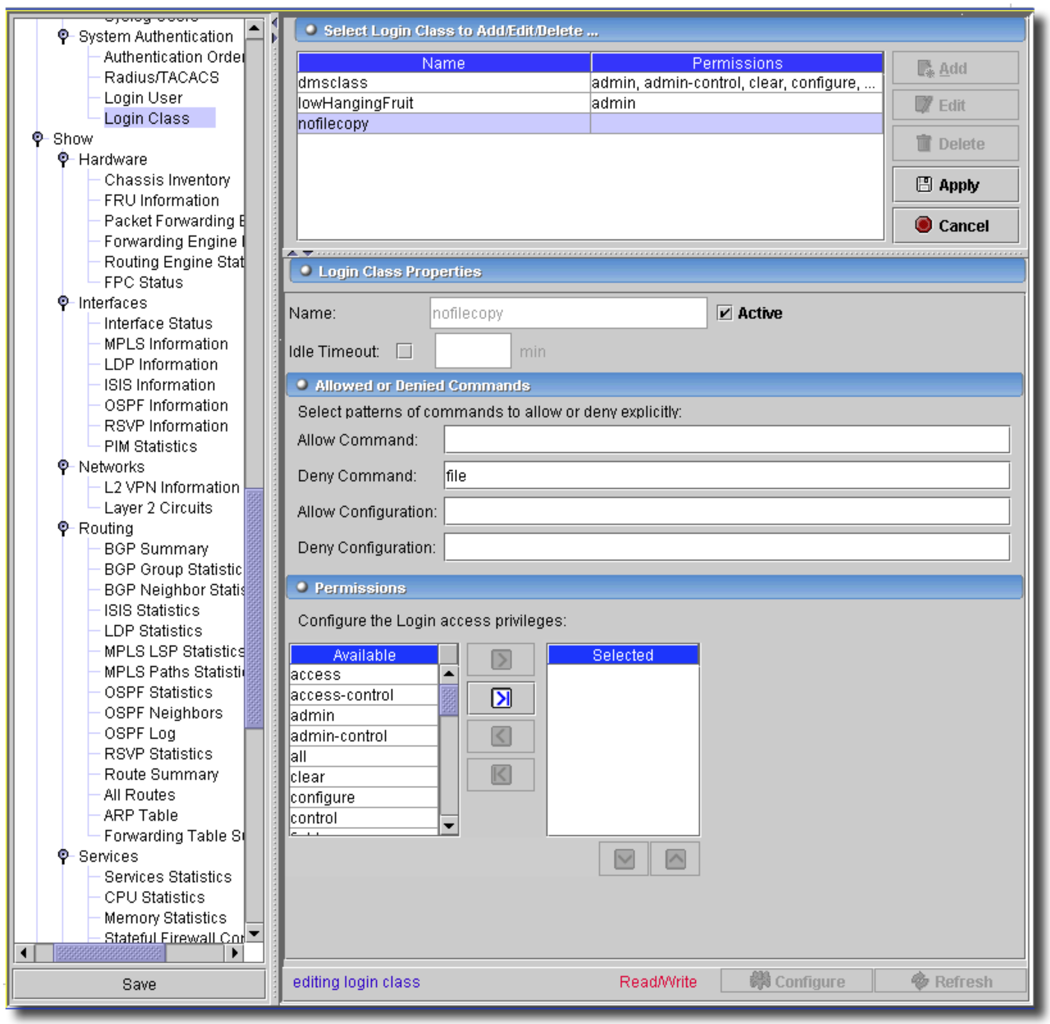
- **Authentication**—Select either *Plain text password (autoencrypted)*, *Secure Shell-DSA Public Keyring* or *Secure Shell-RSA Public Keyring*. If you select *plain-text-password*, the *Password* and *Confirm Password* fields appear in *Authentication Parameters*. If you select the *Secure Shell* alternatives, the *Key* field appears activated—a string distributed to remote IPs.

- Click *Apply* to accept your edits, or *Cancel* to abandon them.

System Authentication -> Login Class

This screen lets you configure authentication classes.

Figure 13-121. Authentication Class



Name	Permissions
dmsclass	admin, admin-control, clear, configure, ...
lowHangingFruit	admin
nofilecopy	

Name: nofilecopy ☑ Active

Idle Timeout: □ min

Select patterns of commands to allow or deny explicitly:

Allow Command:

Deny Command: file

Allow Configuration:

Deny Configuration:

Configure the Login access privileges:

Available	Selected
access	
access-control	
admin	
admin-control	
all	
clear	
configure	
control	

editing login class Read/Write

Click *Export* to save a description of the listed items. With the buttons on the upper screen, you can *Add*, *Edit* and *Delete* classes with the following characteristics:

Login-Class Properties

- **Name**—User Name.

- **Idle Timeout**—Check to enable this property, then set the maximum idle time (in minutes) before logout occurs.

Allowed or Denied Commands

These fields let you enter regular expressions for commands and configurations to allow or deny.

Permissions

Select from the operation categories available, moving the desired permissions to the *Selected Privileges* on the right side of the table.

Click A*pply* to accept your edits, and *Cancel* to abandon them. The *Configure* button at the bottom of this screen sends your login(s) to the device. The *Refresh* button queries to update information displayed.

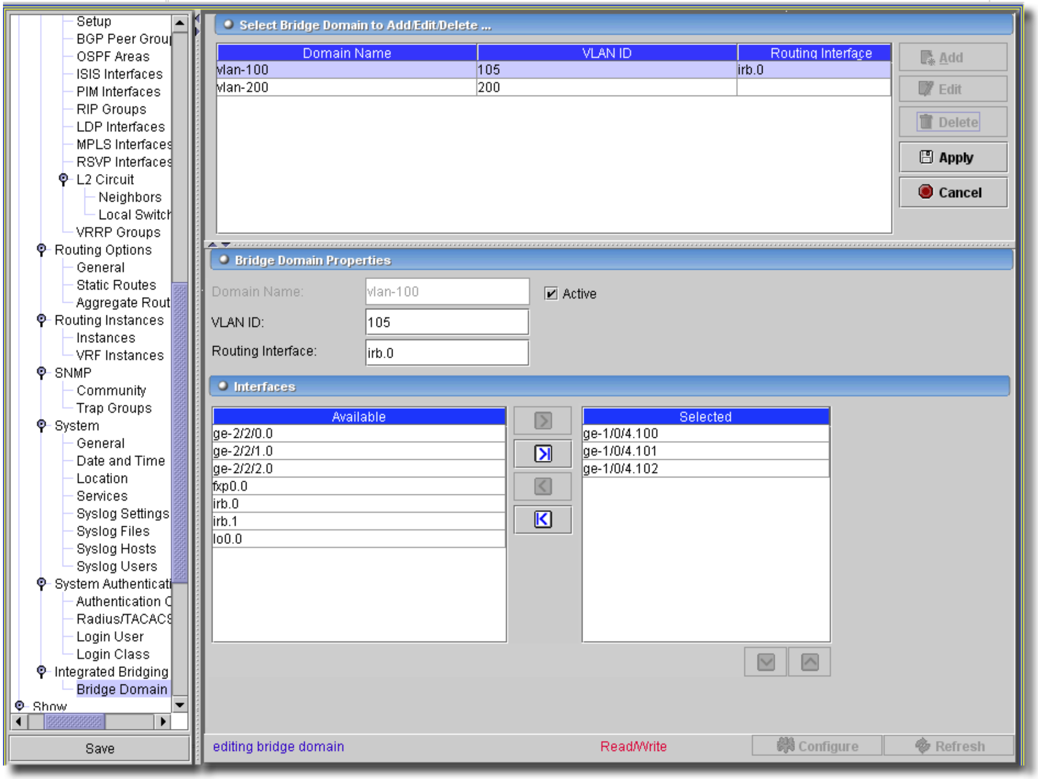
Integrated Bridging -> Bridge Domain

On MX routers, you can configure Integrated Routing and Bridging (IRB) with the IRB interface at the bridge domain level of the configuration. Configure IRB ports with port and unit screens. If an IRB port does not exist on the selected device, resync creates an empty one to allow access to these screens. Discovery also finds existing IRB ports.

IRB provides simultaneous support for Layer 2 (L2) bridging and Layer 3 (L3) routing within the same bridge domain. Packets arriving on an interface of the bridge domain are L2 switched or L3 routed based on the destination MAC address. Packets addressed to the router's MAC address are routed to other L3 interfaces. If the MAC address on the arriving frame is the same as that of the IRB interface, then the packet inside the frame is routed. Otherwise, the MAC address is learned or looked up in the MAC address database. The Virtual Router Redundancy Protocol (VRRP) is configured on the IRB interface so that both links can carry traffic between the bridge domain and the router network. See Protocols -> VRRP Groups on page 529 for more about VRRP Groups that include IRB.

The following screen lets you manage the Bridge Domains for the selected equipment.

Figure 13-122. Integrated Bridging -> Bridge Domain



Domain Name	VLAN ID	Routing Interface
vlan-100	105	irb.0
vlan-200	200	

Domain Name: vlan-100   ☑ Active

VLAN ID: 105

Routing Interface: irb.0

Available
ge-2/2/0.0
ge-2/2/1.0
ge-2/2/2.0
fxp0.0
irb.0
irb.1
lo0.0

Selected
ge-1/0/4.100
ge-1/0/4.101
ge-1/0/4.102

editing bridge domain   Read/Write

Use the *Add*, *Edit*, and *Delete* buttons to manage rows of Bridge domains in this table. Click *Export* to save a description of the listed items. When you *Add* or *Edit* a selected row, the editor panel at the bottom of the screen appears. Click *Apply* to accept your edits, or *Cancel* to abandon them. This screen has the following fields:

- **Domain Name**—A unique name for the domain you are configuring. When you edit an existing domain, this is read-only.
- **Enable**—Check this to enable the bridge domain.
- **VLAN ID**—The numeric ID for the bridge domain's VLAN.
- **Routing Interface**—The routing interface for the bridge domain. For example irb.0.

Interfaces

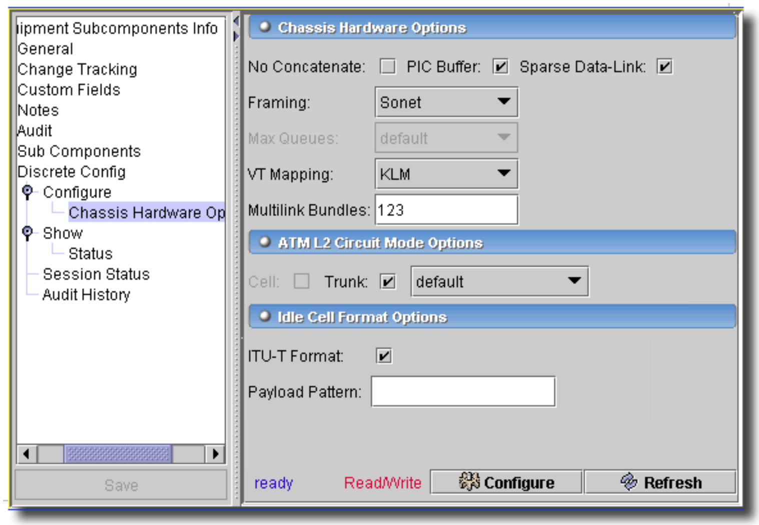
To include interfaces, use the arrows to move displayed interfaces from the *Available* to the *Selected* area.

Click *Apply* to accept your edits, and *Cancel* to abandon them. The *Configure* button at the bottom of this screen sends your login(s) to the device. The *Refresh* button queries to update information displayed.

PIC Configure -> Chassis Hardware

This screen appears when you open a selected PIC in Equipment Manager.

Figure 13-123. PIC Chassis Hardware



Chassis Hardware Options

No Concatenate: □ PIC Buffer: ☑ Sparse Data-Link: ☑

Framing: Sonet

Max Queues: default

VT Mapping: KLM

Multilink Bundles: 123

ATM L2 Circuit Mode Options

Cell: □ Trunk: ☑ default

Idle Cell Format Options

ITU-T Format: ☑

Payload Pattern:

ready Read/Write

It has the following fields:

Chassis Hardware Options

- **No Concatenate**—Do not concatenate channels.

- **PIC buffer**—Run in large delay buffer mode.

- **Sparse Data-Link**—Run in sparse data-link connection identifier mode.

- **Framing**—Framing mode. Select from the following: *default*, *SDH*, *Sonet*.

- **Max Queues**—Maximum number of queues per interface on QOS-capable PIC (- 4, - 8). This attribute is on only these devices: M320, T320, T640 & Tx Matirx.

- **VT Mapping**—Virtual tunnel mapping mode. Select from the pick list (*default*, *ITU-T*, *KLM*).

- **Multilink Bundles**—Number of multilink Frame Relay UNI NNI (FRF.16) bundles to allocate on PIC (1-255)

ATM l2 Circuit Mode Options

The following enable ATM Layer 2 circuit transport mode. Check or select where appropriate. Cell and trunk options are mutually exclusive.

- **Cell**—ATM Layer 2 circuit cell mode

- **Trunk**—Set ATM Layer 2 circuit trunk mode. The following trunk selections from the pick list to the right of this checkbox are optional:

  Network-to-Network–ATM Layer 2 circuit network-to-network interface trunk mode

  User-to-Network–ATM Layer 2 circuit user-to-network interface trunk mode.

Idle Cell Format Options

- **ITU-T Format**—ITU-T idle cell header format. Check for itu-t -> ITU-T mode, uncheck for KLM mode.

- **Payload Pattern**—Payload pattern byte (0x00-0xff).

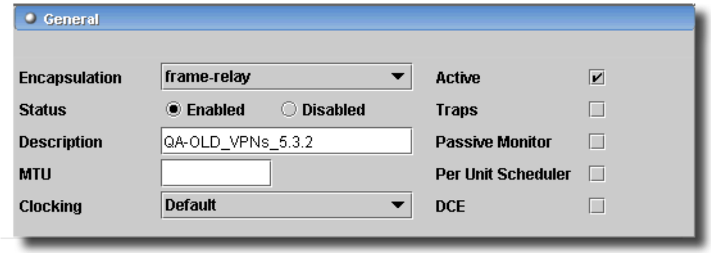
The *Configure* button at the bottom of this screen sends your configuration to the device. The *Refresh* button queries to update information displayed.

Configuring Interfaces

This screen lets you configure several port types. The general options are common to all port types. Depending on the port selected various tabs let you configure them. (See Options on page 578)

General

Figure 13-124. Interface Configuration—General



General

Encapsulation	frame-relay	Active	☑
Status	● Enabled ○ Disabled	Traps	□
Description	QA-OLD_VPNs_5.3.2	Passive Monitor	□
MTU		Per Unit Scheduler	□
Clocking	Default	DCE	□

NOTE:

Viewing this screen may require you to navigate to an interface.

The General part of this screen lets you configure the following fields/pick lists:

- **Encapsulation**—Physical link-layer encapsulation. Available options include the following:

  atm-ccc-cell-relay—ATM cell relay encapsulation for cross-connect.

  atm-pvc—ATM permanent virtual circuits.

  cisco-hdlc—Cisco-compatible HDLC framing.

cisco-hdlc-ccc—Cisco-compatible HDLC framing for a cross-connect.

cisco-hdlc-tcc—Cisco-compatible HDLC framing for a translational cross-connect.

ethernet-ccc—Ethernet cross-connect.

ethernet-over-atm—Ethernet over ATM encapsulation.

ethernet-tcc—Ethernet translational cross-connect.

ethernet-vpls—Ethernet Virtual Private LAN Service (VPLS).

extended-frame-relay-ccc—Any Frame Relay DLCI for cross-connect.

extended-frame-relay-tcc— Any Frame Relay DLCI for translational cross-connect.

extended-vlan-ccc—Nonstandard TPID tagging for a cross-connect.

extended-vlan-tcc—802.1Q tagging for a translational cross-connect.

extended-vlan-vpls—Extended VLAN Virtual Private LAN Service (VPLS).

flexible-frame-relay—Multiple Frame Relay encapsulations.

frame-relay—Frame Relay encapsulation.

frame-relay-ccc—Frame Relay for cross-connect.

frame-relay-tcc—Frame Relay for translational cross-connect.

multilink-frame-relay-uni-nni—Multilink Frame Relay UNI NNI (FRF.16) encapsulation.

ppp—Serial PPP device.

ppp-ccc—Serial PPP device for a cross-connect.

ppp-tcc—Serial PPP device for a translational cross-connect.

vlan-ccc—802.1Q tagging for a cross-connect.

vlan-vpls—VLAN Virtual Private LAN Service (VPLS).

Status—Enable or Disable the physical link

Description—Text description of interface

MTU—Maximum transmit packet size (256 - 9192)

Clocking—Interface clock source. This has the following potential values:

external—Clocking provided by DCE (loop timing).

internal—Clocking provided by local system.

- **Traps**—Enable SNMP notifications on state changes
- **Passive Monitor**—Use interface to tap packets from another router
- **Per Unit Scheduler**—Enable subunit queueing on Frame Relay or VLAN QPP interface
- **DCE**—Respond to Frame Relay status enquiry messages

Options

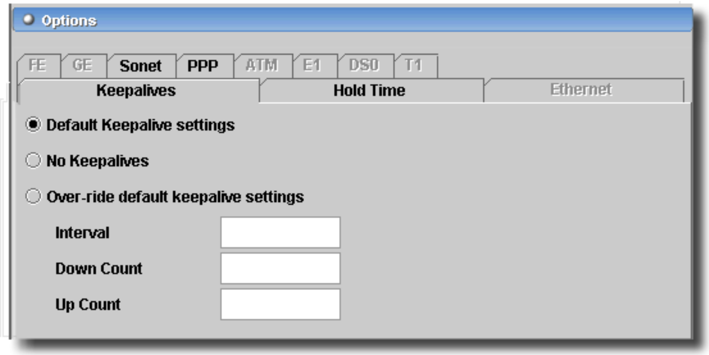
The following sections describe tabs that appear based on port type you are configuring. Available tabs appear not grayed out.

- KeepAlives
- Hold Time
- Ethernet
- Fast Ethernet
- GE (Gigabit Ethernet)
- Sonet
- PPP
- ATM
- E1
- DS0
- T1
- Serial

KeepAlives

This screen configures sending or demanding keepalive messages.

Figure 13-125. Interface Configuration—KeepAlives



● Default Keepalive settings

○ No Keepalives

○ Over-ride default keepalive settings

Interval

Down Count

Up Count

- **Default Keepalive settings**—Remove any keepalive configuration from the interface and use system defaults.

No Keepalives—Do not send or demand keepalive messages.

- **Over-ride default keepalive settings**—Configures the entered interval, up and down count settings

Interval—Keepalive period (1 - 32767 seconds)

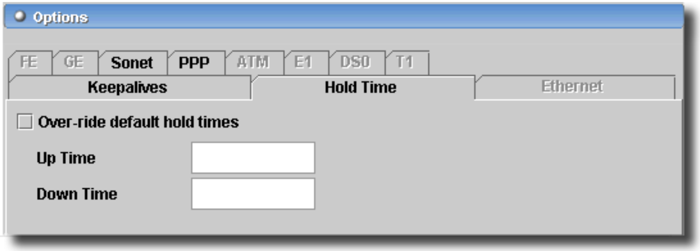
Down Count—Keepalive missed to bring link down (1 - 255)

Up Count—Keepalive received to bring link up (1 - 255)

Hold Time

This screen configures the hold time for link up and link down.

Figure 13-126. Interface Configuration—Hold Times



☐ Over-ride default hold times

Up Time

Down Time

The checkbox (*Over-ride default hold times*) enables the following fields:

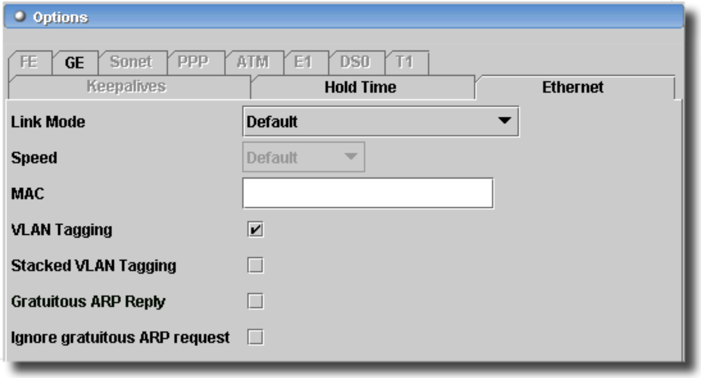
- **Up Time**—Link up hold time (0 - 65,534 milliseconds)

- **Down Time**—Link down hold time (0 - 65,534 milliseconds)

Ethernet

This screen configures ethernet parameters.

Figure 13-127. Interface—Ethernet



Link Mode: Default

Speed: Default

MAC

VLAN Tagging ☑

Stacked VLAN Tagging ☐

Gratuitous ARP Reply ☐

Ignore gratuitous ARP request ☐

- **Link Mode**—Link operational mode (*Full Duplex* or *Half Duplex*).

- **Speed**—Link speed, 10m or 100m (Fast Ethernet only).

- **MAC**—Hardware MAC address.

- **VLAN Tagging**—802.1Q VLAN tagging support.

- **Stacked VLAN Tagging**—Stacked 802.1Q VLAN tagging support (Gigabit Ethernet only).

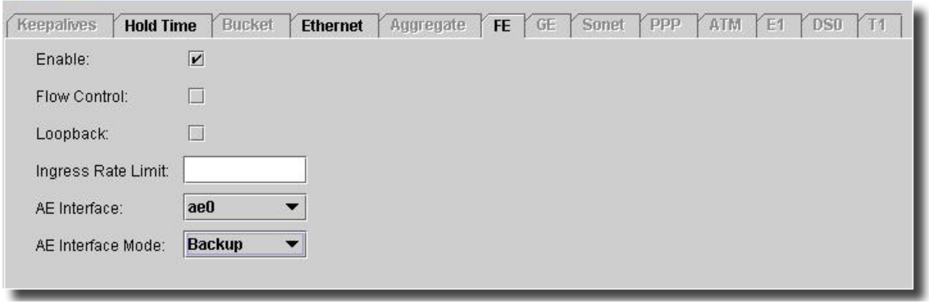
- **Gratuitous ARP Reply**—Enable/Disable gratuitous ARP reply.

- **Ignore gratuitous ARP request**—Ignore gratuitous ARP request.

Fast Ethernet

This screen configures fast ethernet parameters.

Figure 13-128. Interface—Fast Ethernet



Enable: ☑

Flow Control: □

Loopback: □

Ingress Rate Limit:

AE Interface: ae0

AE Interface Mode: Backup

The *Enable* checkbox lets you use the following fields:

- **Flow Control**—Enable/Disable flow control.

- **Loopback**—Enable/Disable loopback.

- **Ingress Rate Limit**—Ingress rate at the port (1 - 100 megabits per second).

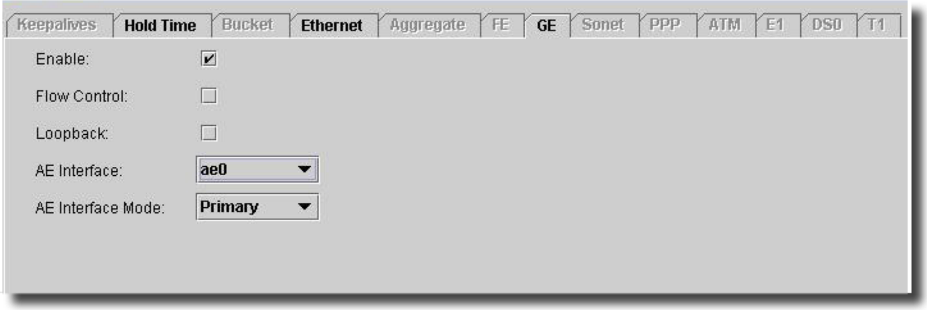
- **AE Interface—**Select which aggregate interface with a pick list (not available for all devices).

- **AE Interface Mode—**Select which aggregate interface mode with a pick list (*Primary* / *Backup*—not available for all devices).

GE (Gigabit Ethernet)

This screen configures gigabit ethernet parameters.

Figure 13-129. Interface—Gigabit Ethernet



Enable: ☑

Flow Control: □

Loopback: □

AE Interface: ae0

AE Interface Mode: Primary

The *Enable* checkbox lets you use the following fields:

- **Flow Control—**Enable/Disable flow control.

- **Loopback—**Enable/Disable loopback.

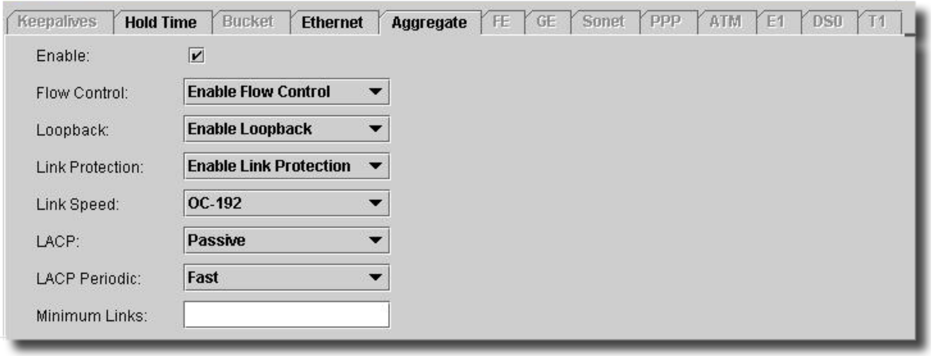
- **AE Interface—**Select which aggregate interface with a pick list (not available for all devices).

- **AE Interface Mode—**Select which aggregate interface mode with a pick list (*Primary* / *Backup*—not available for all devices).

Aggregate

This screen configures aggregate ethernet interface options.

Figure 13-130. Interface—Aggregate



Enable: ☑

Flow Control: Enable Flow Control

Loopback: Enable Loopback

Link Protection: Enable Link Protection

Link Speed: OC-192

LACP: Passive

LACP Periodic: Fast

Minimum Links:

The *Enable* checkbox lets you use the following fields:

- **Flow Control—**Enable/Disable flow control.

- **Loopback—**Enable/Disable loopback.

- **Link Protection**—Elect to *Enable* / *Disable* link protection.

- **Link Speed**—Select from the pick list. On aggregated Ethernet interfaces, you can set the required link speed for all interfaces included in the bundle. All interfaces that make up a bundle must be the same speed. For aggregated Ethernet links, you can specify speed in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).

  Aggregated SONET/SDH links can have one of the following speed values.

  - oc3—Links are OC-3c or STM-1c.
  - oc12—Links are OC-12c or STM-4c.
  - oc48—Links are OC-48c or STM-16c.
  - oc192—Links are OC-192c or STM-64c.

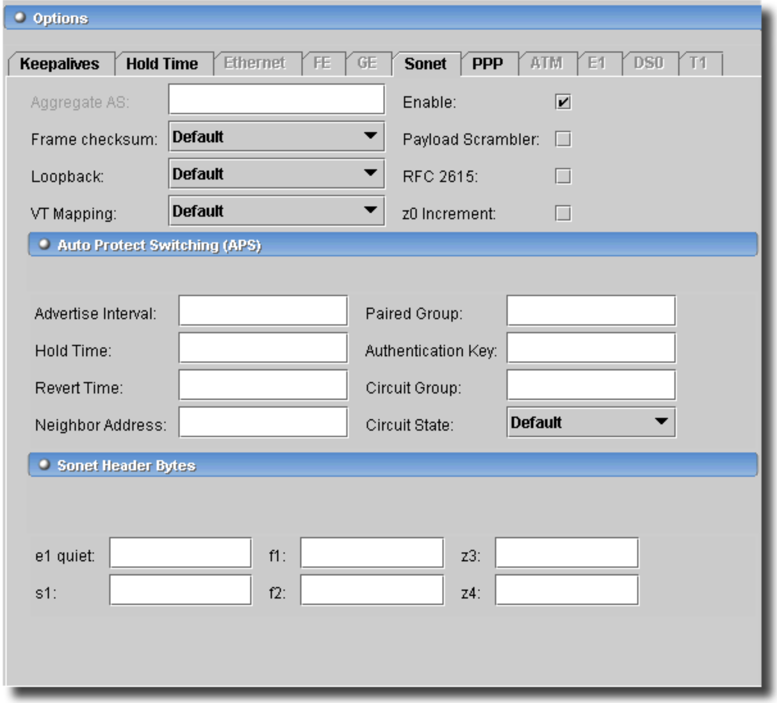
- **LACP**—Select from the pick list. The LACP mode can be *Active* or *Passive*. If the actor and partner are both in passive mode, they do not exchange LACP packets, which results in the aggregated Ethernet links not coming up. If either the actor or partner is active, they do exchange LACP packets. By default, LACP is in passive mode on aggregated Ethernet interfaces. To initiate transmission of LACP packets and response to LACP packets, you must enable LACP *Active* mode.

- **LACP Periodic**—By default, the actor and partner send LACP packets every second. You can configure the interval at which the interfaces send LACP packets in this field.
- **Minimum Links**—Enter the minimum number of links. On aggregated Ethernet interfaces, you can configure the minimum number of links that must be *up* for the bundle as a whole to be labeled *up*. By default, only one link must be up for the bundle to be labeled up.

Sonet

This screen configures Sonet options.

Figure 13-131. Interface—Sonet



Options

Keepalives | Hold Time | Ethernet | FE | GE | Sonet | PPP | ATM | E1 | DS0 | T1

Aggregate AS:
Enable: ☑
Frame checksum: Default
Payload Scrambler: □
Loopback: Default
RFC 2615: □
VT Mapping: Default
z0 Increment: □

Auto Protect Switching (APS)

Advertise Interval:
Paired Group:
Hold Time:
Authentication Key:
Revert Time:
Circuit Group:
Neighbor Address:
Circuit State: Default

Sonet Header Bytes

e1 quiet:
f1:
z3:
s1:
f2:
z4:

The *Enable* checkbox lets you use the following fields:

General Sonet Options

- **Aggregate AS**—Join a SONET aggregate
- **Frame Checksum**—Configure frame checksum to default, 16 bit mode or 32 bit mode
- **Loopback**—Set loopback to default, Local or Remote
- **VT Mapping**—Set VT mapping mode to ITU-T or KLM
- **Payload Scrambler**—Enable/Disable payload scrambling

- **RFC 2615**—RFC 2615 compliance
- **Z0 Increment**—Increment Z0 in SDH mode

Auto Protection Switching Options

- **Advertise Interval**—Advertise interval (milliseconds)
- **Hold Time**—Hold time (milliseconds)
- **Revert Time**—Circuit revert time (seconds)
- **Neighbor Address**—IP Address of Neighbor
- **Paired Group**—Name of paired APS group
- **Authentication Key**—Authentication key
- **Circuit Group**—Working or Protected circuit group name, based on state.
- **Circuit State**—Request/Force circuit state. This lets you select from the following options:

  default—System default

  lockout—Lockout protection

  request-working—Request working circuit state

  request-protect—Request protect circuit state

  force-working—Force working circuit state

  force- protect—Force protect circuit state

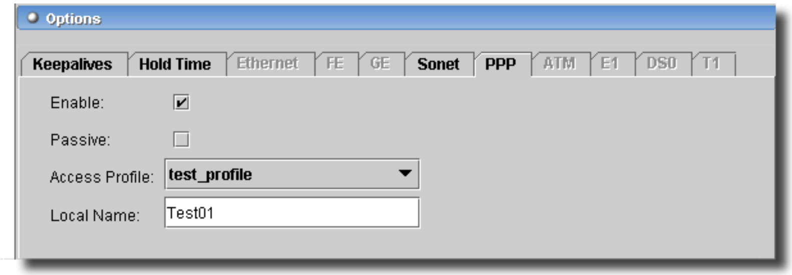
Sonet Header Bytes Options

- **E1 Quiet**—E1-quiet value (0 - 255)
- **S1**—S1/Z1 value (stratum clock by convention) (0 - 255)
- **F1**—F1 user value (0 - 255)
- **F2**—F2 user value (0 - 255)
- **Z3**—Z3 user value (0 - 255)
- **Z4**—Z4 user value (0 - 255)

PPP

This screen lets you configure the ppp chap parameters.

Figure 13-132. Interface—PPP



Enable: ☑

Passive: □

Access Profile: test_profile

Local Name: Test01

The *Enable* checkbox lets you use the following fields:

- **Access Profile**—Profile containing client list and access parameters.

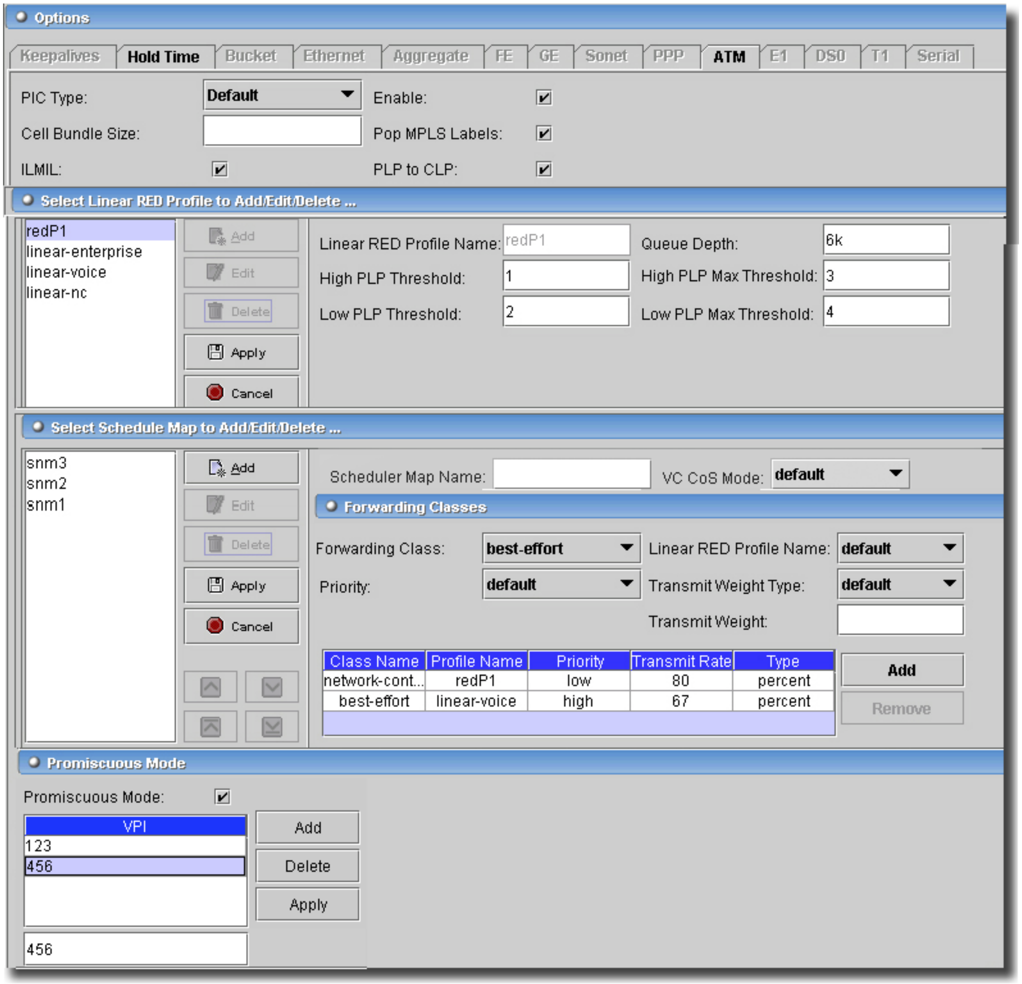
- **Local Name**—Name sent in CHAP-Challenge and CHAP-Response.

- **Passive**—Handle incoming CHAP requests only.

ATM

This screen is where you configure ATM parameters.

Figure 13-133. Interface—ATM



PIC Type: Default

Enable: ☑

Cell Bundle Size:

Pop MPLS Labels: ☑

ILMIL: ☑

PLP to CLP: ☑

Select Linear RED Profile to Add/Edit/Delete ...

redP1
linear-enterprise
linear-voice
linear-nc

Linear RED Profile Name: redP1

Queue Depth: 6k

High PLP Threshold: 1

High PLP Max Threshold: 3

Low PLP Threshold: 2

Low PLP Max Threshold: 4

Select Schedule Map to Add/Edit/Delete ...

snm3
snm2
snm1

Scheduler Map Name:

VC CoS Mode: default

Forwarding Classes

Forwarding Class: best-effort

Linear RED Profile Name: default

Priority: default

Transmit Weight Type: default

Transmit Weight:

Class Name	Profile Name	Priority	Transmit Rate	Type
network-cont...	redP1	low	80	percent
best-effort	linear-voice	high	67	percent

Promiscuous Mode

Promiscuous Mode: ☑

VPI
123
456

456

The *Enable* checkbox lets you use the following fields:

- **PIC Type**—Type of ATM PIC (ATM II or ATM I).
- **Cell Bundle Size**—L2 circuit cell bundle size (1 - 176 cells).
- **ILMIL**—Enable Interim Local Management Interface.
- **Pop MPLS Labels**—Pop all MPLS labels off incoming packets.
- **PLP to CLP**—Enable ATM2 PLP to CLP copy.

Linear RED Profiles

Click *Add* to create a new profile, or *Edit* to alter an existing, selected one. *Delete* removes a selected, listed profile. The editor for this panel has the following fields:

- **Linear RED Profile Name**—ATM2 CoS virtual circuit drop profiles.

- **High PLP Threshold**—Enter the threshold. This is the fill level percentage when linear RED is applied for high PLP (1-100).

- **Low PLP Threshold**—Enter the L2 circuit cell bundle size (1-176 cells)

- **Queue Depth**—Enter the maximum queue depth (1 - 64,000 cells).

- **High PLP Max Threshold**—Enter the fill level percentage with 100 percent packet drop for high PLP (0 - 100).

- **Low PLP Max Threshold**—Enter the fill level percentage with 100 percent packet drop for low PLP (0 - 100).

Click *Apply* to accept your edits, or *Cancel* to abandon them. Use the up/down arrows to re-order selected RED profiles that appear in this list.

Schedule Map

Click *Add* to create a new schedule map, or *Edit* to alter an existing, selected one. *Delete* removes a selected, listed schedule map. The editor for this panel has the following fields:

Scheduler Map Name—Enter a text identifier for the scheduler map.

VC CoS Mode—Select from the pick list. Options include *default*, *alternate*, *strict*.

Forwarding Classes

- **Forwarding Class**—Select from the pick list. Options include *best-effort*, *expedited-forwarding*, *assured-forwarding*, *network-control*.

Linear RED Profile Name—Select from the pick list.

Priority—Select from the pick list. Options include *default*, *high*, *low*.

- **Transmit Weight Type**—Select from the pick list. Options include *default*, *cells*, *percent*.

Transmit Weight—Enter a weight.

Click *Add* to add the configured forwarding class to those listed. Click *Remove* to delete a selected, listed forwarding class from the list.

Click *Apply* to accept your edits to the listed forwarding classes to the schedule map you are configuring, or *Cancel* to abandon them. Use the up/down arrows to re-order selected schedule maps that appear in this list.

Promiscuous Mode

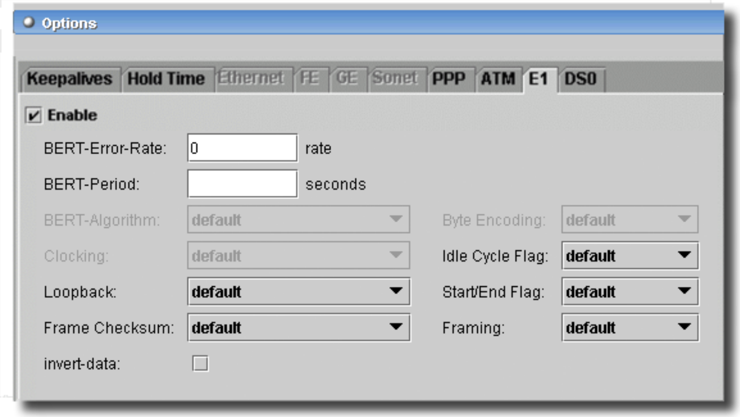
- **Promiscuous Mode**—Check to set the ATM interface to promiscuous mode. This opens the listed VPIs (0 - 255) in promiscuous mode.

Enter a VPI below the table in this panel, and click *Add* to list a VPI. You can also select a VPI, and edit it in the field below the list. Click *Apply* to accept your edits. Select a VPI and click *Delete* to remove it from the list.

E1

This screen lets you configure E1 options.

Figure 13-134. Interface - E1



☑ Enable

BERT-Error-Rate: 0 rate

BERT-Period: seconds

BERT-Algorithm: default

Byte Encoding: default

Clocking: default

Idle Cycle Flag: default

Loopback: default

Start/End Flag: default

Frame Checksum: default

Framing: default

invert-data: □

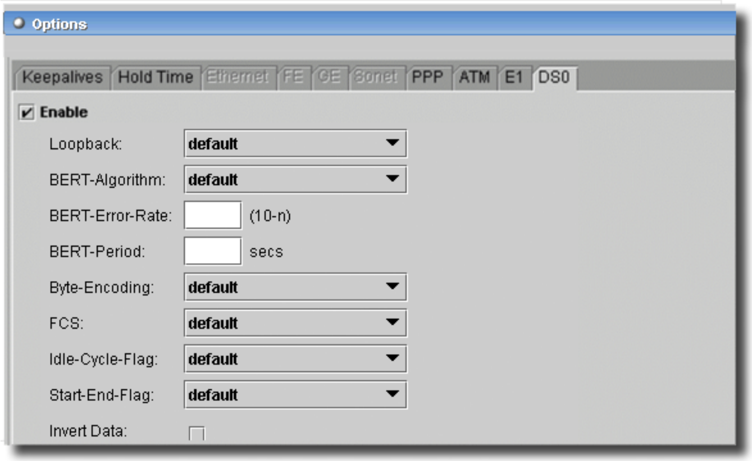
The *Enable* checkbox lets you use the following fields:

- **BERT Algorithm**—Set BERT algorithm.
- **BERT Error Rate**—Bit error rate to use in BERT test (10^-n) (0 - 7).
- **BERT Period**—Length of BERT test (1 - 240 seconds).
- **Frame Checksum**—Frame checksum; *16* or *32-bit mode*.
- **Framing Mode**—Framing mode. Select from the following options:
  - *g704*—G704 mode with CRC4
  - *g704-no-crc4*—G704 mode without CRC4
  - *unframed*—Unframed mode
- **Idle Cycle Flag**—Value to transmit in idle cycles: *0x7E* or *0xFF.*
- **Invert Data**—Invert data.
- **Loopback Mode**—Loopback Mode: *local* or *remote*.
- **Start/End Flag**—Set start/end flags on transmission. Select from the following options:
  - *filler*—Send two idle cycles between start/end flags.
  - *shared*—Share start/end flags on transmit.

DS0

This screen lets you configure DS0 options.

Figure 13-135. Interface—DS0



☑ Enable

Loopback: default

BERT-Algorithm: default

BERT-Error-Rate: (10-n)

BERT-Period: secs

Byte-Encoding: default

FCS: default

Idle-Cycle-Flag: default

Start-End-Flag: default

Invert Data: □

- **BERT Algorithm**—Set BERT algorithm.
- **BERT Error Rate**—Bit error rate to use in BERT test (10^-n) (0 - 7).
- **BERT Period**—Length of BERT test (1 - 240 seconds).
- **Frame Checksum**—Frame checksum; *16* or *32-bit mode*.
- **Byte Encoding**—Byte encoding; *7* or *8 bits per byte*.
- **Idle Cycle Flag**—Value to transmit in idle cycles; *0x7E* or *0xFF.*
- **Invert Data**—Invert data.
- **Loopback Mode**—Loopback mode; Default or Payload.
- **Start/End Flag**—Set start/end flags on transmission.

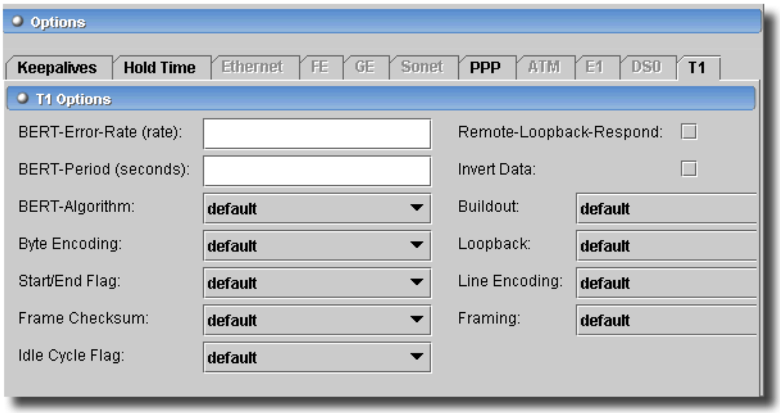
  filler—Send two idle cycles between start/end flags

  shared—Share start/end flags on transmit

T1

This screen lets you configure T1 options.

Figure 13-136. Interfaces—T1



BERT-Error-Rate (rate):

BERT-Period (seconds):

BERT-Algorithm: default

Byte Encoding: default

Start/End Flag: default

Frame Checksum: default

Idle Cycle Flag: default

Remote-Loopback-Respond: □

Invert Data: □

Buildout: default

Loopback: default

Line Encoding: default

Framing: default

This tab has the following fields:

- **BERT-error-rate (rate)**—Bit error rate (10 ^ -n for n > 0, and zero for n = 0) (0-7)
- **Remote-Loopback-Respond**—Respond to loop requests from remote end.
- **BERT-period (seconds)**—Length of BERT test (1-240 seconds)
- **Invert Data**—Check to invert data.
- **BERT-algorithm**—Use the pick list to set the BERT algorithm. The following are available options:

  all-ones-repeating–Repeating one bits

  all-zeros-repeating–Repeating zero bits

  alternating-double-ones-zeros–Alternating pairs of ones and zeros

  alternating-ones-zeros–Alternating ones and zeros

  pseudo-2e10–Pattern is 2 ^ 10 - 1

  pseudo-2e11-o152–Pattern is 2 ^ 11 -1 (per O.152 standard)

  pseudo-2e15-o151–Pattern is 2 ^ 15 - 1 (per O.151 standard)

  pseudo-2e17–Pattern is 2 ^ 17 - 1

  pseudo-2e18–Pattern is 2 ^ 18 - 1

  pseudo-2e20-o151–Pattern is 2 ^ 20 - 1 (per O.151 standard)

  pseudo-2e20-o153–Pattern is 2 ^ 20 - 1 (per O.153 standard)

  pseudo-2e21–Pattern is 2 ^ 21 - 1

  pseudo-2e22–Pattern is 2 ^ 22 - 1

  pseudo-2e23-o151–Pattern is 2 ^ 23 (per O.151 standard)

  pseudo-2e25–Pattern is 2 ^ 25 - 1

pseudo-2e28–Pattern is 2 ^ 28 - 1

pseudo-2e29–Pattern is 2 ^ 29 - 1

pseudo-2e3–Pattern is 2 ^ 3 - 1

pseudo-2e31–Pattern is 2 ^ 31 - 1

pseudo-2e32–Pattern is 2 ^ 32 - 1

pseudo-2e4–Pattern is 2 ^ 4 - 1

pseudo-2e5–Pattern is 2 ^ 5 - 1

pseudo-2e6–Pattern is 2 ^ 6 - 1

pseudo-2e7–Pattern is 2 ^ 7 - 1

pseudo-2e9-o153–Pattern is 2 ^ 9 - 1 (per O.153 standard)

repeating-1-in-4–1 bit in 4 is set

repeating-1-in-8–1 bit in 8 is set

repeating-3-in-24–3 bits in 24 are set

- **Buildout**—Line buildout. Options include:

  0-132–Line buildout is between 0-132 feet

  133-265–Line buildout is between 133-265 feet

  266-398–Line buildout is between 266-398 feet

  399-531–Line buildout is between 399-531 feet

  532-655–Line buildout is between 532-655 feet

- **Byte-encoding**—Byte encoding. Options include the following:

  nx56–7 bits per byte

  nx64–8 bits per byte

- **Loopback mode**—Options include:

  local–Local loopback

  payload–Payload loopback

  remote–Remote loopback

- **Start/End Flag**—Set start/end flags on transmission. Options include:

  filler–Send two idle cycles between start/end flags

  shared–Share start/end flags on transmit

- **Line encoding**—Set line encoding with the following options:

  ami–Automatic mark inversion

  b8zs–8-bit zero suppression

- **Frame checksum**—Options include:

16–16-bit mode

32–32-bit mode

- **Framing**—Options include:

  esf–Extended super frame

  sf–Super frame

- **Idle Cycle Flag**—Value to transmit in idle cycles.

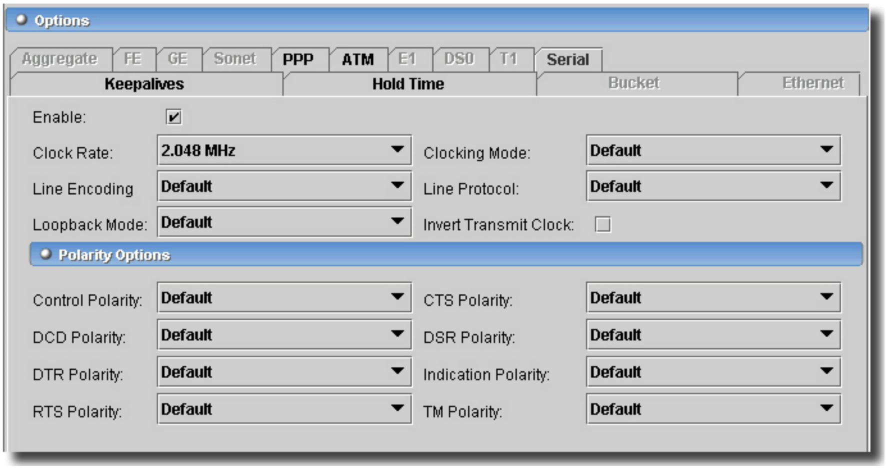
  flags–Transmit 0x7E in idle cycles

  ones–Transmit 0xFF (all ones) in idle cycles

Serial

This screen lets you configure serial options.

Figure 13-137. Interfaces—Serial



Enable: ☑

Clock Rate: 2.048 MHz

Clocking Mode: Default

Line Encoding: Default

Line Protocol: Default

Loopback Mode: Default

Invert Transmit Clock: □

Control Polarity: Default

CTS Polarity: Default

DCD Polarity: Default

DSR Polarity: Default

DTR Polarity: Default

Indication Polarity: Default

RTS Polarity: Default

TM Polarity: Default

This screen has the following fields:

- **Enable**—Check to enable
- **Clock Rate**—Select from the pick list.
- **Line Encoding**—Select from the pick list.
- **Loopback Mode**—Select from the pick list.
- **Clocking Mode**—Select from the pick list.
- **Line Protocol**—Select from the pick list.
- **Invert Transmit Clock**—Check to enable

Polarity Options

- **Control Polarity**—Select from the pick list.

- **DCD Polarity**—Select from the pick list.

- **DTR Polarity**—Select from the pick list.

- **RTS Polarity**—Select from the pick list.

- **CTS Polarity**—Select from the pick list.

- **DSR Polarity**—Select from the pick list.

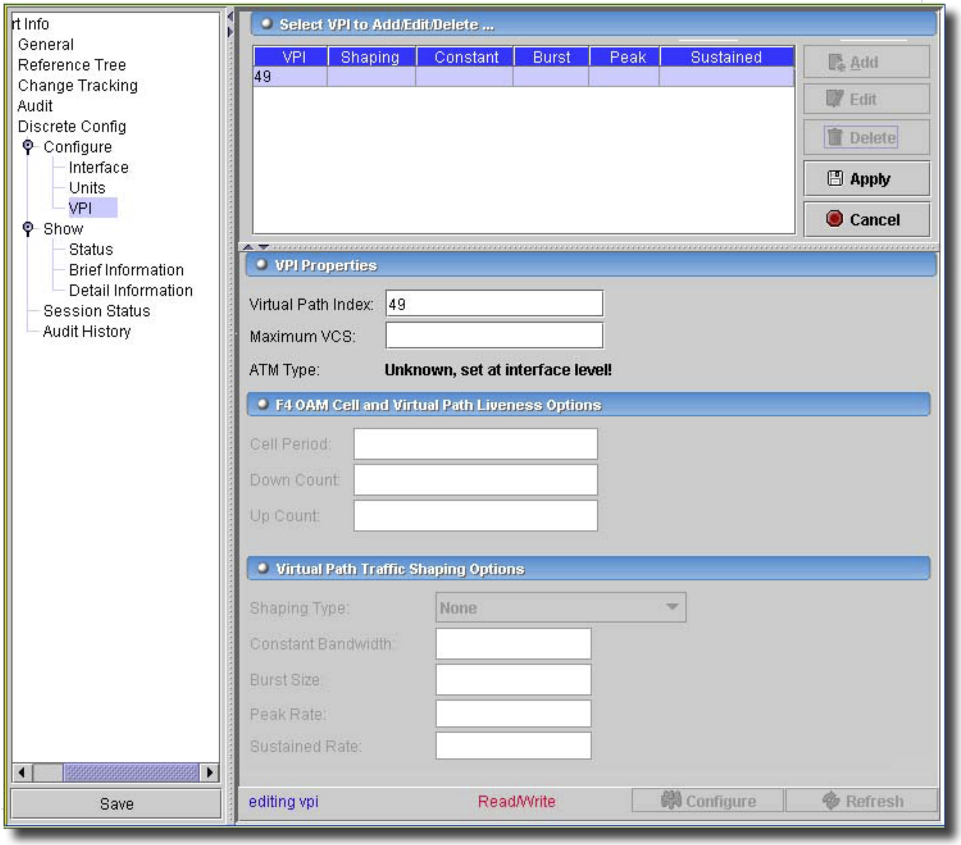
- **Indication Polarity**—Select from the pick list.

- **TM Polarity**—Select from the pick list.

ATM Port -> VPI

This screen appears when you edit an ATM physical port and select the VPI options under configure. Click *Export* to save a description of the listed items. Select a listed VPI to *Add* or *Edit* (you can also *Delete* these), and the lower panel displays the editor where you can alter parameters. The editor screen that appears in the lower panel depends on the VPI you select.

Figure 13-138. Editing ATM I



VPI	Shaping	Constant	Burst	Peak	Sustained
49					

Virtual Path Index: 49

Maximum VCS:

ATM Type: Unknown, set at interface level!

Shaping Type: None

editing vpi

Read/Write

You can only configure two parameters for ATM I: the *Virtual Path Index* and the *Maximum VCS*.

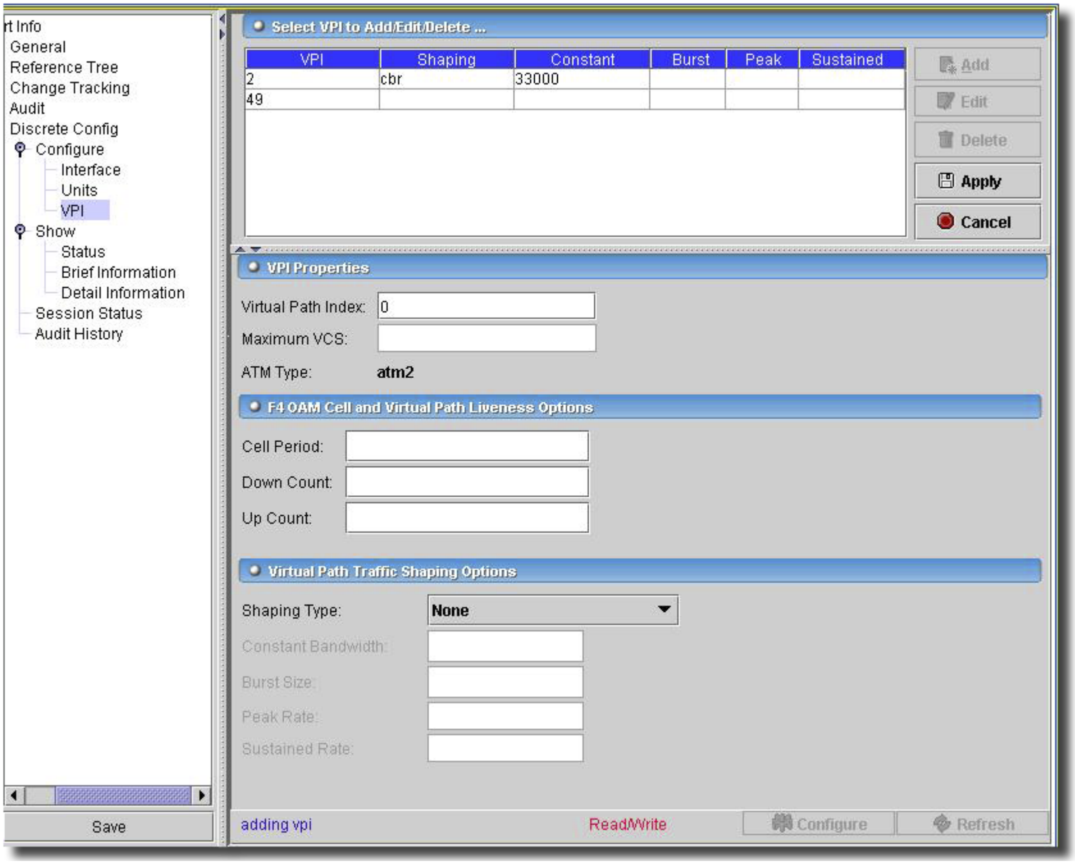
F4 OAM Cell and Virtual Path Liveness Options

Maximum VCS is not supported For ATM II. Instead you can configure F4 OAM cell options: *Period*, *Down Count* and *Up Count*.

ATM II Virtual Path Traffic Shaping Options

Along with shaping options, the editing screen for adding, editing and deleting an ATM II VPI statement lets you alter the following parameters:

Figure 13-139. Editing ATM II VPI



VPI	Shaping	Constant	Burst	Peak	Sustained
2	cbr	33000			
49					

Virtual Path Index: 0

Maximum VCS:

ATM Type: atm2

Cell Period:

Down Count:

Up Count:

Shaping Type: None

Constant Bandwidth:

Burst Size:

Peak Rate:

Sustained Rate:

adding vpi

Read/Write

Click *Add* or *Edit* a selected row to open the editor in the bottom panel. Click *Apply* to accept your edits, or *Cancel* to abandon them. The editor has the following fields:

- **Virtual path index**—Define a virtual path index (0 - 255).

- **Maximum VCS**—Maximum number of virtual circuits on this VPI.

- **ATM Card Type**—Displays the current card type and mode (*atm1* or *atm2*).

F4 OAM Cell and Virtual Path Liveness Options

Cell period—F4 OAM cell period (1 - 900 seconds).

Down Count—Number of F4 OAM cells to consider VP down (1 - 255).

Up Count—Number of F4 OAM cells to consider VP up (1 - 255).

Virtual Path Traffic Shaping Options

- **Shaping type**—Virtual path traffic-shaping type. Options include the following:

cbr—Constant bandwidth utilization.

rtvbr—ATM2 real-time variable bandwidth utilization.

vbr—Variable bandwidth utilization.

- **Constant Bandwidth**—(For shaping type cbr only) Constant bandwidth utilization (*33,000 - 542,526,792*).

Burst size—For shaping type vbr and rtvbr, (*1 - 4,000*).

Peak rate—For shaping type vbr and rtvbr, (*33,000 - 542,526,792*).

Sustained rate—For shaping type vbr and rtvbr (*33,000 - 542,526,792*).

Click A*pply* to accept the edits you make on this screen, and C*ancel* to abandon them.

Unit Configuration

Unit configuration screens include an upper screen (for General configuration) that varies, depending on the unit type and encapsulation selected, and a lower screen with tabs that are enabled/disabled, depending on the upper screen.

In all cases, click the *Configure* button at the bottom of the screen to send your edits to the selected equipment and *Refresh* to update the current screen.

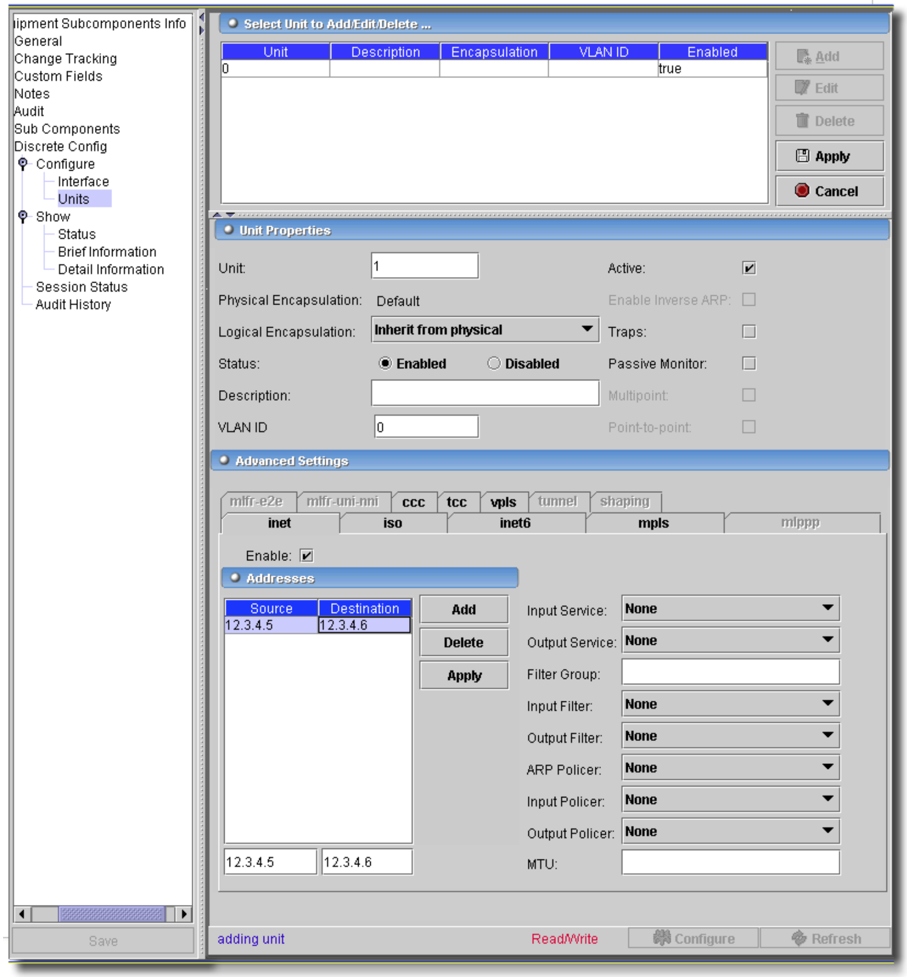
The following sections describe these lower, *Family* screens:

- Inet on page 599
- Iso - OSI ISO protocol on page 601
- inet6 - IPv6 protocol on page 601
- Mpls - Multiprotocol Label Switching on page 602
- Mlppp - Multilink PPP protocol parameters on page 603
- mlfr-e2e - Multilink Frame Relay end-to-end on page 603
- mlfr-uni-nni - Multilink Frame Relay UNI NNI on page 603
- Ccc - Circuit Cross-Connect on page 604
- Tcc - Translational Cross-Connect on page 604
- Vpls - Virtual Private LAN Service on page 605
- Tunnel Configuration / GRE Unit Tunnel on page 606
- Shaping on page 606
- Unit Services on page 607
- Service Options on page 608

General Unit configuration options include the following screens. See Policy Options -> Firewall Filters on page 468 and Policy Options -> Policers on page 467 for information about how to configure filters and policers. Not all options are enabled for all equipment.

For Ethernet port types:

Figure 13-140.   Ethernet Port Unit



Select Unit to Add/Edit/Delete ...

Unit	Description	Encapsulation	VLAN ID	Enabled
0				true

Unit Properties

Unit: 1

Physical Encapsulation: Default

Logical Encapsulation: Inherit from physical

Status: ● Enabled ○ Disabled

Description:

VLAN ID 0

Active: ☑

Enable Inverse ARP: □

Traps: □

Passive Monitor: □

Multipoint: □

Point-to-point: □

Enable: ☑

Addresses

Source	Destination
12.3.4.5	12.3.4.6

12.3.4.5 12.3.4.6

Input Service: None

Output Service: None

Filter Group:

Input Filter: None

Output Filter: None

ARP Policer: None

Input Policer: None

Output Policer: None

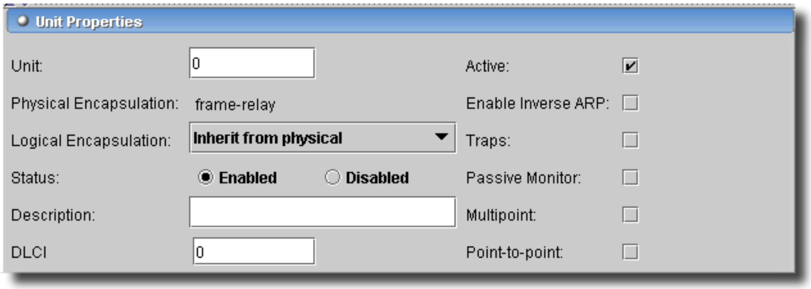
MTU:

adding unit

Read/Write

For SONET and E1 port types:

Figure 13-141. Sonet and E1 Port Unit Sonet and E1 Port Unit

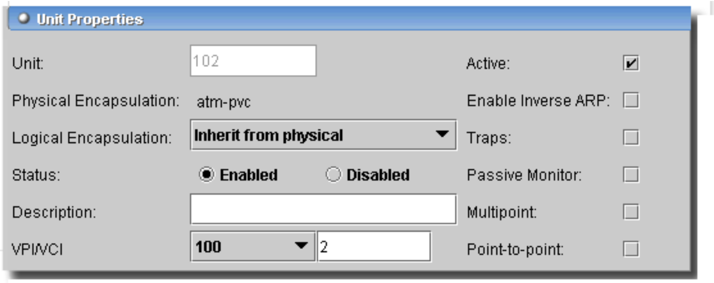


Unit Properties

Unit:	0	Active:	☑
Physical Encapsulation:	frame-relay	Enable Inverse ARP:	□
Logical Encapsulation:	Inherit from physical	Traps:	□
Status:	● Enabled ○ Disabled	Passive Monitor:	□
Description:		Multipoint:	□
DLCI	0	Point-to-point:	□

For ATM port types:

Figure 13-142. ATM Port Unit

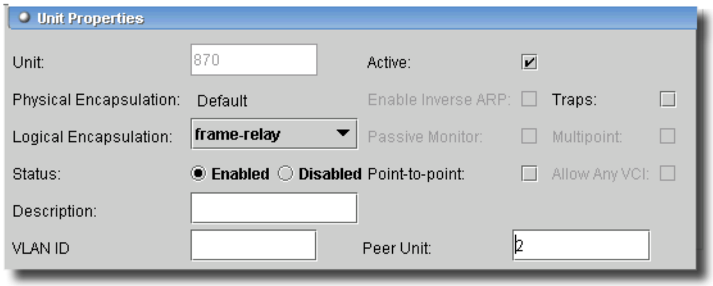


Unit Properties

Unit:	102	Active:	☑
Physical Encapsulation:	atm-pvc	Enable Inverse ARP:	□
Logical Encapsulation:	Inherit from physical	Traps:	□
Status:	● Enabled ○ Disabled	Passive Monitor:	□
Description:		Multipoint:	□
VPI/VCI	100 2	Point-to-point:	□

And for lt Port types:

Figure 13-143. Lt Port Unit



Unit Properties

Unit:	870	Active:	☑		
Physical Encapsulation:	Default	Enable Inverse ARP:	□	Traps:	□
Logical Encapsulation:	frame-relay	Passive Monitor:	□	Multipoint:	□
Status:	● Enabled ○ Disabled	Point-to-point:	□	Allow Any VCI:	□
Description:					
VLAN ID		Peer Unit:	2		

Click *Export* to save a description of the listed interfaces. Click *Add, Edit* or *Delete* to manage the listed Units. The following describes the fields in these General screens:

- **Unit**—Logical unit number

- **Physical Encapsulation**—Physical link-layer encapsulation. The following are its options:

atm-ccc-cell-relay—ATM cell relay encapsulation for cross-connect.

atm-pvc—ATM permanent virtual circuits.

ethernet-over-atm—Ethernet over ATM encapsulation.

ethernet-ccc—Ethernet cross-connect.

ethernet-tcc—Ethernet translational cross-connect.

ethernet-vpls—Ethernet Virtual Private LAN Service (VPLS).

extended-vlan-ccc—Nonstandard TPID tagging for a cross-connect.

extended-vlan-tcc—802.1Q tagging for a translational cross-connect.

extended-vlan-vpls—Extended VLAN Virtual Private LAN Service (VPLS).

vlan-ccc—802.1Q tagging for a cross-connect.

vlan-vpls—VLAN Virtual Private LAN Service (VPLS).

cisco-hdlc—Cisco-compatible HDLC framing.

cisco-hdlc-ccc—Cisco-compatible HDLC framing for a cross-connect.

cisco-hdlc-tcc—Cisco-compatible HDLC framing for a translational cross-connect.

frame-relay—Frame Relay encapsulation.

frame-relay-ccc—Frame Relay for cross-connect.

frame-relay-tcc—Frame Relay for translational cross-connect.

multilink-frame-relay-uni-nni—Multilink Frame Relay UNI NNI (FRF.16) encapsulation.

ppp—Serial PPP device.

ppp-ccc—Serial PPP device for a cross-connect.

ppp-tcc—Serial PPP device for a translational cross-connect.

flexible-frame-relay—Multiple Frame Relay encapsulations.

extended-frame-relay-ccc—Any Frame Relay DLCI for cross-connect.

extended-frame-relay-tcc—Any Frame Relay DLCI for translational cross-connect.

- **Logical Encapsulation—**This includes the following options:

atm-ccc-cell-relay—ATM cell relay for CCC.

atm-ccc-vc-mux—ATM VC for CCC.

atm-cisco-nlpid—Cisco-compatible ATM NLPID encapsulation.

atm-mlppp-llc—ATM MLPPP over AAL5/LLC.

atm-nlpid— ATM NLPID encapsulation.

atm-ppp-llc—ATM PPP over AAL5/LLC.

atm-ppp-vc-mux—ATM PPP over raw AAL5.

atm-snap—ATM LLC/SNAP encapsulation.

atm-tcc-snap—ATM LLC/SNAP for translational cross-connect.

atm-tcc-vc-mux—ATM VC for translational cross-connect.

atm-vc-mux—ATM VC multiplexing.

ether-over-atm-llc—Ethernet over ATM (LLC/SNAP) encapsulation.

ether-vpls-over-atm-llc—Ethernet VPLS over ATM (bridging) encapsulation.

dix—Ethernet DIXv2 (RFC 894).

vlan-ccc—802.1Q tagging for a cross-connect.

vlan-vpls—VLAN Virtual Private LAN Service (VPLS).

frame-relay—Frame Relay DLCI.

frame-relay-ccc—Frame Relay DLCI for CCC.

frame-relay-tcc—Frame Relay DLCI for translational cross-connect.

multilink-frame-relay-end-to-end—Multilink Frame Relay end-to-end (FRF.15).

multilink-ppp —Multilink PPP.

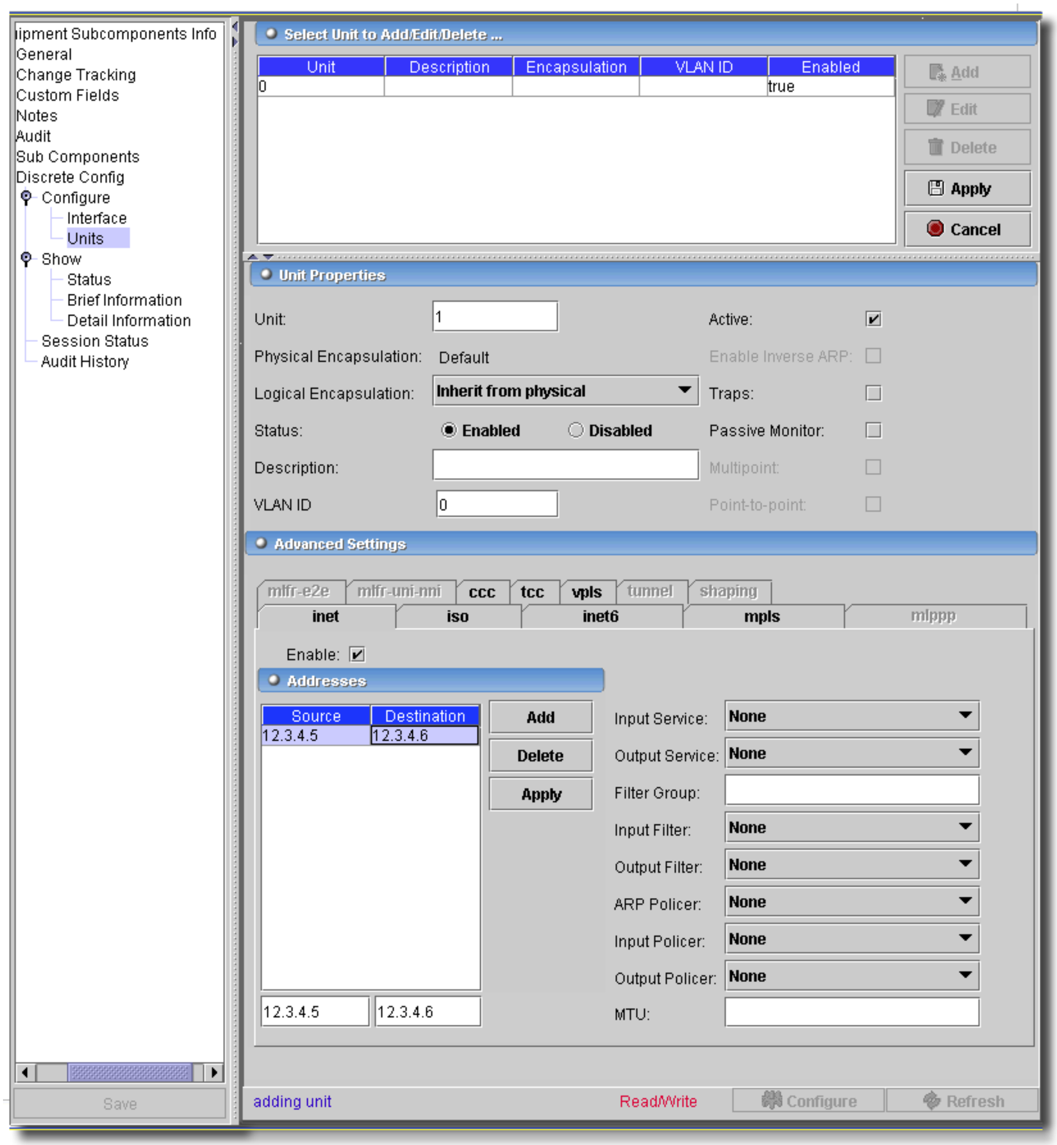
- **Status**—Enable/Disable this logical interface.
- **Description**—Text description of the interface.
- **DLCI**—Frame Relay link control identifier (1 - 1022). Appears only for Sonet ports.
- **VLAN ID**—Virtual LAN identifier value for 802.1Q VLAN tags (0 - 4094). Appears only for ethernet or lt ports.
- **VPI**—Allow all VCIs in this VPI to open in atm-ccc-cell-relay mode (0 - 255). Appears only for ATM ports.
- **VCI**—ATM point-to-point virtual circuit identifier. Appears only for ATM ports.
- **Active**—Check to activate this unit.
- **Enable Inverse ARP**—Enable/Disable Inverse ARP.
- **Traps**—Enable SNMP notifications on state changes.
- **Passive Monitor Mode**—Use interface to tap packets from another router.
- **Multipoint**—Multipoint connection.
- **Point to point**—Point-to-point connection.
- **Allow any VCI**—Allow any ATM point-to-point virtual circuit identifier.
- **Peer Unit**—Enter an identifier for a peer unit. Appears only for lt ports.

The sections below describe Unit configuration *Family* options. These tabs appear enabled depending on the type of interface you select:

Inet

This screen configures Inet parameters.

Figure 13-144. Unit inet Configuration



Unit	Description	Encapsulation	VLAN ID	Enabled
0				true

Unit:	1
Physical Encapsulation:	Default
Logical Encapsulation:	Inherit from physical
Status:	● Enabled ○ Disabled
Description:	
VLAN ID	0
Active:	☑
Enable Inverse ARP:	□
Traps:	□
Passive Monitor:	□
Multipoint:	□
Point-to-point:	□

Enable: ☑

Source	Destination
12.3.4.5	12.3.4.6

12.3.4.5 12.3.4.6

Input Service:	None
Output Service:	None
Filter Group:	
Input Filter:	None
Output Filter:	None
ARP Policer:	None
Input Policer:	None
Output Policer:	None
MTU:	

adding unit ReadWrite

Use *Add*, *Edit*, *Delete* or *Export* to manage the listed parameters. Click *Export* to save a description of these items in a file. When you add or edit, an editor opens with the following fields.

Enable—Enable/Disable Family option on logical interface

The next two fields appear at the bottom of the *Addresses* table, and let you *Add*, *Delete*, or *Apply* the *Source/Destination* interface pairs to the table.

Source Address—Interface address prefix.

Destination Address—Interface address destination.

Input / Output Service—Select from the pick list.

Filter Group—Group of which this interface is a member.

Input Filter—Filter applied to received packets.

Output Filter—Filter applied to transmitted packets.

ARP Policer—Policer applied to arp packets. (see

Input Policer—Policer applied to received packets.

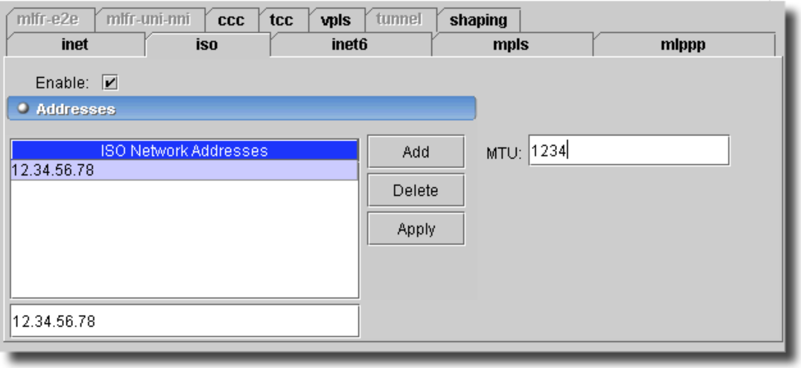
Output Policer—Policer applied to transmitted packets.

MTU—Maximum transmit packet size (256 - 9192).

Iso - OSI ISO protocol

This screen configures ISO parameters.

Figure 13-145. Unit OSI ISO Protocol



Enable: ☑

ISO Network Addresses
12.34.56.78

MTU: 1234

12.34.56.78

Enable—Enable/Disable Family option on logical interface.

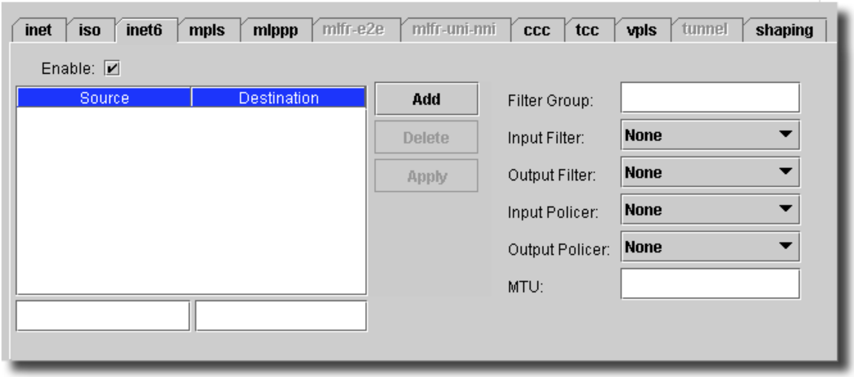
MTU—Maximum transmit packet size (256 - 9192).

Enter an ISO Network address at the bottom of this screen, then click *Add* to list it in the table on the left. Click *Delete* to remove a selected existing row, and *Apply* to accept your changes.

inet6 - IPv6 protocol

This screen configures Inet6 parameters.

Figure 13-146. Unit Inet6 - IPv6 Protocol



Enable: ☑

Filter Group:

Input Filter: None

Output Filter: None

Input Policer: None

Output Policer: None

MTU:

Enable—Enable/Disable Family option on logical interface.

The next two fields appear at the bottom of the *Addresses* table, and let you *Add*, *Delete*, or *Apply* the *Source/Destination* interface pairs to the table.

Source Address—Interface address prefix.

Destination Address—Interface address destination.

Filter Group—Group of which this interface is a member.

Input Filter—Filter applied to received packets.

Output Filter—Filter applied to transmitted packets.

Input Policer—Policer applied to received packets.

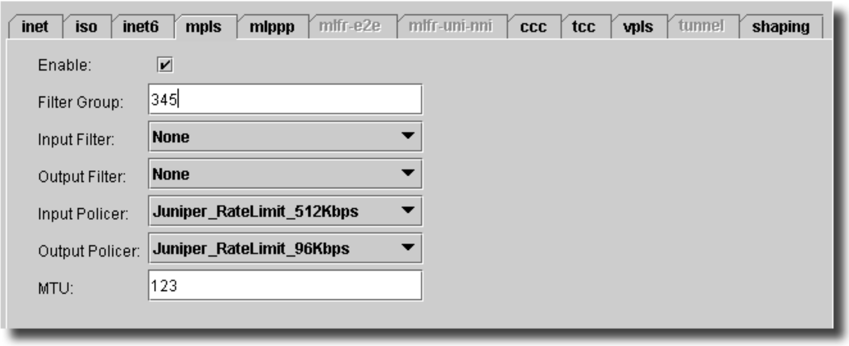
Output Policer—Policer applied to transmitted packets.

MTU—Maximum transmit packet size (256 - 9192).

Mpls - Multiprotocol Label Switching

This screen configures MPLS parameters.

Figure 13-147. Unit Mpls



Enable: ☑

Filter Group: 345

Input Filter: None

Output Filter: None

Input Policer: Juniper_RateLimit_512Kbps

Output Policer: Juniper_RateLimit_96Kbps

MTU: 123

Enable—Enable/Disable Family option on logical interface.

Filter Group—Group where this interface is a member.

Input Filter—Filter applied to received packets.

Output Filter—Filter applied to transmitted packets.

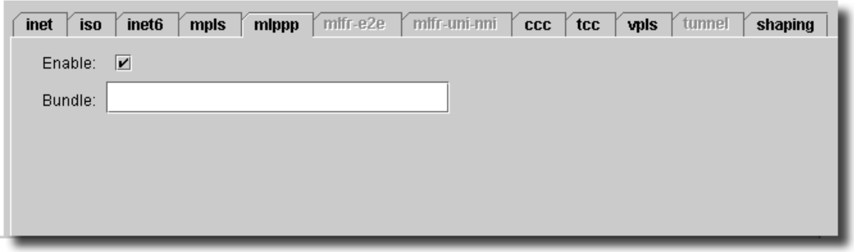
Input Policer—Policer applied to received packets.

Output Policer—Policer applied to transmitted packets.

MTU—Maximum transmit packet size (256 - 9192).

Mlppp - Multilink PPP protocol parameters

This screen configures Multilink PPP parameters.



Enable: ☑

Bundle:

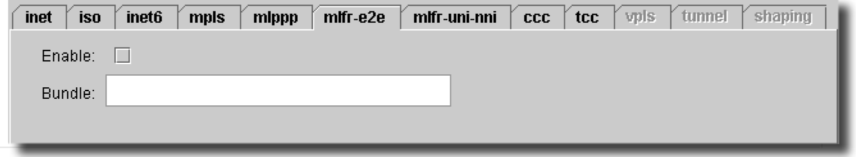
Figure 13-148. Unit MIppp Protocol

Enable—Enable/Disable Family option on logical interface

Bundle—Logical interface name this link joins.

mlfr-e2e - Multilink Frame Relay end-to-end

This screen configures multilink frame relay end-to-end parameters.



Enable: □

Bundle:

Figure 13-149. Unit Multilink Frame Relay end-to-end Protocol

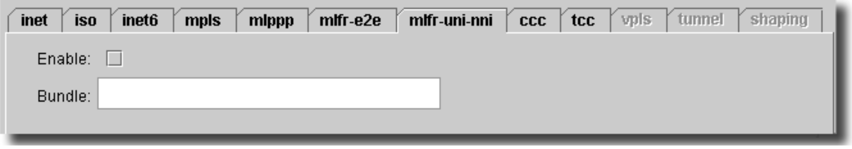
Enable—Enable/Disable Family option on logical interface.

Bundle—Logical interface name this link joins.

mlfr-uni-nni - Multilink Frame Relay UNI NNI

This screen configures multilink frame relay UNI NNI parameters.

Figure 13-150. Unit Multilink Frame Relay UNI NNI protocol



Enable: □

Bundle:

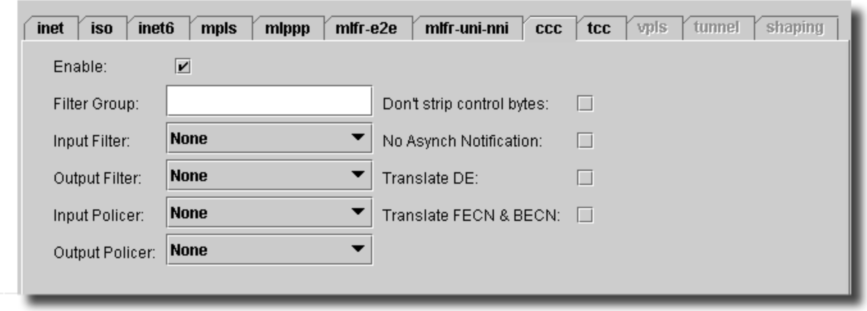
Enable—Enable/Disable Family option on logical interface.

Bundle—Logical interface name this link joins.

Ccc - Circuit Cross-Connect

This screen configures circuit cross-connect parameters.

Figure 13-151. Ccc - Circuit cross-connect



Enable: ☑

Filter Group:

Input Filter: None

Output Filter: None

Input Policer: None

Output Policer: None

Don't strip control bytes: □

No Asynch Notification: □

Translate DE: □

Translate FECN & BECN: □

Enable—Enable/Disable Family option on logical interface.

- **Filter Group**—Group where this interface is a member.

- **Input Filter**—Filter applied to received packets.

- **Output Filter**—Filter applied to transmitted packets.

- **Input Policer**—Policer applied to received packets.

- **Output Policer**—Policer applied to transmitted packets.

- **Don't strip control bytes**—Do not strip PPP address and control bytes.

- **No Asynch Notification**—Do not send asynchronous notification upon link failure.

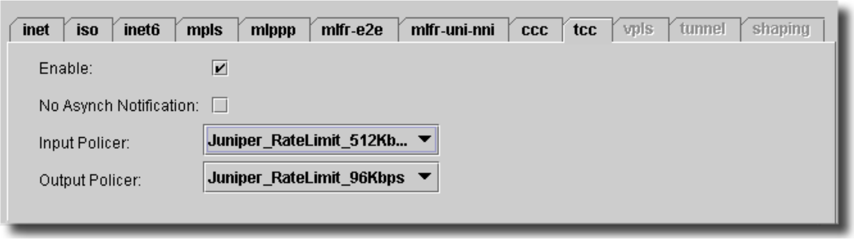
- **Translate DE**—Translate Discard Eligible bit.

- **Translate FECN & BECN**—Translate FECN and BECN bits.

Tcc - Translational Cross-Connect

This screen configures translational cross-connect parameters.

Figure 13-152. Tcc - Translational Cross-Connect



Enable: ☑

No Asynch Notification: □

Input Policer: Juniper_RateLimit_512Kb...

Output Policer: Juniper_RateLimit_96Kbps

- **Enable**—Enable/Disable Family option on logical interface.

- **Input Filter**—Filter applied to received packets.

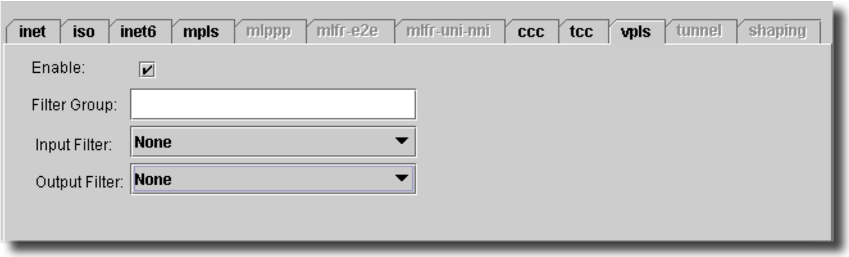
- **Output Filter**—Filter applied to transmitted packets.

- **No Asynch Notification**—Do not send asynchronous notification on link failure.

Vpls - Virtual Private LAN Service

This screen configures VPLS parameters.

Figure 13-153. Vpls - Virtual Private LAN Service



Enable: ☑

Filter Group:

Input Filter: None

Output Filter: None

Enable—Enable/Disable Family option on logical interface.

Filter Group—Group where this interface is a member.

Input Filter—Filter applied to received packets.

Output Filter—Filter applied to transmitted packets.

Input Policer—Policer applied to received packets.

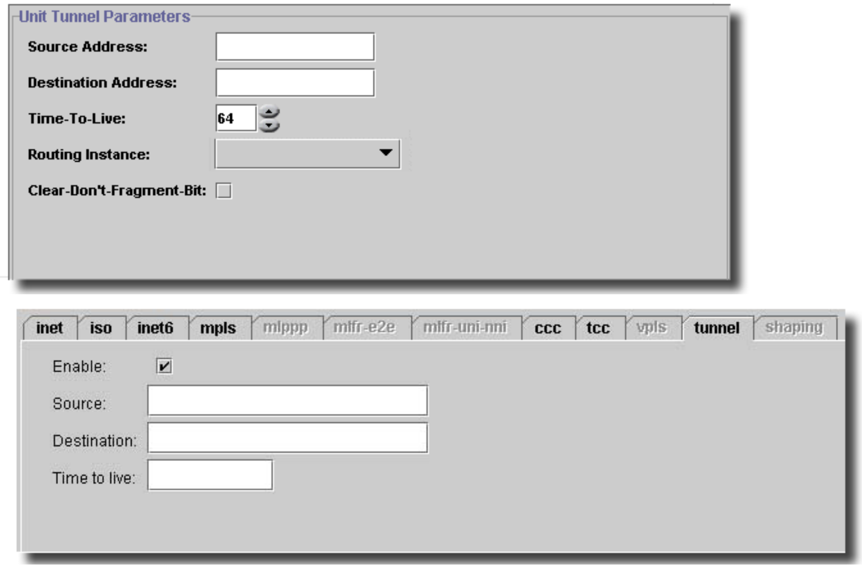
Output Policer—Policer applied to transmitted packets.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Tunnel Configuration / GRE Unit Tunnel

By encapsulating arbitrary packets inside a transport protocol, tunneling provides a private, secure path through an otherwise public network. Tunnels connect discontinuous subnetworks and enable encryption interfaces, virtual private networks (VPNs), and Multiprotocol Label Switching (MPLS).

Figure 13-154. Tunnel Configuration and GRE Unit Tunnel



Unit Tunnel Parameters

Source Address:

Destination Address:

Time-To-Live: 64

Routing Instance:

Clear-Don't-Fragment-Bit: ☐

Enable: ☑

Source:

Destination:

Time to live:

Configure the following fields in this screen:

- **Source Address**—The IP address of the tunnel source.

- **Destination Address**—The IP address of the tunnel destination.

- **Time-to-Live**—The lifetime of this tunnel.

- **Routing Instance**—Select from the pick list.

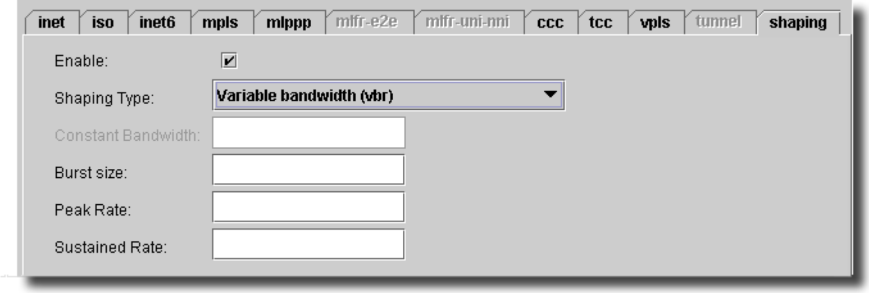
- **Clear-don't fragment**—Sets the bit on a GRE tunnel when used on the AS PIC.

The Unit is an endpoint for the GRE Tunnel.

Shaping

This tab enables and configures VCI shaping for the selected unit.

Figure 13-155. Shaping



Enable: ☑

Shaping Type: Variable bandwidth (vbr)

Constant Bandwidth:

Burst size:

Peak Rate:

Sustained Rate:

It has the following fields:

- **Enable**—Check to enable shaping.

- **Shaping Type**—Select from a pick list. Either set VPI Shaping to *None* to allow *Constant Bandwidth* (CBR) or set VBR Shaping at the Unit level only. Alternatively, you can use the *Shaping Type* of CBR at both the VPI and Unit levels provided you set a CBR value at the Unit level that meets or exceeds the Constant bandwidth value set at the VPI level.

  Unless you do this, you cannot set Shaping Type of VBR at both the VPI and Unit levels. If your settings do not meet these conditions, then a configure error message appears: (ATM2 cannot configure VC Shaping when VP Shaping for VPI#1 is configured)

- **Constant Bandwidth**—Enabled if you select CBR. Specify the constant bandwidth in this field.

The following fields appear if you do not select constant bandwidth:

- **Burst size**—Enter a number. Burst size (maximum 4,000 for ATM2, 255 for ATM1) (1 - 4,000)

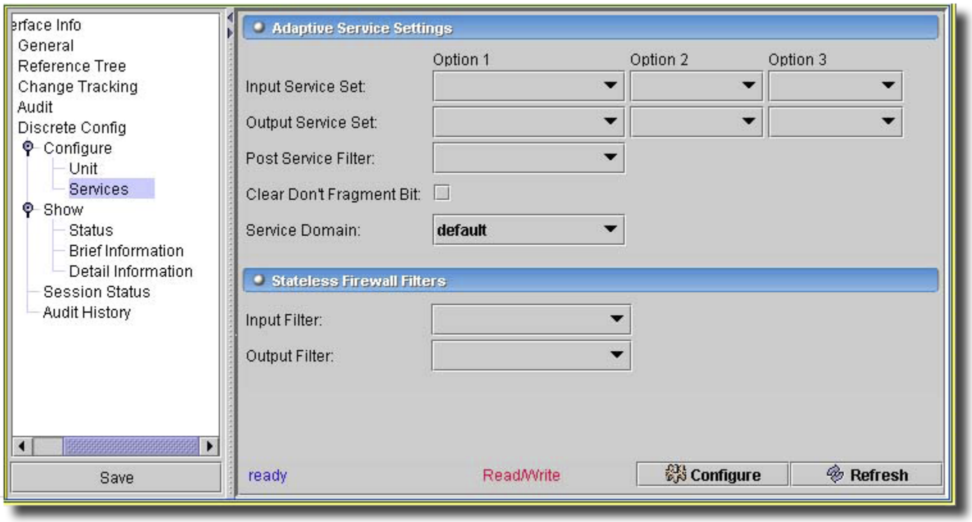
- **Peak rate**—Enter a peak rate number. Peak rate (33000 - 2,170,107,168).

- **Sustained rate**—Enter a sustained rate (33,000 - 2,170,107,168).

Unit Services

These let you apply Service-sets to one or more installed units. You can configure up to three different service sets on the input and output sides of the interface.

Figure 13-156. Unit Services Configuration



Adaptive Service Settings

	Option 1	Option 2	Option 3
Input Service Set:			
Output Service Set:			
Post Service Filter:			
Clear Don't Fragment Bit:	□		
Service Domain:	default		

Stateless Firewall Filters

Input Filter:

Output Filter:

You can configure the following:

Input Parameters

- **Input Service-Set** (1,2,3)—Select from the pick list.

- **Filter**—Select from the pick list for the selected input service.

- **Post-Service-Set**—Select from the pick list.

Output Parameters

- **Output Service-Set** (1,2,3)—Select from the pick list.

- **Filter**—Select from the pick list to filter the selected service.

General Parameters

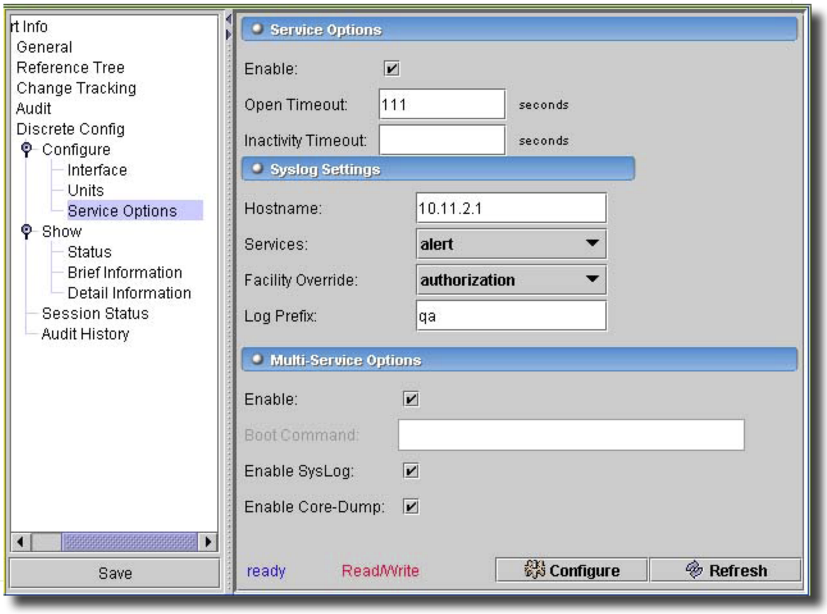
- **Service Domain**—Service-domain specifies whether the interface is used within the network or to communicate with remote devices.

Optionally include filters before or after each service set to refine the target and additionally process the traffic.

Service Options

This configures a port's ability to use syslog and other options.

Figure 13-157. Unit Service Options



Service Options

Enable: ☑

Open Timeout: 111 seconds

Inactivity Timeout: seconds

Syslog Settings

Hostname: 10.11.2.1

Services: alert

Facility Override: authorization

Log Prefix: qa

Multi-Service Options

Enable: ☑

Boot Command:

Enable SysLog: ☑

Enable Core-Dump: ☑

Service Options

These are the service options to be applied on an interface:

- **Inactivity Timeout**—For adaptive services interfaces, configures the inactivity timeout period for established flows. default: 30 secs 1-200000.
- **Open Timeout**—Configure timeout period for TCP session establishment. default: 30 secs 1-216000.

Multi-Service Options

For monitoring services interfaces only, configure multiservice-specific interface properties.

- **Enable Core-Dump**—Enable the core dumping operation.
- **Enable SysLog**—Enable PIC system logging.
- **Boot Command**—Specifies the filename containing the JUNOS software image for the monitoring services PIC relative to the directory path |/usr/share/pfe|. By default, the name of the boot image for the monitoring services PIC is |monitor.jbf|.

Syslog

- **Hostname**—Specifies the hostname for system logging utility.
- **Facility**—Overrides the default facility for system log reporting. Select from the pick list.

- **Priority**—Specifies the system logging priority level. Select from the pick list.

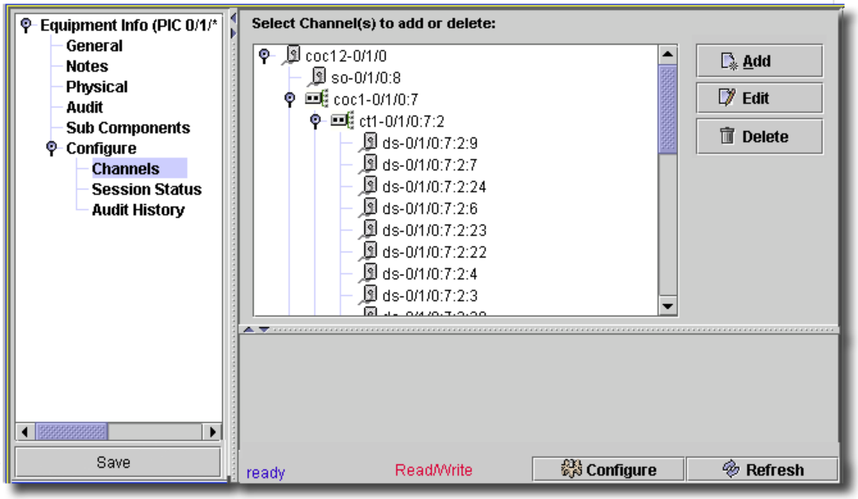
- **LogPrefix**—Sets the system logging prefix value. Enter a string.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

Channelized PICs -> Channel Groups

This screen (or one like it) appears for channelized QPP and channelized PIC selections (PIC level).

Figure 13-158. Channelized: Channel Groups



To edit a node on the displayed tree, click the node, then click *Edit*. An edit screen like the one in Channel Properties on page 611, or in DS0 Channel Properties on page 612 (depending on the type of node) appears in the lower portion of the screen. The “trident” icon indicates a channelizable node, while the standard port icons indicate that node is not channelizable.

Select Use the *Add* or *Remove* buttons to further manage nodes in the table. Enter text in the edit screen, once you add a node.

The *Configure* button at the bottom of this screen sends the selected configuration to the device. The *Refresh* button queries to update information displayed.

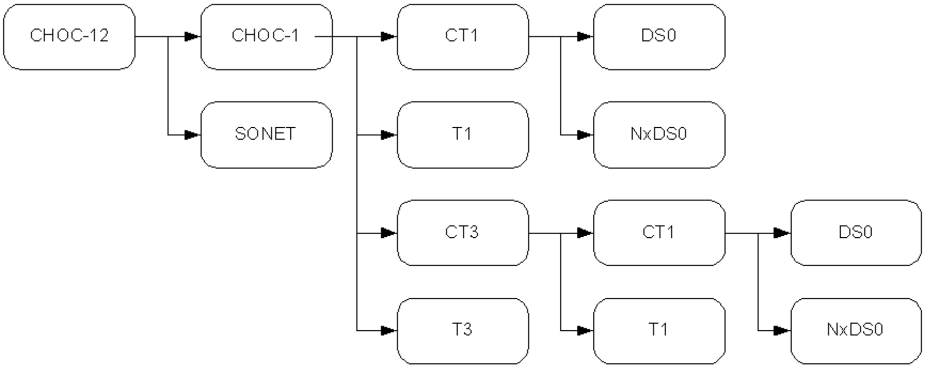
For more about Audit History, see Audit / Results on page 184.

Channelized PICs

Some Channelized QPP PICs allow the creation of multilevel channels. For example with the new Channelized OC-12 QPP PIC (CHOC12) you can channelize the CHOC12 down to Channelized OC-1's. You can channelize these OC-1's further to Channelized T3's or Channelized T1's and so on, all the way to the DS0 level.

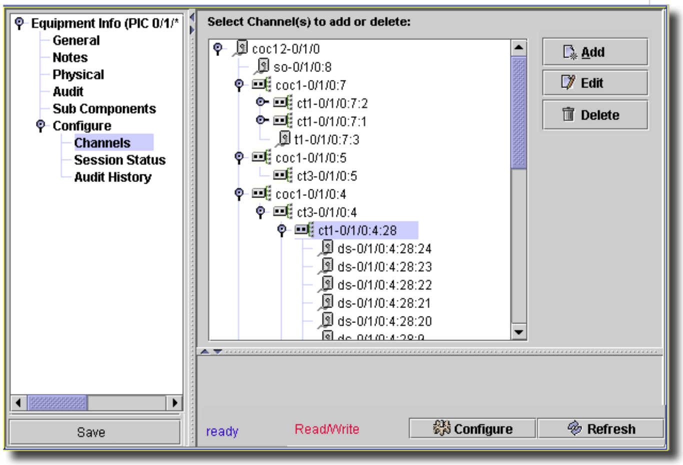
The following flow diagram details the CHOC-12 and potential components of each channel type.

Figure 13-159. Channel Components



The DDI Service for the *Channels* Service should appear for any discovered SONETPIC managed object. It supports *Add*, *Edit* or *Delete* actions against any channel in the hierarchy.

Figure 13-160. Channelized OC-12 Layout



The icons on the tree represent the types of channels. The icons with double arrows indicate sub-channels are permitted. The standard port icon indicates no sub-channels are possible.

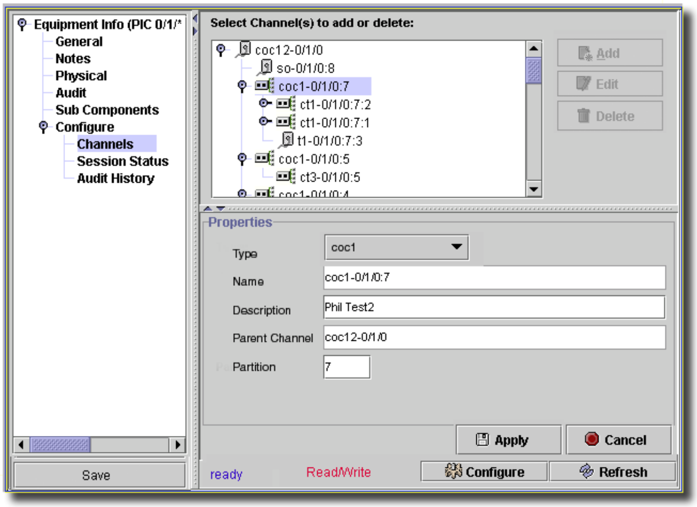
—These permit sub-channels.

—These do not.

Channel Properties

The following screen in Equipment Editor displays the channel properties for the selected PIC.

Figure 13-161. Channel Properties



Type: coc1

Name: coc1-0/1/0:7

Description: Phil Test2

Parent Channel: coc12-0/1/0

Partition: 7

- **Type**—Available Sub-Channel Types that belong to the Channel

- **Name**—Auto-assigned name, based upon Sub-Channel Type, Parent Channel ID and Partition

- **Description**—User-assigned description of the Sub-Channel

- **Parent Channel**—Channel to which the Sub-Channel belongs to.

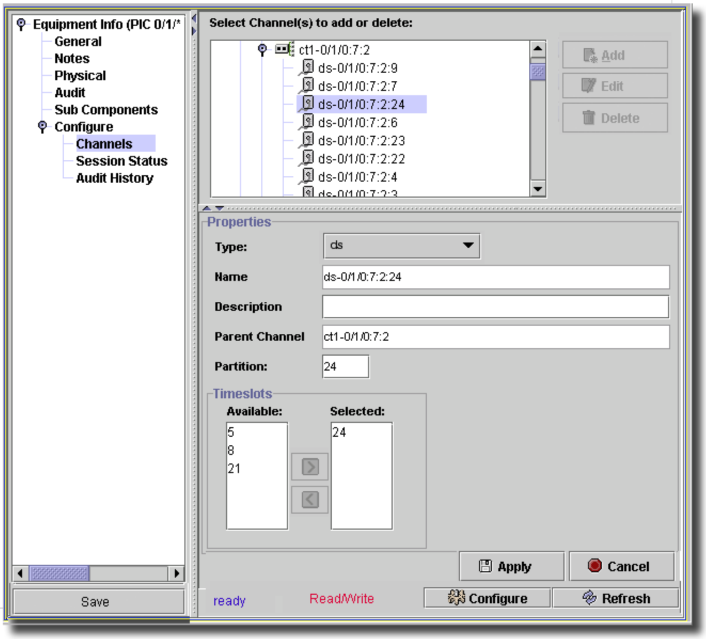
- **Partition**—Which portion of the Channel which is assigned to the Sub-Channel

See Add Channels on page 613 and Set All Channels on page 614 for information about managing channels.

DS0 Channel Properties

The following screen displays the DS0 properties for the selected PIC.

Figure 13-162.   DS0 Channel Properties



Select Channel(s) to add or delete:

ct1-0/1/0:7:2
ds-0/1/0:7:2:9
ds-0/1/0:7:2:7
ds-0/1/0:7:2:24
ds-0/1/0:7:2:6
ds-0/1/0:7:2:23
ds-0/1/0:7:2:22
ds-0/1/0:7:2:4
ds-0/1/0:7:2:3

Properties

Type: ds

Name ds-0/1/0:7:2:24

Description

Parent Channel ct1-0/1/0:7:2

Partition: 24

Timeslots

Available: 5 8 21

Selected: 24

It contains the following fields:

- **Type**—Available Sub-Channel Types that belong to the Channel

- **Name**—Auto-assigned name based upon Sub-Channel Type, Parent Channel ID and Partition.

- **Description**—User-assigned description of the Sub-Channel.

- **Parent Channel**—Channel to which the Sub-Channel belongs.

- **Partition**—Which portion of the Channel is assigned to the Sub-Channel.

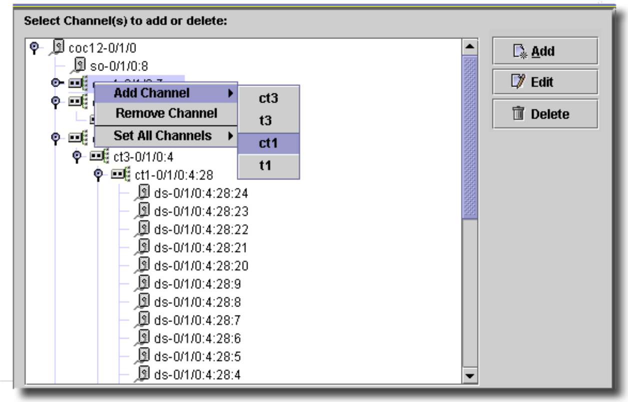
- **Timeslots**—DS0s support multi-bandwidth channels (NxDS0s) so they can contain anywhere from 1-24 Sub-Channels from the Channelized T1, but still be identified as a single channel.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Add Channels

Right clicking on the Channel tree hierarchy provides quick ways to manage Sub-Channels.

Figure 13-163. Add PIC Channels

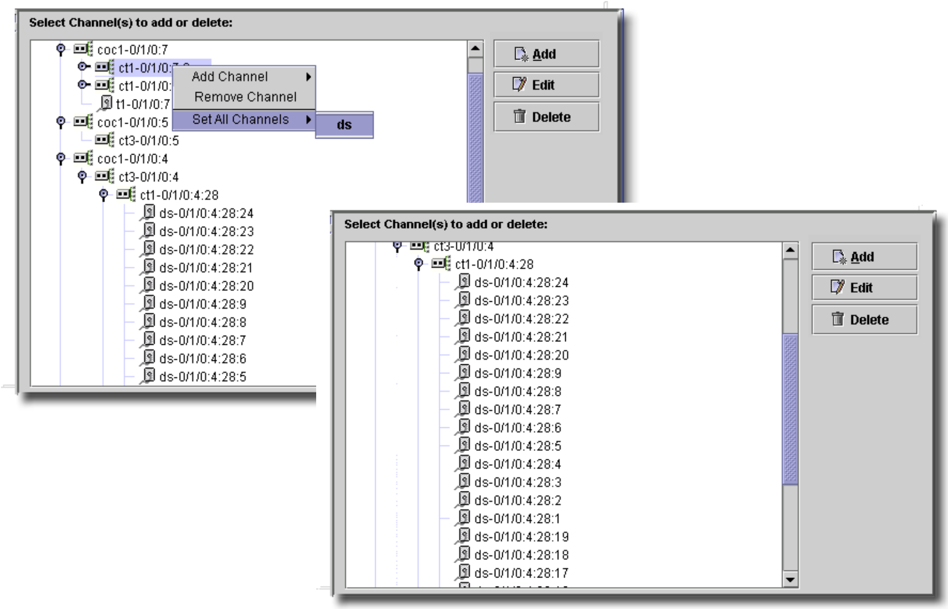


When you select *Add Channel* from the menu, the sub-menu presents types of channels you can add.

Set All Channels

If you want to set the Sub-Channels to the same Channel-Type for a given Channel then select *Set All Channels*.

Figure 13-164. Set All Channels

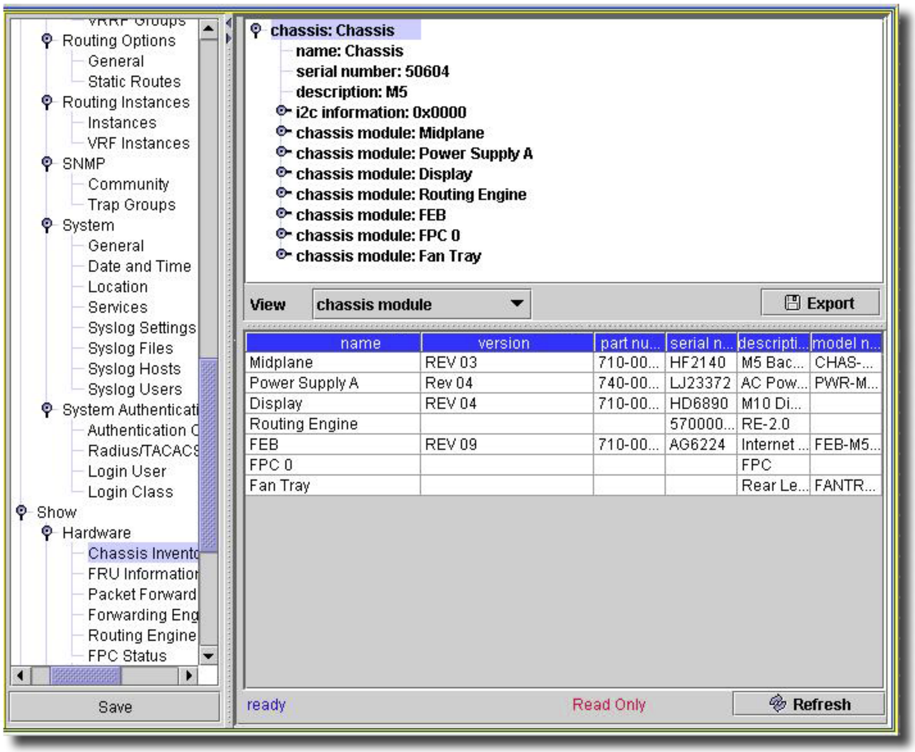


Manage channels with the *Add*, *Edit*, and *Delete*, or with the right click menu.

Show Screens

Show screens are read-only equivalents to the JUNOS *show* command. They appear, depending on your selection in the *Show* node of the Equipment Editor tree, and depending on your selected *View* item (see the pick list roughly in mid-screen).

Figure 13-165. Show Screens



VRRP Groups
- Routing Options
  - General
  - Static Routes
- Routing Instances
  - Instances
  - VRF Instances
- SNMP
  - Community
  - Trap Groups
- System
  - General
  - Date and Time
  - Location
  - Services
  - Syslog Settings
  - Syslog Files
  - Syslog Hosts
  - Syslog Users
- System Authenticati
  - Authentication C
  - Radius/TACACS
  - Login User
  - Login Class
- Show
  - Hardware
    - Chassis Invento
    - FRU Informatior
    - Packet Forward
    - Forwarding Eng
    - Routing Engine
    - FPC Status

chassis: Chassis
- name: Chassis
- serial number: 50604
- description: M5
- i2c information: 0x0000
- chassis module: Midplane
- chassis module: Power Supply A
- chassis module: Display
- chassis module: Routing Engine
- chassis module: FEB
- chassis module: FPC 0
- chassis module: Fan Tray

View: chassis module

name	version	part nu...	serial n...	descripti...	model n...
Midplane	REV 03	710-00...	HF2140	M5 Bac...	CHAS-...
Power Supply A	Rev 04	740-00...	LJ23372	AC Pow...	PWR-M...
Display	REV 04	710-00...	HD6890	M10 Di...	
Routing Engine			570000...	RE-2.0	
FEB	REV 09	710-00...	AG6224	Internet ...	FEB-M5...
FPC 0				FPC	
Fan Tray				Rear Le...	FANTR...

You can *Export* this information to a file, if you click that button. Select the equipment sub-components in the upper screen and view the information related to the *View* pick list in the lower screen. Only what appears in the lower screen is exported, if you click *Export*. Here are the screens available with this driver, and their JUNOS command line equivalents:

Routing Show Commands

- **BGP Summary**—show bgp summary
- **BGP Group Statistics**—show bgp group
- **BGP Neighbor Statistics**—show bgp neighbor
- **ISIS Statistics**—show isis statistics
- **LDP Statistics**—show ldp statistics

- **OSPF Statistics**—show ospf statistics

- **RSVP Statistics**—show rsvp statistics

- **Route Summary**—show route summary

- **ARP Table**—show arp

- **MPLS LSP Statistics**—show mpls lsp

- **MPLS Paths Statistics**—show mpls path

- **OSPF Neighbors**—show ospf neighbors

- **OSPF Log**—show ospf log

- **All Routes**—show route all

- **Fowarding Table Summary**—show route forwarding-table

Interface Show Commands

Interface Status—show interfaces statistics

MPLS Information—show mpls interface

LDP Information—show ldp interface

ISIS Information—show isis interface

OSPF Information—show ospf interface

PIM Statistics—show pim statistics

RSVP Information—show rsvp interface

Network Show Commands

L2 VPN Summary Information—show l2vpn connections summary

Layer 2 Summary Information—show l2circuit connections

System Show Commands

Storage—show system storage

Up Time—show system uptime

FPC Status—show chassis fpc

Commit History—show system commit

Alarms—show chassis alarms

Environment—show chassis environment

Firmware—show chassis firmware

Software—show system software

SNMP Statistics—show snmp statistics

Active Users—show system users

Hardware Show Commands

Chassis Inventory—show chassis hardware extensive

FRU information—show chassis hardware frus

Forwarding Engine Board Status—show chassis feb

System Control Board Status—show chassis scb

System Switch Board Status—show chassis ssb

Switch Interface Board Status—show chassis sibs

Switching and Forwarding Module Status—show chassis sfm

Routing Engine Status—show chassis routing-engine

Status—show chassis fpc pic-status

Packet Forwarding Engine Status—show pfe terse

PIC Show Commands

Status—show chassis pic

Interface and Unit Show Commands

- **Status**—show interfaces terse
- **Brief Information**—show interfaces brief
- **Detail Information**—show interfaces detail
- **Extensive Information**—show interfaces extensive
- **Filter Information**—show interfaces filters

Services Show Commands

The following appear in services show screens

- **Services Statistics**—show services service-identification statistics
- **CPU Statistics**—show services service-sets cpu-usage
- **Memory Statistics**—show services service-sets memory-usage
- **Stateful Firewall Conversations**—show services stateful-firewall conversations
- **Stateful Firewall Flow Table**—show services stateful-firewall flows
- **IDS Destination Table**—show services ids destination-table
- **IDS Pair Table**—show services ids pair-table
- **IDS Source Table**—show services ids source-table
- **NAT Pool Information**—show services nat pool

- **IPSec Statistics**—show services ipsec-vpn ipsec statistics

- **IPSec Associations**—show services ipsec-vpn ipsec security-associations

- **Certificates Information**—show ipsec certificates Firewall Log - show firewall log

Configuration File Show Commands

The following are screens that show a portion of the current configuration file on the router:

- Applications
- Services
- Groups
- System
- Chassis
- Interfaces
- SNMP
- Routing Options
- Protocols
- Policy Options
- Class of Service
- Firewall
- Routing Instances

Channelized IQ Interface Partitioning

The 5.0.2 driver supports Channelized IQ (QPP) Interface partitioning and clear channel configuration in the application's discrete configuration for the following interfaces:

- cau4Channelized AU-4 IQ interface
- coc1Channelized OC-1 IQ interface
- coc12Channelized OC-12 IQ interface
- cstm1Channelized STM-1 IQ interface
- ct1Channelized T1 IQ interface
- ct3Channelized T3 IQ interface
- ce1Channelized E1 IQ interface

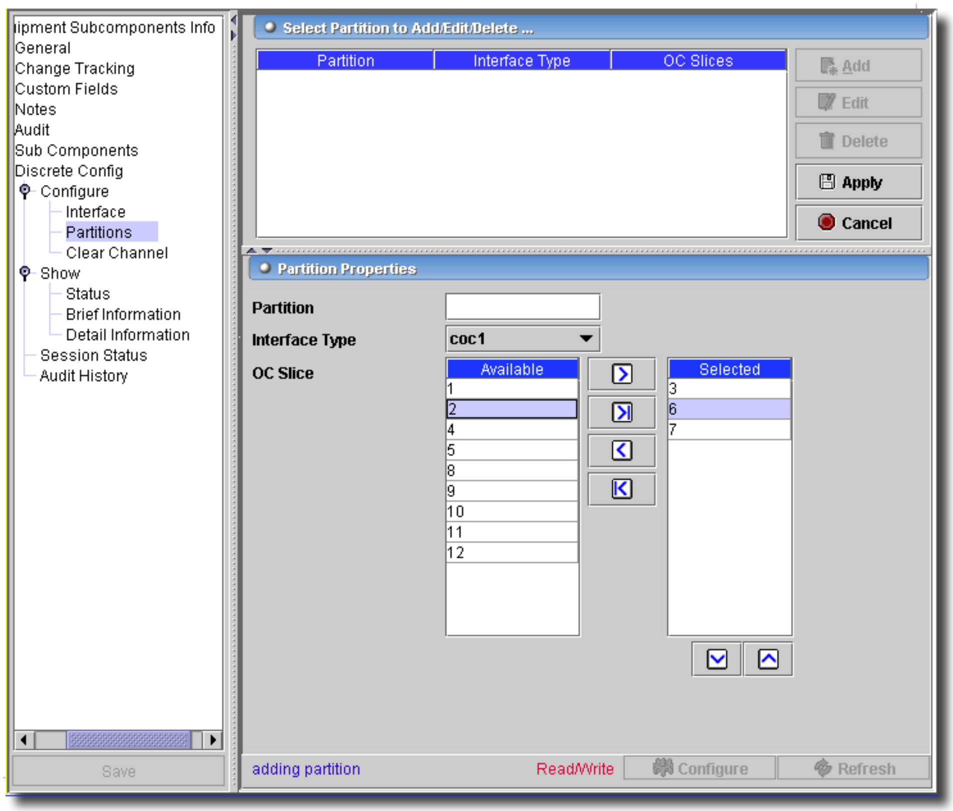
These interfaces are on the following PIC's;

- Channelized DS3 IQ,
- Channelized STM1 IQ,
- Channelized E1 IQ
- Channelized OC12 IQ

Channelized Interface Configure -> Partitions

You can add, edit and delete partitions for channelized interfaces from the port configuration screen.

Figure 13-166. Channelized Interface Configure -> Partitions



Partition

Interface Type: coc1

OC Slice

Available	Selected
1	3
2	6
4	7
5	
8	
9	
10	
11	
12	

adding partition

Read/Write

A warning appears if a clear channel exists for the selected interface. Adding a partition deletes the clear channel. Click *Add* (or select an existing partition listed at the top of the screen, and click *Edit*), and configure the partition in the fields and selector at the bottom of the screen. Click *Export* to save a description of these items in a file. Click *Apply* to accept your edits, or *Cancel* to abandon them. This screen has the following fields:

- **Partition**—A partition number.

- **Interface Type**—Select from the pick list.

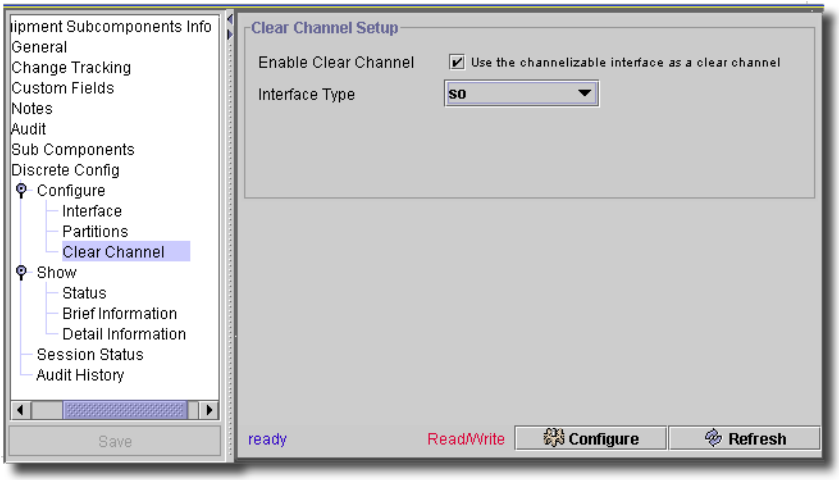
- **Timeslots**—The available timeslots appear on the left of the screen. Use the arrows between *Available* and *Selected* boxes to select timeslots for this partition. You can also re-order *Selected* timeslots with the arrows below that portion of the screen.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

Configure -> Clear Channel

You can convert channelized interfaces into clear channel (no partitions) by configuring clear channel options.

Figure 13-167. Channelized Interface Configure -> Clear Channel (no partition)



Clear Channel Setup

Enable Clear Channel ☑ Use the channelizable interface as a clear channel

Interface Type so

ready ReadWrite

If partitions exist for the selected interface, the application warns that setting up the clear channel deletes them. This screen has the following configurable fields:

- **Enable Clear Channel**—Check to use the channelization interface as a clear channel.

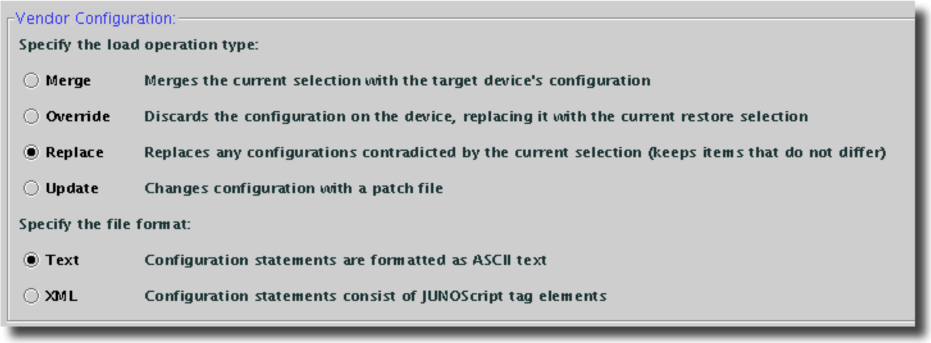
- **Interface type**—Select from a pick list.

The *Configure* button at the bottom of these screens executes the desired configuration on the selected equipment.Click the *Refresh* button to re-query for these items.

J-series Restore

If you have the File Management option installed, this panel configures restoration on (non-E-Series) J-series devices.

Figure 13-1. Restore Type



Vendor Configuration:

Specify the load operation type:

○ Merge — Merges the current selection with the target device's configuration

○ Override — Discards the configuration on the device, replacing it with the current restore selection

● Replace — Replaces any configurations contradicted by the current selection (keeps items that do not differ)

○ Update — Changes configuration with a patch file

Specify the file format:

● Text — Configuration statements are formatted as ASCII text

○ XML — Configuration statements consist of JUNOScript tag elements

NOTE:

If you select “snapshot” as part of a file management action, you must have external media, like a USB drive, plugged into the device, or an error appears.

This panel has two sets of radio buttons that let you configure the type of restoration you want to do.

Specify the load operation type

- **Merge**—Merges the currently selected configuration file with the device’s configuration. Statements in the selection replace any on the device when they differ. Otherwise, this selection simply adds configuration statements to the device.
- **Override**—Discards the configuration on the device, replacing it with the selected configuration file.
- **Replace** —Replaces any currently contradicted by the current selection. Items that do not differ in the restore selection, item-by-item, remain the same.
- **Update**—Changes the current configuration with a patch file.

Specify the file format

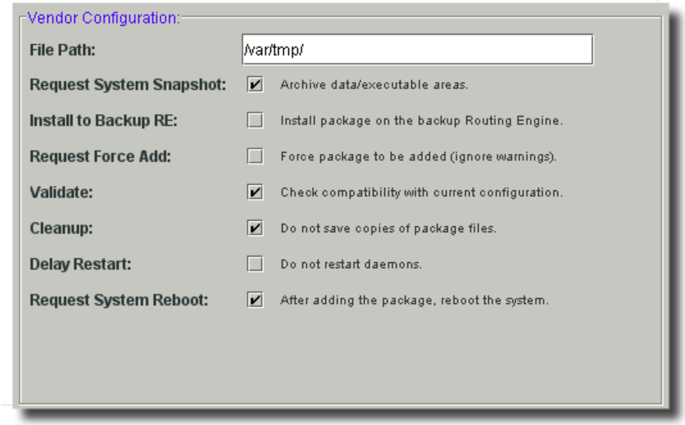
- **Text**—Configuration statements are formatted as ASCII text. They use newline characters, tabs, braces, brackets and white space to indicate hierarchical relationships. This is the format used in configuration files stored on the routing platform and displayed by the command line show configuration.
- **XML**—Configuration statements consist of JUNOScript tag elements. These are typically developer-created files, not configuration file backups from the device.

See Adjusting Time-outs on page 625 for changes you can make to device response time-out problems.

J-series Deploy

This vendor panel appears when you deploy to a J-series (M/T/J) device.

Figure 13-2. J-series Deploy



Vendor Configuration:

File Path: /var/tmp/

Request System Snapshot: ☑ Archive data/executable areas.

Install to Backup RE: □ Install package on the backup Routing Engine.

Request Force Add: □ Force package to be added (ignore warnings).

Validate: ☑ Check compatibility with current configuration.

Cleanup: ☑ Do not save copies of package files.

Delay Restart: □ Do not restart daemons.

Request System Reboot: ☑ After adding the package, reboot the system.

This screen has the following fields:

- **File Path**—Pre-populated with `/var/tmp/` (where most J-series devices suggest you place the package for upgrade). You can specify a different path to place the package for upgrade. Best practice is to use `/var/tmp/`.
- **Install to Backup RE**—Installs the package on the backup routing engine. This is valid only for devices that support dual routing engines.
- **Request Force Add**—Forces the addition of a package (ignores warnings).
- **Validate**—Checks compatibility with current configuration.
- **Cleanup**—Deletes the downloaded image from the router after deploy.
- **Delay Restart**—Processes will not restart on router.
- **Request System Reboot**—Reboots the router after upgrade. Discards the configuration on the device, replacing it with the selected configuration file.

NOTE:

Below this screen, a reminder appears to reboot the device to take full advantage of any new features exposed by the deployment.

See Adjusting Time-outs for changes you can make to device response time-out problems.

Adjusting Time-outs

If you receive time-out errors, you can change a few properties to increase the File Server and Deploy time outs.

First, you can increase the FTP timeout for the Management Interface in the Resource editor for a device.

To change Netrestore timing, change `juniper.properties` (in `owareapps/juniper/lib`)

```
# The following 3 properties control the timeout factor (will be
multiplied by the timeout set in the authentication)

# for netrestore functions since these function take more time the average
command to execute

# -- uncomment the appropriate line below and set to an appropriate value
to over-ride the default

#com.dorado.juniper.nr.backup.timeout.factor=10

#com.dorado.juniper.nr.restore.timeout.factor=15

#com.dorado.juniper.nr.deploy.timeout.factor=30
```

Also, in from fx.properties (owareapps/filexferapi/lib)

```
#this is the default ftp file transfer timeout in number of seconds

 com.dorado.redcell.filexferapi.ftptimeout=500
```

NOTE:

As always, best practice is to override default property settings by copying the revised property into `owareapps/installprops/lib/installed.properties`. The advantage of doing this is that it does not change if you upgrade your application.

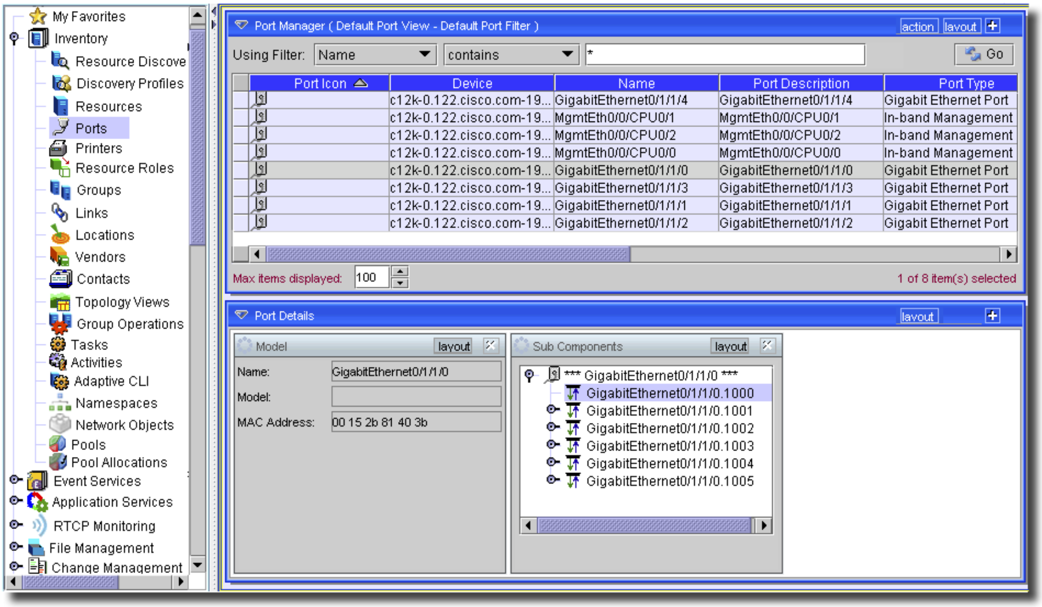
14

Ports

Introducing Ports Manager

Access Port Manager from the navigation window, or from the *Inventory* sub-menu. This screen provides a handy display of available ports on your equipment. If you do a little more discovery, as described in Learned MAC Address on page 629, you can also display learned MAC addresses on those ports.

Figure 14-1. Ports



Port Manager (Default Port View - Default Port Filter)

Using Filter: Name contains *

Port Icon	Device	Name	Port Description	Port Type
	c12k-0.122.cisco.com-19...	GigabitEthernet0/1/1/4	GigabitEthernet0/1/1/4	Gigabit Ethernet Port
	c12k-0.122.cisco.com-19...	MgmtEth0/0/CPU0/1	MgmtEth0/0/CPU0/1	In-band Management
	c12k-0.122.cisco.com-19...	MgmtEth0/0/CPU0/2	MgmtEth0/0/CPU0/2	In-band Management
	c12k-0.122.cisco.com-19...	MgmtEth0/0/CPU0/0	MgmtEth0/0/CPU0/0	In-band Management
	c12k-0.122.cisco.com-19...	GigabitEthernet0/1/1/0	GigabitEthernet0/1/1/0	Gigabit Ethernet Port
	c12k-0.122.cisco.com-19...	GigabitEthernet0/1/1/3	GigabitEthernet0/1/1/3	Gigabit Ethernet Port
	c12k-0.122.cisco.com-19...	GigabitEthernet0/1/1/1	GigabitEthernet0/1/1/1	Gigabit Ethernet Port
	c12k-0.122.cisco.com-19...	GigabitEthernet0/1/1/2	GigabitEthernet0/1/1/2	Gigabit Ethernet Port

Max items displayed: 100

1 of 8 item(s) selected

Name: GigabitEthernet0/1/1/0

Model:

MAC Address: 00 15 2b 81 40 3b

*** GigabitEthernet0/1/1/0 ***
GigabitEthernet0/1/1/0.1000
GigabitEthernet0/1/1/0.1001
GigabitEthernet0/1/1/0.1002
GigabitEthernet0/1/1/0.1003
GigabitEthernet0/1/1/0.1004
GigabitEthernet0/1/1/0.1005

Use the pick lists at the top of this screen to filter ports on discovered equipment that appear in the screen below. The filters let you search for ports using logical operators. You can filter not only by ports' descriptions, but also by whether they are operational. You can also click the columns headings to sort contents in these columns to order ports, for example, by their operational state.

The *In Use* column indicates whether a link is tied to the port.

NOTE:

If functional permissions do not allow Port editing, then the *Save* button for Ports is disabled. This solution applies to port components only when they are opened from Resource Manager, Topology or the Port Manager.

The details for selected ports appear at the bottom of the screen. See Detail Panels on page 628.

CAUTION:

Unless you create a filter and save it as described in Chapter 28, Filters, any filters you create here are not preserved.

Use the *Action* menu or right-click to *Open* a selected port, and the Resource Editor for that port appears. The following options are also available in this menu:

- **Print**—Prints the current view to an Acrobat® file. Use the filters at the top of this screen to determine which ports appear in this report.

NOTE:

You must have Acrobat reader installed for this to function correctly.

- **Open**—Edits the port. See Chapter 5, *Resources*, and the sections (particularly the device driver screens) that follow for details about what appears in the editor.
- **Delete**—Removes the port(s) selected from those listed.
- **Map**—Display a topology view that includes the selected port(s). When mapping port objects from this menu item, the associated parent objects for the Port also appear—for example, a card and the top-level equipment.
- **Resync**—Resyncs the port(s) selected.
- **Alarms**—Display the alarms for the selected port(s).
- **Help**—Open online help for this screen.

Detail Panels

The following detail panels appear when you select a port listed at the top of the screen.

Model

This panel discloses the following attributes:

- **Name**—The name of the port.
- **Model**—The name of the port.
- **MAC Address**—The port’s Media Access Control (MAC) address.

SubComponents

This panel displays a tree of the port and any of its subcomponents.

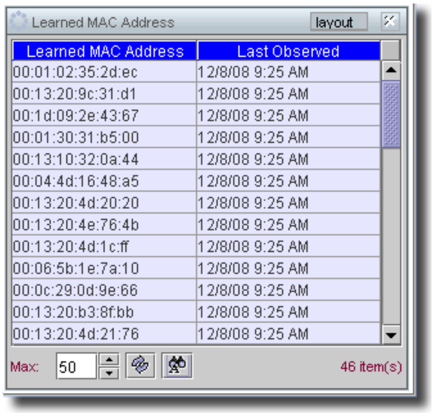
The following panels are available, but do not appear by default. Click the + at the top right of the details panels to add them.

Learned MAC Address

Port Manager lets you discover any learned MAC addresses on discovered ports. Do this either manually (click the button at the bottom of the detail panel), or by configuring and executing a *Learned MAC Address Discovery* schedule. See Scheduling Learned MAC Discovery, below.

This detail panel does not appear by default. If you elect to display it, after learned MAC address discovery, any learned MAC addresses for the selected port appear, along with the time and date they were last observed.

Figure 14-2. Learned MAC Address Detail Panel



Learned MAC Address	Last Observed
00:01:02:35:2d:ec	12/8/08 9:25 AM
00:13:20:9c:31:d1	12/8/08 9:25 AM
00:1d:09:2e:43:67	12/8/08 9:25 AM
00:01:30:31:b5:00	12/8/08 9:25 AM
00:13:10:32:0a:44	12/8/08 9:25 AM
00:04:4d:16:48:a5	12/8/08 9:25 AM
00:13:20:4d:20:20	12/8/08 9:25 AM
00:13:20:4e:76:4b	12/8/08 9:25 AM
00:13:20:4d:1c:ff	12/8/08 9:25 AM
00:06:5b:1e:7a:10	12/8/08 9:25 AM
00:0c:29:0d:9e:66	12/8/08 9:25 AM
00:13:20:b3:8f:bb	12/8/08 9:25 AM
00:13:20:4d:21:76	12/8/08 9:25 AM

Max: 50

46 item(s)

It its bottom, this panel has a setting for maximum displayed rows that you may alter to see more of the learned MAC addresses on the selected port. It also has the following buttons:

- **Refresh**—This updates the display based on the database. This is useful to update the display based on a scheduled discovery (see Scheduling Learned MAC Discovery on page 630).
- **Collect Learned MAC Addressees from Device**—Click this button to query the device, not this application's database, for its learned MAC addresses. This is the manual equivalent of what is described in **Scheduling Learned MAC Discovery on page 630**.

You must collect learned MAC addresses on the connected network devices before you can discover links between Windows (WMI) or Unix (WBEM) hosts and network devices.

Notes

This panel does not appear by default. When you display it, use the *Edit* button on this panel to enter text notes about the selected port.

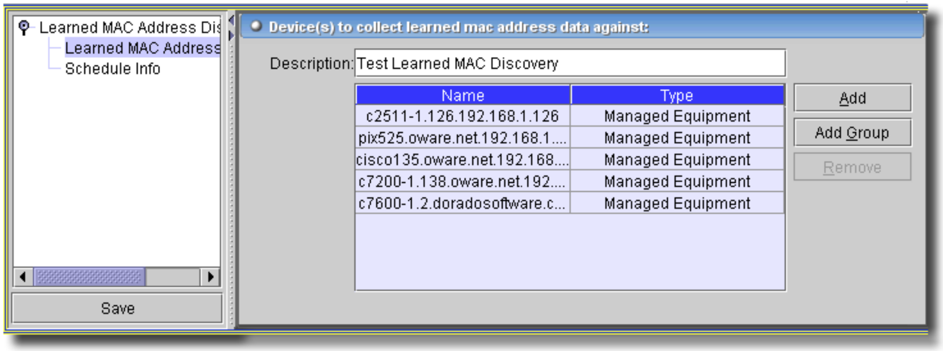
CLI-Based Discovery

For some supported devices, reading the SNMP MIB is not as reliable as command-line interface (CLI) interaction, so this application uses the latter.

Scheduling Learned MAC Discovery

If you create a new schedule and select *Learned MAC Discovery*, you must simply name this schedule and then select the devices where you plan to discover learned MAC addresses.

Figure 14-3. Scheduling Learned MAC Discovery



Description: Test Learned MAC Discovery

Name	Type
c2511-1.126.192.168.1.126	Managed Equipment
pix525.oware.net.192.168.1....	Managed Equipment
cisco135.oware.net.192.168....	Managed Equipment
c7200-1.138.oware.net.192....	Managed Equipment
c7600-1.2.doradosoftware.c...	Managed Equipment

Click *Add* or *Add Group* to select devices individually or by equipment group. The *Remove* button deletes any device or group you select in this list. Use the *Schedule Info* screen to configure the time this discovery is to run. See Schedule Info on page 750 for more about the Schedule Info screen.

CAUTION:
OpenManage Network Manager does not come with a database aging policy (DAP) for learned MAC address, by default. You must create and schedule one for it to be effective in limiting the impact of Learned MAC Discovery on the database.

15

Resource Roles

Introducing Resource Roles

The Resource Roles Managers provides functionality and screens that let you manage resource roles in your network—another kind of grouping. Groups are not the same as roles. Both are ways of addressing collections of resources you have discovered. The optional Group Operations capabilities let you act on groups of resources.

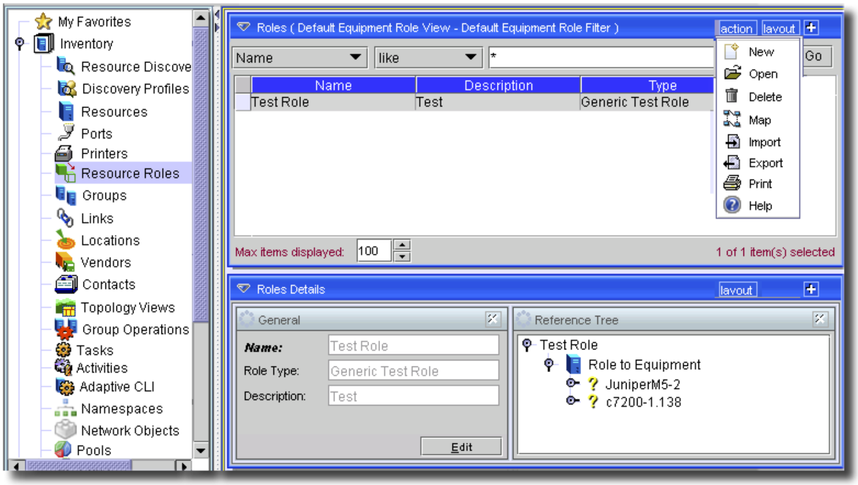
Resource roles also let you group pieces of equipment together. You can specify a role for selected resources in the *General* Panel of the Resource Editor, or by opening Resource Role Manager from the navigation window.

Resource instances refer to roles, as opposed to the optional resource groups. You can filter resources based upon a role but from the roles perspective you cannot see the list of resources. Permissions may be set for roles automatically. On the other hand, resource groups refer to the resources. From the resource group's perspective you can see its member resources. Group operations use the resource groups. Resource groups also allow for dynamic membership as well as supported nested groups for easier management. Other than these somewhat subtle differences groups and roles basically accomplish the same thing.

CAUTION:
Unless you create a filter and save it as described in Chapter 28, Filters, any filters you create here are not preserved.

Select *Resource Roles* from the *File* -> *Open* -> *Inventory* menu or the Navigation Window to display the Resource Role Manager.

Figure 15-1. Resource Role Manager



Name	Description	Type
Test Role	Test	Generic Test Role

Name: Test Role

Role Type: Generic Test Role

Description: Test

Test Role
Role to Equipment
JuniperM5-2
c7200-1.138

The following are the Action or right-click menu controls on the Resource Role Manager:

- **New**—Creates a new resource role. Select the type of role in the screen that appears after you click *New* to select either a *Resource* or *Configuration File* role.
- **Open**—Opens the selected resource role for modification with the editor described in Creating or Modifying Resource Roles.
- **Delete**—Deletes an resource role. Select the role to remove and click *Delete*. The application prompts you for confirmation.
- **Map**—Open a Topology view containing the resources that are members of a selected role. See Chapter 21, Topology Views for more about what appears when you select this option.
- **Export/Import**—Export or import the listed items as/from XML. Import brings in an resource role. The *Export* menu item exports an resource role to a text file (RC-EquipmentRole_entities.oof by default). These exported files can serve as backups or as seed files, and can be imported by clients running on other servers.
- Print—Print the listed items to an Acrobat file. (You must have Acrobat reader installed for this to work properly.) Change the filter and click *Go* to change this printed report's appearance.
- **Help**—Open the context-sensitive help for this screen.

Creating or Modifying Resource Roles

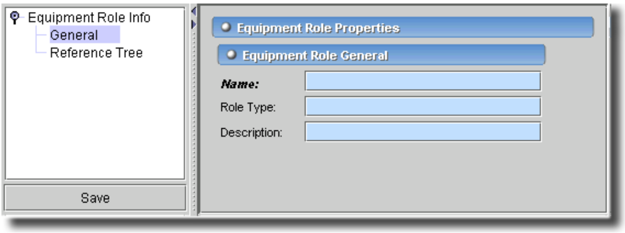
To edit an existing role, select it and click *Open*. To create a new role, click *New*. If you click *New*, you must decide whether to create a *Generic Role* (described in the following sections), or, if you have the *File Management* option installed, you can create a *Configuration File Role*.

- General Tab
- Reference Tree

General Tab

The General tab sets the most general information about the resource role.

Figure 15-2. Role Editor



Name:

Role Type:

Description:

The following are the fields on the Resource Role Editor:

- **Name**—A unique name for the role.

- **Role Type**—An optional description of the role type.

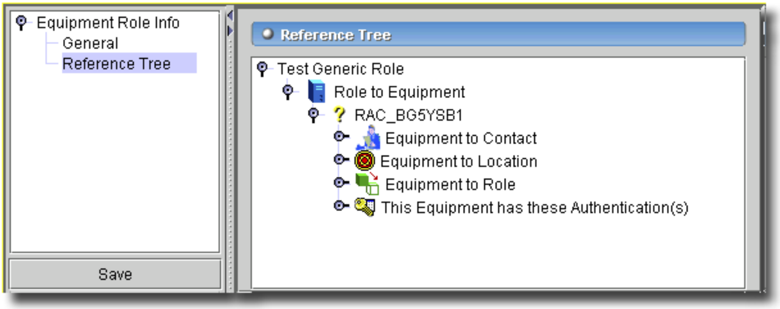
- **Description**—An optional description of the role.

Click the *Save* icon (or *File -> Save*) to save the new role.

Reference Tree

This tab displays any references to this role in tree format.

Figure 15-3. Reference Tree



Test Generic Role
Role to Equipment
RAC_BG5YSB1
Equipment to Contact
Equipment to Location
Equipment to Role
This Equipment has these Authentication(s)

This is similar to the *Preview* detail panel that appears in the editor. Subnodes appear for the resources that use this role, and subsequent sub-nodes describe

16

Groups

Introducing Groups

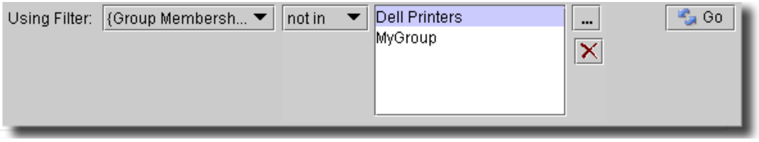
Groups manager provides functionality and screens that let you manage groups of resources in your network. Group Operations let you select groups of resources, then use the optional *Group Operations Manager* to manage those resources.

Certain dynamic groups are seeded by installing this software. For example *All Devices* is a dynamic group containing all resources. Similarly, discovery automatically produces vendor groups for all discovered resources.

NOTE:

You can now filter on group membership in *Resource Manager* when groups are configured before the filtering operation.

Figure 16-1. Filtering on Group Membership



Using Filter: {Group Membersh... ▼ not in ▼ Dell Printers MyGroup

NOTE:

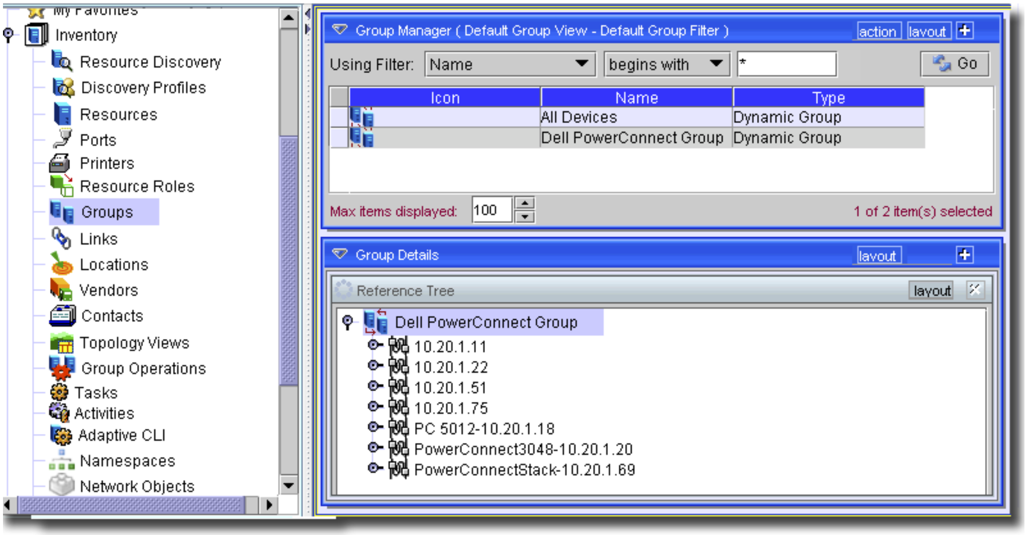
When using such a filter, click the command button (...) to select one or more groups, and use the red “X” to delete a selected group. The operators are *in* and *not in*.

Groups Manager

This Manager lets you define resource groups to perform operations that act on several resources at once. Access it from the Navigation Window, or from *File -> Open -> Inventory -> Groups*.

Group Manager provides two types of groups, *static* and *dynamic*. A static group stores a static list of Resource references. A dynamic group stores a filter definition that can dynamically query for Resource.

Figure 16-2. Groups Manager



Using Filter: Name begins with *

Icon	Name	Type
	All Devices	Dynamic Group
	Dell PowerConnect Group	Dynamic Group

Max items displayed: 100

1 of 2 item(s) selected

Dell PowerConnect Group
- 10.20.1.11
- 10.20.1.22
- 10.20.1.51
- 10.20.1.75
- PC 5012-10.20.1.18
- PowerConnect3048-10.20.1.20
- PowerConnectStack-10.20.1.69

Filter the groups that appear by checking *Filter*, and selecting their *Name* (characters or wildcards) and click the *Go* button to populate the list of available groups.

CAUTION:
Unless you create a filter and save it as described in Chapter 28, Filters, any filters you create here are not preserved.

With *Action* (or right-click) menu items), you can do the following:

- **New**—Opens a screen where you can select whether you want to create groups as described in Static Groups on page 637 or Dynamic Groups on page 638. Whenever you open these editors, the *Group Info* tab lets you name the group. The other tab lets you select (or filter for) the resources in the group.
- **Open**—Opens the selected group for modification in the appropriate editor.
- **Print**—Prints the listed groups to an Acrobat file (you must have Acrobat reader installed). To change the list printed, use the filter at the top of this screen.
- **Delete**—Deletes the selected group. Select the group to remove and click *Delete*. The application prompts you for confirmation.

CAUTION:
When you delete a group that is the target for group operations, the group operation no longer works correctly.

- **Map**—Opens the Topology Viewer, displaying the selected group’s resources. See Creating or Modifying Topology Views on page 662 for more information.
- **Import** —Imports an XML file of groups.

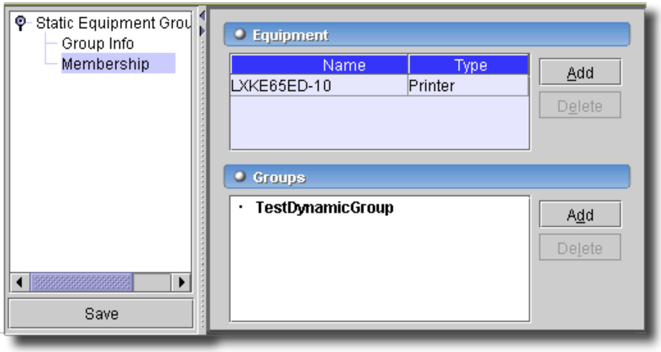
- **Export**—Exports an XML file of the listed groups to a directory you select. Exported files can serve as backups or as seed files, and can be imported by clients running on other servers.
- **Help**—Opens the online help screen for this manager

When you select a group in the upper panel, the lower panel displays a tree, with the group's membership as sub-nodes. If you right-click a sub-node, an appropriate action menu appears; if you click a resource node, the options mirror the action menu described in Action Button / Right-Click Menu on page 213.

Static Groups

If you selected a static group, then you can click on the *Membership* node of the tree on the left. (See Dynamic Groups on page 638 for the alternative).

Figure 16-3. Group Editor - Static Group Editor



Name	Type
LXKE65ED-10	Printer

NOTE:

If you select equipment in Resources manager, then click the New Group button, the Static Group screen displays the selected equipment in its list.

This displays a table of entities with columns for *Name* and *Type*. Click the *Add* button to display a screen where you can select the resources for this static group. You can also add sub-groups in the *Groups* panel below the *Equipment* panel. These appear as group nodes. You can add a dynamic group as a sub-group. Its contents are updated whenever the application runs the query that populates it.

Click *Save* to confirm your selection. The resources in the group appears in the groups details screen for this group, as described in Groups Manager on page 635.

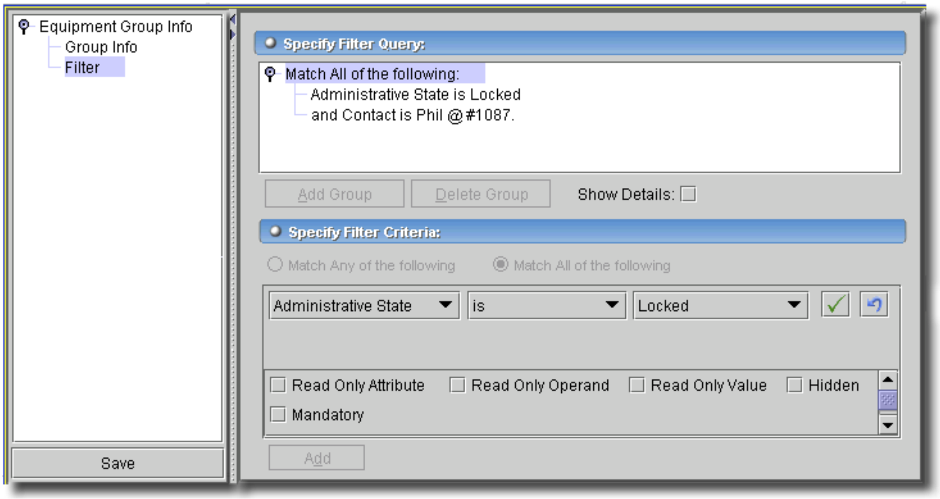
NOTE:

If resources are in both the super- and sub-group, the application recognizes this and eliminates any conflict.

Dynamic Groups

If you selected a dynamic group, then you can click on the *Filter* node of the tree to see the filter criteria.

Figure 16-4. Group Editor - Dynamic Group Filter



Equipment Group Info
- Group Info
- Filter

Specify Filter Query:

Match All of the following:
- Administrative State is Locked
- and Contact is Phil @#1087.

Show Details: □

Specify Filter Criteria:

○ Match Any of the following ● Match All of the following

Administrative State | is | Locked

□ Read Only Attribute □ Read Only Operand □ Read Only Value □ Hidden □ Mandatory

Click the radio button for *Match Any of the following* ("OR"), or *Match All of the following* ("AND"), then click the *Add* button at the bottom of the screen, and select an item to match, an operator, and the match criteria. For more information (about the *Show Details* checkbox and the checkboxes for *Read Only, Hidden* and *Mandatory* attributes, see *Filter Editor on page* 736.

CAUTION:

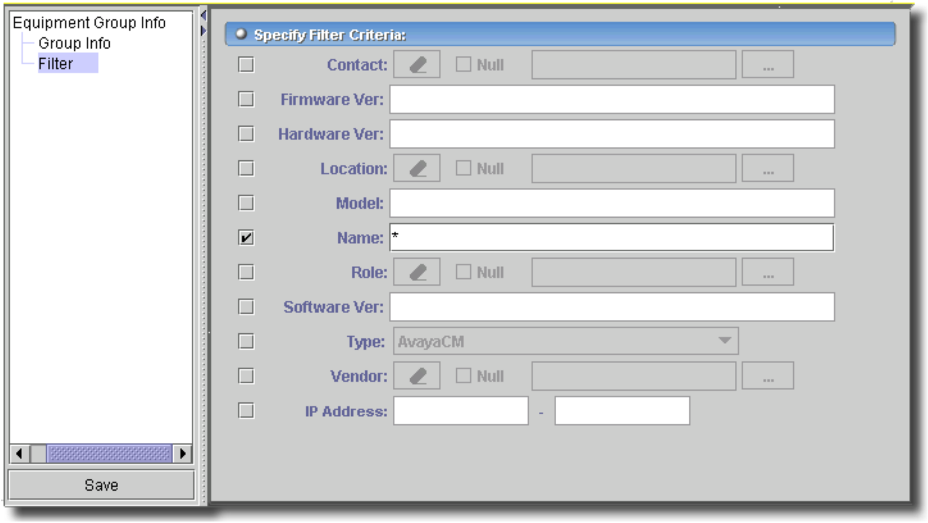
Groups that filter to select ranges of IP addresses are limited to a total of 254. If you are selecting from a range larger than that, create several groups.

Click *Save* to confirm your filter selection. The filtered resources appears in the groups details screen for this group, as described in Groups Manager on page 635.

Legacy Dynamic Groups

Some groups from previous versions of this software may have a different filter screen.

Figure 16-5. Group Editor – Legacy Dynamic Groups



☑ Name: *

□ Type: AvayaCM

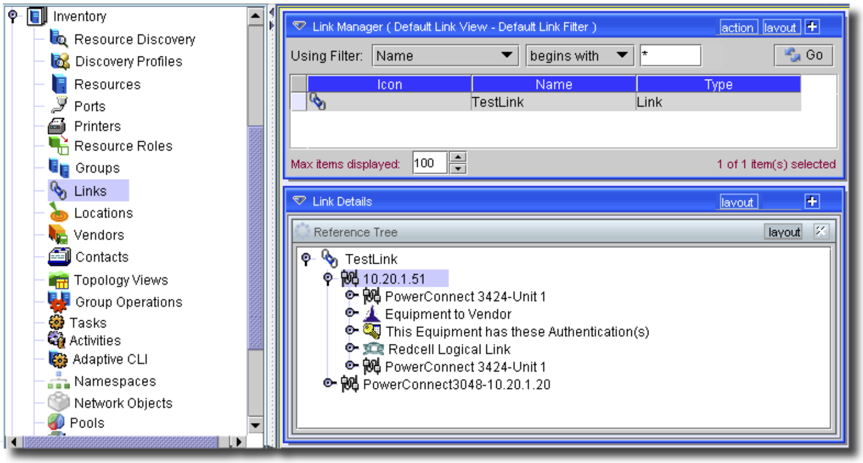
Check the criteria you want, and fill in the fields next to the checkbox with specifics, or with wildcard characters.

Links

Links Overview

The Link Manager lets you create and edit both logical and physical links. Select *Inventory -> Links* from the *File -> Open* NetManagermenu or the Navigation Window to display the Link Manager.

Figure 17-1. Links



Using Filter: Name begins with *

Icon	Name	Type
	TestLink	Link

Max items displayed: 100

1 of 1 item(s) selected

The following are the controls on the Link Manager’s action (or right-click) menu:

- **New**—Opens the Link Editor, through which you can define a new link. If you have not selected a link type from the Link Type drop-down menu you are prompted to select one from the Link Type dialog. See Creating or Modifying a Link on page 646 for more information on the Link Editor.

- **Open**—Opens the selected link for modification. See Creating or Modifying a Link on page 646 for more information.

- **Print**—Prints the listed links to an Acrobat® file (you must have Acrobat reader installed). To change the list of links, use the filter at the top of this screen.

- **Delete**—Deletes the selected link. Select the link to remove and click *Delete*. The application prompts you for confirmation.

- **Discover Links**—Opens a wizard to discover existing links. See Discovering Links on page 642.

- **Map**—Opens the Topology Viewer, displaying the selected link. See Creating or Modifying Topology Views on page 662 for more information.
- **Extended Map**—Displays the actual endpoints of a link as applicable. For example, if a link exists between a port on device A and a port on device B, the regular *Map* command displays only device A and B nodes and a link between them. This command displays the two ports and the link between them along with the associated parent entities.
- **Help**—Opens the online help screen for this manager.

Filtering the List of Links

The Link Manager displays a tree listing all defined links. You can filter the listing by any combination of three fields (located at the top of the Link Manager):

- **Name**—Enter characters, or wildcards to restrict the display.
- **Type**—Select a link type from the drop-down menu to restrict the display.

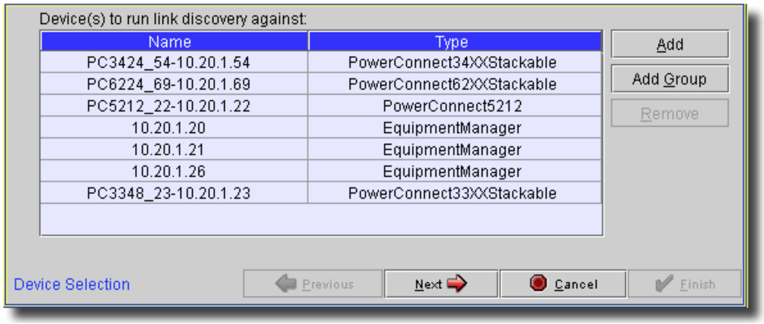
Check the *One Sided* check box to make this filter one sided (links have only one connection). Click *OK* to continue.

CAUTION:
Unless you create a filter and save it as described in Chapter 28, Filters, any filters you create here are not preserved.

Discovering Links

When you click *Discover Links* in the Link Manager screen, the link discovery wizard appears.

Figure 17-2. Link Discovery Wizard—Select Equipment



Device(s) to run link discovery against:

Name	Type
PC3424_54-10.20.1.54	PowerConnect34XXStackable
PC6224_69-10.20.1.69	PowerConnect62XXStackable
PC5212_22-10.20.1.22	PowerConnect5212
10.20.1.20	EquipmentManager
10.20.1.21	EquipmentManager
10.20.1.26	EquipmentManager
PC3348_23-10.20.1.23	PowerConnect33XXStackable

This wizard walks you through the following steps:

- Device Selection
- Link Discovery Options

- Link Discovery Status

NOTE:

This software will discover ethernet links between devices that have CDP, EDP, or LLDP enabled. These protocols are often enabled by default in network devices.

When you discover links between devices and entire network, an out-of-domain indicator appears if the end point of a link is not yet discovered. If you discover that missing end point, the topology does not change unless you perform link discovery again.

Discovering Ethernet Links for WBEM and WMI devices

If a discovered Windows (WMI) or Unix / WBEM host has an ethernet port, you can discover links between these hosts and the network devices to which they connect, provided you first perform or schedule Learned MAC address discovery on the network device(s) to which they connect. See Learned MAC Address on page 629 and Scheduling Learned MAC Discovery on page 630 for details. After you have discovered the learned MAC addresses for a device, link discovery functions on these Windows and Unix devices.

Device Selection

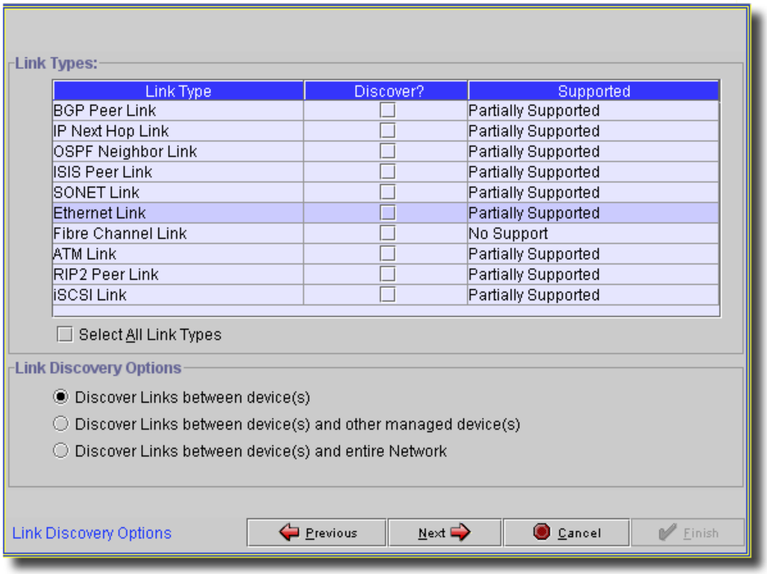
In the first screen, you select the equipment to query for links. Click *Add* or *Add Group* to display an equipment or group selection screen, and click *Select* after clicking on the equipment or equipment groups. You can also select a listed item and click *Remove* to deleted it from the equipment to be queried.

Unless you are selecting devices for a scheduled discovery, after you have selected all equipment and groups you want, click *Next*.

Link Discovery Options

This subpanel displays options enabling discovery of a variety of routes.

Figure 17-3. Link Discovery Wizard—Options



Link Types:

Link Type	Discover?	Supported
BGP Peer Link	□	Partially Supported
IP Next Hop Link	□	Partially Supported
OSPF Neighbor Link	□	Partially Supported
ISIS Peer Link	□	Partially Supported
SONET Link	□	Partially Supported
Ethernet Link	□	Partially Supported
Fibre Channel Link	□	No Support
ATM Link	□	Partially Supported
RIP2 Peer Link	□	Partially Supported
iSCSI Link	□	Partially Supported

□ Select All Link Types

Link Discovery Options

● Discover Links between device(s)

○ Discover Links between device(s) and other managed device(s)

○ Discover Links between device(s) and entire Network

NOTE:

Ethernet Link Discovery requires at least two devices to be specified for links to be created.

Link Types

Click the check boxes to select any type of link to discover (or check *Select All Link Types*). Notice that the *Supported* column displays whether the link type listed is supported by what you have selected.

Link Discovery Options

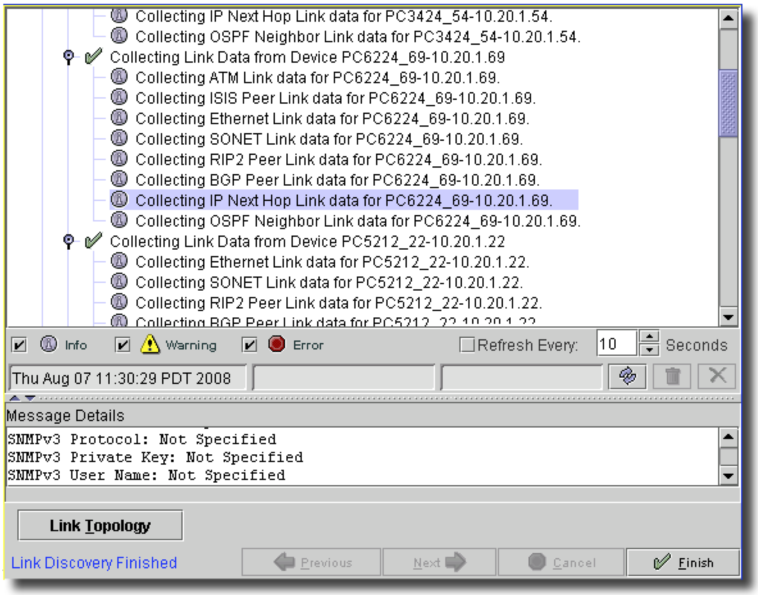
You can also select to discover links between the equipment you selected only, between those selected devices and other managed devices, or between selected devices and the entire network with the radio buttons at the bottom of this screen.

Unless you are selecting devices for a scheduled discovery, click *Next*, *Previous* or to proceed. Click *Cancel* to quit discovery.

Link Discovery Status

If you click *Next*, a progress screen opens.

Figure 17-4. Link Discovery—Status



```
Collecting IP Next Hop Link data for PC3424_54-10.20.1.54.
Collecting OSPF Neighbor Link data for PC3424_54-10.20.1.54.
Collecting Link Data from Device PC6224_69-10.20.1.69
    Collecting ATM Link data for PC6224_69-10.20.1.69.
    Collecting ISIS Peer Link data for PC6224_69-10.20.1.69.
    Collecting Ethernet Link data for PC6224_69-10.20.1.69.
    Collecting SONET Link data for PC6224_69-10.20.1.69.
    Collecting RIP2 Peer Link data for PC6224_69-10.20.1.69.
    Collecting BGP Peer Link data for PC6224_69-10.20.1.69.
    Collecting IP Next Hop Link data for PC6224_69-10.20.1.69.
    Collecting OSPF Neighbor Link data for PC6224_69-10.20.1.69.
Collecting Link Data from Device PC5212_22-10.20.1.22
    Collecting Ethernet Link data for PC5212_22-10.20.1.22.
    Collecting SONET Link data for PC5212_22-10.20.1.22.
    Collecting RIP2 Peer Link data for PC5212_22-10.20.1.22.
    Collecting BGP Peer Link data for PC5212_22-10.20.1.22
```

☑ Info ☑ Warning ☑ Error □ Refresh Every: 10 Seconds

Thu Aug 07 11:30:29 PDT 2008

Message Details

```
SNMPv3 Protocol: Not Specified
SNMPv3 Private Key: Not Specified
SNMPv3 User Name: Not Specified
```

Link Discovery Finished

This displays the status as discovery progresses. Click the *Link Topology* button at the bottom of the screen to see a logical topology view of what has been discovered (see *Chapter 21, Topology Views* for specifics).

SNMP-Based Discovery

For many of the two link endpoints, the application interrogates the Bridge-MIB for values in following tables.

`.iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dBase.dot1dBasePortTable`

`.iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dTp.dot1dTpFdbTable`

Learned ports in Dot1dTpFdbTable are the basis for all links created.

Once L2 links are known, link discovery tries to resolve the L2 learned links to L3 links using `.iso.org.dod.internet.mgmt.mib-2.ip.ipNetToMediaTable`. This table shows the L2 MAC address mapping to L3 IP addresses. At this point all link parameters have been discovered from the device. The application must then associate the L3 address to known devices to represent the links.

If the application cannot resolve an L3 IP address from the above process to the the port level of a device, then it uses the top level managed object (MO) to represent the link endpoint.

If two devices have the same port level IP address when the link is being created, the application uses the first address found to create the link. If the first one found is the on the wrong MO, port level link creation will default to using the top level MO of the device selected for link discovery rather than the incorrect MO. In this case the endpoint appears as the top level MO rather than the port.

NOTE:

To search the database for the duplicate, first execute startbombrowser, then set the package to RedCell.config, the Class to NetworkResourceIPLookup, selection IPAddress as the attribute, and set Value to the <ip address> you are looking for. This is the port IP address on the device that is *not* showing port level link discovery. Do *not* edit anything with the BOMbrowser. If the BOM Query does find duplicate IPs, reconfigure the device(s) IPs and run resync on the MO to remove duplicates from the database.

Creating or Modifying a Link

When you click *New* or *Edit* in the Link Manager, the Link Editor appears. When you have made all necessary changes click *OK* to save it or *Cancel* to discard it.

When you click *New*, you are prompted to select which kind of link to create. For example: *ATM Link*, *BGP Peer Link*, *Site Logical Connection*, and so on. The actual list of choices depends on the application options you have installed.

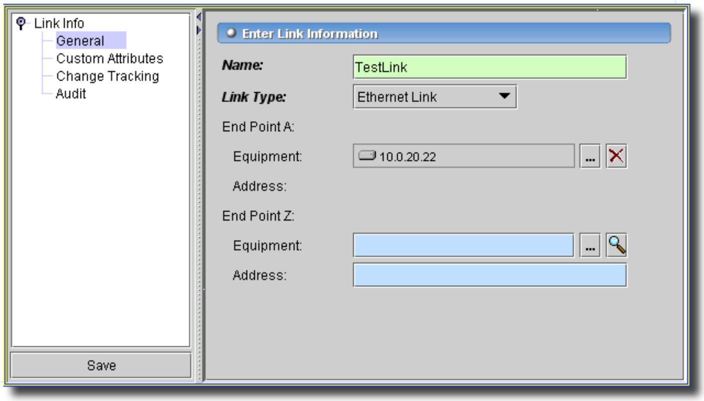
NOTE:

Manually added links reflect the alarm state of their terminating equipment.

General Panel

This panel contains general information about the link to be created.

Figure 17-5. Link Manager: General Panel



Name: TestLink

Link Type: Ethernet Link

End Point A:

Equipment: 10.0.20.22

Address:

End Point Z:

Equipment:

Address:

Complete the following fields:

- **Name**—Enter a unique name for the new link.
- **Link Type**—For existing, discovered links, displays the type of link. For new links, lets you select the type from a pick list.
- **End Point 1**—Click the search magnifying glass, or command button to display a list of Equipment. Select the appropriate device and click *OK*. See Chapter 13, Resources for more information about managing Equipment.
- **End Point 2**—Click the search magnifying glass, or command button to display a list of Equipment. Select the appropriate device and click *OK*. See Chapter 13, Resources for more information about managing Equipment.
- **Sub Links**—Sublinks appear in this lowest panel. Click *Add* to add one, or *Delete* to remove a selected sublink. A link selection screen appears when you do this.

NOTE:

The application’s title bar also displays information about the link.

The *Custom Attributes* tab lets you configure previously configured attributes. See Custom Fields on page 178.

The *Change Tracking* screen displays changes to attributes you have already configured for tracking. See Change Tracking on page 180.

The *Audit* tab displays a history of the action related to this link. See *Audit on page* 228 for more information.

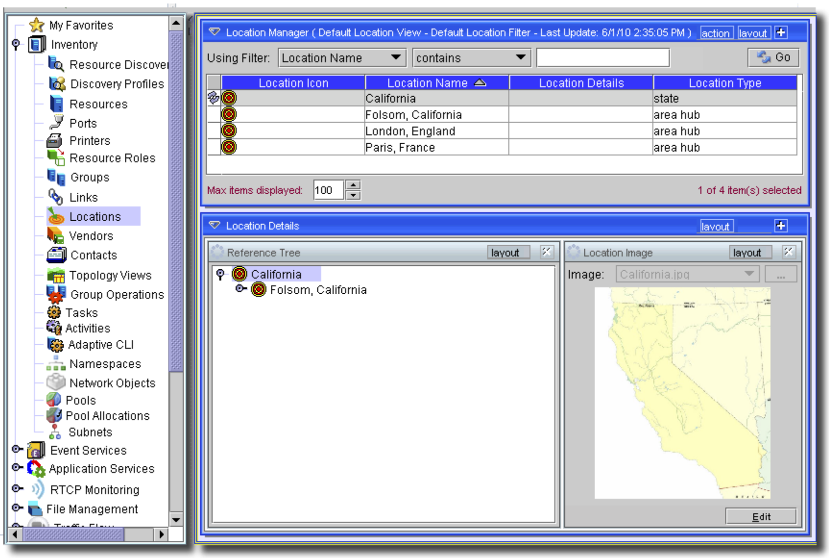
Locations

Locations Overview

You can specify equipment locations within the Locations screen. Note that locations can have “Parent” Locations, they can be subsets of another location. For example, if network objects are on the third floor of a facility, you can designate both the building and the specific floor as locations; the building would be the parent of the floor.

To access the Locations screen, select *Inventory* -> *Locations* from the *File* -> *Open* -> NetManagermenu or the Navigation Window. The Locations screen appears.

Figure 18-1. Locations Screen



Location Manager (Default Location View - Default Location Filter - Last Update: 6/1/10 2:35:05 PM)

Using Filter: Location Name contains

Location Icon	Location Name	Location Details	Location Type
●	California		state
●	Folsom, California		area hub
●	London, England		area hub
●	Paris, France		area hub

Max items displayed: 100

1 of 4 item(s) selected

Location Details

Reference Tree

- California
  - Folsom, California

Location Image

Image: California.jpg

The drop-down menu at the top of the window lets you apply a top-level location filter to restrict the display. Click *Go* when the Locations screen opens to display all defined locations.

CAUTION:

Unless you create a filter and save it as described in Chapter 28, Filters, any filters you create here are not preserved.

The following are the *Action* menu and right-click menu controls on the Locations screen (not all appear, necessarily):

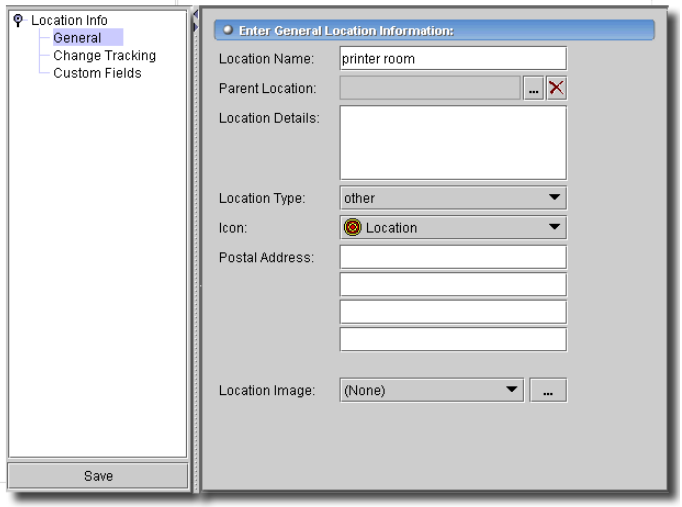
- **New**—Opens the Location Editor, through which you can define a new location. See Location Editor on page 651 for more information. If you have selected an existing location when you click this, the application prompts you to elect whether the new location is a sub-location from the selected one.
- **Open**—Opens a Location Editor for the selected location. You must select a location before this option appears in the context (right-click) menu. See Location Editor on page 651 for more information.
- **Delete**—Deletes the selected location. Select the location to remove and click Delete. The application prompts you for confirmation.

  When deleting a parent location, the application prompts you before deleting its associated child locations.
- **Print**—Create an Acrobat report of the items displayed in the inventory (change the filter and click *Go* to change this display). You must have the free Acrobat reader installed for this to function. See www.adobe.com to download and install this application.
- **Map**—Opens the Topology Viewer, displaying the selected location. If you select more than one location clicking *Map* opens a new map with the world map as the default background. If you select only one location, then that location appears using the background *Location image* specified. See Creating or Modifying Topology Views on page 662 for more information.
- **Import / Export**—This imports / exports a comma-separated value (CSV) file with information about all locations as a text file (`Location_entities.csv` by default). Exported files can serve as backups or as seed files, and can be imported by clients running on other servers. These files include a comma-separated heading row of value labels followed by a row of values for each location.
- **Event Management**—Lets you view alarms selected by location.
- **Help**—Opens the help for this screen.

Location Editor

When you click *New* or *Edit* in the Locations screen the Location Editor appears. Enter or modify information about the Location; you can specify name, parent location, address, and details, among other things.

Figure 18-2. Location Editor - General



Enter General Location Information:

Location Name: printer room

Parent Location:

Location Details:

Location Type: other

Icon: Location

Postal Address:

Location Image: (None)

If you click *New* with an existing location selected, the application prompts you to see whether this is a sub-location of the selected item. This editor has the following tabs:

- General
- Change Tracking
- Custom Fields

The following sections describe these.

General

The following are the fields in the Location Editor:

- **Location Name**—A unique name for the Location.

NOTE:

If you alter the name of an existing location already in use by existing equipment, the editor creates a new location. To change a location name, you must delete the original location and the equipment using it then re-make it. You can change the name of an unused location without deleting anything.

- **Parent Location**—The “parent” of this location (the location to which this location is subordinate). Click the Command button (...) to open a Browser through which you can select a Parent Location. Click the Eraser icon to clear the Parent Location field.

△ **CAUTION:**
15 is the maximum number of levels supported.

- **Location Type**—Type of location, as selected from the drop-down menu. Available types are: Customer, Provider, State, Area Hub, Regional Hub, National Hub, and Other.
- **Icon**—Select an icon from the drop-down list to associate it with the location.
- **Postal Address**—The address of location.
- **Location Image**—Select an image for the location. Once you select a file, it appears on the pick list, and is available from whatever client you chose (its location is on the application server). Typically these load from `\owareapps\redcell\backgrounds`. Any `.jpg, .gif`, or `.png` file can be an image. Once you load a file, it is available to all clients.

Click the *Save* icon to save the Location.

Change Tracking

This field is blank unless you have set it up in Change Tracking on page 180 (selecting a Vendor in Inventory Config on page 174. If you have done so, a log of changes to the selected inventory type and attributes appear in this screen.

Custom Fields

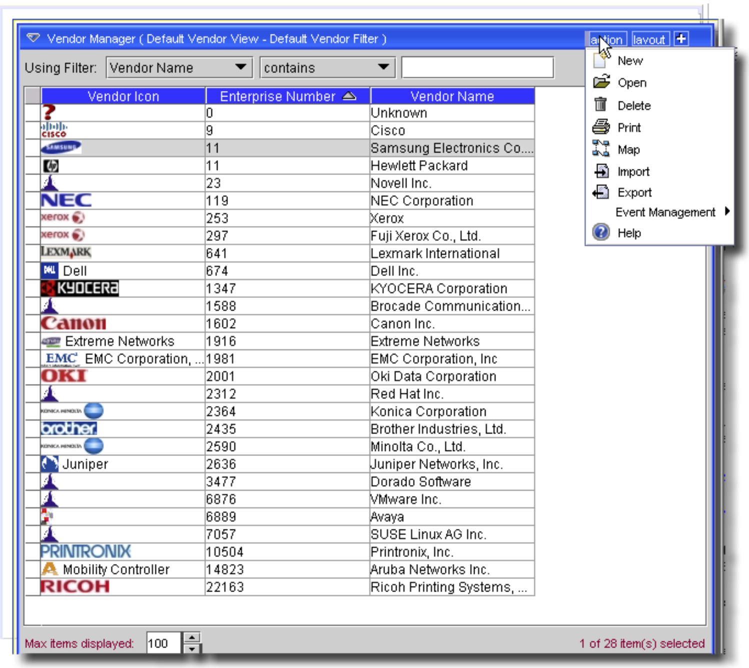
This panel is empty unless you have configured *Custom Fields* previously. See *Inventory Config on page 174* for instructions about how to configure custom fields, and Custom Fields on page 178 for examples.-

Vendors

Vendors Overview

You can create and modify contact information for vendors who supply equipment through the Vendors screen. To access the *Vendors* screen, select this from the *File -> Open -> Inventory* menu or the Navigation Window.

Figure 19-1. Vendors screen



Vendor Manager (Default Vendor View - Default Vendor Filter)

Using Filter: Vendor Name contains

Vendor Icon	Enterprise Number	Vendor Name
?	0	Unknown
cisco	9	Cisco
SAMSUNG	11	Samsung Electronics Co....
	11	Hewlett Packard
	23	Novell Inc.
NEC	119	NEC Corporation
xerox	253	Xerox
xerox	297	Fuji Xerox Co., Ltd.
LEXMARK	641	Lexmark International
Dell	674	Dell Inc.
KYOCERA	1347	KYOCERA Corporation
	1588	Brocade Communication...
Canon	1602	Canon Inc.
Extreme Networks	1916	Extreme Networks
EMC EMC Corporation, ...	1981	EMC Corporation, Inc
OKI	2001	Oki Data Corporation
	2312	Red Hat Inc.
KONICA MINOLTA	2364	Konica Corporation
brother	2435	Brother Industries, Ltd.
KONICA MINOLTA	2590	Minolta Co., Ltd.
Juniper	2636	Juniper Networks, Inc.
	3477	Dorado Software
	6876	VMware Inc.
	6889	Avaya
	7057	SUSE Linux AG Inc.
PRINTRONIX	10504	Printronix, Inc.
Mobility Controller	14823	Aruba Networks Inc.
RICOH	22163	Ricoh Printing Systems, ...

Max items displayed: 100

1 of 28 item(s) selected

The Vendors screen provides predefined filters to let you restrict the display, and also incorporates a search feature. Check the *Match All* box and configure the search term, operator and match term differently to restrict the list of filters displayed.

CAUTION:
Unless you create a filter and save it as described in Chapter 28, Filters, any filters you create here are not preserved.

Click column titles to sort on that column (repeated clicking toggles ascending/descending sort). Right click a listed item to view the context menu providing controls for the Vendors screen. It has the following menu items:

- **New**—Creates a new vendor. See Creating Vendors on page 654 for more information.
- **Open**—Edit an existing Vendor. See Creating Vendors on page 654 for more information.
- **Delete**—Deletes the selected vendor. The application prompts you for confirmation before removing the vendor from the system.

> NOTE:
>
> When you delete a vendor through the Vendors screen it does not delete the relevant contacts. You must delete them through the Contacts screen.

- **Print**—Create an Acrobat report of the items displayed in the inventory (change the filter and click *Go* to change this display). You must have the free Acrobat reader installed for this to function. See www.adobe.com to download and install this application.
- **Map**—Displays the instances of managed objects from this vendor in a Topology Viewer. See Creating or Modifying Topology Views on page 662 for more information.
- **Import / Export**—This appears in the *Action* button menu and imports / exports information about all vendors as a text file. Exported files can serve as backups or as seed files, and can be imported by clients running on other servers.
- **Event Management -> Alarms**—Alarms on this vendor's equipment displayed in an alarm manager.
- **Help**—Open the help for this screen.

Creating Vendors

Creating or modifying a vendor displays the Vendor Editor, which contains the following panels:

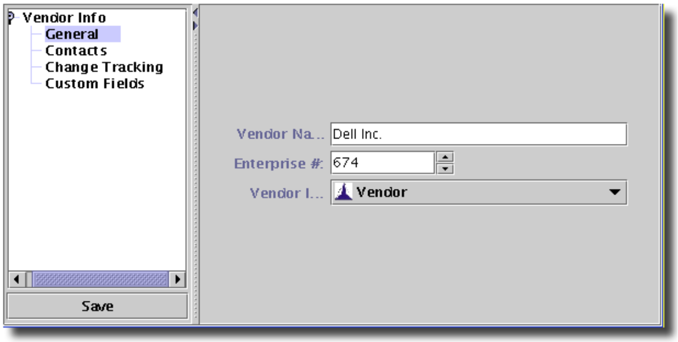
- General Panel
- Contacts Panel

Make changes as needed, then click *Save* to save the data or *Cancel* to close the editor without saving any changes.

General Panel

- This panel displays general information about the vendor.

Figure 19-2. Vendors screen—Information Panel



Vendor Na... Dell Inc.

Enterprise #: 674

Vendor I... Vendor

- The following are the fields on this panel:

- **Vendor Name**—The name of the vendor. This entry must be unique.

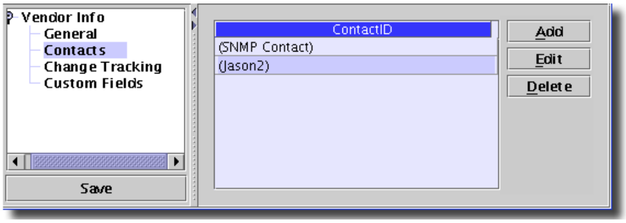
- **Enterprise #**—The unique number assigned this vendor. Best practice is *not* to change this.

- **Vendor Icon**—The icon associated with the vendor, selected from the drop-down list.

Contacts Panel

This panel displays contacts associated with a vendor. See Chapter 20, Contacts for more information on contacts.

Figure 19-3. Vendors screen—Contacts Panel



ContactID
(SNMP Contact)
(Jason2)

Click any of the following buttons:

- **Add**—Opens the Contacts screen. Select the contact to add and click *OK* to add it to the list.

- **Delete**—Removes the selected contact from the list.

Change Tracking

This field is blank unless you have set it up in Change Tracking on page 180 (selecting a Vendor in Inventory Config on page 174. If you have done so, a log of changes to the selected inventory type and attributes appear in this screen.

Custom Fields

This panel is empty unless you have configured *Custom Fields* previously. See *Inventory Config on page 174* for instructions about how to configure custom fields.

Contacts

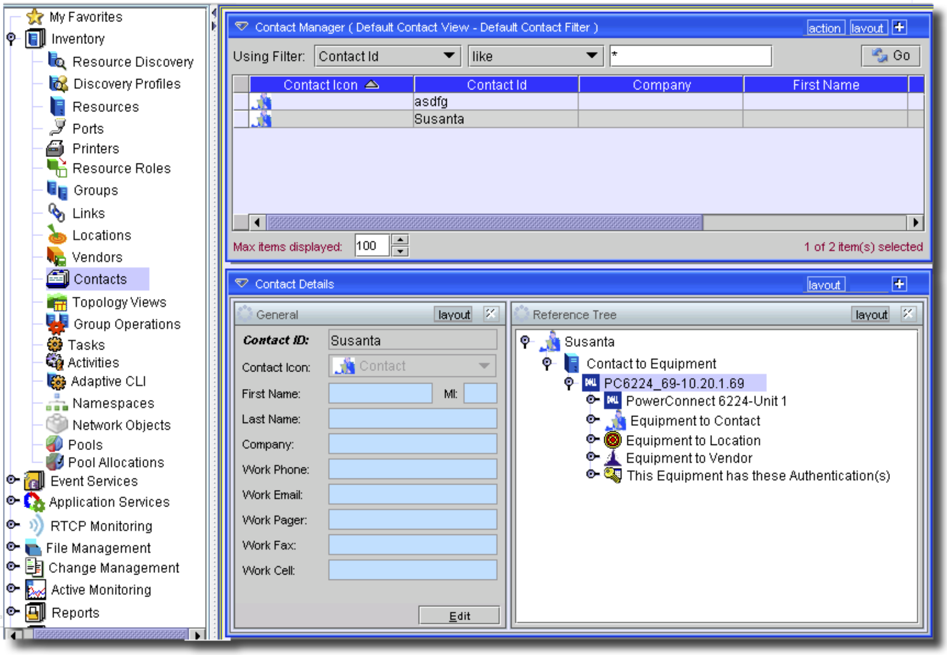
Contacts Overview

The Contacts screen lets you organize and manage your contacts. To access the *Contacts* screen, select it from the *File -> Open -> Inventory* menu, click its icon in the Navigation pane.

Click *Go* when the Contacts screen dialog initially opens to display all defined contacts. You can filter the display by configuring a search term, operator and match term, then clicking *Go.* For more information about Filters, see *Filter Wildcards on page* 738.

CAUTION:
Unless you create a filter and save it as described in Chapter 28, Filters, any filters you create here are not preserved.

Figure 20-1. .Contacts screen



Contact Manager (Default Contact View - Default Contact Filter)

Using Filter: Contact Id like *

Contact Icon	Contact Id	Company	First Name
	asdfg		
	Susanta		

Max items displayed: 100

1 of 2 item(s) selected

Contact ID: Susanta
Contact Icon: Contact
First Name:
MI:
Last Name:
Company:
Work Phone:
Work Email:
Work Pager:
Work Fax:
Work Cell:

When you select a contact, the *Details* panels at the bottom of this screen display specifics about the contact. See Creating or Modifying a Contact on page 659 for details of what can appear here. You can edit information in individual panels by clicking *Edit*. Click *Apply* after editing to save this information to the database.

To work with listed contacts or create new ones in this inventory, right click a listed item. The following context menu items appear:

- **New**—Creates a new contact. See Creating or Modifying a Contact on page 659 for more information.

- **Open**—Opens the selected contact for modification. See Creating or Modifying a Contact on page 659 for more information.

- **Delete**—Deletes the selected contact. The application prompts you for confirmation before removing the contact from the system.

- **Print**—Create an Acrobat report of the items displayed in the inventory (change the filter and click *Go* to change this display). You must have the free Acrobat reader installed for this to function. See www.adobe.com to download and install this application.

- **Map**—Displays the contact in the Topology Viewer. See Creating or Modifying Topology Views on page 662 for more information.

- **Import / Export**—This appears in the *Action* button menu, and imports / exports information about all contacts as a text file. Exported files can serve as backups or as seed files, and can be imported by clients running on other servers.

NOTE:

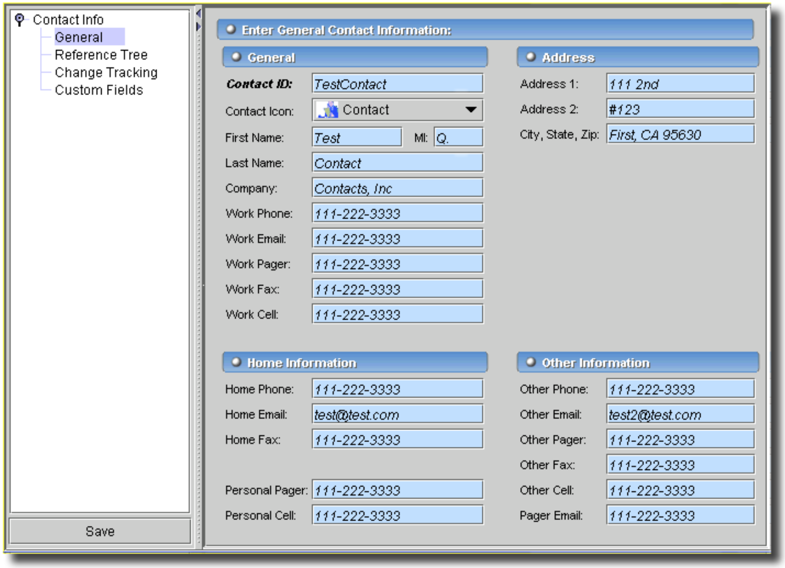
This report limits the number of columns to those that can fit on a single page width.

- **Help**—Opens the help for this screen.

Creating or Modifying a Contact

When you create or modify a contact the Contact Editor appears

Figure 20-2. Contact Editor



Enter General Contact Information:

General

Contact ID: TestContact

Contact Icon: Contact

First Name: Test MI: Q.

Last Name: Contact

Company: Contacts, Inc

Work Phone: 111-222-3333

Work Email: 111-222-3333

Work Pager: 111-222-3333

Work Fax: 111-222-3333

Work Cell: 111-222-3333

Address

Address 1: 111 2nd

Address 2: #123

City, State, Zip: First, CA 95630

Home Information

Home Phone: 111-222-3333

Home Email: test@test.com

Home Fax: 111-222-3333

Personal Pager: 111-222-3333

Personal Cell: 111-222-3333

Other Information

Other Phone: 111-222-3333

Other Email: test2@test.com

Other Pager: 111-222-3333

Other Fax: 111-222-3333

Other Cell: 111-222-3333

Pager Email: 111-222-3333

Close or save this screen with the icons on the toolbar, or items in the *File* menu. this screen has the following nodes:

- General
- Reference Tree
- Change Tracking
- Custom Fields

The following sections describe these screens in more detail.

General

The following are the fields in this screen:

- **Contact ID**—A unique identifier for this contact.

- **Contact Icon**—The icon associated with this contact. Select an icon from the drop-down list.

The next sections of this screen contain fields for the contact’s name, company, address and a variety of phone numbers.

Click the *Save* icon (or *File* -> *Save*) to save and close the contact, or click the *Close icon* to close it without saving changes.

Reference Tree

This panel displays icons reflecting relationships with a selected contact, as described in Reference Tree on page 221.

Change Tracking

This field is blank unless you have set it up in Change Tracking on page 180 (selecting a Vendor in Inventory Config on page 174. If you have done so, a log of changes to the selected inventory type and attributes appear in this screen.

Custom Fields

This panel is empty unless you have configured *Custom Fields* previously. See *Inventory Config on page 174* for instructions about how to configure custom fields.

21

Topology Views

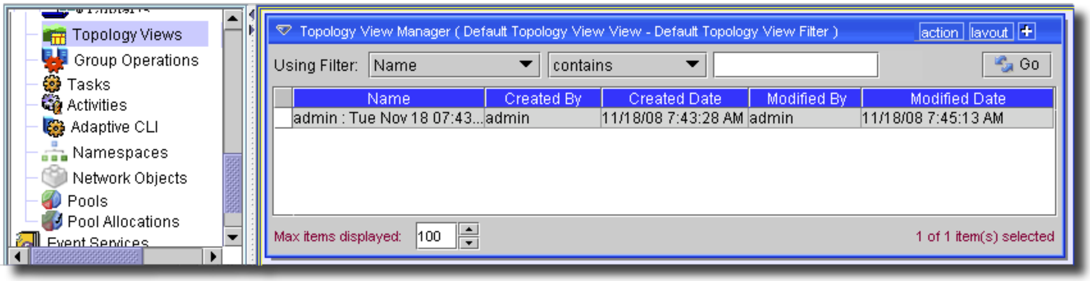
Overview

Topologies can model equipment locations, both logically and geographically, and can display their hierarchical relationships. The Chassis Viewer provides a representation of the device and any internal components. The Topology viewers let you view and monitor network devices, and respond to network alarms.

Topology Views

You can access topology views through the *Map* button in various screens like the Resources manager, for example (see Chapter 13, Resources), or by opening or creating a topology view from the Topology Views screen (available in the navigation window, or from *File -> Open -> Inventory -> Topology Views*).

Figure 21-1. Topology Views



Topology View Manager (Default Topology View View - Default Topology View Filter)

Using Filter: Name contains

Name	Created By	Created Date	Modified By	Modified Date
admin : Tue Nov 18 07:43...	admin	11/18/08 7:43:28 AM	admin	11/18/08 7:45:13 AM

Max items displayed: 100

1 of 1 item(s) selected

You can filter multiple views as described in *Filter Wildcards on page* 738. If you want to create a view, click the *New* button. Columns in this manager track the view name—by default, the creator's login ID and the creation date—as well as the creator, modifier, and date of creation and modification.

⚠ **CAUTION:**

Unless you create a filter and save it as described in Chapter 28, Filters, any filters you create here are not preserved.

Use the *Action* button to open the menus, or right-click the list of views. The following are the available items in this menu:

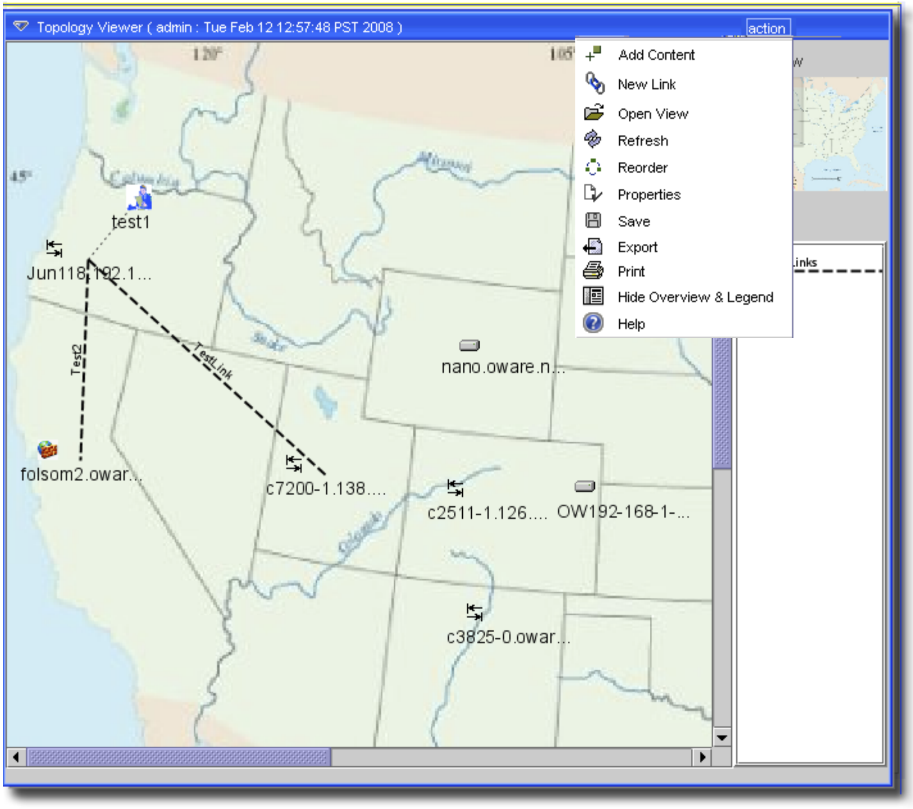
- **New**—Create a new, blank topology view.

- **Open**—Open an existing topology view to edit.
- **Delete**—Delete an existing, selected topology view.
- **Copy**—Copy an existing topology view as the basis for a new view.
- **Print**—Print a list of views. To alter the list, use the filter at the top of this screen. The printout appears as an Acrobat file, from which you can send the list to a printer, or save it as a file. You must have the free Acrobat reader installed for this to work correctly.
- **Help**—Create a new topology view.

Creating or Modifying Topology Views

When you *Open* or create a *New* view, the screen that appears displays the equipment with the arrangement and background you select.

Figure 21-2. Viewing Topology



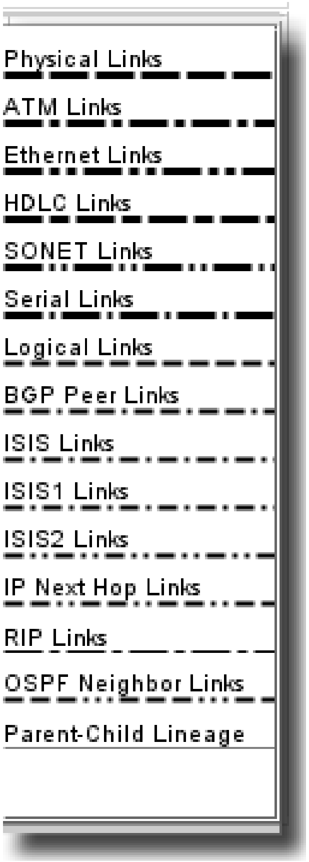
The view that appears on the left is often a detail of a larger layout. To move your point of view through the larger layout, click and drag the *Overview* rectangle in the top of the right panel.

NOTE:

In addition to panning the view, you can click and drag the mini-icons in the *Overview* rectangle. The larger icons in the topology view move to reflect their movements in *Overview*.

The *Legend* in the lower right corner displays the line conventions for various links between the icons.

Figure 21-3. Link Legend



The legend displays only the types of links that actually appear in the topology view.

NOTE:

No legend appears when links specified are really associations—for example, Equipment - to - Contact, or associations related to a displayed service and its components.

The topology view panel includes the following *Action* menu items:

- **Add Content**—This opens a pair of component chooser screens. First, you must select the type of component you want to add. For example: *Contact*, *Customer*, *Equipment Subcomponents* (which lets you add both), *Link*, *Location*, *Printer*, *Service*, and *Vendor*. Notice that if you add a *Contact* connected with a subcomponent, a dotted line connects them when they appear together in the view.

  You can also map supported *Adaptive Services*. See *Service Topology on page 683* for additional information about those.

  See also *Creating or Modifying a Contact on page 659*,*Chapter 13, Resources*, *Creating or Modifying a Link on page 646*, *Location Editor on page 651*, or Creating Vendors on page 654 for more about the screen that appears once you select the type of object you want to add to the view.

NOTE:

Until you select a link from the subsequent screen, no links appear in a view, even if you select linked equipment. If you Add a link, the equipment endpoints of the link will appear, even if you do not initially see them in your view.

- **New Link**—Select (at least) two components within the view, then click this item. You are prompted for the type of link you will create. For example: *ATMLink*, *BGPPeerLink*, *EthernetLink*, *FibreChannelLink*, *IPNextHopLink*, *ISIS1PeerLink*, *ISIS2PeerLink*, *ISISPeerLink*, *LogicalLink*, *OSPFNeighborLink*, *PhysicalLink*, *RIPPeerLink*, *SONETLink*. See *Creating or Modifying a Link on page 646* for more information about configuring the link you are about to create.

  When you discover links between devices and entire network, an out-of-domain indicator appears if the end point of a link is not yet discovered. If you discover that missing end point, the topology does not change unless you perform link discovery again.
- **Open View**—Returns you to the manager described in Topology Views on page 661.
- **Refresh**—Update the display.
- **Reorder**—Update the display, calculating the new order based on any changes you have made to the configuration in *Properties*.
- **Properties**—Alter the properties of this view. See Topology View Properties on page 666.
- **Save**—Save the view. By default its name is concatenates the creating login ID, date and time. You can change this in the screen described in Topology View Properties on page 666.
- **Print**—Print the display. See Printing Topology Views on page 684 for details.
- **Hide Overview & Legend**—This conceals the right-hand portion of the screen.
- **Help**—Opens online help for this topic.
- You can also configure the display with Context Menus.

Context Menus

If you right-click an icon, or the background, context menus appear. Refer to Action Button / Right-Click Menu on page 213 for information about more available menu items. Their exact content depends on the selection, but can include the following items:

- **Set Layout Root**—If your Properties have a selected layout that requires a root (like *Hierarchical*), then this item makes the selected object the root of that layout.
- **Remove**—Deletes the selected icon from the view. If you click *Remove* on a primary object (one not present because of filtering), it deletes the object from the Topology view. If you remove a secondary object (one present because of filtering), it's hidden.
- **Center**—Move the selected icon to the center of the view. This does not center icons on the edge of the view, but makes its best effort to move the selected icon toward the center. Best practice is to zoom first, then center.
- **Refresh**—Update the display.
- **Zoom In / Out / 100%**—These manipulate the magnification of the selected view. Saving does not preserve magnification, but it will preserve the placement of icons onscreen.
- **Expand / Collapse**—This displays the selected object's sub-components (assuming they have been discovered), or hides them once again if you have already expanded them.
- **Drill Down**—Goes from parent object to child object(s), opening another viewer.
- **Highlight / Unhighlight**—Paints the selected icon a different color, or toggles the highlight off.
- **Hide**—Conceal the selected object in this view.
- **Open**—Opens the appropriate editor for the selected object; for example, the Resource Editor.
- **Delete**—Lets you delete the selected object, after confirming that is what you want to do.
- **Map**—Display the single, selected item in its own, new view, alone.
- **Print Test Page**—Appears if the selected object is a printer.
- **Direct Access**—Opens a browser (or command line) session with the selected object. (See Direct Access Details on page 215 for more about cut thru sessions.)
- **Replace Drum / Fuser / Roller / Network Adaptor**—Opens the service log for the selected printer to log these replacements.
- **Update HTTP Password / SNMP Communities** —Lets you update the authentication for the selected printer.
- **Decommission Printer**—Stops polling and thresholding on the selected printer.
- **Initiate / Stop Printer Polling**—Starts or stops polling for reports and consumables estimates.
- **Restart Printer**—Restarts the selected printer.
- **New Group**—Lets you make a new group that would use OpenManage Network Manager's optional Group Operations.
- **Add to Group**—Lets you add the selected object to a group.

- **Resync**—Query the selected device to update its attributes.

- **Group Op**— Initiate a group operation on the selected equipment. This opens the Group Operations screen.

- **Discover**—Open the Resource Discovery Wizard.

In addition to the zoom menu items mentioned previously, the following items appear if you click a non-icon area on the view:

- **Refresh**—Update the display.

- **Reorder**—Update the display, calculating the new order based on any changes you have made to the configuration in *Properties*.

- **Add**—The same as the *Add* button described previously.

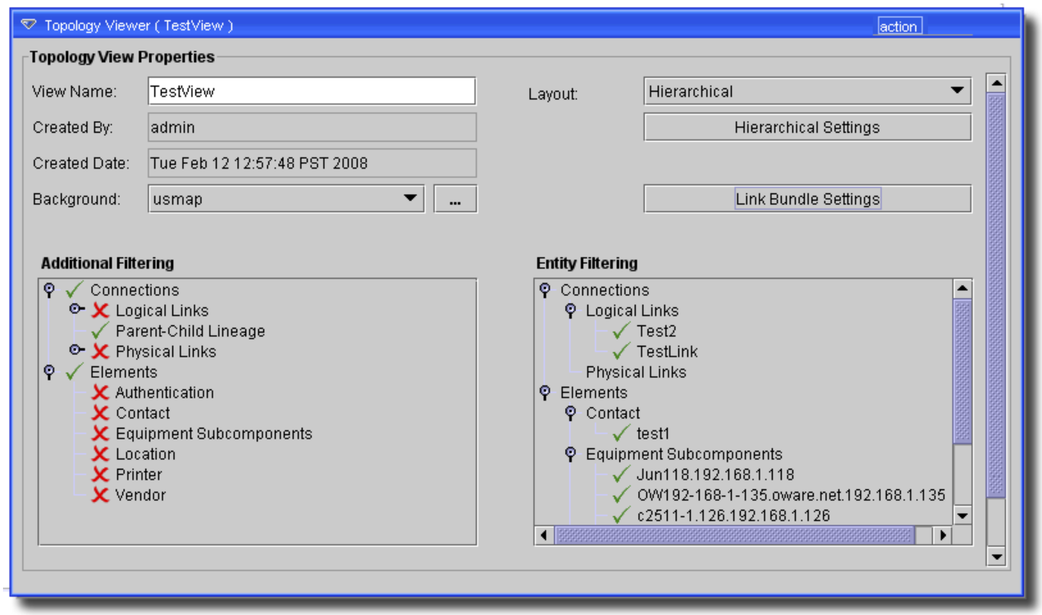
- **Properties**—The same as the *Properties* button described previously.

- **Print**—Print the display. See Printing Topology Views on page 684 for details.

Topology View Properties

This dialog lets you alter properties in your topology views.

Figure 21-4. Topology View Properties



Topology Viewer (TestView)

Topology View Properties

View Name: TestView

Created By: admin

Created Date: Tue Feb 12 12:57:48 PST 2008

Background: usmap

Layout: Hierarchical

Additional Filtering

- ✓ Connections
  - ✗ Logical Links
  - ✓ Parent-Child Lineage
  - ✗ Physical Links
- ✓ Elements
  - ✗ Authentication
  - ✗ Contact
  - ✗ Equipment Subcomponents
  - ✗ Location
  - ✗ Printer
  - ✗ Vendor

Entity Filtering

- Connections
  - Logical Links
    - ✓ Test2
    - ✓ TestLink
  - Physical Links
- Elements
  - Contact
    - ✓ test1
  - Equipment Subcomponents
    - ✓ Jun118.192.168.1.118
    - ✓ OW192-168-1-135.oware.net.192.168.1.135
    - ✓ c2511-1.126.192.168.1.126

You can access it with the *Properties* button in the topology view, or by right clicking an object in a view and selecting properties.

In this screen you can view or configure the following:

- **View Name**—A text field where you can enter, or alter an identifier for this view. If you change the name, you can select *File -> Save*, and the view name is altered in the Topology Views screen. You can also *File -> Save As*... a copy of the view once you have changed the name (but only after you change the name).
- **Created By**—A read-only reminder of the username who created the view.
- **Created Date**—The view's creation date (read-only).
- **Background**—Use this pick list to select a background for the view. The backgrounds must be `.png, .gif` or `jpg` files. Load a background by selecting the image file after you click the command button (...) to the right of the pick list. Once you load the background image this way, it appears in the pick list. Using these backgrounds, you can display your equipment topology on a map or as sub-modules of a rack.

  The default resolution for backgrounds is 1600 X 1200 pixels (width to height). You can change the default width and height globally by overriding two properties:

  ```
  com.dorado.redcell.topology.view.width=[pixels]
  ```

  and

  ```
  com.dorado.redcell.topology.view.height=[pixels]
  ```

  The application maintains the original image's aspect ratio between width and height to avoid stretching images, widening or lengthening the image until it reaches the smallest dimension, regardless of what you enter in the properties.

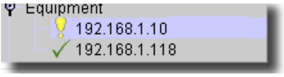
  Any background you select stretches to fill the screen's width when you import the image. If you want a background that is a tall, slender rectangle, like a rack on which you can place equipment, you may want to add white space to its right and left so that it appears without filling the screen.

NOTE:

Best practice is to override property files in `owareapps\installprops\lib.` Create a text file there with the `.properties` extension, and enter the above properties. The advantage of overriding properties like this is that installations of updates or patches do not overwrite your property tunings. In any case, you must restart application server before the application recognizes the changes.

- **Additional Filtering**—This tree displays possibilities for global topology filtering. Click the turners to expand the tree. Elements next to a green check appear in the display; elements with a red "X" do not. Click the element to toggle between check and X.
- **Entity Filtering**—This panel lets you configure the appearance of topology connections or equipment by specific entity (rather than global type). It also lets you configure the appearance of special indicators. Click the turners to expand the tree. Elements next to a green check appear in the display; elements with a red "X" do not. Click the element to toggle between check, X or the yellow exclamation point. This third category highlights the selected icon, surrounding it with a colored rectangle.

Figure 21-5. Topology Highlight Filtering



Equipment
192.168.1.10
192.168.1.118

- **Layout**—The pick list to the right of this label lets you select from several layout possibilities. You can further configure these layouts by selecting one, then clicking the *<Layout Type> Settings* button. When you select *Settings*, you can *Apply* your settings, or *Reorder* (recalculated the layout using available data) the display with the buttons at the bottom of this screen. *Close* abandons your edits. See on page 669 for details of the available *Settings*.

- **Link Bundle Settings**—These settings arrange overlapped links (links that connect the same two handles) in a bundle-like representation. You can configure the spacing between two links (inter link offset), to change between displaying all the links or only one thick segment (see setShrinked method), Clicking this button opens a dialog with the following settings:

Propagate–When selected, changes to any individual entity recalculates any other connected entities.

Shrinked–When shrinked, the link bundle appears as a single thick link.

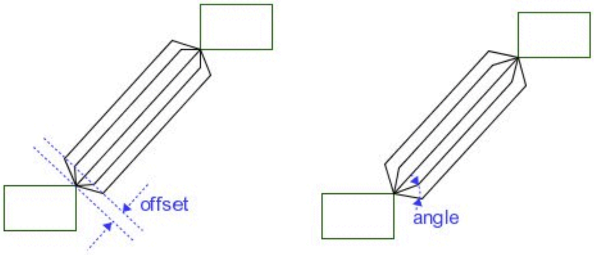
Autorun–Enables configured bundling to automatically recompute each time one of the two connected objects is moved or resized.

Start on border–When enabled, links start and/or end at the border of the objects

Reduce overlapping–Activates an algorithm to reduce link overlaps.

Use the radio buttons to select from the following alternatives. The *Spacing*, *Offset* and *Angle* fields become active, depending on your selection.

Figure 21-6. Link Bundle Offset / Angle Spacing



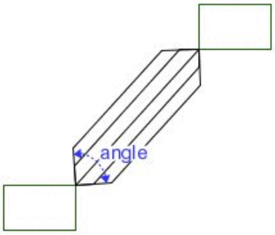
This sets the method to compute the link extremities. Depending of the method used, you can specify also the size of the links extremities or their angles (spacing or amplitude).

Offset method–Activates the *Spacing* and *Offset* fields.

Angle spacing method–Activates the *Spacing* and *Angle* fields.

Angle Amplitude method—Activates the *Spacing* and *Angle* fields.

Figure 21-7. Link Bundle Angle Amplitude



NOTE:

Each link keeps its own graphic attributes (color, line style, and so on).

After configuring link bundles, you can click buttons to *Apply* your settings, or *Reorder* (recalculated the layout using available data) the display. *Close* abandons your edits.

-

Layout

After configuring layout settings, you can *Apply* your settings, or *Reorder* (recalculated the layout using available data) the display. *Close* abandons your edits. Possible layouts and their accompanying *Settings* include several layouts that may help you manage the display more complex arrangements. You can experiment with these and see what works best.

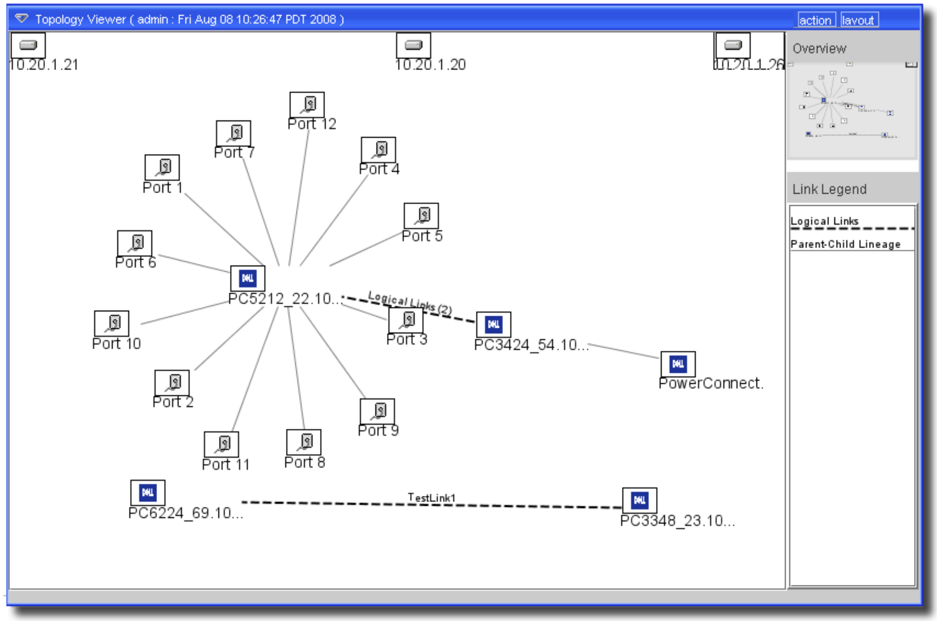
NOTE:

Automated layouts may give you the beginning of a clear topology view, but there is a limit to what selecting a Tree layout can do, for just one example. The layouts that display their contents with the most clarity typically include some manual icon moving.

Spring

Spring Layout connects entities by their centers, as if they were connected by springs. The arrangement of the entities adjusts automatically until it reaches equilibrium.

Figure 21-8. Topology View—Spring Layout



The *Spring Settings* for spring layout include the following:

- **Propagate**—When selected, changes to any individual entity cause the positions of connected entities to be recalculated.

- **Specify layout size**—In pixels. You must check this before specifying the number.

- **Horizontal / vertical alignment**—Enter the number of pixels between objects (applied if *Automatic horizontal spacing* is unchecked).

- **Use object's sizes**—Uses the size of each object to determine its weighting and relative placement, rather than a point.

- **Fix selected objects**—Specifies that the selected objects remain in their current position.

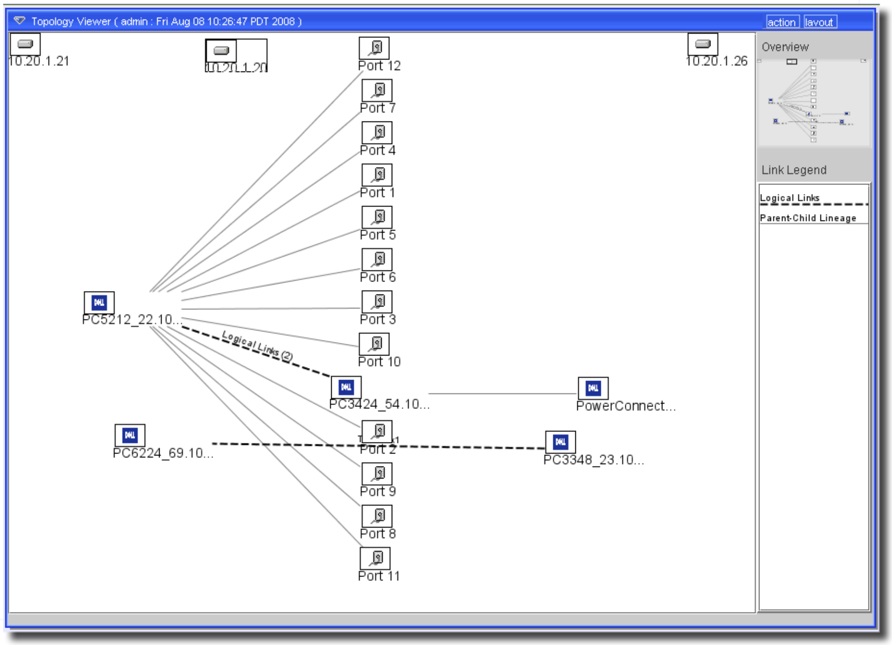
- **Automatic edge length**—This calculates the length of the links and the relative spacing of the entities with respect to the containing window. Click to select, or provide the *Edge length constant* (the length of links and the relative spacing of entities), *Repaint period* (seconds between screen refreshes), and *Epsilon* (when the iterative process for the spring embedder should stop. The greater this constant, the faster the layout, but the more distant the final position from the optimal layout.).

- **Single components settings**—Automate these by checking *Automatic horizontal spacing*, or manually enter Horizontal or Vertical Spacing (in pixels).

Tree

Tree layout displays objects as a hierarchy, beginning with the root node. The tree can be oriented vertically or horizontally.

Figure 21-9. Topology View–Tree Layout



Tree layout and the balloon tree layout require a root node. To select a root, tight click on a node, and select the first option: *Set Layout Root*. A tree represent a hierarchy of objects. It takes into account all links between the managed objects which define the tree structure. Here are the available *Tree Settings* for this layout:

- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.
- **Root**–Displays the read-only root node.
- **Grab root**... — Click this button to display the Grab root dialog, which lets you specify the root entity with your next selection within the view.
- **Tree Orientation**–Select whether you want the root on the *Left*, *Top*, *Right* or *Bottom* with the radio buttons. A tree orientation of Top, for example, places the root node of the tree at the top, with each successive level appearing toward the bottom.
- **Layout Order**–Specifies whether to place the entities according to their order in the database listing (*List Order*) or according to their current position (*Closest position*) relative to the root node.

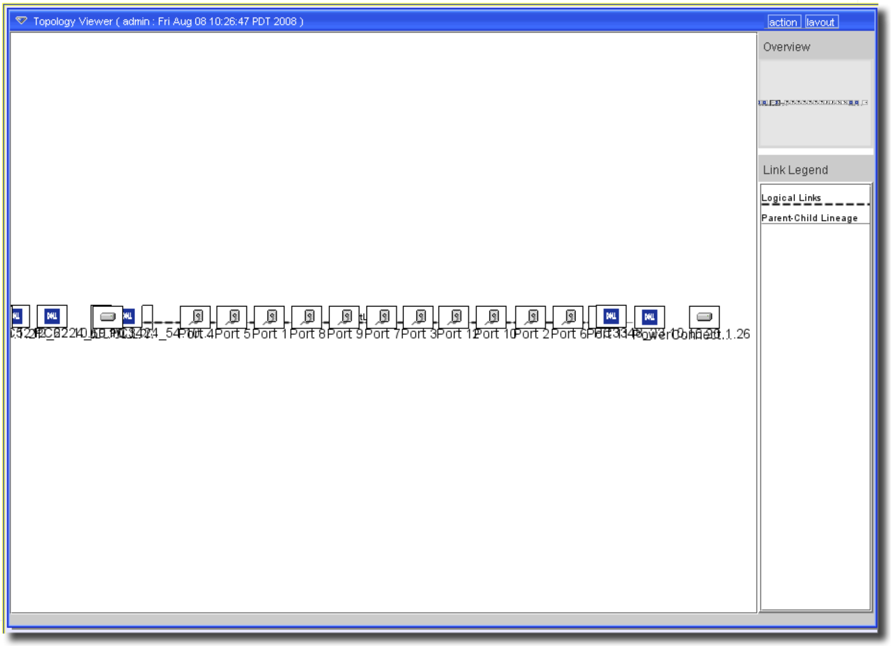
- **Layout method**–Check whether you want the layout to include the following methods: *Compact* (put objects as close together as possible), *Fixed Spacing* (a specified distance from each other) and/or *Use objects' sizes* (considers the size of the object, not just a point, to determine its placement with respect to the other objects).

When you elect *Fixed Spacing* you can specify *Horizontal / Vertical fixed spacing*—the distance between objects—in pixels.

Align

Select this option to align objects along an axis.

Figure 21-10. Topology View–Align Layout



Here are the available *Align Settings* for this layout:

- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.
- **Layout Order**–Select whether you want objects laid out in *List Order* or *Closest position.*
- **Orientation**–Select whether you want the axis*Vertical* or *Horizontal* with the radio buttons.
- **Alignment axis action** –Select whether you want objects on the axis to *Space evenly, Use objects' sizes* (rather than their central points), or whether you ant them to align in the *Center, Top/ Left, Bottom Right* or *None* with the radio buttons.

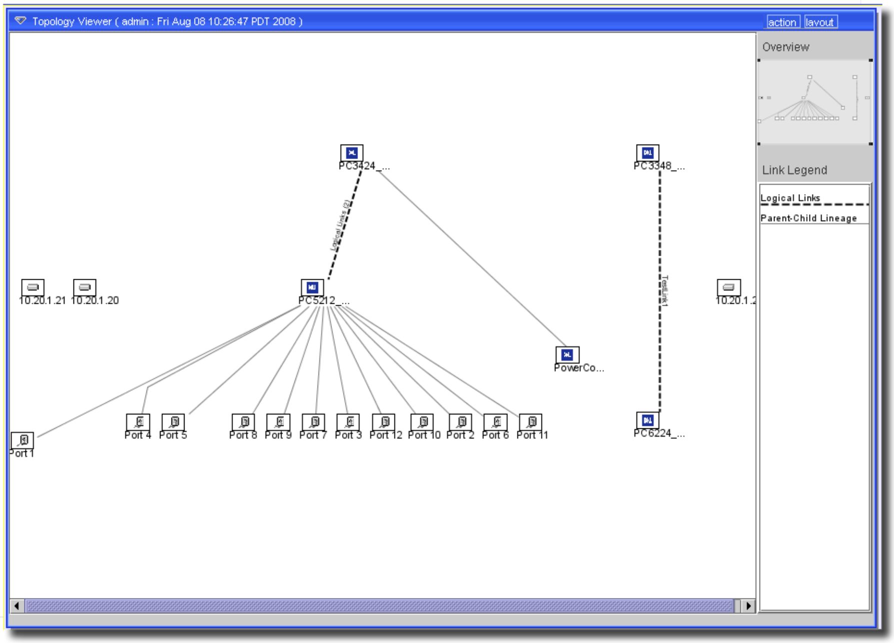
In some align layouts you can specify the pixels between objects with the *Fixed spacing* field.

- **Normal axis action**–Select whether you want the axis to *Center*, *Top/Left*, *Bottom Right* or *None* with the radio buttons.

Hierarchical

This layout represents a hierarchy of objects, taking all links into account.

Figure 21-11. Topology View–Hierarchical Layout



The links' orientation determines the hierarchical relationship between components. This layout tries to find a root component (a component without any incoming link). If it cannot find a root, or if there are several possible roots, you should manually set a root component or by selecting it on the graph.

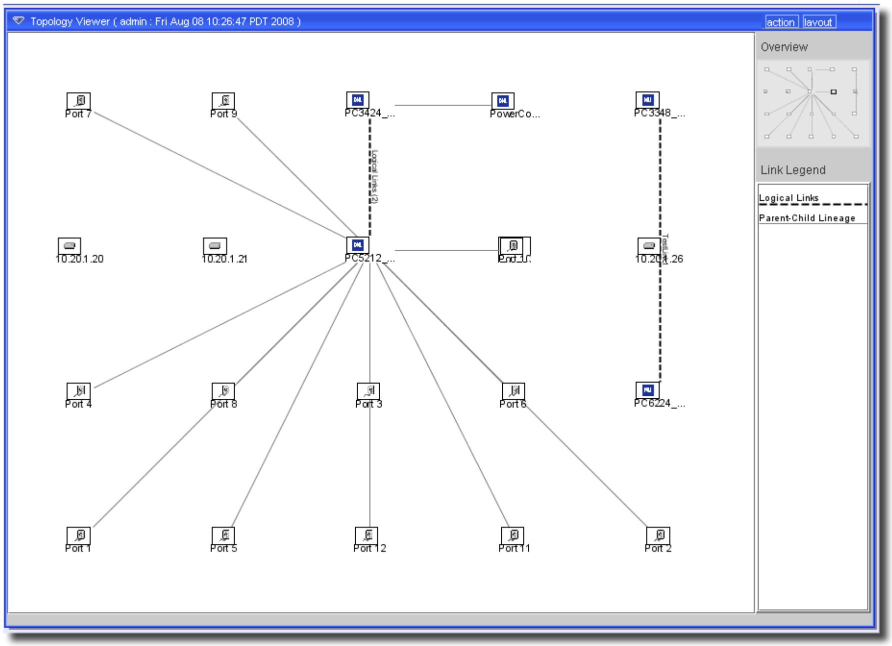
It supports the following *Hierarchical Settings*:

- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.
- **Layout direction**–Select whether you want the hierarchy *Top to bottom*, *Bottom to top*, *Left to right* or *Right to left* with the radio buttons.
- **Layout Alignment** –Select whether you want *Upper left corner* or *Center.*
- **Root Selection**–Check if you want the *Selected component as root*.
- In some hierarchies you can specify *Horizontal / Vertical spacing*.
- **Straighten paths**–Check if you want to straighten the paths between displayed objects.

Table

Select this for a table layout, arranging objects on a grid.

Figure 21-12. Topology View–Table Layout



It offers the following *Table Settings*:

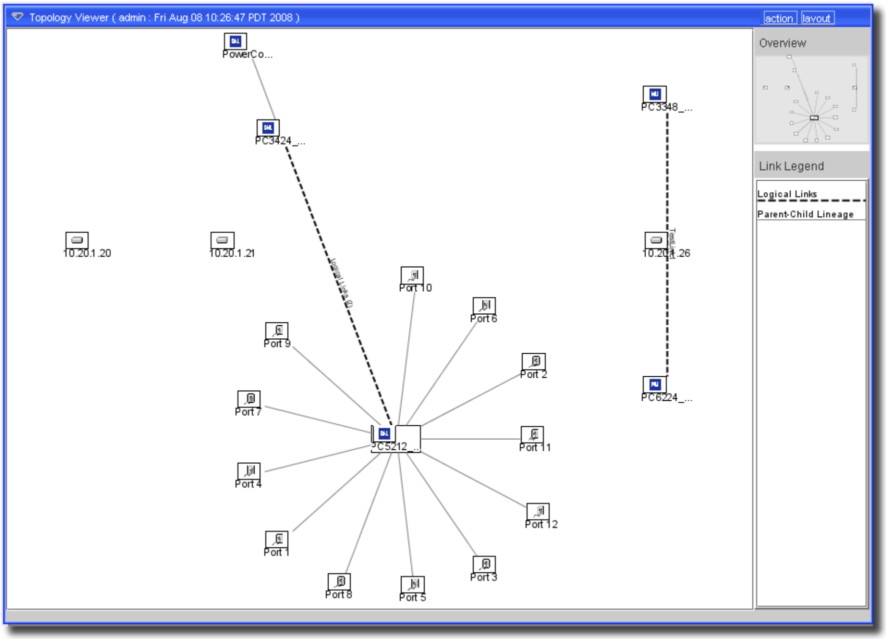
- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.
- **Layout Order**–Select whether you want objects laid out in *List Order, Closest position* or *Closest position, selected first* (the selected object would be closest).
- **Layout method**–Select one the following method: *Fill horizontally, Fill vertically, Fill Best Direction*, *Fill Both*, or *Fixed spacing*.

If you select *Fixed Spacing*, you can specify the *Horizontal / Vertical fixed spacing* and *Fill Ratio.*

Balloon Tree

Balloon trees accounts for all links between the managed objects which define a tree structure. You must define a root node. Its position determines the orientation of the tree. To select a root, tight click on a node, and select the first option: *Set Layout Root*. Children of a given node spread over a specified angle range, with radiuses computed so that their own line of descent does not overlap with the line of descent of their siblings.

Figure 21-13.   Topology View–Balloon Tree Layout



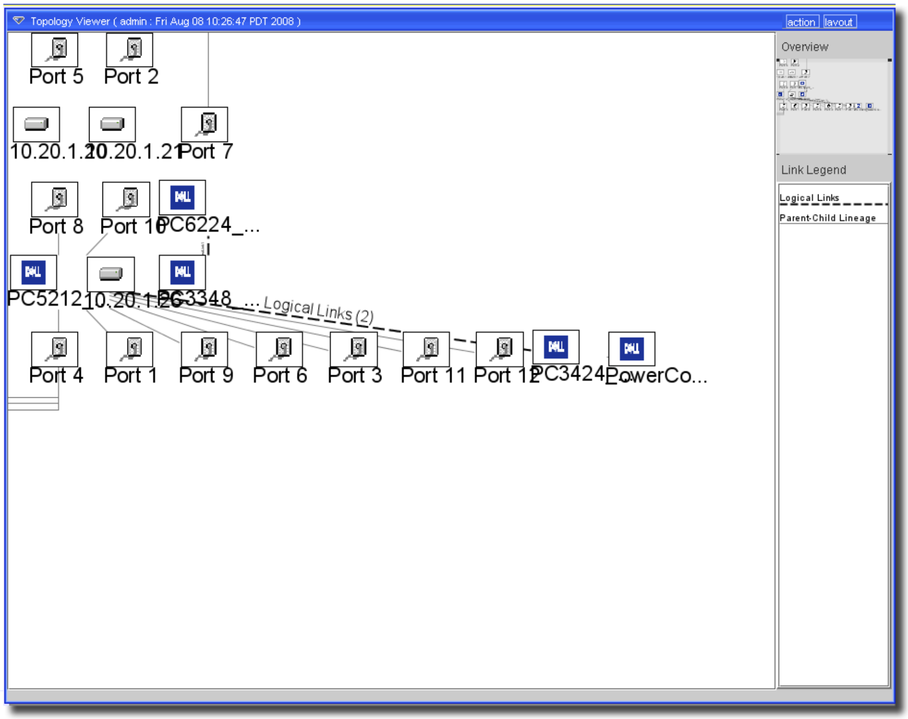
You can specify several angle extents (extent for children of the root, extent for leaves (children without children) and general extent for all other nodes), as well as sharing these extents between children (regularly or according to the weight of every children's line of descent) Here are the available *Balloon Tree Settings* in this layout:

- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.
- **Root**–Displays the read-only root node. Click *Grab root* to make the next icon you select the root.
- **Method**–Select whether you want the Angle spacing *Regular,* or *Proportional*, and whether you want Order *List*, *Angle*, or *Surface* with the pick lists.
- **Angle range**–Specify the range of angles from *Root*, *Leaves*, and *Others* for sub-nodes.
- **Initial angle**–Specify the layout's initial angle for subnodes of the root node.

Tier

This view displays tiers based on an algorithm that organizes interconnected nodes into a hierarchical layout of vertices, minimizing the number of link crossings, creating straight short and long lines for the links between nodes, making connected nodes appear together, and finally, balancing the overall layout of edges.

Figure 21-14. Topology View–Tier Layout



It has the following *Tier Settings*:

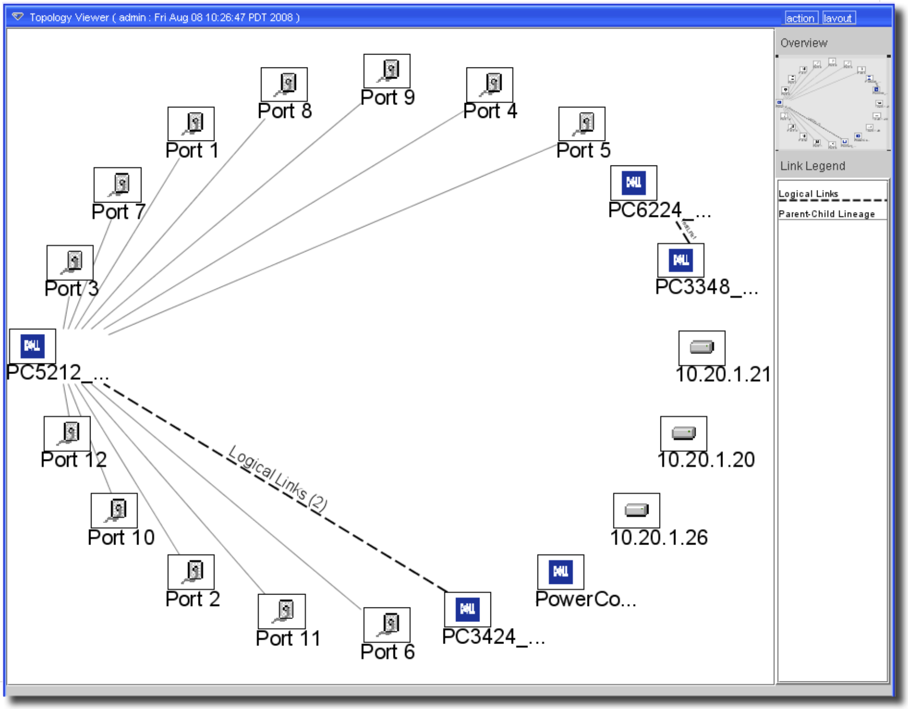
- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.
- **Use object's sizes**–When checked, this arranged tiers based on the entire size of the selected objects, not just the points where they appear.
- **Beautify Spacing**–When checked, this automatically "beautifies" tiered displays—nodes of the layout are evenly distributed over the display's width or height.
- **Fit to bounds**–When checked, this arranged tiers within the bounds of the available screen real estate.
- **Orientation**–Select from *Horizontal*, or *Vertical*.
- **Inter-tier gap, Inter-node gap**–Set the number of pixels for these gaps.
- **Intra-link / Skip-link spacing**–Set the number of pixels for these spaces.
- **Iteration count**–Set the number of iterations for tiered displays.

- **Priority 1/2/3**– To minimize the number of crossings, the view calculates how to display nodes according to their priority. Set priorities with the pick list (*None*, *Intra*—Links between adjacent nodes, *Adjacent*—Links between nodes of adjacent tiers, or *Skip*—Links between nodes in non adajacent tiers). Priority 1 is highest.
- **Weights**–Set the number weighting the selected priorities (the previous item).

Circular

This lays out the relevant objects in a circle. You can specify the number of circles, the spacing between this circles (in percentage of the specified radius) and specify a center node when displayed as a star. If not specified, the node which has most links connected acts as the center.

Figure 21-15. Topology View–Circular Layout



This layout has the following *Circular Settings:*

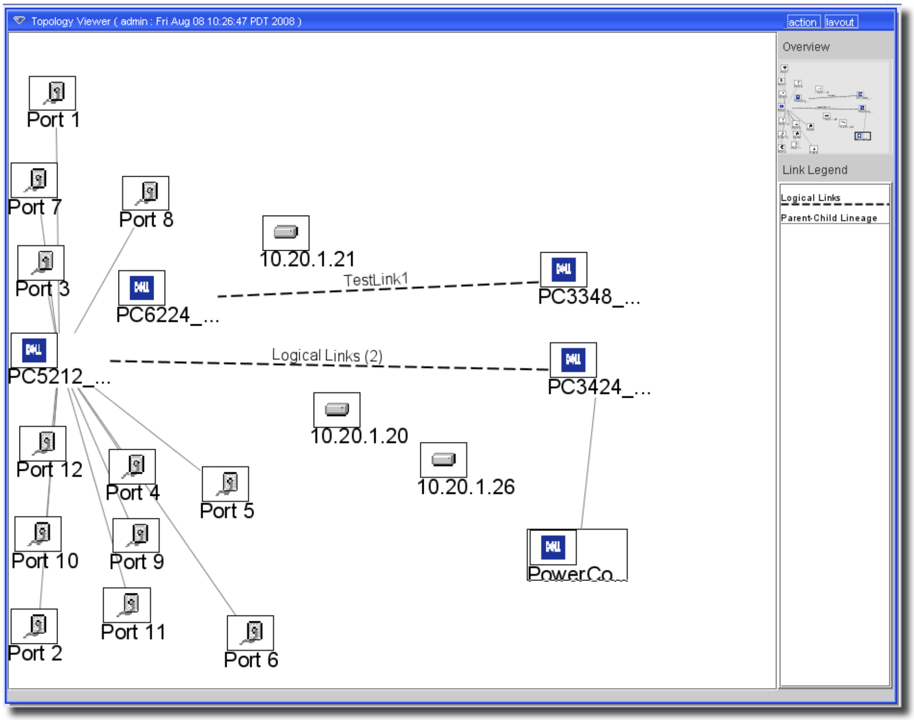
- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.
- **Node Order**–Select from the pick list (*List*–as nodes are listed in the database—or *Optimal*–the nodes appear so the overall length of all links is a minimum).
- **Best fit**–When checked, this arranges the circle within the bounds of the available screen real estate.

- **Star display**–When checked, this arranges the circled items so their connections can form a star pattern.
- **Progressive**–When checked, this arranged the circle progressively. Eventually, the progressive option specifies that the algorithm can be run progressively to find a better solution.
- **Circles**–The number of circles to make. The *Circle Spacing* determines the pixels between multiple circles.

Declutter

This removes some clutter from an existing display, minimizing the screen real estate consumed by links. The declutter layout manager spreads objects so that they do not overlap. This handles non-zoomable objects. As you zoom out, non zoomable objects tend to appear on top of each other. Declutter calculates the overlaps and spreads the objects apart.

Figure 21-16. Topology View–Declutter Layout



It has the following *Declutter Settings*:

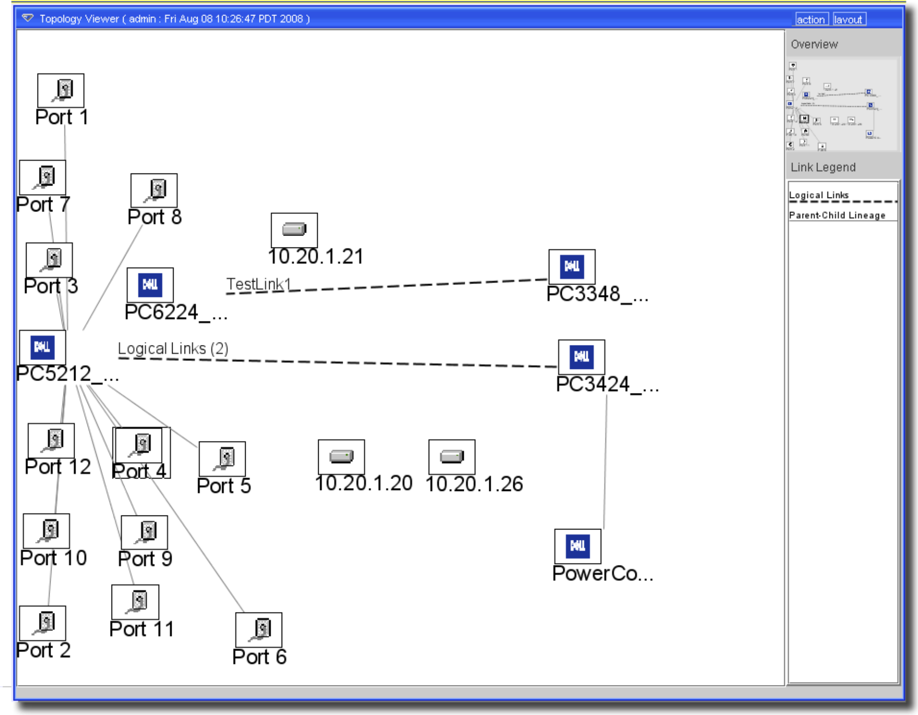
- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.
- **Object padding**–Enter the number of pixels with which to surround objects.

- **Arrow line thickness**–The pixel thickness of connecting lines.
- **Draw arrows**–When checked, objects moved away from their real position have an arrow drawn from their current center to their real position. Arrows are also updated correctly.
- **Non zoomable arrows**–When true, any arrows drawn look the same regardless of the zoom factor.

Label Optimizer

This optimizes the placement of link annotations. It tries to find the best location of the annotation on the link. Three positions are checked on each segment of the link and the best one is selected. This preserves other attributes, like the link's orientation.

Figure 21-17. Topology View–Label Optimizer



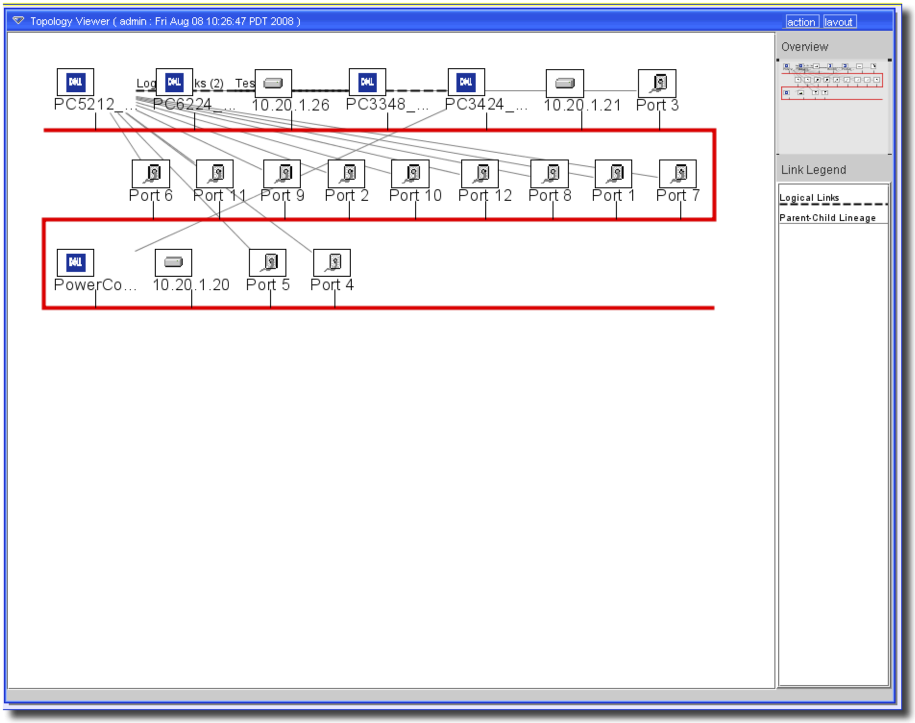
It has the following *Label Optimizer Settings*:

- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.
- **Minimum segment length**–Enter the minimum number of pixels for a segment.
- **Points per segment**–The minimum number of points (1/72 inch) in a segment.

Bus

Bus Layout is designed for bus topologies as they occur in networking and telecommunications. The layout represents the bus as a polyline and considers the size of nodes so that no overlapping occurs. Several ordering, alignment and flow direction options are available.

Figure 21-18. Topology View–Bus Layout



The bus connecting the icons is the red line in the display. You can move that red line by clicking and dragging it. This layout has the following *Bus Settings*:

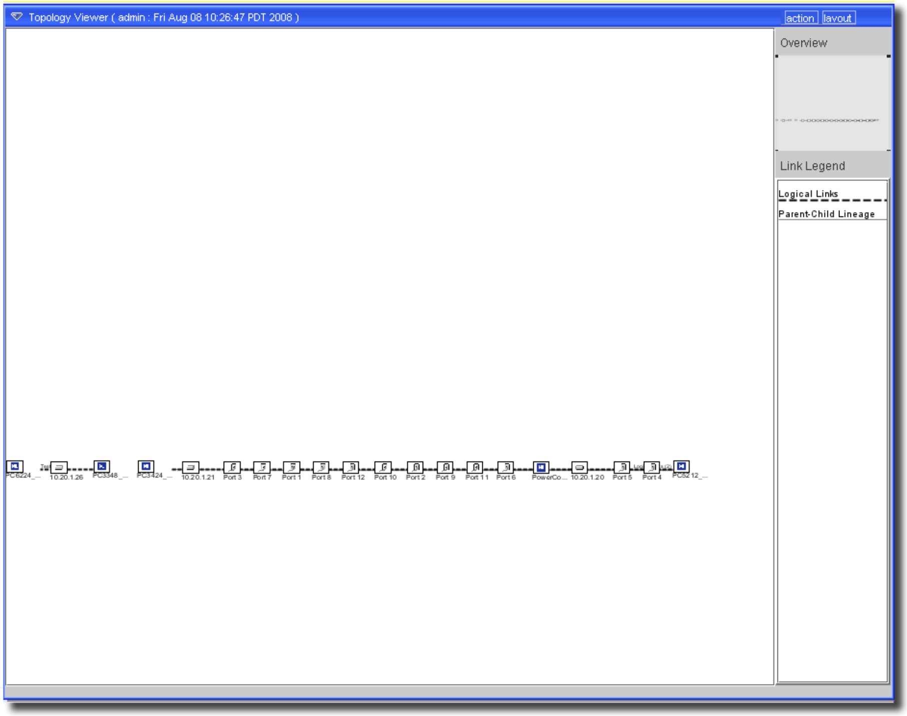
- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.
- **Layout**–Select from the pick boxes for bus *Orientation (Horizontal, Vertical)*, *Object Alignment (Center, Top/Left, Bottom/Right)*, also for the *Nodes Relative Position (Before/After Bus)*, and *Node Order (List Order, Closest, Ascending / Descending Width / Height / Surface)*.
- **Spacing**–Check *Use Objects Size* to have the display account for that. You can also set the pixel width *To/From Next/Previous Level*, *Between Nodes*, and on the *Bus Margin*.
- **Fit to Bounds Policy**–The items on this pick list configure how the bus fits within the bounds of the screen displayed: *Never, Always*, or *As Needed*.

Hierarchy

This layout option configures how to display child objects in relation to their parents. It follows a three-step process to do this:

1. Layering - This display partitions nodes into levels, then builds a hierarchy by reversing and splitting edges until each edge is directed downwards and connects two nodes on neighbored layers.
2. Cross-minimization step - The view reorders nodes on each layer to reduce the number of edge-crossings. It traverses layers top to bottom, bottom to top, or both, depending on the method you choose in *Hierarchy Settings*, until the total number of crossings no longer decreases.
3. Bend-reduction step - The view computes the final layout of the hierarchy. This interface assigns coordinates to nodes and bend points to edges.

Figure 21-19. Topology View–Hierarchy Layout



It supports the following *Hierarchy Settings* (some refer to the layout process above):

- **Propagation**–Check to propagate. When selected, changes to any individual entity automates recalculation of the positions of connected entities.

The rest of the settings include three tabs (*Layout*, *Node Rank* and *Node Order*):

Layout

- **Direction**–Select whether you want the hierarchy *Top to bottom*, *Bottom to top*, *Left to right* or *Right to left* with the pick list.
- **Fit to Bounds**–The items on this pick list configure how the hierarchy fits within the bounds of the screen displayed: *Never, Always,* or *As Needed*. Check *Keep Ratio* or *Resize Nodes* to activate these.
- **Straighten Links when**–Select from the pick list: *Never* (the default), *No Nodes* (creates straight links when no node obstacles exist), *No Links* (creates straight links when no link obstacles exist), *No Nodes nor Links* (creates straight links when no node or link obstacles exist), or *Always.*
- **Components Spacing**–The number of pixels between components.
- **Node Placement** –Select from the pick list: *Rubber* (assigns positions to nodes and links as if they are attached to a rubber band), or *Basic* (considers the node spacing and rank spacing used between node centers; calculates the center of the layout by counting the maximum rank count and placing each node relative to the center).
- **Simplify Links**–Check this to activate this algorithm.
- **Minimal Node /Edge / Rank Spacing**–See the steps described immediately below Hierarchy on page 681.
- **Variable Rank Spacing**–Check this to activate it.
- **Node Alignment**–Select from the pick list: *Center, Leading,* or *Trailing.*
- **Avoid Node Crossings**–Check this to activate an algorithm that avoids node crossings.
- **Traversal Method**–Select from the pick list: *Pendulum, Top to Bottom,* or *Bottom to Top.* See the steps described immediately below Hierarchy on page 681.
- **Allowed Retry**–Enter the number retries.
- **Max Iteration Count**–Enter the number iterations.

Node Rank

- **Ranking Policy**–Select from the pick list (*BFS, DFS, As is,* or *Random*)

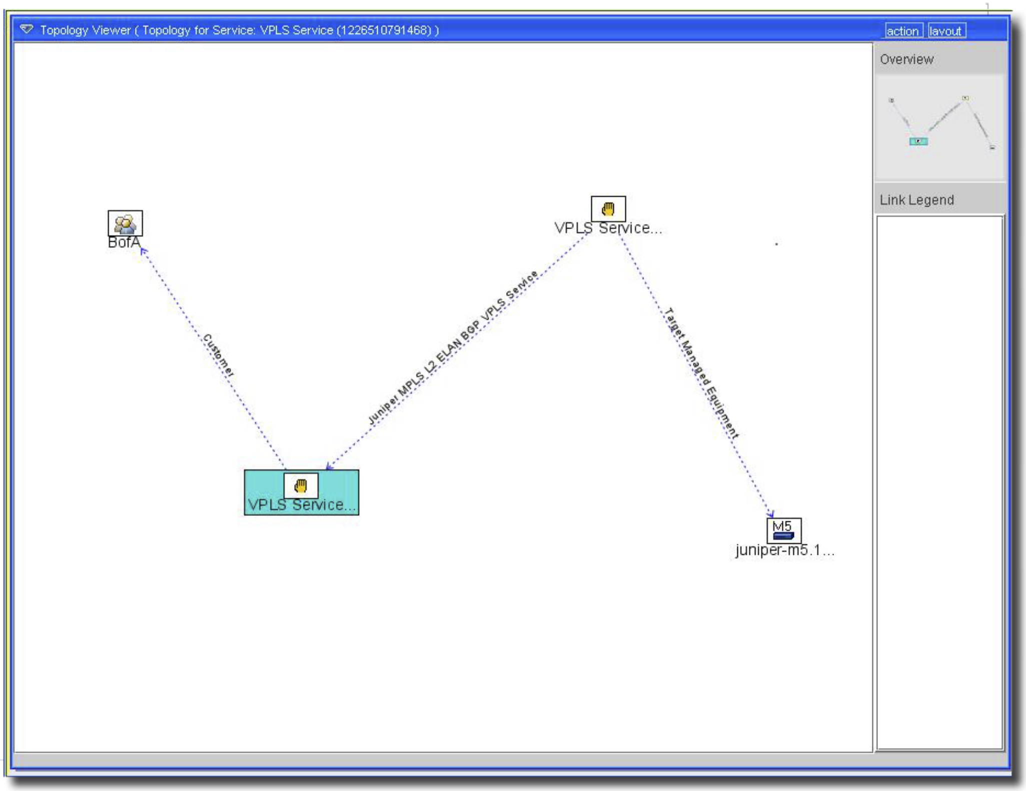
Node Order

- **Allowed Reducing Fails**–Enter a number for the permitted number of failures.
- **Allowed Node Shuffle Count**–Enter a number that specifies the number of times that the display algorithm can shuffle the nodes of each rank. Node shuffling can significantly improve the result, which allows the algorithm to find new solutions to crossing problems.
- **Traversal Method**–Select from the pick list: *Pendulum, Top to Bottom,* or *Bottom to Top.*
- **Weight Heuristic**– Select from the pick list: *Barycenter, Median* or *None. Barycenter* and *Median* are heuristics that reorder nodes in the graph and reduce crossings.

Service Topology

You can display supported (*Adaptive*) services in topology views. Essentially the items visible in the *Reference tree* detail panel can appear in a topology view. You can either add these to Topology Views with the *action -> Add Content* menu from the topology manager, or select the service within the *Services* manager and use *action -> Map* to create a topology view that contains the selected service.

Figure 21-20. Service Topology

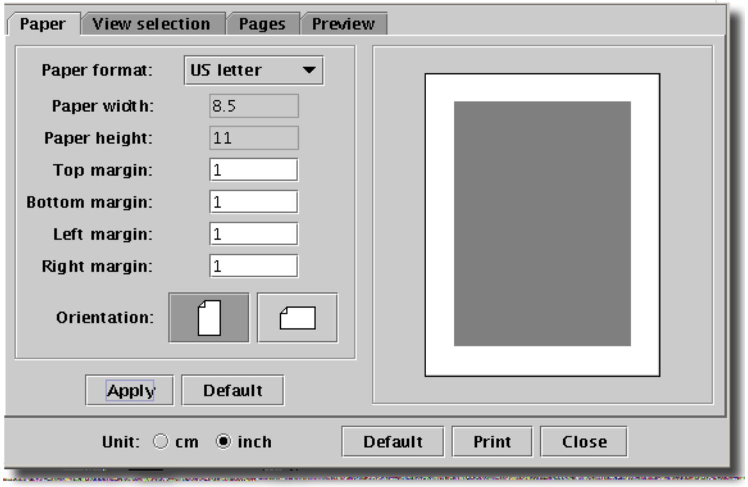


You can *Expand* a service or its sub-components to view its parts as you would in the *Reference tree* detail panel. The difference here is that the links appear labeled, and include directional arrows. Mapped services can coexist with other mapped devices and links. Mapped services do not, however, display alarm information.

Printing Topology Views

If you print a topology, a configuration dialog appears with four tabs.

Figure 21-21. Print Dialog–Paper Tab



Paper format: US letter

Paper width: 8.5

Paper height: 11

Top margin: 1

Bottom margin: 1

Left margin: 1

Right margin: 1

Orientation:

Unit: ○ cm ● inch

Paper

The *Paper* tab has the following fields:

- **Paper Format**—Select from the pick list (*A3*, *A4*, *A5*, *US Executive*, *US Letter*, *US Legal*, and *Custom*). The current default is *A4* (and measurements default to *cm*).
- **Paper width / height**—A pair of read-only fields, unless you select *Custom* in the pick list above them.

NOTE:

Set the units for this display at the bottom of the Print dialog.

Bottom / Top / Left / Right Margin—Set the margins in these fields.

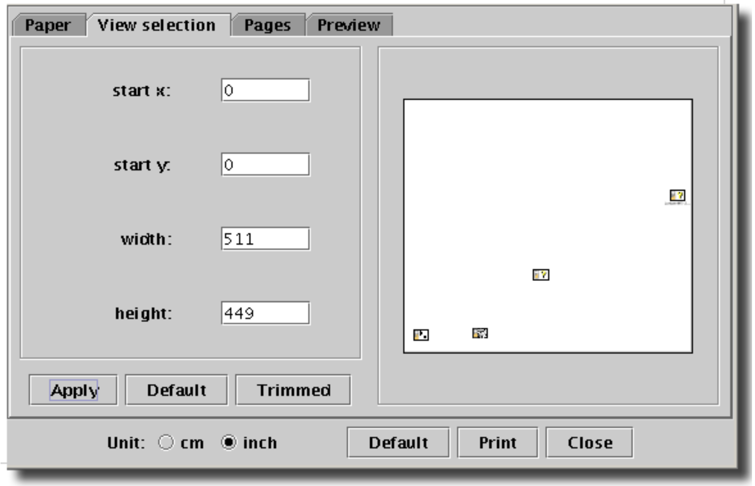
Orientation—Click on the icons to select

Click *Apply* to execute any edits on this print job, click *Default* on this tab to return to the tab's defaults. Click *Default* at the bottom of the screen to reset all tabs' defaults. Click *Print* to print the screen, or *Close* to abandon the print job and close this screen.

View selection

This screen previews the print job on the right, and lets you select what portion of the screen you want to print.

Figure 21-22. Topology Print–View Selection



start x: 0

start y: 0

width: 511

height: 449

Unit: ○ cm ● inch

You can configure the printed screen with the following fields:

- **start x / y** —Number of pixels to move the printed area (horizontal / vertical). Minus numbers move to the left/down, positive numbers move to the right/up.

- **start y**—The vertical pixel to start printing (from zero at the bottom).

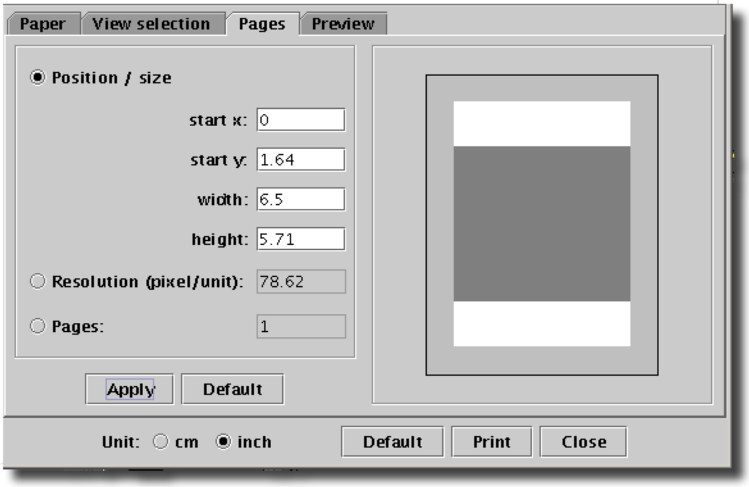
- **width / height**—Measured in pixels.

Click *Apply* to execute any edits on this print job, click *Default* on this tab to return to the tab’s defaults. Click *Trimmed* to crop the printed area so it does not display white space in the preview the right. Click *Default* at the bottom of the screen to reset all tabs’ defaults. Click *Print* to print the screen, or *Close* to abandon the print job and close this screen.

Pages

You can select the way your view appears on paper (preview on the right) three different ways.

Figure 21-23. Topology Print–Pages



● Position / size

start x: 0

start y: 1.64

width: 6.5

height: 5.71

○ Resolution (pixel/unit): 78.62

○ Pages: 1

Unit: ○ cm ● inch

Select the way with the radio buttons.

- **Position / Size**—Enter the *start x/y*, *width / height* in the appropriate fields and the preview rearranges the appearance (resolution, pages) to match.
- **Resolution (pixel/unit)**—Select a resolution, and the preview will display how Position/size and pages change.
- **Pages**—Select the number of pages to cover with your print job. The other elements of this display change too if you elect to tile your print job over several pages.

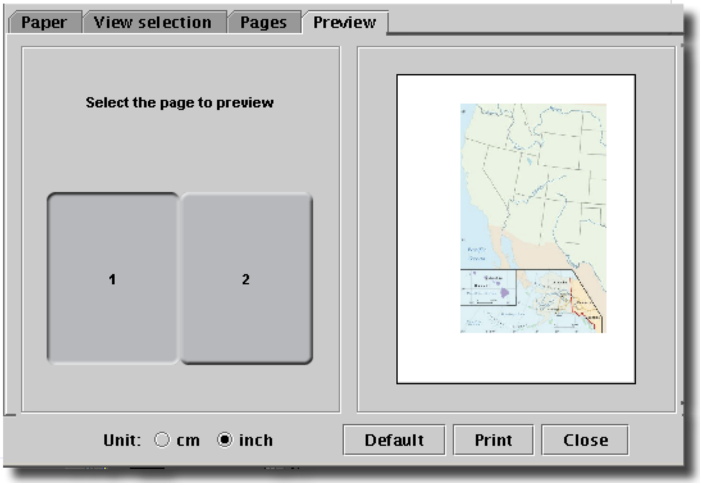
NOTE:

If you make the number of pages very large—for example, 100,000—generating the print job or preview will adversely impact performance.

Preview

If you want to preview multiple pages, you can see them by clicking on the page icons to the left of the preview panel.

Figure 21-24. Topology Print–Preview

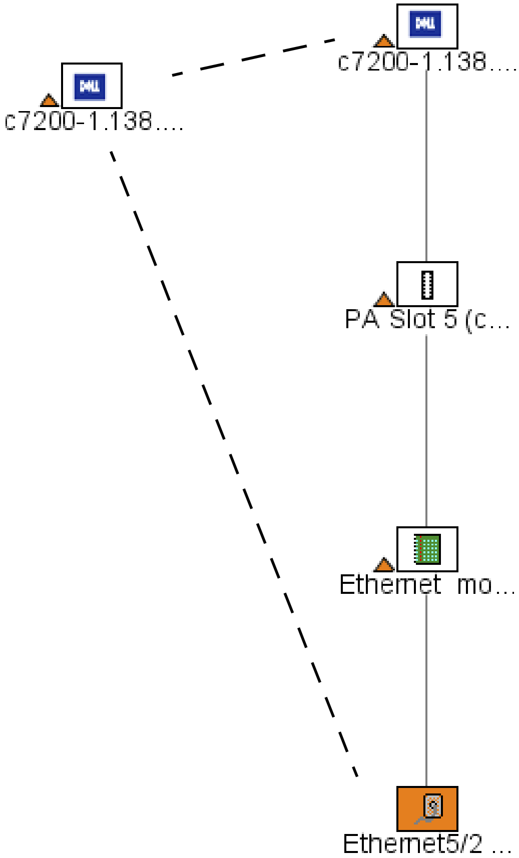


Click *Default* to return all tabs to their defaults, *Print* to execute the print job you have configured, or *Close* to abandon the print job and close this window.

Alarms in Topology

If you have Event Management installed, Topology views display the color of the highest severity alarm on a device in the color of its icon. To distinguish between alarms on equipment and sub-components of that equipment, OpenManage Network Manager displays child alarms (alarms on subcomponents) in a small triangle to the left of the device's icon in topology.

Figure 21-25. Child Alarms, Contracted and Expanded View



If you expand the view of a device with such a triangle next to it, the subcomponent from which the alarm originated appears with its icon colored in that alarm state's default color. If no subcomponent alarm exists, no triangle appears next to the device's icon.

Resync Alarms

If you have the Event Services option installed, you can monitor alarms within your topological display. When you open a topology window, you can see the current alarm state of the displayed objects. The application also resynchronizes the displayed objects from time to time, but doing so can slow application performance.

To manually update the represented topology without the performance penalty, click Resync Alarms button on Resources manager (see Chapter 13, Resources) where you can manually update the alarm state of a selected object.

Figure 21-26. Resync Alarms Button

When you select equipment in Resources manager clicking this button resynchronizes the topology display with the equipment's alarm state in the system.

NOTE:

You must select the parent equipment; you cannot resync a port or interface.

Also: This does *not* resync alarms or communicate with the device or any northbound system, and is completely different from device resync.

This resyncs alarm state for topology. For example, if a device receives a critical open alarm, the topology view for the equipment should go red. If for some reason if the topology view does not reflect the alarm state properly, you can select the equipment and click alarm resync which will force the application to resync between alarms and topology.

22

Group Operations

Group Operations Overview

The application's (optional) Group operations let you act on groups of devices—even heterogeneous groups. You must make the groups before you can operate on them. See Groups Manager on page 635 for details about how to do this. You can make groups of interfaces too, not just entire devices.

NOTE:

This feature is an option that can be standard in some versions. You must also have drivers installed that support group operations before you can use them. Consult the section of this guide that discusses the product or addon for more information about specific Group Operations.

Open the Group Operations Manager from the *Group Op* button in *Resources manager*, from *File -> Open -> Inventory -> Group Operations*, or from its node in the Navigation Pane. A typical manager appears. See Group Operations Manager on page 699 for details.

Group operations are asynchronous. You can monitor them as they occur, and have occurred, in an Audit History screen.

NOTE:

Group operations are sometimes limited, in comparison to the screens available in Resource Editor.

NOTE:

Use Group Ops to schedule operations on more than one device at the same time instead of scheduling multiple individual operations at the same time.

Group Operations Wizard

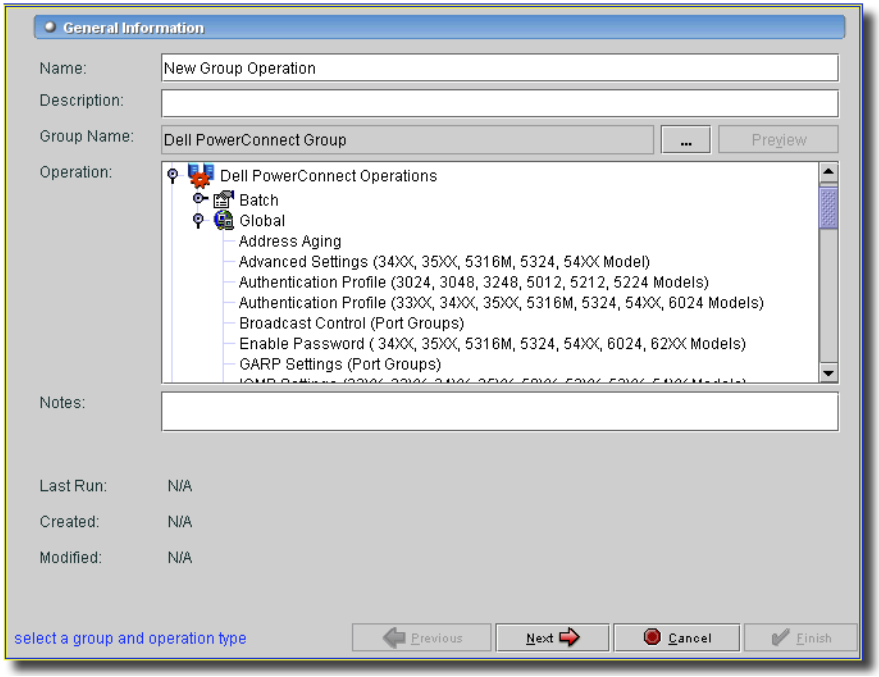
Clicking *New* opens the *Group Operations Wizard*. This walks you through creating a group operation with the following steps:

- Group and Type
- Action Screen
- Save and Execute Options
- Status

Group and Type

The first screen in this Wizard lets you select a group and type of operation.

Figure 22-1. Select a Group and Operation Type



General Information

Name: New Group Operation

Description:

Group Name: Dell PowerConnect Group

Operation:

- Dell PowerConnect Operations
  - Batch
  - Global
    - Address Aging
    - Advanced Settings (34XX, 35XX, 5316M, 5324, 54XX Model)
    - Authentication Profile (3024, 3048, 3248, 5012, 5212, 5224 Models)
    - Authentication Profile (33XX, 34XX, 35XX, 5316M, 5324, 54XX, 6024 Models)
    - Broadcast Control (Port Groups)
    - Enable Password (34XX, 35XX, 5316M, 5324, 54XX, 6024, 62XX Models)
    - GARP Settings (Port Groups)

Notes:

Last Run: N/A

Created: N/A

Modified: N/A

select a group and operation type

The exact contents of this panel depend on the applications and device drivers you have installed. It has the following information:

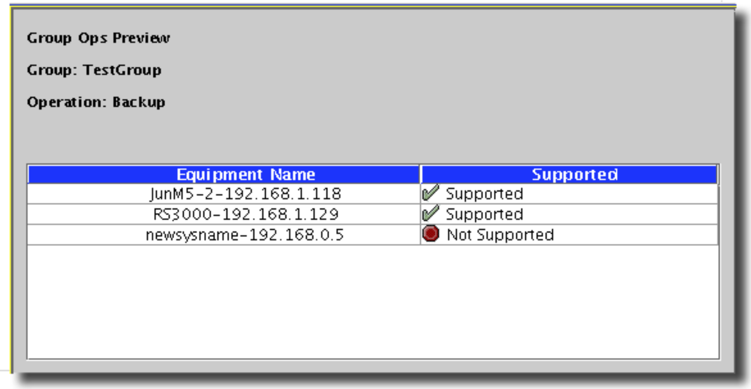
- **Name**—The unique identifier for the group operation you are creating.
- **Description**—A text description of the group operation.
- **Group**—The (previously created) equipment group on which this operation acts. Use the command button (...) to change the selection.
- **Operation**—Consists of nodes for drivers and applications, in addition to the standard *System Operations* node. Under these nodes, *Global* operations essentially do the same thing to the entire group. *Batch* operations do group-, device- or instance-specific actions.

  To set the SNMP community string to *public*, on all devices use a Global operation. This performs the same action, using the same values. To change the SNMP community string on all devices to box## then do a batch operation and change the value one-by-one. This is the same action, but with different values.

  System Information actions work for any device that supports SNMP MIB 2 (and those that do not if you are only updating the database). Other devices require that a Device Driver be installed and support the given type.

- **Notes**—A text field where you can enter notes about the group operation you are creating.
- **Last Run**—(Read only) The time this operation last ran.
- **Created**—(Read only) The time you created this operation.
- **Modified**—(Read only) The time you last modified this operation.
- **Preview**—Click this button so the application can test the group operation against the equipment in the selected group. The subsequent screen tells whether the devices support the action.

Figure 22-2. Group Operations Preview Screen



Group Ops Preview

Group: TestGroup

Operation: Backup

Equipment Name	Supported
JunM5-2-192.168.1.118	✓ Supported
RS3000-192.168.1.129	✓ Supported
newsysname-192.168.0.5	● Not Supported

You can proceed with the group operation, or abandon it, as appropriate, based on this screen.

NOTE:

Some ACLI (Adaptive CLI) Group Operations also request parameters. Supply them in the screen that appears after you select the group operation. The ACLI will run only on target devices within the selected group that support it. To use the full capabilities of ACLI, you must have Perl installed.

Action Screen

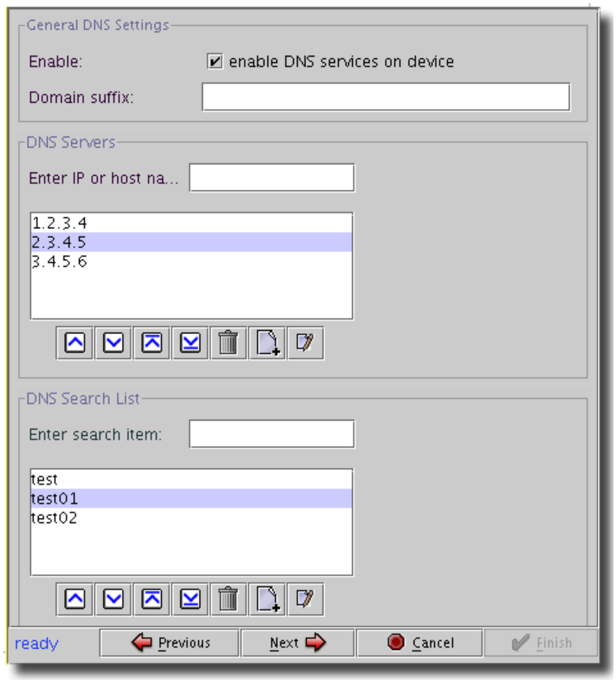
The next screen (click *Next* to get there) lets you specify the parameters for the action you selected in the first screen. Here are some action screens that can appear:

- DNS Servers
- Gateway
- Network Services
- Port Speed & Duplex
- System Information
- Time Servers
- Task
- Batch Operations

DNS Servers

You can set the DNS Server attributes in this screen.

Figure 22-3. Group Operations DNS Servers



General DNS Settings

Enable: ☑ enable DNS services on device

Domain suffix:

DNS Servers

Enter IP or host na...

1.2.3.4
2.3.4.5
3.4.5.6

DNS Search List

Enter search item:

test
test01
test02

It has the following fields, checkboxes and tables (defined when not self-evident):

- **Enable**—A checkbox you must select before any fields are writable below it.

- **Domain Suffix**—DNS domain suffix.

Enter devices in this screen in fields above the lists of devices, then click the *Add New Item* icon to insert the text you type into these lists. You can manage the priority of items with the arrow buttons, and delete or edit selected items with the buttons for those functions once you select an item displayed in the table.

DNS Servers

- **Enter IP or Hostname**—Enter the DNS server hostname you want to add to the servers in the table here.

DNS Search List

- **Enter Search Item**—Enter the DNS server hostname you want search for (and that you want to appear in the table) here.

Gateway

Selecting this in the previous screen means you must type the (default) *Gateway IP Address* for the selected group in the subsequent screen.

Network Services

Selecting this in the previous screen means you can click to disable desired network services in the subsequent screen. Available network services are:

- HTTP
- Telnet
- SSH

Checks in the checkbox(es) for these enable them on the group of devices selected in the previous screen. They are enabled by default.

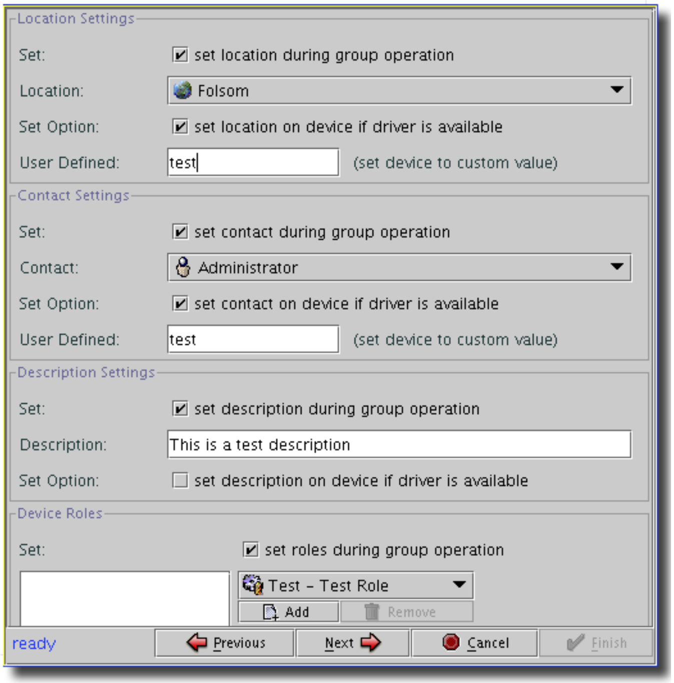
Port Speed & Duplex

Selecting this in the previous screen means you can reset the (default) *Port Speed* (automatically filled in) and select the type of *Duplex* for the selected devices in the subsequent screen. Select the type of duplexing from a pick list offering *full*, *half*, and *auto*.

System Information

Selecting this in the previous screen means you can type several system fields in the subsequent screen.

Figure 22-4. Group Operations: System Information



Location Settings

Set: ☑ set location during group operation

Location: Folsom

Set Option: ☑ set location on device if driver is available

User Defined: test (set device to custom value)

Contact Settings

Set: ☑ set contact during group operation

Contact: Administrator

Set Option: ☑ set contact on device if driver is available

User Defined: test (set device to custom value)

Description Settings

Set: ☑ set description during group operation

Description: This is a test description

Set Option: □ set description on device if driver is available

Device Roles

Set: ☑ set roles during group operation

Test - Test Role

ready

This screen has the following:

Location Settings

- **Set**—This checkbox enables setting a location during group operations.
- **Location**—Select from the available locations in the system with this pick list.
- **Set Option**—If a device driver is available, and the device supports it, you can enable setting the location on the device.
- **User-Defined**—Lets you type a custom location in the field. This updates the device with a different value than the database. If it is blank the device and database are updated with the same values.

Contact Settings

- **Set**—This checkbox enables setting a contact during group operations.
- **Contact**—Select from the available contacts in the system with this pick list.

- **Set Option**—If a device driver is available, and the device supports it, you can enable setting the contact on the device.
- **User-Defined**—Lets you type a custom contact in the field.

Description Settings

- **Set**—This checkbox enables setting a description during group operations.
- **Description**—Type a description to set.
- **Set Option**—If a device driver is available, and the device supports it, you can enable setting the description on the device.

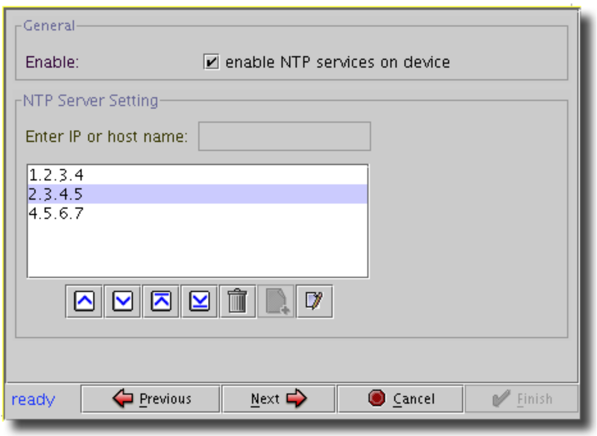
Task

This screen allows you to create a group operation to run a selected *Task* on the selected group of devices. Refer to online help for a description of how to configure these.

Time Servers

Assign time servers to the selected group.

Figure 22-5. Group Operations: Time Servers



General

Enable: ☑ enable NTP services on device

NTP Server Setting

Enter IP or host name:

1.2.3.4
2.3.4.5
4.5.6.7

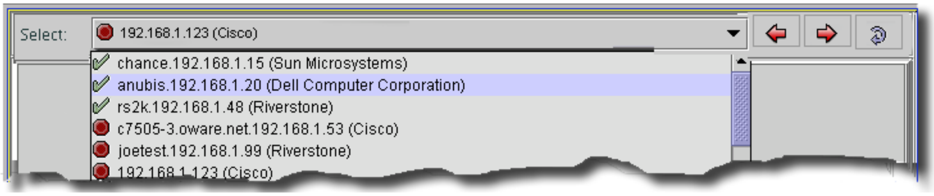
Click the checkbox to enable NTP services for the group.

Enter server names in the *Enter IP or host name* field, and use the *Add New Item* button to add the name to the list displayed. You can also delete and edit selected items on this list with the buttons below it. The arrow buttons manage the order of the list.

Batch Operations

Global operations essentially do the same thing to the entire group. *Batch* operations do group-, device- or instance-specific actions. Screens that appear in batch operations depend on the devices in the group, and what they support. You can select the device from the pick list that appears in this subsequent screen.

Figure 22-6. Group Operations: Batch Screen



Select: ● 192.168.1.123 (Cisco)

✓ chance.192.168.1.15 (Sun Microsystems)
✓ anubis.192.168.1.20 (Dell Computer Corporation)
✓ rs2k.192.168.1.48 (Riverstone)
● c7505-3.oware.net.192.168.1.53 (Cisco)
● joetest.192.168.1.99 (Riverstone)
● 192.168.1.123 (Cisco)

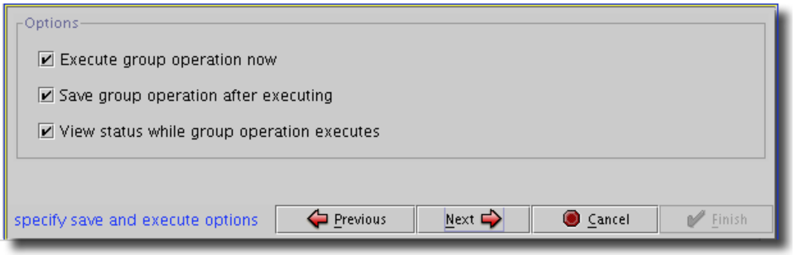
You can use the arrows to the right of the pick list to step through the list, and the circular arrow to refresh the batch data for the currently selected managed object. The icons next to each device change from red to green when you have completed the device's screen.

Typical batch operations include Port Configuration, BGP, IS-IS, OSPF, RIP. Select members in the group, and modify the subsequent screens that appear as appropriate for the configuration you want sent in the batch operation to the selected group.

Save and Execute Options

The next screen lets you select options for saving, executing, and viewing operations you have specified.

Figure 22-7. Group Operations: Save and Execute Options



Options

☑ Execute group operation now

☑ Save group operation after executing

☑ View status while group operation executes

specify save and execute options

By clicking the checkboxes, you enable the following:

- Execute Group Operation Now
- Save Group Operation after Executing
- View status while group operation executes.

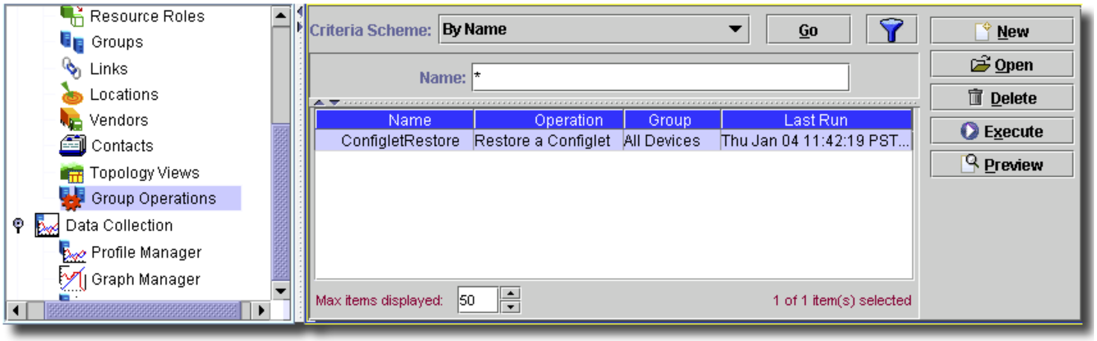
Status

The final screen that appears displays the status of the group operation (provided you elected to view that status).

Group Operations Manager

Once you have created a group operation, you can view and alter portions of it in the Group Operations Manager.

Figure 22-8. Group Operations Manager



Criteria Scheme: By Name

Name: *

Name	Operation	Group	Last Run
ConfigletRestore	Restore a Configlet	All Devices	Thu Jan 04 11:42:19 PST...

Max items displayed: 50

1 of 1 item(s) selected

When you select an existing group operation, you can *Open*, *Delete*, or *Execute* it with the buttons on the right of this manager. If you *Open* it, the Group Operations Editor appears. When you select *New*, the *Group Operations Wizard on page 691* appears.

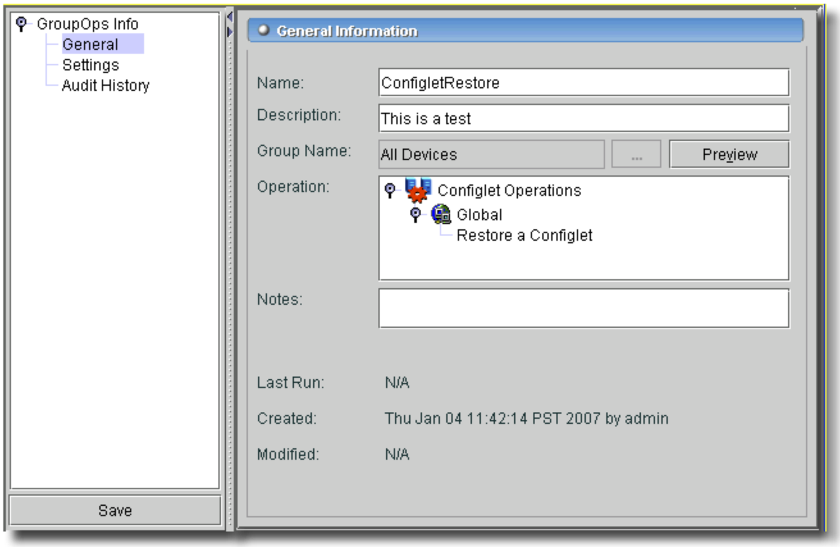
△ **CAUTION:**

When you delete a group that is the target for group operations, the group operation will no longer work correctly.

Group Operations Editor

This editor has several panels that let you manage existing groups.

Figure 22-9. Group Operations: Editor, General.



Name: ConfigletRestore

Description: This is a test

Group Name: All Devices ... Preview

Operation: Configlet Operations / Global / Restore a Configlet

Notes:

Last Run: N/A

Created: Thu Jan 04 11:42:14 PST 2007 by admin

Modified: N/A

The panels are:

- General
- Settings
- Audit History

General

The General panel re-iterates the screen you saw first in Group and Type on page 692. You can alter the description and notes, but the other fields are read-only.

Settings

This panel depends on the operation selected. In our example, we made a batch operation setting the IP address on the selected devices. The *Settings* panel is therefore one like *Action Screen on page* 693.

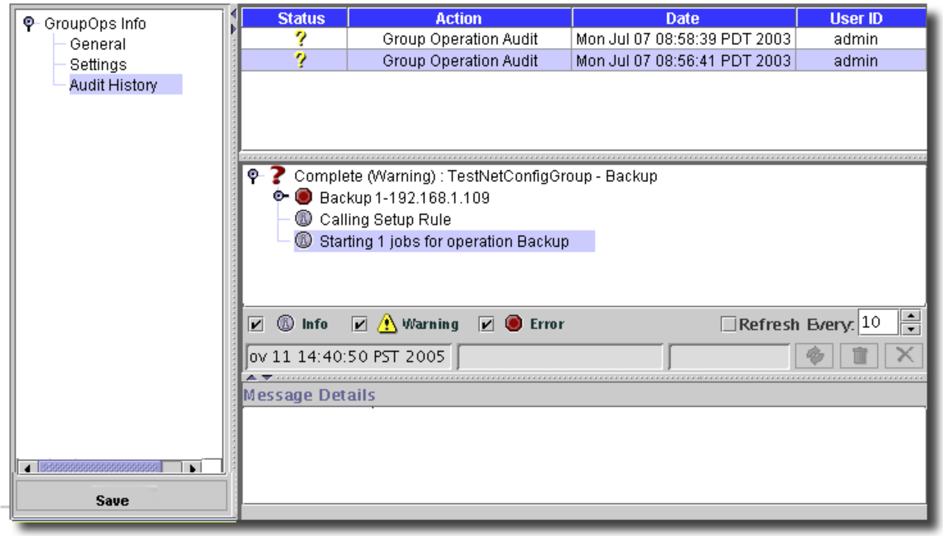
NOTE:

For NETGEAR equipment, a panel appears at the bottom of this screen where you can select to which image the device reboots. Use the pick list to select which image reboot uses.

Audit History

This panel displays the history of group operations in some detail.

Figure 22-10. Group Operations: Audit History



Status	Action	Date	User ID
?	Group Operation Audit	Mon Jul 07 08:58:39 PDT 2003	admin
?	Group Operation Audit	Mon Jul 07 08:56:41 PDT 2003	admin

```
Complete (Warning) : TestNetConfigGroup - Backup
    Backup 1-192.168.1.109
    Calling Setup Rule
    Starting 1 jobs for operation Backup
```

☑ Info ☑ Warning ☑ Error □ Refresh Every: 10

ov 11 14:40:50 PST 2005

Message Details

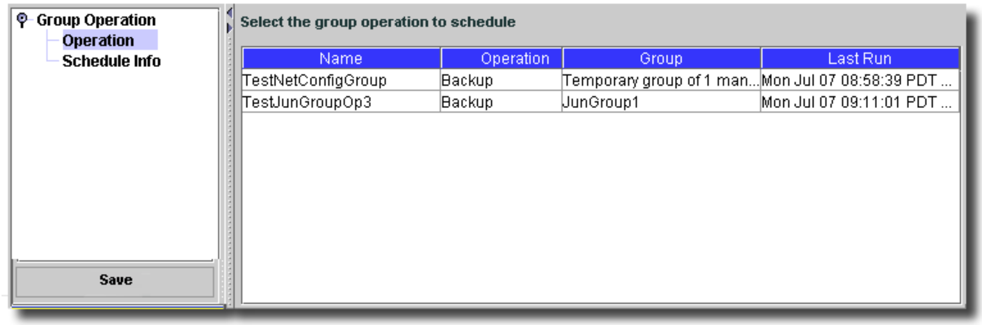
Notice that the top panel lists group operations runs, while the middle panel displays the details of the selected run, and the lowest panel shows the contents of a selected node in the middle panel.

The bar between the lowest and middle panels displays the details concerning a specific message: its start and end time, and the user requesting the operation. You can also use the buttons on the right of this bar to *Refresh*, or *Delete* the currently selected job or *Cancel* a running job.

Scheduling Group Operations

You can schedule group operations from the *File -> Open -> System Services -> Schedules* menu item. If you create a new entry and select Group Operations you open a Group Operation screen where you select which group operation to schedule. Use the *Schedule Info* tab to enter the specifics of how it is to be scheduled.

Figure 22-11. Scheduling a New Group Operation



Select the group operation to schedule

Name	Operation	Group	Last Run
TestNetConfigGroup	Backup	Temporary group of 1 man...	Mon Jul 07 08:58:39 PDT ...
TestJunGroupOp3	Backup	JunGroup1	Mon Jul 07 09:11:01 PDT ...

After you have created a scheduled item you can edit it by clicking *Open* in the Schedules screen. Editing an item displays the Group Operation that is being scheduled in a similar list.

Reports

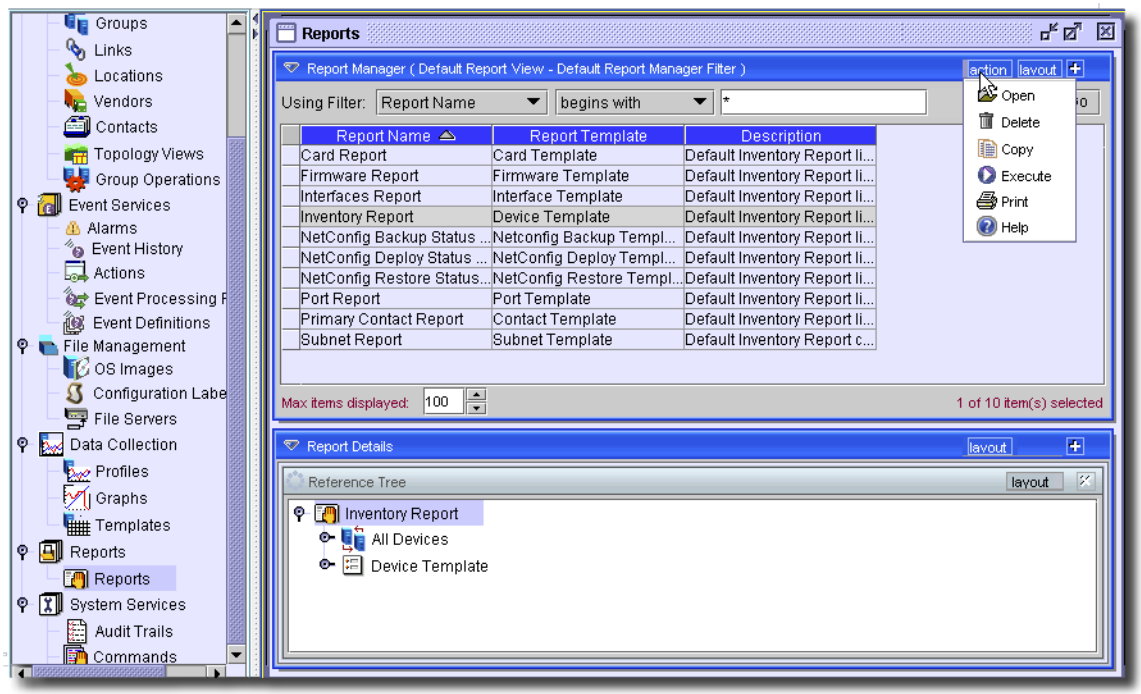
Reports Overview

In the reporting portion of this application, you can run reports that come configured for the application.

Inventory Reports

This screen manages the specific reports that use pre-configured templates that come with this application.

Figure 23-1. Inventory Report Manager



Using Filter: Report Name ▼ begins with ▼ *

Report Name	Report Template	Description
Card Report	Card Template	Default Inventory Report li...
Firmware Report	Firmware Template	Default Inventory Report li...
Interfaces Report	Interface Template	Default Inventory Report li...
Inventory Report	Device Template	Default Inventory Report li...
NetConfig Backup Status ...	Netconfig Backup Templ...	Default Inventory Report li...
NetConfig Deploy Status ...	NetConfig Deploy Templ...	Default Inventory Report li...
NetConfig Restore Status...	NetConfig Restore Templ...	Default Inventory Report li...
Port Report	Port Template	Default Inventory Report li...
Primary Contact Report	Contact Template	Default Inventory Report li...
Subnet Report	Subnet Template	Default Inventory Report c...

Max items displayed: 100

1 of 10 item(s) selected

In the *Action* (or right-click) menu of Inventory Reports Manager, you can configure reports to run (click *Open* a selected report to configure it), and execute them (click *Execute*). See Executing Reports on page 708 for more about this option. Select a report and click *Delete* to remove it from the available list. Click *Copy* to open the report editor (as in *Configuring A Report*) with *CopyOf* prepended to the selected report's name. You must change this name—and any other parameters you like—before you can save the copy.

If you select *Print* from the *Action* menu, an Acrobat report listing all available reports, their templates and description appears. If you select *Help*, the online help for this screen appears.

Notice that the attributes and devices referred to by a report appear in the lower (*Report Details*) panel of this screen when you select a report.

Configuring A Report

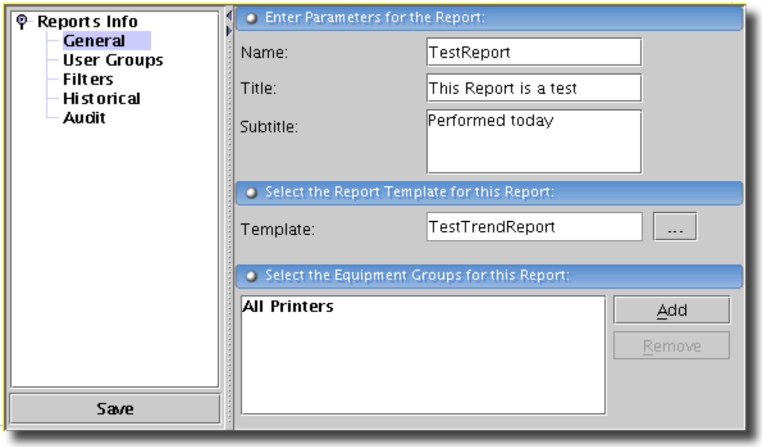
Click *Open* to edit the selected report's settings. The subsequent screens let you configure the report. This editor has the following screens:

- General
- User Groups
- Filters
- Historical
- Audit

General

- This tab lets you configure general information about the report.

Figure 23-2. Reports Info -> General



Reports Info
General
User Groups
Filters
Historical
Audit
Save
Enter Parameters for the Report:
Select the Report Template for this Report:
Select the Equipment Groups for this Report:
...
Add
Remove

Name: TestReport

Title: This Report is a test

Subtitle: Performed today

Template: TestTrendReport

All Printers

This screen contains the following fields:

- **Name**—The identifier for this report.

- **Description**—An optional text description of the report.

- **Title**— The title printed in the report.

Report Template

- **Template**—A read-only reminder of the template selected for this report.

Equipment Groups

Use the *Add* button to select equipment groups this report is to cover.

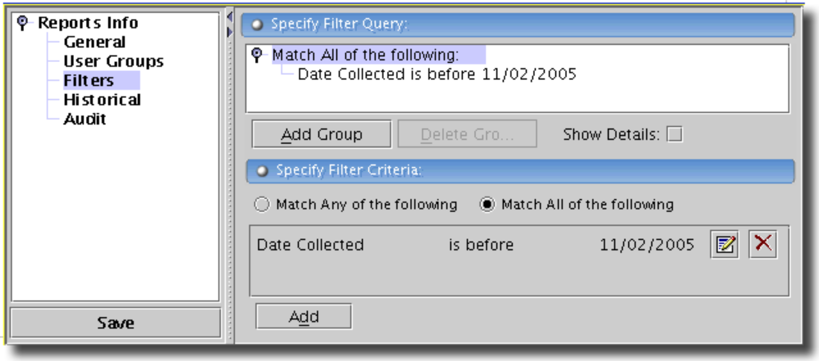
User Groups

Click *Add* to select user groups for this report.

Filters

Here, you can add specific conditions to specify what is reported.

Figure 23-3. Reports Info -> Filters



Match All of the following:
Date Collected is before 11/02/2005

○ Match Any of the following ● Match All of the following

Date Collected is before 11/02/2005

For example, you could request all equipment where the *Name* field contains the word “oware”. The *Add* / *Delete* group buttons let you use group functionality, creating advanced reporting. For example you could match all values within Group 1 but any values within Group 2. For example, Group 1 could match “vendor = 'Dell'” AND “location contains 'cali'” and Group 2 could match “serial number starts with '20' OR contact name contains 'Brian'”.

To add criteria, first click *Add Group* in the upper panel. The *Filter Attributes* radio buttons (*Match Any of the Following* or *Match All of the Following*) determine part of the filter’s operation.

The *Show Details* check box displays additional filter information to the right of listed criteria as they appear in the upper panel. This information displays codes for additional filtering properties you can select when you create the filter components in the lowest panel.

Available detail codes depend on the data type filtered. The *AND*ed or *OR*ed sum of the filter components' codes appears at the top level node. The codes for these attributes are the following:

Code	Meaning	Comment
H or V	Hidden / Visible	
ROO or WRO	Read Only / Read-Write Operand	
ROA or WRA	Read Only / Read-Write Attribute	
ROV or RWV	Read Only / Read-Write Value	Grays out the operand and attribute checkboxes since those are not functional if you make this read-only.
ROO or WRO	Read Only / Read-Write Operand	
ROA or WRA	Read Only / Read-Write Attribute	
M or O	Mandatory / Optional	
EL or IL	Exclude / Include Low	Valid only when you select a range of values. This determines whether you include or exclude the endpoint of the range
EH or IH	Exclude / Include High	Valid only when you select a range of values. This determines whether you include or exclude the endpoint of the range
CS or NC	Case Sensitive / Not Case Sensitive	Does not appear for numeric values.
ML or NM	Multi-line Support / No Multi-Line Support	Filter on multiple-line values (or not).

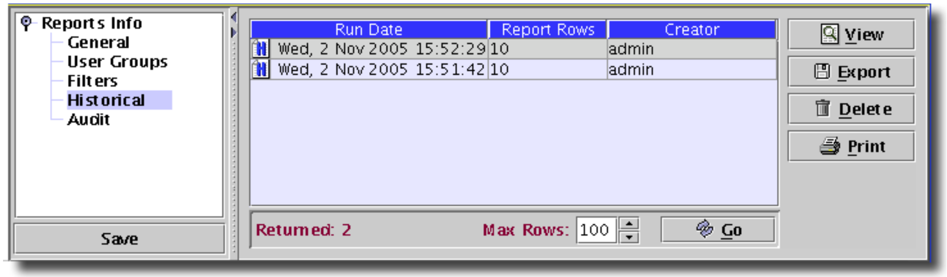
When you select *Read Only* for an attribute, operand or value, some additional impacts are that, for example, reports ordinarily let you alter filters when you manually execute them, but if they have only read-only filtering, then the report executes immediately without a pause to alter filtering.

Specifying the remaining filtering occurs when you click *Add* at the bottom of this screen. Enter attribute / operand / value combinations after clicking *Add*.

Historical

When you run reports, they generate notes in this *Historical* tab.

Figure 23-4. Reports Info -> Historical



Run Date	Report Rows	Creator
Wed, 2 Nov 2005 15:52:29	10	admin
Wed, 2 Nov 2005 15:51:42	10	admin

Returned: 2

Max Rows: 100

The table listing individual reports as rows displays the *Run Date*, *Report Rows* (rows in the report), and *Creator* (the login of the user who ran the report). You can also select a report and use the following buttons:

- **View**—See the report in read-only mode.

- **Execute**—Re-run the selected report. See Executing Reports on page 708.

- **Export**—Export the report in an electronic format. These formats include XLS (Excel), pdf, comma-separated values (CSV), and HTML.

NOTE:

You can save a report from the web client, but cannot export its contents.

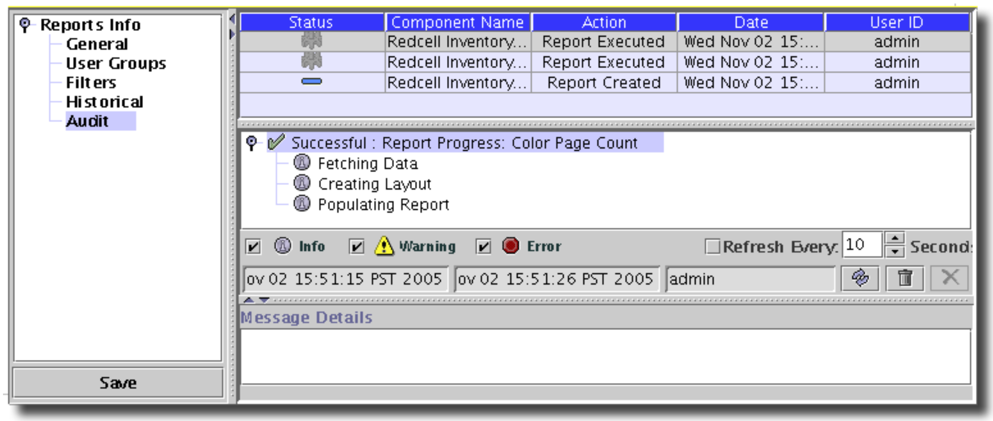
- **Delete**—Remove the listed report.

- **Print**— Print the selected report.

Audit

This screen presents an audit trail for the selected report.

Figure 23-5. Reports Info -> Audit



Reports Info
- General
- User Groups
- Filters
- Historical
- Audit

Status	Component Name	Action	Date	User ID
	Redcell Inventory...	Report Executed	Wed Nov 02 15:...	admin
	Redcell Inventory...	Report Executed	Wed Nov 02 15:...	admin
▬	Redcell Inventory...	Report Created	Wed Nov 02 15:...	admin

✓ Successful : Report Progress: Color Page Count
- Fetching Data
- Creating Layout
- Populating Report

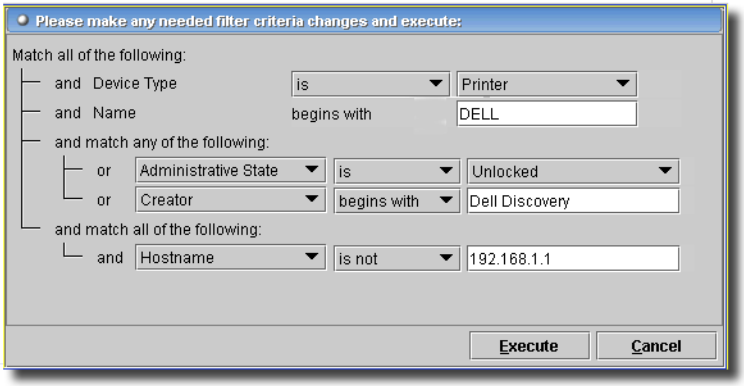
ov 02 15:51:15 PST 2005 | ov 02 15:51:26 PST 2005 | admin

This screen catalogs the action of running the selected report. In this you can see what made a report succeed, or fail.

Executing Reports

When you configure a report, you can *Execute* it. If you have created a filter for a particular report, then you can alter the filtering that produces the report.

Figure 23-6. Filter Screen

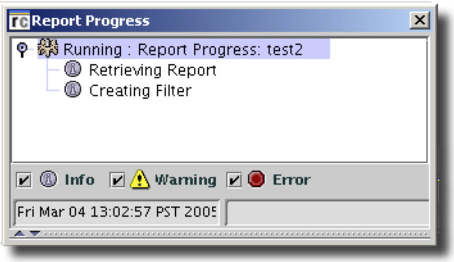


Please make any needed filter criteria changes and execute:

Match all of the following:
- and Device Type is Printer
- and Name begins with DELL
- and match any of the following:
  - or Administrative State is Unlocked
  - or Creator begins with Dell Discovery
- and match all of the following:
  - and Hostname is not 192.168.1.1

The appearance of this screen depends on what is configured in Filters on page 705. Click *Execute* after having made any appropriate alterations to the filter that ultimately produces the report, then a progress indication dialog appears his screen resembles the Audit screen.

Figure 23-7. Report Execution Progress.



Report Progress

Running : Report Progress: test2

Retrieving Report

Creating Filter

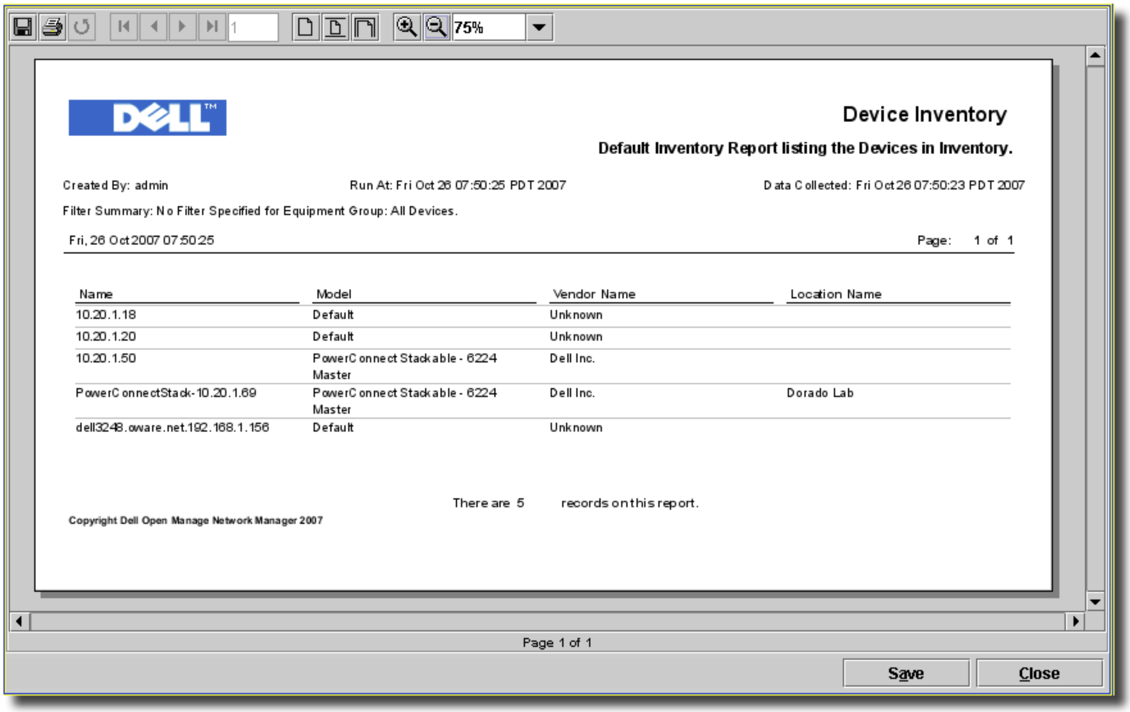
☑ Info ☑ Warning ☑ Error

Fri Mar 04 13:02:57 PST 2005

If the filter you created for this report contains only *Read-only* values, then no interruption to alter the filter occurs. Report execution starts right away.

Report execution produces a preview. of the report itself

Figure 23-8. Report Execution



Device Inventory

Default Inventory Report listing the Devices in Inventory.

Created By: admin   Run At: Fri Oct 26 07:50:25 PDT 2007   Data Collected: Fri Oct 26 07:50:23 PDT 2007

Filter Summary: No Filter Specified for Equipment Group: All Devices.

Fri, 26 Oct 2007 07:50:25   Page: 1 of 1

Name	Model	Vendor Name	Location Name
10.20.1.18	Default	Unknown	
10.20.1.20	Default	Unknown	
10.20.1.50	PowerConnect Stackable - 6224 Master	Dell Inc.	
PowerConnectStack-10.20.1.69	PowerConnect Stackable - 6224 Master	Dell Inc.	Dorado Lab
dell3248.oware.net.192.168.1.156	Default	Unknown	

There are 5 records on this report.

Copyright Dell Open Manage Network Manager 2007

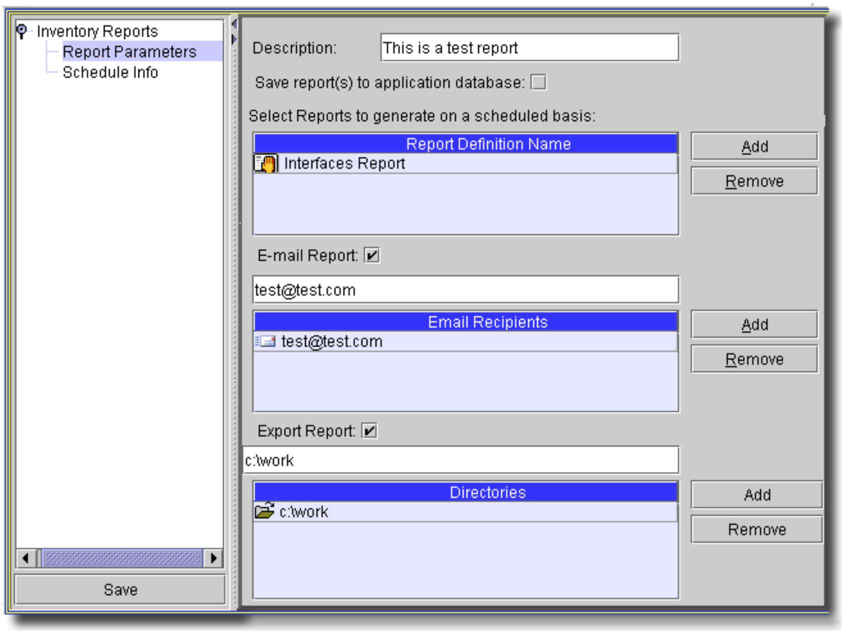
Page 1 of 1

You can schedule, and re-run, execution (see Scheduling Reports on page 710). Note the *Save* button at the bottom of the frame; it saves the report for later viewing. The button bar at the top of this screen lets you navigate through multiple screens, if they exist, manage the magnification of this view, save (export), or print the report.

Scheduling Reports

You can use this application's *Schedules* screen to automate report execution. Click *New* on the *Schedules* screen, and select *Inventory Report*. The *Schedule Info* tab is where you configure the standard scheduling information (see *Schedule Info on page* 750).

Figure 23-9. Scheduling Inventory Reports– Report Parameters



Description: This is a test report

Save report(s) to application database: □

Select Reports to generate on a scheduled basis:

Report Definition Name
Interfaces Report

E-mail Report: ☑

test@test.com

Email Recipients
test@test.com

Export Report: ☑

c:\work

Directories
c:\work

This screen has the following fields:

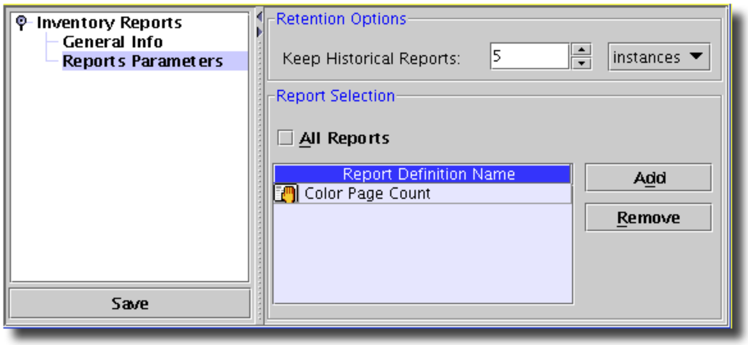
- **Description**—Enter a unique identifier for this scheduled item.
- **Select Reports**...—Click *Add* to select templates from which to generate reports. When you select a template, the list headed by *Report Definition Name* grows.
- **E mail Report**—If you check this checkbox, the application e-mails any generated reports to the recipient list. Enter an e-mail address in the field below the checkbox, then click *Add* to compile the list.

In either list, you can select an item, then click *Remove* to delete it.

Aging Inventory Report Retention

The database retains all reports unless you set database aging parameters. To do this, open the DAP Manager, and click *New*. Then select *Inventory Reports*. The first screen is generic to DAP (see General Info on page 718). On the second tab, you can configure how to retain specific reports.

Figure 23-10. Database Aging Policy–Inventory Reports



Keep Historical Reports: 5 instances

☐ All Reports

Report Definition Name
Color Page Count

On this screen you can configure the following:

Retention Options

- **Keep Historical Reports**—Fill in a number, then select from the pick list whether this number is *Instances*, *Days*, *Weeks*, *Months*, or *Years*.

Report Selection

- **All Reports**—Select this to apply this policy to all reports.

Click *Add* to select individual reports, rather than all available reports. You can select one or more reports, and they appear listed below *Report Definition Name.* Select a listed report and click *Remove* to delete it from the list.

Click *Save* when you have completed this screen and the *General Info* screen. This configuration then appears in the DAP Manager (see *Chapter 25, DB Aging*). Click *Close* in the toolbar to abandon your edits without saving.

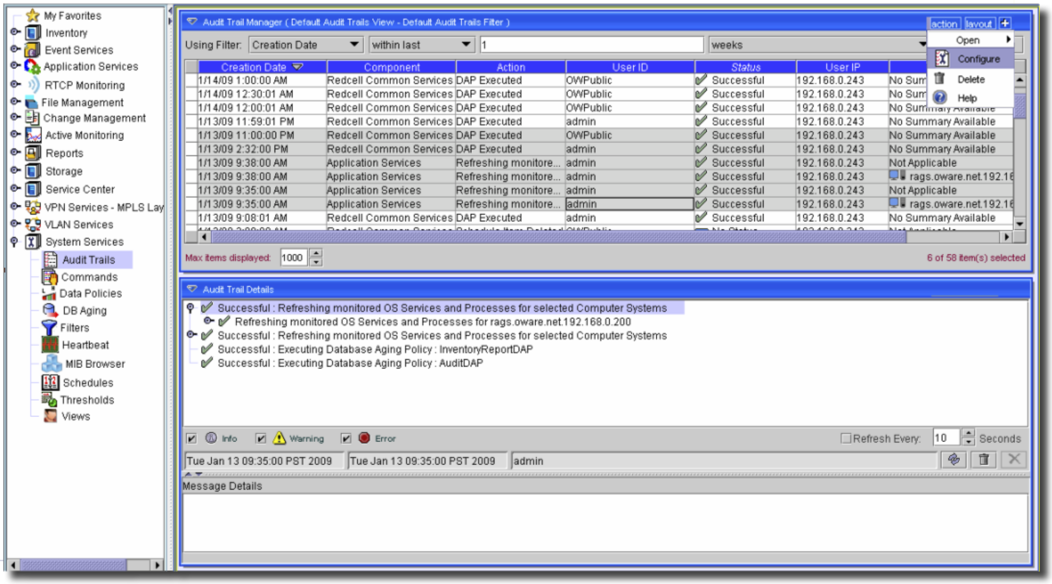
24

Audit Trails

Introducing Audit Trails

You can see the same messages described in Audit / Results on page 184 in the Audit Trails screen. Open this screen from *File -> Open -> System Services -> Audit Trails*, or from the node on the navigation window.

Figure 24-1. Audit Trails Manager



Audit Trail Manager (Default Audit Trails View - Default Audit Trails Filter)

Using Filter: Creation Date | within last | 1 | weeks

Creation Date	Component	Action	User ID	Status	User IP	
1/14/09 1:00:00 AM	Redcell Common Services	DAP Executed	OWPublic	✓ Successful	192.168.0.243	No Sum
1/14/09 12:30:01 AM	Redcell Common Services	DAP Executed	OWPublic	✓ Successful	192.168.0.243	No Sum
1/14/09 12:00:01 AM	Redcell Common Services	DAP Executed	OWPublic	✓ Successful	192.168.0.243	No Sum
1/13/09 11:59:01 PM	Redcell Common Services	DAP Executed	admin	✓ Successful	192.168.0.243	No Summary Available
1/13/09 11:00:00 PM	Redcell Common Services	DAP Executed	OWPublic	✓ Successful	192.168.0.243	No Summary Available
1/13/09 2:32:00 PM	Redcell Common Services	DAP Executed	admin	✓ Successful	192.168.0.243	No Summary Available
1/13/09 9:38:00 AM	Application Services	Refreshing monitore...	admin	✓ Successful	192.168.0.243	Not Applicable
1/13/09 9:38:00 AM	Application Services	Refreshing monitore...	admin	✓ Successful	192.168.0.243	rags.oware.net.192.16
1/13/09 9:35:00 AM	Application Services	Refreshing monitore...	admin	✓ Successful	192.168.0.243	Not Applicable
1/13/09 9:35:00 AM	Application Services	Refreshing monitore...	admin	✓ Successful	192.168.0.243	rags.oware.net.192.16
1/13/09 9:08:01 AM	Redcell Common Services	DAP Executed	admin	✓ Successful	192.168.0.243	No Summary Available

Max items displayed: 1000

6 of 58 item(s) selected

Audit Trail Details

- ✓ Successful : Refreshing monitored OS Services and Processes for selected Computer Systems
  - ✓ Refreshing monitored OS Services and Processes for rags.oware.net.192.168.0.200
- ✓ Successful : Refreshing monitored OS Services and Processes for selected Computer Systems
- ✓ Successful : Executing Database Aging Policy : InventoryReportDAP
- ✓ Successful : Executing Database Aging Policy : AuditDAP

☑ Info ☑ Warning ☑ Error □ Refresh Every: 10 Seconds

Tue Jan 13 09:35:00 PST 2009 | Tue Jan 13 09:35:00 PST 2009 | admin

Message Details

The manager has a standard filter at its top that lets you limit the trails listed. By default, they appear listed by creation date. See Filter Editor on page 736 for instructions about creating and customizing filters. Use *Layout -> Filter* to select any other *Audit Trail* filters in the system you want to apply—for example you can filter the listed trails by Job Status (*Canceled*, *Failed*, *No Job Status*, *Running*, *Successful*, *Unknown*), and display only *Successful* audits, limit visible trails to a single vendor and/or operation, and so on.

When you select a listed audit trail at the top of this screen, its messages appear in the *Audit Trail Details* screen at the bottom of this manager. Dates and times for individual, selected messages appear in the middle of this lower screen area, which is like Audit / Results on page 184. The messages (*Type*, *Time* and *Message*) appear in the lowest portion of the screen. Checking the checkboxes next to the various icons further filters what messages appear.

Right click a selected audit trail, or click the *action* button after you select a trail for the following options:

- **Open -> Entity—**Open the associated configuration panel for the selected entity.

- **Open -> Audit Details**—Open the Audit Trails Editor Panel to manage the selected trail.

- **Configure**—Configure (enable / disable) specific types of audit trails. See Audit Control Settings on page 716.

- **Delete**—Remove the selected audit trail.

- **Help**—Open the online help relevant to this screen.

Audit Trails Editor Panel

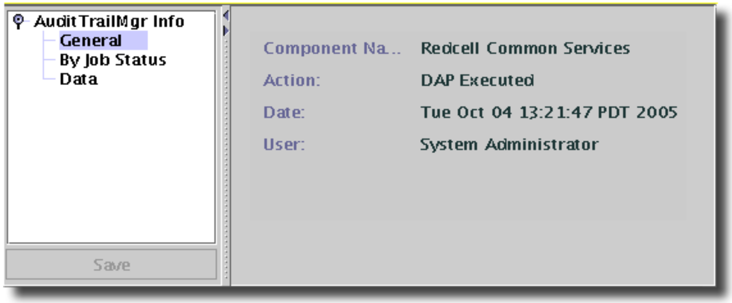
When you open a history item, the Audit Trails Editor panel appears. It has the following panels (described in subsequent sections):

- General
- By Job Status
- Data

General

When you select a component, then click the *Open* button, a multi-panel editor appears.

Figure 24-2. Audit Trails Editor - General



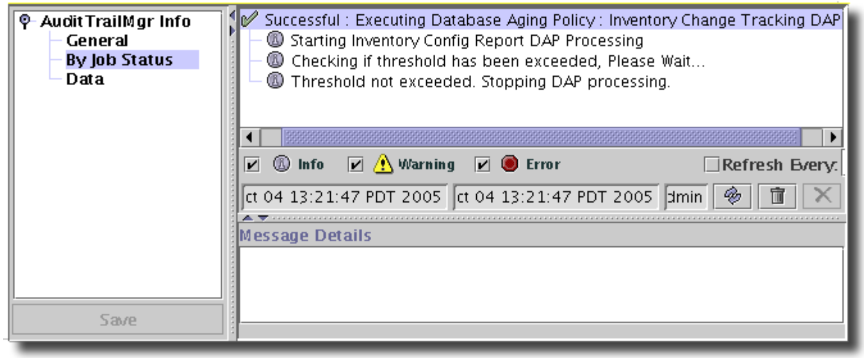
Component Na... Redcell Common Services
Action: DAP Executed
Date: Tue Oct 04 13:21:47 PDT 2005
User: System Administrator

The first panel (*General*), reiterates the *Component Name*, *Action*, *Date*, and *User* for the selected item.

By Job Status

This screen outlines the status message information for the selected component(s).

Figure 24-3. Audit Trail Editor - By Job Status



✓ Successful : Executing Database Aging Policy : Inventory Change Tracking DAP
- Starting Inventory Config Report DAP Processing
- Checking if threshold has been exceeded, Please Wait...
- Threshold not exceeded. Stopping DAP processing.

☑ Info ☑ Warning ☑ Error □ Refresh Every:

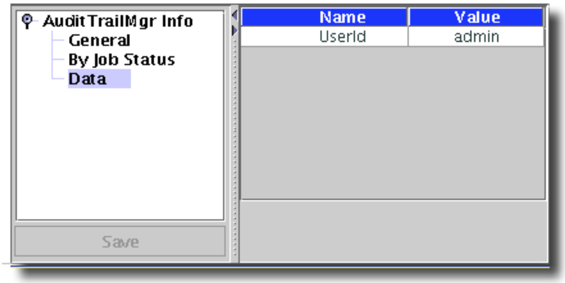
ct 04 13:21:47 PDT 2005 | ct 04 13:21:47 PDT 2005 | dmin

This is a standard audit screen. Messages appear at the top. The date and time of the selected message appear in the middle, and any details about that message appear in the lowest panel.

Data

This screen lets you view and edit the selected trail's data.

Figure 24-4. Audit Trail Editor - Data



Name	Value
UserId	admin

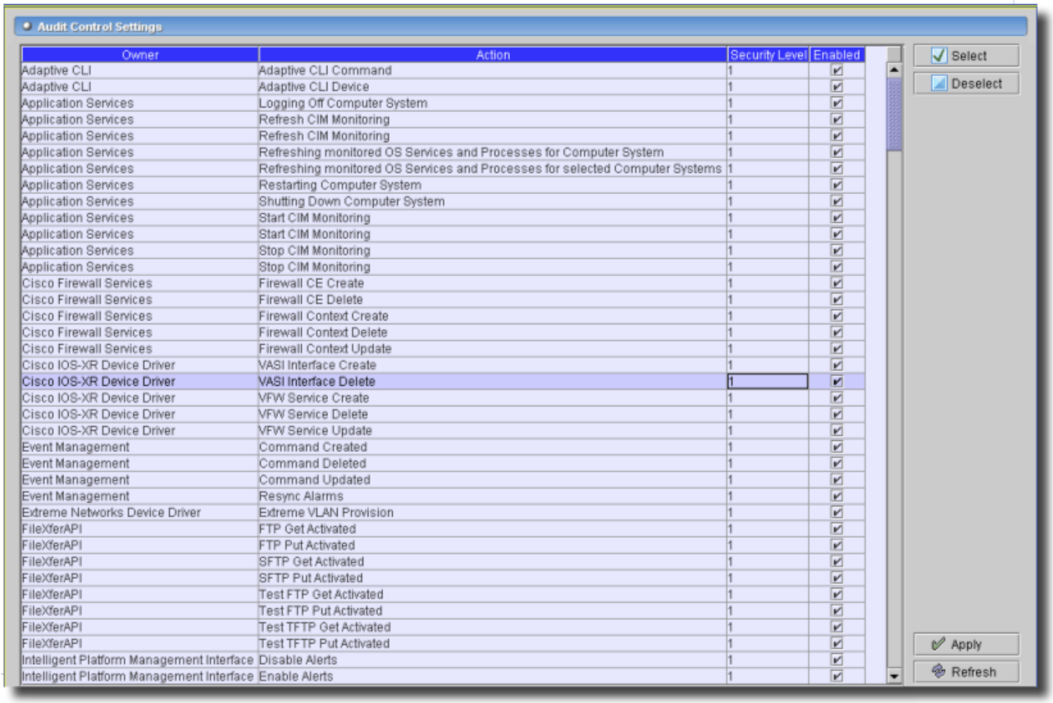
The exact appearance of the screen depends on the audit action selected before you click *Open*. For some jobs, it does not appear at all.

In some screens, you can also click *View* buttons, where they appear, to see existing data.

Audit Control Settings

This screen appears after you select *action -> Configure* in the audit trail manager.

Figure 24-5. Audit Control Settings



Audit Control Settings

Owner	Action	Security Level	Enabled
Adaptive CLI	Adaptive CLI Command	1	☑
Adaptive CLI	Adaptive CLI Device	1	☑
Application Services	Logging Off Computer System	1	☑
Application Services	Refresh CIM Monitoring	1	☑
Application Services	Refresh CIM Monitoring	1	☑
Application Services	Refreshing monitored OS Services and Processes for Computer System	1	☑
Application Services	Refreshing monitored OS Services and Processes for selected Computer Systems	1	☑
Application Services	Restarting Computer System	1	☑
Application Services	Shutting Down Computer System	1	☑
Application Services	Start CIM Monitoring	1	☑
Application Services	Start CIM Monitoring	1	☑
Application Services	Stop CIM Monitoring	1	☑
Application Services	Stop CIM Monitoring	1	☑
Cisco Firewall Services	Firewall CE Create	1	☑
Cisco Firewall Services	Firewall CE Delete	1	☑
Cisco Firewall Services	Firewall Context Create	1	☑
Cisco Firewall Services	Firewall Context Delete	1	☑
Cisco Firewall Services	Firewall Context Update	1	☑
Cisco IOS-XR Device Driver	VASI Interface Create	1	☑
Cisco IOS-XR Device Driver	VASI Interface Delete	1	☑
Cisco IOS-XR Device Driver	VFW Service Create	1	☑
Cisco IOS-XR Device Driver	VFW Service Delete	1	☑
Cisco IOS-XR Device Driver	VFW Service Update	1	☑
Event Management	Command Created	1	☑
Event Management	Command Deleted	1	☑
Event Management	Command Updated	1	☑
Event Management	Resync Alarms	1	☑
Extreme Networks Device Driver	Extreme VLAN Provision	1	☑
FileXferAPI	FTP Get Activated	1	☑
FileXferAPI	FTP Put Activated	1	☑
FileXferAPI	SFTP Get Activated	1	☑
FileXferAPI	SFTP Put Activated	1	☑
FileXferAPI	Test FTP Get Activated	1	☑
FileXferAPI	Test FTP Put Activated	1	☑
FileXferAPI	Test TFTP Get Activated	1	☑
FileXferAPI	Test TFTP Put Activated	1	☑
Intelligent Platform Management Interface	Disable Alerts	1	☑
Intelligent Platform Management Interface	Enable Alerts	1	☑

This screen lets you check to enabled audited items. The *Owner* column describes the application or module that contains the audited action. The *Action* column describes the action to be enabled / disabled in more detail. The *Security Level* column informs you about the security level of the audited action. Only security events (see the *Administration Section* for a list) are level 0. All others are level 1. Only administrative users can see level 0 events in the actual audit trail itself in Audit Trail Manager. The checkboxes in the *Enabled* column are checked, by default. Unchecking these disables auditing for the selected action(s). You must click *Apply* before any revised settings take effect.

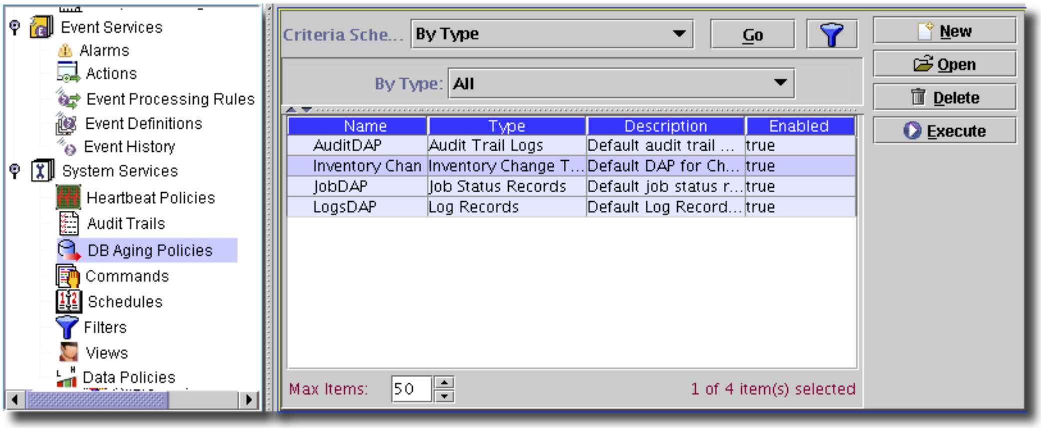
25-

DB Aging

Database Aging Overview

The database aging policy option automates your database management tasks for records that may otherwise overwhelm it. You can create, edit, delete and execute these policies in the DAP Manager, accessible in *File -> Open -> System Services -> DB Aging*, or from the Navigation Window.

Figure 25-1. DB Aging screen



Criteria Sche... By Type

By Type: All

Name	Type	Description	Enabled
AuditDAP	Audit Trail Logs	Default audit trail ...	true
Inventory Chan	Inventory Change T...	Default DAP for Ch...	true
JobDAP	Job Status Records	Default job status r...	true
LogsDAP	Log Records	Default Log Record...	true

Max Items: 50

1 of 4 item(s) selected

This screen displays a list of existing policies, by *Name*, *Type*, *Description*, and whether they are *Enabled* (true/false). As with most managers, you can filter what appears with the selections you make at the top of the screen. See *Filter Wildcards on page* 738 for more information.

You can click *New*, and when you select a policy *Open*, *Delete* or *Execute* it. Clicking a column heading sorts the list based on that column. Click twice to change from an ascending to a descending sort.

⚠ **CAUTION:**
Database aging policies run only on the scheduled intervals, so data this application collects can exceed set limits between those intervals.

You can also export (or import) an XML representation of the listed policies. Use *File -> Export* or *File -> Import*.

NOTE:

Saved, recurring reports are one example of data to archive with the policies described below.

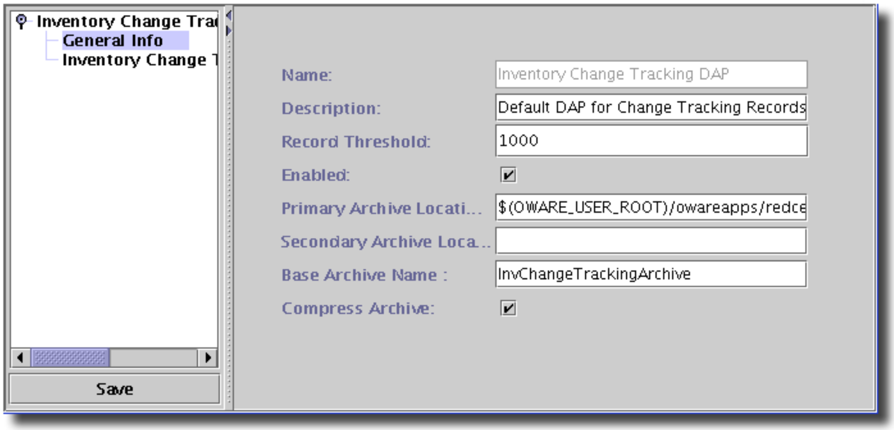
Database Aging Policy Editor

Click the *New* button, and the next screen lets you select a type policy based on the records archived. Available selections include *Alarms*, *Audit Trail Logs*, *Configuration File Records*, *Job Status Records*, *Log Records*, *Inventory Change Records*, and *Syslog*. You can also select an existing policy and click *Open* to edit it.

General Info

Once you select a new policy's type (or if you have selected an existing policy and clicked *Open*), most screens appear, letting you select general information about the database aging policy.

Figure 25-2. DAP General Info



Name: Inventory Change Tracking DAP
Description: Default DAP for Change Tracking Records
Record Threshold: 1000
Enabled: ☑
Primary Archive Locati...: $(OWARE_USER_ROOT)/owareapps/redce
Secondary Archive Loca...:
Base Archive Name : InvChangeTrackingArchive
Compress Archive: ☑

This screen is generic—similar, if not identical, no matter what type of policy you are creating or editing (see Order Summaries on page 726 for an exception). It contains the following selections:

- **Name**—A unique identifier for this policy

- **Description**—A text description.

- **Record Threshold**—The number of records that must exist before archiving begins.

- **Primary Archive Location**—A disk location for archiving.

- **Secondary Archive Location**—A disk location for archiving if the primary location fails.

CAUTION:
You must enter disk locations on the application server, otherwise archiving fails.

If the Primary path fails when writing the archive then if a secondary path exists the application uses the secondary path. If writing to the secondary path is successful, then the DAP job cleans up the database issuing a warning. If the secondary path is not successful, then the DAP job closes without removing database records, and issues an error. Similarly, if the secondary path is not specified then the DAP job will close with an error.

NOTE:

Currently two different notification behaviors exist. Audit DAP returns a warning when the primary path fails, however Alarm DAP does not return a warning.

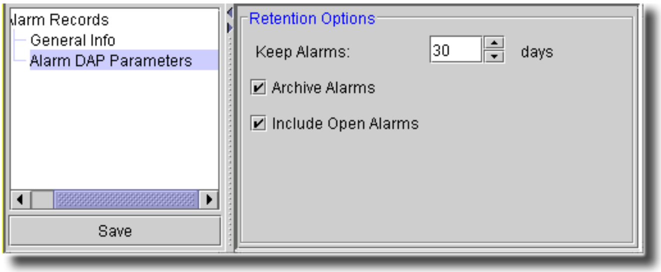
- **Base Archive Name**—The base name for the archive (part of the filename).
- **Compress Archive**—A checkbox that enables compression of the archive.
- **Enabled**—Determines whether the policy is enabled/disabled. Check to enable.

NOTE:

The archived data is in an XML or compressed XML format in the location specified. You can use your favorite XML or text viewer to see archived data. As a convenience, OpenManage Network Manager supplies the `dapviewer`. Run this utility from a command shell where you have sourced the oware environment (run `oware` or `.  ./etc/.dsienv`). Select your archived XML with the command button (...), then click *Load*. The *Advanced* settings let you customize the columns displayed. This utility does not display compressed files; you must uncompress them first. **Note**: You can view archived audit trails with `dapviewer`, but not archived Alarm or Event History.

Alarm DAP Parameters

Figure 25-3. In addition to the General Info screen, this one appears in policies for Event Services Alarm Logs. DAP for Event Services Alarm Logs



Keep Alarms: 30 days
☑ Archive Alarms
☑ Include Open Alarms

In this screen, you can add *Sub-Policies* for managing alarm archiving. First, fill in the fields at the bottom of the list of sub-policies:

- **Include Open Alarms**—This enables logging of open alarms.

- **Days to Retain (Retention)**—How long to retain the records of the selected status (in 24-hour periods).

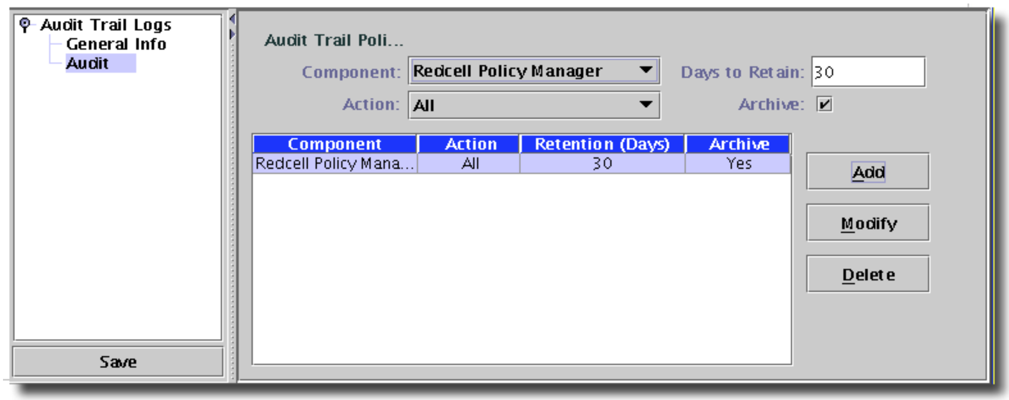
- **Archive**—Whether to archive the alarms.

Click the *Add* button to add the sub-policy to the list. You can also select and *Modify* a sub-policy with that button. Select and *Delete* unwanted sub-policies.

Audit Trail Logs

In addition to the General Info screen, this one appears in policies for Audit Trail Logs.

Figure 25-4. DAP Audit Trail Logs



Audit Trail Poli...

Component: Redcell Policy Manager

Days to Retain: 30

Action: All

Archive: ☑

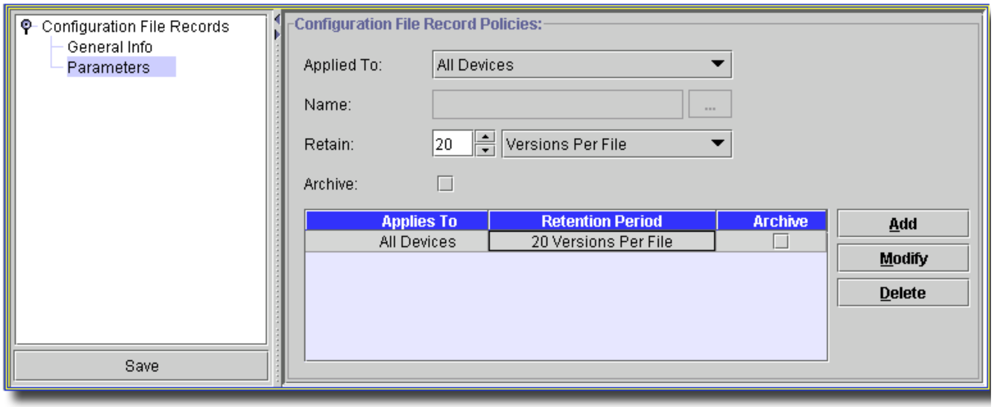
Component	Action	Retention (Days)	Archive
Redcell Policy Mana...	All	30	Yes

This screen lets you add policies for selected device's audit trails. Select the device(s) by filtering on *Component* and *Action*. Enter a *Days to Retain* number indicating how long to retain the records of the selected status (in 24-hour periods)., and click the *Archive* checkbox if you want to archive the selected records after their retention period is done. Specify the archive location in the *General Info* screen. You can select different combinations of *Component* and *Action* and have multiple lines in the policy table to handle multiple types of Audit Trail logs with a single policy.

Configuration File Records

With File Management installed, you can manage configuration file storage.

Figure 25-5. Configuration File Records DAP Parameters



Configuration File Records
General Info
Parameters
Save
Configuration File Record Policies:
Add
Modify
Delete

Applied To: All Devices

Name:

Retain: 20 Versions Per File

Archive: □

Applies To	Retention Period	Archive
All Devices	20 Versions Per File	□

Besides the General Info screen, this DAP editor lets you select the following for Configuration File Record aging:

- **Applied to**—Select from *All Devices*, *Group* or *Single Device* from the pick list.

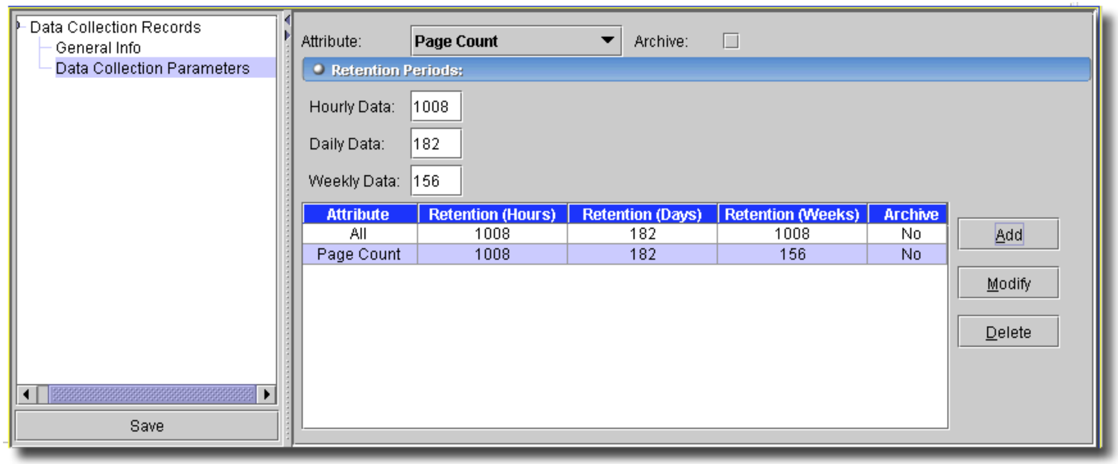
- **... (ellipsis)**—This command button lets you select devices or groups.

- **Retain**—Select a number, and whether to retain *Days* or *Versions per file*.

- **Archive**—Check here to activate archiving for this item.

Use the *Add*, *Modify* or *Delete* buttons to manage the table below the above fields. Click *Save* to confirm your additions, edits or deletions.

Figure 25-6. Data Collection



Attribute: Page Count

Archive: □

Hourly Data: 1008

Daily Data: 182

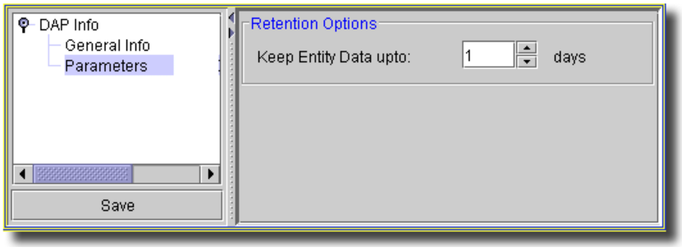
Weekly Data: 156

Attribute	Retention (Hours)	Retention (Days)	Retention (Weeks)	Archive
All	1008	182	1008	No
Page Count	1008	182	156	No

Discovery Definition Data Records

This screen manages retention of data retrieved and retained from service discovery. It only appears if you have the service discovery option installed.

Figure 25-7. Discovery Definition Data Records



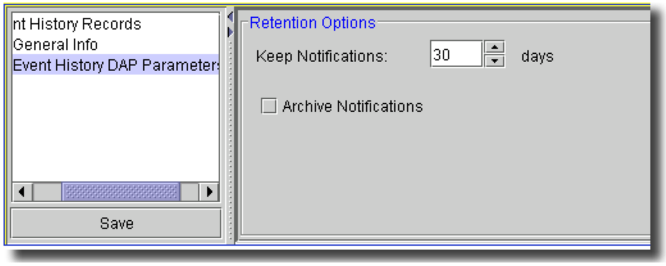
Keep Entity Data upto: 1 days

Successful service discovery deletes most retrieved data as it creates service instances in the OpenManage Network Manager database. Remnants of incomplete or interrupted discovery, device configuration files or CSV files of customers may remain, however, and this DAP deletes such data from the database. Configure the number of days to retain this data as is appropriate for your system. Best practice is to remove the retained data relatively soon (one or two days).

Event History DAP Parameters

This screen configures the archiving of events (notifications).

Figure 25-8. Event History DAP Parameters



Keep Notifications: 30 days

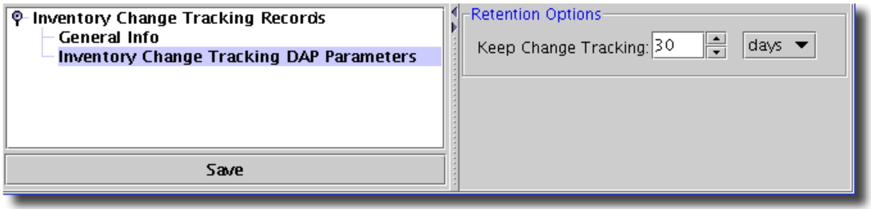
□ Archive Notifications

Select how long you want to keep events, and whether you want them archived after they are discarded.

Inventory Change and Tracking DAP Parameters

In addition to the General Info screen, creating or editing inventory change or inventory change tracking policies let you set retention policies for these records.

Figure 25-9. Inventory Change and Tracking DAP Parameter


Inventory Change Tracking Records
General Info
Inventory Change Tracking DAP Parameters
Save
Retention Options

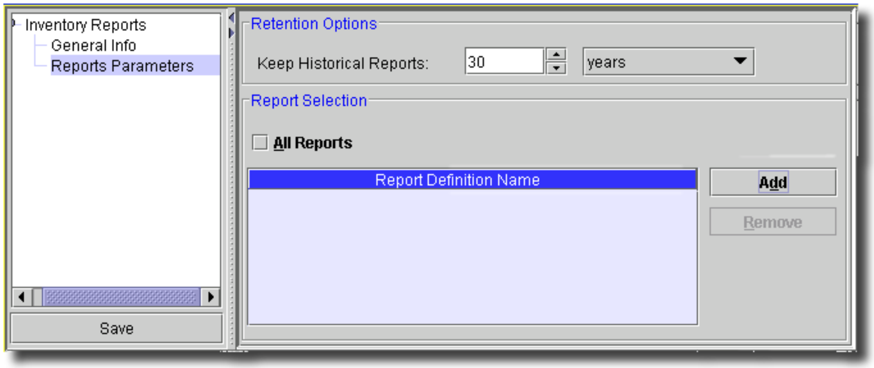
Keep Change Tracking: 30 days

These screens are similar.

Inventory Records

This screen manages retention of inventory records. It has an abbreviated version of the General Info screen.

Figure 25-10. Inventory Records



Keep Historical Reports: 30 years

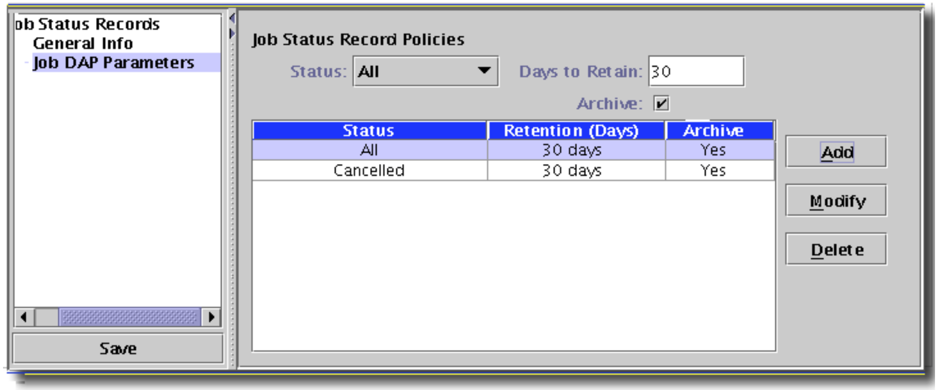
□ All Reports

Add a period to retain reports to the list of *Report Definition Name* by selecting a reporting period with the pick list, then clicking *Add*. Click *Remove* to delete a selected report on the list. You can also check *All Reports* to retain them all the period selected.

Job DAP Parameters

In addition to the General Info screen, creating or editing job status records policies let you set policies for these records.

Figure 25-11. Job DAP Parameters



Status: All

Days to Retain: 30

Archive: ☑

Status	Retention (Days)	Archive
All	30 days	Yes
Cancelled	30 days	Yes

Select from the following parameters and click *Add* to create a policy. You can create multiple policies to handle records with different statuses.

- **Status**—Select from the options available in the pick list: *Failed*, *All*, *Unknown*, *Successful*, and *Cancelled*.
- **Days to Retain**—How long to retain the records of the selected status (in 24-hour periods).
- **Archive**—Checking this enables archiving. Otherwise, records are discarded after the *Days to Retain* deadline.

You can also *Modify* or *Delete* selected policies with the buttons on the right. Click the *Save* icon on the toolbar, or select *File -> Save* to persist this policy.

Learned MAC Address DAP Parameters

Set the number of days to keep stale addresses with the spinner on this screen. A seeded DAP defaults of 10 days, and has a record threshold of 10,000.

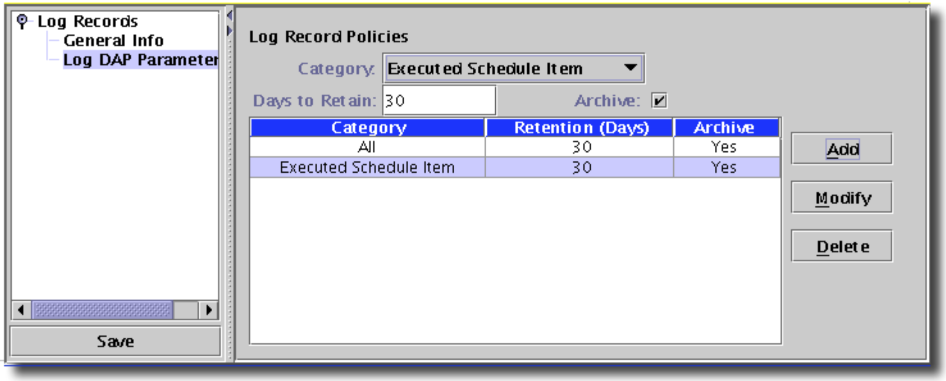
NOTE:

This is not created or scheduled by default. You must create a DAP, and schedule it for it to be effective.

Log DAP Parameters

In addition to the General Info screen, this screen appears in policies for Log Records.

Figure 25-12. Log DAP Parameters



Log Record Policies

Category: Executed Schedule Item

Days to Retain: 30

Archive: ☑

Category	Retention (Days)	Archive
All	30	Yes
Executed Schedule Item	30	Yes

Select from the following parameters and click *Add* to create a policy. You can create multiple policies to handle records with different categories.

- **Category**—Select from the options available in the pick list.

NOTE:

This list may change, depending on the installed applications.

- **Days to Retain**— How long to retain the records of the selected status (in 24-hour periods).

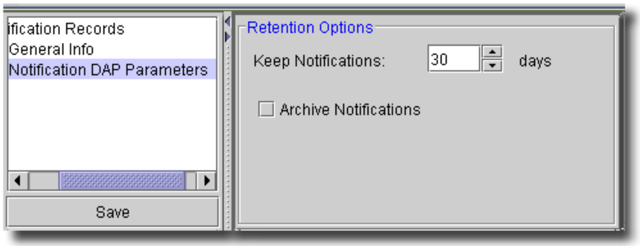
- **Archive**—Checking this enables archiving. Otherwise, records are discarded after the *Days to Retain* deadline.

You can also *Modify* or *Delete* selected policies with the buttons on the right. Click the *Save* icon on the toolbar, or select *File -> Save* to persist this policy.

Notification DAP Parameters

This screen manages the retention of notification records. It adds to the General Info screen.

Figure 25-13. Notification DAP Parameters



Keep Notifications: 30 days

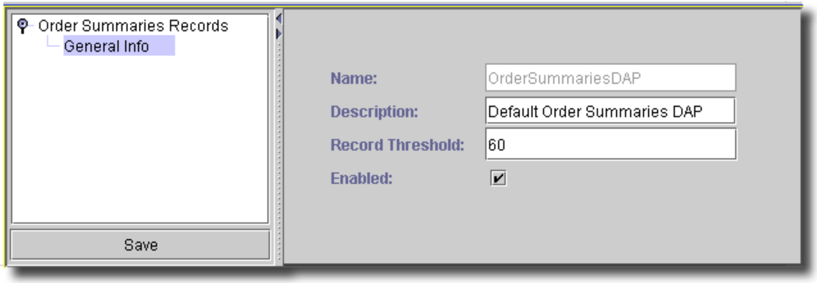
☐ Archive Notifications

Select a period to keep notifications, and check to *Archive* those notifications.

Order Summaries

This screen manages the retention of the order summary portion of the Consumables Calculated Life summary reports. This is separate from the retention of reports in the *History* tab in *Inventory Reports*.

Figure 25-14. Order Summaries



Name: OrderSummariesDAP

Description: Default Order Summaries DAP

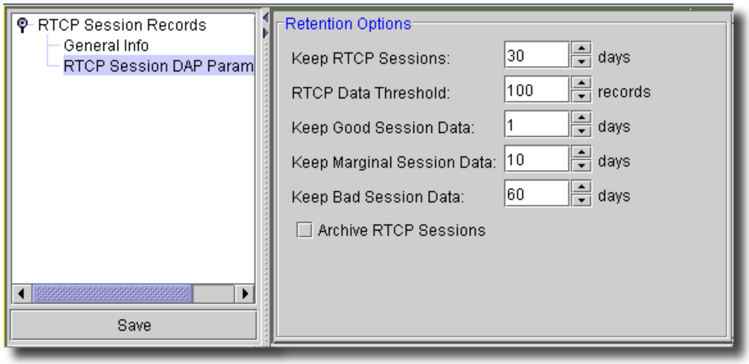
Record Threshold: 60

Enabled: ☑

This screen has the following fields:

- **Name**—A unique identifier for this policy
- **Description**—A text description
- **Record Threshold**—The number of records to archive. Numbers greater than this are discarded. Records are the order summary only, not the entire report.
- **Enabled**—Determines whether the policy is enabled/disabled. Check to enable.

Figure 25-15. RTCP Session DAP Parameters



Retention Options

Keep RTCP Sessions: 30 days

RTCP Data Threshold: 100 records

Keep Good Session Data: 1 days

Keep Marginal Session Data: 10 days

Keep Bad Session Data: 60 days

□ Archive RTCP Sessions

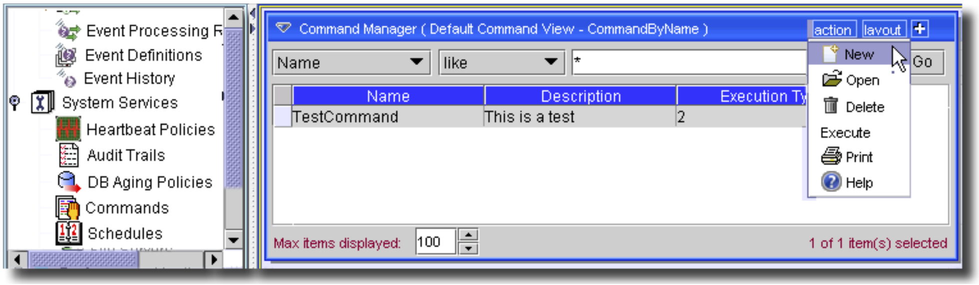
26

Commands

Commands Manager

Correlated notifications can trigger external scripts. These script commands can even have parameters that come from values in the Notification’s attributes, or other assigned constants. To see available script commands, you must open the script Commands screen.

Figure 26-1. Commands screen



Name ▼ like ▼ *

Name	Description	Execution Ty
TestCommand	This is a test	2

Max items displayed: 100

1 of 1 item(s) selected

Access this Commands screen from the Navigation pane. The manager lists available script commands. You can create, edit and delete script commands with the *Action* or context menu on this manager. Here are those menu commands:

- **New**—Opens the Command Editor, through which you can define a new command. See Command Editor on page 728 for more information about the Action Editor.
- **Open**—Opens the selected command for modification. See Command Editor on page 728 for more information.
- **Delete**—Deletes the selected command. Select the command to remove and click *Delete*. The application prompts you for confirmation.
- **Execute**—If you configure an action with the *Execute Manually* checkbox checked, this menu item controls that manual execution.

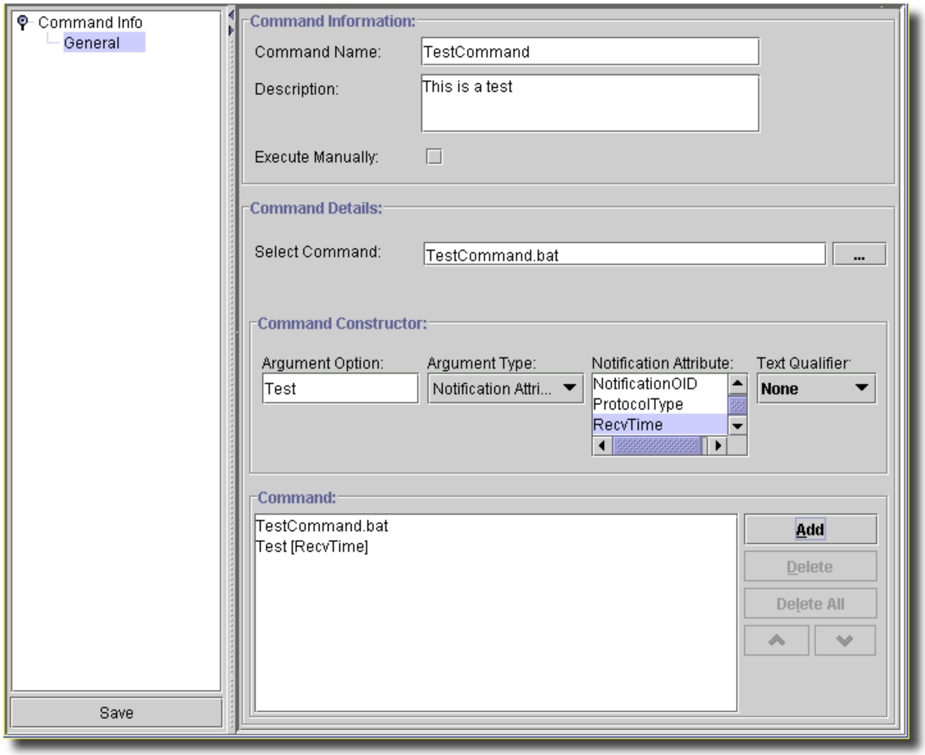
CAUTION:
Executing scripts that refer to additional software—for example, Perl scripts—requires that software be installed on the application / mediation server before attempting to execute the script. See the Administration Section for more about Perl.

- **Print**—Print the listed commands to an Acrobat® file. (You must have Acrobat reader installed for this to work properly.) Change the filter and click *Go* to change this printed report's appearance.
- **Import / Export**—Export an XML representation of the commands listed (not the commands themselves).
- **Help**—Open the context-sensitive help for this screen.

Command Editor

When you want to automate running a script or other program, and customize its command line, you must store it as a OpenManage Network Manager Command. To start doing this, click the *New* button in the Command Manager to create, or select an existing command you want to automate and click *Edit* to edit it, and Command Editor opens.

Figure 26-2. Command Editor



Command Name: TestCommand

Description: This is a test

Execute Manually: □

Select Command: TestCommand.bat

Argument Option: Test

Argument Type: Notification Attri...

Notification Attribute: NotificationOID
ProtocolType
RecvTime

Text Qualifier: None

TestCommand.bat
Test [RecvTime]

You can configure your script with the following fields:

Command Information

- **Command Name**—A unique text identifier.

- **Description**—A text description.

- **Execute Manually**—Enable manual execution. When you enable manual execution, and select such commands in the Commands manager, it enables the *Execute* menu item.

Command Details

- **Select Command**—The script to run with this command. You can enter the file name and path manually, or select it with the command button (...), which opens a file chooser.

Command Constructor

Enter parameters to append to the selected script here. The *Argument Option* can be something like `-a`. The *Argument Type* pick list lets you select either a constant or an EventInfo attribute. If you select a constant, the next field is *Constant Value* (a text field). If you select EventInfo attribute, the next field is a pick list of the attributes available. The final field is *Text Qualifier* which lets you select whether this parameter needs double, single quotes, or no qualifier. When you select quotes, the parameter looks like this: `-a "surrounded by quotes"`

Command

This section of the screen displays the script command as you assemble it. Click the *Add* button on the right to assemble the complete script command. Added parameters always appear last on the list in this area, but you can use the arrow keys to re-arrange their order, and the *Delete* button to remove parameters (but not the script). *Delete All* removes everything.

Select *File* -> *Save* or click the *Save* icon to add your command script to the list of those available.

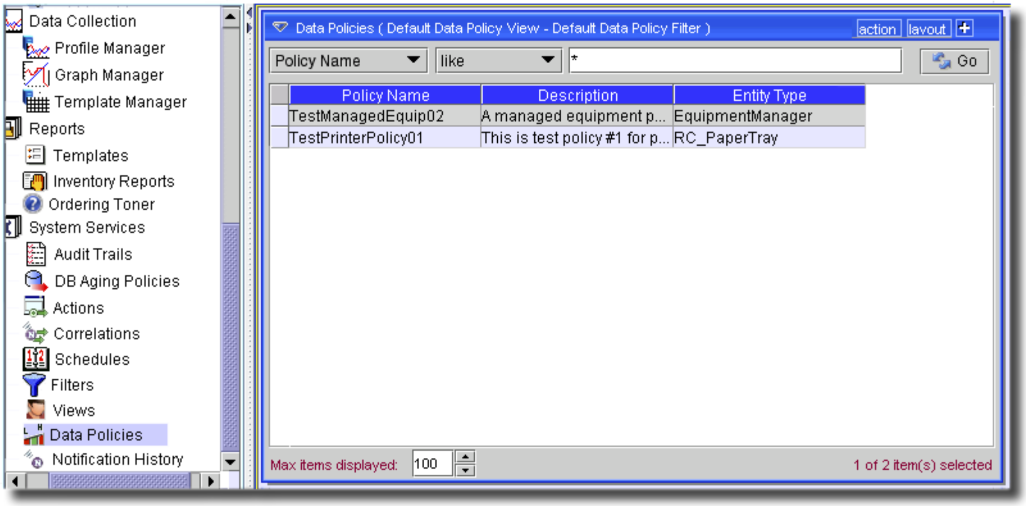
27

Data Policies

Data Policies Manager

This screen lets you manage data policies. These policies let you scan equipment for compliance with them, and emit notifications (see Chapter 34, Events, Rules and Actions) that describe them when you save or poll equipment.

Figure 27-1. Data Policies



Data Policies (Default Data Policy View - Default Data Policy Filter)

Policy Name | like | *

Policy Name	Description	Entity Type
TestManagedEquip02	A managed equipment p...	EquipmentManager
TestPrinterPolicy01	This is test policy #1 for p...	RC_PaperTray

Max items displayed: 100

1 of 2 item(s) selected

The policies appear listed at the top of this screen. You can filter the items displayed when you check the *Use Filter* checkbox. The details panel at the bottom of this screen display details of the selected policy. The *Action* button (or right click) menu contains the following items:

- **New**—Opens the Data Policy Editor, through which you can define a new mapping. See Data Policy Editor - General on page 732 for more information about the Mapping Editor.

- **Open**—Opens the selected Data Policy for modification. See Data Policy Editor - General on page 732 for more information.

- **Delete**—Deletes the selected policy. Select the policy to remove and click *Delete*. The application prompts you for confirmation.

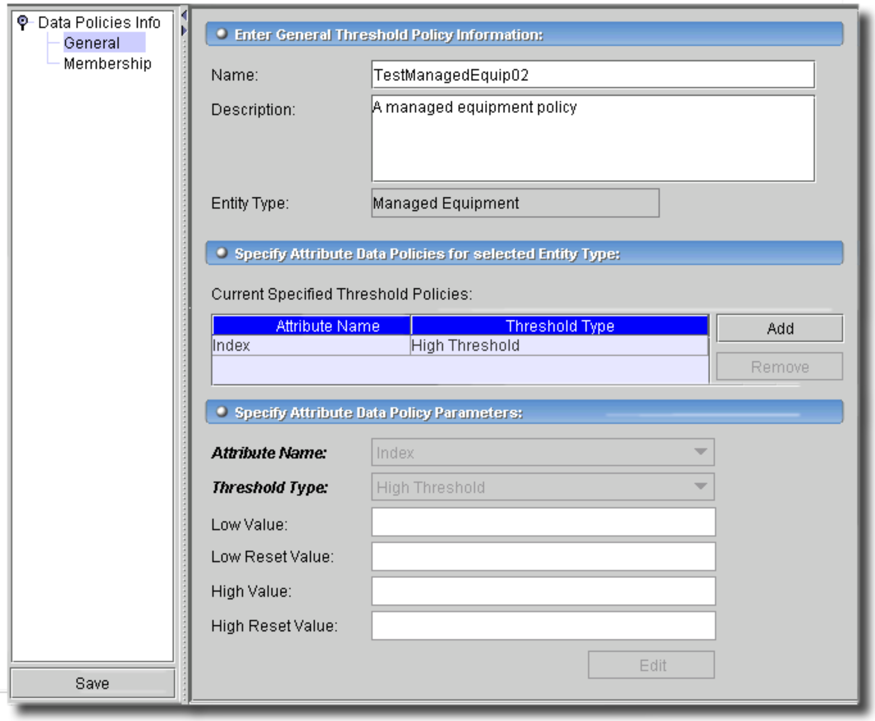
- **Print**—Print the listed items to an Acrobat file. (You must have Acrobat reader installed for this to work properly.) Change the filter and click *Go* to change this printed report's appearance.

- **Help**—Open the context-sensitive help for this screen.

Data Policy Editor - General

This screen creates or alters data policies.

Figure 27-2. Data Policy Editor



Enter General Threshold Policy Information:

Name: TestManagedEquip02

Description: A managed equipment policy

Entity Type: Managed Equipment

Specify Attribute Data Policies for selected Entity Type:

Current Specified Threshold Policies:

Attribute Name	Threshold Type
Index	High Threshold

Specify Attribute Data Policy Parameters:

Attribute Name: Index

Threshold Type: High Threshold

Low Value:

Low Reset Value:

High Value:

High Reset Value:

This screen has the following fields:

- **Name**—A text identifier for the policy.
- **Description**—A text description for the policy.
- **Entity Type**—Select from the entities available in the pick list. These can include *Correlation*, *Interface*, *Link*, *Printer*, *Printer - Input Trays*, *Printer - Output Trays*, *Printer - Toner*, *Process*, and *Vendor*.

Threshold Policies

This table contains the specified threshold policies. Click *Add* to activate the lowest panel's editor, where you can specify the policy's parameters, or select a policy and click *Remove* to delete it.

Policy Editor

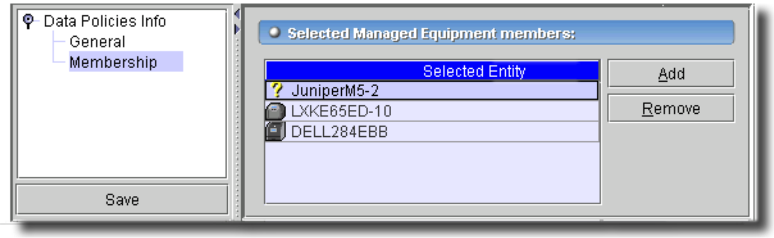
- **Attribute Name**—Select from the pick list. Options vary, depending on the *Entity Type* selected at the top panel of this screen.
- **Threshold Type**—Select from *High Threshold*, or *Low Threshold*, and enter the *High / Low Value* and *High / Low Reset Value*. Reset values reset the data notification for the selected parameter. If equipment exceeds the Low Threshold at 10, and something makes that parameter 40 when the Low Reset value is only 30, then the application clears the Low Threshold event.

Click *Save* to preserve your edits.

Data Policy Editor - Membership

This screen lets you manage the equipment membership monitored by your data policies.

Figure 27-3. Data Policy Editor - Membership



Click *Add* to select equipment where you want to apply the policy configured in the Data Policy Editor - General screen. Select a piece of equipment and click *Remove* to delete it.

Click *Save* to preserve your edits.

28

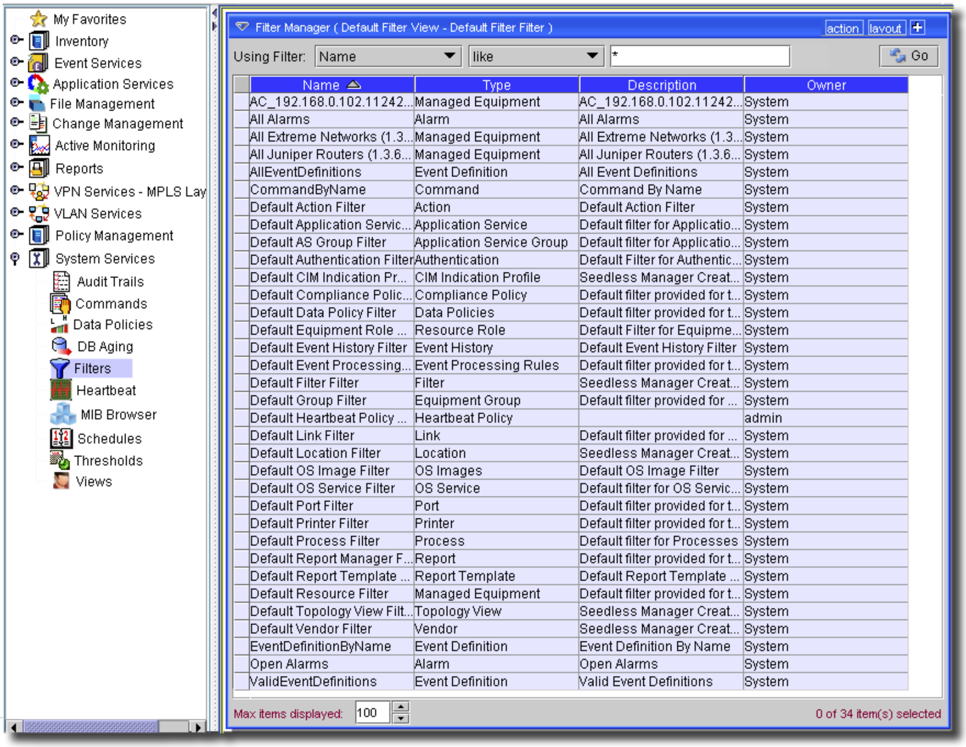
Filters

Filters Manager

Managers typically use filters to reduce the number of records shown.You can configure the filters that appear by default in the application's managers with the Filters screen, and through the key icon at the top of many managers.

Access Filters screen through the navigation window or through *Settings -> Configuration -> Filter Config*.

Figure 28-1. Filters screen



Filter Manager (Default Filter View - Default Filter Filter)

Using Filter: Name like *

Name	Type	Description	Owner
AC_192.168.0.102.11242...	Managed Equipment	AC_192.168.0.102.11242...	System
All Alarms	Alarm	All Alarms	System
All Extreme Networks (1.3...	Managed Equipment	All Extreme Networks (1.3...	System
All Juniper Routers (1.3.6...	Managed Equipment	All Juniper Routers (1.3.6...	System
AllEventDefinitions	Event Definition	All Event Definitions	System
CommandByName	Command	Command By Name	System
Default Action Filter	Action	Default Action Filter	System
Default Application Servic...	Application Service	Default filter for Applicatio...	System
Default AS Group Filter	Application Service Group	Default filter for Applicatio...	System
Default Authentication Filter	Authentication	Default Filter for Authentic...	System
Default CIM Indication Pr...	CIM Indication Profile	Seedless Manager Creat...	System
Default Compliance Polic...	Compliance Policy	Default filter provided for t...	System
Default Data Policy Filter	Data Policies	Default filter provided for t...	System
Default Equipment Role ...	Resource Role	Default Filter for Equipme...	System
Default Event History Filter	Event History	Default Event History Filter	System
Default Event Processing...	Event Processing Rules	Default filter provided for t...	System
Default Filter Filter	Filter	Seedless Manager Creat...	System
Default Group Filter	Equipment Group	Default filter provided for ...	System
Default Heartbeat Policy ...	Heartbeat Policy		admin
Default Link Filter	Link	Default filter provided for ...	System
Default Location Filter	Location	Seedless Manager Creat...	System
Default OS Image Filter	OS Images	Default OS Image Filter	System
Default OS Service Filter	OS Service	Default filter for OS Servic...	System
Default Port Filter	Port	Default filter provided for t...	System
Default Printer Filter	Printer	Default filter provided for t...	System
Default Process Filter	Process	Default filter for Processes	System
Default Report Manager F...	Report	Default filter provided for t...	System
Default Report Template ...	Report Template	Default Report Template ...	System
Default Resource Filter	Managed Equipment	Default filter provided for t...	System
Default Topology View Filt...	Topology View	Seedless Manager Creat...	System
Default Vendor Filter	Vendor	Seedless Manager Creat...	System
EventDefinitionByName	Event Definition	Event Definition By Name	System
Open Alarms	Alarm	Open Alarms	System
ValidEventDefinitions	Event Definition	Valid Event Definitions	System

Max items displayed: 100

0 of 34 item(s) selected

The filter at the top of this manager manages which filters appear in this screen. See Filtering and Searching on page 158 for more about that filter. For the *Basic Filter Editor*, in screens like *Group Operations*, click the filter (funnel) icon to edit an existing or create a new filter.

To create a new filter or modify an existing one in Filter Manager, you can click *Action -> New* or *Action -> Open* (to edit a selected existing filter), or you can click on the Filter command button (a funnel icon that appears in various locations, depending the screen). You can create or edit filters with the following editors.

- Filter Editor—For newer screens.
- Basic Filter Editor—For basic screens.

See also Filter Wildcards on page 738 for supported features within filters.

This application also supports view filters as described in Filtering and Searching on page 158.

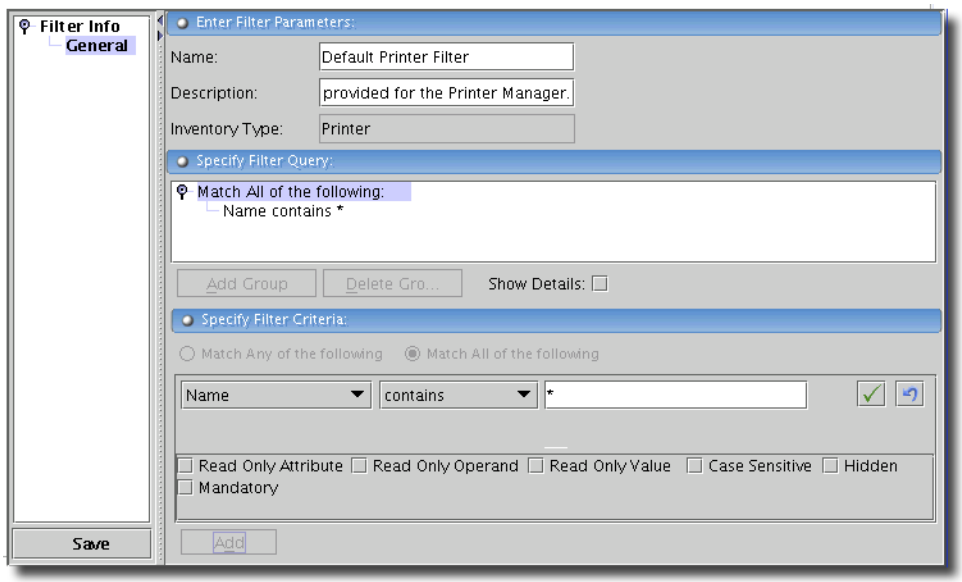
NOTE:

Filters created by one user are not visible to another user.

Filter Editor

When you click the *New* menu at the top of the filter manager, you can elect to create new (or with *Open*, edit existing) filters.

Figure 28-2. Filter Editor



Filter Info
General

Enter Filter Parameters:

Name: Default Printer Filter

Description: provided for the Printer Manager.

Inventory Type: Printer

Specify Filter Query:

Match All of the following:
Name contains *

Show Details: □

Specify Filter Criteria:

○ Match Any of the following ● Match All of the following

Name ▼ contains ▼ *

□ Read Only Attribute □ Read Only Operand □ Read Only Value □ Case Sensitive □ Hidden
□ Mandatory

For example, you could request all equipment where the *Name* field contains the word “oware” or a wildcard (asterisk [*] means any combination of characters). The *Add* / *Delete* group buttons let you use group functionality, creating advanced filtering. For example you could match all values within Group 1 but any values within Group 2. For example, Group 1 could match “vendor = 'Dell'” and Group 2 could match “model number starts with '20' OR firmware version contains '2'”.

Before you begin creating a new filter, you must click *[Select an Inventory Type]*, and use the pick list to configure the manager screens where this filter can appear.

After you have selected the *Inventory Type*, you can add criteria for the filter that are specific to that type. To add criteria, first click *Add Group* in the upper panel. The *Filter Attributes* radio buttons (*Match Any of the Following* or *Match All of the Following*) determine the next part of the filter's operation.

In the Filter Editor, you can specify attributes for filtering when you click *Add* at the bottom of this screen. Enter attribute / operand / value combinations after clicking *Add*. To edit an existing filtered item, select the node above it and click the *Edit Filter Criteria* button (sheet of paper icon) in the lowest panel. You can delete it with the red X.

These filters can have attributes or operands that are *Read Only*, or *Hidden*. The *Show Details* check box displays these qualities to the right of listed criteria as they appear in the upper panel. This information displays codes for additional filtering properties you can select when you create the filter components in the lowest panel.

Available detail codes depend on the data type filtered. The *AND*ed or *OR*ed sum of the filter components' codes appears at the top level node. The codes for these attributes are the following:

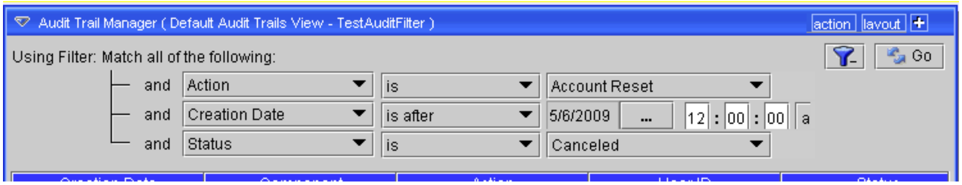
Code	Meaning	Comment
H or V	Hidden / Visible	
ROO or WRO	Read Only / Read-Write Operand	
ROA or WRA	Read Only / Read-Write Attribute	
ROV or RWV	Read Only / Read-Write Value	Grays out the operand and attribute checkboxes since those are not functional if you make this read-only.
ROO or WRO	Read Only / Read-Write Operand	
ROA or WRA	Read Only / Read-Write Attribute	
M or O	Mandatory / Optional	
EL or IL	Exclude / Include Low	Valid only when you select a range of values. This determines whether you include or exclude the endpoint of the range

Code	Meaning	Comment
EH or IH	Exclude / Include High	Valid only when you select a range of values. This determines whether you include or exclude the endpoint of the range
CS or NC	Case Sensitive / Not Case Sensitive	Does not appear for numeric values.
ML or NM	Multi-line Support / No Multi-Line Support	Filter on multiple-line values (or not).

When you select *Read Only* for an attribute, operand or value, some additional impacts are that, for example, reports ordinarily let you alter filters when you manually execute them, but if they have only read-only filtering, then the report executes immediately without a pause to alter filtering.

When you do *not* specify *Read Only*, then click the Filter icon when it displays a plus (+), the filter expands to display all attributes and operands as drop-down lists.

Figure 28-3. Expanded Filter in a Manager



Audit Trail Manager (Default Audit Trails View - TestAuditFilter)

Using Filter: Match all of the following:

and Action is Account Reset

and Creation Date is after 5/6/2009 ... 12 : 00 : 00 a

and Status is Canceled

You can then alter the filter's composition with those drop-downs. You can contract the filter to its original, smaller size by clicking the Filter icon when it appears with a minus (-).

Filter Wildcards

This application supports wildcard characters for specifying entity searches of the various list fields. When applying filters to lists of objects in the application, you can use the listed wildcard characters as part of the search criteria:

Character	Usage
*	Matches any sequence of characters in a string, including an empty sequence. In new filters, this does not work by itself. Use a blank space instead.
?	Matches any single character in a string.

Filters appear at the top of most managers and inventory screens, to limit displayed items.

Filter Wildcard Examples

In Basic Filters, if you want to match *white, which* and *whole*, then enter the filter string *wh**. In new filters, use *contains* and *wh*.

If you want to match *fee*, *fie*, and *foe*, then enter the filter string *f?e*.

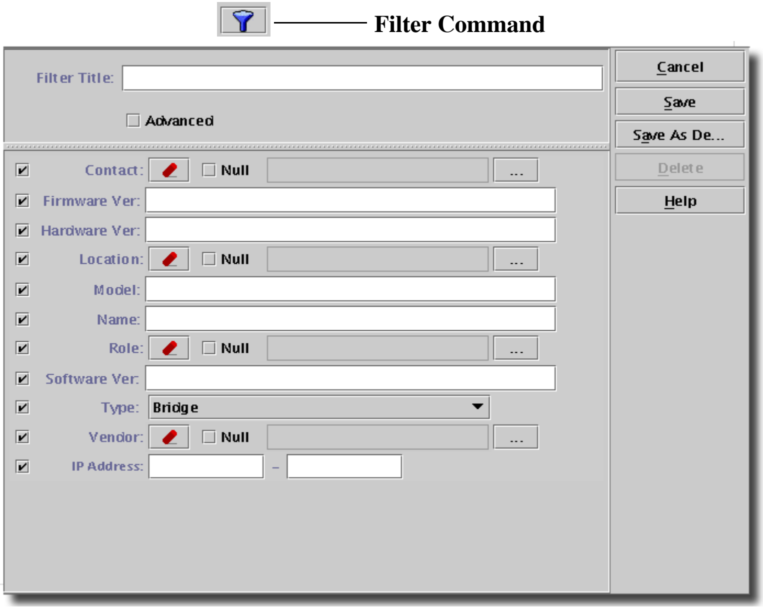
You can also combine filter wildcards. The string *P?n** would match *Pine*, or *Pinetop*, for example.

Basic Filter Editor

In addition to clicking *New* in the Filters screen, you can create a new filter by clicking the *Filter Command Button* (looks like a blue funnel) at the top of a manager, and then selecting ****New**** from the filter pick list at the top the next screen. Enter a name in the empty *Filter Name* field that replaces the pick list, and enter filter criteria where appropriate. To modify an existing filter, select it from the *Filter Name* drop-down list and modify the appropriate filter criteria.

The data screen configures the actual filter. Its appearance varies, depending on the manager from which you configure the filter.

Figure 28-4. Key Icon Filter Editor



Filter Title:

☐ Advanced

☑ Contact: ☐ Null ...
☑ Firmware Ver:
☑ Hardware Ver:
☑ Location: ☐ Null ...
☑ Model:
☑ Name:
☑ Role: ☐ Null ...
☑ Software Ver:
☑ Type: Bridge
☑ Vendor: ☐ Null ...
☑ IP Address: –

NOTE:

The filter may contain custom fields (see Inventory Config on page 174

Check the box to the left of each item to use it in the filter. Notice that fields are disabled, unless you check this box. The *Null* checkbox to the right of the field eraser means this filter selects only items without that value.

The following items are potential fields for the filter to match:

- **Contact**—Click on the command button to select a contact.

- **Firmware ver**—The firmware version (text).

- **Hardware ver**—The hardware version (text).

- **Location**—Click on the command button to select a location.

- **Model**—The equipment's model designation (text).

- **Name**—Enter a name or portion of a name.

- **Role**—From the drop-down list, select an equipment role.

- **Software ver**—The software version (text).

- **Type**—Select an equipment type from the drop-down list.

- **Vendor**—Click on the command button to select a vendor.

- **IP Address**—The IP Address (range) of the device (text).

Click on *Set as Default* to set the selected filter as the default view. Clicking *Set as Default* means the configured filter automatically appears each time this screen opens. Click on *Save* to save and apply the filter. The list of items appears based on the filter you created, and the manager from which you open the filter.

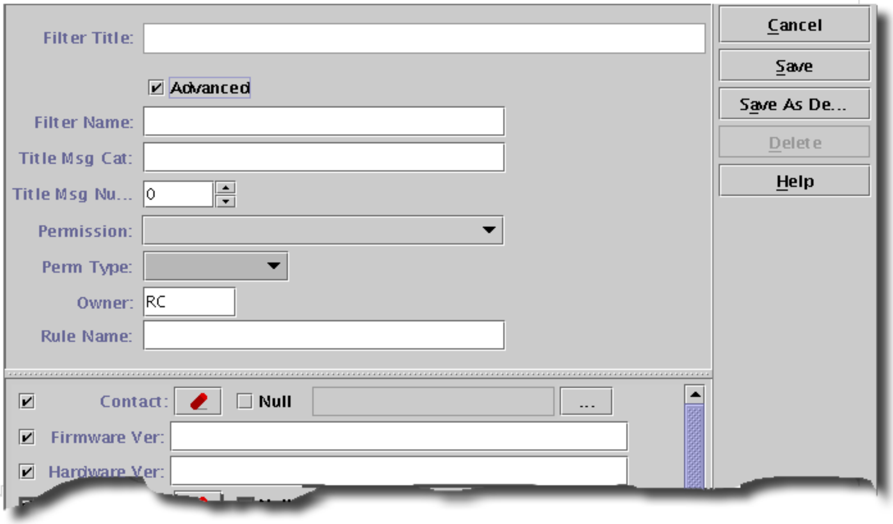
NOTE:

A default set of filters comes with the application. Criteria vary, depending on the manager.

Advanced Settings

This portion of the Filter Editor screen appears when you check the *Advanced* checkbox in the Filter editor. This checkbox only appears when you select a ****New**** filter, from the *Filter Title* pick list. Permission to configure these aspects of filtering is typically confined to application administrators and developers. When permissions are unavailable, the *Advanced* checkbox does not appear.

Figure 28-5. Filter Advanced Settings



☑ Advanced

Title Msg Nu...: 0

Owner: RC

☑ Contact

☑ Firmware Ver

☑ Hardware Ver

This sub-panel the has the following fields:

- **Filter Title**—The title that appears with the filter.

- **Filter Name**—A unique identifier for the filter.

- **Title Msg Cat:**—The message categories that are defined in messages properties file `rcmsgsusenglish`. For Example: `RC_GENERAL, RC_EQUIPMENT, RC_QUERYNAMES`.

- **Title Msg Num**—A read-only field displaying the message number. The message numbers that are defined in messages properties file `rcmsgsusenglish`. For Example: `RC_GENERAL.11, RC_EQUIPMENT.43, RC_QUERYNAMES.10`

- **Permission**—Use the pick list to select you can select the permissions required for this filter to appear, or be applied.

- **Permission Type**—Select a permission type (*Add*, *Delete*, *Execute*, *Read*, *Write*).

- **Owner**—The owner of this filter is the product/component to which this filter belongs; in other words the product/component which creates this filter. For Example “Dell” for Dell, and so on.

- **Rule Name**—The rule name along with its package, which does the query for this filter.

Click *Save* to persist the filter configuration your edits make.

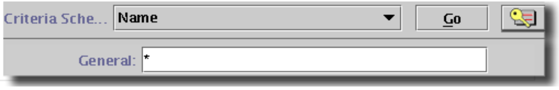
NOTE:

Exporting advanced filter options exports the Title Message category and number, but not the file to which they refer.

Quick Searches

Once you define a filter you can use a Quick Search defined there. For example, to create a Quick Search using Equipment Name, create a Filter called *Search by Name* and check the Name checkbox under the filter criteria. Do not enter a value in the text field. When you return to the Manager, you can see the *Name* field under the Filter drop-down list.

Figure 28-6. Filter Name Field



Criteria Sche... Name

General: *

Enter criteria for the Quick Search and click on *Go*.

29

Heartbeat Policies

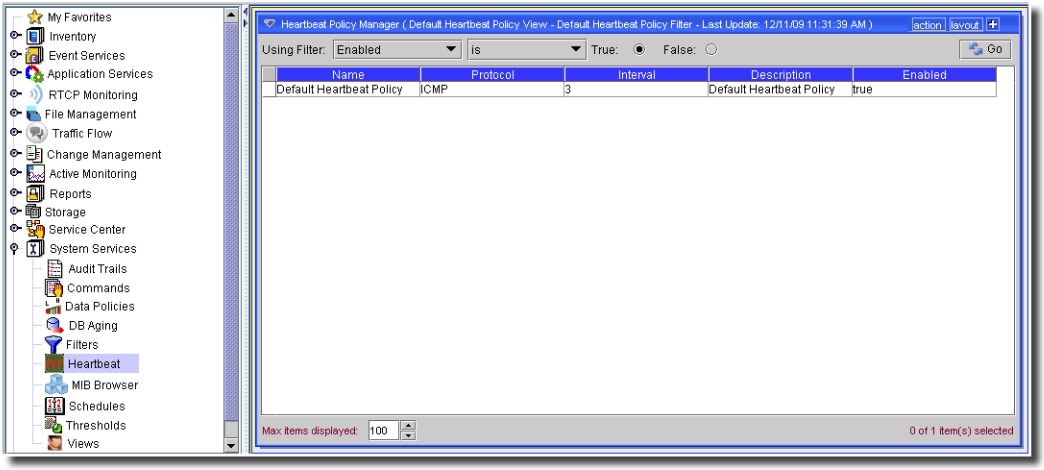
Introducing Heartbeats

Heartbeats are ICMP, SNMP, or HTTP pings to devices. These ensure the device is “alive and well” to respond to network events. (Ping operations pass to the operating system and use its default settings, including TTL.)

Heartbeat Policies

To manage equipment heartbeats more elaborate than ICMP ping, you must create items in the Heartbeat Policy Manager. Open this with the Navigation Window, or *File -> Open -> System Services -> Heartbeat Policies*

Figure 29-1. Heartbeat Policies



Heartbeat Policy Manager (Default Heartbeat Policy View - Default Heartbeat Policy Filter - Last Update: 12/11/09 11:31:39 AM)

Using Filter: Enabled ▼ is ▼ True: ● False: ○

Name	Protocol	Interval	Description	Enabled
Default Heartbeat Policy	ICMP	3	Default Heartbeat Policy	true

Max items displayed: 100

0 of 1 item(s) selected

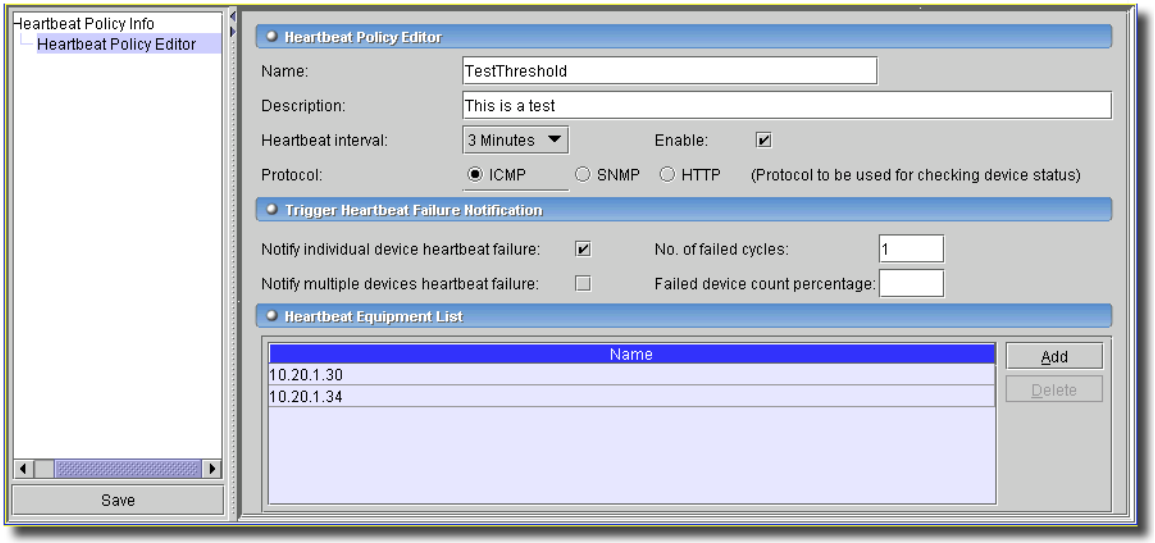
This manager displays listed heartbeat policies according to the filter selected at the top of the screen. Click *Go* to refresh that screen. Click *New* to create a new heartbeat policy, or *Open* to edit a selected policy. Click *Delete* to remove a selected policy. When you click *New* or *Open*, the Heartbeat Policy Editor opens.

Some policies may be seeded with the OpenManage Network Manager application options.

Heartbeat Policy Editor

This editor lets you configure heartbeats.

Figure 29-2. Heartbeat Policy Editor



Name: TestThreshold

Description: This is a test

Heartbeat interval: 3 Minutes Enable: ☑

Protocol: ● ICMP ○ SNMP ○ HTTP (Protocol to be used for checking device status)

Notify individual device heartbeat failure: ☑ No. of failed cycles: 1

Notify multiple devices heartbeat failure: □ Failed device count percentage:

Name
10.20.1.30
10.20.1.34

This screen has the following fields:

Heartbeat Policy Editor

- **Name**—A unique identifier for the heartbeat policy.
- **Description**—A text description for the heartbeat policy.
- **Heartbeat interval**—Select from 1 - 60 minutes with the pick list.
- **Enable**—Check to enable this heartbeat policy.
- **Protocol**—Select the protocol to use when checking device's status with the radio buttons. Select from among the available protocols: *ICMP, SNMP,* or *HTTP.*

Trigger Heartbeat Failure Notification

The following parameters configure the kinds of notifications that can occur for this policy.

- **Notify individual device heartbeat failure**—Checking this sends a trap notifying users of an individual device's failure to respond to a heartbeat.
- **Notify multiple devices heartbeat failure**—Checking this sends a trap notifying users of the listed group of devices' failure to respond to a heartbeat.
- **No. of failed cycles**—The failure must exceed the configured threshold before the application produces a notification.

- **Failed Device percent**—(optional) The percentage of devices that must fail before the application issues a heartbeat failed notification.

Heartbeat Equipment List

Click A*dd* to select equipment for this heartbeat policy. Select listed equipment and click *Delete* to remove them.

NOTE:

Equipment deleted from OpenManage Network Manager is also deleted from Heartbeat policies.

Click *Save* to preserve this policy.

30

Schedules

Introducing Scheduling

You can schedule a variety of actions with this application. The following sections describe how to do this.

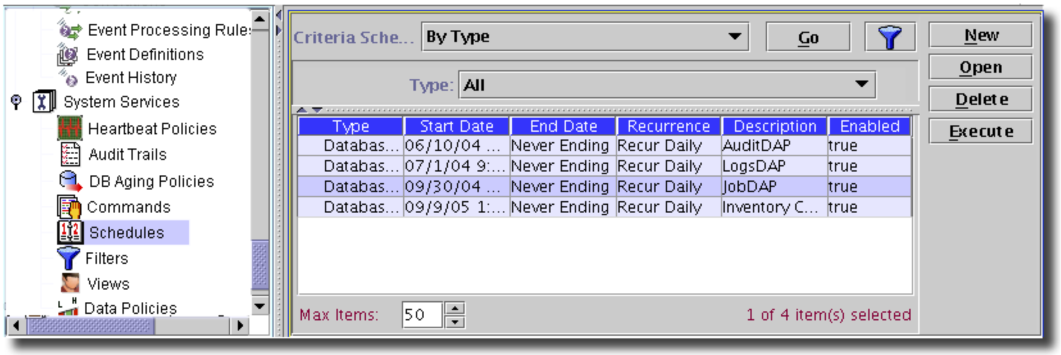
NOTE:

Use Group Ops to schedule operations on more than one device at the same time instead of scheduling multiple individual operations at the same time.

Using Schedules

Use the Schedules screen to set the start and stop time, as well as any recurrence pattern for processes that support this feature. You can *Edit*, *Execute* and *Delete* scheduled items in the Schedules screen (under the *System Services* node of the navigation window or from *File* -> *Open* -> *System Services* -> *Schedules*).

Figure 30-1. Schedules screen



Criteria Sche... By Type

Type: All

Type	Start Date	End Date	Recurrence	Description	Enabled
Databas...	06/10/04 ...	Never Ending	Recur Daily	AuditDAP	true
Databas...	07/1/04 9:...	Never Ending	Recur Daily	LogsDAP	true
Databas...	09/30/04 ...	Never Ending	Recur Daily	JobDAP	true
Databas...	09/9/05 1:...	Never Ending	Recur Daily	Inventory C...	true

Max Items: 50

1 of 4 item(s) selected

This manager uses typical filtering (see Basic Filter Editor on page 739). You can also select *File* -> *Import* and *Export* back up schedules or configure other systems.

CAUTION:

Best practice is to allow plenty of time between jobs rather than concentrating them within a short period. This conserves computing resources and avoids bottlenecks. While the application lets you schedule many jobs within a short period, the risk is that they may take longer than the time allotted. If that occurs, the application works on the jobs sequentially, creating a queue of unfinished work that it continues to process. Processing this backlog during something like a network slowdown may cause resource issues within the application server itself.

New Schedules

When you click *New*, the application prompts you for the type of schedule to create (available types depend on your installation). Depending on the type you select, the next screen changes. *Device Resync* and *Device Discovery* are the default scheduled task types available. The Schedule Info on page 750 is common to all schedules. You can schedule several things, including the following tasks:

- **Database Aging Policy—**Policy implementation. See Chapter 25, DB Aging.
- **Device Discovery**—Select a Resource Discovery Profile, then enter what's described in Schedule Info on page 750.
- **Device Resync**—See Resynchronization, below.
- **Firmware Download—**Schedules updates from supported Firmware suppliers. See Firmware Download on page 749.
- **Group Operation**—Schedule a group operation.
- **Inventory Reports**—This allows you to schedule already configured reports.
- **Link Discovery**— See Discovering Links on page 642 for more information about what you are configuring here.

The following appear if you have installed the optional File Management:

- **Configuration File Restore**—Push backed up configuration file down to device.
- **Configuration File Backup**—Backup configuration files from the device.
- **OS Image Deploy**—Push operating system (or patch to O/S) to device.

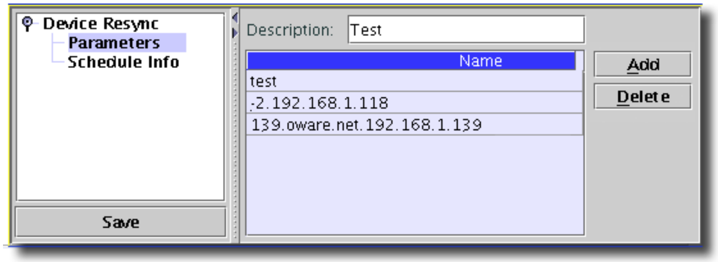
NOTE:

If you start equipment-specific tasks from the Schedule Manager, you must select the equipment in addition to selecting the schedule parameters with the command (...) button next to the appropriate field in the scheduler screens.

Resynchronization

If you select *Device Resync* when creating a new schedule, you can select devices to re-query (resync) so the database contains the latest device configuration.

Figure 30-2. Resynchronization Scheduler



Description: Test

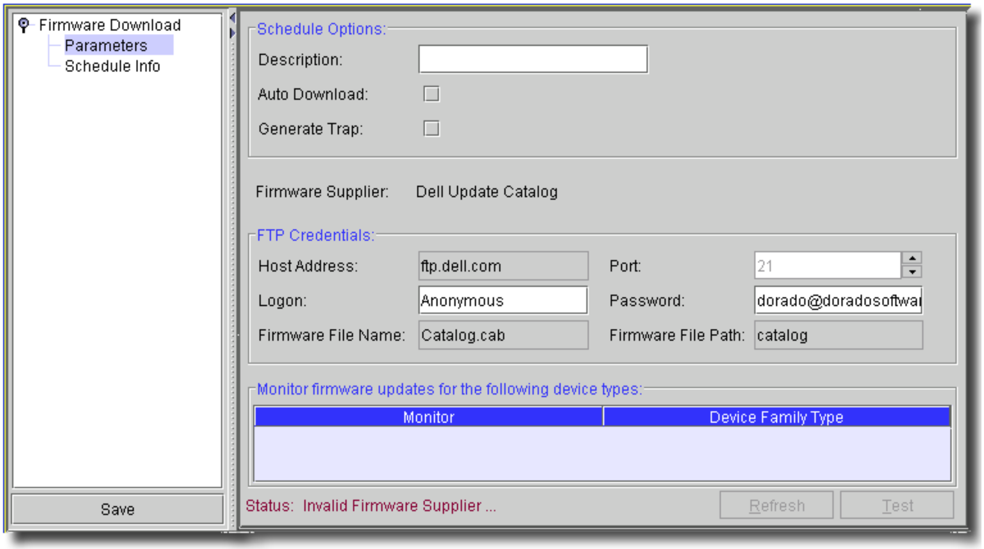
Name
test
-2.192.168.1.118
139.oware.net.192.168.1.139

Type the *Name* of the schedule, then click *Add* to select devices for this resynchronization. The *Schedule Info* tab is where you set the schedule times. See Schedule Info on page 750 for details.

Firmware Download

If you select this scheduling firmware download, and have a supplier who supports automated downloads of firmware, you can configure that download with this screen.

Figure 30-3. Schedule Firmware Download Parameters



Description:

Auto Download: □

Generate Trap: □

Firmware Supplier: Dell Update Catalog

Host Address: ftp.dell.com

Port: 21

Logon: Anonymous

Password: dorado@doradosoftwar

Firmware File Name: Catalog.cab

Firmware File Path: catalog

Monitor	Device Family Type

Status: Invalid Firmware Supplier ...

You can configure the following with this screen:

Schedule Options

- **Description**—A text identifier for the scheduled download.

- **Auto Download**—Check to activate automated download.

- **Generate Trap**—Check to activate trap generation on download.

- **Firmware Supplier**—The vendors known to support this feature (currently: none support scheduled downloads).

FTP Credentials

- **Host Address / Port**—The address and port for FTP connection. The default port is 21.
- **Logon / Password**—The FTP logon / password combination.
- **Firmware File Name / Path**—The name of the firmware file and path.

Monitor firmware updates for the following device types

Select (or multi-select with Ctrl+Click) devices for which you want firmware updates.

Click *Refresh* to update the list, and *Test* to test the download.

Discovery

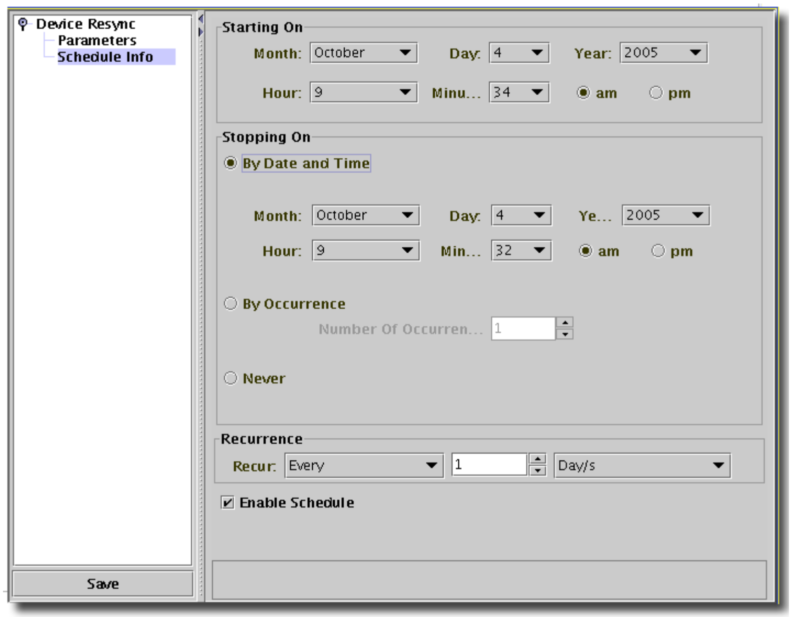
If you schedule *Discovery*, then you can select a discovery profile (see Discovery on page 187), then enter the information in Schedule Info on page 750.

Schedule Info

The *Schedule Info* screen is the same, regardless of the kind of task you schedule. Consult the appropriate application manuals for information about parameters screens. Click the *Save* icon (or *File* -> *Save*) to confirm your selection. Click the *Close* icon (*File* -> *Close*, or Ctrl + F4) to close without saving.

You can also schedule items from the items' creation dialog. When you create a new schedule, from whatever location, you can see the *Schedule* dialog's *Schedule Info* screen.

Figure 30-4. **Schedule Info Screen**



Device Resync
Parameters
Schedule Info

Starting On
Month: October Day: 4 Year: 2005
Hour: 9 Minu... 34 ● am ○ pm

Stopping On
● By Date and Time
Month: October Day: 4 Ye... 2005
Hour: 9 Min... 32 ● am ○ pm
○ By Occurrence
Number Of Occurren... 1
○ Never

Recurrence
Recur: Every 1 Day/s

☑ Enable Schedule

Save

The following are the fields on the Schedule Info dialog:

- **Starting On**—This section defines the date and time when the schedule becomes active. Select values for Month, Day, Year, Hour, and Minute from the appropriate drop-down lists.
- **Stopping On**—This section defines when the schedule stops being active. Select one of the following options:

  By Date and Time—Select this option, then select the Month, Day, Year, Hour, and Minute from the appropriate drop-down lists.

  By Occurrence—Select this option, then specify the number of occurrences of the scheduled process after which it becomes inactive.

  Never—Select this option to specify that the scheduled process never stop.
- **Recurrence**—The Recurrence section determines how often the schedule recurs in relation to the settings in the Stopping On section.

  Recur—Select a recurrence option. Available options are *Every, Only Once* (at the scheduled time), *Increment* (by minute), *Only at Startup* (in other words, only at application server startup). If you select *Every*, specify an interval. The following are interval options: *Minute/s*, *Weekend Day/s*, *Hour/s*, *Week/s*, *Day/s*, *Month/s*, *Weekday/s*, *Year/s*

CAUTION:
The scheduler calculates the execution interval based on the last execution time. So, if you executed a 24-hour recurring schedule item manually at 2:32 pm, it continues to run at that time each day, even if it was originally scheduled to run at 3 pm daily.

Some items scheduled for execution *Only at Startup* may not perform as expected. For example, this unexpected behavior could occur if a target device was not accessible from the application server. (Scheduling runs from the application server.) Unexpected behavior could occur if the target device was offline.

- **Enable Schedule**—Uncheck this to disable the schedule. By default it is enabled.

Click the *Save* button (or toolbar icon) to save this schedule to the database.

31

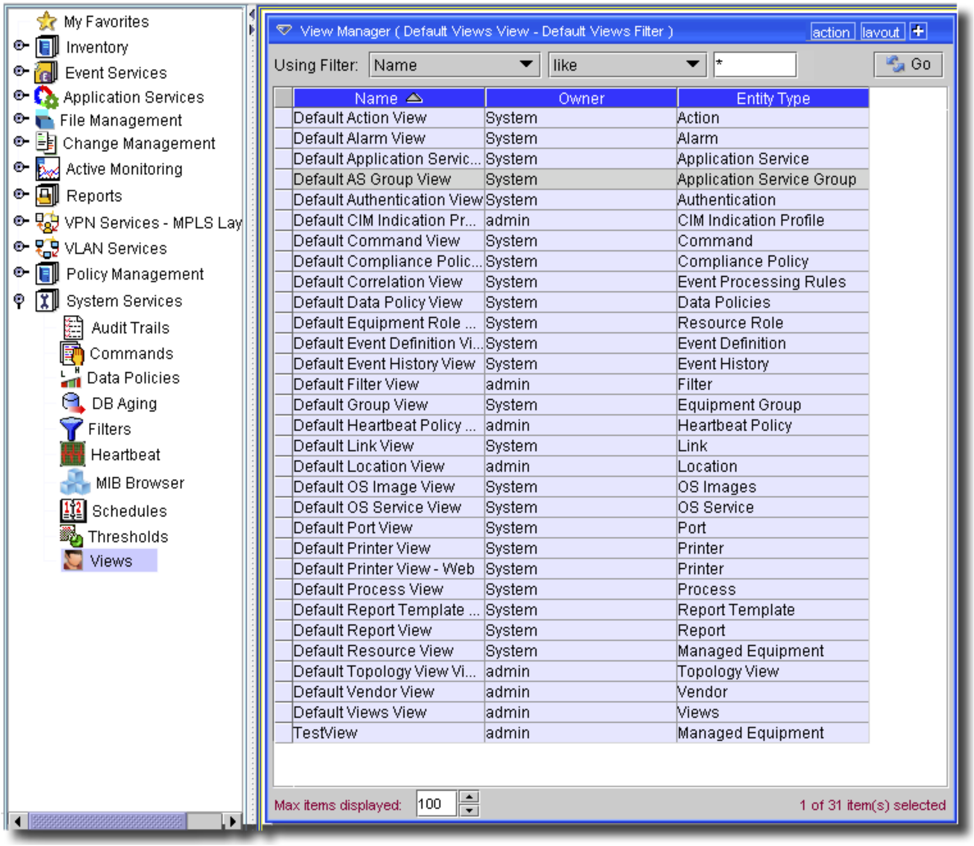
Views

Introducing Views

To further tailor displays to your preferences, you can create and manage views. These specify columns that appear in managers, inventories and other displays.

With the Views screen, you can arrange the screen appearance in managers, specifying visible columns and their order, for some inventory and manager screens.

Figure 31-1. Views screen



Using Filter: Name like *

Name	Owner	Entity Type
Default Action View	System	Action
Default Alarm View	System	Alarm
Default Application Servic...	System	Application Service
Default AS Group View	System	Application Service Group
Default Authentication View	System	Authentication
Default CIM Indication Pr...	admin	CIM Indication Profile
Default Command View	System	Command
Default Compliance Polic...	System	Compliance Policy
Default Correlation View	System	Event Processing Rules
Default Data Policy View	System	Data Policies
Default Equipment Role ...	System	Resource Role
Default Event Definition Vi...	System	Event Definition
Default Event History View	System	Event History
Default Filter View	admin	Filter
Default Group View	System	Equipment Group
Default Heartbeat Policy ...	admin	Heartbeat Policy
Default Link View	System	Link
Default Location View	admin	Location
Default OS Image View	System	OS Images
Default OS Service View	System	OS Service
Default Port View	System	Port
Default Printer View	System	Printer
Default Printer View - Web	System	Printer
Default Process View	System	Process
Default Report Template ...	System	Report Template
Default Report View	System	Report
Default Resource View	System	Managed Equipment
Default Topology View Vi...	admin	Topology View
Default Vendor View	admin	Vendor
Default Views View	admin	Views
TestView	admin	Managed Equipment

Max items displayed: 100

1 of 31 item(s) selected

As with most managers, the top of this screen lets you filter the list of views, limiting it to those most useful for you. See Filtering and Searching on page 158 for more about arranging these filters.

Click *Action* -> *New* to create a new view, or *Open* to edit a selected view. Click *Action* -> *Delete* to remove a selected, listed view, or *Action* -> *Help* to open online help for this screen. As always, the *Action* button menu is a duplicate of the right-click menu.

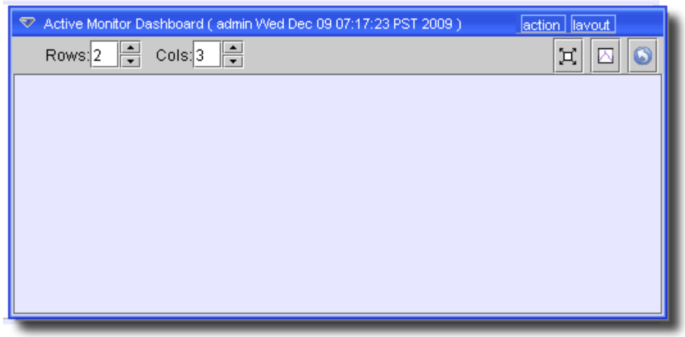
NOTE:

Views created by one user are not visible to another user.

View Editor

When you click *New* or *Open* in view Manager, the View Editor appears.

Figure 31-2. View Editor


Active Monitor Dashboard (admin Wed Dec 09 07:17:23 PST 2009)
action
layout
Rows: 2
Cols: 3

Views apply to some managers (currently Contact, Vendor, Location, Port, and Printer) This screen has the following fields:

- **View Name**—A unique identifier for the view.

- **Inventory Type**—Select the type of inventory on the pick list. The effects of the view modifications are available when you open the manager for this type of inventory.

Select the column attributes for this manager

Below this is a list of available attributes for the selected inventory type's manager. Check the *Selected* column to include a row as the columns that appear in the manager, when open. Select a row and use the *Up/Down* arrows to the right of this list to re-order the list. The *Re-Order* button moves selected columns to the top of those listed.

Click *Save* to preserve the view in the database. When you open the manager for the inventory type selected for the first time, the default view appears. After the first time you open a manager, the last view selected persists. This is connected to the login user. All *Admin* users, for example, would see each others' changes.

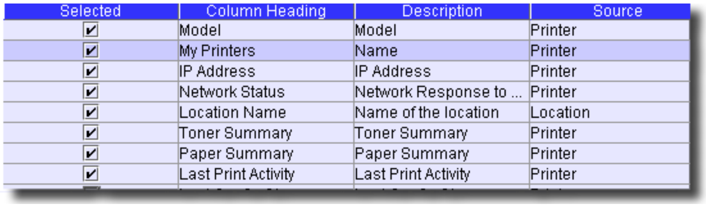
NOTE:

Creating several admin users would preserving selected views. In some managers, altering the default view means all users will see that alteration. If you want a view that is uniquely your own, create a new one.

Column Titles

Column titles that appear in views are editable here, too.

Figure 31-3. Editable Column Titles



Selected	Column Heading	Description	Source
☑	Model	Model	Printer
☑	My Printers	Name	Printer
☑	IP Address	IP Address	Printer
☑	Network Status	Network Response to ...	Printer
☑	Location Name	Name of the location	Location
☑	Toner Summary	Toner Summary	Printer
☑	Paper Summary	Paper Summary	Printer
☑	Last Print Activity	Last Print Activity	Printer

Click the contents of a column in this editor, and start typing to change the title. After you edit a column header this way, you can preserve the view it appears in, and use that view in a layout. Click *Layout* -> *View* -> *Select View* to select the altered view. If you change a layout this way, the altered view remains in the layout. Therefore, you can have several copies of the same set of columns in several views, with headers named differently in each set of columns, and use them to fit various layouts you configure.

32

Active Performance Monitor

This chapter describes Active Performance Monitor. This application's capabilities include configuring Monitors that receive device performance information, Dashboard View Managers that display that information, and Retention Policies that describe how to archive that information. The following sections describe those capabilities in detail.

NOTE:

> See the Administration Section for advice about setting up and configuring performance monitoring, and about configuring a separate database for more responsive performance monitoring.

Active Performance Monitoring (APM) lets you retrieve data from a managed entity and evaluate it against various criteria. This lets you determine health and availability of that equipment. With this application, you can regularly poll critical health characteristics from multiple sources to immediately identify problems with IT devices, networks and services. It also lets you test and identify transactional problems with application & network services.

Advanced monitoring capacities provide domain-specific monitoring of both availability and performance. Monitors isolate key health attributes and characteristics for IT devices, networks and application/network services.

APM stores collected data in a central database and retains it according to a configurable policy (see Creating or Updating a Retention Policy on page 788).

You can display the data collected from monitors by creating graphs and charts. You can also retain it (roll it up) in historical tables. These historical tables hold summaries of the data at various fixed intervals or periods.

Events and alarms can report on a monitor's execution. Monitors report failures as events so operators can see when certain devices are not behaving as expected and why. Events may also report changes in health or availability for an individual device or service.

Some major features of this capability include the following:

- Management of monitoring configurations
- A dashboard view where you can see both current and historical data,
- Management for historical data's roll-up and retention
- Using current and historical data for reporting.

Examples

You can see examples of some of these capabilities in the following:

- SNMP Performance Monitoring Example

See Monitors on page 770 for a more the beginning of a more general description of how to create and configure monitors.

NOTE:

OpenManage Network Manager Active Performance Monitoring supports monitoring SNMP devices and subcomponents that support the IETF Entity MIB Definition (RFC 2037, 2737 and/or 4133) without requiring a specific OpenManage Network Manager Device Driver for that device type.

Retention

The basis of all reporting and dashboard presentations is retained data from established monitors. In other words, each monitor provides a simple schema from which you can produce a chart, graph or report.

To reduce resource impacts, the scope of retained data may exclude some of the collected data. A monitor may have no retained data and only emit events based on transient results in the execution/calculation.

For example, the application can derive a metric from several collected values and you may opt to retain only the derived result.

All monitors rely on a polling engine which provides runtime mediation activities for distributed device interaction at regular intervals.

Several types of monitors are available in this release:

- SNMP Attributes (Interfaces or Scalars) - Scalars are compatible with any SNMP agent, but do not support indexing for table support. This integrates with inventory at the chassis level.
- **SNMP Interface**—Compatible with any SNMP agent supporting the IF-MIB and integrates to managed inventory at the subcomponent level. Supports data in any table indexed by an ifIndex value.
- See Monitor Entities on page 773 and following for more about these monitors.

All monitors have the following behaviors:

- **Retention**—To retain monitor data, a retention policy is associated with the monitor. Monitors may share a retention policy. The retention policy controls how long data is held per roll-up period.

Reachability state—The reachability of the target agent is determined per collection interval. Any state change results in an event which updates the alarm view.

Availability state—The availability of the target is determined per collection interval. Availability is retained according to the monitor retention policy. Any state change results in an event which updates the alarm view.

Calculated Metrics—Any numeric values collected by the monitor may be used to produce derived metrics. A metric is defined by an algebraic formula which may include collected values.

- Thresholds—A collected value or a derived metric supports defined value ranges. Charts reflect these defined ranges when plotting data. The application may generate threshold alarms when the current value(s) falls in a different range than previous value(s). You can configure an average over n values or n consecutive values for range assessment.

  You can retain range results to support trending. For example, how often an interface has been overused.

- **Fault handling**—If the monitor fails to determine reachability, the application generates an appropriate alarm. If the monitor fails to collect all the data as configured, the application generates an alarm.

SNMP Performance Monitoring Example

You can actively monitor performance, as described in this section, or you can monitor event and alarm activity. To set up a performance monitor, follow these steps:

1 Create an SNMP Monitor

2 Create a Dashboard View

3 Install a Monitor in the View

NOTE:

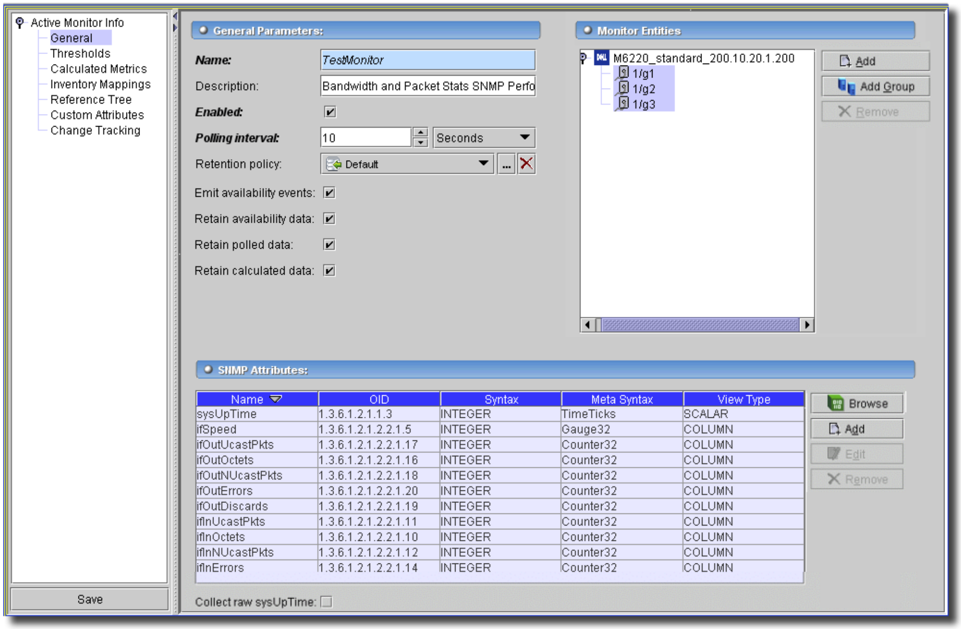
You can use the standard SNMP Interfaces: Performance Monitor - Bandwidth to make capacity planning decisions, and be proactive in configuring your network.

Create an SNMP Monitor

1 Open the *Active Monitoring* -> *Monitor* manager, and create a new monitor with *action* -> *New*, or edit an existing SNMP monitor.

2 Select the type of monitor in the next screen. For this example, we create an *SNMP Interfaces: Performance Monitor - All* monitor. Consult the online help for more specific instructions about other types of monitors. This monitor can be a template for other, modified monitors.

3 In the *General* screen, enter a name (here “TestMonitor”), check *Enabled*, enter a polling interval (here 1 minute, the default). For this example, check *Retain polled data* and accept the remaining defaults for checkboxes and the retention policy.



Name: TestMonitor

Description: Bandwidth and Packet Stats SNMP Perfo

Enabled: ☑

Polling interval: 10 Seconds

Retention policy: Default

Emit availability events: ☑

Retain availability data: ☑

Retain polled data: ☑

Retain calculated data: ☑

M6220_standard_200.10.20.1.200
1/g1
1/g2
1/g3

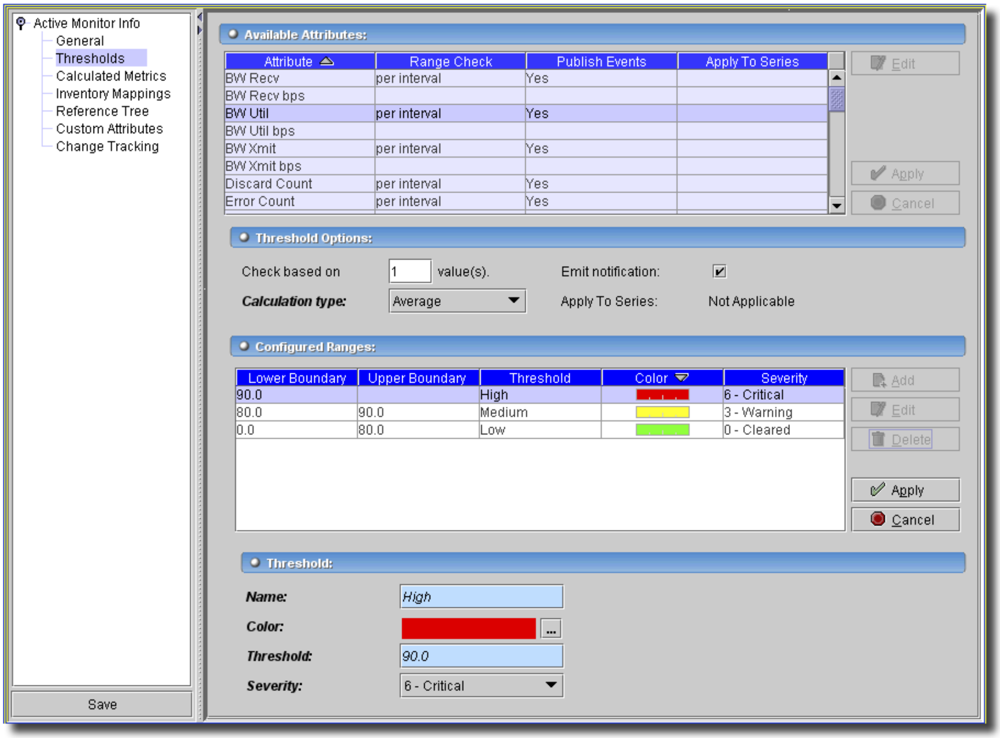
Name	OID	Syntax	Meta Syntax	View Type
sysUpTime	1.3.6.1.2.1.1.3	INTEGER	TimeTicks	SCALAR
ifSpeed	1.3.6.1.2.1.2.2.1.5	INTEGER	Gauge32	COLUMN
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	INTEGER	Counter32	COLUMN
ifOutOctets	1.3.6.1.2.1.2.2.1.16	INTEGER	Counter32	COLUMN
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18	INTEGER	Counter32	COLUMN
ifOutErrors	1.3.6.1.2.1.2.2.1.20	INTEGER	Counter32	COLUMN
ifOutDiscards	1.3.6.1.2.1.2.2.1.19	INTEGER	Counter32	COLUMN
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	INTEGER	Counter32	COLUMN
ifInOctets	1.3.6.1.2.1.2.2.1.10	INTEGER	Counter32	COLUMN
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12	INTEGER	Counter32	COLUMN
ifInErrors	1.3.6.1.2.1.2.2.1.14	INTEGER	Counter32	COLUMN

Collect raw sysUpTime: □

You can accept the default *SNMP Attributes*, or alter them to include fewer or more attributes (click *Add* or *Remove* next to the attributes). For the sake of this example, we accept the default list of attributes to monitor.

4 Select the interfaces you want to monitor by clicking *Add* in the top right corner of the screen. A selection screen appears, when you do. You must typically select a device in the upper panel, then select at least one an interface in the lower one. You can multi-select by left-clicking while holding down the Ctrl key. You can also click *Add Group* if you have previously created a group.

5 In the *Thresholds* screen, examine existing thresholds by clicking on the listed threshold in the upper panel, then clicking *Edit*. For example *BW Util* (utilized bandwidth) has thresholds at 90% (High, Critical), 80% (Medium, Warning), and 0% (Low, Cleared). When the data crosses thresholds, the monitor reacts.



Attribute	Range Check	Publish Events	Apply To Series
BW Recv	per interval	Yes	
BW Recv bps			
BW Util	per interval	Yes	
BW Util bps			
BW Xmit	per interval	Yes	
BW Xmit bps			
Discard Count	per interval	Yes	
Error Count	per interval	Yes	

Check based on 1 value(s).
Emit notification: ☑
Calculation type: Average
Apply To Series: Not Applicable

Lower Boundary	Upper Boundary	Threshold	Color	Severity
90.0		High	🟥	6 - Critical
80.0	90.0	Medium	🟨	3 - Warning
0.0	80.0	Low	🟩	0 - Cleared

Name: High
Color: 🟥
Threshold: 90.0
Severity: 6 - Critical

Available attributes depend on the type of monitor you are creating. Notice that if you click *Edit* in the upper *Attribute* panel, you can alter whether crossing this threshold emits a notification (an alarm that would appear on the Alarm panel), the type of calculation, and so on. You can even alter existing thresholds, by selecting one, then clicking *Edit* to the right of the selected threshold.

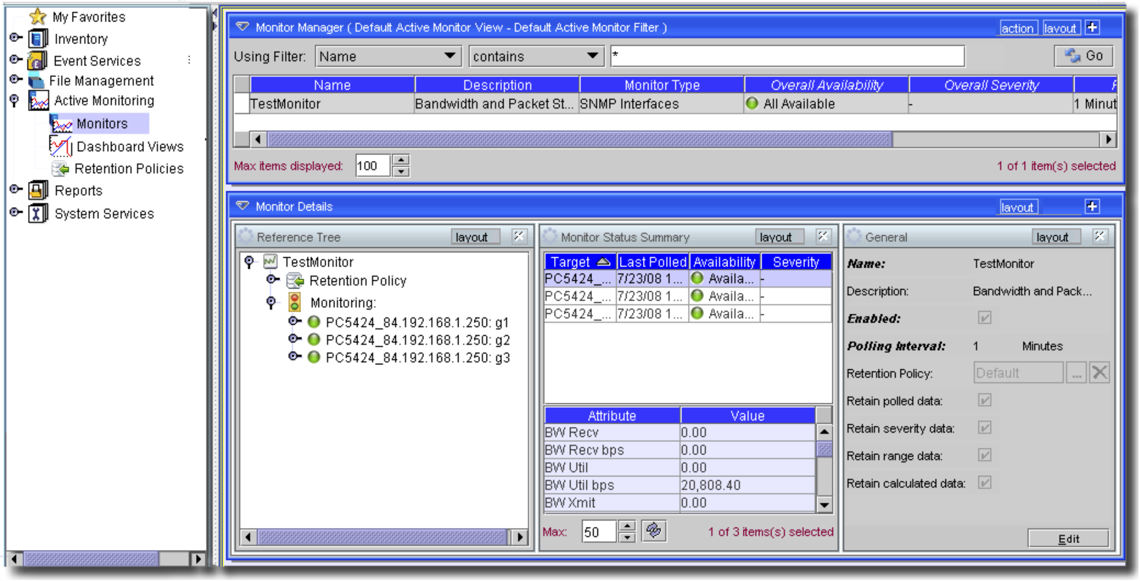
For the sake of this monitor, we will only examine these capabilities, not alter any thresholds. Click *Cancel* (twice) to return this screen to its original appearance.

NOTE:

If a threshold's counter is an SNMP Counter32 (a 32-bit counter) monitoring can exceed its capacity with a fully utilized gigabit interface in a relatively short period of time. The defaults configured in this monitor account for this, but if you know that this is an issue, you can probably configure the monitor to account for it too.

After taking a look at Thresholds no more configuration is required. Notice, however, that you can also configure *Metrics* on another screen in this editor to calculate additional values based on the monitored attributes. Consult online help for more information about the other screens and their capabilities.

6 Click *Save* and the monitor is now active.



Monitor Manager (Default Active Monitor View - Default Active Monitor Filter)

Using Filter: Name contains *

Name	Description	Monitor Type	Overall Availability	Overall Severity	F
TestMonitor	Bandwidth and Packet St...	SNMP Interfaces	● All Available	-	1 Minut

Max items displayed: 100

1 of 1 item(s) selected

Monitor Details

TestMonitor
Retention Policy
Monitoring:
PC5424_84.192.168.1.250: g1
PC5424_84.192.168.1.250: g2
PC5424_84.192.168.1.250: g3

Target	Last Polled	Availability	Severity
PC5424_...	7/23/08 1...	● Availa...	-
PC5424_...	7/23/08 1...	● Availa...	-
PC5424_...	7/23/08 1...	● Availa...	-

Attribute	Value
BW Recv	0.00
BW Recv bps	0.00
BW Util	0.00
BW Util bps	20,808.40
BW Xmit	0.00

Max: 50

1 of 3 items(s) selected

Name: TestMonitor
Description: Bandwidth and Pack...
Enabled: ☑
Polling Interval: 1 Minutes
Retention Policy: Default
Retain polled data: ☑
Retain severity data: ☑
Retain range data: ☑
Retain calculated data: ☑

Notice that the *Availability* icon appears at the top of this screen in the monitor's row to indicate a responding monitor. When you select the monitor, that same icon appears for each interface you selected in the detail panels in the lower part of the screen. These detail panels include information about the monitors status, performance metrics and bandwidth utilization.

Click on an interface in the *Monitor Status Summary* detail panel, and the attribute values for that device appear in the lower half of the detail panel.

NOTE:

Values displayed in the Overall Availability column of the Monitor Manager do not automatically refresh and may be out of date. The value displayed arrives when you execute the manager's filter and does not change until you manually refresh the manager display (click Go). Note that up-to-date individual target availability data appears in a detail panel beneath the tabular view and does refresh automatically.

Create a Dashboard View

1 To see the data monitored, you must create a Dashboard View for your new monitor. Click *Active Monitoring -> Dashboard Views* to open the view manager.

NOTE:

You can also select a device or alarm in Resources, Topology, or Alarm managers and click *action -> Show Performance* and see the Automatic Performance View. When you select this command OpenManage Network Manager finds all of the performance attributes being monitored for the selected equipment and creates a dashboard with one dashboard component for each attribute.

If you multi-select more than one device, each component shows the top five metrics for each attribute. If you select only one top-level device, OpenManage Network Manager searches the device's interface and port children for performance attributes and these attributes appear with the top five children for each attribute.

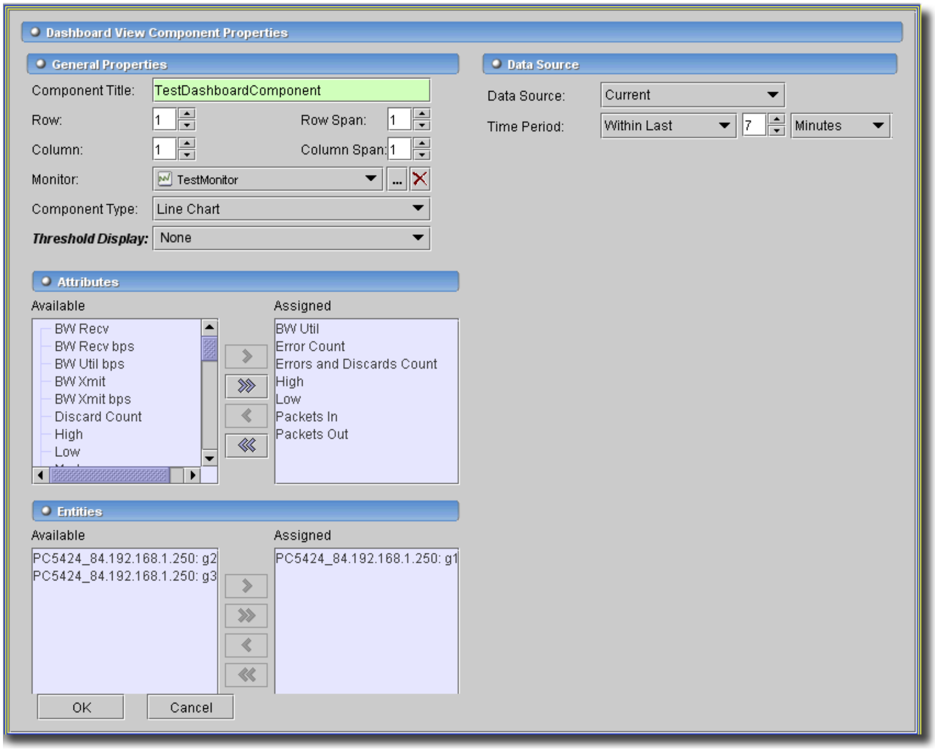
The data that appears is based on the monitors that are monitoring that device and where Retain Data is checked. If you have several monitors and you are retaining data on those monitors, the screen reflects those data points.

If you select two devices in Resources manager and click action -> Show performance, OpenManage Network Manager displays both of the devices' common attributes in the form. (You cannot display interface data because the devices do not have interfaces in common.)

2 Click *action -> New* to create a new view. By default this appears with two rows and three columns. You can, however, change those numbers and click *Update* to create a different layout. For simplicity, our example has one column and row.

Install a Monitor in the View

1 Click *action -> Add Component* then click *Action -> properties* inside the view's cell. The *Dashboard View Component Properties* screen appears.



Dashboard View Component Properties

General Properties

Component Title: TestDashboardComponent

Row: 1 Row Span: 1

Column: 1 Column Span: 1

Monitor: TestMonitor

Component Type: Line Chart

Threshold Display: None

Attributes

Available	Assigned
BW Recv	BW Util
BW Recv bps	Error Count
BW Util bps	Errors and Discards Count
BW Xmit	High
BW Xmit bps	Low
Discard Count	Packets In
High	Packets Out
Low	

Entities

Available	Assigned
PC5424_84.192.168.1.250: g2	PC5424_84.192.168.1.250: g1
PC5424_84.192.168.1.250: g3	

Data Source

Data Source: Current

Time Period: Within Last 7 Minutes

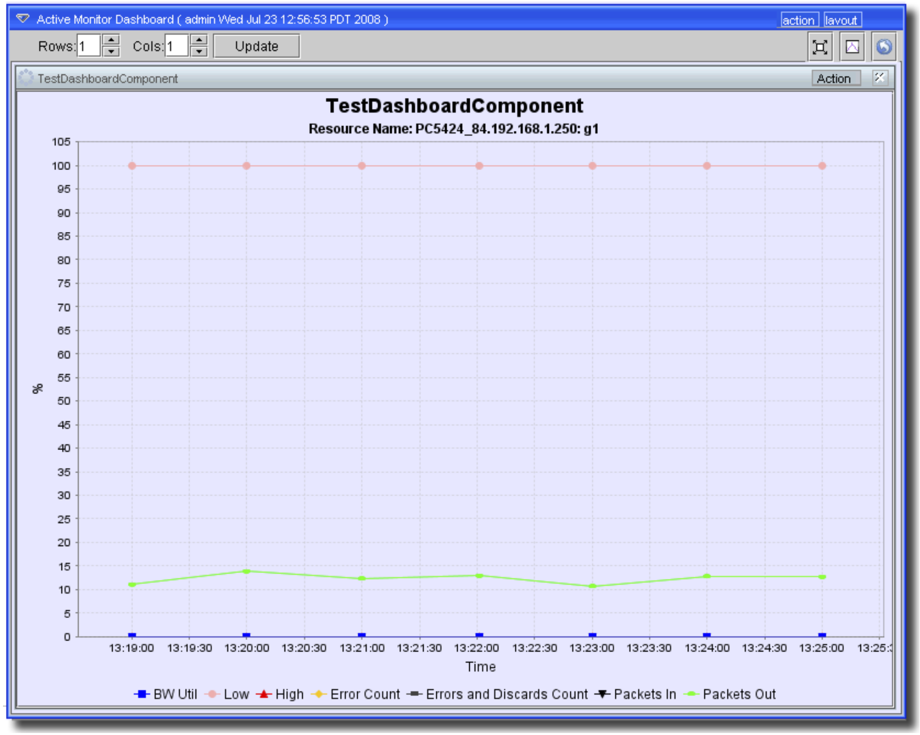
2 Enter a name for this component (TestDashboardComponent, here), and select a monitor and display type (here, we select the monitor configured in Create an SNMP Monitor, and a line chart. Notice also that for this example we leave *Threshold Display* as *none* (displaying thresholds as a part of the graph is also possible).

3 If you plan to monitor more than a single attribute, then select one entity to monitor at the bottom of the screen (select an entity, then use the arrow to move it from *Available* to *Selected*) and any number of attributes to monitor above that. Alternatively, you can select several entities to monitor, but only one attribute. In our example, we select a single interface, and monitor several attributes (*BW Util*, *Error Count*, *Errors and Discards Count*, *High*, *Low*, *Packets In*, *Packets Out*).

The exact configuration of this portion of the screen depend on the *Component Type* you select.

4 Notice you can also configure items in the *Data Source* portion of the screen. For this example we accept the defaults. Consult the online help for additional information about these.

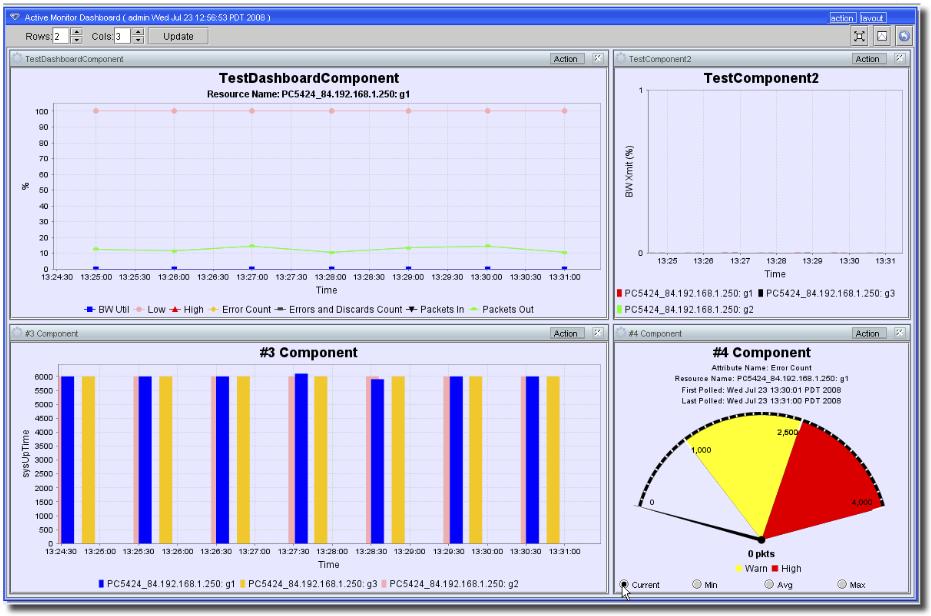
5 Finally, click *OK* to display the monitored data within the dashboard view you have configured.



NOTE:

You may have to wait until monitoring intervals are relevant. If you monitor every minute, you will have to wait at least that long to get data.

6 Notice that our simple example does not exploit all possibilities for these views. For example, you can have several components within a single view. In the example below, the same monitor appears in all four panels, displaying the monitoring for different attributes in different graph types

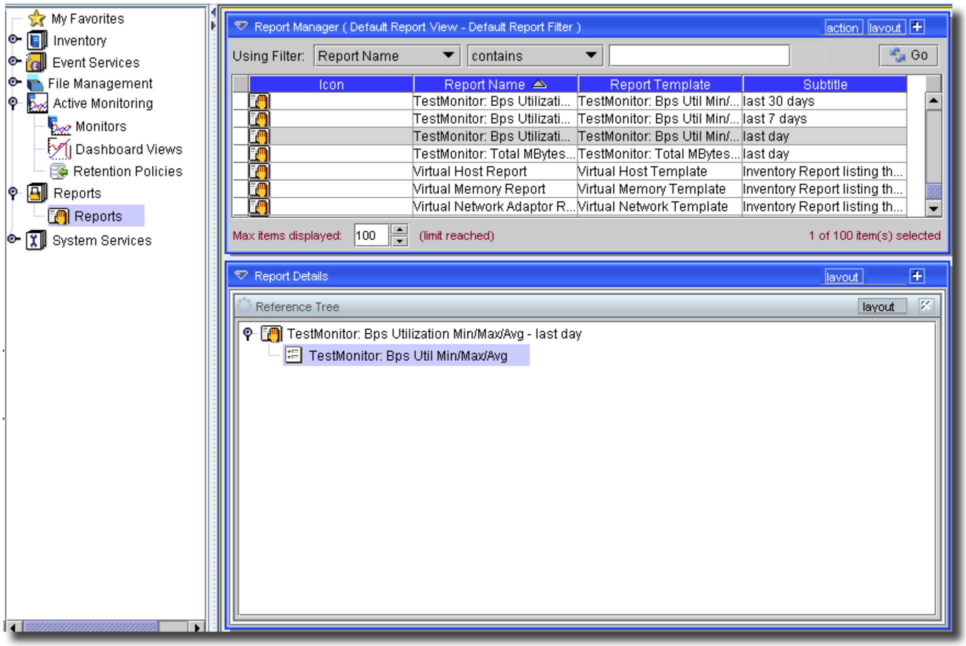


Click *action* -> *Save View* to save any view you have configured. You can also configure a variety of views to reflect different monitoring needs, and with *OpenManage Network Manager*'s multi-windowing capabilities, flip back and forth between the different views.

Reports From Monitors

When you create a monitor, a report template and several reports automatically appear for it in the *Reports* section of the application.

Figure 32-1. Monitor Reports.



Report Manager (Default Report View - Default Report Filter)

Using Filter: Report Name contains

Icon	Report Name	Report Template	Subtitle
	TestMonitor: Bps Utilizati...	TestMonitor: Bps Util Min/...	last 30 days
	TestMonitor: Bps Utilizati...	TestMonitor: Bps Util Min/...	last 7 days
	TestMonitor: Bps Utilizati...	TestMonitor: Bps Util Min/...	last day
	TestMonitor: Total MBytes...	TestMonitor: Total MBytes...	last day
	Virtual Host Report	Virtual Host Template	Inventory Report listing th...
	Virtual Memory Report	Virtual Memory Template	Inventory Report listing th...
	Virtual Network Adaptor R...	Virtual Network Template	Inventory Report listing th...

Max items displayed: 100 (limit reached) 1 of 100 item(s) selected

Report Details

Reference Tree

TestMonitor: Bps Utilization Min/Max/Avg - last day

TestMonitor: Bps Util Min/Max/Avg

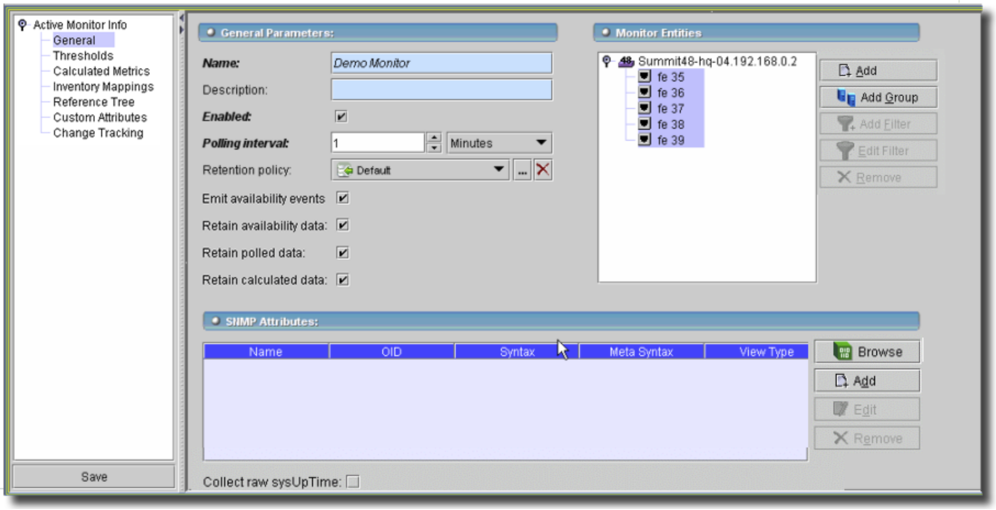
You can modify these reports, but by default, they include the monitored attributes and/or devices. The reports appear for the day, week, and last 30 days, at least. These intervals too are modifiable. Consult the online help for more information about customizing reports.

CAUTION:

To report on Avg/Max/Min attributes you must specify a period that is not *Detail* within the report filter itself since average min and max are not available with data that has not been rolled up to hourly, daily, weekly, and so on.

NOTE:

If you check the *Collect from ifXTable* checkbox, then OpenManage Network Manager attempts to fetch attributes from the ifXTable. These attributes are ifHighSpeed, ifHCInOctets, ifHCInUcastPkts, ifHCOutOctets and ifHCOutUcastPkts. If any of these attributes are not available, then it fetches from ifTable. The ifXTable checkbox option enables use of 64-bit counters instead of 32-bit counters (from ifTable).



Active Monitor Info
- General
- Thresholds
- Calculated Metrics
- Inventory Mappings
- Reference Tree
- Custom Attributes
- Change Tracking

General Parameters:

Name: Demo Monitor
Description:
Enabled: ☑
Polling interval: 1 Minutes
Retention policy: Default
Emit availability events ☑
Retain availability data: ☑
Retain polled data: ☑
Retain calculated data: ☑

Monitor Entities

Summit48-hq-04.192.168.0.2
- fe 35
- fe 36
- fe 37
- fe 38
- fe 39

SNMP Attributes:

Name	OID	Syntax	Meta Syntax	View Type

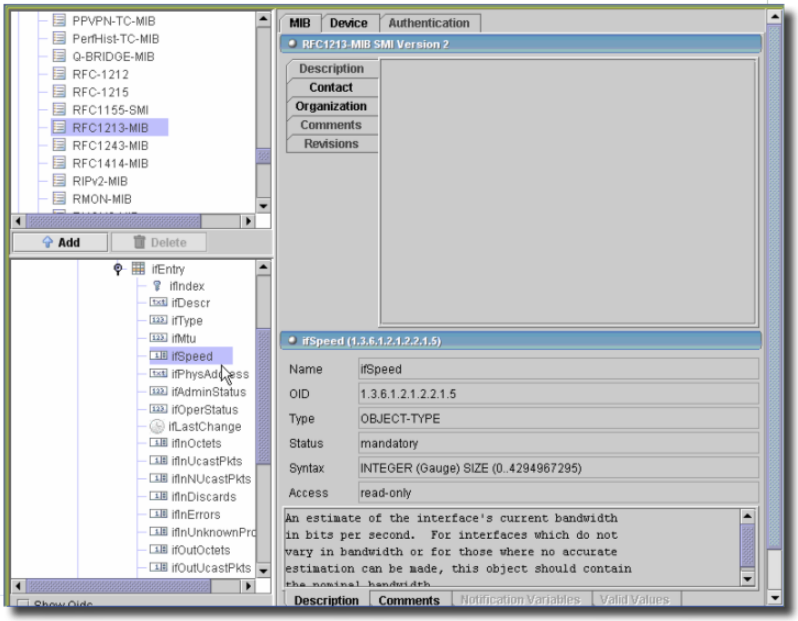
Collect raw sysUpTime: □

NOTE:

If you select devices with Add Group, you could automate monitoring of devices that are part of a group—either dynamic or static.

CAUTION:

If you receive the following message: *Device fault: Return packet too big.* in the Monitor Status Summary,



Name	ifSpeed
OID	1.3.6.1.2.1.2.2.1.5
Type	OBJECT-TYPE
Status	mandatory
Syntax	INTEGER (Gauge) SIZE (0..4294967295)
Access	read-only

```
An estimate of the interface's current bandwidth
in bits per second.  For interfaces which do not
vary in bandwidth or for those where no accurate
estimation can be made, this object should contain
the nominal bandwidth
```

then you have selected too many SNMP attributes to poll in a single request. Please modify your monitor to request smaller numbers of attributes

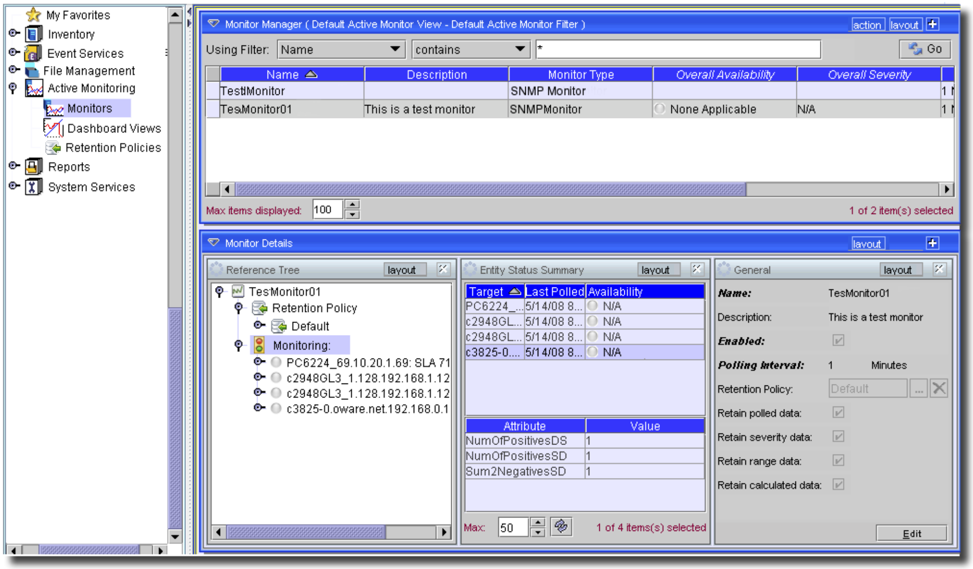
Standard Monitoring Functionality

You can now create dashboards, reports and all the other standard monitoring functions. See Monitors on page 770, Dashboard View Manager on page 781.

Monitors

This screen manages monitor configurations for Active Performance Monitor.

Figure 32-2. Monitors



Using Filter: Name ▾ contains ▾ * Go

Name	Description	Monitor Type	Overall Availability	Overall Severity	
TestIMonitor		SNMP Monitor			1
TesMonitor01	This is a test monitor	SNMPMonitor	○ None Applicable	N/A	1

Max items displayed: 100   1 of 2 item(s) selected

TesMonitor01
- Retention Policy
  - Default
- Monitoring:
  - PC6224_69.10.20.1.69: SLA 71
  - c2948GL3_1.128.192.168.1.12
  - c2948GL3_1.128.192.168.1.12
  - c3825-0.oware.net.192.168.0.1

Target	Last Polled	Availability
PC6224_...	5/14/08 8...	○ N/A
c2948GL...	5/14/08 8...	○ N/A
c2948GL...	5/14/08 8...	○ N/A
c3825-0....	5/14/08 8...	○ N/A

Attribute	Value
NumOfPositivesDS	1
NumOfPositivesSD	1
Sum2NegativesSD	1

Max: 50   1 of 4 items(s) selected

Name: TesMonitor01
Description: This is a test monitor
Enabled: ☑
Polling Interval: 1 Minutes
Retention Policy: Default
Retain polled data: ☑
Retain severity data: ☑
Retain range data: ☑
Retain calculated data: ☑

Configured monitors appear at the top of the screen. The topmost line includes a filter to limit this list. Click *Go* to refresh the list or enforce the filter. Monitors appear with an icon (green, red or yellow) indicating the monitor is *Available*, *Not Available*, or has received only *Partial Results*. Availability is archived even if all other data types are not if a retention policy exists for the monitor.

Right-click a monitor, or after selecting it, click the *Action* button to see the following capabilities:

- **New**—This menu item creates a new monitor. See Creating or Updating a Monitor on page 771. The next screen lets you pick the type of monitor to create. The contents of this menu depend on which options you have installed.

- **Open—**Edit an existing, selected monitor. See Creating or Updating a Monitor on page 771.

- **Delete**—Remove a listed monitor.

- **Copy**—Copy a listed monitor as the basis for a new one. This copies the entire content of the monitor including attributes, targets, intervals and so on. You must rename the copy.

NOTE:

You must manually delete the monitored targets from copied monitors for them to work correctly.

- **Enable / Disable**—Click one of these to enable or disable the selected monitor, to begin polling the target devices as defined within the monitor.

- **Refresh Monitor**—Manually refreshes the device membership of the target groups configured for the selected monitor(s). See Scheduling Refresh Monitor Targets on page 799 for a description of how to automate this manual task.
- **Restore Defaults**—This opens a list of seeded monitors. Select the monitor(s) you want to revert to their original, seeded state, and click *OK*. Each monitor listed appears listed with a *Loaded* or *Not Loaded* status and, if applicable, the time and date that the monitor was loaded. To force the loading of a monitor which was not initially loaded or to revert to the default loaded settings (overwriting any changes made to the monitor since it was originally loaded), select it in the table and click the *Ok* button. Multi-select is possible.

NOTE:

To modify default monitors, you can also select *action -> Copy* and create copies to alter.

Default monitors appear in the list of seeded defaults only if their supporting drivers are installed.

- **Import / Export**—Click this to export a selected monitor to an XML file, or to import a previously exported monitor. When you export a file, a dialog appears to let you name that file.
- **Help**—Click this to open online help for this screen.

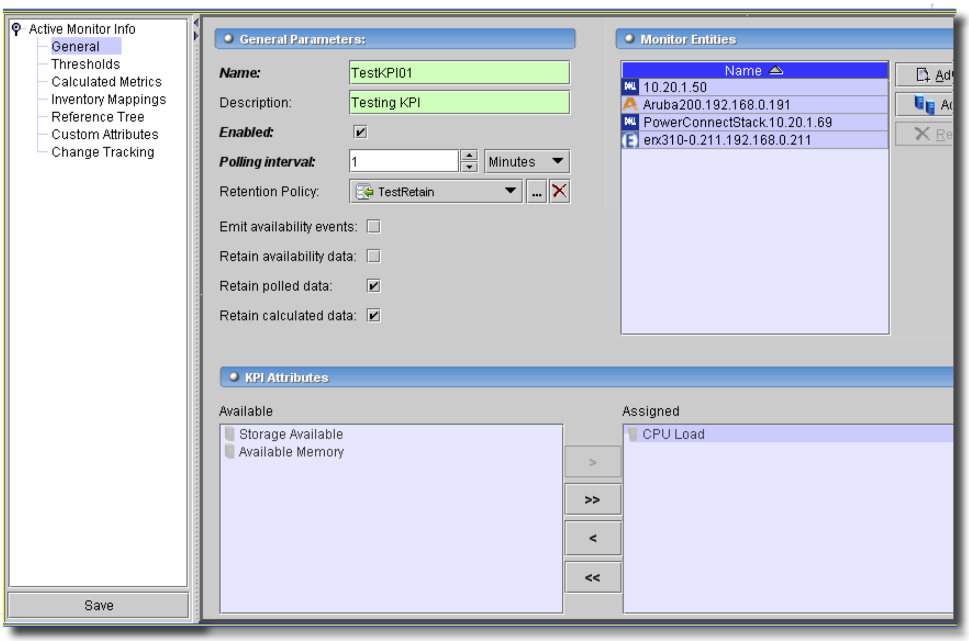
When you select a listed monitor, its components and the status of the entities it monitors appear in the detail panels at the bottom of this screen (in its standard configuration). Click the turners to view the Retention Policies and the state of the monitored equipment. The turners next to the state of the monitored equipment open to reveal the equipment icons.

The lines in the *Entity Status Summary* detail panel correspond to devices selected for the monitor. Click one of them to see the *Attribute* and *Value* combinations retrieved by the monitor in the lowest portion of that panel. You can see only retained data in the detail panel.

Creating or Updating a Monitor

This screen appears when you click *Open* when you have selected a monitor. It configures the monitor's capabilities and target devices.

Figure 32-3. Monitor Editor—General (Key Metric)



Name: TestKPI01

Description: Testing KPI

Enabled: ☑

Polling interval: 1 Minutes

Retention Policy: TestRetain

Emit availability events: ☐

Retain availability data: ☐

Retain polled data: ☑

Retain calculated data: ☑

Name
10.20.1.50
Aruba200.192.168.0.191
PowerConnectStack.10.20.1.69
erx310-0.211.192.168.0.211

Available	Assigned
Storage Available	CPU Load
Available Memory	

This editor has the following tabs:

- General
- Thresholds
- Calculated Metrics
- Inventory Mappings
- Reference Tree
- Custom Attributes—These depend on what users configure. See Custom Fields on page 178 for instructions about configuring these.
- Change Tracking—This is the standard change tracking panel. See Change Tracking on page 180 for instructions about configuring these.
- Audit—The Audit trail for transactions connected to the selected monitor. See Audit / Results on page 184 for more about that panel.

See Core and Default Monitors on page 789 for descriptions of the kinds of monitors available.

General

This screen's appearance depends on the type of monitor you have created. It typically has the following fields:

General Parameters

- **Name**—An identifier for the monitor.

- **Description**—An optional text description.
- **Enabled**—Check this to enable the monitor.
- **Polling Interval**—The frequency of monitor execution in *Hours*, *Minutes*, or *Seconds*. Ten seconds is the smallest supported interval.
- **Retention Policy**—Enter some text and select a retention policy from the search icon (magnifying glass) pick list, or create one with the command button (...). See Retention Policies on page 787 for more about creating and maintaining such policies.

  The checkboxes beneath *Retention Policy* determine exactly what is retained. These included *Emit availability events*, *Retain availability data*, *Retain polled data*, and *Retain calculated data*. Check these to retain the data.

  If you turn uncheck *Retain polled data* only calculated data remains, you cannot view data retrieved from monitored entities. Turning off *Retain polled data* discards the data as it arrives from the device.

  You must *Retain availability data* to enabled alarms. If you define thresholds, you should retain availability data.

  Retain availability data stores the Boolean values of whether availability data was in the range your defined metrics.

  Retain calculated data complements *Retain polled data*. If checked, it stores the calculated results which came from the raw poll data received from the device.

Monitor Entities

Click *Add* or *Add Group* to select, in a subsequent screen, entities this monitor will poll. In the SNMP Interfaces screen, you can also filter target interfaces with *Add Filter / Edit Filter.* This opens a standard OpenManage Network Manager filter screen where you can configure how to target the interfaces within a selected group or device. See Chapter 28, Filters for details.

Click *Remove* to delete a selected entity from the list. The targets for monitors can be members of groups. To ensure the membership of these groups is current, you can create or edit a scheduled refresh of the target groups as described in Scheduling Refresh Monitor Targets on page 799.

NOTE:

When you select equipment with large numbers of Monitor Entities, for example a device with 1,000 interfaces, even loading the list from which to select may take a long time.

Monitor-Specific Configuration

The type of attribute polled depends on the type of monitor selected. The lowest portion of the screen reflects the monitor type you have selected. For SNMP monitors, you can *Browse* to open the OpenManage Network Manager MIB browser, and select attributes that way, or you can *Add* to open an editor with SNMP attribute parameters that you can fill in. See SNMP Attributes (Interfaces or Scalars) on page 793 for details.

Check *Collect raw sysUpTime* at the bottom of this screen to monitor that attribute.

Several monitors come seeded with the application. These include Core and Optional add-on monitors. See *Core and Default Monitors on page* 789 for a more about additional available monitors and how to configure them.

Thresholds

This tab configures thresholds for the selected monitor. Here you can define value ranges reflecting these thresholds for each monitored attribute, and give each range a name, color and severity. The selected color appears in Dial charts for this monitor, but does not configure the color for any alarm generated by crossing threshold for a range. See Core and Default Monitors on page 789 for an explanation of the available attributes (they depend on the kind of monitor you are creating).

A threshold value is interpreted here as the lower boundary of some range. The upper boundaries are calculated automatically to prevent gaps and simplify configuration. Lower boundaries are inclusive while upper boundaries are exclusive.

You can also create more than one range with the same name. You can even create more than one range with the same severity.

Each time the application collects data, it determines the correct threshold range for the attribute value. When you base range checks on more than a single data point (with the *Range check based on ___ value(s)* field), the application classifies the value as in a range previously determined until criteria is met for a different range. If not enough data points exist (for example, the first time a monitor runs), the application still determines a range, even one based on less data than the *Range check based on ___ value(s)* selection.

For example, if you want an average of four data samples to determine whether some threshold has been crossed, the first value collected by the monitor determines the range, based on what ranges you specify in this *Thresholds* screen. The next time the monitor runs, it determines the range based on the average of two values, and so on until it reaches, and averages four values. Then it continues to rely on the average of most recent four data samples to determine the current range. This practice therefore establishes an initial threshold range when the monitor first runs.

The application produces an event when the range for a value changes. In other words: the event occurs when the application determines a threshold has been crossed. This event also appears when the monitor first starts, and its state changes from *no range* to *initial range*.

The event is a *monitorAttributeTrend* event from *RedcellMonitor-MIB*. The severity for the range entered dictates the severity of the event. The default event definition produces an alarm with a message showing monitor name, attribute name and range name.

A boolean value tracks each range in each attribute. These are *range results* for the monitor. Only one of the boolean range results values is true no matter how many ranges an attribute has. If you configure multiple ranges to have the same name, then only one boolean range result exists for that range name.

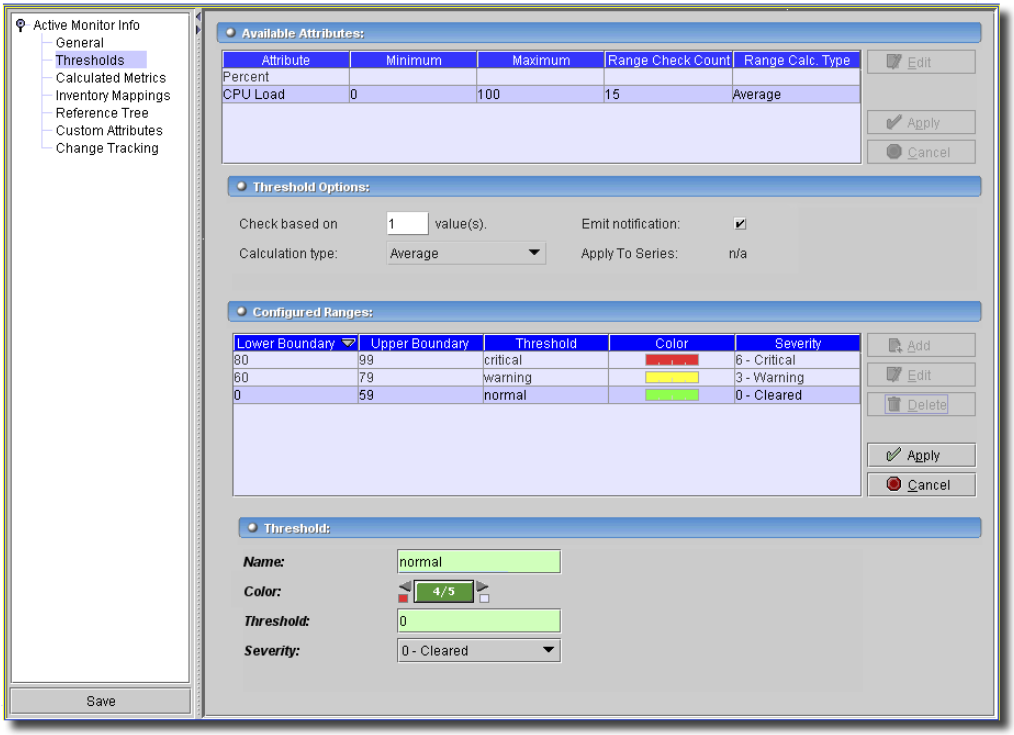
As data accumulates, and is rolled up, these booleans begin to appear as percentages—reflecting the percentage of monitor executions producing results in the specified range. Note that this is *not* a count or percent related to number of times the range changed.

If, for example, you had *bad* vs. *good* ranges, and based range determination on more than one data sample, the following would occur. If the range is originally *bad* then it stays *bad* until we receive enough data to change to *good*. Although results may occasionally be in the *good* range, the history (trend) will not indicate data ever was in the *good* range until enough data points appear in *good*. Therefore the monitor may indicate *good* although many intermittent results may fall outside of the *good* range.

NOTE:

If ranges cover all possible values for an attribute, the daily percentages per range should add up to 100%.

Figure 32-4. Monitor Editor—Thresholds



Available Attributes:

Attribute	Minimum	Maximum	Range Check Count	Range Calc. Type
Percent				
CPU Load	0	100	15	Average

Threshold Options:

Check based on 1 value(s).

Emit notification: ☑

Calculation type: Average

Apply To Series: n/a

Configured Ranges:

Lower Boundary	Upper Boundary	Threshold	Color	Severity
80	99	critical	🟥	6 - Critical
60	79	warning	🟨	3 - Warning
0	59	normal	🟩	0 - Cleared

Threshold:

Name: normal

Color: 4/5

Threshold: 0

Severity: 0 - Cleared

Available Attributes appear at the top of this screen. Click *Add* to create a new threshold, or *Edit* to modify an existing, selected one. This activates the *Threshold Options* editor. Click *Apply* to accept your edits, or *Cancel* to abandon them. You can enter the following fields there:

- **Check based on ___ value(s)** —This configures the number of consecutive values that are combined for a range check. Typically the larger the number here, the less “flutter” in reporting threshold crossings.

- **Calculation Type**— Select whether the range calculation done is based on *Average* or *Consecutive* values.

- **Emit Notification**— Check this to create an event when the threshold is crossed.

- **Apply to Series**—This applies only to composite values in (typically) Key Metric-type monitors, and displays the “Not Applicable” label if the monitored values are not composites.

  Checking this applies the threshold to individual elements within the series. When it is unchecked, the threshold applies only to aggregate measurements (the overall value of the series), not individual elements within the series.

  For example; a Key Metric monitor for CPU utilization on a device with two CPUs actually monitors both CPUs. When unchecked, the threshold applies to the average of both CPUs, when checked, the threshold applies to each individual CPU.

Click *Add* to create a new range, or *Edit* to modify an existing one in the *Configured Ranges* section of the screen. Click *Apply* to accept your edits, or *Cancel* to abandon them. The following fields appear in the *Threshold* portion of the screen:

- **Threshold Name**—An identifier for the threshold. Avoid using special characters in this name, they can invalidate the threshold.

- **Color**—A color for the threshold. By default, a simple, five-color selector appears in this field. Click the right/left arrows to select a color. The small colored boxes below the arrows preview the colors for the next selection right or left.

  If you want a wider color selection, double-click the color field, and another possibility appears. Clicking the command button (...) opens this color selector.

  NOTE:

  You can further configure default colors. Refer to the owareapps\performance\lib\pm.properties file for the properties and instructions for changing colors. As always, best practice is to override these properties in \owareapps\installprops\lib\installed.properties.

  The colors set here also appear as ranges in dial charts, if that is your selected display, as described in Creating or Updating a Dashboard on page 782.

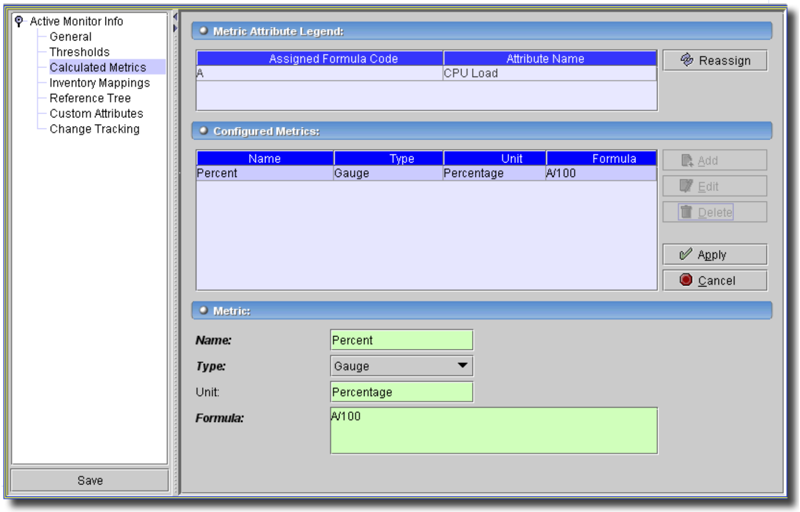
- **Threshold**—A value for the threshold. Although thresholds appear to be ranges, you can set only the lower range boundary as the threshold value. For example, if you set *Critical*, *Warning*, and *Normal* thresholds, then you only need to set a single minimum value for each. If, in this example the ranges are 0 - 60, 60 - 80, 80 - 100, then all you set is 0, 60, and 80, respectively. The application fills in the upper value for the range based on the values set for the next higher range. You can set maximum values for the attributes created in the Calculated Metrics tab.

Click *Save* to preserve this monitor. Once you save it, it should appear in the screen *Monitors on page* 770.

Calculated Metrics

This screen configures monitor metrics. Each metric defines an additional data value provided by the monitor

Figure 32-5. Monitor Editor—Metrics



Metric Attribute Legend:

Assigned Formula Code	Attribute Name
A	CPU Load

Configured Metrics:

Name	Type	Unit	Formula
Percent	Gauge	Percentage	A/100

Metric:

Name: Percent

Type: Gauge

Unit: Percentage

Formula: A/100

If necessary, you can define expressions to calculate additional attribute data for dashboard views or reports so it appears in a more useful form.

For example, to create a calculated metric of the difference of attributes A and B called *Difference* (for example *Requests* minus *Discards*), you could enter a formula: A-B. This would then be an attribute available for reports or dashboards. In reports, you can only see a single attribute, but the calculated attributes' *Average Min*, *Max* and *Total* are automatically available for reporting. See Operators on page 778 for a list of available operators for these calculations.

Collected attributes appear in the *Metric Attribute Legend* portion of the screen and are automatically assigned a letter usable in formulas (the assigned formula code). Only collected attributes are available for creating additional metrics. Click *Reassign* to re-order the alphabetic characters that stand for those attributes in metric formulas. Formulas are inspected and updated accordingly as part of this operation.

⚠ **CAUTION:**

Reassign does not automatically update formulas in the metrics' calculations, so click that button only before configuring formulas, not after. If you do click after creating formulas, then existing formulas may require edits after reassigning attribute symbols.

Select an attribute there, and the associated *Configured Calculations* appear listed in that portion of the screen. Click *Add* to create a new metric, or *Edit* to modify an existing one you have selected. Click *Delete* to remove a selected metric. The metric editor includes the following fields:

- **Name**—An identifier for this metric.
- **Type**—Select a result type from the pick list. Available options include *Count* and *Gauge*. *Gauge* values are averaged on rollup, and *Count* values are totalled.

CAUTION:
When editing an existing monitor, changing a metric type (Gauge or Count) invalidates existing retained data. The application drops all retained data for a calculated attribute when you save a metric type change.

- **Unit**—Enter an optional text identifier for the units for this metric. Units appear where appropriate on charts and reports.
- **Max Value**—Enter an optional maximum value for the calculation.
- **Formula**—Enter an expression to calculate the value for the metric. Attributes appear at the top of this screen with automatically assigned character codes for use in expressions.

Operators

Available operators (in order of precedence) and functions include the following:

Operator	Symbol
Power	^
Unary Plus, Unary Minus	+n, ¡n
Modulus	%
Division	/
Multiplication, Addition, Subtraction	*, +, -

Function	Symbol
Sine	sin()
Cosine	cos()
Tangent	tan()
Arc Sine	asin()
Arc Cosine	acos()
Arc Tangent	atan()
Hyperbolic Sine	sinh()
Hyperbolic Cosine	cosh()
Hyperbolic Tangent	tanh()
Inverse Hyperbolic Sine	asinh()
Inverse Hyperbolic Cosine	acosh()

Function	Symbol
Inverse Hyperbolic Tangent	atanh()
Natural Logarithm	ln()
Logarithm base 10	log()
Absolute Value / Magnitude	abs()
Random number [0; 1]	rand()
Square Root	sqrt()
Sum	sum()

The *Entity Status Summary* detail panel in the *Monitor Manager* displays calculation errors, if they occur.

NOTE:

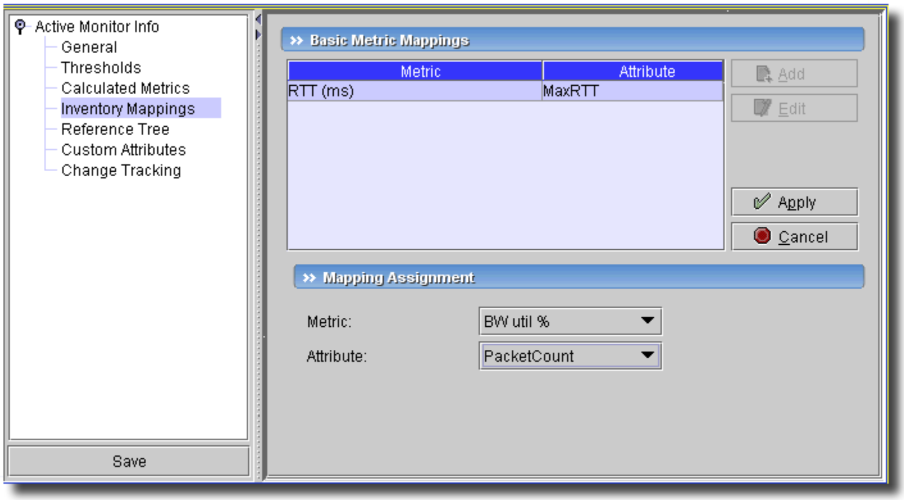
Expressions are not validated in this screen. Such validation occurs when the expression is evaluated for collected data.

Click *Apply* to accept your edits, or *Cancel* to abandon them.

Inventory Mappings

This panel lets you map retrieved attributes to common metrics that appear in monitors, and reports throughout OpenManage Network Manager.

Figure 32-6. Inventory Mappings



Metric	Attribute
RTT (ms)	MaxRTT

Metric: BW util %

Attribute: PacketCount

Click *Add* to create a new mapping. Metrics are common in the Resources manager, monitors and reports. These include *CPU util %*, *Memory util %*, *RTT (ms)* (Round Trip Time in milliseconds), *Disk full %*, and *BW util %* (Bandwidth utilization percent).

NOTE:

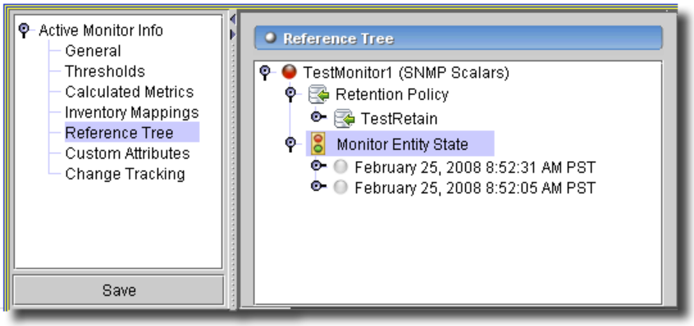
You can configure these monitors to appear in Resource manager columns.

Select the *Metric* you want to appear and the *Attribute* you want mapped to it with the pick lists. The available *Attributes* depends on which attributes are monitored. Click *Apply* to accept your mapping, or *Cancel* to abandon them.

Reference Tree

This panel displays the associations with retention policies and target devices for the selected monitor.

Figure 32-7. Reference Tree

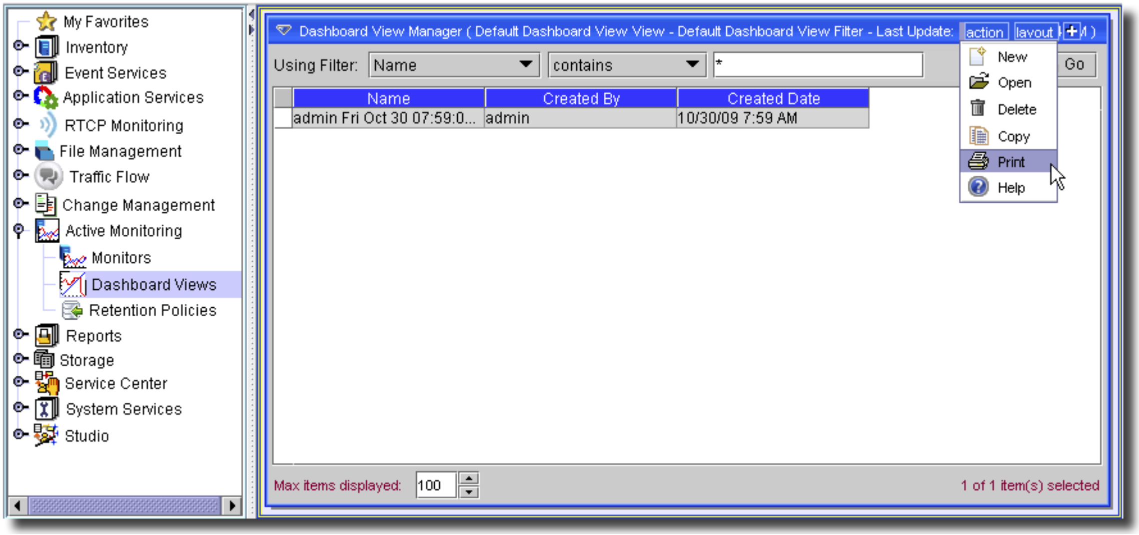


Click the turners to un-pack the tree and reveal the associated retention policies and target devices.

Dashboard View Manager

This screen lets you manage dashboard views.

Figure 32-8. Dashboard View Manager



Dashboard View Manager (Default Dashboard View View - Default Dashboard View Filter - Last Update:

Using Filter: Name contains *

Name	Created By	Created Date
admin Fri Oct 30 07:59:0...	admin	10/30/09 7:59 AM

Max items displayed: 100

1 of 1 item(s) selected

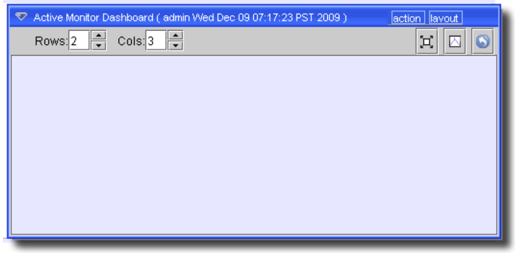
Click the following *Action* menu items to create and modify views:

- **New**—This menu item creates a new dashboard view. See Creating or Updating a Dashboard on page 782.
- **Open—**Edit an existing, selected dashboard view. See Dashboard Viewer on page 783.
- **Delete**—Remove a listed view.
- **Copy**—Create a copy of an existing view to re-name and re-configure.
- **Print**—Print the list of views.
- **Help**—Open online help for this screen.

Creating or Updating a Dashboard

After you click *New*, a blank dashboard view appears.

Figure 32-9. View Editor



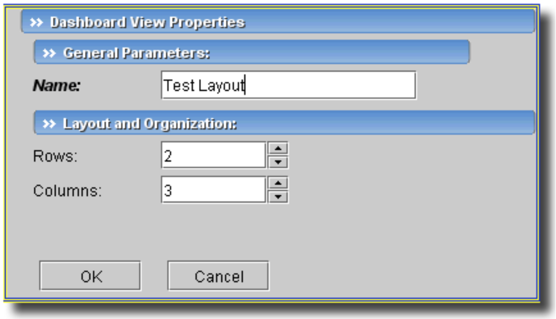
Active Monitor Dashboard (admin Wed Dec 09 07:17:23 PST 2009)

Rows: 2 Cols: 3

In this screen, configure the Row and Columns for monitor display. Enter numbers or use the spinners to select a number of rows and columns for the view you want to create. Click *action* -> *Add Component* to add elements to the rows and columns of display. The *action* -> *Save View* menu item lets you preserve your configuration.

The *action* -> *Properties* menu lets you change the row and column configuration and change the default name.

Figure 32-10. Dashboard Properties



Dashboard View Properties

General Parameters:

Name: Test Layout

Layout and Organization:

Rows: 2

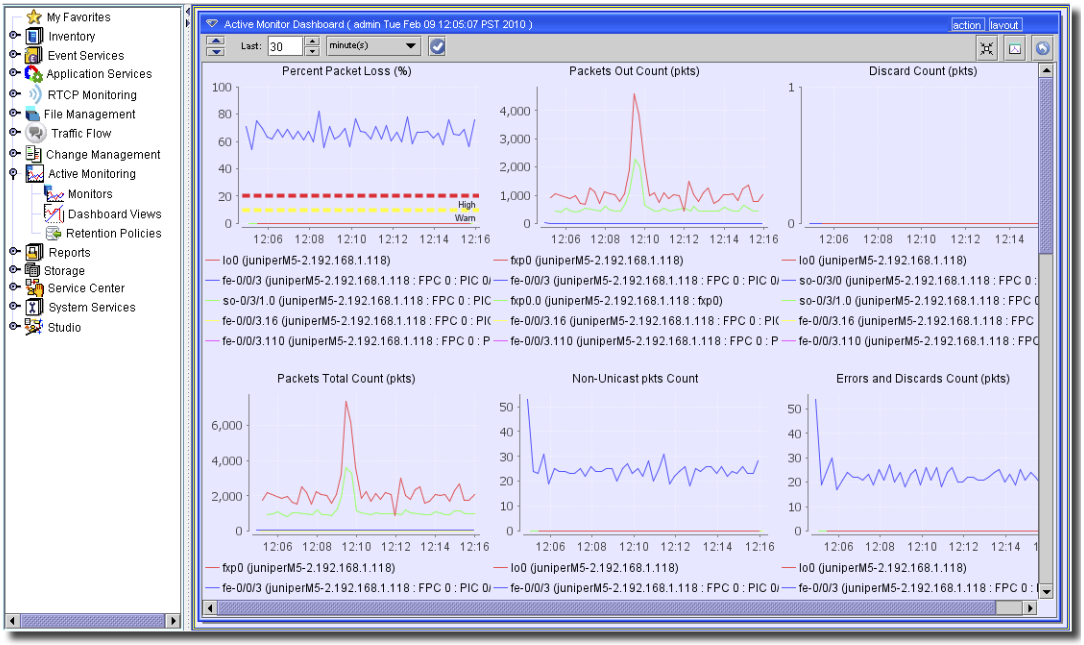
Columns: 3

When you save a view, the name defaults to a combination of the saving user, and the time and date.

Dashboard Viewer

Dashboard Viewers display the results of monitoring in graphical form.

Figure 32-11. Dashboard



The three icons at the top right of this screen, from left to right, let you *Fit / Unfit* the dashboard (view it in its natural size, not confined to the current screen), *Unlock / Lock Components* (which *Hides / Shows Title Bars*) on components, and *Refresh* the view. You can also configure the refresh intervals and collection dates viewable with the two sets of spinners that appear when you click the icon on the upper left side of the screen. Click the up/down arrows that appear on the left to see both time and date intervals. Click the check mark that appears to the right of these fields to close them and accept your configuration.

Click *Refresh* to have the display reflect any changes to the column or row numbers. Click *action -> Add Component* to add "receptacles" for monitoring information.

NOTE:

By default, title bars do not appear, but you must use the action menus in component title bars to configure them.

You can click the *Min*, *Avg*, and *Max* radio buttons at the bottom of the Dial chart panels to see the readings based on the minimum, average or maximum figures, respectively.

Clicking the *Action* button at the upper right corner of the dashboard opens the following menu items:

- **Add Component**—This adds a panel to the lower right corner of the existing dashboards. Use this panel's *action* -> *Properties* menu item to configure it.

- **Properties**—This opens a panel where you can *Name* (or re-name) the dashboard you are configuring, and select its layout *Rows* and *Columns*. Click *OK* to accept what you have configured.

- **Save View**—This saves the dashboard as you have configured it.

- **Save As...**—This saves the dashboard as you have configured it, but lets you re-name it. After you have saved it with a different name, you can re-configure the view.

- **Help**—Opens the online help for this screen.

Clicking the A*ction* button at the upper right corner of each component panel opens the following menu items:

- **Properties**—This opens the panel described in Dashboard Component Properties on page 784 that configures the contents of the panel.

- **Refresh**—Refreshes the panel

- **Expand/Contract**—This lets you expand or contract the selected panel to fill the space up/down/right/left.

CAUTION:
If panels are smaller if roughly 250 pixels square a horizontal scroll bar cannot appear in the panel.

Export—Exports an XML representation of a monitor.

Edit Monitor—Opens the monitor editor for the selected panel. See Creating or Updating a Monitor on page 771.

Dashboard Component Properties

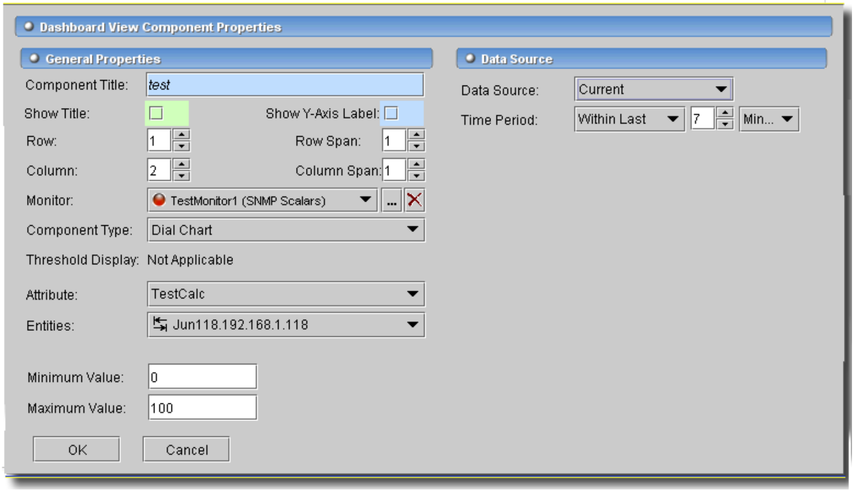
When you open this screen, it appears with the following panels:

- Configure
- Attributes and Equipment
- Data Source

Configure

The configure screen determines the component’s monitor and appearance.

Figure 32-12. Dashboard Component Action -> Configure



Component Title: test

Show Title: □ Show Y-Axis Label: □

Row: 1 Row Span: 1

Column: 2 Column Span: 1

Monitor: TestMonitor1 (SNMP Scalars)

Component Type: Dial Chart

Threshold Display: Not Applicable

Attribute: TestCalc

Entities: Jun118.192.168.1.118

Minimum Value: 0

Maximum Value: 100

Data Source: Current

Time Period: Within Last 7 Min...

It lets you select the following for the selected component:

- **Component Title**—Enter an identifier for the component that appears as its onscreen title.
- **Show Title / Y-Axis Label**—Check these boxes to display the title and/or Y-axis labels in the graph.
- **Row / Rowspan**—Use the spinners to enter the row number (from the top of the screen) where this dashboard component appears, and the number of rows it spans.
- **Column / Rowspan**—Use the spinners to enter the column number (from the left of the screen) where this dashboard component appears, and the number of columns it spans.
- **Monitor**—Click the search icon (magnifying glass) or command button (...) to select a monitor. A description of how these are configured appears in Monitors on page 770.
- **Component Type**—Select the display type for this component from the pick list. Available options include *Dial Chart* (Select the device charted from the *Entities* pick list), *Line Chart* and *Bar Chart* (configure as described in Attributes and Equipment on page 786).

NOTE:

Dial charts also display *Low/Medium/High* ranges in different, if you have set the thresholds for this as described in Thresholds on page 774.

To display data from the most active components of your network, select *Top Talkers*. Configure the *Order* (Ascending / Descending) and *Max # of Entities* to monitor with those fields that appear once you select *Top Talkers*.

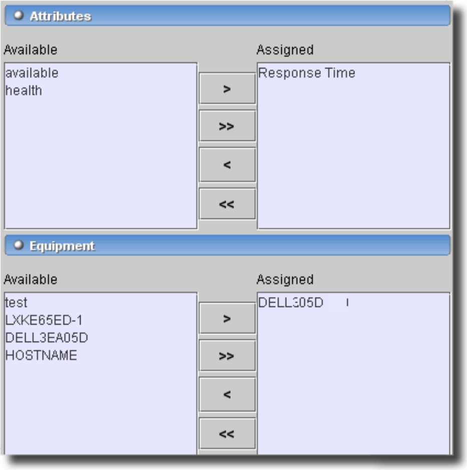
- **Threshold Display**—Select the threshold from the pick list. Available options include *None*, *Interval* and *Value*.
- **Attribute**—Select the attribute to monitor from the pick list if you selected a *Dial Chart* or *Top Talkers*. These include *Available*, *Severity*, and any calculations you configure as described in *Calculated Metrics on page 777*.

  Since *Line Chart* and *Bar Chart* permit multiple attribute monitoring, use the arrows to move attributes from the *Available* to *Assigned* panels to select those attributes.
- **Order** —*Ascending / Descending* for *Top Talkers* Component Type.
- **Max # of Entities**—Enter the maximum number of monitored entities for the *Top Talkers* Component Type.
- **Minimum / Maximum Value** —These attributes appear if you selected a *Dial Chart*.

Attributes and Equipment

The appearance of the lowest portion of the screen depends on the *Component Type* you select above.

Figure 32-13. Line and Bar Chart Attributes



Attributes — Available: available, health; Assigned: Response Time

Equipment — Available: test, LXKE65ED-1, DELL3EA05D, HOSTNAME; Assigned: DELL305D

- **Entities**—Select the equipment to monitor from the pick list if you selected a *Dial Chart* or *Top Talkers*. Since *Line Chart* and *Bar Chart* permit multiple device monitoring, use the arrows to move attributes from the *Available* to *Assigned* panels that appear with those selections, to select that equipment.

NOTE:

Dial components appear with radio buttons for Current, Min, Avg and Max readings.

Data Source

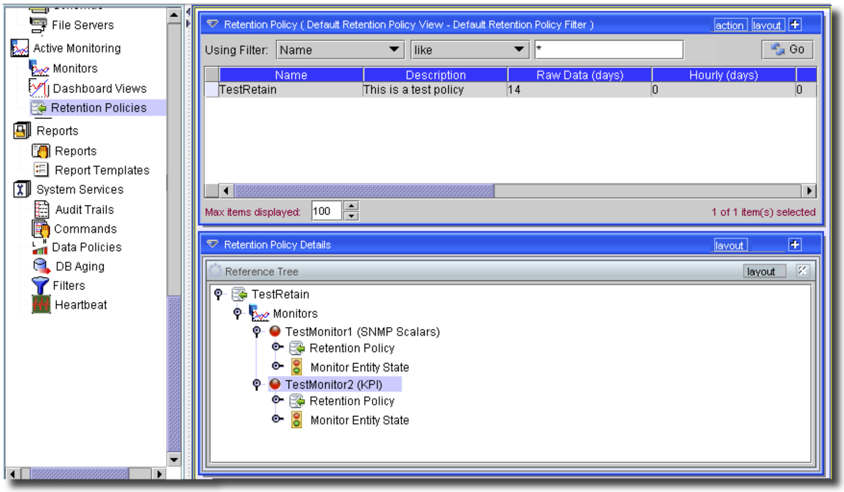
This panel configures the data source for monitoring. It has the following fields:

- **Data Source**—Select the source from the pick list. Options include *Current*, *Hourly*, *Daily*, *Monthly* and *Yearly*.
- **Time Period**—Use the fields and pick lists following this label to elect the time periods. If you select a *Current* data source, you can only elect *Within last* enumerated *Minutes*, *hours*, *days*, and so on. Other than *Current* data sources also permit *Between* time selections.

Retention Policies

This screen manages retention policies for the various monitors.

Figure 32-14. Retention Policy Manage



Retention Policy (Default Retention Policy View - Default Retention Policy Filter)

Using Filter: Name like *

Name	Description	Raw Data (days)	Hourly (days)	
TestRetain	This is a test policy	14	0	0

Max items displayed: 100

1 of 1 item(s) selected

Retention Policy Details

Reference Tree

```
TestRetain
  Monitors
    TestMonitor1 (SNMP Scalars)
      Retention Policy
      Monitor Entity State
    TestMonitor2 (KPI)
      Retention Policy
      Monitor Entity State
```

Click the following *Action* menu items to create and modify views:

- **New**—This menu item creates a new retention policy. See Creating or Updating a Dashboard on page 782.
- **Open—**Edit an existing, selected retention Policy. See Creating or Updating a Retention Policy on page 788.
- **Print—**Print the listed policies to an Acrobat file. You must install the free Acrobat reader for this to work correctly. Change the filter on this manager to change the contents of the list.
- **Import/Export—**Import or export an XML description of the listed policies. Change the filter on this manager to change the contents of the list.

NOTE:

When you import them, Retention policies do not include associated monitors. On the other hand, imported monitors do retain associated retention policies, when imported

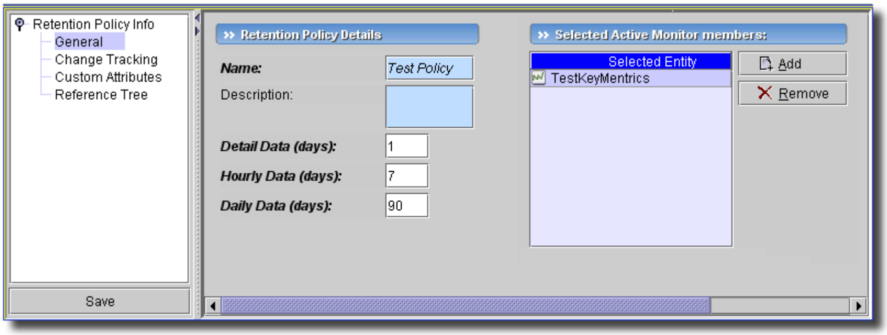
- **Delete**—Remove a selected policy.

- **Help**—Click this to open online help for this screen.

Creating or Updating a Retention Policy

This editor appears when you create a new policy or edit an existing one.

Figure 32-15. Retention Policy Editor



Name: Test Policy

Description:

Detail Data (days): 1

Hourly Data (days): 7

Daily Data (days): 90

Selected Entity
TestKeyMentrics

This screen contains the following fields:

Retention Policy Details

- **Name**—A text identifier for the policy.

- **Description**—An optional description of the policy.

The following fields describe the retention period and rollups that occur with data.

- **Detail Data (days)**—This is the number of days to store raw data.

- **Hourly Data (days)**—This is the number of days to store hourly data.

- **Daily Data (days)**—This is the number of days to store daily data.

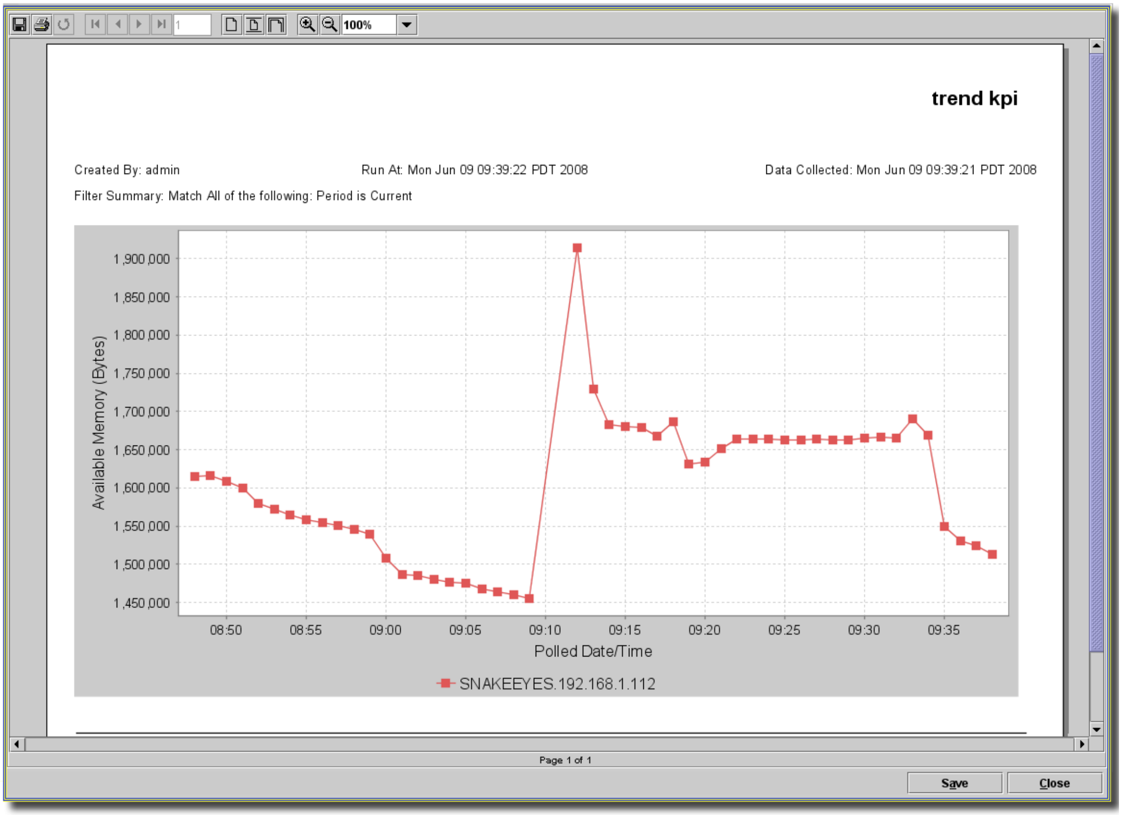
Only dashboards use the Detail Data (days) value on the retention policy. Best practice is to enter only one or two days as a duration. Performance can suffer if this value is more than a handful of days. The remaining fields on the retention policy are for historical reporting. You can define these to retain data for longer periods.

Select Active Monitor members

Use the *New* button (the blank sheet of paper) to select entities whose monitor policies' data are to be stored according to the Retention Policy Details described above.

Standard tabs for *Change Tracking*, *Custom Attributes* and *Reference Tree* also appear in this editor. See Change Tracking on page 180, Custom Fields on page 178 and Reference Tree on page 221 for more about these.

Figure 32-16. Active Performance Monitor Data



trend kpi

Created By: admin

Run At: Mon Jun 09 09:39:22 PDT 2008

Data Collected: Mon Jun 09 09:39:21 PDT 2008

Filter Summary: Match All of the following: Period is Current

Core and Default Monitors

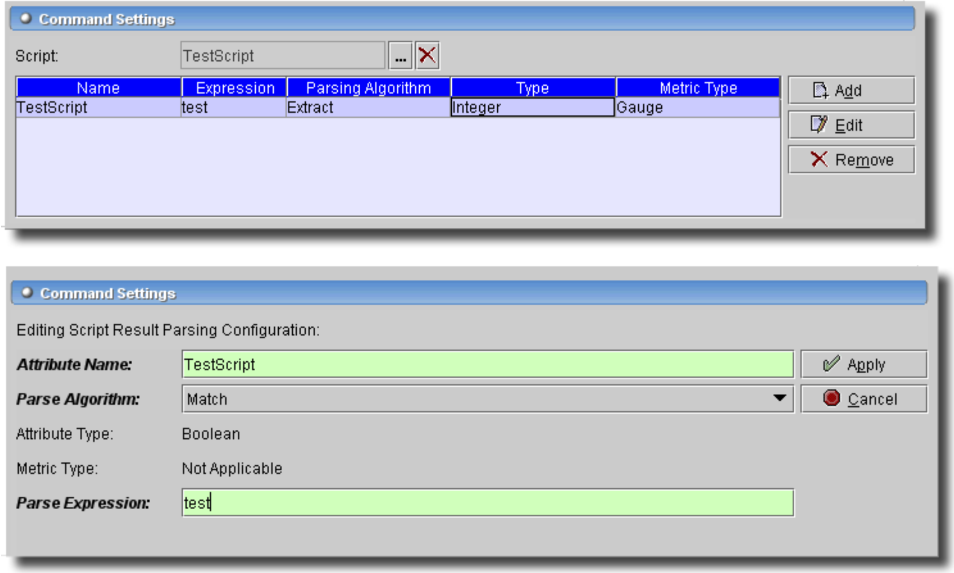
The following are the types of monitor you can configure. Some *Default Monitors* come with this application (see Default Monitors on page 796). The exact list of seeded, default monitors depends on the package you install. You can configure Core monitors with the monitor editor too, as described in Creating or Updating a Monitor on page 771.

When you click *New*, you must first select one of the following types to configure a monitor.

- ICMP
- SNMP Attributes (Interfaces or Scalars)

You can typically modify or copy any seeded monitor to fit your particular needs. The following sections describe these portions of the screen.

Figure 32-17. Command Monitor - Command Settings / Editor



Command Settings

Script: TestScript

Name	Expression	Parsing Algorithm	Type	Metric Type
TestScript	test	Extract	Integer	Gauge

Command Settings

Editing Script Result Parsing Configuration:

Attribute Name: TestScript

Parse Algorithm: Match

Attribute Type: Boolean

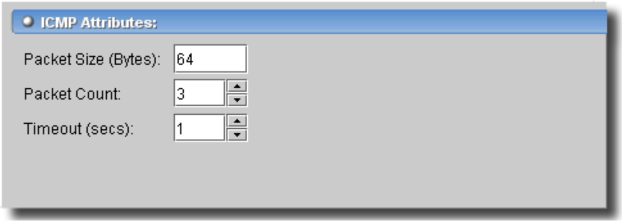
Metric Type: Not Applicable

Parse Expression: test

ICMP

This monitor performs an ICMP ping for each target in addition to the common fields described above.

Figure 32-18. ICMP Attributes



ICMP Attributes:

Packet Size (Bytes): 64

Packet Count: 3

Timeout (secs): 1

In this screen, you can configure the following:

- **Packet Size (Bytes)**—The send buffer size. Range: 64 to 64000. Default: 64

- **Packet Count**—The number of echo requests to send in the ICMP ping sent the monitored device. Range 1 to 9. Default: 3.

- ‘**Timeout (secs)**—The interval to wait for a reply. Range: 1 to 9, default: 1.

Attributes not visible in this screen also appear in the Calculated Metrics screen. These include Average, Minimum and Maximum round-trip times (*AvgRTT, MinRTT, MaxRTT*) and a *Packet Count* attribute.

Configure a Key Metric monitor if you want to have long-term monitoring, and Dashboard View Manager capabilities. For shorter-terms, you can also configure Key Metric monitoring in the following ways:

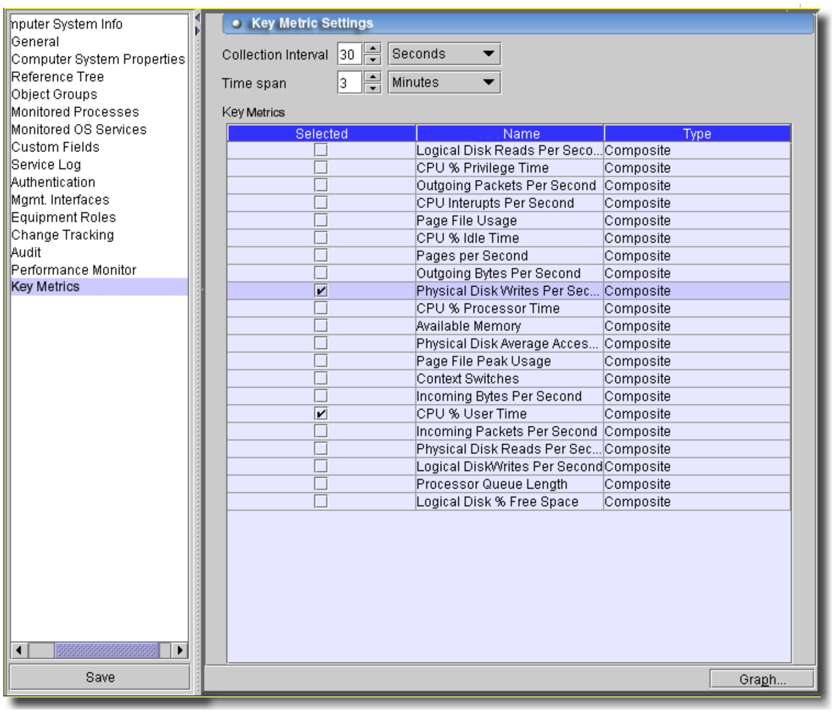
- Key Metrics in Resources Editor
- Key Metrics for Multiple Devices

You must keep these screens open for monitoring to occur. The following sections describe these capabilities.

Key Metrics in Resources Editor

In addition to configuring Key Metric Monitors, some devices display monitor data in the Resource Editor. This data appears as a detail panel in Resource Manager and as a node in the Resource Editor tree, lets you configure real-time performance monitoring for driver-supplied attributes. After you select a device in the Resources manager, click *action -> Open* to display that screens that include Key metrics for that device.

Figure 32-19. Key Metrics – Settings



nputer System Info
General
Computer System Properties
Reference Tree
Object Groups
Monitored Processes
Monitored OS Services
Custom Fields
Service Log
Authentication
Mgmt. Interfaces
Equipment Roles
Change Tracking
Audit
Performance Monitor
Key Metrics

Key Metric Settings

Collection Interval 30 Seconds

Time span 3 Minutes

Key Metrics

Selected	Name	Type
☐	Logical Disk Reads Per Seco...	Composite
☐	CPU % Privilege Time	Composite
☐	Outgoing Packets Per Second	Composite
☐	CPU Interupts Per Second	Composite
☐	Page File Usage	Composite
☐	CPU % Idle Time	Composite
☐	Pages per Second	Composite
☐	Outgoing Bytes Per Second	Composite
☑	Physical Disk Writes Per Sec...	Composite
☐	CPU % Processor Time	Composite
☐	Available Memory	Composite
☐	Physical Disk Average Acces...	Composite
☐	Page File Peak Usage	Composite
☐	Context Switches	Composite
☐	Incoming Bytes Per Second	Composite
☑	CPU % User Time	Composite
☐	Incoming Packets Per Second	Composite
☐	Physical Disk Reads Per Sec...	Composite
☐	Logical DiskWrites Per Second	Composite
☐	Processor Queue Length	Composite
☐	Logical Disk % Free Space	Composite

Select a monitoring *Collection Interval* and a *Time Span* (to determine the width of the graph) at the top of this screen. Then, you can check to monitored Indicators in the table below. The attributes available depend on the device and the driver selected. Click *Graph* to see their performance in real time. Graphing begins when you click this button. Leave the graph open to watch its progress (you can perform other tasks on other application screens while this one is open too).

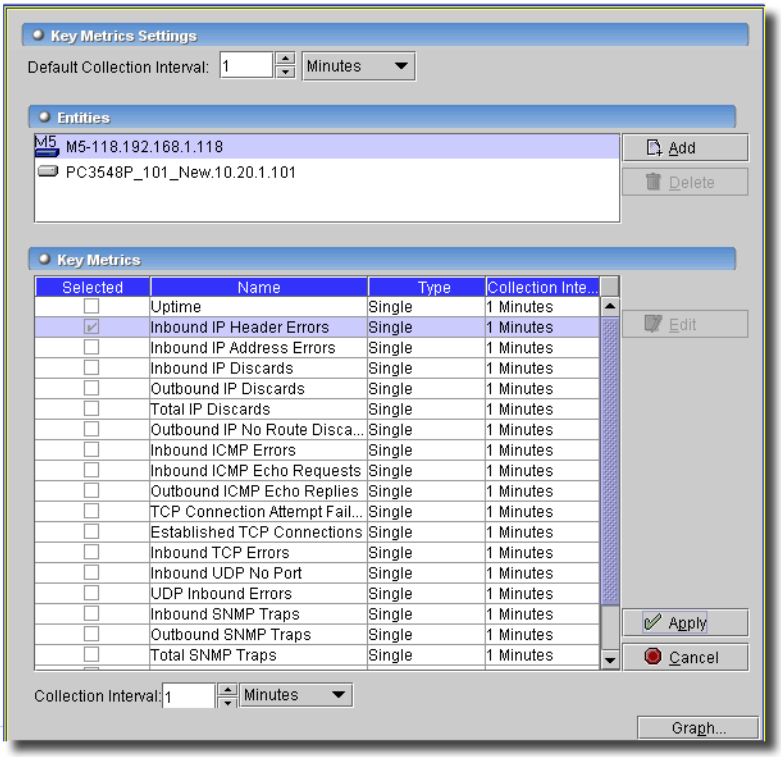
If you click multiple attributes, the graph may appear with multiple indexes (on the left). Composite attributes graph multiple lines, one for each of their components. Click *Settings* to return to the settings screen.

Key Metrics for Multiple Devices

In addition to configuring Key Metrics monitors, as described in Creating or Updating a Monitor on page 771, OpenManage Network Manager lets you select multiple devices in Resources, Topology or Chassis View, and use the action menu to select *Key Metrics* for those devices. This opens a screen where you can configure which key metrics to monitor for the selected devices.

OpenManage Network Manager assumes group targets represent the corresponding top level managed objects. Subcomponent support in Key Metrics monitor is only for explicitly configured subcomponent targets.

Figure 32-20. Key Metrics for Multiple Devices



Default Collection Interval: 1 Minutes

M5-118.192.168.1.118
PC3548P_101_New.10.20.1.101

Selected	Name	Type	Collection Inte...
☐	Uptime	Single	1 Minutes
☑	Inbound IP Header Errors	Single	1 Minutes
☐	Inbound IP Address Errors	Single	1 Minutes
☐	Inbound IP Discards	Single	1 Minutes
☐	Outbound IP Discards	Single	1 Minutes
☐	Total IP Discards	Single	1 Minutes
☐	Outbound IP No Route Disca...	Single	1 Minutes
☐	Inbound ICMP Errors	Single	1 Minutes
☐	Inbound ICMP Echo Requests	Single	1 Minutes
☐	Outbound ICMP Echo Replies	Single	1 Minutes
☐	TCP Connection Attempt Fail...	Single	1 Minutes
☐	Established TCP Connections	Single	1 Minutes
☐	Inbound TCP Errors	Single	1 Minutes
☐	Inbound UDP No Port	Single	1 Minutes
☐	UDP Inbound Errors	Single	1 Minutes
☐	Inbound SNMP Traps	Single	1 Minutes
☐	Outbound SNMP Traps	Single	1 Minutes
☐	Total SNMP Traps	Single	1 Minutes

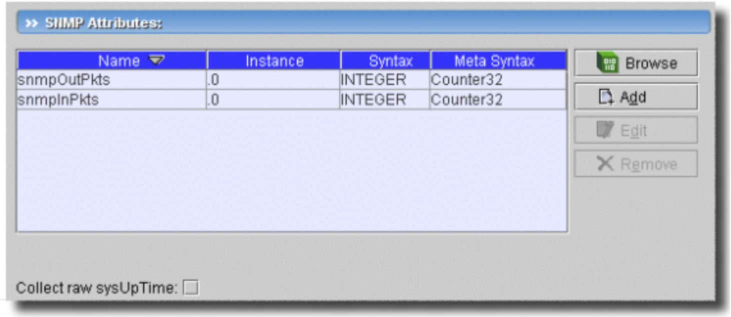
Collection Interval: 1 Minutes

Click the device in the upper portion of the screen to display its key metrics in the bottom portion of the screen. Click the *Selected* checkbox to begin monitoring the Key Metrics for the selected device. You can alter the monitoring interval globally in the upper *Default Collection Interval*. Click *Edit* in the lower portion of the screen to alter the interval for individual metrics with the *Collection Interval* fields at the bottom of the *Key Metrics* panel. Click *Apply* to accept any interval edits, or *Cancel* to abandon such edits. As with basic Key Metrics, click the *Graph* button in the lower right panel to see a graph of all selected devices' Key Metrics combined.

SNMP Attributes (Interfaces or Scalars)

This panel appears if you are creating an SNMP monitor. The application stores not absolute numbers from counters but the counter's change since its last measurement.

Figure 32-21. SNMP Attribute Management



Name	Instance	Syntax	Meta Syntax
snmpOutPkts	.0	INTEGER	Counter32
snmpInPkts	.0	INTEGER	Counter32

Collect raw sysUpTime: □

Columns include the SNMP Attribute *Name*, *OID*, *Syntax*, and *Meta Syntax*.

NOTE:

If you check the *Collect from ifXTable* checkbox, then OpenManage Network Manager attempts to fetch attributes from the ifXTable. These attributes are ifHighSpeed, ifHCInOctets, ifHCInUcastPkts, ifHCOutOctets and ifHCOutUcastPkts. If any of these attributes are not available, then it fetches from ifTable.

Clicking the buttons to the right opens either an editor at the bottom of the screen, or a MIB browser where you can retrieve these attributes. See the following sections for details.

- MIB Browser
- Add / Edit SNMP Attributes

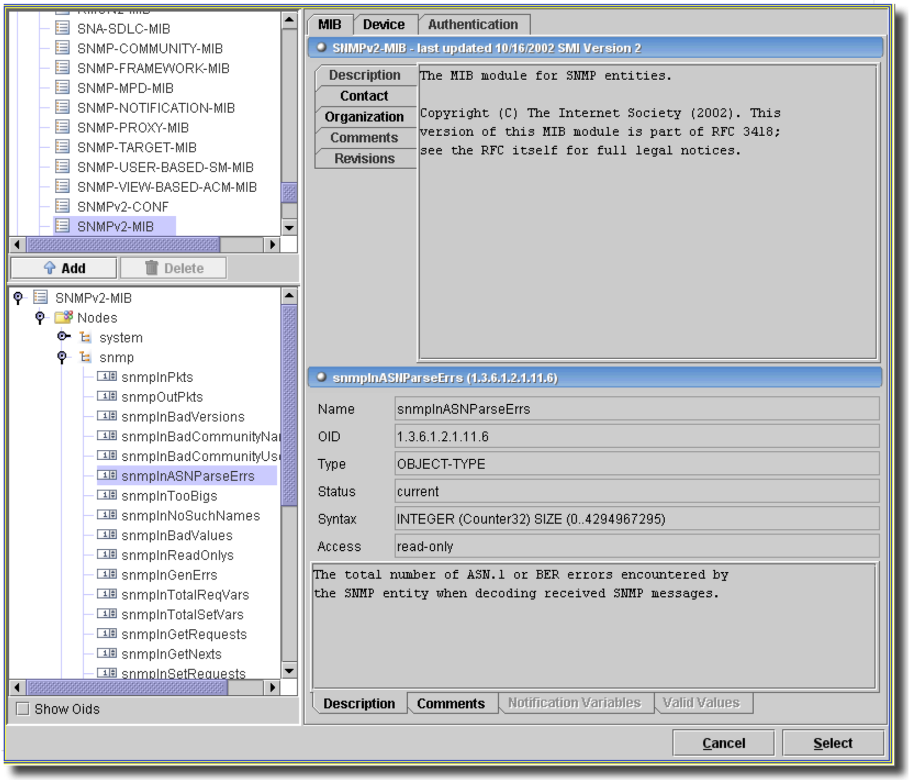
CAUTION:

If you receive the following message: *Device fault: Return packet too big.* in the Monitor Status Summary, then you have selected too many SNMP attributes to poll in a single request. Please modify your monitor to request smaller numbers of attributes

MIB Browser

When you click *Browse*, MIB browser appears when you do so. Select the MIB (top left), and the MIB variable (bottom left), and confirm the variable is the correct performance indicator (right panel) before adding this variable to a monitor with the *Select* button at the bottom of this browser. Not all values are necessarily available (or sensible) to monitor.

Figure 32-22. MIB Browser



```
The MIB module for SNMP entities.

Copyright (C) The Internet Society (2002). This
version of this MIB module is part of RFC 3418;
see the RFC itself for full legal notices.
```

Name	snmpInASNParseErrs
OID	1.3.6.1.2.1.11.6
Type	OBJECT-TYPE
Status	current
Syntax	INTEGER (Counter32) SIZE (0..4294967295)
Access	read-only

```
The total number of ASN.1 or BER errors encountered by
the SNMP entity when decoding received SNMP messages.
```

Notice that you can use the *Add / Delete* buttons near the top, left of this screen to add or delete new MIBs, too. You can check *Show OIDs* in the bottom left corner of the screen to display the numeric values for OID nodes in the MIB tree.

SNMP monitoring of Counter64 types cannot return values greater than 9,223,372,036,854,775,807 (the maximum signed 64-bit value). Counter64 types can capture the change per polling interval. This works, but the change must be less than the allowed maximum value or the application drops it.

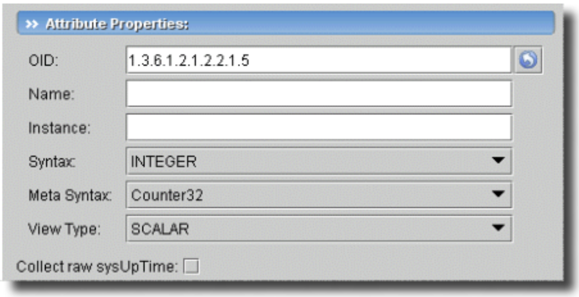
NOTE:

Monitoring generally is currently limited to the maximum value of a signed 64-bit number.

Add / Edit SNMP Attributes

Click *Delete* to remove a selected, already listed SNMP attribute. Click *Add* or *Browse* to create new variables to monitor. When you click *Add*, an editor panel with SNMP attribute parameters appears.

Figure 32-23. SNMP *Add* Editor



Attribute Properties:

OID: 1.3.6.1.2.1.2.2.1.5

Name:

Instance:

Syntax: INTEGER

Meta Syntax: Counter32

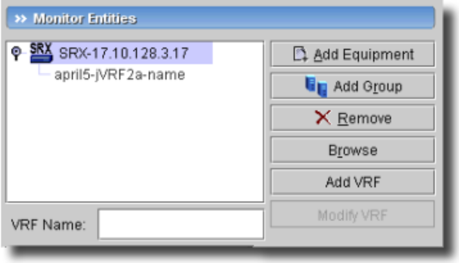
View Type: SCALAR

Collect raw sysUpTime: □

This panel displays the following fields where you can edit SNMP parameters:

- **OID**—The Object identifier for the attribute. Click the arrow to the right of this field to have OpenManage Network Manager populate the rest of the fields for the OID you enter. You can also manually add OIDs.
- **Name**—The text identifier for the OID
- **Instance**—The OID instance.
- **Syntax**—Select the type of variable with the pick list. For example: INTEGER
- **Meta Syntax**—Further refine the variable type with the pick list. For example: Counter32.
- **View type**—Select the type of view for the monitor with the pick list. For example: SCALAR.

Figure 32-24. VRF Monitor—Monitor Entities



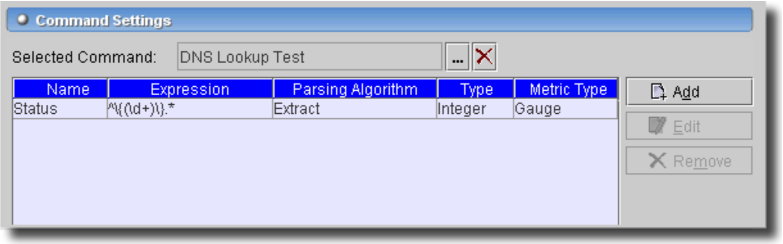
Monitor Entities

SRX-17.10.128.3.17
april5-jVRF2a-name

VRF Name:

When you select a device, or group of devices, and OpenManage Network Manager monitors all VRF names for the selected device(s). To confine monitoring to specific VRFs, this monitor includes *Browse*, *Add VRF* and *Modify VRF* buttons in the *Monitor Entities* portion of the General screen. *Browse* lets you select any VRF for the selected device. When you click *Add*, you can enter a VRF name below the listed monitored entities, and click *Add* to have it appear with the equipment. Click *Modify VRF* to revise the name of a selected VRF. Click *Remove* to delete either a device or a VRF.

Figure 32-25. DNS Lookup



Command Settings

Selected Command: DNS Lookup Test

Name	Expression	Parsing Algorithm	Type	Metric Type
Status	^\{(\d+)\}.*	Extract	Integer	Gauge

Default Monitors

Other, seeded monitors are available to add to the core set of monitors. Most packages include the monitors described in the following section. For some packages, these are active, by default, monitoring the group of all discovered entities, and for other packages, they are inactive, by default. Consult your sales representative for specifics.

- Interface Monitor
- ICMP Monitor
- WMI Monitor

You can *action -> Open* some of these monitors and edit them to provide more customized monitoring for your system.

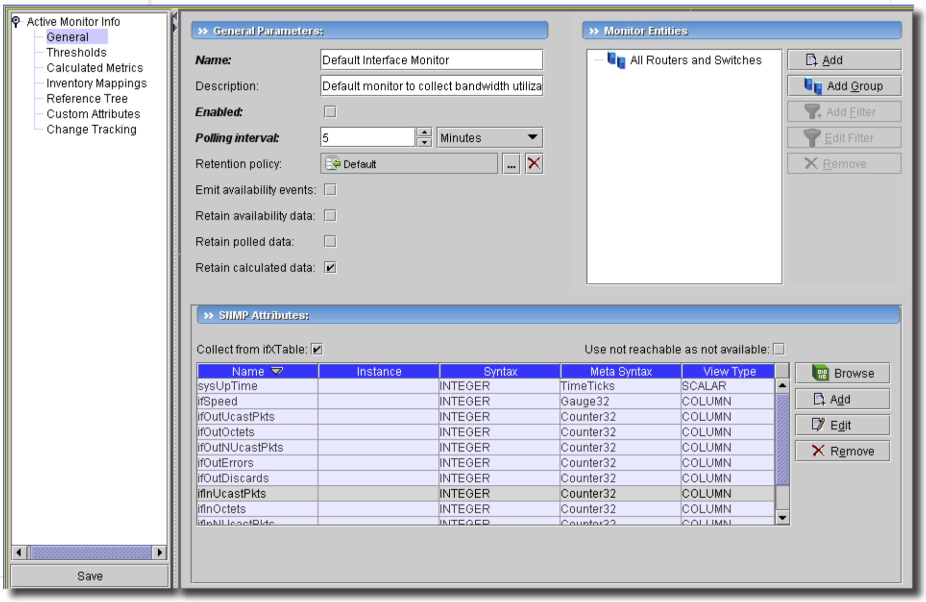
NOTE:

You can copy default monitors to customize them for your system. Monitors also provide report templates. Create a new report to configure the specifics, and select the automatically-provided template as its basis.

Interface Monitor

This monitor collects bandwidth utilization and error counts for interfaces

Figure 32-26. Default Interface Monitor



Name: Default Interface Monitor

Description: Default monitor to collect bandwidth utiliza

Enabled: □

Polling interval: 5 Minutes

Retention policy: Default

Emit availability events: □

Retain availability data: □

Retain polled data: □

Retain calculated data: ☑

All Routers and Switches

Collect from ifxTable: ☑

Use not reachable as not available: □

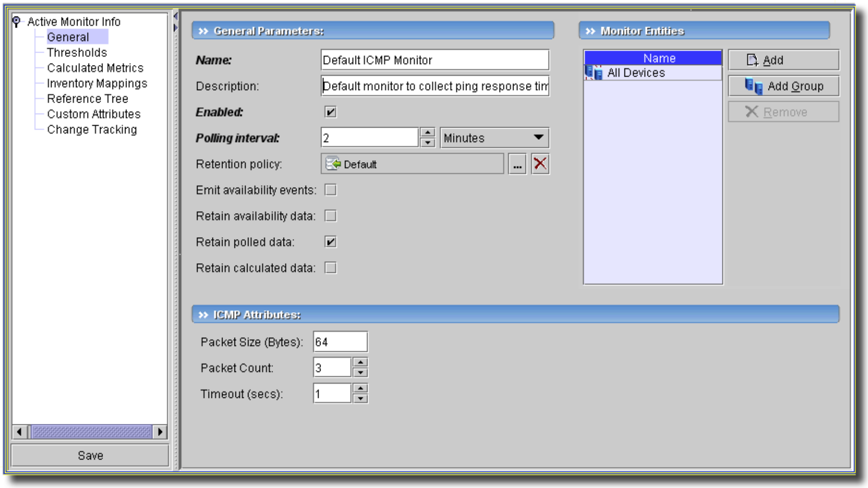
Name	Instance	Syntax	Meta Syntax	View Type
sysUpTime		INTEGER	TimeTicks	SCALAR
ifSpeed		INTEGER	Gauge32	COLUMN
ifOutUcastPkts		INTEGER	Counter32	COLUMN
ifOutOctets		INTEGER	Counter32	COLUMN
ifOutNUcastPkts		INTEGER	Counter32	COLUMN
ifOutErrors		INTEGER	Counter32	COLUMN
ifOutDiscards		INTEGER	Counter32	COLUMN
ifInUcastPkts		INTEGER	Counter32	COLUMN
ifInOctets		INTEGER	Counter32	COLUMN
ifInNUcastPkts		INTEGER	Counter32	COLUMN

The initial screen displays the SNMP attributes collected from the devices' ifxTable. The default group of interfaces comes from the *All Routers and Switches* group. The *Thresholds* and *Calculated Metrics* screens display the specifics of how these collected attributes are monitored. This is an SNMP monitor. See SNMP Attributes (Interfaces or Scalars) on page 793 for a discussion of SNMP monitoring capabilities.

ICMP Monitor

The default ICMP Monitor reports on ping response times for all devices.

Figure 32-27. Default ICMP Monitor



Name: Default ICMP Monitor

Description: Default monitor to collect ping response tim

Enabled: ☑

Polling interval: 2 Minutes

Retention policy: Default

Emit availability events: □

Retain availability data: □

Retain polled data: ☑

Retain calculated data: □

Name
All Devices

Packet Size (Bytes): 64

Packet Count: 3

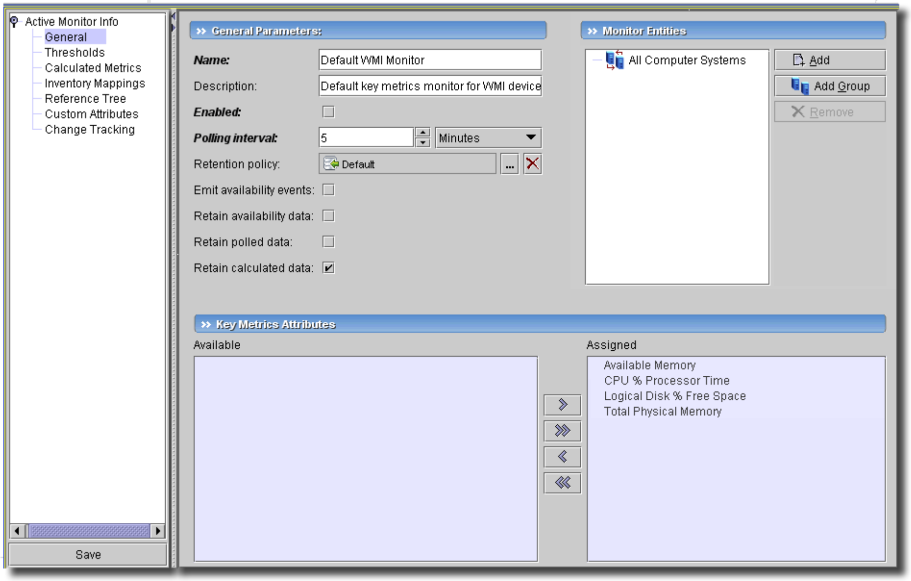
Timeout (secs): 1

The default sends three 64 byte packets every second to the *All Devices* group. See *ICMP on page 790* for more about this kind of monitor.

WMI Monitor

This is the default key metrics monitor for WMI devices

Figure 32-28. Default WMI Monitor



Name: Default WMI Monitor

Description: Default key metrics monitor for WMI device

Enabled: □

Polling interval: 5 Minutes

Retention policy: Default

Emit availability events: □

Retain availability data: □

Retain polled data: □

Retain calculated data: ☑

Monitor Entities: All Computer Systems

Available

Assigned

Available Memory
CPU % Processor Time
Logical Disk % Free Space
Total Physical Memory

By default, this monitor reports on the CPU, Memory Utilization, Logical Disk % Free Space, and Total Physical Memory for all Computer Systems. The *Thresholds* and *Calculated Metrics* screens display the specifics of how these collected attributes are monitored.

Scheduling Refresh Monitor Targets

Because monitors can address targets that are members of dynamic groups, refreshing these ensures that group memberships are up-to-date. To do this, you can create or alter the schedule for Monitor Target Refresh. When executed, this updates monitors with groups as targets based on current memberships. This removes targets no longer members of a monitored group and adds new group members. A seeded schedule refreshes these every six hours, by default.

The only information required when you create this schedule is a name to identify it and the *Schedule Info* that describes how often it occurs and when. See Chapter 30, Schedules for additional information about schedules.

33

Alarms

Alarms Overview

The Alarm screen lets you manage alarms and notifications (alarms are typically a subset of notifications or events). It displays information about, and lets you acknowledge, received alarms or events. This screen also provide tools that help operators diagnose and correct alarms. Select *File -> Open -> Event Services -> Alarms* from the menu or the Navigation Pane to display Alarms.

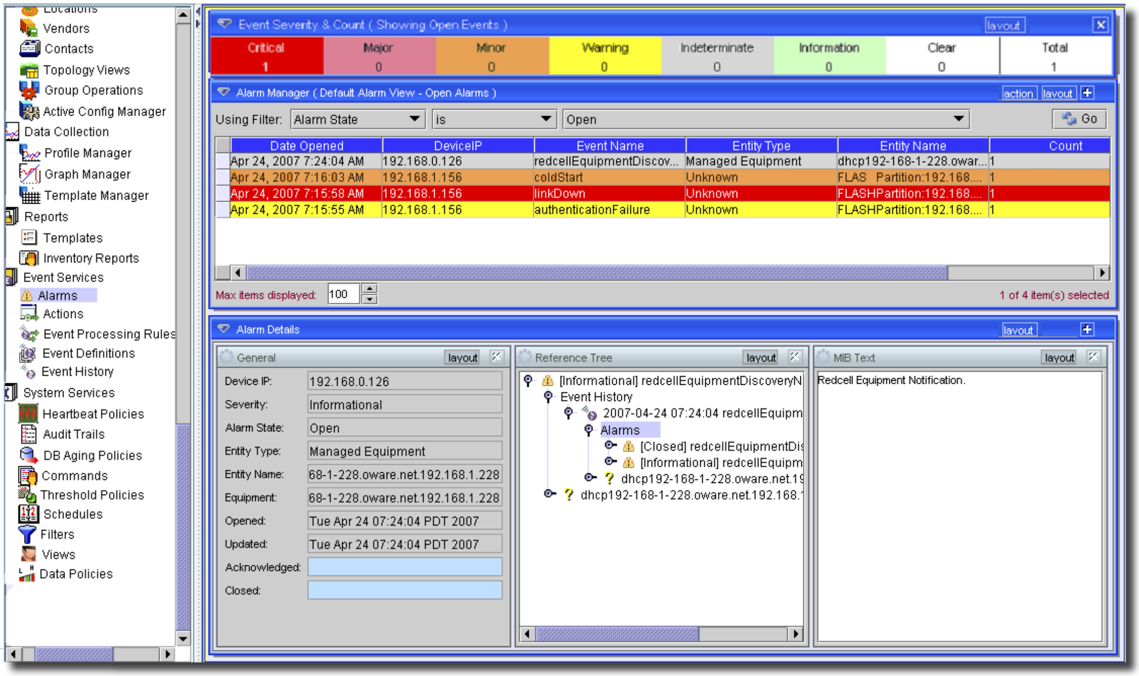
CAUTION:
While there is no theoretical limit to the number of active alarms, you can optimize application performance by keeping less than 100,000 active alarms with database aging policies. (See Chapter 25, DB Aging, specifically Alarm DAP Parameters on page 719, for more about that capability).

Event History lets you view all notifications, not just the alarm subset. See Event History on page 832.

Alarms

The Alarm screens display real time updates of new Alarms entering the system, or alarms created from the window launch time or change of view time. It can include the Alarm Severity and Count panel at the top of the screen, the *Alarm Manager* panel to display and manage events and alarms, and the *Alarm Details* panels in the lowest part of this screen that displays details about the alarm selected in the *Manager* panel.

Figure 33-1. Alarms



Event Severity & Count (Showing Open Events)

Critical	Major	Minor	Warning	Indeterminate	Information	Clear	Total
1	0	0	0	0	0	0	1

Alarm Manager (Default Alarm View - Open Alarms)

Using Filter: Alarm State is Open

Date Opened	DeviceIP	Event Name	Entity Type	Entity Name	Count
Apr 24, 2007 7:24:04 AM	192.168.0.126	redcellEquipmentDiscov...	Managed Equipment	dhcp192-168-1-228.owar...	1
Apr 24, 2007 7:16:03 AM	192.168.1.156	coldStart	Unknown	FLAS Partition:192.168....	1
Apr 24, 2007 7:15:58 AM	192.168.1.156	linkDown	Unknown	FLASHPartition:192.168....	1
Apr 24, 2007 7:15:55 AM	192.168.1.156	authenticationFailure	Unknown	FLASHPartition:192.168....	1

Max items displayed: 100

1 of 4 item(s) selected

Alarm Details

General

Device IP:	192.168.0.126
Severity:	Informational
Alarm State:	Open
Entity Type:	Managed Equipment
Entity Name:	68-1-228.oware.net.192.168.1.228
Equipment:	68-1-228.oware.net.192.168.1.228
Opened:	Tue Apr 24 07:24:04 PDT 2007
Updated:	Tue Apr 24 07:24:04 PDT 2007
Acknowledged:	
Closed:	

Reference Tree

```
[Informational] redcellEquipmentDiscoveryN
  Event History
    2007-04-24 07:24:04 redcellEquipm
      Alarms
        [Closed] redcellEquipmentDis
        [Informational] redcellEquipm
      dhcp192-168-1-228.oware.net.19
  dhcp192-168-1-228.oware.net.192.168.1
```

MIB Text

Redcell Equipment Notification.

A specialized layout displays alarms internal to the OpenManage Network Manager system. See Self Management / EMS Alarms on page 810. The following sections discuss these Alarm-related topics:

- Alarm Severity and Count
- Alarm Manager
- Alarm Table Columns
- Alarm Details
- Archiving Alarms

See also Alarm Table Columns on page 807 for a description of the columns visible in this display of alarms.

You can make changes to a view by clicking and dragging columns in the Alarm tables directly in the Alarm screen. Such changes last only for the current session. You can also change the displayed columns with the plus (+) sign above the panel displaying alarms. Available columns are described in Alarm Table Columns on page 807.

You can also do the following:

- Sort Ascending/descending.
- Remove /Insert columns. See Alarm Table Columns on page 807 for a brief explanation of each Alarm attribute column type.

- Move Columns—Click the column header of the column you want to move and drag it to its new location.
- Resize Columns—Click the column header of the column you want to resize and drag to resize the column. The column margin is located between the column headers. Typically, best practice is to click the column margin to the right of the column you want to resize.

Alarms displayed here refresh every 30 seconds, unless you modify or override the default interval as specified in `redcell.properties`.

Unrecognized Events

Installed device drivers classify events in the Event Definitions (see Event Definitions on page 825). The default behavior is contained in that classification. You can look in the Event Definitions to find a specific event, and open it to see what alarm (or other) behavior occurs when that event arrives.

The global default occurs when the event does not match any installed by the drivers. Such events are name-resolved, as far as is possible, and appear as *Indeterminate* alarms.

Alarm Severity and Count

This panel displays the count of Alarms by severity, and totals them on the right.

This can either display *All Alarms* or *Open Alarms*. Change between these counts by clicking the *Layout* button. Select *Change Filter* and choose the *All Alarms* or *Open Alarms* items. The alarm counts that appear in each panel may exceed the rows of alarms in the Alarm Manager since one row can concatenate several alarms.

Alarms displayed are color-coded based on their severity, and appear until cleared. A total of uncleared alarms, listed both by category and in sum, appears at the top of the Alarm screen. The *Alarm Severity & Count* table at the top of the Alarm screen contains totals for the filtered view (all and unacknowledged), not grand totals from a database count.

See Chapter 34, Events, Rules and Actions for information about defining events for display in the Alarm screen. Because the Alarm window is asynchronously threaded, the behavior of the progress bar may be inconsistent. It may start and stop one or more times during a transitional start (for example: changing filters).

⚠ **CAUTION:**
Unless you create a filter and save it as described in Chapter 28, Filters, filters you make here are not preserved.

The application ships with a set of default event/alarm severity definitions each with its own default color and sound. You can change the colors and sounds in the menu item *Settings -> Configuration -> Control Settings*, in the *Alarm Severities* tab. See the A*dministration Section* for more information.

The default severity definitions are:

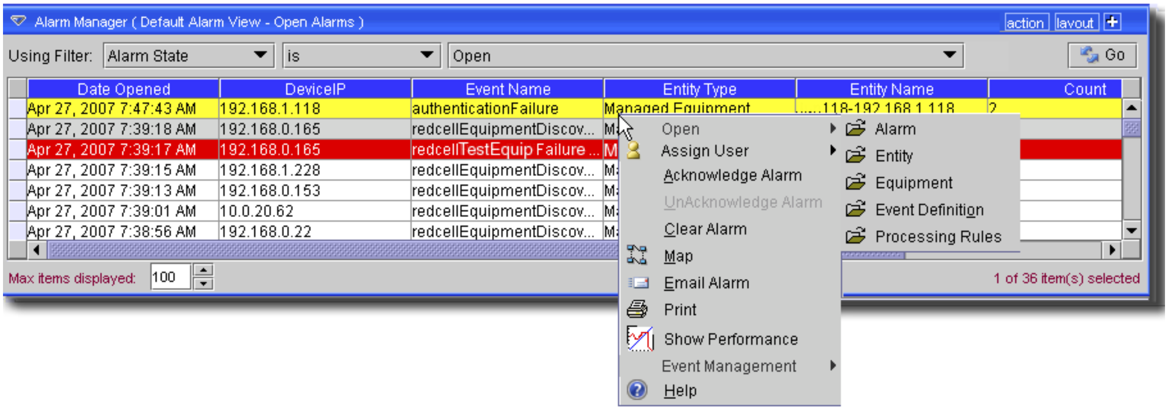
- **Critical**—A service-halting condition occurs, requiring immediate corrective action. The equipment is completely out of service and you must restore its capability.
- **Major**—A service-affecting condition has developed and corrective action is required. There is a severe degradation in the equipment's capability and you must restore its full capability.
- **Minor**—A non-service-affecting fault condition exists and corrective action should be taken in order to prevent a more serious fault. The detected alarm condition is not currently degrading the capacity of the equipment.
- **Warning**—A potential or impending service-affecting fault could occur, and no significant effects have yet been felt. Action should be taken to further diagnose and correct the problem to prevent it from becoming a more serious service-affecting fault. The detected alarm condition does not currently pose a problem, but may degrade the capacity of the equipment if you do not take corrective action.
- **Indeterminate**—The severity level cannot be determined.
- **Information**—General information about the condition of the object, device, or system.
- **Cleared**—The problem is corrected, and the correlated alarm is cleared from the Active Alarm table.

Alarm Manager

In the *Default* filter, only open alarms appear on these screens. You can change displayed columns (Alarm attributes) with the plus (+) button near the top of the screen, and modify filters to restrict the alarms that appear in the display (see Chapter 28, Filters for more about filters). You can filter on most attributes described in Alarm Table Columns on page 807.

For example, you could filter to see alarms that are major and above for only selected equipment.

Figure 33-2. Alarm Manager



Alarm Manager (Default Alarm View - Open Alarms)

Using Filter: Alarm State | is | Open

Date Opened	DeviceIP	Event Name	Entity Type	Entity Name	Count
Apr 27, 2007 7:47:43 AM	192.168.1.118	authenticationFailure	Managed Equipment	......118-192.168.1.118	2
Apr 27, 2007 7:39:18 AM	192.168.0.165	redcellEquipmentDiscov...	Ma		
Apr 27, 2007 7:39:17 AM	192.168.0.165	redcellTestEquip Failure ...	M		
Apr 27, 2007 7:39:15 AM	192.168.1.228	redcellEquipmentDiscov...	Ma		
Apr 27, 2007 7:39:13 AM	192.168.0.153	redcellEquipmentDiscov...	Ma		
Apr 27, 2007 7:39:01 AM	10.0.20.62	redcellEquipmentDiscov...	Ma		
Apr 27, 2007 7:38:56 AM	192.168.0.22	redcellEquipmentDiscov...	Ma		

Max items displayed: 100

1 of 36 item(s) selected

See also Alarm Table Columns on page 807 for a description of the columns visible in this display of alarms. The *Action* or right-click menu displays the following items (some installations conceal some of these):

- **Open -> Entity—**This opens an editor where you can configure the device from which this alarm came. See Editing Resources on page 217.

- **Open -> Alarm—**Opens a screen describing all the details of the selected alarm. See Alarm Details on page 809.

- **Open -> Event Definition—**This opens an editor where you can configure the device from which this alarm came. See Event Definitions on page 825.

- **Open -> Equipment**—This opens an editor where you can configure the device from which this alarm came (an *Entity*, if different, is a subcomponent of the equipment). See Editing Resources on page 217.

- **Open -> Processing Rules**—This opens an editor where you can configure the rules from which this alarm came. See Event Processing Rules on page 815.

- **Acknowledge Alarm**—Acknowledges the selected Alarm(s). The current date and time appear in the Ack Time field, and the name of the currently logged-on user appears in the Ack By field.

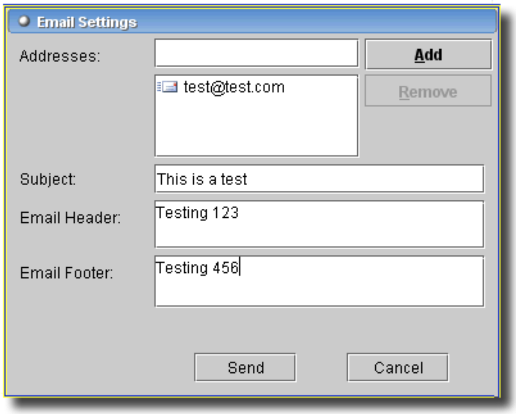
- **Unacknowledge Alarm**—Unacknowledges previously acknowledged alarm(s), and clears the entries in the Ack By and Ack Time fields.

- **Assign User—**Assign this alarm to one of the users displayed in the sub-menu by selecting that user.

- **Map**—Open a topology view displaying the equipment selected alarm(s) came from. See Chapter 21, Topology Views.

- **Email Alarm**—E-mail the alarm.

Figure 33-3. E-mail the Alarm



Email Settings

Addresses: test@test.com

Subject: This is a test

Email Header: Testing 123

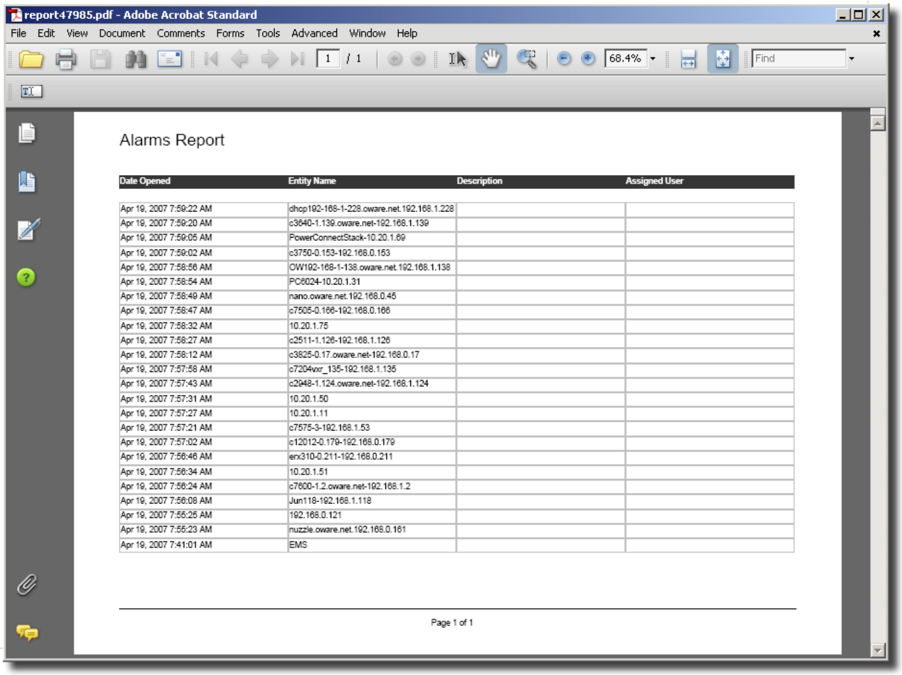
Email Footer: Testing 456

Enter an e-mail address to which you want to mail the alarm’s content, and click *Add* in the subsequent screen when you select this option. You can also type a subject, header and footer in the provided spaces, then click *Send*. Clicking *Cancel* ends this operation without sending e-mail. Refer to the *Administration Section* for instructions about setting up e-mail from this software.

- **Clear Alarm**—Select this option to clear the alarm. Clearing the alarm removes the alarm from the default alarm view and marks it as a candidate for DAP. Essentially it is an indication to the system that the alarm has been resolved/addressed. If propagation policies are enabled it causes a recalculation of dependent alarms.

- **Print**—Prints the displayed Alarms to a pdf file.

Figure 33-4. Printed Alarms (pdf)



Alarms Report

Date Opened	Entity Name	Description	Assigned User
Apr 19, 2007 7:59:22 AM	dhcp192-168-1-228.oware.net.192.168.1.228		
Apr 19, 2007 7:59:20 AM	c3640-1.139.oware.net-192.168.1.139		
Apr 19, 2007 7:59:05 AM	PowerConnectStack-10.20.1.69		
Apr 19, 2007 7:59:02 AM	c3750-0.153-192.168.0.153		
Apr 19, 2007 7:58:56 AM	OW192-168-1-138.oware.net.192.168.1.138		
Apr 19, 2007 7:58:54 AM	PC6024-10.20.1.31		
Apr 19, 2007 7:58:49 AM	nano.oware.net.192.168.0.45		
Apr 19, 2007 7:58:47 AM	c7505-0.166-192.168.0.166		
Apr 19, 2007 7:58:32 AM	10.20.1.75		
Apr 19, 2007 7:58:27 AM	c2511-1.126-192.168.1.126		
Apr 19, 2007 7:58:12 AM	c3825-0.17.oware.net-192.168.0.17		
Apr 19, 2007 7:57:58 AM	c7204vxr_135-192.168.1.135		
Apr 19, 2007 7:57:43 AM	c2948-1.124.oware.net-192.168.1.124		
Apr 19, 2007 7:57:31 AM	10.20.1.50		
Apr 19, 2007 7:57:27 AM	10.20.1.11		
Apr 19, 2007 7:57:21 AM	c7575-3-192.168.1.53		
Apr 19, 2007 7:57:02 AM	c12012-0.179-192.168.0.179		
Apr 19, 2007 7:56:46 AM	erx310-0.211-192.168.0.211		
Apr 19, 2007 7:56:34 AM	10.20.1.51		
Apr 19, 2007 7:56:24 AM	c7600-1.2.oware.net-192.168.1.2		
Apr 19, 2007 7:56:08 AM	Jun118-192.168.1.118		
Apr 19, 2007 7:55:25 AM	192.168.0.121		
Apr 19, 2007 7:55:23 AM	nuzzle.oware.net.192.168.0.161		
Apr 19, 2007 7:41:01 AM	EMS		

Page 1 of 1

You can print or save this report from Acrobat. If you do not have the free Acrobat reader, you can download it from www.adobe.com.

- **Show Performance**—When you select this command OpenManage Network Manager finds all of the performance attributes being monitored for the selected equipment and creates a dashboard with one dashboard component for each attribute. (See Chapter 32, Active Performance Monitor for details.)

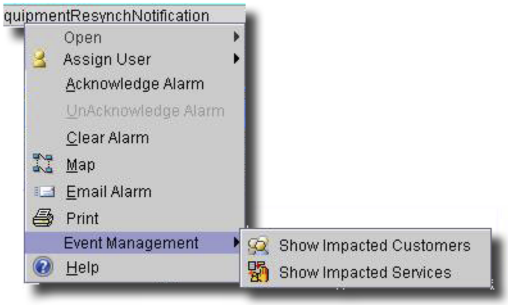
  If you multi-select more than one device, each component shows the top five metrics for each attribute. If you select only one top-level device, OpenManage Network Manager searches the device's interface and port children for performance attributes and these attributes appear with the top five children for each attribute.

The data that appears is based on the monitors that are monitoring that device and where Retain Data is checked. If you have several monitors and you are retaining data on those monitors, the screen reflects those data points.

If you select two devices in Resources manager and click action -> Show performance, OpenManage Network Manager displays both of the devices' common attributes in the form. (You cannot display interface data because the devices do not have interfaces in common.)

- **Event Management**—This menu lets you see Customers or Services related to the selected Alarm.

Figure 33-5. Event Management



Selecting these menu items displays the a filtered Customer or Service manager. If the alarm is unrelated to customers or services, a *No impacted entities were found for the selected alarm(s)* message appears.

NOTE:

If a related entity exists, a reminder of the source alarm appears in the title bar of the manager that appears with the related customer /service.

- **Help**—Select this option to open online help for this screen.

NOTE:

You can automate responses to alarms with Event Processing rules. For example, an alarm can trigger an e-mail. See Event Processing Rules on page 815.

Alarm Table Columns

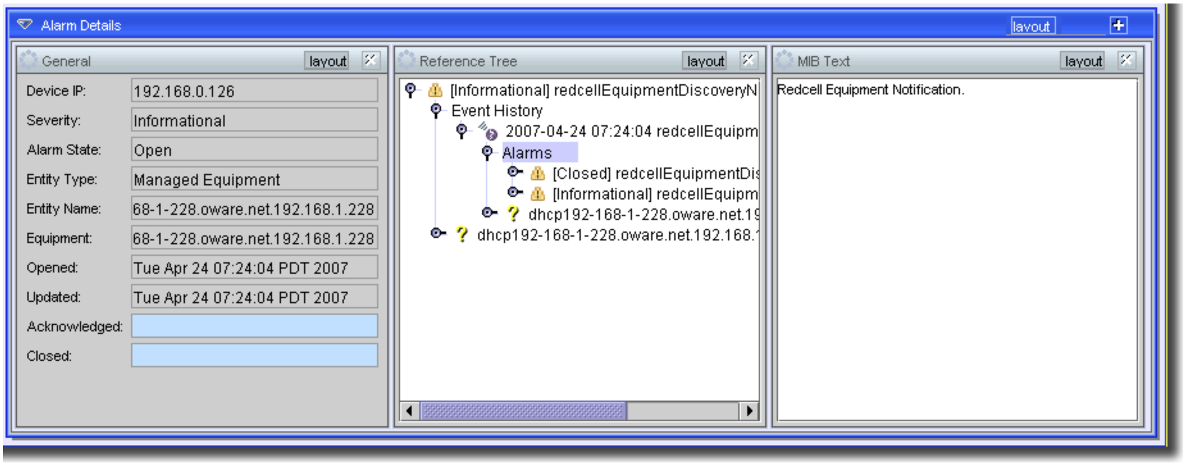
The following describes the columns that appear in the Alarm table. You can use any or all of the attribute columns in a view, and you can use all attribute columns (except as noted). You can alter the view by dragging the column headers up to delete a column, or by clicking the plus (+) at the top right of the manager and selecting column names, then clicking *Add Column*. Added columns appear to the right of those already there. The following are the attribute columns, in alphabetic order following the default columns:

- **Ack By**—Records the user who acknowledged the alarm.
- **Ack Time**—The time the alarm was acknowledged.
- **Acknowledged**—*True* or *False*.
- **Alarm State**—The state (open / closed) of the alarm.
- **Assigned by**—The user who assigned the alarm to the *Assigned User*.
- **Assigned User**—The user who has been assigned this alarm (right click or click *Action* to do this).
- **Count**—The number of similar alarms.
- **Date Assigned**—The date and time that the alarm was assigned.
- **Date Cleared**—The date and time that the alarm was closed.
- **Date Opened**—The date the alarm appeared.
- **DeviceIP**—The IP address of the equipment where the alarm appeared.
- **Entity Name**—The entity emitting this alarm (often within the Equipment).
- **Entity Type**—The object ID of the entity related to this alarm.
- **Equipment**—The name for the entity emitting the alarm.
- **Event Name**—The name for the event at the source of the alarm.
- **Location**—The location where the entity emitting the alarm exists.
- **Message**—The alarm message.
- **Notification OID**—The identifier of the notification displayed as an alarm.
- **Region**—The region (partition) where the equipment emitting this alarm exists.
- **Severity**—The severity of the alarm. The severity only has meaning for Alarms and Security Alarms. Informational Alarms get a severity level of Indeterminate.
- **Service Effecting**—Indicates whether the alarm row is service-effecting. Only service-effecting alarms propagate to appear as components of service- and link-related alarms. Service-effecting alarms are of indeterminate or greater severity.
- **UpdateDate Time**—The time stamp for when this alarm was updated (for an additional count, the time the last duplicate was received).

Alarm Details

The Alarms screen provides a display of a selected Alarm's details at the bottom of the default layout. Display the Alarm Detail window from the Alarm screen by selecting the Alarm for which you want detailed information.

Figure 33-6. Alarm Details



Device IP: 192.168.0.126
Severity: Informational
Alarm State: Open
Entity Type: Managed Equipment
Entity Name: 68-1-228.oware.net.192.168.1.228
Equipment: 68-1-228.oware.net.192.168.1.228
Opened: Tue Apr 24 07:24:04 PDT 2007
Updated: Tue Apr 24 07:24:04 PDT 2007
Acknowledged:
Closed:

[Informational] redcellEquipmentDiscoveryN
Event History
2007-04-24 07:24:04 redcellEquipm
Alarms
[Closed] redcellEquipmentDis
[Informational] redcellEquipm
dhcp192-168-1-228.oware.net.19
dhcp192-168-1-228.oware.net.192.168.1

Redcell Equipment Notification.

This includes the *General*, *Notification Details, and Reference Tree* panels: See Alarm Table Columns on page 807 for a description of the fields in the general panel. Here are the fields in the *Notification Details* panel:

- **Name**—The name of the notification generating the notification.

- **Source IP**—The IP address generating the notification.

- **Receive Time**—The timestamp when this notification arrived at the application server.

- **Region**—The partition generating the notification.

- **Entity name**—The entity generating the notification.

- **Protocol**—The protocol transmitting the notification.

- **Type OID**—The object ID for the type of notification.

- **Instance ID**—The ID for the instance of this type of notification.

- **Entity OID**—The object ID for the entity generating the notification.

- **Entity Type**—The type of entity generating the notification.

The *Reference Tree* displays a graphic description of the connection between this alarm, its originating notification, and any actions and/or correlations.

The *MIB Text* panel displays any text in the MIB for the selected alarm.

The *Advisory Text* panel lets you enter any advisory text needed to accompany the selected alarm.

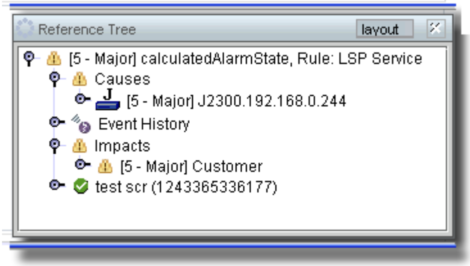
NOTE:

To export alarms to a file, create an alarm report, then save it in the appropriate format.

Causes and Impacts for Links and Service Alarms

In addition to the typical *Reference Tree* nodes that appear for all alarms, sub-components appear with *Reference Tree* nodes displaying *Causes* and *Impacts* for links, and for services when you have OpenManage Network Manager's service applications installed. These nodes catalog alarms related to links or services or their subcomponents

Figure 33-7. Causes and Impacts for Service Alarms



- [5 - Major] calculatedAlarmState, Rule: LSP Service
  - Causes
    - [5 - Major] J2300.192.168.0.244
  - Event History
  - Impacts
    - [5 - Major] Customer
  - test scr (1243365336177)

For *Causes*, these display subnodes with the equipment source(s) of the alarm. *Impacts* also shows the links' or services' configured connection to customers.

Archiving Alarms

To ensure your database does not fill up with Alarms, you can archive them with a Database Aging Policy. See Chapter 25, DB Aging for details. The default database aging policy (DAP) exists for Events in Event History, but is not scheduled, again by default. Events can come into the system at fairly high rates, and as a result can consume space in the database at similar rates. Review the default DAP and default schedule to ensure that it is aggressive enough for your deployed system.

Self Management / EMS Alarms

The *Self Management* layout displays alarms for the Element Management System (EMS) only. These are alarms for internal events like a user's logon. See the Events that contain *ems* in the Event Definitions.

To open this screen and see this set of internal alarms, select the *Self Management* layout at the top of the client window. The display is like what is appears in Alarm Manager on page 804.

Testing Receipt of Alarms

If you want to test whether your system receives traps, you can test it with a trap generating application like Mimic or TrapGen. If you plan to test with artificially generated traps, first use the Discovery Wizard (see Discovery on page 187) to discover the device you want to initiate these traps (otherwise traps appear as “unknown”).

TrapGen is free from www.ncomtech.com. Here is an example command line for an installation of TrapGen:

```
trapgen -d [destination IP]:[port] -i [initiator’s IP] -g [trap type] -s
   [specific type]
```

```
trapgen -d 192.168.0.95:162 -i 192.168.1.156 -g 0 -s 0
```

Use `trapgen -h` to see all available commands.

CAUTION:

If you install a trap viewer, like the free one offered by Network Computing Technologies (they offer TrapGen), other applications competing for the trap listening port (162) do not allow this application to correctly receive traps. TrapGen is not supported as part of this application. Install and use it at your own risk.

34

Events, Rules and Actions

Overview of Events, Rules and Actions

The following screens let you configure this application to react, according to rules, to internal events, and implement configured actions. For example, you can configure the application to act when a backup occurs (and, say, send an e-mail). You can also configure reactions to certain failures. For example, if pushing a configuration file to a device fails, an event can trigger a rule with an action to restore the last known good configuration. This provides powerful capabilities.

CAUTION:
Configuring circular or self-referred actions can severely impact this system’s performance.

The following sections describe correlating and configuring events, and their mapped actions.

Terms

The following terms appear throughout the explanations that follow:

- **Action**—The outcome of the event, after processed by any Event Processing Rules.

- **Alarm**—Some, but not all, events appear as alarms, notifying users in the *Alarm* display.

- **Correlation**—A general term describing the interaction of events. A redundant event that is also an Alarm can simply increase the Alarm count, for example, rather than creating a new Alarm.

- **Event**—A message within the Element Management System (EMS). See Event Definitions on page 825 for a description of configuring these.

- **Event Processing Rules**—Rules that specify the interaction between events, and any *Action* outcome. See Event Processing Rules on page 815, and Actions Manager on page 835

- **Reject**—When you configure an event to be *Reject*ed, it goes no further in the EMS.

- **Suppress**—When you configure an event to be *Suppress*ed, it appears in the screen described in *Event History on page* 832, but nowhere else.

- **Message Template**—Part of Event Definitions. These are messages to be matched when you correlate events. See Message Template on page 829.

Some Example Use Cases

- Without any special configurations, when Alarms arrive at the same severity, they increment the alarm count on the first one that arrives.

- If you configure correlation, then when a correlated incoming alarm's key bindings match the initial alarm, that same count increment occurs. If they do not match, the system generates a new alarm
- If you configure correlation, and the Message Template or Severity do not match for otherwise matching alarms, then the EMS closes the existing alarm and opens a new alarm.

Performance, Syslog and Traps

By default, this application generates alarms and event notifications for every event definition. This provides maximum visibility for messages received. The caveat is that such a strategy can be processor-intensive, unless its is well managed. Best practice is to determine which traps or syslog messages are essential, and should generate events or events and alarms, and which traps to reject without processing.

Because it is typically verbose, syslog has a potential to produce many events that would consume processor time unnecessarily. The default for syslog is for the system to *accept* for such messages, generating an event for Event History without generating an alarm, but even this consumes processor time.

Best practice is therefore to limit syslog messages on the device itself, restricting them even before they get to the EMS. A typical solution is to configure the device to forward only the categories of syslog messages that generate alarms. The alternative is degraded performance.

Escalating Syslog

This application has a single Event Definition for all Syslog messages. If you create a new Event Processing Rule – Syslog, then it can escalate certain Syslog messages. The User Interface displays it as *Syslog Escalation Policy.* See Event Processing Rules below for more about creating these.

Some use cases:

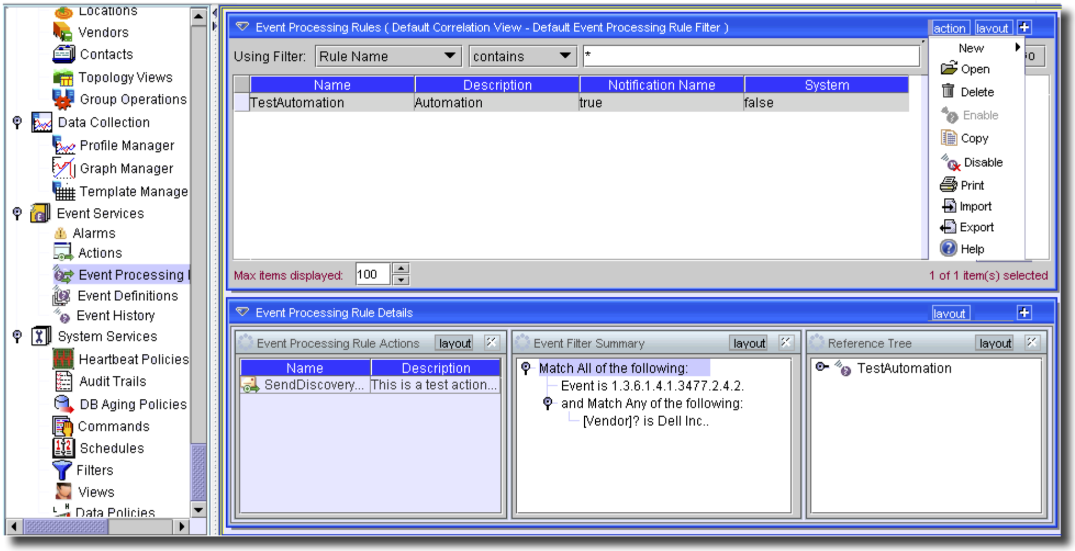
- If you are receiving too many Syslog messages and want to quiet them down some, create a Syslog escalation rule to escalate only the desired messages, then alter the Event Definition for Syslog messages to *reject* all others. This rejects all Syslog messages except the messages you have filtered in the escalation.
- If you want such messages to have a higher severity than the default Syslog Event Definition, then create the escalation with that higher severity.
- If you want to search for certain strings in the Syslog message and raise the severity based on that string, make a new escalation rule with these characteristics.
- If you want to tie an action to a certain Syslog messages, then add an action to the rule. (see Action Editor on page 836)
- If you only want to use Syslog for security purposes, you can create an escalation rule to look for only security messages and reject the rest.

These capabilities increase the power and flexibility of your response to syslog messages.

Event Processing Rules

This manager lets you configure rules for event processing.

Figure 34-1. Event Processing Rules



Event Processing Rules (Default Correlation View - Default Event Processing Rule Filter)

Using Filter: Rule Name | contains | *

Name	Description	Notification Name	System
TestAutomation	Automation	true	false

Max items displayed: 100

1 of 1 item(s) selected

Event Processing Rule Details

Event Processing Rule Actions

Name	Description
SendDiscovery...	This is a test action...

Event Filter Summary

Match All of the following:
Event is 1.3.6.1.4.1.3477.2.4.2.
and Match Any of the following:
[Vendor]? is Dell Inc..

Reference Tree

TestAutomation

This screen lets you filter a list of processing rules based on *Description*, *Enabled*, *Event Name*, *Owner*, *Rule Name*, *Rule Type*, *Valid*. Some of these (and *icon*) are columns in the table of rules.

⚠ **CAUTION:**
Unless you create a filter and save it as described in Chapter 28, Filters, filters you make here are not preserved.

As in a typical manager, the filter is at the top of the screen. With this manager you can configure rules that respond to internal events in the EMS. The manager has the following *Action* menu items (accessed with the *Action* button, or a right-click):

- **New**—Lets you select among the different types of editor for the rule you are configuring. Available types include the following:

  Automation–Opens the Automation Event Processing Rule Editor on page 816 through which you can define a new Action.

  Correlation–Opens the Correlation Event Processing Rule Editor on page 819 where you can create or modify this type of rule.

  Syslog–Opens the Syslog Event Processing Rule Editor on page 823, where you can configure syslog escalation rules.

- **Open**—Opens the selected Action for modification. See Action Editor on page 836 for more information.

- **Enable**—Enables the selected rule(s).
- **Copy**—This copies the selected rule and opens the editor. You must rename it to begin with something other than "CopyOf [Original Name]" (its default name) before you can save the rule.

NOTE:

If you want to change the behavior of a system rule, copy it, then disable it. Then configure the copy do the desired behavior.

- **Disable**—Disables the selected rule(s).
- **Delete**—Deletes the selected action. Select the action to remove and click *Delete*. The application prompts you for confirmation.
- **Print**—Print the listed correlations to an Acrobat file. (You must have Acrobat reader installed for this to work correctly.) Change the filter and click *Go* to change this printed report's appearance.
- **Export/Import**—Export or import the rule as/from XML.

NOTE:

If you export a disabled rule, it is enabled on import, by default.

- **Help**—Open the context-sensitive help for this screen.

Event Processing Rule Details

The lowest portion of this layout contains detail panels that display *Event Processing Rule Actions* for the selected rule. These describe the actions connected to a rule. When rules are not part of the *System*, you can right click an action and edit it in Action Editor.

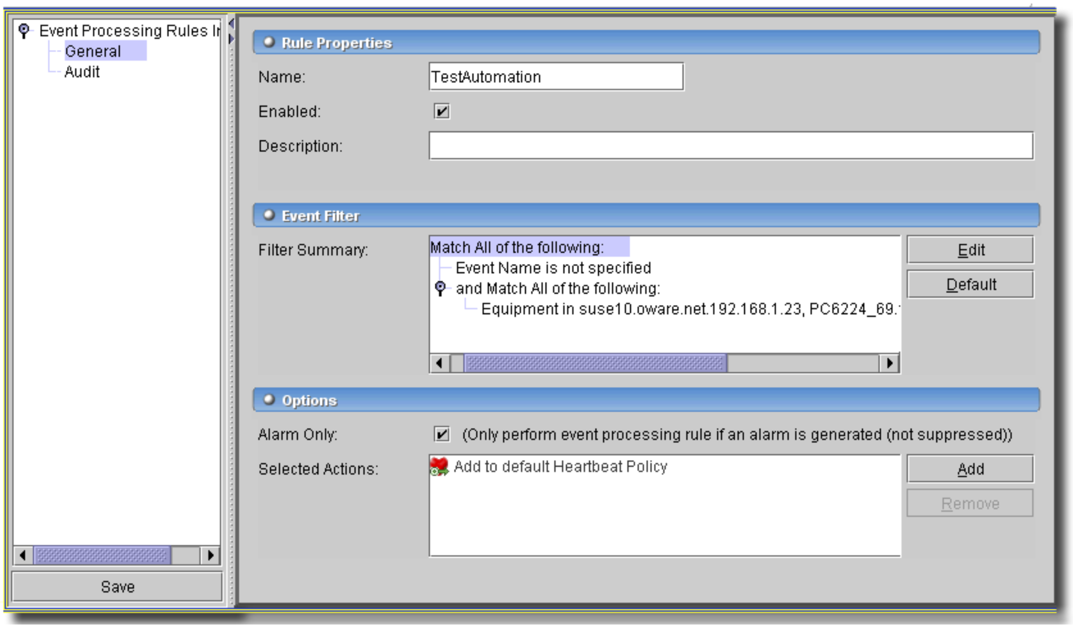
The *Event Filter Summary* displays the filter information for the selected rule in a tree format.

Finally, the *Reference Tree* for the selected rule displays any related actions and event processing rules in a tree.

Automation Event Processing Rule Editor

This editor lets you create new or modify existing event processing automation rules. Among other things, these correlate events with actions that they trigger.

Figure 34-2. Automation Event Processing Rule Editor



Name: TestAutomation

Enabled: ☑

Description:

Filter Summary:
Match All of the following:
Event Name is not specified
and Match All of the following:
Equipment in suse10.oware.net.192.168.1.23, PC6224_69.

Alarm Only: ☑ (Only perform event processing rule if an alarm is generated (not suppressed))

Selected Actions: Add to default Heartbeat Policy

This editor has the following fields and selection options:

Rule Properties

- **Name**—A text identifier for the rule.
- **Enabled**—Check to enable this rule's action.
- **Alarm Only**—Check to enable this rule's action only when the system first generates an alarm without suppressing it. Subsequent alarms do not trigger the rule.
- **Description**—A text description of the rule.

Event Filter

Click *Add* to create an event filter criterion for this rule (or *Edit* to configure an existing set of criteria), so the rule only appears for certain events, equipment, vendors, and so on. This opens the Event Filter Criteria editor. Click *Default* to revert to the event filter's unaltered default criteria. A prompt appears confirming this selection. You must enter a filter before saving.

NOTE:

Fewer rules, and more selective filters favor good system performance.

Options

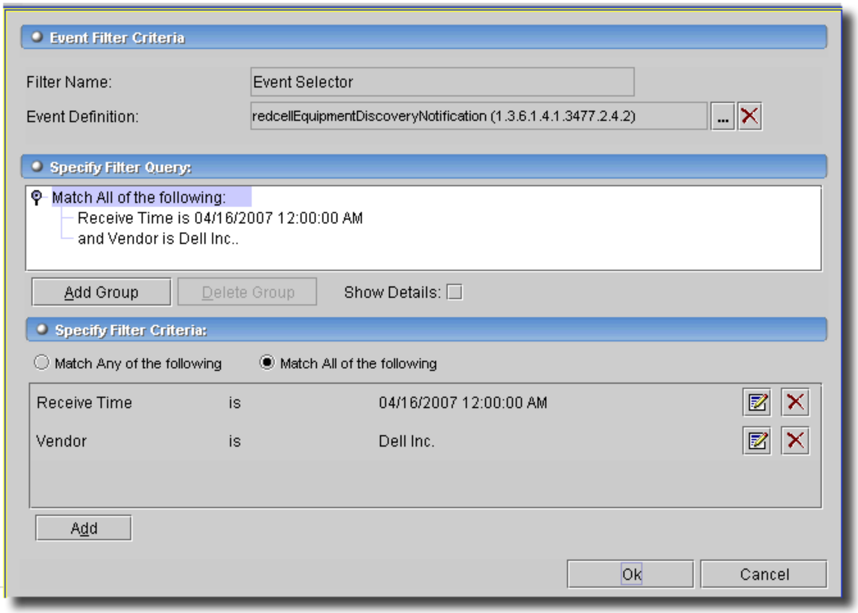
Check the *Alarm Only* checkbox to process an event with this rule only if an alarm is generated, not suppressed. See Correlation Event Processing Rule Editor on page 819 for options that appear when you select a correlation event. These can include Reject Event, Set Severity, Suppress Alarm, Device Access, Frequency and State Flutter.

Click *Add* to select an action created in *Actions Manager on page* 835. You can also click *New* in the subsequent selector screen to create a new action as described in that section. You can create a rule as you would in Actions Manager in the selector too. Notice that you can elect to have multiple actions occur for a single event.

Event Filter Criteria

This screen configures what must match for the processing rule to run.

Figure 34-3. Event Filter Criteria



Event Filter Criteria

Filter Name: Event Selector

Event Definition: redcellEquipmentDiscoveryNotification (1.3.6.1.4.1.3477.2.4.2)

Specify Filter Query:

Match All of the following:
Receive Time is 04/16/2007 12:00:00 AM
and Vendor is Dell Inc..

Show Details: □

Specify Filter Criteria:

○ Match Any of the following ● Match All of the following

Receive Time	is	04/16/2007 12:00:00 AM
Vendor	is	Dell Inc.

It has the following sections, fields and selectors:

Event Filter Criteria

- **Filter Name**—A text identifier for the filter.

- **Event Definition**—You can optionally select an event with the command button (...), or delete it with the red “X” button. Selecting an event is not necessary, but if you do select one, the available filter criteria below are limited to those appropriate to the event selected. If you select no event, then only generic filter criteria appear in the next section of the screen.

NOTE:

If you want to filter on event varbind data, then select the event. The varbind attributes appear in the lowest panel.

Specify Filter Query

Click *Add Group* to create a group of matching criteria. The *Match Any of the following* and *Match All of the following* radio buttons determine whether the selected group of criteria is configured with a logical *OR* or a logical *AND* for its components.

Click *Add* to create criteria. Edit these as described in *Filter Editor on page* 736.

Audit

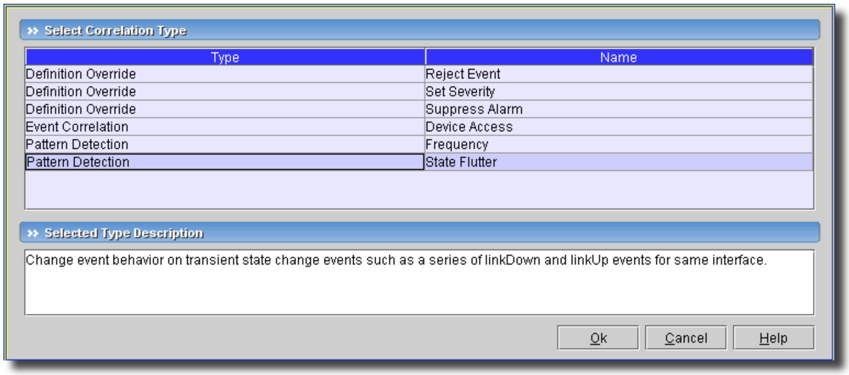
The *Audit* tab displays a history of the rule’s use.

See *Audit on page* 228 for more information.

Correlation Event Processing Rule Editor

When you select *Correlation* as the type of new rule you want to create, or edit, this editor appears. When you are creating a new rule, you must select which type from an intervening screen.

Figure 34-4. Correlation Rule Type Selector



» Select Correlation Type

Type	Name
Definition Override	Reject Event
Definition Override	Set Severity
Definition Override	Suppress Alarm
Event Correlation	Device Access
Pattern Detection	Frequency
Pattern Detection	State Flutter

» Selected Type Description

Change event behavior on transient state change events such as a series of linkDown and linkUp events for same interface.

For new rules, you must select the type from the following:

- Reject Event
- Set Severity
- Suppress Alarm

- Device Access
- Frequency
- State Flutter

If you are editing an existing rule, clicking *Open* selects the correct type automatically. On these panels, the *Audit* tab displays a history of the rule's use. See *Audit on page 228* for more information. A suppressed event does not trigger duplicate lines in the Alarm manager, but does appear in Event History. A rejected event does not appear even in Event History.

The upper portion of the next screen is like Automation Event Processing Rule Editor's. It has a basic description of the rule, and a filter. Choosing the event with which to correlate is the filter's function (see *Event Filter Criteria on page 818*). The bottom, *Options* panel varies, depending on the type of rule you select.

Reject Event

This screen lets you configure how to reject correlated events, discarding them. No *Options* panel appears since the filtered events are to be rejected. *Event Filter Criteria on page 818* describes how to select the event(s) to reject.

Set Severity

This screen lets you set the severity of the correlated event in the *Options* panel which provides a pick list for selecting the severity of the event propagated when the event you correlate appears. *Event Filter Criteria on page 818* describes how you can select the correlated event(s) where you set the severity in the event(s) propagated. Alarms appear in connection with related entities—propagate—based on propagation policies.

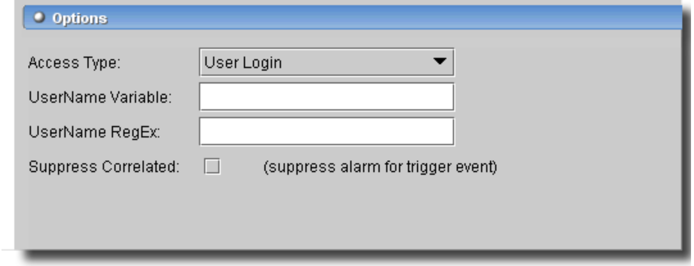
Suppress Alarm

Use this as you would the Automation Event Processing Rule Editor screen. No *Options* panel appears since the filtering on this rule only describes the events to be suppressed. Suppressed events / alarms do not appear in the Alarm display, but, unlike rejected events, the Event History screen can display a record of them. Use *Event Filter Criteria on page 818* to filter for the event(s) / alarm(s) to suppress.

Device Access

This *Event Correlation* creates a specific device access event for user login, logout, login failure or configuration change.

Figure 34-5. Device Access Options



Options

Access Type: User Login

UserName Variable:

UserName RegEx:

Suppress Correlated: □ (suppress alarm for trigger event)

The *Options* panel has the following fields:

- **Access Type**—Select the type of access (*User Login*, *User Logout*, *Login Failure*, *Config Change*).
- **UserName Variable**—Enter the UserName variable label.
- **UserName RegEx**—Enter a regular expression to extract the user name from the event's Username Variable.
- **Suppress Correlated**—Check this if you want to suppress the alarm for an event triggering this rule.

NOTE:

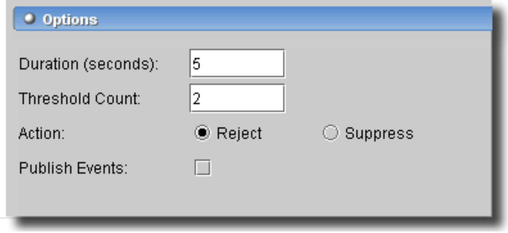
If your filter returns more than a single event, then the UserName Variable and UserName RegEx fields are disabled.

Event Filter Criteria on page 818 describes how you can select the correlated event(s)

Frequency

This is a *Pattern Detection* correlation. It changes event behavior based on occurrence frequency. The Screen that appears next includes the standard *Rule Properties* and *Event Filter* sections, and adds the frequency configuration in the *Options* panel at the bottom of the screen.

Figure 34-6. Frequency Options



Options

Duration (seconds): 5

Threshold Count: 2

Action: ● Reject ○ Suppress

Publish Events: □

The *Options* panel has the following fields:

- **Duration (seconds)**—This is the period during which the application measures event frequency.

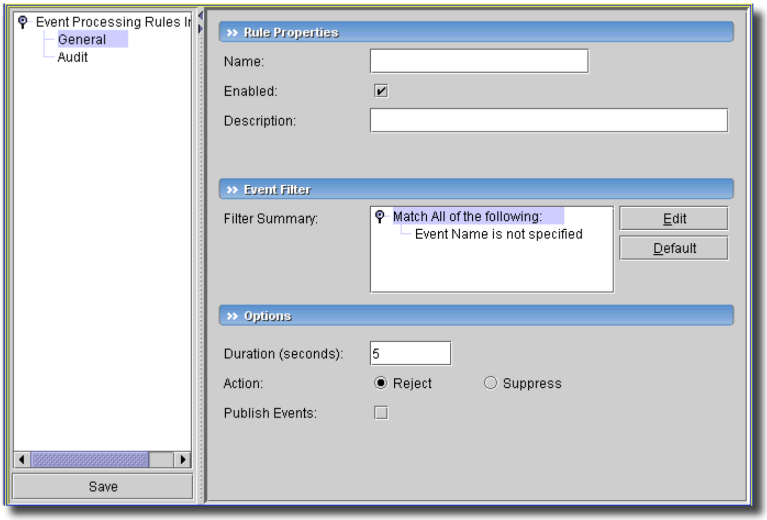
- **Threshold Count**—The number of events that must occur during the period selected in the previous field before the rule is active.
- **Action**—Select *Reject* or *Suppress*.
- **Publish Events**—Check to publish clearing or suppressed events even if the rule was not successful. When you publish an event, subscribers are notified.

Event Filter Criteria on page 818 describes how you can select the correlated event(s)

State Flutter

This *Pattern Detection* correlation detects a rapidly re-occurring condition like linkDown/linkUp traps from a flapping link.

Figure 34-7. State Flutter



Name:

Enabled: ☑

Description:

Filter Summary: Match All of the following:
Event Name is not specified

Duration (seconds): 5

Action: ● Reject ○ Suppress

Publish Events: □

The *Rule Properties* portion of the screen lets you specify a *Name* and *Description* for the correlation pattern, and a checkbox to enable / disable correlation events. The *Event Filter* portion of the screen lets you create a filter to find which events will activate the filter. See Chapter 28, Filters for more information about these.

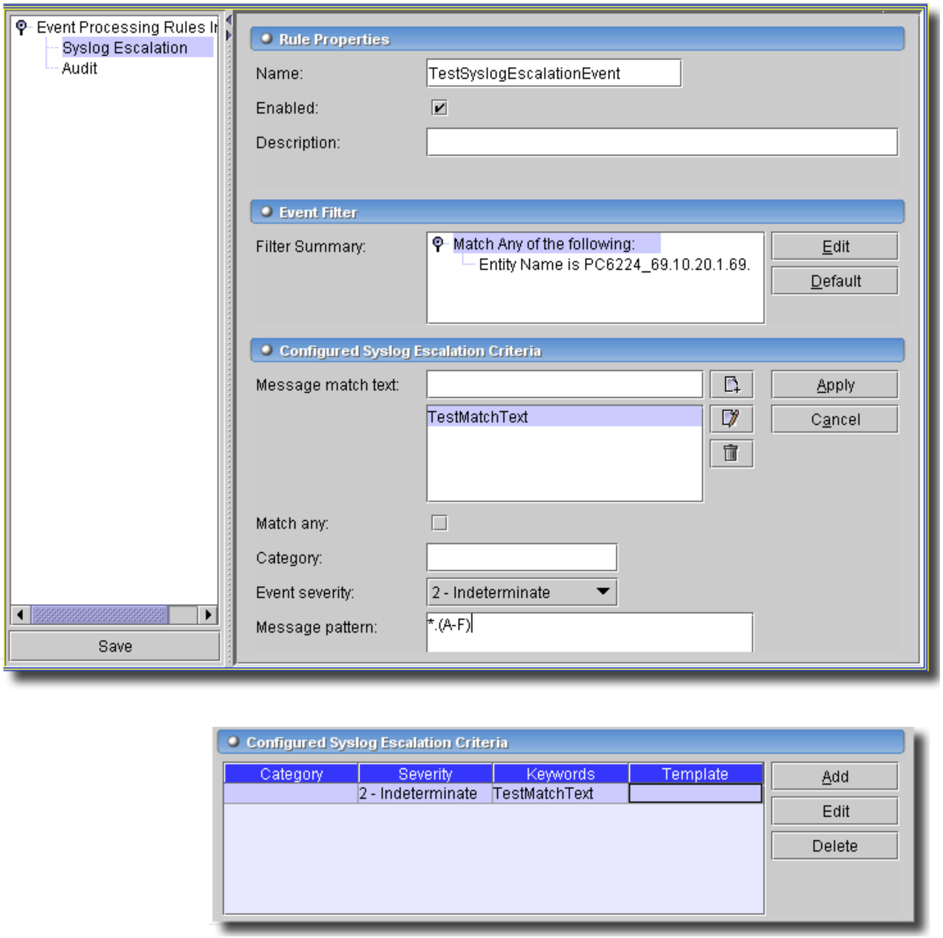
Finally, the *Options* portion of this screen lets you specify the filter *Duration (seconds)*, the *Action* to perform on correlated events (*Reject / Suppress*). *Reject* ignores the event entirely and it does not appear in either Event History or the Alarm viewer. *Suppress* does not display the event in the Alarm viewer, but the event does appear in Event History.

The state flutter filter lets the trigger event pass through without modification, but suppresses or rejects any subsequent events that would change the initial alarm state from the trigger event. It does this until no correlated events appear for the duration specified. Flutter detection always retains the last event until the filter expires. Then it passes the final event as is if it does not match the trigger event. Otherwise it is suppressed/rejected as specified in the rule options. The correlation events are optional. These indicate the start and end of the active filter along with total counts processed, rejected and suppressed by the filter.

Syslog Event Processing Rule Editor

This type of event configures Syslog escalation. To enhance performance, these rules pre-screen syslog messages rather than turning them all into application notifications / events. Syslog messages matching the criteria configured here are escalated to become application notifications or events which may then be further processed.

Figure 34-8. Syslog Escalation Editor



Name: TestSyslogEscalationEvent

Enabled: ☑

Description:

Filter Summary: Match Any of the following:
Entity Name is PC6224_69.10.20.1.69.

Message match text:

TestMatchText

Match any: □

Category:

Event severity: 2 - Indeterminate

Message pattern: *.(A-F)

Category	Severity	Keywords	Template
	2 - Indeterminate	TestMatchText	

The top two panels are like those in the Automation Event Processing Rule Editor screen. *Event Filter Criteria on page 818* describes how you can select the correlated event(s).

NOTE:

This application tries to match syslog messages that are essentially redundant except for their time stamp. If you escalate such messages to alarms, then this matching process will alter the time stamp to the time the message was received by the application, not when it was generated.

The *Configured Syslog Escalation Criteria* panel at the bottom is unique to configuring syslog escalation. Click *Add* to create a new escalation criterion, or *Edit* to modify an existing, selected one. Select a criterion and click *Delete* to remove it from the list. The editor (for *Add* or *Edit*) has the following fields:

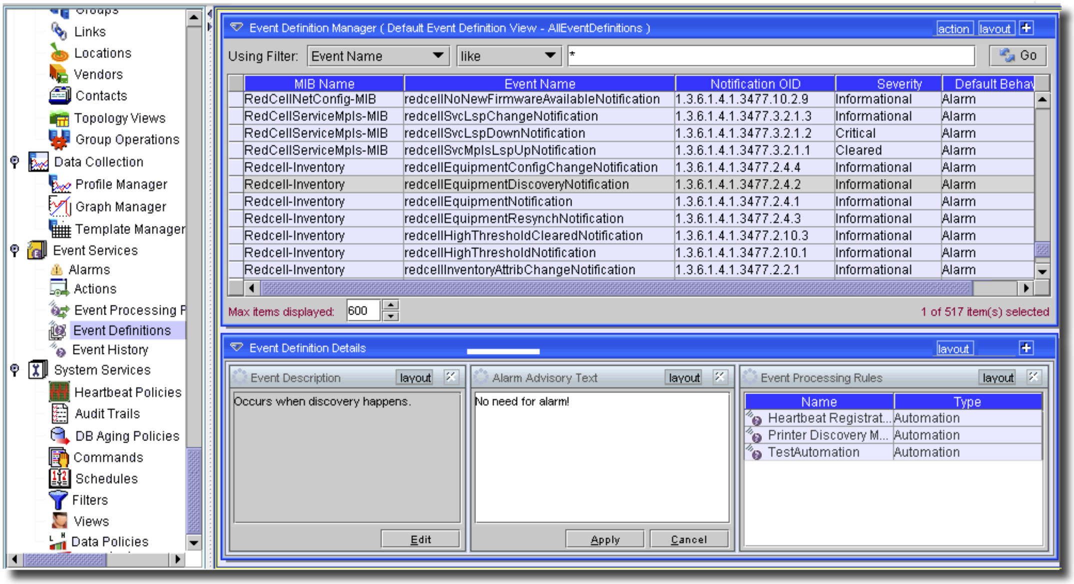
- **Message match text**—This is the syslog text in which a match must occur before escalation occurs. Enter text to match in the field to the right of this label, then click the *New* icon to the right of the list to enter it in the list. You can also *Edit* and *Remove* list members with the icons to the right of the list.
- **Match Any**—Check this to match any text listed in the *Message match text* rather than requiring all such text be present before a match occurs.
- **Category**—Enter a syslog category to match. This is a user-defined classification present here to assist in categorizing the escalation criteria.
- **Event Severity**— Select from the pick list to select a severity to match.
- **Message Pattern**— If you want to further refine a text match, enter a regular expression that matches the desired text in this field.

Click *Apply* to accept your edits, or *Cancel* to abandon them.

Event Definitions

This application lets you define how the system treats messages (events) coming into the system. Administrators can define event behavior deciding whether it is suppressed, rejected or generates an Alarm. The Event Definitions screen manages these responses for your system.

Figure 34-9. Event Definitions



Event Definition Manager (Default Event Definition View - AllEventDefinitions)

Using Filter: Event Name like *

MIB Name	Event Name	Notification OID	Severity	Default Behav
RedCellNetConfig-MIB	redcellNoNewFirmwareAvailableNotification	1.3.6.1.4.1.3477.10.2.9	Informational	Alarm
RedCellServiceMpls-MIB	redcellSvcLspChangeNotification	1.3.6.1.4.1.3477.3.2.1.3	Informational	Alarm
RedCellServiceMpls-MIB	redcellSvcLspDownNotification	1.3.6.1.4.1.3477.3.2.1.2	Critical	Alarm
RedCellServiceMpls-MIB	redcellSvcMplsLspUpNotification	1.3.6.1.4.1.3477.3.2.1.1	Cleared	Alarm
Redcell-Inventory	redcellEquipmentConfigChangeNotification	1.3.6.1.4.1.3477.2.4.4	Informational	Alarm
Redcell-Inventory	redcellEquipmentDiscoveryNotification	1.3.6.1.4.1.3477.2.4.2	Informational	Alarm
Redcell-Inventory	redcellEquipmentNotification	1.3.6.1.4.1.3477.2.4.1	Informational	Alarm
Redcell-Inventory	redcellEquipmentResynchNotification	1.3.6.1.4.1.3477.2.4.3	Informational	Alarm
Redcell-Inventory	redcellHighThresholdClearedNotification	1.3.6.1.4.1.3477.2.10.3	Informational	Alarm
Redcell-Inventory	redcellHighThresholdNotification	1.3.6.1.4.1.3477.2.10.1	Informational	Alarm
Redcell-Inventory	redcellInventoryAttribChangeNotification	1.3.6.1.4.1.3477.2.2.1	Informational	Alarm

Max items displayed: 600

1 of 517 item(s) selected

Event Definition Details

Event Description: Occurs when discovery happens.

Alarm Advisory Text: No need for alarm!

Event Processing Rules

Name	Type
Heartbeat Registrat...	Automation
Printer Discovery M...	Automation
TestAutomation	Automation

This screen displays a filtered list of actions. As in a typical manager, the filter is at the top of the screen. You can filter on the following behavior: *Default Behavior (Alarm, Reject*, or *Suppress*), *Event Name*, *MIB Name*, *Message*, *Notification OID*, *Severity* and *Valid* (*True/False* radio buttons) criteria. In this screen, you can configure events that, when correlated as described in Event Processing Rules on page 815, trigger actions.

CAUTION:

Unless you create a filter and save it as described in Chapter 28, Filters, filters you make here are not preserved.

The manager has the following menu items (accessed with the *Action* button, or a right-click):

- **Open**—Opens the selected Event for modification. See Event Definition Editor for more information.

- **Restore Defaults**—This item restores the original settings for the selected event.

- **Set Behavior**—Use the pick list to select *Alarm*, *Suppress*, or *Reject*. *Alarm* appears in the Alarm viewer and be available in Event History. *Reject* ignores the event entirely and it does not appear in either Event History or the Alarm viewer. *Suppress* does not display the event in the Alarm viewer, but the event does appear in Event History.

- **Set Severity**—The severity of the event (alarm). You can alter the default with the pick list. Any change in severity occurs with the next occurrence of the alarm. No change occurs with what has already been received.
- **Load MIB**—You can load a MIB, if you have one available as a file.
- **Unload MIB**—You can unload the MIB for the selected event if you have another to load that better describes the event. When you unload a MIB the events in it disappear from the Event Definitions manager unless they have previously been altered and saved. In this case such MIB events remain with the *valid* field set to *false*. After you reload the MIB the valid field is set back to *true*.
- **Import**—Import an XML event definition.
- **Export**—Export an XML event definition for the selected rule.
- **Help**—Open the online help for this screen.

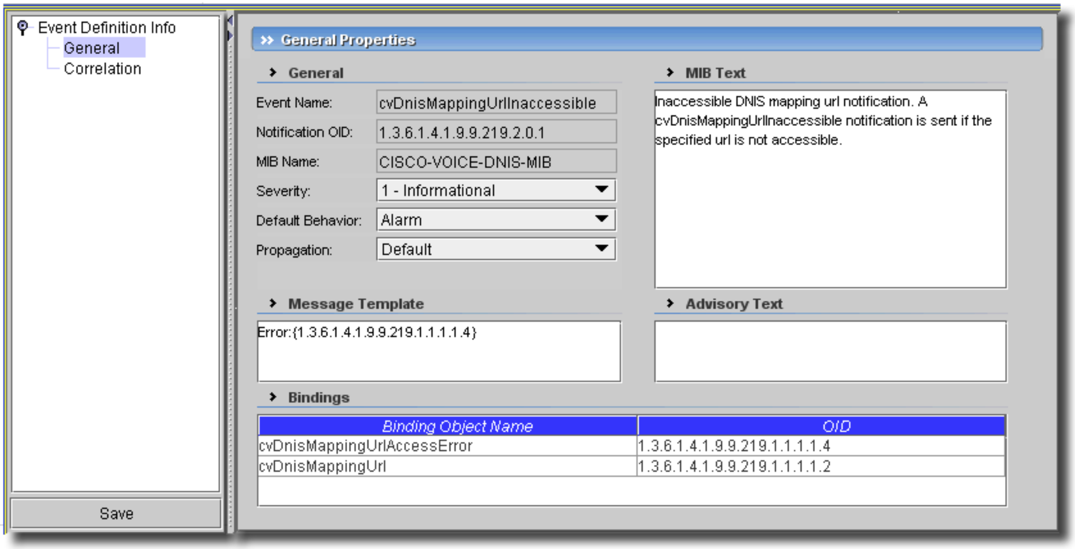
Detail Panels

Detail panels exist for editable text MIB Text and Advisory Text. You can also see listed *Event Processing Rules* that use this event, and their type. Select a rule and double-click or right-click and select *Open* to edit this rule as described in *Automation Event Processing Rule Editor on page 816 or Correlation Event Processing Rule Editor on page 819*. Finally, you can configure a message to accompany this event with the *Event Message Template* detail panel. Click *Edit* to enter text, then *Apply* to accept it. See *MIB Browser on page 166* for instructions about how to add your own MIB.

Event Definition Editor

This screen lets you edit the selected event’s definition.

Figure 34-10. Event Definition Editor - General



General

Event Name: cvDnisMappingUrlInaccessible

Notification OID: 1.3.6.1.4.1.9.9.219.2.0.1

MIB Name: CISCO-VOICE-DNIS-MIB

Severity: 1 - Informational

Default Behavior: Alarm

Propagation: Default

MIB Text

Inaccessible DNIS mapping url notification. A cvDnisMappingUrlInaccessible notification is sent if the specified url is not accessible.

Message Template

Error:{1.3.6.1.4.1.9.9.219.1.1.1.1.4}

Advisory Text

Bindings

Binding Object Name	OID
cvDnisMappingUrlAccessError	1.3.6.1.4.1.9.9.219.1.1.1.1.4
cvDnisMappingUrl	1.3.6.1.4.1.9.9.219.1.1.1.1.2

This has the following panels:

- General
- Correlation

Event or Alarm correlation means locating existing alarms relevant to a new alarm and making the appropriate updates. If an event is suppressed, then the application performs no alarm correlation.

Alarms only correlate if they are for the same entity. By default, a new alarm correlate only against existing alarms for the same event type. You can augment the scope of existing alarms affected by a new alarm by adding correlated events in these screens. To further refine the alarms affected, you can correlate based on key bindings to an event definition. All event data indicated as a key binding must match for alarms to correlate.

NOTE:

You can arrange for alarms from a device to only correlate if they come from, for example, a specified port.

Once a new alarm correlates to an existing alarm, the existing alarm is either closed or its count increases incrementally. Several factors have an impact on this behavior. Generally, the count of an existing alarm only increments for a new alarm of the same type, same message, and same key variable bindings.

The following describes the details in these panels

General

This tab has the following fields

- **Event Name**—A read-only reminder of which event this is.

- **Notification OID**—The object identifier for the event.

- **MIB Name**—The name of the MIB in which this event's information appears.

- **Severity**—If the new alarm is a clearing severity, then any existing alarm to which it correlates is closed. Otherwise, if the new alarm severity does not match the existing severity then the existing alarm is closed and a new alarm opened for the new severity.

- **Default Behavior**—The default that occurs with this event. You can alter the default with the pick list (*Alarm*, *Reject*, *Suppress*). *Alarm* means: Process at the mediation server, generate event history and an alarm. *Suppress* means: Process at the mediation server and generate an event (*not* an alarm). *Reject* means: Reject at the mediation server (do not process)

- **Propagation**—Only service effecting alarms are propagated. By default, events are service-effecting, provided their severity is indeterminate or above. Select the propagation type from the pick list. Options include *Default*, *Impacts subcomponents*, *Impacts top level*, and *Not service effecting*.

  An event definition configures "Impact Propagation" (distinct from "Alarm propagation") based on the event type. Does the event impact the overall device (*Impacts top level*), subcomponents (*Impacts subcomponents*), or just the correlated inventory entity (*Default*)?

  Not Service Effecting means that alarm propagation ignores alarms for this event. In other words, no impact to associated entities occurs. This also means alarms created for this event type appear as *Not Service Effecting* in the alarm manager—handy to help clean up noisy alarm views since you can filter to conceal these.

  For example, link propagation works like this: If one or both associated endpoints have an impacting alarm, then OpenManage Network Manager generates a calculated alarm for the corresponding link at the highest severity of either endpoint. If both endpoints are clear then the resulting, calculated event is clear. This means alarm correlation removes any existing calculated alarm against the link.

  If you upgrade your OpenManage Network Manager system, all alarms migrated to this version will appear as service-effecting, regardless of severity. To alter multiple events' impact propagation, export the event definitions, and alter the XML export to reflect the kind of propagation desired for events.

  Search for the paired `<ImpactPropagation>0</ImpactPropagation>` tags, and alter the numbers within them as follows:

Default—0

Impacts Top Level—1

Impacts Subcomponents—2

Not service effecting—4

Re-import the altered event definition file to update your event definitions.

MIB Text

This is a read-only text field for a description of the event.

Advisory Text

Editable Text to be sent with this event.

Message Template

This is a template for messages that accompany this event. If a message template exists for an existing, correlated alarm and the generated text does not match the original alarm, then the EMS closes the existing alarm, and generates a new one. Leaving this blank transmits the original message.

NOTE:

Putting an OID in curly brackets amounts to a tag replaced by the MIB text for that OID. To look for OIDs and messages, you can open the MIB browser from the navigation pane (as described in MIB Browser on page 166).

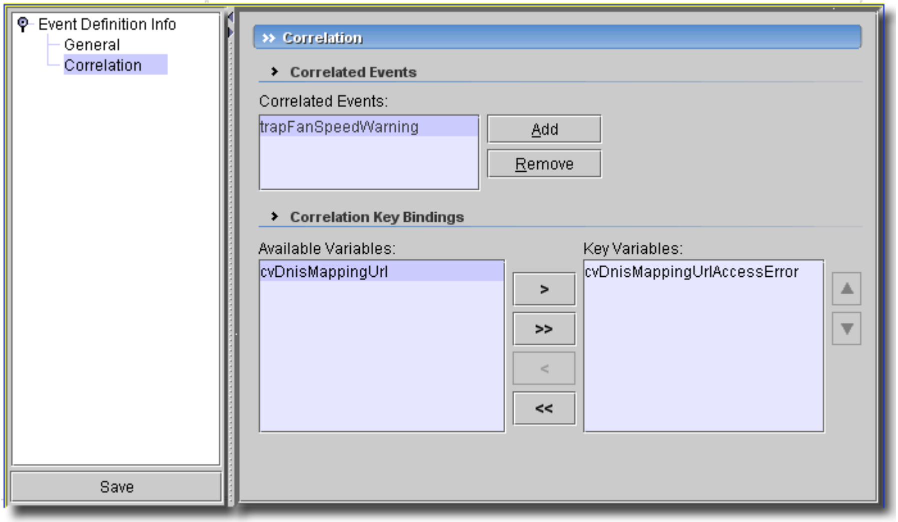
Bindings

This displays the varbind contents of the event, matching the *Binding Object Name* and the *OID* (object identifier).

Correlation

This panel configures the events correlated with the definition you are configuring.

Figure 34-11. Event Definition Editor - Correlation



Correlated Events: trapFanSpeedWarning

Available Variables: cvDnisMappingUrl

Key Variables: cvDnisMappingUrlAccessError

This screen lets you configure the following:

- **Correlated Events**—The list of events correlated with this one. Click *Add* to select events from those available, or *Remove* to delete a selected event.
- **Key Bindings**—This lists the varbinds correlated with this event. Move *Available Variables* (on the left) to *Key Variables* with the arrows between these two panels. The variables considered keys for correlation are the key bindings for the target alarm in the correlation process. This means that if event A is defined to include event B as a correlated event, comparison of the key bindings defined for event B is also considered when comparing a new alarm for event A to an existing alarm for event B.

  When a device has multiple types of suppression, a count of the suppressions on the device and its subcomponents appears in the *Mode* column. If a device has suppressions that are scheduled and created ad hoc, Ad Hoc is the *Mode* that appears in the Resources list.

Schedule Alarm Suppression

You can schedule suppression either from the right-click menu in the Resources, Topology, or Chassis view screens.

The following fields appear in the *Suppression Settings* panel:

- **Schedule Description**—A mandatory description or identifier for the schedule.

- **Suppression Duration**—The *Minutes*, *Hours* or *Days* for suppression. The minimum is 5 minutes, and the default is 1 hour.

NOTE:

Suppression duration information also appears in Audit Trails in the job status for Alarm Suppression Scheduled Start actions.

- **Suppression Targets**—Click *Add* to select the devices or device subcomponents on which you want to suppress. Click *Remove* to delete selected items from the list, or *Remove All* to clear the entire list.

The devices you select in the Resources screen appear as *Targets* in this list, if you initiate scheduling from Resources.

Deleting, stopping or disabling a schedule does not interrupt suppression, once it has started. You must right click selected devices and select the *Stop Alarm Suppression* or *Clear All Alarm Suppression* items. See *Schedule Alarm Suppression Detail Panel on page 831* for a look at the way to stop one of several overlapping types of alarm suppression.

When you set the time for suppression to start in the *Schedule Info* panel, remember that any end (*Stopping on...*) time you set there simply stops the suppression from starting. It does not terminate the suppression if it has already started. See Schedule Info on page 750 for more about the second panel in this editor.

Schedule Alarm Suppression Detail Panel

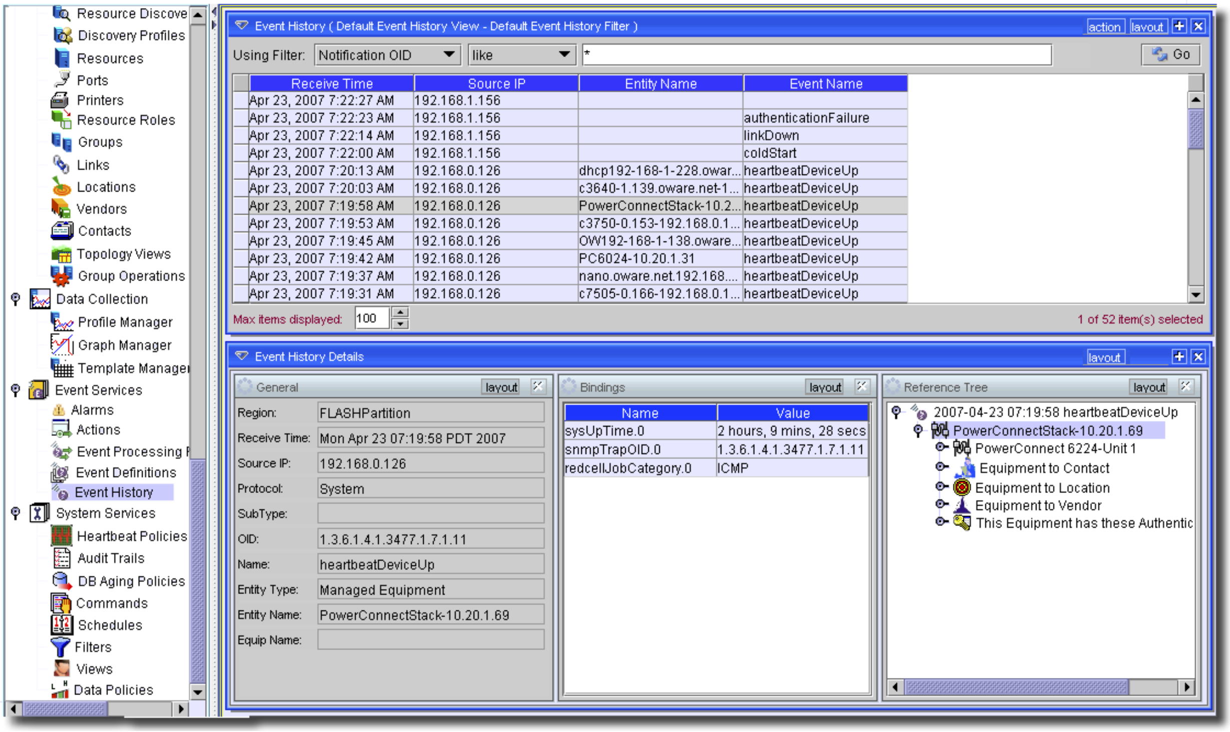
Scheduling alarm suppression also provides more information in the Resource Manager's detail panels.

An additional *Ending on* column appears for scheduled alarm suppression on a device. Ending suppression on components where multiple suppression types or schedules exists must occur within this detail panel. Right-click a selected item to see the menu.

Event History

The Event History manager, accessible from the navigation pane or *File -> Open -> Event Services* menu, lets you see a comprehensive (or filtered) list of events within this application.

Figure 34-12. Event History



Event History (Default Event History View - Default Event History Filter)

Using Filter: Notification OID | like | *

Receive Time	Source IP	Entity Name	Event Name
Apr 23, 2007 7:22:27 AM	192.168.1.156		
Apr 23, 2007 7:22:23 AM	192.168.1.156		authenticationFailure
Apr 23, 2007 7:22:14 AM	192.168.1.156		linkDown
Apr 23, 2007 7:22:00 AM	192.168.1.156		coldStart
Apr 23, 2007 7:20:13 AM	192.168.0.126	dhcp192-168-1-228.owar...	heartbeatDeviceUp
Apr 23, 2007 7:20:03 AM	192.168.0.126	c3640-1.139.oware.net-1...	heartbeatDeviceUp
Apr 23, 2007 7:19:58 AM	192.168.0.126	PowerConnectStack-10.2...	heartbeatDeviceUp
Apr 23, 2007 7:19:53 AM	192.168.0.126	c3750-0.153-192.168.0.1...	heartbeatDeviceUp
Apr 23, 2007 7:19:45 AM	192.168.0.126	OW192-168-1-138.oware...	heartbeatDeviceUp
Apr 23, 2007 7:19:42 AM	192.168.0.126	PC6024-10.20.1.31	heartbeatDeviceUp
Apr 23, 2007 7:19:37 AM	192.168.0.126	nano.oware.net.192.168....	heartbeatDeviceUp
Apr 23, 2007 7:19:31 AM	192.168.0.126	c7505-0.166-192.168.0.1...	heartbeatDeviceUp

Max items displayed: 100

1 of 52 item(s) selected

Event History Details

General

Region:	FLASHPartition
Receive Time:	Mon Apr 23 07:19:58 PDT 2007
Source IP:	192.168.0.126
Protocol:	System
SubType:	
OID:	1.3.6.1.4.1.3477.1.7.1.11
Name:	heartbeatDeviceUp
Entity Type:	Managed Equipment
Entity Name:	PowerConnectStack-10.20.1.69
Equip Name:	

Bindings

Name	Value
sysUpTime.0	2 hours, 9 mins, 28 secs
snmpTrapOID.0	1.3.6.1.4.1.3477.1.7.1.11
redcellJobCategory.0	ICMP

Reference Tree

2007-04-23 07:19:58 heartbeatDeviceUp
PowerConnectStack-10.20.1.69
PowerConnect 6224-Unit 1
Equipment to Contact
Equipment to Location
Equipment to Vendor
This Equipment has these Authentic

The top of this screen displays a list of events. By default, it displays all events, but you can use filters to limit the list that appears. As is typical for these displays, you can also sort by the column name by clicking on the heading of columns (clicking repeatedly toggles the sort order between descending and ascending).

Columns that appear in this table are described in General on page 833 and Alarm Table Columns on page 807.

Right-click an event, or click the *Action* menu for the following options:

- **Open -> Event Detail**—This opens an alarm viewer (see Editing Event History Entity on page 834).

- **Open -> Entity**—This opens an editor where you can configure the entity from which this alarm came. See Editing Resources on page 217.

- **Open -> Equipment—**This opens an editor where you can configure the device (where the Entity may be a subcomponent) from which this alarm came. See Editing Resources on page 217.

- **Open -> Event Definition—**This opens an editor where you can configure the device from which this alarm came. See Event Definitions on page 825.

- **Open -> Processing Rules**—This opens rule manager filtered to display only the rules associated with the selected Event. See Event Processing Rules on page 815 for more about what additional action you can take.

- **Map**—Open a topology view displaying the equipment selected alarm(s) came from. See Chapter 21, Topology Views.

- **Print**—This lets you print the listed events to a pdf file. For this to work correctly, you must have Acrobat installed. To change the contents of this report, change the filter.

- **Help**—Opens the online help for this screen.

When you select an event, its details appear in the detail panels below.

- General
- Bindings
- Reference Tree
- Description

The following sections describe these panels.

General

The first panel displays general information. this includes the following fields:

- **Region**—The partition the notification came from.

- **Receive Time**—The time the event was received and its time zone

- **Source IP**—Its source's IP address.

- **Entity Name**—The name of the entity referred to in the event. Its identity depends on the event configured.

Type—The event's type. (*Subtype* describes SNMPv2 *inform/traps*)

Name—The event's instance identifier.

- **Entity Type**—The event's entity type.

- **Entity OID**—The event's entity object identifier. The entity can differ from the source, for example, if this software wraps a northbound trap.

Bindings

This panel displays the variable binding name and value pairs that accompany the event. The contents of this panel depend the event's configuration. Bindings have appended an identifying number that displays the instance of the event for this binding.

Reference Tree

This panel displays any connections between this event and correlated rules and/or actions in tree form. Click the turner to the left of any node to display the tree. below that node. Double-click or right-click a node and select *Open* and you can edit that component as described in *Chapter 13, Resources*.

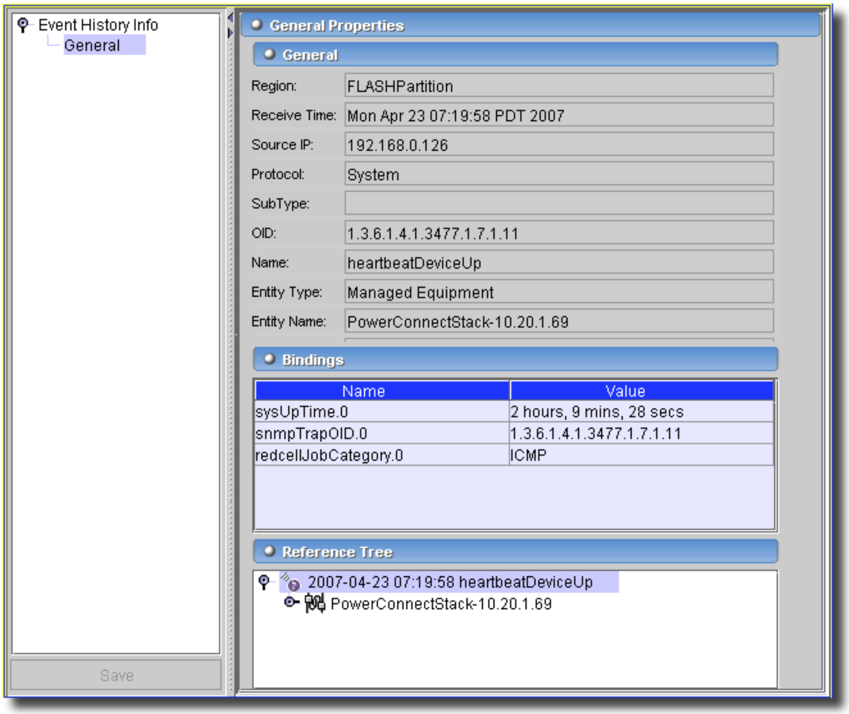
Description

This panel contains a description of the selected event.

Editing Event History Entity

This screen displays the information about a selected event when you click *Open*.

Figure 34-13. Editing Event History Entity



Region: FLASHPartition
Receive Time: Mon Apr 23 07:19:58 PDT 2007
Source IP: 192.168.0.126
Protocol: System
SubType:
OID: 1.3.6.1.4.1.3477.1.7.1.11
Name: heartbeatDeviceUp
Entity Type: Managed Equipment
Entity Name: PowerConnectStack-10.20.1.69

Name	Value
sysUpTime.0	2 hours, 9 mins, 28 secs
snmpTrapOID.0	1.3.6.1.4.1.3477.1.7.1.11
redcellJobCategory.0	ICMP

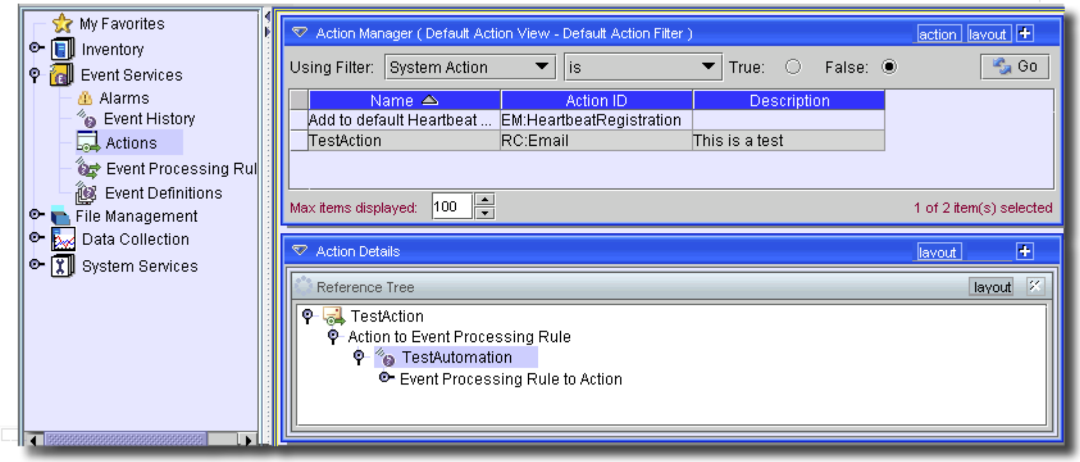
2007-04-23 07:19:58 heartbeatDeviceUp
PowerConnectStack-10.20.1.69

This screen displays the information visible in the General, Bindings and Reference Tree details panels.

Actions Manager

Open Actions Manager by clicking it in the navigation window.

Figure 34-14. Actions Manager



Using Filter: System Action ▾ is ▾ True: ○ False: ●

Name	Action ID	Description
Add to default Heartbeat ...	EM:HeartbeatRegistration	
TestAction	RC:Email	This is a test

Max items displayed: 100

1 of 2 item(s) selected

TestAction
Action to Event Processing Rule
TestAutomation
Event Processing Rule to Action

This screen displays a filtered list of actions. As in a typical manager, the filter is at the top of the screen, in this case in conjunction with *Name*, *Action ID*, *Description* and *System Action* (*True/ False* radio buttons) criteria. System actions are unalterable actions available throughout this software’s system.

In this screen, you can configure actions that will respond to events. The manager has the following menu items (accessed with the *Action* button, or a right-click):

- **New**—Opens the Action Editor, through which you can define a new Action. See Action Editor on page 836 for more information.

- **Open**—Opens the selected Action for modification. See Action Editor on page 836 for more information.

- **Delete**—Deletes the selected action. Select the action to remove and click *Delete*. The application prompts you for confirmation.

- **Copy**—This copies the selected action and opens the editor. You must rename it to begin with something other than “CopyOf [Original Name]” (its default name) before you can save the action.

- **Print**—Print the listed correlations to an Acrobat file. (You must have Acrobat reader installed for this to work properly.) Change the filter and click *Go* to change this printed report’s appearance.

- **Export/Import**—Export or import the action as/from XML.

- **Help**—Open the context-sensitive help for this screen.

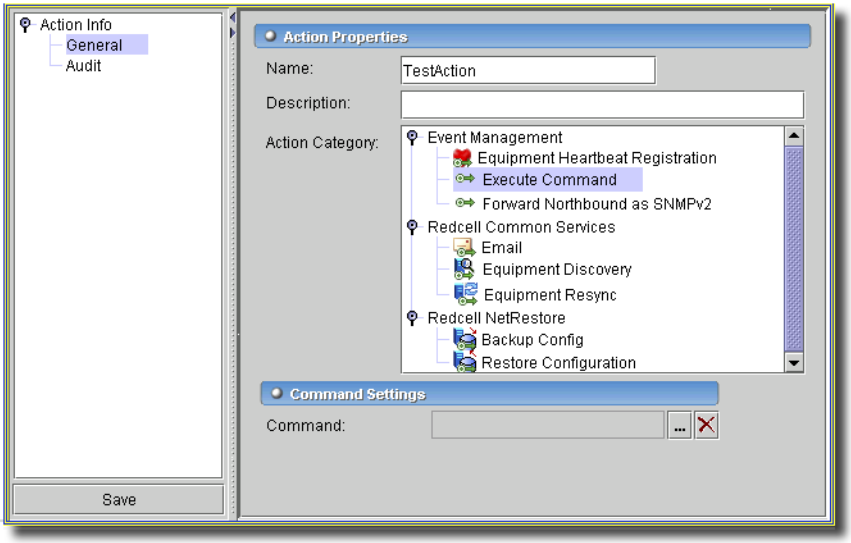
Action Details

The lowest portion of this layout contains a detail panel with a reference tree for the selected action that displays any related events and event processing rules.

Action Editor

When you click *New* or *Open* in Action Manager, you open the Action Editor. Here, you can configure the kind of action you want to respond to internal actions within this EMS.

Figure 34-15. Action



Name: TestAction

Description:

Action Category: Execute Command

Command:

Actions are, in effect, global group operations for the devices in question. The screen where you configure them has the following fields:

Action Properties

- **Name**—A unique identifier for the action.

- **Action Category**—Select from the tree. This selection determines the fields that appear in the lower portion of the screen (many selections make no fields appear). Examples of categories available includes options that vary depending on what options you have installed. The lowest panel in this screen changes, depending on the selection you make. Those selections are like the following:

Event Management

Equipment Heartbeat Registration—Specify the heartbeat policy with the command button (...). It opens a selection screen.

Execute Command—Specify the command executable with the command button (...). It opens a selection screen.

Forward Northbound as SNMP v2—Specify the destination address, port and SNMP community string, and check if you want the notification sent as proxy. See Trap Forwarding Process on page 846 for details.

NOTE:

To enable trap forwarding, first specify 162 as the port. You must also edit `/opt/dorado/owareapps/redcell/lib/redcell.properties.` Do a search for category that will take you to the right section in the property file. Here is the important section whose last line you must change:

```
##This property should be used for linking job with assure. This property

##defines list of jobs for which alarm notification is generated in the
   alarm window.

##The property should be defined in the format <jobcategory>:<notification
   type>

##Valid Notification types are 0 - Job success, 1 - Job failure, 2 - Notify
   Success or Failure, 3 - No Notification

append.oware.job.alarm.notification.list=EQUIPMENT.RESYNC:1,com.dorado.red
   cell.service:2
```

The added phrase is this: `com.dorado.redcell.service:2`

Change Manager

Common Services

Email—Specify a destination address, then click *Add*. You can specify more than one, and specify a header/footer and e-mail message to be triggered by correlation. See Email Options for additional information about customizing the messages sent. See Email Variables from Alarms on page 839 for a description of the available variables themselves.

CAUTION:

Because equipment can frequently generate literally thousands of traps, configure this action with care, limiting e-mails sent to only those events that are significant. Otherwise, performance, and your mail recipients, suffer.

Equipment Discovery—Specify the discovery profile to execute.

Equipment Resync—This triggers a resync of all equipment.

File Management

Backup Config—This triggers a backup of the equipment's configuration.

Restore Configuration—Restore the equipment's configuration to the selected label.

Service Center MPLS

Update LSP Status—This triggers an update of the LSP's status.

Click *Save* once you have configured the action as you would like, or click *Close* (in the toolbar) to abandon your edits.

The *Audit* tab displays a history of the action related to this link.

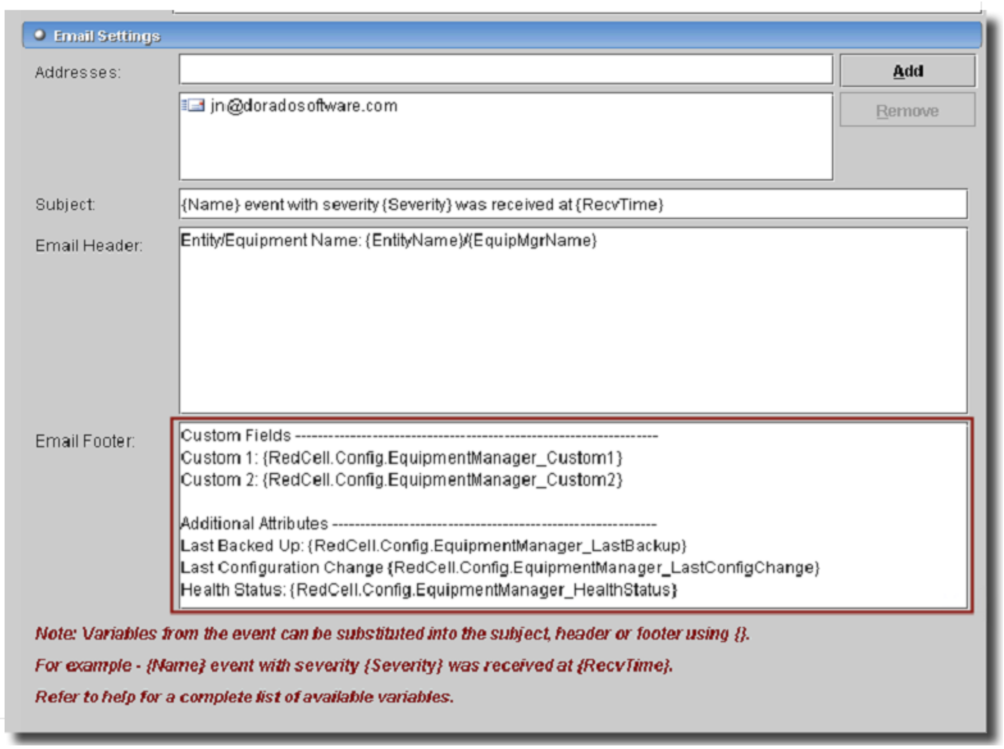
See *Audit on page* 228 for more information.

Email Options

You can use substitution variables to create an Email with exactly the information you want. The Basic substitution variables (see Basic Variables on page 841) remain are preferred because they require no additional database access. Using any other substitution attributes requires a database call, which has a performance impact. See Email Variables from Alarms on page 839 for a list of all variables, in addition to those Basic Variables.

The following example: describes extracting information for an event entity.

Figure 34-16. Example Custom Variables in Email Action



Email Settings

Addresses:

jn@doradosoftware.com

Subject: {Name} event with severity {Severity} was received at {RecvTime}

Email Header: Entity/Equipment Name: {EntityName}/{EquipMgrName}

Email Footer:

```
Custom Fields ------------------------------------------------------------
Custom 1: {RedCell.Config.EquipmentManager_Custom1}
Custom 2: {RedCell.Config.EquipmentManager_Custom2}

Additional Attributes -----------------------------------------------------
Last Backed Up: {RedCell.Config.EquipmentManager_LastBackup}
Last Configuration Change {RedCell.Config.EquipmentManager_LastConfigChange}
Health Status: {RedCell.Config.EquipmentManager_HealthStatus}
```

Note: Variables from the event can be substituted into the subject, header or footer using {}.

For example - {Name} event with severity {Severity} was received at {RecvTime}.

Refer to help for a complete list of available variables.

The email Subject, Header and Footer now let you insert additional attribute variables that appear—if found—in e-mail sent for the entity source of the event.

For example, you can retrieve the following attributes:

```
{RedCell.Config.EquipmentManager_Custom1}
```

```
{RedCell.Config.EquipmentManager_Custom2}
{RedCell.Config.EquipmentManager_LastBackup}
{RedCell.Config.EquipmentManager_LastConfigChange} and
{RedCell.Config.EquipmentManager_HealthStatus}
```

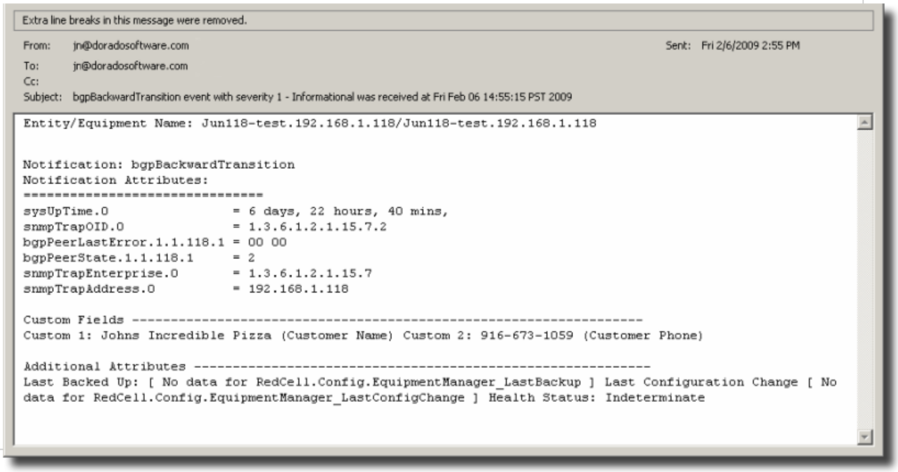
NOTE:

If the entity does not contain/return these values, then the message [No data for <attribute name>] appears in the email instead.

These examples are some of the attributes that are available for the chassis.

This example Email Action instance sends email containing those variables.

Figure 34-17. Example Email from Action



Extra line breaks in this message were removed.

From: jn@doradosoftware.com Sent: Fri 2/6/2009 2:55 PM
To: jn@doradosoftware.com
Cc:
Subject: bgpBackwardTransition event with severity 1 - Informational was received at Fri Feb 06 14:55:15 PST 2009

```
Entity/Equipment Name: Jun118-test.192.168.1.118/Jun118-test.192.168.1.118


Notification: bgpBackwardTransition
Notification Attributes:
===============================
sysUpTime.0                 = 6 days, 22 hours, 40 mins,
snmpTrapOID.0               = 1.3.6.1.2.1.15.7.2
bgpPeerLastError.1.1.118.1 = 00 00
bgpPeerState.1.1.118.1      = 2
snmpTrapEnterprise.0        = 1.3.6.1.2.1.15.7
snmpTrapAddress.0           = 192.168.1.118

Custom Fields ----------------------------------------------------------------
Custom 1: Johns Incredible Pizza (Customer Name) Custom 2: 916-673-1059 (Customer Phone)

Additional Attributes ----------------------------------------------------------
Last Backed Up: [ No data for RedCell.Config.EquipmentManager_LastBackup ] Last Configuration Change [ No
data for RedCell.Config.EquipmentManager_LastConfigChange ] Health Status: Indeterminate
```

Here, we can retrieve the Entity Name, custom 1 and 2 attributes. When we were unable to retrieve LastBackup and LastConfigChange because these values were not set for this device/entity, the *[No data for <attribute name>]* appears.

NOTE:

These variables are case-sensitive, so the application replaces `{SourceIP}` with the IP of the notification's source, but will not replace `{SourceIp}`.

You must configure the application to send e-mail in the first place before this feature is useful. Consult the *Administration Section* for more about that.

Email Variables from Alarms

The following are the Email Action variables you can use in customizing the content of action e-mail. These appear classified as follows:

- Basic Variables

- Managed Equipment Variables
- Entity Type: Port
- Entity Type: Interface, Logical interface
- User-Created Attributes

⚠ **CAUTION:**

To successfully retrieve Custom attributes, you must first enable them in the Inventory Config manager screen.

See Email Options on page 838 for other, more limited variables that are slightly more efficient in performance, if not as detailed as those described in the following section.

Basic Variables

Attribute	Description	Email Action Variable
Name	The event / alarm name	{Name}
Message	Description from the event	{Message}
Entity Name	The entity (interface, card...) name	{EntityName}
Equipment Manager Name	The name of the equipment, parent or chassis.	{EquipMgrName}
Device IP address	the IP of the device in alarm	{DeviceIP}
Entity Type	Type of entity (Router, and so on)	{EntityType}
Instance ID	An identifier for the event	{InstanceID}
Protocol Type	Of originating alarm (SNMP, syslog, etc.)	{ProtocolType}
Protocol Sub Type	Inform, Trap, [blank] (for internal events)	{ProtocolSubType}
Receive Time		{RecvTime}
Region	The mediation server partition name.	{Region}
Severity	0 - cleared, through 6 - critical, from Alarm Definition	{Severity}
Source IP address	The IP of the component sending the alarm	{SourceIP}

The following section describe variables whose use may have a performance impact.

Managed Equipment Variables

Attribute	Description	Email Action Variable
Custom 1	Note that although you can re-name any Custom attribute, you must use the variable's original name. For example here, that is {RedCell.Config.EquipmentManager_Custom1}	{RedCell.Config.EquipmentManager_Custom1}
Custom 2		{RedCell.Config.EquipmentManager_Custom2}
Custom 3		{RedCell.Config.EquipmentManager_Custom3}
Custom 4		{RedCell.Config.EquipmentManager_Custom4}
Custom 5		{RedCell.Config.EquipmentManager_Custom5}
Custom 6		{RedCell.Config.EquipmentManager_Custom6}

Attribute	Description	Email Action Variable
Custom 7		{RedCell.Config.EquipmentManager_Custom7}
Custom 8		{RedCell.Config.EquipmentManager_Custom8}
Custom 9		{RedCell.Config.EquipmentManager_Custom9}
Custom 10		{RedCell.Config.EquipmentManager_Custom10}
Custom 11		{RedCell.Config.EquipmentManager_Custom11}
Custom 12		{RedCell.Config.EquipmentManager_Custom12}
Custom 13		{RedCell.Config.EquipmentManager_Custom13}
Description	Description of the equipment	{RedCell.Config.EquipmentManager_DeviceDescription}
DNS Hostname	Hostname of equipment	{RedCell.Config.EquipmentManager_Hostname}
Equipment Type	Equipment Type	{RedCell.Config.EquipmentManager_CommonType}
Firmware Version	Version of the equipment’s firmware	{RedCell.Config.EquipmentManager_FirmwareVersion}
Hardware Version	Version of the equipment’s hardware	{RedCell.Config.EquipmentManager_HardwareVersion}
Last Backup	Last Backup	{RedCell.Config.EquipmentManager_LastBackup}
Last Configuration Change	Last Configuration Change	{RedCell.Config.EquipmentManager_LastConfigChange}
Last Modified	Timestamp of Last Modified	{RedCell.Config.EquipmentManager_LastModified}
Model	Model number of the equipment	{RedCell.Config.EquipmentManager_Model}
Name	Component name	{RedCell.Config.EquipmentManager_Name}
Network Status	Network Status	{RedCell.Config.EquipmentManager_HealthStatus}
Notes	Equipment Notes	{RedCell.Config.EquipmentManager_Notes}
OSVersion	OSVersion	{RedCell.Config.EquipmentManager_OSVersion}

Attribute	Description	Email Action Variable
Serial Number	Unique identifier for the equipment	{RedCell.Config.EquipmentManager_SerialNumber}
Software Version	Version of the equipment’s software	{RedCell.Config.EquipmentManager_SoftwareVersion}
System Object Id	SNMP based system object identifier	{RedCell.Config.EquipmentManager_SysObjectID}

Entity Type: Port

Attribute	Description	Email Action Variable
Custom 1	Note that although you can re-name any Custom attribute, you must use the variable’s original name. For example here, that is {RedCell.Config.Equipment Manager_Custom1}	{RedCell.Config.Port_Custom1}
Custom 2		{RedCell.Config.Port_Custom2}
Custom 3		{RedCell.Config.Port_Custom3}
Custom 4		{RedCell.Config.Port_Custom4}
Encapsulation	Encapsulation	{RedCell.Config.Port_Encapsulation}
Hardware Version	Version of the port’s hardware	{RedCell.Config.Port_HardwareVersion}
If Index	SNMP If Index	{RedCell.Config.Port_IfIndex}
MAC Address	“Typically a MAC Address, with the octets separated by a space, colon or dash depending upon the device. Note that the separator is relative when used as part of a query.”	{RedCell.Config.Port_UniqueAddress}
Model	Model number of the port	{RedCell.Config.Port_Model}
MTU	Maximum Transmission Unit	{RedCell.Config.Port_Mtu}
Name	Port name	{RedCell.Config.Port_Name}
Notes	Port Notes	{RedCell.Config.Port_Notes}
Port Description	Description of the port	{RedCell.Config.Port_DeviceDescription }
Port Number	Port Number	{RedCell.Config.Port_PortNumber}
Slot Number	Slot Number	{RedCell.Config.Port_SlotNumber}
Speed	Speed	{RedCell.Config.Port_Speed}
Subnet Mask	SubMask	{RedCell.Config.Port_SubMask}

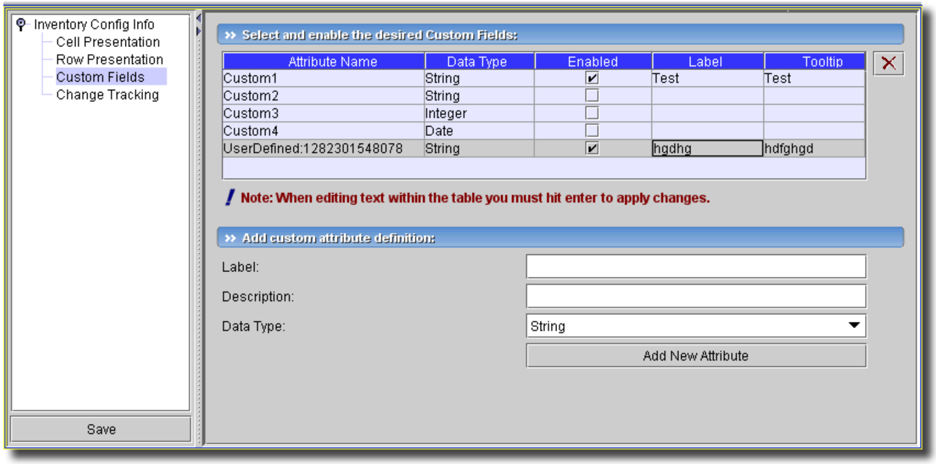
Entity Type: Interface, Logical interface

Attribute	Description	OpenManage Network Manager Email Action variable
Custom 1	Note that although you can re-name any Custom attribute, you must use the variable's original name. For example here, that is {RedCell.Config.EquipmentManager_Custom1}	{RedCell.Config.Interface_Custom1}
Custom 2		{RedCell.Config.Interface_Custom2}
Custom 3		{RedCell.Config.Interface_Custom3}
Custom 4		{RedCell.Config.Interface_Custom4}
Encapsulation	Encapsulation	{RedCell.Config.Interface_Encapsulation}
IfIndex	SNMP Interface Index	{RedCell.Config.Interface_IfIndex}
Interface Description	Description of the Interface	{RedCell.Config.Interface_DeviceDescription}
Interface Number	Interface Number	{RedCell.Config.Interface_InterfaceNumber}
Interface Type	Common Interface Type	{RedCell.Config.Interface_CommonType}
MTU	Maximum Transmission Unit	{RedCell.Config.Interface_Mtu}
Name	Interface name	{RedCell.Config.Interface_Name}
Notes	Interface Notes	{RedCell.Config.Interface_Notes}
Port Number	Port Number	{RedCell.Config.Interface_PortNumber}
Slot Number	Slot Number	{RedCell.Config.Interface_SlotNumber}
Subnet Mask	Subnet Mask of the Interface	{RedCell.Config.Interface_SubMask}

User-Created Attributes

The following describes how to report a created attribute in the notification e-mail. When you create such an attribute (see Custom Fields on page 178), it appears with an automatically-generated number.

Figure 34-18. User-Created Attribute



» Select and enable the desired Custom Fields:

Attribute Name	Data Type	Enabled	Label	Tooltip
Custom1	String	☑	Test	Test
Custom2	String	☐		
Custom3	Integer	☐		
Custom4	Date	☐		
UserDefined:1282301548078	String	☑	hgdhg	hdfghgd

Note: When editing text within the table you must hit enter to apply changes.

» Add custom attribute definition:

Label:

Description:

Data Type: String

Add New Attribute

Once you have created the attribute and recorded its number, you can create an e-mail referring to it with the following:

```
{[Label]:[number]}
```

For example:

```
{UserDefined:1282301548078}
```

NOTE:

You can select the created attribute, and copy the label and number with Ctrl+C. You must delete extraneous text when you paste it, but copying and pasting simplifies creating such notifications.

Best practice is to clarify such attributes by combining them with others that spell out their source.

Trap Forwarding Process

SNMPv1 and SNMPv3 traps become SNMPv2 Traps

SNMPv1 traps are converted according to RFC 1908. SNMPv3 traps are already in SNMPv2 format and the application simply does not use SNMPv3 security when sending these northbound. The following is the relevant snippet from RFC 1908:

> 3.1.2. SNMPv1 -> SNMPv2
>
> When converting responses received from a SNMPv1 entity acting in an agent role into responses sent to a SNMPv2 entity acting in a manager role:
>
> (1) ...
>
> (2) If a Trap-PDU is received, then it is mapped into a SNMPv2-Trap-PDU. This is done by prepending onto the variable-bindings field two new bindings: sysUpTime.0 [6], which takes its value from the timestamp field of the Trap-PDU; and, snmpTrapOID.0 [6], which is

> calculated thusly: if the value of generic-trap field is `enterpriseSpecific', then the value used is the concatenation of the enterprise field from the Trap-PDU with two additional sub-identifiers, `0', and the value of the specific-trap field; otherwise, the value of the corresponding trap defined in [6] is used. (For example, if the value of the generic-trap field is `coldStart', then the coldStart trap [6] is used.) Then, one new binding is appended onto the variable-bindings field: snmpTrapEnterprise.0 [6], which takes its value from the enterprise field of the Trap-PDU. The destinations for the SNMPv2-Trap-PDU are determined in an implementation-dependent fashion by the proxy agent.

This is not completely accurate. Many vendors defined a trap for SNMPv2 and then had to support sending as SNMPv1 protocol. The assembly of v2 OID from v1 enterprise and specific is supposed to include an extra `0'; enterpriseOID.0.specific. However, if a v2 trap is defined that has no '0' in it, so it cannot be sent as v1 and converted back following the specifications

Send as proxy option

This application can forward a trap as though it came from device (sourceIP spoofing) or act as an agent proxy according to the SNMP-COMMUNITY-MIB.

If not sending as proxy, we forward trap from application server cluster as an SNMPv2 notification as though it is coming directly from the originating agent (device). This is common and desired behavior in most cases. Some operating systems prevent packet spoofing as a security measure and this forced us to make this behavior optional.

If sending as proxy, the trap is forwarded from application server cluster using the application server IP as sourceIP. The relevant snippet from SNMP-COMMUNITY-MIB is the following:

```
--
-- The snmpTrapAddress and snmpTrapCommunity objects are included
-- in notifications that are forwarded by a proxy, which were
-- originally received as SNMPv1 Trap messages.
--

snmpTrapAddress OBJECT-TYPE
        SYNTAX  IpAddress
        MAX-ACCESS accessible-for-notify
        STATUS current
        DESCRIPTION
                "The value of the agent-addr field of a Trap PDU which
                is forwarded by a proxy forwarder application using
                an SNMP version other than SNMPv1.  The value of this
                object SHOULD contain the value of the agent-addr field
                from the original Trap PDU as generated by an SNMPv1
                agent."
 -- 1.3.6.1.6.3.18.1.3 --  ::= { snmpCommunityMIBObjects 3 }


snmpTrapCommunity OBJECT-TYPE
        SYNTAX  OCTET STRING
        MAX-ACCESS accessible-for-notify
        STATUS current
        DESCRIPTION
                "The value of the community string field of an SNMPv1
                message containing a Trap PDU which is forwarded by a
                a proxy forwarder application using an SNMP version
                other than SNMPv1.  The value of this object SHOULD
                contain the value of the community string field from
                the original SNMPv1 message containing a Trap PDU as
                generated by an SNMPv1 agent."
 -- 1.3.6.1.6.3.18.1.4 --  ::= { snmpCommunityMIBObjects 4 }
```

This application always adds snmpTrapAddress to every trap forwarded as proxy, (never adding snmpTrapCommunity). The application does not keep track of the community string on the traps received.

35

File Servers

File Server Manager

You can configure a pool of available FTP/TFTP Servers which provides an available FTP/TFTP Server to the component if requested. The FTP/TFTP Server transfers a configuration file, software image, or patch from the application to a device or from a device to the application. The application transfers files to this server (or a temporary directory for the internal TFTP server) and then from there to a Network Device and vice versa.

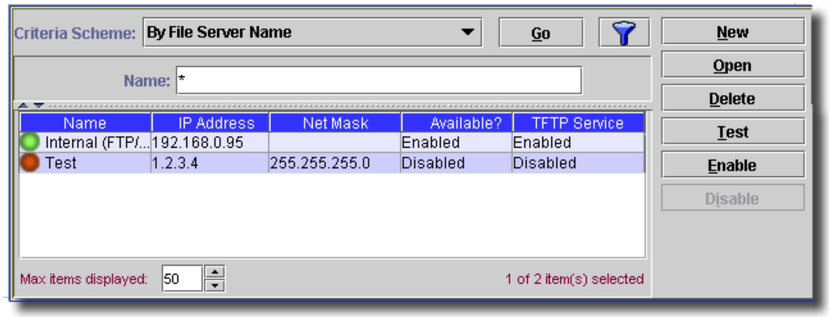
In the process of file transfer, the application queries the pool of existing file servers added to the system. If you have five file servers total, but four of them are disabled, then the application always gets the same enabled file server. If you have two enabled file servers, the application switches between each file server, using each half the time (round robin without weighting).

NOTE:

Some device drivers require both FTP and TFTP on a single server. The application will notify you if that is so.

Therefore, before you can back up, restore or deploy files, you must configure an FTP file server. File Server Manager lets you specify an FTP/TFTP server for file transfers.

Figure 35-1. File Server Manager



Criteria Scheme: By File Server Name

Name: *

Name	IP Address	Net Mask	Available?	TFTP Service
● Internal (FTP/...	192.168.0.95		Enabled	Enabled
● Test	1.2.3.4	255.255.255.0	Disabled	Disabled

Max items displayed: 50

1 of 2 item(s) selected

NOTE:

OpenManage Network Manager has the internal server disabled by default.

Query for available FTP servers by the criteria in the pick list, or enter an asterisk wildcard in the search field and click *Go*. The table of available FTP servers fills with the names and properties of what is available.

You can create a new entry in this table, or edit an existing, selected entry with the *New* and *Open* buttons, respectively. You can also display the Internal File Server Setup screen by clicking the *Open* button when you have selected the internal file server, which exists in *disabled* state by default.

You can *Delete* or *Test* a selected entry with those buttons. Finally, you can select a server, and *Enable* or *Disable* it with those buttons.

NOTE:

When testing, status messages typically come in pairs.

The table of existing servers appears with columns for *Hostname* (including a green/red icon indicating whether the server is working/not working), *FTP Path*, *IP Address*, *Port*, *Available?*, and *TFTP Service*. You can see descriptions of these fields (and the editor where you configure them) in *External Servers on page 850*. You cannot edit the *Internal (FTP/TFTP)* server

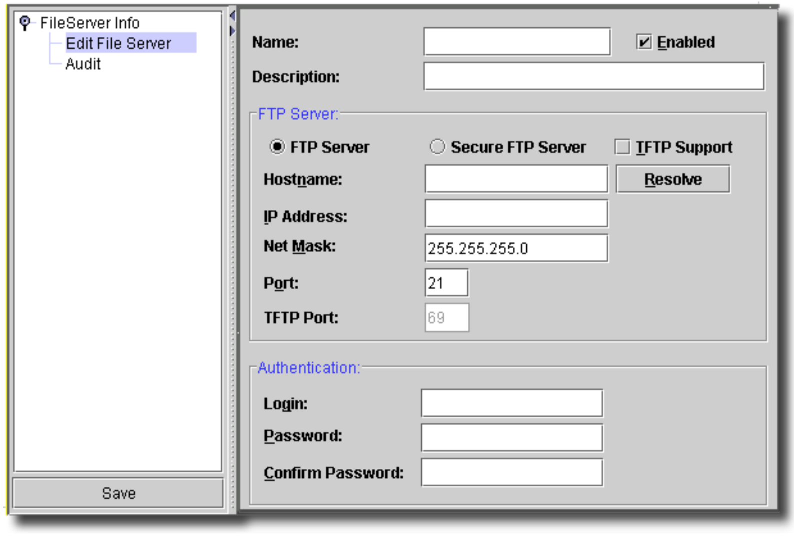
CAUTION:

You must install FTP and TFTP as described in the Administration Section before it can function correctly. **Also:** Ensure you have the correct login/password and enough disk space for the anticipated FTP load before you set up your FTP server.

External Servers

To configure an external file server, click *New* (or select an existing external server and click *Open*) and an FTP Server editor appears (you cannot edit the internal FTP server). Click an editable row in the list of servers and click *Open*, or click *New* (and select *External*) to create a new external FTP server, and the New/Edit FTP Server Form appears.

Figure 35-2. New/Edit FTP Server Form



Name:
☑ Enabled
Description:

● FTP Server ○ Secure FTP Server □ TFTP Support

Hostname:
IP Address:
Net Mask: 255.255.255.0
Port: 21
TFTP Port: 69

Login:
Password:
Confirm Password:

This form has the following fields:

- **Name**—A unique identifier for this configuration.

- **Description—**A text description of this file server

- **Enabled**—When you check this, NetConfig uses a non-weighted round robin of enabled FTP servers to select the server used.

FTP Server

With the radio buttons, select *FTP*, or *Secure FTP*, and check whether you want *TFTP Support*.

When you create SFTP server(s), the following occurs when backing up, restoring, or deploying configuration files and operating system images (provided the driver for the device selected supports secure file copying):

1 If the driver supports secure file copying, the application determines whether a secure file server is in the server list, first looking for one that matches the configured net mask value and the network device's IP address. The application uses the first matching file server in the list.

2 If it cannot make a match based on mask value and device IP, the application determines whether *any* secure file servers are defined and uses the first listed FTP server.

3 If no secure file servers are defined, then the application uses the first listed FTP server.

- **Hostame—**DNS identifier for the FTP server. When you create a *New* FTP server, you can also click the *Resolve* button to the right of this field. This fills in the IP address field (below) with the correct address for this hostname. The *Resolve* button does not appear for existing servers you open to edit.

- **IP Address—**The IP address of this server.

- **Net Mask**—Defaults to 255.255.255.0. The Net Mask helps find the closest external file server for a device using a file server of this type. If this field is blank, then the application will not consider this file server when it tries to find the best/closest external file server for the device in question. Only valid net masks are accepted.

  The audit panel displays a message when the application finds a file server with its closest algorithm: `Determined Closest External File Server: <server name>/<server ip>`.

  If the application could not determine a closest file server, then it chooses one with a round robin algorithm and the following audit message appears: `Retrived External File Server: <server name>/<server ip>`.

  This implies the following about File Management backup (both single and group operations):

  - The application always attempts to find the best/closest file server for the device being backed up by retrieving all external file servers and matching the device ip/file server ip/file server net mask. If the application finds more than one it uses the first one found.

- If no external file servers exist that have a Net Mask, then the application automatically uses a round-robin retrieved server.
- If the application finds no external file servers in the same network, then it falls back to round robin.

- **Port/ TFTP Port**—The port to use for FTP or TFTP when communicating with this server.

Authentication

- **Login**—The login for this server.

- **Password / Confirm Password**—The password for this server.

- Click *Save* to keep your edits, or *Cancel* to abandon them.

Click the *Test* button in the File Server Manager to confirm the server, as you have configured it, works correctly. After clicking this button, the Audit screen appears with messages specifying the success or failure of individual testing steps.

NOTE:

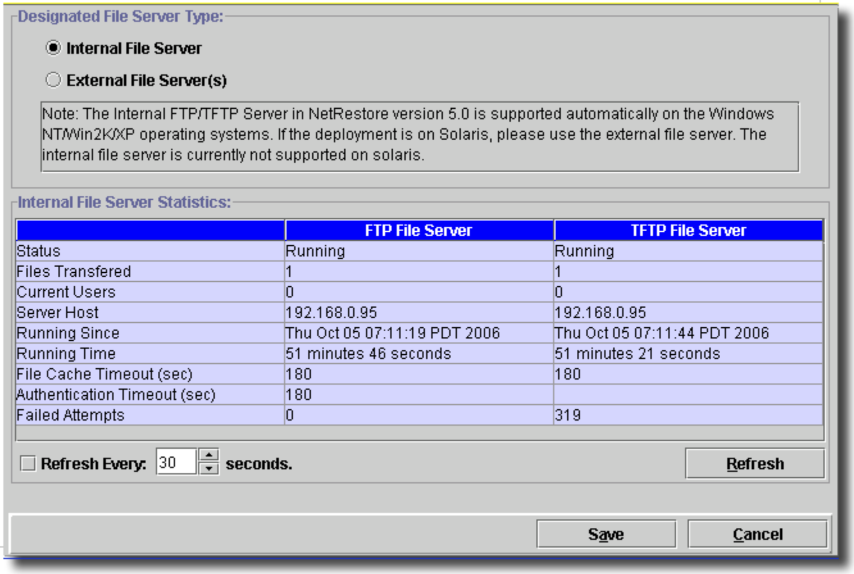
If FTP or SFTP does not function properly, TFTP fails.

If you click the *Test* button, the application creates a test file and uses FTP/TFTP to and from this server to see whether it is correctly connected.

Internal File Server Setup

You can select the internal file server and click *Open* to make this screen appear.

Figure 35-3. File Server Setup



Designated File Server Type:

● Internal File Server

○ External File Server(s)

Note: The Internal FTP/TFTP Server in NetRestore version 5.0 is supported automatically on the Windows NT/Win2K/XP operating systems. If the deployment is on Solaris, please use the external file server. The internal file server is currently not supported on solaris.

Internal File Server Statistics:

	FTP File Server	TFTP File Server
Status	Running	Running
Files Transfered	1	1
Current Users	0	0
Server Host	192.168.0.95	192.168.0.95
Running Since	Thu Oct 05 07:11:19 PDT 2006	Thu Oct 05 07:11:44 PDT 2006
Running Time	51 minutes 46 seconds	51 minutes 21 seconds
File Cache Timeout (sec)	180	180
Authentication Timeout (sec)	180	
Failed Attempts	0	319

□ Refresh Every: 30 seconds.

In File Server Setup you can see the status of the selected server's FTP and TFTP operation. You can also change the selected server from *Internal* to *External File Servers* (or vice-versa).

The internal file server starts when you enable it. Files in transit reside in a temporary file server storage location: `oware\temp\intsvr\`.

⚠ **CAUTION:**
Use the internal file server only for limited production or pre-production testing, not for a production environment. The Administration Section documents how to install and set up third-party, free FTP/TFTP servers.

FTP Timeout

If you have a slow network, you can set the timeout for FTP contact in a property: `com.dorado.redcell.filexferapi.ftptimeout`. It has a default value of 100 seconds. To override this default, add this property, followed by an equal sign and the preferred number of seconds to `\owareapps\installprops\lib\installed.properties`.

36

Backing Up / Restoring

Backup / Restore Elements Overview

The backup / restore and deploy capabilities of this application let you conveniently manage both device configurations and firmware deployments. Before you can use these capabilities, however, you must configure an FTP or TFTP server to retrieve or deploy the files. Chapter 35, File Servers describes this setup.

The following are this application's capabilities for backing up and restoring network element configuration files:

- Retrieve and/or restore a configuration file from/to a specific network element.
- Schedule the backup or restoration of a configuration file or files on any single network element.
- Maintain a history of software installed/deployed on the network element by the element management system.
- Use this application's group operations capabilities for configuration file backups / restores.
- Stage and import the software images/patches, then deploy, or redeploy them to specific network elements.
- Provide a history of all the configuration file backups and restorations performed on any given network element.
- Track the software images and patches deployed to any given network element.
- Schedule the deployment of a software image or patch to any single network element.

This application employs various components, described in the following sections, to do the above.

Managing Backup / Restore by IP Address or Hostname

By default this application manages hosts (and their related backup files) by the IP Address. You can see if it uses IP addresses or hostnames in the following section of `\owareapps\netrestore\lib\nr.properties`:

```
#=============================================
# NetConfig File Server Prefix property
# Valid Options are as follows:
# IP_ADDRESS
# HOSTNAME
#=============================================
redcell.netrestore.file.server.prefix.type=IP_ADDRESS
```

This property lets you select either *IP Address* or *Hostname* (SysName). To change to using Hostname, change `IP_ADDRESS` to `HOSTNAME` on all application servers (and clients). You must restart the application servers after doing this.

NOTE:

Some messages may refer to NetConfig or NetRestore rather than File Management. These are the same.

CAUTION:

When using Hostname as the prefix, all hostnames in the system must be unique. If two devices have the same hostname, a backup group operation with these two devices makes these two devices use a single config file on the file server, resulting in an invalid/garbage backup or restoration.

NOTE:

Use Group Ops to schedule operations on more than one device at the same time instead of scheduling multiple individual operations at the same time.

File Archiving

This application's backup also manages configuration files, including versioning, saving, and retrieving them by key and version number. By default the backup process only stores the file backed up if it detects a change in the file from what was previously backed up. This significantly reduces the amount of space used both in normal operations and in archiving.

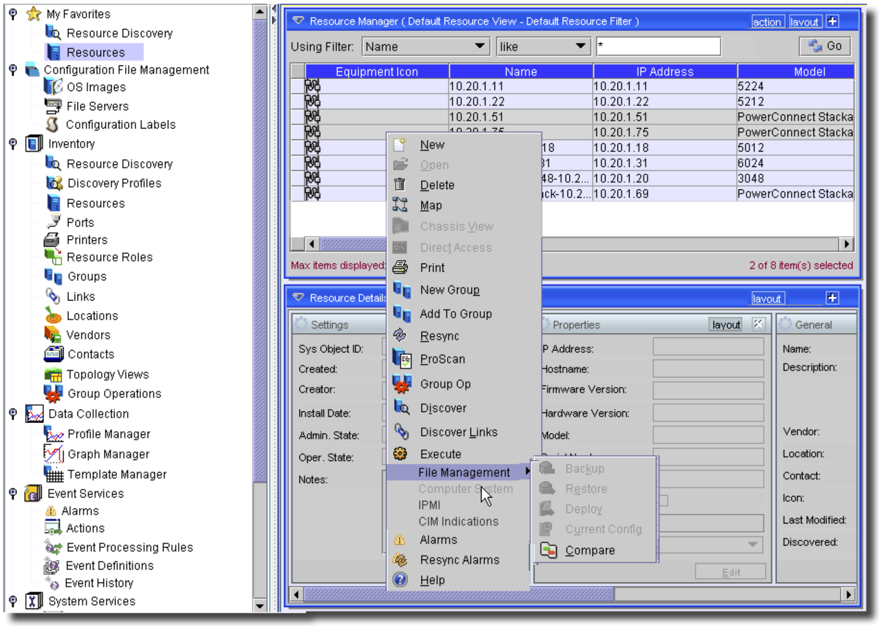
You can change these settings in the *Properties* tab that appears when you select *Settings -> Configuration -> Control Settings*. Find the class `redcell.netrestore.checkin.mode` in the screen, and click *Edit*. Available options are *always* (always check in the backup file) and *changes* (the current default: only check in backup files if they changed since the last backup). Click *OK* to get to the next screen.

Resource Screen Buttons

File Management uses the following items in the Resources manager menus (right click or click the *Action* button to see them):

- **Backup**—Backs up selected configuration files from the selected network elements. See the destination of these backups described in Resource Editor on page 858.
- **Restore** —Restores selected configuration files to the selected network elements (pushes a configuration file down to the device).
- **Deploy** —Pushes device operating system binaries down to the device
- **Compare**—Compares configuration files for any two selected equipment items. See File Management -> Configurations on page 861 or Comparing Files on page 864 for more about this capability.

Figure 36-1. Resources Screen with NetConfig Menu Open



Resource Manager (Default Resource View - Default Resource Filter)

Using Filter: Name like *

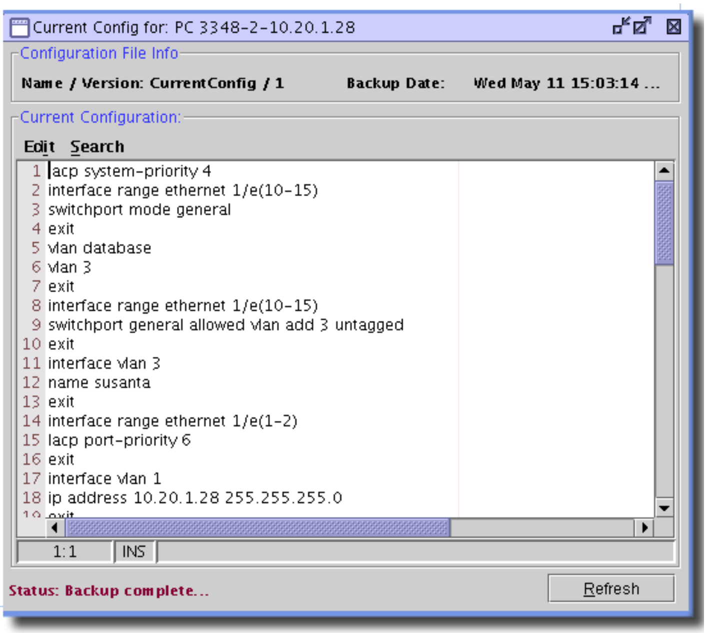
Equipment Icon	Name	IP Address	Model
	10.20.1.11	10.20.1.11	5224
	10.20.1.22	10.20.1.22	5212
	10.20.1.51	10.20.1.51	PowerConnect Stacka
	10.20.1.75	10.20.1.75	PowerConnect Stacka
	18	10.20.1.18	5012
	31	10.20.1.31	6024
	48-10.2...	10.20.1.20	3048
	ck-10.2...	10.20.1.69	PowerConnect Stacka

Max items displayed:

2 of 8 item(s) selected

- **Current Config**—Clicking this button retrieves a config file from the selected device and displays it in a panel in front of Resource Manager.

Figure 36-2. Current Config



Current Config for: PC 3348-2-10.20.1.28

Configuration File Info

Name / Version: CurrentConfig / 1 **Backup Date: Wed May 11 15:03:14 ...**

Current Configuration:

```
lacp system-priority 4
interface range ethernet 1/e(10-15)
switchport mode general
exit
vlan database
vlan 3
exit
interface range ethernet 1/e(10-15)
switchport general allowed vlan add 3 untagged
exit
interface vlan 3
name susanta
exit
interface range ethernet 1/e(1-2)
lacp port-priority 6
exit
interface vlan 1
ip address 10.20.1.28 255.255.255.0
exit
```

1:1 INS

Status: Backup complete...

This panel provides cut/paste/search capabilities with the menus accessible at its top.

Select the network elements from the list, and then click on the menu item for the specific operation.

Resource Editor

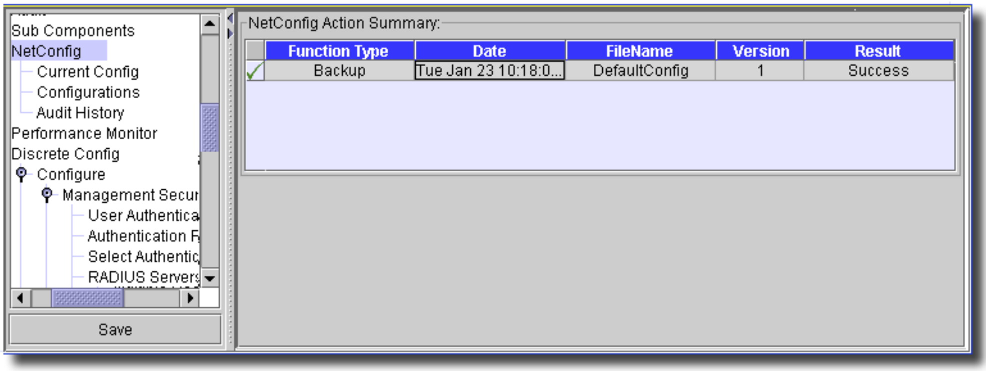
The application also adds the File Management panels to the Resource Editor (when device driver support exists for it). This includes the following panels:

- File Management Panel
- File Management -> Current Config
- File Management -> Configurations
- File Management -> Audit History

File Management Panel

This panel displays a summary of File Management actions on the selected equipment

Figure 36-3. Resource Editor: Action Summary



NetConfig Action Summary:

	Function Type	Date	FileName	Version	Result
✓	Backup	Tue Jan 23 10:18:0...	DefaultConfig	1	Success

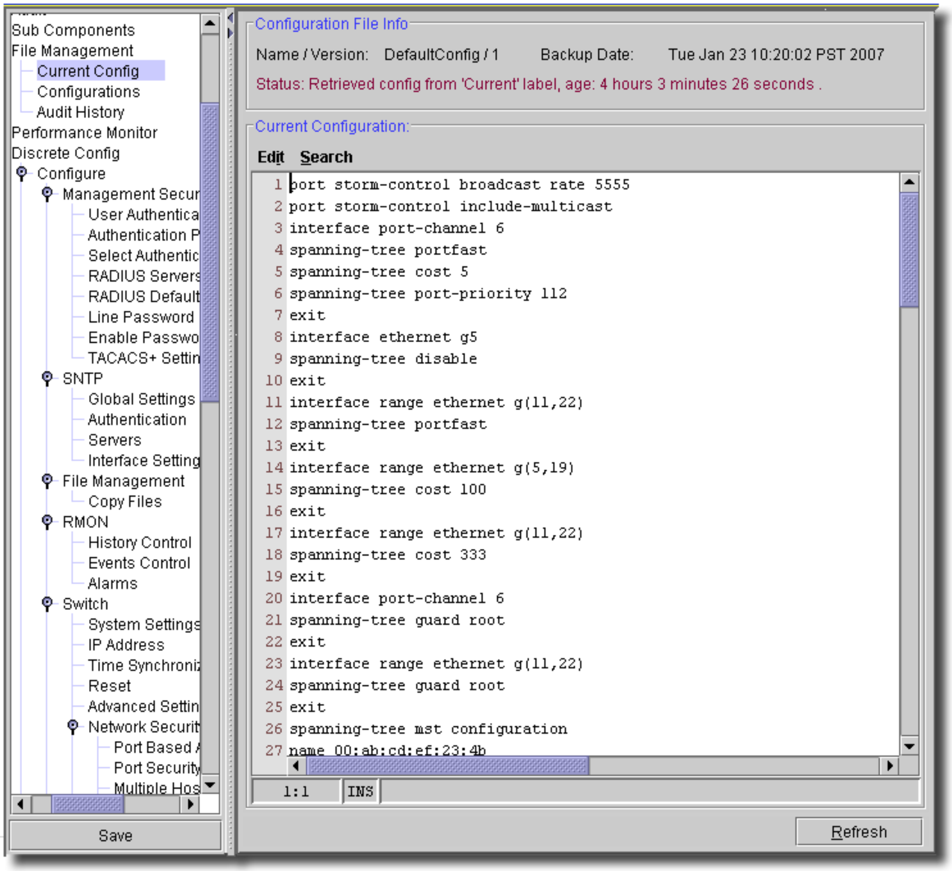
This contains the following columns:

- **Icon**—A green check indicates a successful action. A red stop sign indicates an error in the action.
- **Function Type**—Backup, Restore
- **Date**—The date the action occurred.
- **FileName**—The file connected to the action.
- **Version**—The version of the action.
- **Result**—Success or Failure.

File Management -> Current Config

This panel displays the current device configuration file.

Figure 36-4. Resource Editor: Current Configuration



Name / Version: DefaultConfig / 1   Backup Date: Tue Jan 23 10:20:02 PST 2007

Status: Retrieved config from 'Current' label, age: 4 hours 3 minutes 26 seconds .

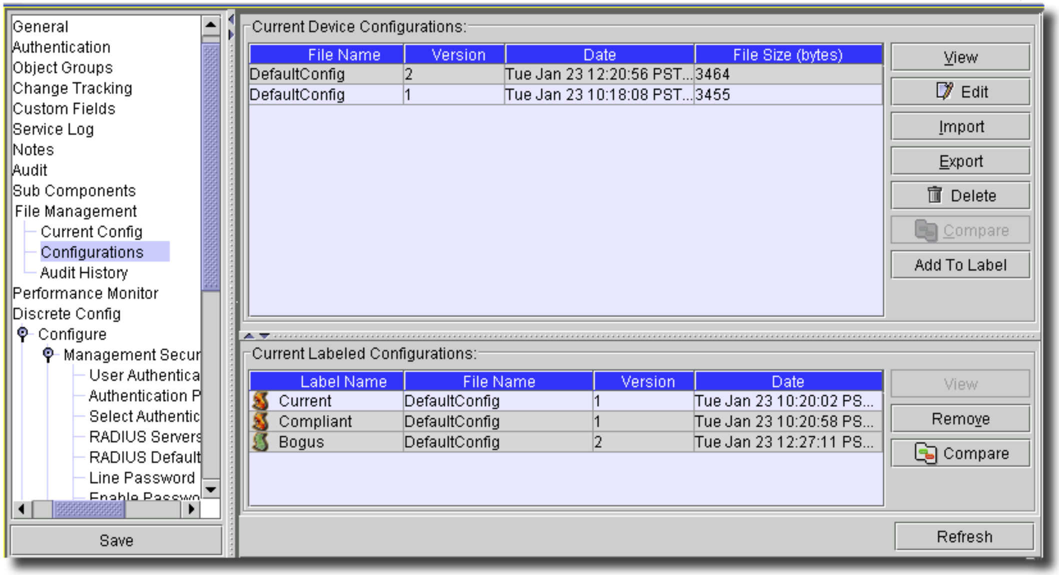
```
port storm-control broadcast rate 5555
port storm-control include-multicast
interface port-channel 6
spanning-tree portfast
spanning-tree cost 5
spanning-tree port-priority 112
exit
interface ethernet g5
spanning-tree disable
exit
interface range ethernet g(11,22)
spanning-tree portfast
exit
interface range ethernet g(5,19)
spanning-tree cost 100
exit
interface range ethernet g(11,22)
spanning-tree cost 333
exit
interface port-channel 6
spanning-tree guard root
exit
interface range ethernet g(11,22)
spanning-tree guard root
exit
spanning-tree mst configuration
name 00:ab:cd:ef:23:4b
```

If no backed up configuration exists, clicking the *Refresh* button at the bottom of this screen performs a backup and displays the configuration file result (named CurrentConfig). The file name and backup date / time for the displayed configuration appear at the top of the screen. The *Edit* and *Search* menus above the file contents also let you find, and copy file contents.

File Management -> Configurations

This screen queries for configuration files.

Figure 36-5. Resource Editor: Configurations



Current Device Configurations:

File Name	Version	Date	File Size (bytes)
DefaultConfig	2	Tue Jan 23 12:20:56 PST...	3464
DefaultConfig	1	Tue Jan 23 10:18:08 PST...	3455

Current Labeled Configurations:

Label Name	File Name	Version	Date
Current	DefaultConfig	1	Tue Jan 23 10:20:02 PS...
Compliant	DefaultConfig	1	Tue Jan 23 10:20:58 PS...
Bogus	DefaultConfig	2	Tue Jan 23 12:27:11 PS...

The backed up files appear in a list at the top of this screen. The following buttons appear to the right of this upper screen:

Current Device Configurations

- **View**—Read the selected configuration file.

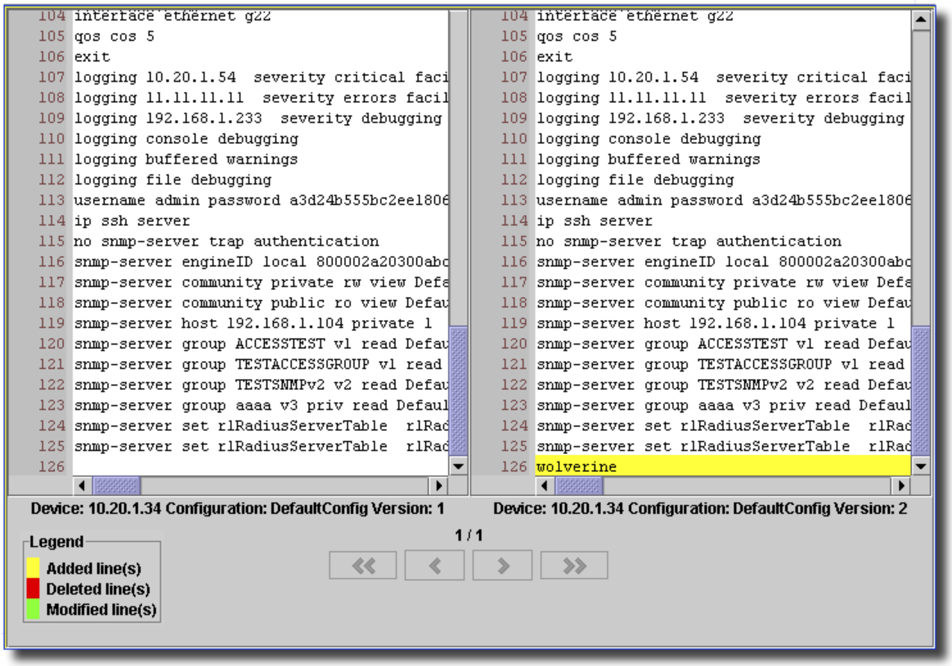
- **Edit**—Edit the selected configuration file.

- **Import**—Import a configuration file. See Restore Action Type on page 863 for more about import capabilities and configuration.

- **Export**—Export the selected configuration file to the local file system.

- **Delete**—Remove the selected configuration file from the list.

- **Compare**—Compare two selected configuration files. Ctrl+click to select files, then click the button. A screen with the two configuration files side-by-side appears, with the differences highlighted.



```
interface ethernet g22
qos cos 5
exit
logging 10.20.1.54  severity critical faci
logging 11.11.11.11  severity errors facil
logging 192.168.1.233  severity debugging
logging console debugging
logging buffered warnings
logging file debugging
username admin password a3d24b555bc2ee1806
ip ssh server
no snmp-server trap authentication
snmp-server engineID local 800002a20300abc
snmp-server community private rw view Defa
snmp-server community public ro view Defau
snmp-server host 192.168.1.104 private 1
snmp-server group ACCESSTEST v1 read Defau
snmp-server group TESTACCESSGROUP v1 read
snmp-server group TESTSNMPv2 v2 read Defau
snmp-server group aaaa v3 priv read Defaul
snmp-server set rlRadiusServerTable  rlRad
snmp-server set rlRadiusServerTable  rlRad
```

Device: 10.20.1.34 Configuration: DefaultConfig Version: 1

```
interface ethernet g22
qos cos 5
exit
logging 10.20.1.54  severity critical faci
logging 11.11.11.11  severity errors facil
logging 192.168.1.233  severity debugging
logging console debugging
logging buffered warnings
logging file debugging
username admin password a3d24b555bc2ee1806
ip ssh server
no snmp-server trap authentication
snmp-server engineID local 800002a20300abc
snmp-server community private rw view Defa
snmp-server community public ro view Defau
snmp-server host 192.168.1.104 private 1
snmp-server group ACCESSTEST v1 read Defau
snmp-server group TESTACCESSGROUP v1 read
snmp-server group TESTSNMPv2 v2 read Defau
snmp-server group aaaa v3 priv read Defaul
snmp-server set rlRadiusServerTable  rlRad
snmp-server set rlRadiusServerTable  rlRad
wolverine
```

Device: 10.20.1.34 Configuration: DefaultConfig Version: 2

- **Add to Label**—This button assigns the selected equipment's backups to a label that you select from a subsequent dialog. Notice that selected labels appear listed in the lower portion of this screen, along with columns that describe the *File Name*, *Version*, and *Date* of the backed up configuration file.

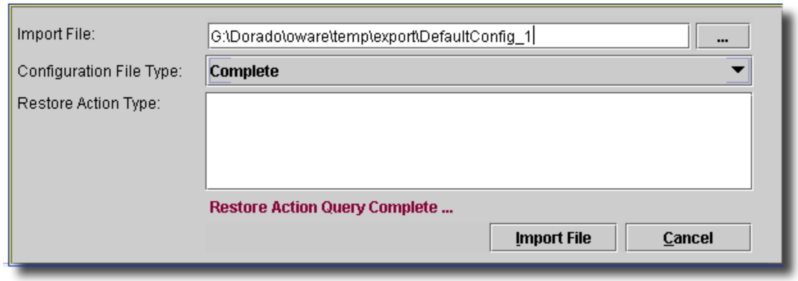
Current Labelled Configurations

This panel lists labelled configurations associated with the selected equipment. You can *View*, or *Remove* selected configurations from this list. The *Add to Label* button in the top half of the screen lets you add more labelled configurations. If you select two configurations, you can click *Compare*, and the side-by-side comparison of the two configurations appears, with the differences highlighted.

Restore Action Type

When you import a configuration file, you can select the file itself, and the type of restoration. When the equipment's driver supports it, you can choose a *Restore Action Type* from a list box, after you select the *Configuration File Type* (for example: *Partial*, *Complete*) from the pick list.

Figure 36-6. Import Configuration File



Import File: G:\Dorado\oware\temp\export\DefaultConfig_1

Configuration File Type: Complete

Restore Action Type:

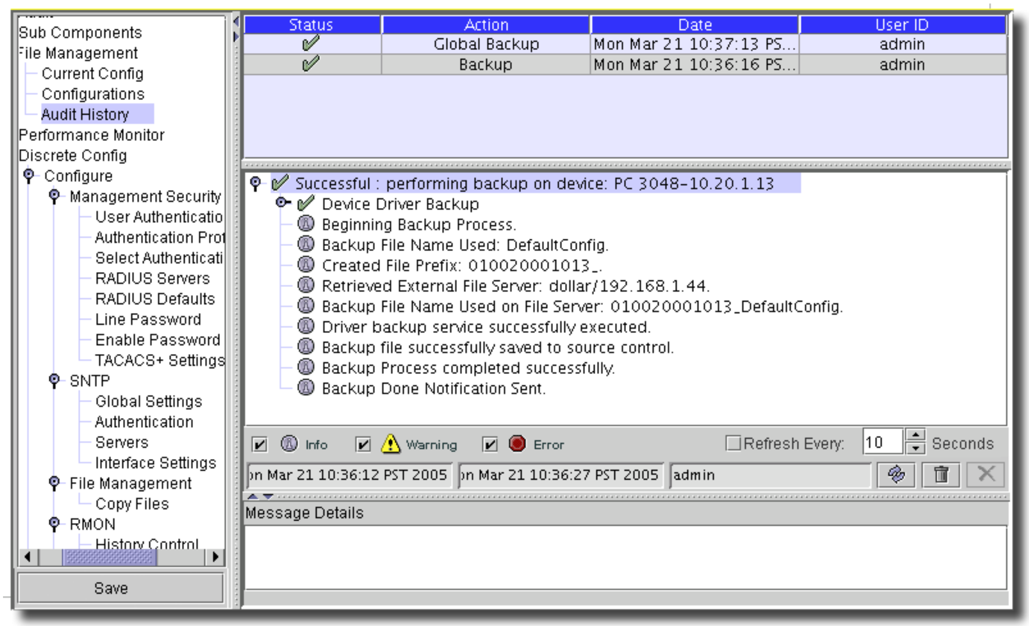
Restore Action Query Complete ...

The driver provides the restore action types. Some example action types: *merge*, *override*, *replace*, and *patch*. The list of action types depends on the driver's capabilities.

File Management -> Audit History

The Audit History panel shows the history of any File Management configuration steps you initiated on the selected device.

Figure 36-7. Status Messages



Status	Action	Date	User ID
✓	Global Backup	Mon Mar 21 10:37:13 PS...	admin
✓	Backup	Mon Mar 21 10:36:16 PS...	admin

```
✓ Successful : performing backup on device: PC 3048-10.20.1.13
  ✓ Device Driver Backup
    Beginning Backup Process.
    Backup File Name Used: DefaultConfig.
    Created File Prefix: 010020001013_.
    Retrieved External File Server: dollar/192.168.1.44.
    Backup File Name Used on File Server: 010020001013_DefaultConfig.
    Driver backup service successfully executed.
    Backup file successfully saved to source control.
    Backup Process completed successfully.
    Backup Done Notification Sent.
```

on Mar 21 10:36:12 PST 2005 | on Mar 21 10:36:27 PST 2005 | admin

The upper part of this screen displays nodes for each job done. When you select a job, the next lower screen lets you display a tree of nodes describing individual steps. If you select a node, the bar below this screen displays details like its start and end times, and the classification of message (for example: admin). The lowest panel displays even more details for any selected message. The messages displayed there depend on which checkboxes you select at the bottom of the screen. You can select the level of error display: *Debug*, *Info*, *Warning*, *Error.* You can also elect to *include child job messages*, or *auto update*.Clicking on a message displays the details of the message in the text area at the bottom of the screen.

NOTE:

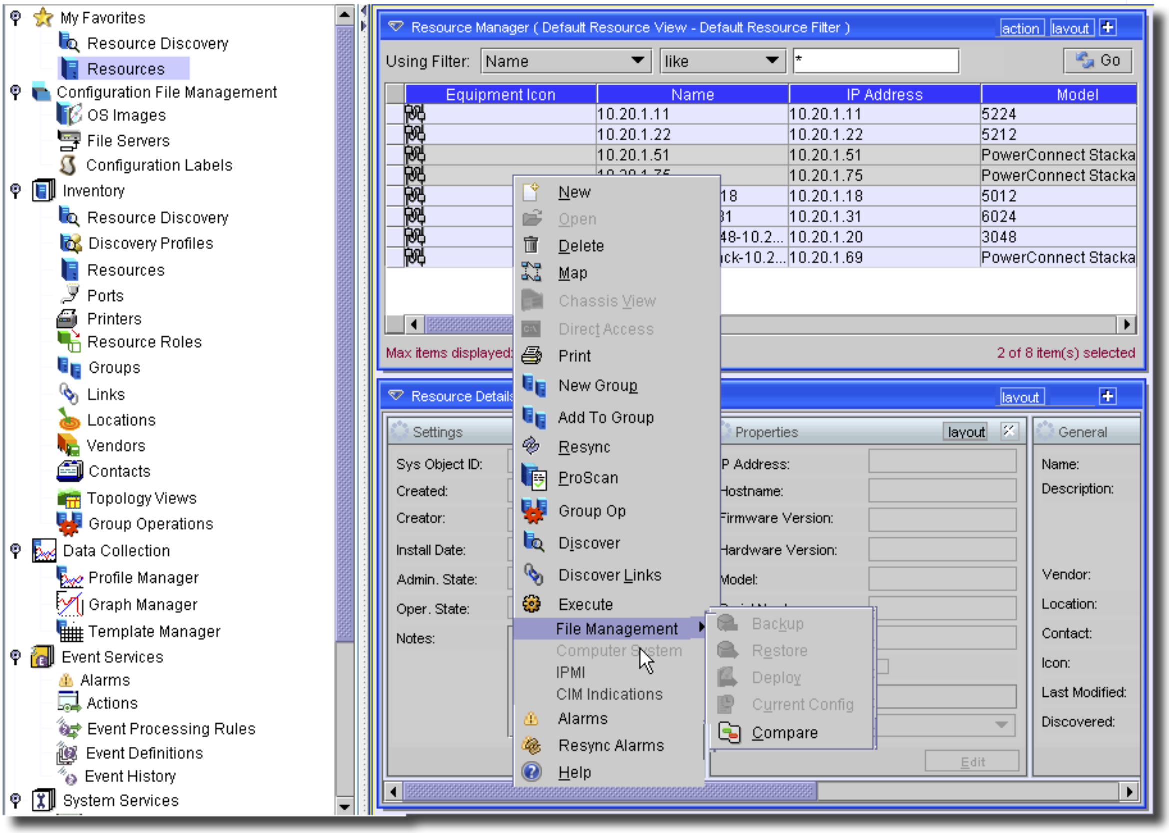
Only Debug and Error messages' details appear in the bottom Message Details box

The circular double arrows refresh this screen, and the trash can discards selected messages, and the "X" cancels a running job.

Comparing Files

You can compare the following backed up files for a single device or for two devices. By default, the comparison is text-based, but application administrators can set comparison to *binary.* To do this, open *Settings* -> *Configuration* -> *Control Settings* and select the *Properties* tab. Change the following property to have all checkins compared as binary: `redcell.netrestore.filetype=text`. The alternative is `redcell.netrestore.filetype=binary.` Select one or two pieces of equipment in Resource Manager, and click the Compare button. You can also compare from the Configuration Node in Resource Editor.

Figure 36-8. Click *Compare* after Selecting



Resource Manager (Default Resource View - Default Resource Filter)

Using Filter: Name like *

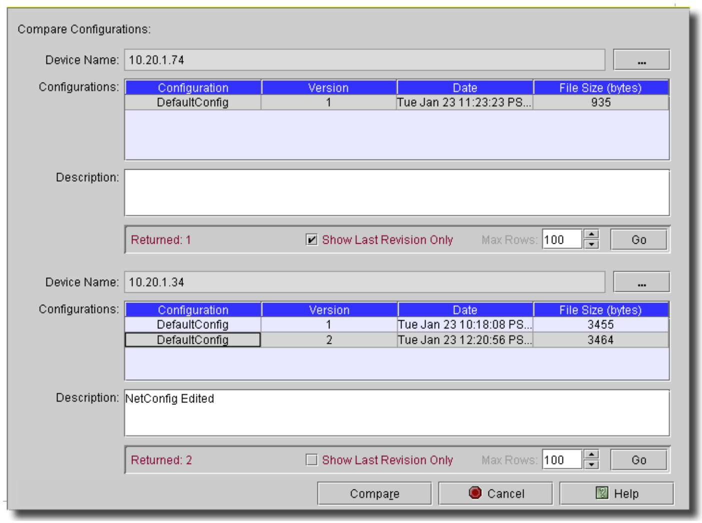
Equipment Icon	Name	IP Address	Model
	10.20.1.11	10.20.1.11	5224
	10.20.1.22	10.20.1.22	5212
	10.20.1.51	10.20.1.51	PowerConnect Stacka
	10.20.1.75	10.20.1.75	PowerConnect Stacka
	18	10.20.1.18	5012
	31	10.20.1.31	6024
	48-10.2...	10.20.1.20	3048
	ck-10.2...	10.20.1.69	PowerConnect Stacka

Max items displayed:

2 of 8 item(s) selected

To compare two device's files, select them in the subsequent screen, then click the *Compare* button.

Figure 36-9. Compare Configurations for Two Devices



Compare Configurations:

Device Name: 10.20.1.74

Configurations:

Configuration	Version	Date	File Size (bytes)
DefaultConfig	1	Tue Jan 23 11:23:23 PS...	935

Description:

Returned: 1 ☑ Show Last Revision Only Max Rows: 100

Device Name: 10.20.1.34

Configurations:

Configuration	Version	Date	File Size (bytes)
DefaultConfig	1	Tue Jan 23 10:18:08 PS...	3455
DefaultConfig	2	Tue Jan 23 12:20:56 PS...	3464

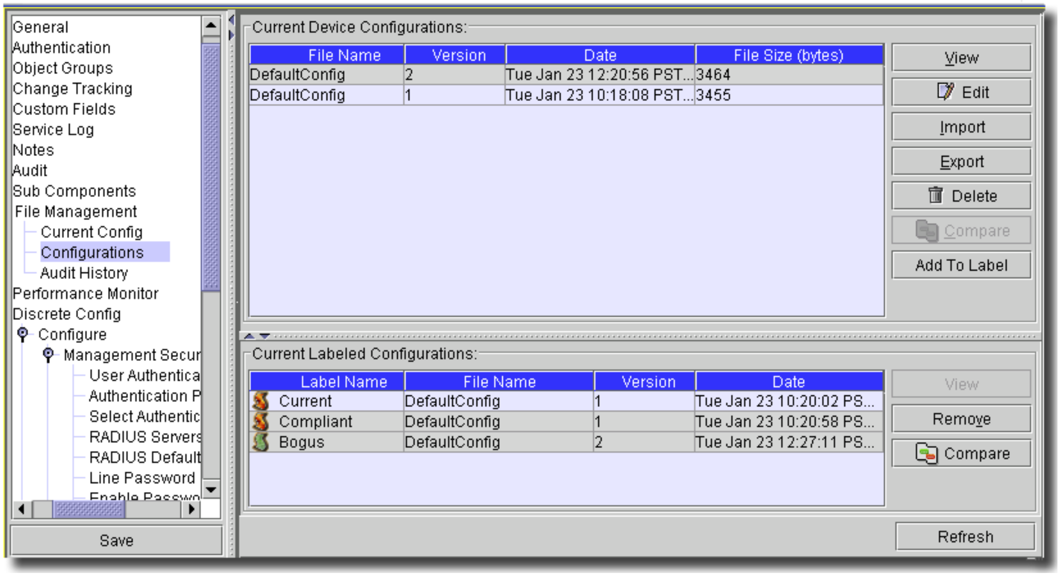
Description: NetConfig Edited

Returned: 2 □ Show Last Revision Only Max Rows: 100

The *Go* buttons below the tables of configurations queries the database, and refreshes the list. You can also check *Show Last Revision Only* or alter *Max Rows* to limit that query. You can select files on two devices, or different versions of files on a single device.

You can also compare configuration files for a single device. Click *Open* once you select the device in the Resource Manager, and open the Configurations node in the display.

Figure 36-10. Compare Files on One Device



Current Device Configurations:

File Name	Version	Date	File Size (bytes)
DefaultConfig	2	Tue Jan 23 12:20:56 PST...	3464
DefaultConfig	1	Tue Jan 23 10:18:08 PST...	3455

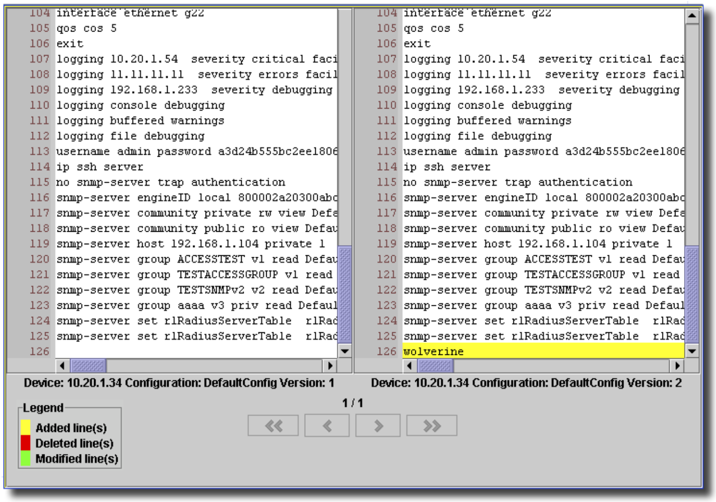
Current Labeled Configurations:

Label Name	File Name	Version	Date
Current	DefaultConfig	1	Tue Jan 23 10:20:02 PS...
Compliant	DefaultConfig	1	Tue Jan 23 10:20:58 PS...
Bogus	DefaultConfig	2	Tue Jan 23 12:27:11 PS...

Select the two listed files you want to compare, and click the *Compare* button.

The resulting dialog shows the two files side-by-side.

Figure 36-11. File Comparison



```
interface ethernet g22
qos cos 5
exit
logging 10.20.1.54  severity critical faci
logging 11.11.11.11  severity errors facil
logging 192.168.1.233  severity debugging
logging console debugging
logging buffered warnings
logging file debugging
username admin password a3d24b555bc2ee1806
ip ssh server
no snmp-server trap authentication
snmp-server engineID local 800002a20300abc
snmp-server community private rw view Defa
snmp-server community public ro view Defau
snmp-server host 192.168.1.104 private 1
snmp-server group ACCESSTEST v1 read Defau
snmp-server group TESTACCESSGROUP v1 read
snmp-server group TESTSNMPv2 v2 read Defau
snmp-server group aaaa v3 priv read Defaul
snmp-server set rlRadiusServerTable  rlRad
snmp-server set rlRadiusServerTable  rlRad

```

Device: 10.20.1.34 Configuration: DefaultConfig Version: 1

```
interface ethernet g22
qos cos 5
exit
logging 10.20.1.54  severity critical faci
logging 11.11.11.11  severity errors facil
logging 192.168.1.233  severity debugging
logging console debugging
logging buffered warnings
logging file debugging
username admin password a3d24b555bc2ee1806
ip ssh server
no snmp-server trap authentication
snmp-server engineID local 800002a20300abc
snmp-server community private rw view Defa
snmp-server community public ro view Defau
snmp-server host 192.168.1.104 private 1
snmp-server group ACCESSTEST v1 read Defau
snmp-server group TESTACCESSGROUP v1 read
snmp-server group TESTSNMPv2 v2 read Defau
snmp-server group aaaa v3 priv read Defaul
snmp-server set rlRadiusServerTable  rlRad
snmp-server set rlRadiusServerTable  rlRad
wolverine
```

Device: 10.20.1.34 Configuration: DefaultConfig Version: 2

Legend
- 🟨 Added line(s)
- 🟥 Deleted line(s)
- 🟩 Modified line(s)

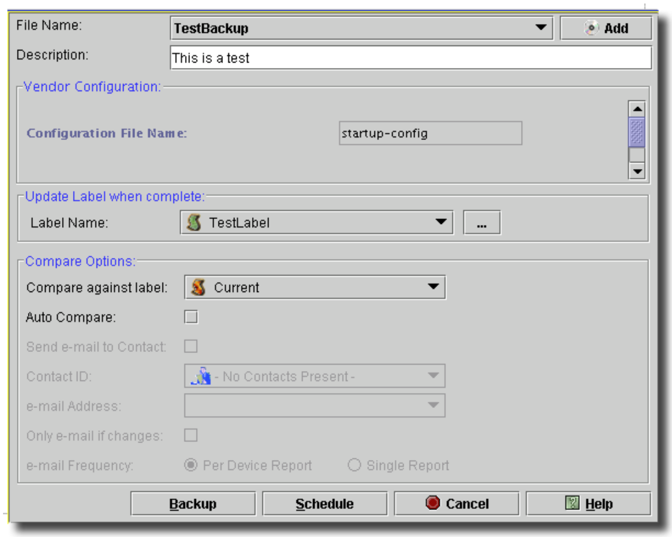
Differences between the two files are highlighted (the *Legend* in the lower left corner of this panel describes the significance of the colors).

Backup

To use the backup function, follow these steps:

1. Launch the Resources manager.
2. Using a filter, retrieve the list of network elements; they appear in the Resource manager table.
3. Select the desired network elements in the table and then click on the *Backup* button. (See Figure 36-1, Resources Screen with NetConfig Menu Open on page 857).
4. When you click the *Backup…* button, the form that appears next shows the network elements selected from the resource manager. The combo box in the *Configuration File* section shows the list of already used configuration file names for that particular network element. Clicking the *Add* button lets you add a different file name. Click *Save* and the added file appears in the pick list.

5 Select the Configuration File to back up



File Name: TestBackup ▼

Description: This is a test

Vendor Configuration:

Configuration File Name: startup-config

Update Label when complete:

Label Name: TestLabel ▼

Compare Options:

Compare against label: Current ▼

Auto Compare: □

Send e-mail to Contact: □

Contact ID: - No Contacts Present - ▼

e-mail Address: ▼

Only e-mail if changes: □

e-mail Frequency: ● Per Device Report ○ Single Report

The Vendor Configuration portion of this screen varies, depending on the type of equipment you are backing up. Hover your cursor over the offered alternatives for more information. For example, a Netscreen device lets you check *Save Config to Last Good* (label).

6 You can also select a label to update (*Update Label when complete*) to add this configuration backup.

Compare Options

7 *Compare against label* lets you compare a current backup against an existing, labelled backup.

NOTE:

If you select *Current* as the label to compare with, remember that *Current* automatically collects the most recent backups for the selected device. After the backup you are configuring here is complete, the application updates *Current* so it now points to this backup.

8 The *Auto Compare* checkbox lets you automatically detect whether any difference exists between the current backup and the selected label.

9 Enter a description, and select any other vendor-specific information from the available fields.

10 Set *Send e-mail to contact* if you want to send e-mail to the selected contacts after you complete the backup. The checkbox enables this function. This sends standard e-mails to the selected contact with subject lines like this:

```
Backup: JunM5-1-192.168.1.109 December Rev: 4 --> No Change
```

If the backup is a file that is different from previous versions, the differences are in a file attached to the e-mail. To use this function, you must set up the following fields:

Contact ID—Select a contact from the pick list. These are the contacts in the application's Contact Manager.

e-mail Address—A pick list to select an e-mail address if the contact has more than one.

Only e-mail if changes—Check this to send e-mail only if the application detects a difference between the current backup and the selected label.

To produce e-mails that do not count a shift in a config file line's position as a change, modify the following property in `\owareapps\netrestore\lib\nr.properties` (or, better, override it in `owareapps\installprops\lib\installed.properties`):

```
#============================================
# NetConfig Move Omit Property:
# Terms specified will be used to let NetConfig
# know what movement changes in config files should be
# included in configuration changes emails.
#
# Note: This property is only used if
# identical(!) lines move in config files.
#
# Example:
# Old Changes:
#   line 259: ntp server 10.20.0.1
# New Changes:
#   line 273: ntp server 10.20.0.1
#
# In the above case the line moved from line 259 to 273.
# This change will show up in the email sent to the specified
# end user.
# To omit this change from the email, include 'ntp server' in
# the property below.
# Best practice is to place this property in
# ...\owareapps\installprops\lib\installed.properties
#============================================
#append.com.dorado.redcell.netrestore.backup.move.omit=,## Last
```

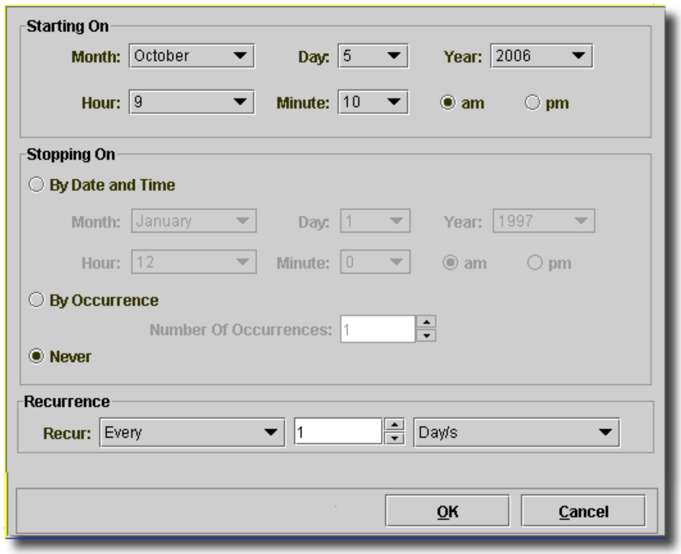
If the e-mail attachment describing config changes is empty, the e-mail sent says "No changes" in the subject.

e-mail Frequency—These radio buttons become active if you are scheduling a backup as part of a group operation (see Chapter 22, Group Operations). If you select *Per Device Report*, then each device backed up sends a single e-mail. If you select *Single Report*, then all devices' e-mails are concatenated into a single e-mail.

NOTE:

Sending e-mail is also available as part of backup set through the group operations option. If you do a group of backups, requesting e-mail, then the application generates an e-mail for each device for each backup.

11 Then either click on the *Backup* button to start the backup process, or the *Schedule* button to launch the scheduler form.



Starting On

Month: October Day: 5 Year: 2006

Hour: 9 Minute: 10 ● am ○ pm

Stopping On

○ By Date and Time

Month: January Day: 1 Year: 1997

Hour: 12 Minute: 0 ● am ○ pm

○ By Occurrence

Number Of Occurrences: 1

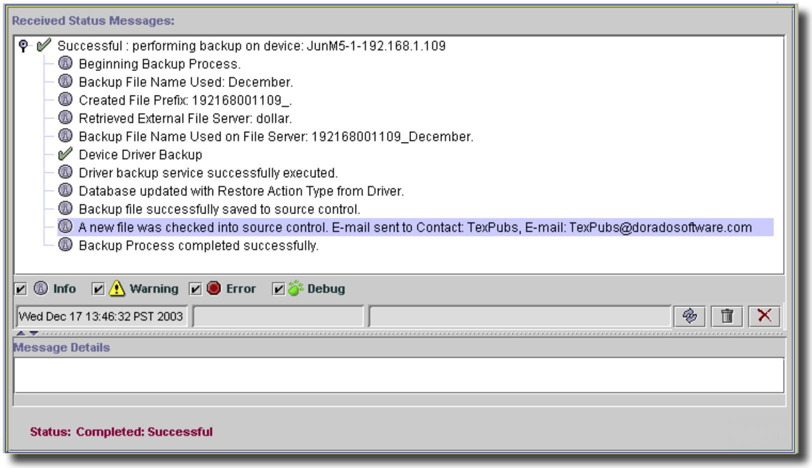
● Never

Recurrence

Recur: Every 1 Day/s

If you schedule backup, set the time, recurrence, and so on in this screen. Clicking on the *OK* button in this screen schedules the backup job using the parameters selected. The *Cancel* button returns to the previous screen.

12 If you select *Backup*, the status of the backup actions appears on a subsequent screen.



Received Status Messages:

```
Successful : performing backup on device: JunM5-1-192.168.1.109
  Beginning Backup Process.
  Backup File Name Used: December.
  Created File Prefix: 192168001109_.
  Retrieved External File Server: dollar.
  Backup File Name Used on File Server: 192168001109_December.
  Device Driver Backup
  Driver backup service successfully executed.
  Database updated with Restore Action Type from Driver.
  Backup file successfully saved to source control.
  A new file was checked into source control. E-mail sent to Contact: TexPubs, E-mail: TexPubs@doradosoftware.com
  Backup Process completed successfully.
```

☑ Info ☑ Warning ☑ Error ☑ Debug

Wed Dec 17 13:46:32 PST 2003

Message Details

Status: Completed: Successful

These messages display the job's status.

NOTE:

If the backup sends e-mail, that act appears as a message in this status screen.

Global Backup

Global backup is what notifications and actions call. If, for example, the optional Change Manager detects a compliant network element, then notifications and actions can automate backup that compliant configuration. The defaults that appear in the equipment's backup screen are the kind of backup that occurs in such a case.

To select a backup protocol and which configuration to backup, OpenManage Network Manager supports a preference ordering so you can set the order of preference. The values, in order, are:

Protocol—SFTP, SCP, FTP, TFTP, HTTPS, HTTP.

Device Config File—Running, Startup, Backup.

The device driver selects the first value in the list that they support, and supplies a default.

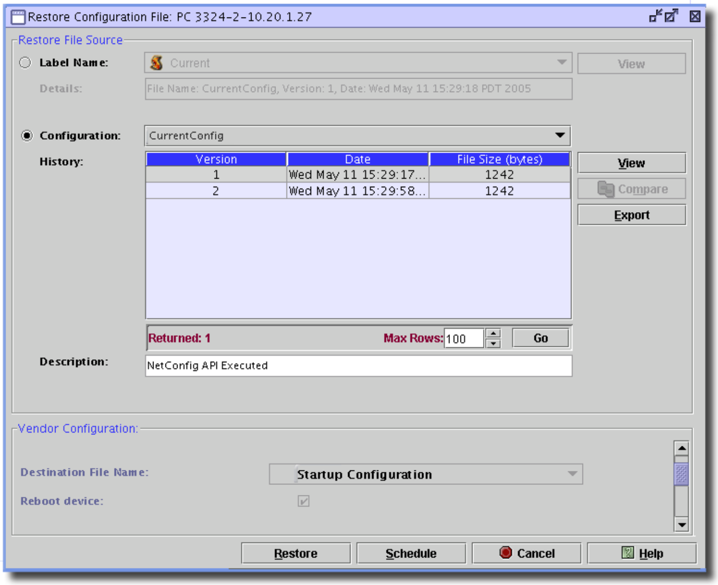
Restore

Restore a backed up configuration file with the following procedure:

1 Launch the Resource Manager.

2 Using the filter, retrieve the list of network elements, which would then appear in the Resource Manager table.

3 Select the desired network elements in the table and then click on the *Restore…* button. The restoration form appears.



Restore Configuration File: PC 3324-2-10.20.1.27

Restore File Source

○ Label Name: Current

Details: File Name: CurrentConfig, Version: 1, Date: Wed May 11 15:29:18 PDT 2005

● Configuration: CurrentConfig

History:

Version	Date	File Size (bytes)
1	Wed May 11 15:29:17...	1242
2	Wed May 11 15:29:58...	1242

Returned: 1 Max Rows: 100

Description: NetConfig API Executed

Vendor Configuration:

Destination File Name: Startup Configuration

Reboot device: ☑

The table in the center of the screen shows a list of historical backups. You can use the buttons to its right to *View*, *Compare*, or *Export* files. The comparison lets you compare two versions of a backup file. See Comparing Files on page 864 for further discussion about this feature.

Use the *Configuration* combo box to select from the list of configuration files valid for that particular network element row. The *Go* button below the table queries the database for the history, and can refresh the list.

The appearance of the *Vendor Configuration* section of this screen depends on the type of equipment you are restoring. For example, it can display a file name for this vendor's configuration, and a checkbox that enables a device reboot after restoration. Hover the cursor over the available alternatives for additional information.

Notice there are buttons that let you *View*, *Export*, or *Compare* selected files. You must select more than one before you can *Compare*.

4 Select the Configuration File and the Version to be restored for each network element.

To begin restoration, either click on the *Restore* button to start the restore process, or click the *Schedule* button to launch the Scheduler form. Clicking the *Cancel* button returns you to the previous screen.

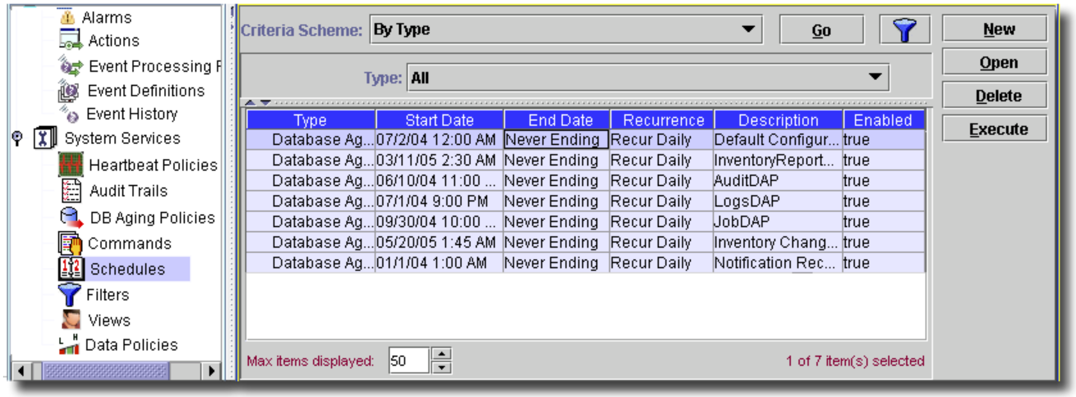
Global Restoration

Global restoration is what notifications and actions call. If, for example, the optional Change Manager detects an out-of-compliance network element, then notifications and actions can automate restoring a compliant configuration. The defaults that appear in the equipment's restoration screen are the kind of restoration that occurs in such a case.

Scheduling File Operations

Backup, and Restore (sometimes called *NetRestore*) use the System Services scheduler manager to see and manage scheduled backups, restorations or deployments you create as you use those features of this application.

Figure 36-12. Network Services Scheduler



Criteria Scheme: By Type

Type: All

Type	Start Date	End Date	Recurrence	Description	Enabled
Database Ag...	07/2/04 12:00 AM	Never Ending	Recur Daily	Default Configur...	true
Database Ag...	03/11/05 2:30 AM	Never Ending	Recur Daily	InventoryReport...	true
Database Ag...	06/10/04 11:00 ...	Never Ending	Recur Daily	AuditDAP	true
Database Ag...	07/1/04 9:00 PM	Never Ending	Recur Daily	LogsDAP	true
Database Ag...	09/30/04 10:00 ...	Never Ending	Recur Daily	JobDAP	true
Database Ag...	05/20/05 1:45 AM	Never Ending	Recur Daily	Inventory Chang...	true
Database Ag...	01/1/04 1:00 AM	Never Ending	Recur Daily	Notification Rec...	true

Max items displayed: 50

1 of 7 item(s) selected

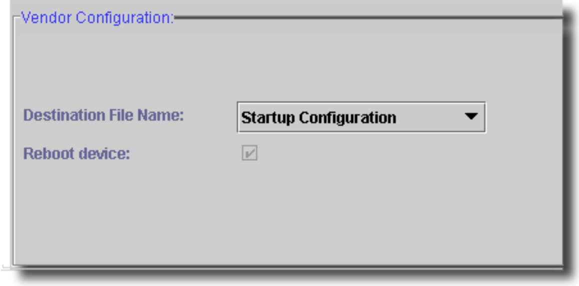
New lets you create a new job downloading firmware. The *Open* button lets you edit a selected job scheduled in the table. Both launch the schedule editor.

The *Execute* Button lets you run the selected job. The *Delete* button lets you delete the job.

Dell Restore

If you have the File Management option installed, this panel lets you configure the restoration destination.

Figure 36-1. Dell Restore Vendor Panel



Vendor Configuration:

Destination File Name: Startup Configuration

Reboot device: ☑

Select *Running Configuration*, *Startup Configuration*, or *Backup Configuration* using the pick list. Some models also let you check *Reboot Device* so the equipment reboots after restoration.

37

Deploying

Deploy Elements Overview

The Deploy capabilities of this application let you conveniently manage both device configurations and firmware deployments. Before you can use these capabilities, however, you may want to configure an FTP or TFTP server to retrieve or deploy the files. Chapter 35, File Servers describes this setup. The internal FTP/TFTP server is enabled by default.

The following are this application's capabilities for deploying network element firmware or operating system files:

- Maintain a history of software installed/deployed on the network element by the element management system.
- Stage and import the software images/patches, then deploy, or redeploy them to specific network elements.
- Track the software images and patches deployed to any given network element.
- Schedule the deployment of a software image or patch to any single network element.

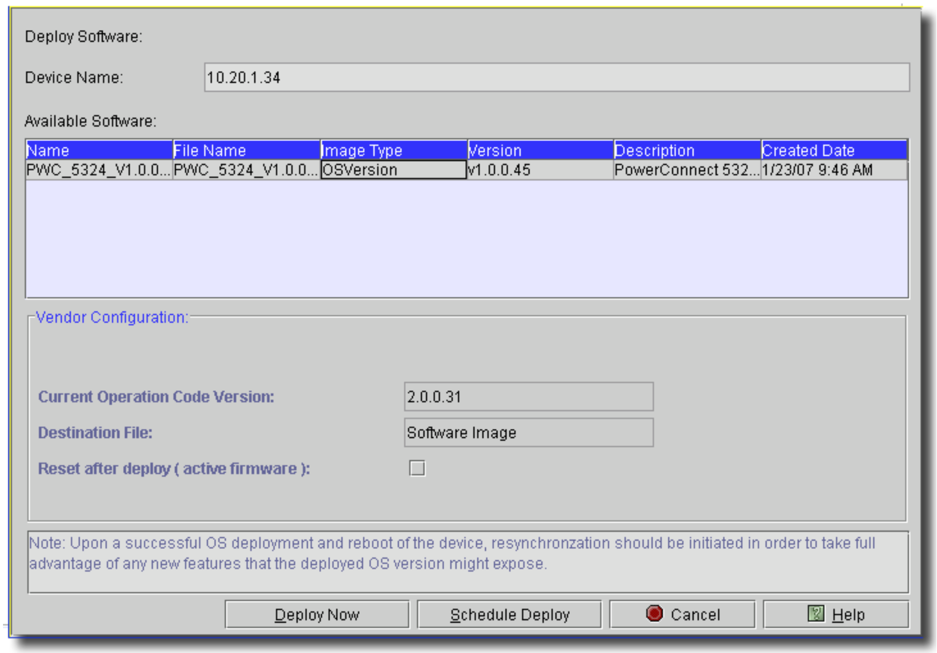
This application employs various components, described in the following sections, to do the above.

Deploy

The following section describes using NetConfig to deploy software (firmware, or O/S patches). You can deploy to groups of network equipment too (see Deploying Globally on page 880). Follow these steps to deploy software to individual devices:

1. Launch the Resource Manager.
2. Using the filter, retrieve the list of network elements, which then appear in the Resource Manager table.

3 Select the desired network elements in the table and then click on the *Deploy…* menu item in the *Action* or right-click menu. This launches the deployment form.



Deploy Software:

Device Name: 10.20.1.34

Available Software:

Name	File Name	Image Type	Version	Description	Created Date
PWC_5324_V1.0.0...	PWC_5324_V1.0.0...	OSVersion	v1.0.0.45	PowerConnect 532...	1/23/07 9:46 AM

Vendor Configuration:

Current Operation Code Version: 2.0.0.31

Destination File: Software Image

Reset after deploy (active firmware): ☐

Note: Upon a successful OS deployment and reboot of the device, resynchronzation should be initiated in order to take full advantage of any new features that the deployed OS version might expose.

The appearance of this screen may be different for some devices.

4 The table shown under *Available Software* displays all the software entries available for the network element(s) selected.

5 When you click on a table row in the *Available Software* tab, the software row selected has already been validated against all the network element entries in the list (The validation checks if the vendors for the network elements in the list are included as providers of the equipment to which the software may be applied.).

6 When you select a row in the *Available Software* table, File Management activates the *Deploy Now* and *Schedule Deploy* buttons on this screen.

Depending on the installed drivers, for some devices, you can also elect to *Remove unused operation images* and *Reboot Device* with the check boxes in the *Vendor Configuration* portion of the screen. The *Current Operation Code Version* and *Current Operation Code Image* fields are read-only.

Other vendor panels include a pick list for a deployment *Protocol* (*TFTP / FTP*), a *File System* on the device, and you may enable *Verify Install* with a checkbox, if the device has this capability. This checks whether the active software is verified (and possibly repaired) for consistency. This is performed after the specified software is installed during the deploy process.

7 To begin the deployment process, either click on the *Deploy Now* button to start the deploy process, or click on the *Schedule Deploy…* button to launch the scheduler form (see Scheduling Downloads on page 888). Clicking the *Cancel* button aborts this operation.

Reboot

Some devices require a reboot after you deploy firmware. For example, Dell Powerconnect devices have (2) OS image banks – one active and one inactive. During the deployment process, the inactive bank receives the image. You must then restart the device to make this newly updated bank the active one. Deploying does not update the remaining downlevel image bank (now inactive).

This software displays a message in job status and the audit trail stating that, if the upgrade to the new firmware version/bootcode is successful, you must ensure that the other image also is upgraded to the new firmware. You can elect to reboot as part of the deployment too.

Best Practices

Executing or scheduling a resynchronization on your systems before and after performing updates is suggested. By performing a scan before, you ensure that you have retrieved the latest driver, firmware, and BIOS inventory information from your systems before comparing their configuration to the latest available update package. Scanning after the update ensures that you capture the latest information about the new inventory so that the latest information appears in the server audit history and as a reference.

Best practice is also to download any updates each quarter (see Download on page 885). This ensures that you have the latest version of download packages and captures any interim changes that could have been made to those packages if you downloaded them previously.

NOTE:

If the name of the download package has not changed but you know its contents changed, you may need to delete the previous version from the OS Manager to have the new package appear as available for download.

If a patch fails during the deployment, the update process stops. To receive the patches that come sequentially after the failed update, you must unselect the failed patch in the next update try.

Deploying Globally

Here are the steps for globally deploying software to equipment groups.

1 Import the new OS to OS Images Manager (see OS Images on page 882).

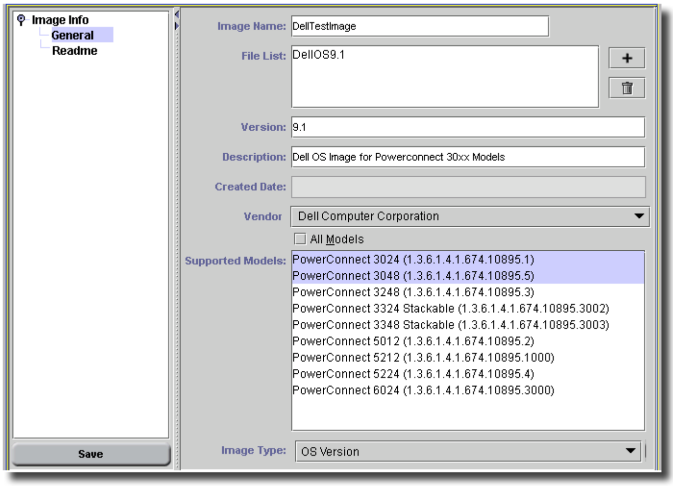


Image Name: DellTestImage

File List: DellOS9.1

Version: 9.1

Description: Dell OS Image for Powerconnect 30xx Models

Created Date:

Vendor Dell Computer Corporation

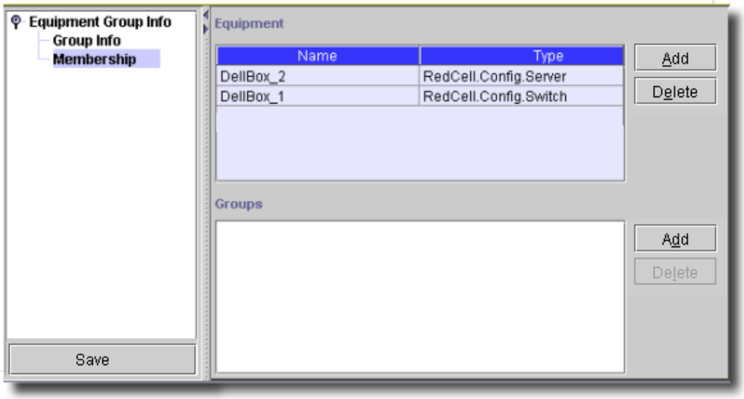
□ All Models

Supported Models:
PowerConnect 3024 (1.3.6.1.4.1.674.10895.1)
PowerConnect 3048 (1.3.6.1.4.1.674.10895.5)
PowerConnect 3248 (1.3.6.1.4.1.674.10895.3)
PowerConnect 3324 Stackable (1.3.6.1.4.1.674.10895.3002)
PowerConnect 3348 Stackable (1.3.6.1.4.1.674.10895.3003)
PowerConnect 5012 (1.3.6.1.4.1.674.10895.2)
PowerConnect 5212 (1.3.6.1.4.1.674.10895.1000)
PowerConnect 5224 (1.3.6.1.4.1.674.10895.4)
PowerConnect 6024 (1.3.6.1.4.1.674.10895.3000)

Image Type: OS Version

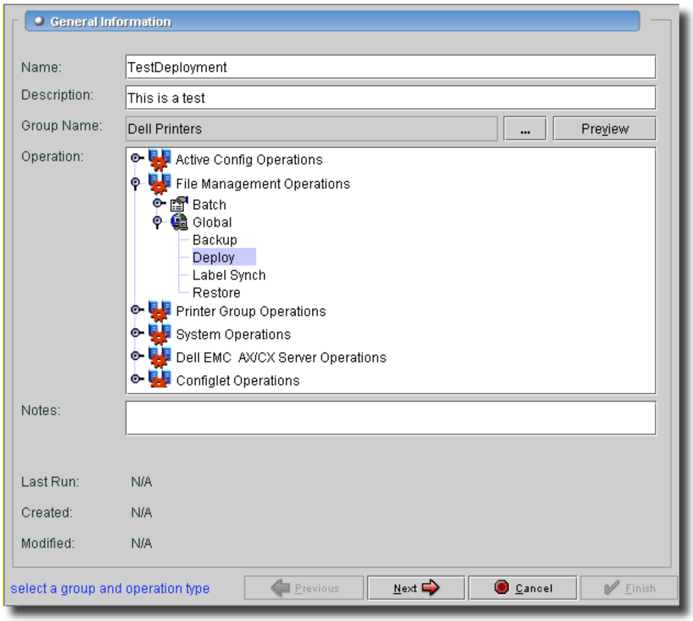
For example, specify *Dell Computer Corporation* as the Vendor.

2 Add devices to a Group from the Group Manager/Editor or create a Dynamic Group. Global Deployment then uses this Group. (See the *Equipment Group Manager* section of the *User Guide* for more about groups). This example has two Dell devices.



Name	Type
DellBox_2	RedCell.Config.Server
DellBox_1	RedCell.Config.Switch

3 Launch the Group Operation Wizard, and specify *File Management Operations -> Global -> Deploy*.



General Information

Name: TestDeployment

Description: This is a test

Group Name: Dell Printers

Operation: File Management Operations > Global > Deploy

Notes:

Last Run: N/A

Created: N/A

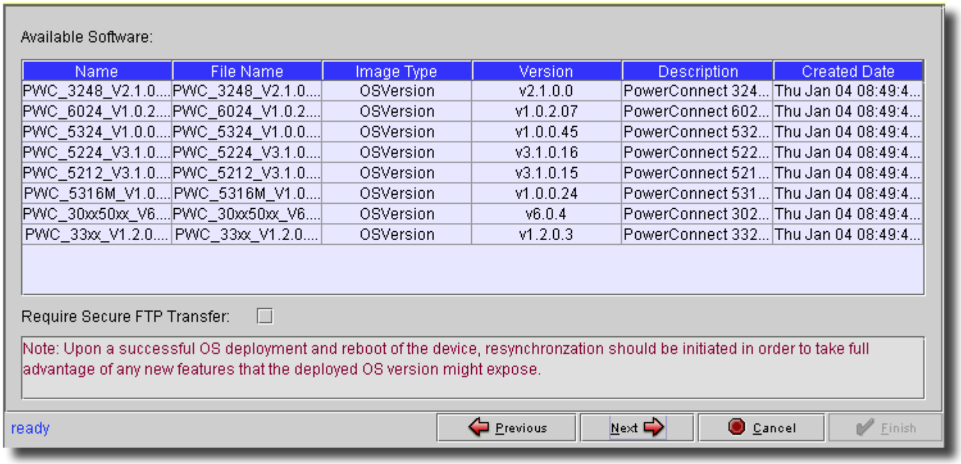
Modified: N/A

select a group and operation type

NOTE:

You can click the *Preview* button to see an operation's consequences before you execute or schedule it.

4 After you click *Next*, choose the OS to deploy to the selected group.



Available Software:

Name	File Name	Image Type	Version	Description	Created Date
PWC_3248_V2.1.0....	PWC_3248_V2.1.0....	OSVersion	v2.1.0.0	PowerConnect 324...	Thu Jan 04 08:49:4...
PWC_6024_V1.0.2....	PWC_6024_V1.0.2....	OSVersion	v1.0.2.07	PowerConnect 602...	Thu Jan 04 08:49:4...
PWC_5324_V1.0.0....	PWC_5324_V1.0.0....	OSVersion	v1.0.0.45	PowerConnect 532...	Thu Jan 04 08:49:4...
PWC_5224_V3.1.0....	PWC_5224_V3.1.0....	OSVersion	v3.1.0.16	PowerConnect 522...	Thu Jan 04 08:49:4...
PWC_5212_V3.1.0....	PWC_5212_V3.1.0....	OSVersion	v3.1.0.15	PowerConnect 521...	Thu Jan 04 08:49:4...
PWC_5316M_V1.0....	PWC_5316M_V1.0....	OSVersion	v1.0.0.24	PowerConnect 531...	Thu Jan 04 08:49:4...
PWC_30xx50xx_V6....	PWC_30xx50xx_V6....	OSVersion	v6.0.4	PowerConnect 302...	Thu Jan 04 08:49:4...
PWC_33xx_V1.2.0....	PWC_33xx_V1.2.0....	OSVersion	v1.2.0.3	PowerConnect 332...	Thu Jan 04 08:49:4...

Require Secure FTP Transfer: □

Note: Upon a successful OS deployment and reboot of the device, resynchronzation should be initiated in order to take full advantage of any new features that the deployed OS version might expose.

ready

This screen contains all imported OS Images. You must select one before you can proceed.

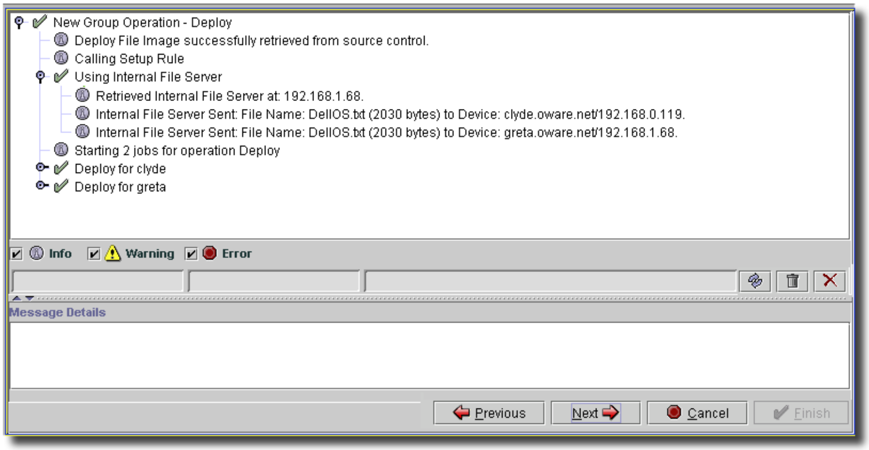
You can also *Require Secure FTP Transfer* with a checkbox. This uses the FTP setup you have already configured in *File Servers on page 849*.

This screen also reminds you that you may need to resync to retrieve any new information the deployment exposes.

5 After clicking *Next*, you may also see a vendor panel with more information about the deployment. When you select a device with the pick list at the top, this screen allows you to further configure deployment.

Use the arrows at the top of the screen to cycle through the available devices, and the circular arrows to *Refresh* that list.

6 After you click next, deployment proceeds. You can monitor deployment in a status screen.



```
New Group Operation - Deploy
    Deploy File Image successfully retrieved from source control.
    Calling Setup Rule
    Using Internal File Server
        Retrieved Internal File Server at: 192.168.1.68.
        Internal File Server Sent: File Name: DellOS.txt (2030 bytes) to Device: clyde.oware.net/192.168.0.119.
        Internal File Server Sent: File Name: DellOS.txt (2030 bytes) to Device: greta.oware.net/192.168.1.68.
    Starting 2 jobs for operation Deploy
    Deploy for clyde
    Deploy for greta
```

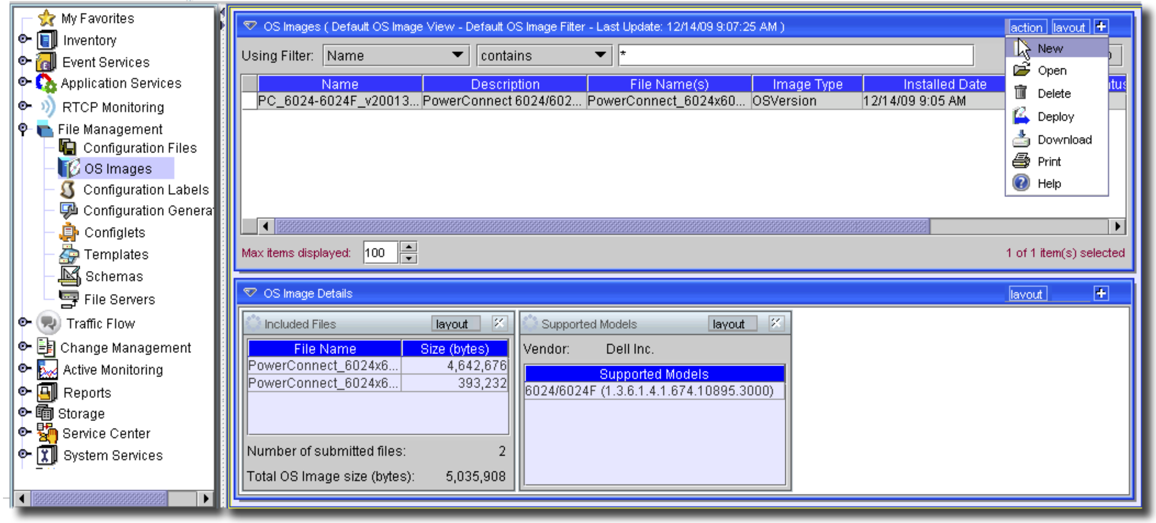
In the illustration two devices (greta/clyde) were members of the group and they both were sent DellOS.txt. Information displayed in this status screen can include:

- The File Server used
- Devices that deployed successfully
- If a device failed, the reason for failure.

OS Images

OS Images Manager tracks deployed software. Open it by selecting *OS Images* under the *File Management* node in the navigation window, or under the *File -> Open -> File Management* menu.

Figure 37-1. OS Images Manager



OS Images (Default OS Image View - Default OS Image Filter - Last Update: 12/14/09 9:07:25 AM)

Using Filter: Name contains *

Name	Description	File Name(s)	Image Type	Installed Date
PC_6024-6024F_v20013...	PowerConnect 6024/602...	PowerConnect_6024x60...	OSVersion	12/14/09 9:05 AM

Max items displayed: 100

1 of 1 item(s) selected

OS Image Details

Included Files

File Name	Size (bytes)
PowerConnect_6024x6...	4,642,676
PowerConnect_6024x6...	393,232

Number of submitted files: 2

Total OS Image size (bytes): 5,035,908

Supported Models

Vendor: Dell Inc.

Supported Models
6024/6024F (1.3.6.1.4.1.674.10895.3000)

Existing operating system images appear listed in the OS *Images* panel at the top of this screen. Downloaded operating systems appear with a disk icon; those created manually with OS Editor do not have that icon.

CAUTION:
This application does not prevent you from deploying an invalid image file or an image file with an invalid file name or file extension

This screen has the following action menu items:

- **New**—Create a new association between an archived OS file and equipment by clicking the *New* button. See OS Editor on page 884 for details.

- **Open—**You can also edit existing associations with the *Open* menu item. See OS Editor on page 884 for details.

- **Delete—**The archive manager's *Delete* Button lets you delete the selected Software Archive.

- **Deploy**—Lets you deploy the selected OS. This opens a global group operation for deployment. See Chapter 22, Group Operations for details.

- **Download**—Lets you automate downloading the selected OS. See Download on page 885 for details.

- **Print**—Print the list of images.

- **Help**—Opens online help for this screen.

OS Images Details

The two details panels display details for selected images. The first displays the files that comprise an individual, deployable image (their count, size and total size). The second panel displays models supported by the selected image.

OS Editor

The OS Editor opens when you click *New* or *Open*. Here, you can edit the selected or new *Image Name*, *File Name* (if necessary, use the plus [+] button to select this file), *Version*, *Description*, and the *Vendor*, *Image Type* and *Supported Models* to which the software/correction applies.

Figure 37-2. OS Editor

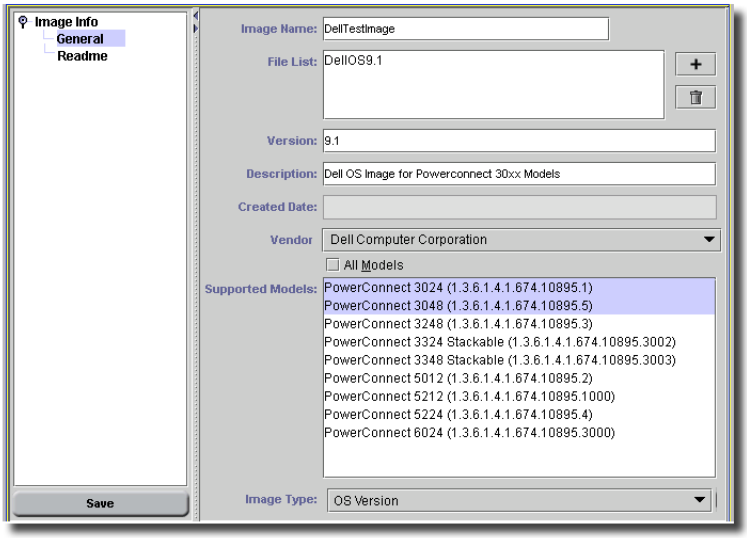


Image Name: DellTestImage

File List: DellOS9.1

Version: 9.1

Description: Dell OS Image for Powerconnect 30xx Models

Created Date:

Vendor: Dell Computer Corporation

□ All Models

Supported Models:
PowerConnect 3024 (1.3.6.1.4.1.674.10895.1)
PowerConnect 3048 (1.3.6.1.4.1.674.10895.5)
PowerConnect 3248 (1.3.6.1.4.1.674.10895.3)
PowerConnect 3324 Stackable (1.3.6.1.4.1.674.10895.3002)
PowerConnect 3348 Stackable (1.3.6.1.4.1.674.10895.3003)
PowerConnect 5012 (1.3.6.1.4.1.674.10895.2)
PowerConnect 5212 (1.3.6.1.4.1.674.10895.1000)
PowerConnect 5224 (1.3.6.1.4.1.674.10895.4)
PowerConnect 6024 (1.3.6.1.4.1.674.10895.3000)

Image Type: OS Version

The vendors displayed in the *Vendor* pick list are only those whose installed device driver supports this feature. You can select listed *Supported Models* (or check *All Models* to select them all), and the *Image Type* pick list automatically offers the supported types of files available for the selection.

Once you complete an archive description and save it, you have effectively assigned the image file to the selected vendor / image type / model combination(s) selected.

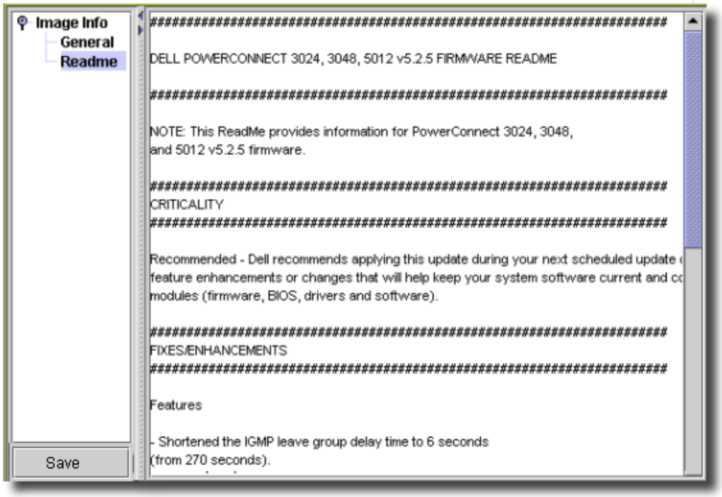
NOTE:

The OS image can be anywhere it can be seen by the application client. If you want it on the sftp server, that directory needs to be mounted on the client machine so the OS images Manager can navigate to it.

Readme Tab

The Readme tab displays any `readme` file associated with the operating system or firmware.

Figure 37-3. Show Readme



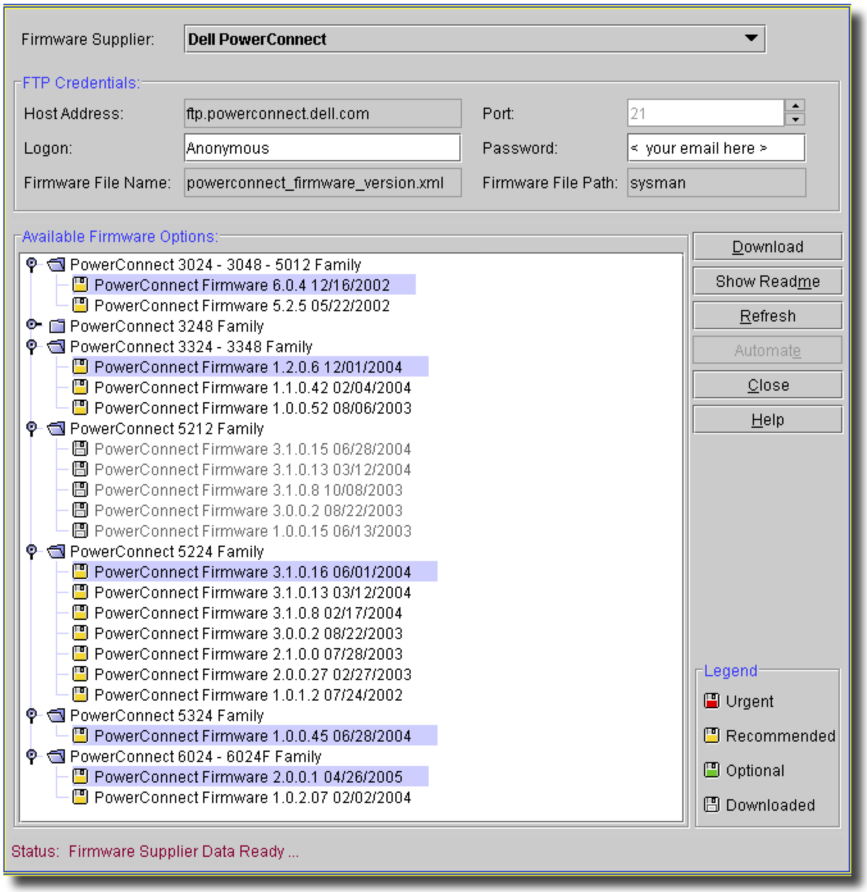
```
########################################################################

DELL POWERCONNECT 3024, 3048, 5012 v5.2.5 FIRMWARE README

########################################################################

NOTE: This ReadMe provides information for PowerConnect 3024, 3048,
and 5012 v5.2.5 firmware.

########################################################################
CRITICALITY
########################################################################

Recommended - Dell recommends applying this update during your next scheduled update
feature enhancements or changes that will help keep your system software current and c
modules (firmware, BIOS, drivers and software).

########################################################################
FIXES/ENHANCEMENTS
########################################################################

Features

- Shortened the IGMP leave group delay time to 6 seconds
(from 270 seconds).
```

To close this panel navigate away from this tab.

Download

The download screen opens to let you pick from available firmware to download to the configured devices.

Figure 37-4. File Management Download



Firmware Supplier: Dell PowerConnect

FTP Credentials:

Host Address: ftp.powerconnect.dell.com

Port: 21

Logon: Anonymous

Password: < your email here >

Firmware File Name: powerconnect_firmware_version.xml

Firmware File Path: sysman

Available Firmware Options:

- PowerConnect 3024 - 3048 - 5012 Family
  - PowerConnect Firmware 6.0.4 12/16/2002
  - PowerConnect Firmware 5.2.5 05/22/2002
- PowerConnect 3248 Family
- PowerConnect 3324 - 3348 Family
  - PowerConnect Firmware 1.2.0.6 12/01/2004
  - PowerConnect Firmware 1.1.0.42 02/04/2004
  - PowerConnect Firmware 1.0.0.52 08/06/2003
- PowerConnect 5212 Family
  - PowerConnect Firmware 3.1.0.15 06/28/2004
  - PowerConnect Firmware 3.1.0.13 03/12/2004
  - PowerConnect Firmware 3.1.0.8 10/08/2003
  - PowerConnect Firmware 3.0.0.2 08/22/2003
  - PowerConnect Firmware 1.0.0.15 06/13/2003
- PowerConnect 5224 Family
  - PowerConnect Firmware 3.1.0.16 06/01/2004
  - PowerConnect Firmware 3.1.0.13 03/12/2004
  - PowerConnect Firmware 3.1.0.8 02/17/2004
  - PowerConnect Firmware 3.0.0.2 08/22/2003
  - PowerConnect Firmware 2.1.0.0 07/28/2003
  - PowerConnect Firmware 2.0.0.27 02/27/2003
  - PowerConnect Firmware 1.0.1.2 07/24/2002
- PowerConnect 5324 Family
  - PowerConnect Firmware 1.0.0.45 06/28/2004
- PowerConnect 6024 - 6024F Family
  - PowerConnect Firmware 2.0.0.1 04/26/2005
  - PowerConnect Firmware 1.0.2.07 02/02/2004

Status: Firmware Supplier Data Ready ...

This screen has the following fields and buttons:

- **Firmware Supplier**—Select from the pick list. Subsequent portions of the screen reflect the selected vendor. You can only configure one vendor's download (or scheduled download) at a time.

  Some Dell devices require an update to boot code before you can upgrade other firmware. This application automates updating that boot code when you download and deploy the firmware upgrade.

CAUTION:

Best practice is to back up your configuration before any upgrade. Downgrades (reverting to a previous firmware or boot code) can cause configuration incompatibilities.

FTP Credentials

This section lists the *IP address*, *Port*, *Logon*, and *Password* of the equipment vendor's FTP server. It also shows the *Firmware File Name* and *Path* to the configuration file that provides information about available firmware updates. These values are read-only (except *Logon*, *Port* and *Password*) and are seeded with supporting device drivers' installation.

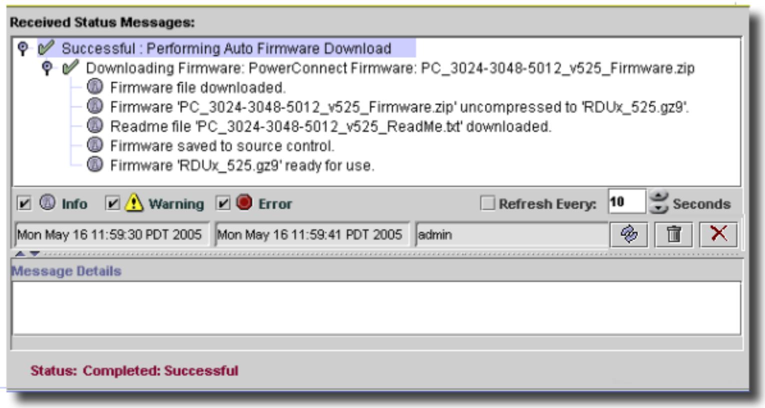
Available Firmware Options

This panel lists firmware options. Options for discovered devices appear as nodes under the tree. If you have installed the device driver that supports this feature, but discovered no equipment that supports it, the tree remains packed, concealing its sub-nodes. Click options to select them. Ctrl+click to select multiple items.

The following buttons also appear on this screen:

- **Download**—Download the selected equipment's latest firmware updates from the equipment vendor (with the FTP Credentials' port and password) immediately. The status screen opens to track the download

Figure 37-5. Download Status.



Received Status Messages:

✓ Successful : Performing Auto Firmware Download
✓ Downloading Firmware: PowerConnect Firmware: PC_3024-3048-5012_v525_Firmware.zip
Firmware file downloaded.
Firmware 'PC_3024-3048-5012_v525_Firmware.zip' uncompressed to 'RDUx_525.gz9'.
Readme file 'PC_3024-3048-5012_v525_ReadMe.txt' downloaded.
Firmware saved to source control.
Firmware 'RDUx_525.gz9' ready for use.

☑ Info ☑ Warning ☑ Error □ Refresh Every: 10 Seconds

Mon May 16 11:59:30 PDT 2005 Mon May 16 11:59:41 PDT 2005 admin

Message Details

Status: Completed: Successful

- **Show Readme**—This displays the Readme file associated with the selected operating system or firmware. This is like the Readme Tab on page 884.
- **Refresh**—Re-query for the latest information for this screen.
- **Automate** —Use the application's scheduler to automate the scan for and/or download of the most recent firmware from the equipment vendor.
- **Close**—Close this screen.
- **Help**—Open help for this screen.

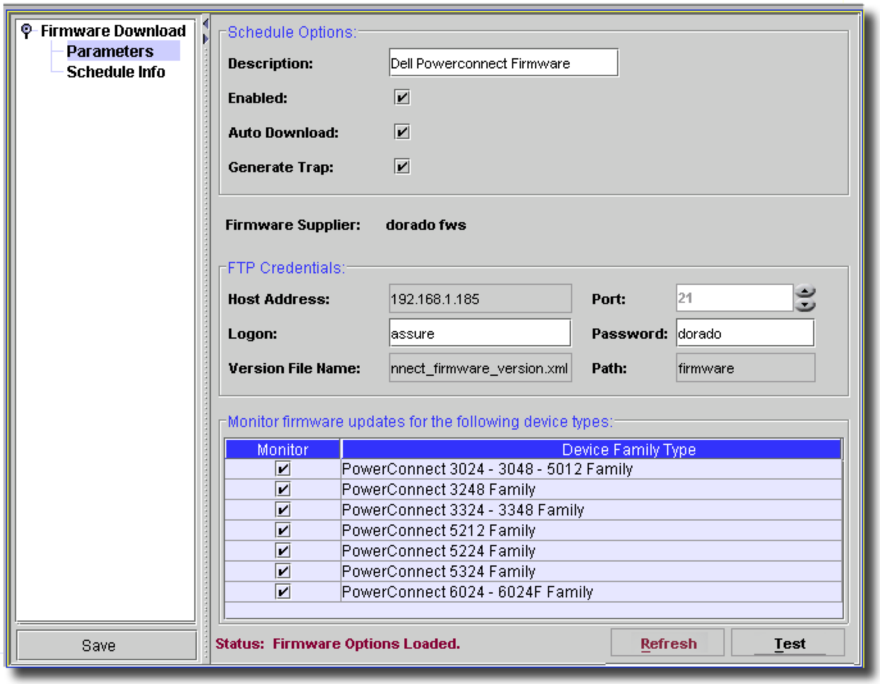
FTP Download Limitations with Two NICs

If you install OpenManage Network Manager on a dual-home server or later add a second NIC to the server, the NIC you select during installation provides access to the only network OpenManage Network Manager sees. The other NIC and its network is not be accessible to OpenManage Network Manager. This is particularly important if you are attempting to use the Firmware Download Manager in OS Images and the other NIC is your only access to the internet. In that case you must find or create a different path to the internet outside of the OpenManage Network Manager server itself.

Scheduling Downloads

When you elect to schedule a download, in addition to the standard scheduler screen, this one appears.

Figure 37-6. Download Schedule Parameters



Schedule Options:

Description: Dell Powerconnect Firmware

Enabled: ☑

Auto Download: ☑

Generate Trap: ☑

Firmware Supplier: dorado fws

FTP Credentials:

Host Address: 192.168.1.185

Port: 21

Logon: assure

Password: dorado

Version File Name: nnect_firmware_version.xml

Path: firmware

Monitor firmware updates for the following device types:

Monitor	Device Family Type
☑	PowerConnect 3024 - 3048 - 5012 Family
☑	PowerConnect 3248 Family
☑	PowerConnect 3324 - 3348 Family
☑	PowerConnect 5212 Family
☑	PowerConnect 5224 Family
☑	PowerConnect 5324 Family
☑	PowerConnect 6024 - 6024F Family

Status: Firmware Options Loaded.

This screen has the following fields:

Schedule Options

- **Description**—A text description of the scheduled download action.

- **Enabled**—Check to enable scheduled downloading or scanning for firmware updates.

- **Auto Download**—Check to enable. This automatically downloads the firmware.
- **Generate Trap**—Check to enable a trap generated when an updated download is available. You can configure the application's reaction to this trap by correlating it with an action. See the online help about *Actions* for more information.
- **Firmware Supplier**—A read-only field listing the equipment vendor who supplies firmware updates.

FTP Credentials

These are seeded with supporting device drivers:

Host Address / Port—The address and port of the FTP server.

Logon/ Password—The logon/password for this server.

Version File Name / Path—The name and path for the firmware file.

Monitor firmware updates for the following device types

This lists the firmware device types that accept firmware updates as configured here. Automating firmware updates means that, on the selected schedule, this application scans for new firmware in the file/path configured, and downloads them, if they are updated. Check *Monitor* to activate monitoring for the selected *Device Family Type*.

Click *Refresh* to update this screen's information about available firmware. Click *Test* to test connectivity to the device, and *Save* to preserve this schedule.

38

Configuration Labels

Introducing Configuration Labels

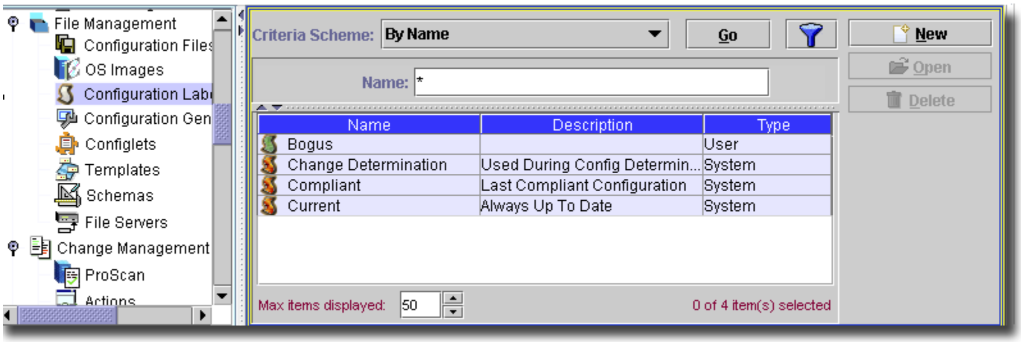
Labels let you describe actions, and dynamically collect backed up configuration files for File Management. If you wanted to do a group operation like a global restoration (in case of a catastrophic system failure), the easiest way would be to restore all configuration files in the *Current* label. You can manually execute (or schedule) group operations to restore a limited number of devices based on labels too.

The last backup for a device always updates into the *Current* Label, which, as a consequence, refers to all the most recent backups done. A Restore also updates the *Current* Label to point to the Restored Version. Using NetRestore, you can also compare a backup to a labelled configuration file. With configured *Actions*, you can also trigger application actions (e-mail, a restoration) based on that comparison.

If a Label does not contain an item for any device in a group, then a warning/info audit/job message appears telling why the selected operation does not occur for that device. Otherwise, messages appear in the audit trail tracking the status of the operation (see Audit on page 894).Configuration Labels

This is the screen where you can start to manage and create labels.

Figure 38-1. Configuration Labels



Criteria Scheme: By Name

Name: *

Name	Description	Type
Bogus		User
Change Determination	Used During Config Determin...	System
Compliant	Last Compliant Configuration	System
Current	Always Up To Date	System

Max items displayed: 50

0 of 4 item(s) selected

As in most managers, you can change the appearance the list of label with the fields and buttons at the very top of this screen.

The configuration labels screen has the following buttons:

- **New**—Opens the Label Editor, through which you can define a new label. See Creating or Modifying a Label on page 893 for more information about the Label Editor.
- **Open**—Opens the selected Label for modification. See Creating or Modifying a Label on page 893 for more information.
- **Delete**—Deletes the selected label. Select the label to remove and click *Delete*. The application prompts you for confirmation.

System Labels

Labels appearing here are either *System* labels, which you cannot alter, or *User* labels that you can create and edit. *System* labels have a red icon, *User* labels a green icon. *System* labels can include *Current*, and (if you have Change Manager installed) *Compliant* and *Change Determination*.

Change Determination and Compliant Labels

The *Change Determination* system label keeps a Label Item (pointer to a configuration file/version for a single device) for each device that been through Change Determination. For example: Three devices have been through Change Determination. The Change Determination Label then contains three Label Items, each pointing to a single Config File/Version for those devices.

The application does the following for each device in the Change Determination Process:

1. Retrieve configuration file indicated by the Change Determination Label (if any).
2. Retrieve configuration file indicated by the Current Label (which should be the same as the device in the network).
3. Compare these two files.
4. Write Old and New changes to History Records that will be used during Change Reporting.
5. Move Change Determination Label for this device to the configuration file pointed to by the Current Label.

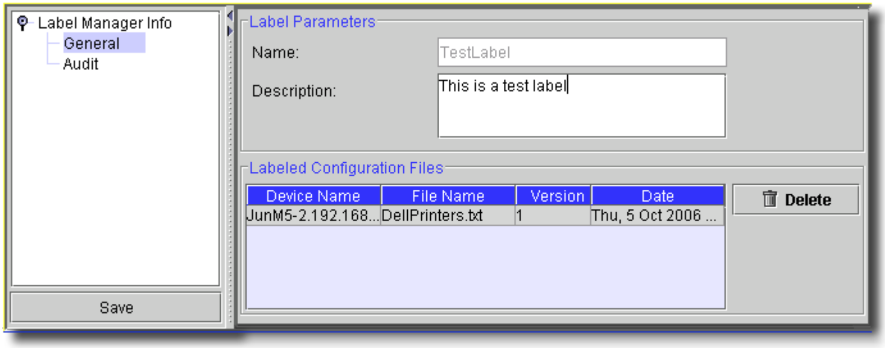
If the Change Determination Label points to no configuration file for this device, it must be the very first time this device is processed by the Change Determination Process: It creates a Change Determination Label Item for this Device.

The compliant label contains a pointer to the last configuration file that was compliant for each device that has been through ProScan. If a device fails ProScan, you can automatically restore the last compliant configuration file, indicated by the compliant label.

Creating or Modifying a Label

This editor lets you create a new label, or modify parts of an existing one.

Figure 38-2. Label Editor (General)



Name: TestLabel

Description: This is a test label

Device Name	File Name	Version	Date
JunM5-2.192.168...	DellPrinters.txt	1	Thu, 5 Oct 2006 ...

This editor has the following tabs and fields:

General

This tab has the following fields:

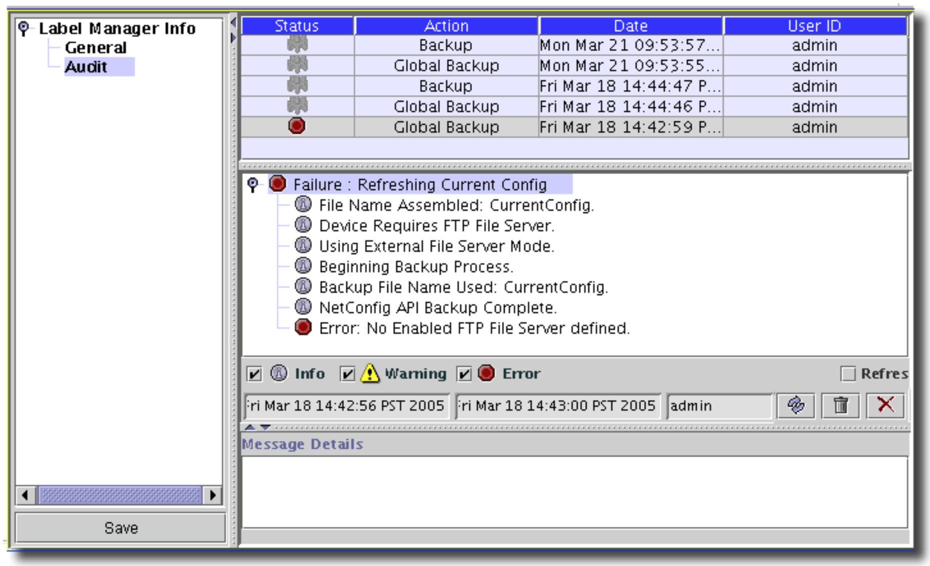
- **Name**—A unique identifier for this label.

- **Description**—A text description of this label that appears in the Configuration labels list.

Audit

This screen displays the jobs that involve this label.

Figure 38-3. Label Editor (Audit)



- Label Manager Info
  - General
  - Audit

Status	Action	Date	User ID
	Backup	Mon Mar 21 09:53:57...	admin
	Global Backup	Mon Mar 21 09:53:55...	admin
	Backup	Fri Mar 18 14:44:47 P...	admin
	Global Backup	Fri Mar 18 14:44:46 P...	admin
●	Global Backup	Fri Mar 18 14:42:59 P...	admin

- ● Failure : Refreshing Current Config
  - File Name Assembled: CurrentConfig.
  - Device Requires FTP File Server.
  - Using External File Server Mode.
  - Beginning Backup Process.
  - Backup File Name Used: CurrentConfig.
  - NetConfig API Backup Complete.
  - ● Error: No Enabled FTP File Server defined.

☑ Info ☑ Warning ☑ Error □ Refres

ri Mar 18 14:42:56 PST 2005 | ri Mar 18 14:43:00 PST 2005 | admin

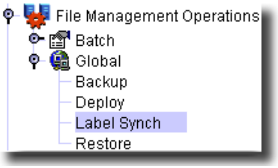
Jobs involving the label appear at the top of the screen. Select one to see the individual messages in the middle of the screen. Message details appear at the bottom of the screen.

Click *Save* to preserve your label definition, or *Close* (on the tool bar) to abandon it.

Label Group Operations

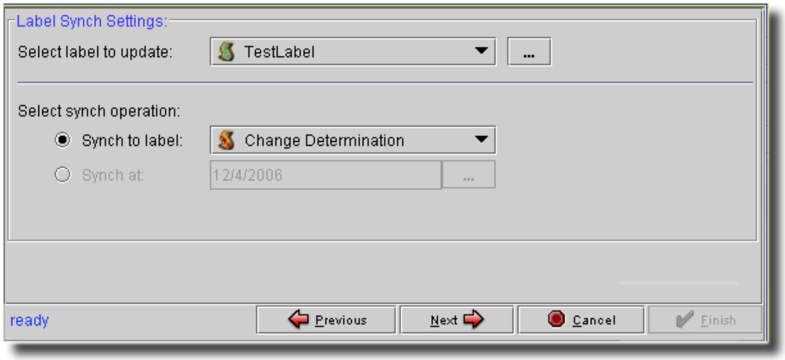
You can update labels for groups of equipment with a File Management Group Operations. From the Group Operations Manager, select the equipment group, name the group operation, and select *Label Synch* as the type of group operation.

Figure 38-4. Selecting Label Synch



Click *Next*, and the *Label Synch Settings* screen appears.

Figure 38-5. Label Synch Settings



Label Synch Settings:

Select label to update: TestLabel

Select synch operation:

● Synch to label: Change Determination

○ Synch at: 12/4/2006

In this screen, you can configure the following:

- **Select label to update**—This presents a pick list of available labels to synchronize. Notice that no System labels are available in this list. You can also use the command button (...) to open the Configuration Labels, where you can make a new label.
- **Select synch operation**—Either select a label to provide the source for updating, or a date. If you select the *Current* label, for example, the group operation makes the *label to update* point to the most recent configuration file. If you select a date, the configuration file closest to that date is what the *label to update* signifies.

Continue the group operation by clicking *Next*, selecting the appropriate items on subsequent screens.

A

Database Sizing

Introducing Database Sizing

This appendix suggests sizing solutions, but any final sizing decisions must realistically be guided by business managers working with DBAs to weigh data storage requirements versus costs.

NOTE:

A typical recommendation is to size your database 20% larger than the expected data.

You can store roughly 0.5 million traps per 1G of disk space. Performance typically does not suffer if you oversize. Twenty gigabytes of storage is typical.

Database Aging Policy

This application includes a Database Aging Policy (DAP) Manager, which lets you set up policies that control the length of time that data persists in the database. Best practice is to set up DAPs for records that are continually persisted. Several aging policies come with the application. You can edit them to suit your needs, too. Consult the *User Guide* for information about how to do this. See Chapter 7, Database Management for more information about database backup.

Autoextend

The embedded MySQL database lets you define an initial size and an autoextend ceiling. This ceiling is a hard coded value in the MySQL config file. To change this, define the following in the `my.ini/my.cnf` files at creation time:

```
[Installation root]/oware3rd/mysql/ibdata/
ibdata1:1024M:autoextend:max:2048M
```

What this says is to create a 1G data file at initiation and allow it to grow to a maximum of 2G, as needed. Once 2G is reached the server will start issuing errors (number 1114) for each insert attempted. If this occurs, you must add another data file to the system and revise Database Aging Policies accordingly.

The installer also lets you choose these MySQL values, defaulting to 1024M for initial and 8096M for the ceiling.

One example system would add a data file to the database to account for alarm/event history data:

```
[Installation root\/oware3rd/mysql/ibdata/ibdata1:2048M;c:/dorado/
oware3rd/mysql/ibdata/ibdata2:2048M:autoextend:max:2048M
```

The autoextend property can only be found in the last data file specified. YOu must specify the size to which the first file grew when adding the second data file. See MySQL's documentation on the addition or removal of innoDB data files to determine the syntax. It is located at *dev.mysql.com/doc/refman/4.1/en/adding-and-removing.html*

The process essentially follows these steps:

1 Shutdown the application

2 Shutdown MySQL

3 Modify `my.ini/my.cnf`

4 Restart MySQL

5 Restart the application

If you store more historical data online (in your database) you must size it accordingly. This avoids databases filling before you are ready to manage the system.

B

SNMP MIBs

SNMP MIB Locations

Locations of this application’s MIB Files, are as follows:

Ocp	Location	File Name	Description
redcell.ocp	owareapps/Redcell/mibs	DoradoSoftware-MIB	Base MIB for all other MIBs. Contains the enterprise MIB registration.
eventmgmt.ocp	owareapps/assure/mibs	AssureAlarms-MIB	Contains SNMP Notifications encompassing Oware, OpenManage Network Manager and Event Management ocp functionality.
netrestore.ocp	owareapps/netrestore/mibs	RedCellNetConfig-MIB	Contains SNMP Notification definitions for the Netrestore product. Currently contains notifications (traps) for backup, restore and deploy failures.

NOTE:

The location of MIB files is subject to change without notice.

Glossary

ACCESS CONTROL — Refers to mechanisms and policies that restrict access to computer resources. An access control list (ACL), for example, specifies what operations different users can perform on specific files and directories.

ALARM — A signal alerting the user to an error or fault. Alarms are produced by events. Alarms produce a message within the Alarm Window.

API — Application Programing Interface—A set of routines used by the application to direct the performance of procedures by the computer's operating system.

AUTHENTICATION — The process of determining the identity of a user that is attempting to access a network. Authentication occurs through challenge/response, time-based code sequences or other techniques. See CHAP and PAP.

AUTHORIZATION — The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.

COS — Class of Service—Describes the level of service provided to a user. Also provides a way of managing traffic in a network by grouping similar types of traffic.

DATABASE — An organized collection of Oware objects.

DEPLOYMENT — The distribution of solution blades throughout the domain.

DIGITAL CERTIFICATE — A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

DOMAIN — A goal-oriented environment that can include an industry, company, or department. You can use Oware to create solutions within your particular domain.

ENCRYPTION — Scrambling data in such a way that it can only be unscrambled through the application of the correct cryptographic key.

EQUIPMENT — A network device managed by the system.

ETHERNET TRUNK — An Ethernet Trunk service represents a point-to-point connection between two ports of two devices. Ethernet frames transported by the connection are encapsulated according to IEEE 802.1Q protocol. The each tag ID value in 802.1Q encapsulated Ethernet frames distinguishes an Ethernet traffic flow. Thus, an Ethernet trunk can aggregate multiple Ethernet VLANs through a same connection which is why "trunk" describes these.

ETHERNET TRUNK PORT — An Ethernet trunk port is a port that terminates a point-to-point Ethernet trunk. Since Ethernet trunk is a point-to-point connection, each Ethernet trunk contains two Ethernet trunk ports.

ETHERNET SERVICE — An Ethernet service represents a virtual layer broadcast domain that transports or transmits Ethernet traffic entering from any one endpoint to all other endpoints.

Often, this is a VLAN service across multiple devices.

An Ethernet service may or may not use Ethernet trunk, depending on the desired connection between two neighboring devices. If the connection is exclusively used for this Ethernet service, no Ethernet trunk is needed. On the other hand, if the connection is configured as an aggregation which can be shared by multiple Ethernet services, an Ethernet trunk models such a configuration.

Each Ethernet service can have multiple Ethernet Access Ports through which Ethernet traffic flows get access to the service.

ETHERNET ACCESS SERVICE — Since an Ethernet trunk can be shared by multiple Ethernet Services, each Ethernet Service relates to a shared trunk via a unique Ethernet Access component.

Because Ethernet trunk is a point-to-point connection, there are two Ethernet Access Services per trunk per Ethernet service instance.

ETHERNET ACCESS POINT — These represent the access points through which Ethernet frames flow in and out of an Ethernet service.

For an Ethernet Service that uses an Ethernet Trunk Service, an Ethernet Access Port must be associated with either one of the two Ethernet Access Services.

EVENT — Notification received from the NMS (Network Management System). Notifications may originate from the traps of network devices or may indicate an occurrence such as the closing of a form. Events have the potential of becoming alarms.

EVENT DEFINITION — Parameters that define what an event does. For example, you can tell Oware that the event should be to wait for incoming data from a remote database, then have the Oware application perform a certain action after it receives the data.

EVENT INSTANCE — A notification sent between two Oware components. An event instance is the action the event performs per the event definition.

EVENT TEMPLATE — Defines how an event is going to be handled.

EVENT THRESHOLD — Number of events within a given tomfooleries that must occur before an alarm is raised.

EXPORTING — Saving business objects, packages, or solution blades to a file for others to import.

FILTER — In network security, a filter is a program or section of code that is designed to examine each input or output request for certain qualifying criteria and then process or forward it accordingly.

GUI — Graphical User Interface

ISATAP — The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is an IPv6 transition mechanism which is defined as a tunneling IPv6 interface and is meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network.

KEY — In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.

KEY MANAGEMENT — The establishment and enforcement of message encryption and authentication procedures, in order to provide privacy-enhanced mail (PEM) services for electronic mail transfer over the Internet.

MANAGED OBJECT — A network device managed by the system.

MEDIATION — Communication between this application and external systems or devices, for example, printers. Mediation services let this application treat these devices as objects.

MEDIATION AGENT — Any communication to and from equipment is handled by the Mediation Agent. This communication includes SNMP requests, ASCII requests, and unsolicited ASCII messages. In addition, the Mediation Agent receives and translates emitted SNMP traps and converts them into events.

MEG — Maintenance Entity Group

MEP — Maintenance End Point

MIB — Management Information Base. A database (repository) of equipment containing object characteristics and parameters that can be monitored by the network management system.

OAM — Operation, Administration and Maintenance

OID — Object ID.

OSPF — Open Shortest Path First routing protocol.

POLICY — A rule made up of conditions and actions and associated with a profile. Policy objects contain business rules for performing configuration changes in the network for controlling Quality of Service and Access to network resources. Policy can be extended to perform other configuration functions, including routing behavior, VLAN membership, and VPN security.

POLICY ENFORCEMENT POINTS (PEP) — In a policy enforced network, a policy enforcement point represents a security appliance used to protect one or more endpoints. PEPs are also points for monitoring the health and status of a network. PEPs are generally members of a policy group.

POLICY ROUTING — Routing scheme that forwards packets to specific interfaces based on user-configured policies. Such policies might specify that traffic sent from a particular network should be routed through interface, while all other traffic should be routed through another interface.

POLICY RULES — In a policy enforced network (PEN), policy rules determine how the members and endpoint groups of a policy group communicate.

PPTP (POINT-TO-POINT TUNNELING PROTOCOL) — Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public networks, such as the Internet.

Private Key — In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a private key.

Profile — A profile is an abstract collection of configuration data that is utilized as a template to specify configuration parameters to be applied to a device as a result of a policy condition being true.

Public Key — A public key is a value provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures. The use of combined public and private keys is known as asymmetric encryption. A system for using public keys is called a public key infrastructure (PKI).

QoS — Quality of Service. In digital circuits, it is a measure of specific error conditions as compared with a standard. The establishment of QoS levels means that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. Often related to Class of Service (CoS).

RADIUS — RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

RIP — Routing Information Protocol

Self-signed Certificate

A self-signed certificate uses its own certificate request as a signature rather than the signature of a CA. A self-signed certificate will not provide the same functionality as a CA-signed certificate. A self-signed certificate will not be automatically recognized by users' browsers, and a self-signed certificate does not provide any guarantee concerning the identity of the organization that is providing the website.

SMTP — Simple Mail Transfer Protocol.

SNMP — Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides the means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Spanning Tree Protocol (STP) — The inactivation of links between networks so that information packets are channeled along one route and will not search endlessly for a destination.

SSH (Secure Shell) — A protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted connection between an SSH client and an SSH server.

SSL (Secure Sockets Layer) — A program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application (such as your Web browser or HTTP) and the Internet's TCP/IP layers. The “sockets” part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer.

TRAP (SNMP TRAP) — A notification from a network element or device of its status, such as a server startup. This notification is sent by an SNMP agent to a Network Management System (NMS) where it is translated into an event by the Mediation Agent.

TRAP FORWARDING — The process of re-emitting trap events to remote hosts. Trap Forwarding is available from the application through Actions and through the Resource Manager.

VLAN — A virtual local area network (LAN), commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

Index