



---

# ExtremeWare™ EPICenter™ Software Installation and User Guide

Version 3.1

Extreme Networks, Inc.  
3585 Monroe Street  
Santa Clara, California 95051  
(888) 257-3000

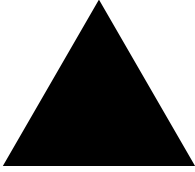
<http://www.extremenetworks.com>

Published: August, 2001  
Part number: 100081-00 Rev. 02

©2001 Extreme Networks, Inc. All rights reserved. Extreme Networks and BlackDiamond are registered trademarks of Extreme Networks, Inc. in the United States and certain other jurisdictions. EPICenter, ExtremeWare, ExtremeWare Vista, ExtremeWorks, ExtremeAssist, ExtremeAssist1, ExtremeAssist2, PartnerAssist, Extreme Standby Router Protocol, ESRP, SmartTraps, Alpine, Summit, Summit1, Summit4, Summit4/FX, Summit7i, Summit24, Summit48, Summit Virtual Chassis, SummitLink, SummitGbX, SummitRPS and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. The Extreme Turbodriven logo is a service mark of Extreme Networks, which may be registered or pending registration in certain jurisdictions. Specifications are subject to change without notice.

Solaris is a trademark of Sun Microsystems, Inc.

All other registered trademarks, trademarks and service marks are property of their respective owners.



# Contents

---

<b>Preface</b>	
<b>Introduction</b>	<b>xxiii</b>
Terminology	xxiii
<b>Conventions</b>	<b>xxiv</b>
<b>Related Publications</b>	<b>xxv</b>
<b>1 EPICenter Overview</b>	
<b>Introduction</b>	<b>1-1</b>
<b>Summary of Features</b>	<b>1-2</b>
Simple Inventory Management	1-3
The Alarm System	1-3
The Configuration Manager	1-4
Interactive Telnet Applet	1-4
The Grouping Manager	1-4
The IP/MAC Address Finder	1-5
ExtremeView Configuration and Status Monitoring	1-5
Real-Time Statistics	1-5
Topology Views	1-5
Enterprise-wide VLAN Management	1-6
The ESRP Manager	1-6
Dynamic Reports	1-6
Scalable Mode	1-7

Security Management	1-7
EPICenter Stand-alone Utilities	1-8
<b>EPICenter Components</b>	<b>1-8</b>
Extreme Networks Switch Management	1-10
<b>Extreme Networks Device Support</b>	<b>1-10</b>
<b>Third-Party Device Support</b>	<b>1-10</b>
<b>EPICenter Client Requirements</b>	<b>1-11</b>
<b>2 Installing the EPICenter Software</b>	
<b>Installation Overview</b>	<b>2-1</b>
<b>Server Requirements</b>	<b>2-2</b>
Windows NT or Windows 2000	2-2
Solaris	2-3
<b>Client Requirements</b>	<b>2-3</b>
<b>EPICenter Software Licensing</b>	<b>2-4</b>
Obtaining an Evaluation License	2-4
Obtaining a Permanent License	2-5
Upgrading an Evaluation License	2-5
Adding a License for an Optional Product	2-5
<b>Upgrading from a Previous Release</b>	<b>2-6</b>
<b>Installing on a Windows NT or Windows 2000 System</b>	<b>2-6</b>
Adding or Updating the License Key	2-10
<b>Installing on a Solaris System</b>	<b>2-10</b>
Required Patches	2-11
Local Name Resolution	2-11
Installing the EPICenter Server	2-11
Adding or Updating a License Key	2-17
<b>Installing the EPICenter Client</b>	<b>2-17</b>
<b>Uninstalling the EPICenter Server</b>	<b>2-18</b>
Uninstalling in Windows NT or Windows 2000	2-18
Uninstalling in Solaris	2-19

<b>3</b>	<b>Starting ExtremeWare EPICenter</b>	
	<b>Running the EPICenter Software under Windows</b>	<b>3-1</b>
	Starting the EPICenter Server	3-2
	Shutting Down the EPICenter Server Components	3-2
	Restarting the EPICenter Server Components as Services	3-3
	<b>Running the EPICenter Software under Solaris</b>	<b>3-3</b>
	Starting or Restarting the EPICenter Server	3-4
	Shutting Down the EPICenter Server Components	3-4
	<b>Launching the ExtremeWare EPICenter Client</b>	<b>3-4</b>
	<b>Navigating the EPICenter Applications</b>	<b>3-11</b>
	The Navigation Toolbar	3-12
	Main Applet Frame	3-14
	The Component Tree	3-16
	The Status/Detail Information Panel	3-16
	Moving the Component Tree Boundary	3-18
	Resizing and Sorting Columns	3-18
	Applet Function Buttons	3-18
	Printing from EPICenter	3-20
	<b>Running the EPICenter Server in Scalable Mode</b>	<b>3-20</b>
<b>4</b>	<b>Using the Inventory Manager</b>	
	<b>Overview of the EPICenter Device Inventory</b>	<b>4-1</b>
	Gathering Device Status Information	4-2
	<b>Displaying the Network Device Inventory</b>	<b>4-3</b>
	<b>Viewing Device Status Information</b>	<b>4-5</b>
	<b>Discovering Network Devices</b>	<b>4-8</b>
	<b>Adding Devices and Device Groups</b>	<b>4-14</b>
	Adding a Device	4-15
	Creating a Device Group	4-16
	<b>Modifying Devices and Device Groups</b>	<b>4-18</b>
	Modifying a Device	4-18
	Modifying a Device Group	4-19

<b>Deleting Devices and Device Groups from the Database</b>	<b>4-21</b>
Deleting a Device	4-21
Deleting a Device Group	4-23
<b>Updating Device Information</b>	<b>4-24</b>
<b>Finding Devices</b>	<b>4-25</b>
<b>5 The EPICenter Alarm System</b>	
<b>Overview of the EPICenter Alarm System</b>	<b>5-1</b>
<b>The Alarm Log Browser</b>	<b>5-2</b>
Acknowledging an Alarm	5-5
Deleting Alarms	5-5
Viewing Alarm Details	5-5
Filtering the Alarm Display	5-6
<b>Defining Alarms</b>	<b>5-8</b>
Creating New Alarm Definitions	5-10
Modifying Alarm Definitions	5-20
Deleting Alarm Definitions	5-20
<b>Alarm Categories</b>	<b>5-21</b>
Creating a New Alarm Category	5-21
Modifying an Alarm Category	5-21
Deleting an Alarm Category	5-21
<b>Event Configuration</b>	<b>5-22</b>
Creating an Event Rule	5-26
Modifying a Rule	5-35
Deleting a Rule	5-36
Resynchronizing the RMON Rules	5-37
Configuring Other SNMP Trap Events	5-38
<b>Setting EPICenter as a Trap Receiver</b>	<b>5-38</b>
<b>Writing Tcl Scripts for Alarm Actions</b>	<b>5-39</b>
The Tcl Scripting Environment	5-39

<b>6</b>	<b>Configuration Manager</b>	
	Overview of the Configuration Manager	<b>6-1</b>
	Uploading Configurations from Devices	<b>6-5</b>
	Archiving Configuration Settings	<b>6-7</b>
	Downloading Configuration Information to a Device	<b>6-8</b>
	Downloading an Incremental Configuration to Devices	<b>6-10</b>
	Creating an Incremental Configuration File	6-12
	Upgrading Device Software Images	<b>6-12</b>
	Specifying the Current Software Versions	<b>6-15</b>
	Configuring the TFTP Server	<b>6-16</b>
	Finding Devices	<b>6-18</b>
<b>7</b>	<b>Using the Interactive Telnet Application</b>	
	Overview of the Interactive Telnet Applet	<b>7-1</b>
	Using Telnet with Extreme Switches	<b>7-2</b>
	Running ExtremeWare Command Macros	7-3
	Running a Telnet Session on an Individual Switch	7-8
	Using Interactive Telnet with Third-Party Devices	<b>7-11</b>
	Finding Devices	<b>7-12</b>
<b>8</b>	<b>The Grouping Manager</b>	
	Overview of the Grouping Manager	<b>8-1</b>
	Displaying EPICenter Groups and Resources	<b>8-4</b>
	Resource Details	8-6
	Grouping Manager Functions	8-8
	Creating a New Resource	<b>8-9</b>
	Deleting Resources	<b>8-11</b>
	Adding a Resource as a Child of a Group	<b>8-12</b>
	Removing A Child Resource from a Group	<b>8-15</b>

<b>Adding Relationships to a Resource</b>	<b>8-16</b>
Removing Relationships from a Resource	8-19
<b>Adding and Removing Attributes</b>	<b>8-19</b>
<b>Searching for a Resource</b>	<b>8-23</b>
Setting up a Resource Search	8-23
Searching from the Main Toolbar	8-26
Searching from the Add Resources or Add Relationship Window	8-27
<b>Importing Resources</b>	<b>8-28</b>
Importing from an LDAP Directory	8-30
Importing from a File	8-32
Importing from an NT Domain Controller or NIS Server	8-36
<b>9 Using the IP/MAC Address Finder</b>	
<b>Overview of the IP/MAC Finder Applet</b>	<b>9-1</b>
<b>Tasks List Summary Window</b>	<b>9-2</b>
<b>Creating a Search Task</b>	<b>9-4</b>
<b>Detailed Task View</b>	<b>9-7</b>
Exporting Task Search Results to a File	9-9
<b>10 Using ExtremeView</b>	
<b>Overview of the ExtremeView Application</b>	<b>10-1</b>
<b>Viewing Device Status Information</b>	<b>10-3</b>
<b>Viewing Switch Configuration Information</b>	<b>10-8</b>
<b>Viewing Switch Statistics</b>	<b>10-10</b>
<b>Finding Devices</b>	<b>10-11</b>
<b>11 Real-Time Statistics</b>	
<b>Overview of Real-Time Statistics</b>	<b>11-1</b>
<b>Displaying Multi-port Statistics</b>	<b>11-3</b>
<b>Displaying Statistics For a Single Port</b>	<b>11-7</b>
<b>Changing the Display Mode</b>	<b>11-9</b>



	<b>Setting Graph Preferences</b>	<b>11-11</b>
	<b>Taking Graph Snapshots</b>	<b>11-14</b>
<b>12</b>	<b>Network Topology Views</b>	
	<b>Overview of EPICenter Topology Views</b>	<b>12-1</b>
	<b>Displaying a Network Topology View</b>	<b>12-2</b>
	Map Elements	12-4
	Map Element Description Panel	12-8
	<b>Manipulating Map Views</b>	<b>12-9</b>
	Creating a New View or a New Map	12-9
	Adding Elements to the Map	12-11
	Editing the Map	12-15
	Map Viewing Functions	12-19
	<b>Device Information Views</b>	<b>12-26</b>
	Device Alarms	12-26
	Device Browse	12-26
	Device Statistics	12-27
	Device Telnet	12-27
	Device View	12-27
<b>13</b>	<b>Using the VLAN Manager</b>	
	<b>Overview of Virtual LANs</b>	<b>13-1</b>
	<b>Displaying a VLAN</b>	<b>13-2</b>
	<b>Adding a VLAN</b>	<b>13-6</b>
	<b>Deleting a VLAN</b>	<b>13-9</b>
	<b>Modifying a VLAN</b>	<b>13-10</b>
	<b>Adding and Deleting Protocol Filters</b>	<b>13-13</b>
<b>14</b>	<b>The ESRP Manager</b>	
	<b>Overview of the ESRP Manager</b>	<b>14-1</b>
	<b>Viewing ESRP Detail Information</b>	<b>14-3</b>

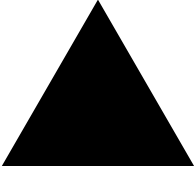
<b>15</b>	<b>Administering EPICenter</b>	
	<b>Overview of User Administration</b>	<b>15-1</b>
	Controlling EPICenter Access	15-2
	The EPICenter RADIUS Server	15-3
	Setting EPICenter Server Properties	15-3
	<b>Starting the EPICenter Client for the First Time</b>	<b>15-3</b>
	Changing the Admin Password	15-5
	<b>Adding or Modifying User Accounts</b>	<b>15-6</b>
	<b>Deleting Users</b>	<b>15-7</b>
	<b>Changing Your Own User Password</b>	<b>15-8</b>
	<b>RADIUS Administration</b>	<b>15-10</b>
	<b>Server Properties Administration</b>	<b>15-12</b>
	Devices Properties	15-13
	Scalability Properties	15-14
	SNMP Properties	15-14
	Topology Properties	15-15
	Other Properties	15-15
<b>16</b>	<b>Dynamic Reports</b>	
	<b>Overview of EPICenter Reports</b>	<b>16-1</b>
	<b>Network Summary Report</b>	<b>16-2</b>
	Devices Managed by the Server	16-4
	Devices Not Responding	16-5
	Critical Alarms Defined	16-6
	Critical Alarms for Last 24 Hours	16-6
	Unacknowledged Critical Alarms	16-6
	SNMP Unreachable Alarms	16-7
	Invalid Login Alarms	16-7
	Authentication Failure Alarms	16-8
	VLANs Report	16-9

<b>Dynamic Reports</b>	<b>16-9</b>
<b>Viewing Predefined EPICenter Reports</b>	<b>16-10</b>
Report Filtering	16-10
Server State Summary Report	16-12
Device Inventory Report	16-13
Device Status Report	16-14
VLAN Summary Report	16-15
Interface Report	16-15
Resource to Attribute Mapping Report	16-16
User to Host Mapping Report	16-17
Alarm Log Report	16-17
Event Log Report	16-19
Configuration Management Log Report	16-20
<b>Printing EPICenter Reports</b>	<b>16-20</b>
<b>Creating New Reports</b>	<b>16-21</b>
Creating or Modifying a Report	16-22
Adding a User-Defined Report to the Reports Menu	16-24
Debugging	16-24
<b>A Troubleshooting</b>	
<b>Troubleshooting Aids</b>	<b>A-1</b>
<b>EPICenter Client Initialization</b>	<b>A-2</b>
<b>EPICenter Server Issues</b>	<b>A-4</b>
<b>VLAN Manager</b>	<b>A-6</b>
<b>Alarm System</b>	<b>A-7</b>
<b>ESRP Manager</b>	<b>A-9</b>
<b>Inventory Manager</b>	<b>A-9</b>
<b>ExtremeView</b>	<b>A-11</b>
<b>Grouping Manager</b>	<b>A-12</b>
<b>Printing</b>	<b>A-12</b>
<b>Topology</b>	<b>A-13</b>

<b>B</b>	<b>EPICenter Utilities</b>	
	<b>The DevCLI Utility</b>	<b>B-1</b>
	Using the DevCLI Commands	B-2
	DevCLI Examples	B-3
	<b>Inventory Export Scripts</b>	<b>B-4</b>
	Using the Inventory Export Scripts	B-4
	Inventory Export Examples	B-6
	<b>The SNMPCLI Utility</b>	<b>B-7</b>
	Using the SNMPCLI Utility	B-7
	SNMPCLI Examples	B-8
	<b>Port Configuration Utility</b>	<b>B-9</b>
<b>C</b>	<b>EPICenter Database Views</b>	
	<b>Device Report View</b>	<b>C-1</b>
	<b>Interface Report View</b>	<b>C-4</b>
	<b>Database Event Log View</b>	<b>C-5</b>
	<b>Database Alarm Log View</b>	<b>C-7</b>
<b>D</b>	<b>Event Types for Alarms</b>	
	<b>SNMP Trap Events</b>	<b>D-1</b>
	<b>RMON Rising Trap Events</b>	<b>D-6</b>
	<b>RMON Falling Trap Events</b>	<b>D-6</b>
	<b>EPICenter Events</b>	<b>D-6</b>
<b>E</b>	<b>EPICenter Backup</b>	
	<b>EPICenter Log Backups</b>	<b>E-1</b>
	<b>Database Utilities</b>	<b>E-2</b>
	<b>The Validation Utility</b>	<b>E-2</b>
	Using the DBVALID Command-line Utility	E-3
	Database Connection Parameters	E-4

<b>The Backup Utility</b>	<b>E-4</b>
The DBBACKUP Command-line Utility	E-4
Database Connection Parameters	E-5
Installing a Backup Database	E-6

## **Index**



# Figures

---

<b>1-1</b>	ExtremeWare EPICenter software architecture	1-9
<b>3-1</b>	EPICenter start-up page	3-5
<b>3-2</b>	ExtremeWare EPICenter login page	3-7
<b>3-3</b>	Java Plug-inSecurity Warning	3-8
<b>3-4</b>	The Network Summary Report page	3-9
<b>3-5</b>	The About EPICenter page	3-11
<b>3-6</b>	The EPICenter Home page	3-12
<b>3-7</b>	VLAN Manager applet running in a browser window	3-15
<b>3-8</b>	Inventory Manager applet	3-17
<b>3-9</b>	Pop-up dialog box for adding a VLAN in the VLAN Manager	3-19
<b>4-1</b>	The Inventory Manager applet, main page	4-4
<b>4-2</b>	Inventory Manager device group summary status	4-6
<b>4-3</b>	Inventory Manager device status information	4-7
<b>4-4</b>	Inventory Manager information for a 3Com device	4-8
<b>4-5</b>	Inventory Manager Device Discovery set up window	4-9
<b>4-6</b>	Results of a discovery, with details visible	4-11
<b>4-7</b>	Setting default device options for discovered devices	4-12
<b>4-8</b>	Message window showing Add Device progress	4-13
<b>4-9</b>	Message window showing errors from the Add Device process	4-14
<b>4-10</b>	Add Device window in the Inventory Manager	4-15
<b>4-11</b>	Add Device Group window in the Inventory Manager	4-17
<b>4-12</b>	Devices tab of the Modify Devices and Device Groups window	4-18
<b>4-13</b>	Device Groups tab of the Modify Devices and Device Groups window	4-20

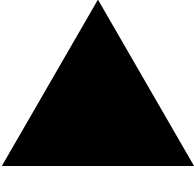
<b>4-14</b>	Devices tab of the Delete Devices and Device Groups window	4-22
<b>4-15</b>	Device Groups tab of the Delete Devices and Device Groups window	4-23
<b>4-16</b>	Synchronize Devices dialog	4-24
<b>4-17</b>	Find Devices dialog	4-26
<b>5-1</b>	The Alarm Log Browser page	5-3
<b>5-2</b>	Detailed view of an Alarm Log entry	5-6
<b>5-3</b>	Alarm Log filter definition pop-up window	5-7
<b>5-4</b>	Alarm System: Alarm Definition page	5-9
<b>5-5</b>	The New Alarm Definition window, Basic definition	5-10
<b>5-6</b>	The New Alarm Definition window, Scope definition	5-14
<b>5-7</b>	The New Alarm Definition window, Action definition	5-16
<b>5-8</b>	Setting up E-mail for EPICenter alarm actions	5-18
<b>5-9</b>	The event Configuration window showing RMON rules	5-23
<b>5-10</b>	The event Configuration window showing CPU Configuration rules	5-25
<b>5-11</b>	New Configuration window	5-26
<b>5-12</b>	A list of MIB variables available for use in RMON rules	5-27
<b>5-13</b>	RMON Alarm event generation	5-30
<b>5-14</b>	CPU Utilization event generation	5-32
<b>5-15</b>	RMON target selection window	5-33
<b>5-16</b>	Modify Configuration window	5-36
<b>5-17</b>	The Synchronize RMON Rules window	5-37
<b>6-1</b>	Configuration Manager showing summary device status	6-2
<b>6-2</b>	Configuration and Software status for an individual device	6-4
<b>6-3</b>	The Upload Config window	6-5
<b>6-4</b>	Schedule Upload Config window	6-7
<b>6-5</b>	Download configuration window	6-9
<b>6-6</b>	Download incremental configuration window	6-11
<b>6-7</b>	Upgrade Image on Devices window	6-13
<b>6-8</b>	Configure New Image window	6-16
<b>6-9</b>	Configure TFTP Server window	6-17
<b>6-10</b>	Find Devices dialog	6-18
<b>7-1</b>	The Telnet applet, macro interface	7-2
<b>7-2</b>	The Telnet record and play buffer	7-4
<b>7-3</b>	Saving a macro to the database	7-7
<b>7-4</b>	Loading a macro from the database	7-7

<b>7-5</b>	A newly-opened Telnet session	7-9
<b>7-6</b>	An open Telnet session showing the pop-up edit menu	7-10
<b>7-7</b>	Find Devices dialog	7-12
<b>8-1</b>	Resource Details view	8-5
<b>8-2</b>	Adding a new resource	8-9
<b>8-3</b>	Adding Resources to a Group	8-13
<b>8-4</b>	Adding Relationships to a Resource	8-17
<b>8-5</b>	Resource attribute display	8-21
<b>8-6</b>	Adding attributes to a resource	8-22
<b>8-7</b>	Searching for a resource	8-24
<b>8-8</b>	Importing resources	8-29
<b>8-9</b>	Monitoring the progress of an Import function	8-30
<b>9-1</b>	IP/MAC Address Finder main page	9-2
<b>9-2</b>	Tasks List summary	9-3
<b>9-3</b>	Find Addresses window	9-5
<b>9-4</b>	Search in progress	9-7
<b>9-5</b>	Address search results in the Detailed Task view	9-8
<b>10-1</b>	The ExtremeView applet, main page	10-2
<b>10-2</b>	The ExtremeView applet, Status summary	10-3
<b>10-3</b>	The ExtremeView applet, switch status	10-5
<b>10-4</b>	The ExtremeView applet, port status	10-6
<b>10-5</b>	A third-party device with unknown configuration	10-7
<b>10-6</b>	The ExtremeView applet, Configuration summary	10-8
<b>10-7</b>	The ExtremeView applet, Configuration details	10-9
<b>10-8</b>	The ExtremeView applet, Statistics summary	10-10
<b>10-9</b>	The ExtremeView applet, Statistics details	10-11
<b>10-10</b>	Find Devices dialog	10-12
<b>11-1</b>	Real-Time Statistics main page	11-4
<b>11-2</b>	Bar chart showing port statistics for a group of ports	11-5
<b>11-3</b>	Warning displayed when the EPICenter server cannot retrieve data	11-6
<b>11-4</b>	Utilization data over time for an individual port on a device	11-8
<b>11-5</b>	Individual errors in a single-port chart	11-9
<b>11-6</b>	Setting 3D graph preferences	11-12
<b>11-7</b>	Setting graph color preferences	11-13
<b>11-8</b>	Setting data color preferences	11-13
<b>11-9</b>	Setting other graph preferences	11-14
<b>11-10</b>	Snapshot of Real-Time Statistics graph display	11-15



<b>12-1</b>	The Topology View	12-3
<b>12-2</b>	Example of device nodes, including an unknown device type	12-4
<b>12-3</b>	Example of a submap node	12-5
<b>12-4</b>	Example of an L2 cloud node	12-5
<b>12-5</b>	Example of hyper node icons representing a device and an L2 cloud	12-6
<b>12-6</b>	Example of a decorative node	12-6
<b>12-7</b>	Example of a gigabit link showing endpoint connectivity and Up status	12-7
<b>12-8</b>	Adding a new map	12-11
<b>12-9</b>	Adding a decorative node to the map	12-13
<b>12-10</b>	Adding a link to your map	12-14
<b>12-11</b>	Specifying ports for a new link connection	12-15
<b>12-12</b>	Finding a node in the current view	12-23
<b>12-13</b>	Setting Map Properties for the current map	12-24
<b>13-1</b>	VLAN Manager applet, showing devices organized by VLAN	13-3
<b>13-2</b>	VLAN topology shown by switch	13-4
<b>13-3</b>	VLAN member ports on a selected switch	13-5
<b>13-4</b>	Switch member ports for a selected VLAN	13-6
<b>13-5</b>	Add VLAN dialog, Properties and Ports page	13-7
<b>13-6</b>	Add VLAN dialog, IP Forwarding page	13-9
<b>13-7</b>	The Delete VLAN page	13-10
<b>13-8</b>	The Modify VLAN dialog, Properties and Ports page	13-11
<b>13-9</b>	The Modify VLAN dialog, IP Forwarding page	13-12
<b>13-10</b>	Protocol Panel dialog box, View/Delete page	13-13
<b>13-11</b>	Protocol Panel dialog box, Add Protocol page	13-14
<b>14-1</b>	ESRP Manager showing summary ESRP-enabled VLAN status	14-2
<b>14-2</b>	ESRP detail for an individual ESRP-enabled VLAN	14-4
<b>15-1</b>	User Administration window	15-4
<b>15-2</b>	Edit User window	15-5
<b>15-3</b>	New User and Edit User windows	15-6
<b>15-4</b>	Change Password window	15-9
<b>15-5</b>	Radius Administration page	15-10
<b>15-6</b>	Server Properties Configuration page, initial properties list	15-12
<b>16-1</b>	Network Summary Report page	16-2
<b>16-2</b>	Network Summary Detail report	16-3
<b>16-3</b>	Report filter specification	16-11

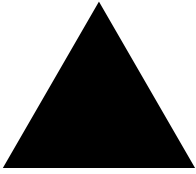
<b>16-4</b>	Device Ports filter specification	16-16
<b>16-5</b>	Attribute specification for Resource to Attribute Mapping report	16-16
<b>16-6</b>	Alarm Log filter specification	16-18
<b>16-7</b>	Event Log filter specification	16-19
<b>16-8</b>	Configuration Management Log filter specification	16-20
<b>B-1</b>	ExtremeWare EPICenter Port Configuration Utility	B-10



# Tables

---

<b>1</b>	Notice Icons	xxiv
<b>2</b>	Text Conventions	xxiv
<b>4-1</b>	Inventory Manager Device Status Indicators	4-6
<b>5-1</b>	EPICenter Alarm Variables	5-12
<b>5-2</b>	Command Restrictions in EPICenter Tcl Safe Interpreter	5-40
<b>7-1</b>	ExtremeView Macro Variables	7-5
<b>10-1</b>	ExtremeView Device Status Indicators	10-4
<b>11-1</b>	Definition of RMON Utilization Variable Used in Port Utilization Displays	11-2
<b>11-2</b>	Definition of RMON etherHistory Error Variables for Port Error Displays	11-2
<b>B-1</b>	DevCli command options	B-2
<b>B-2</b>	Inventory script command options	B-5
<b>B-3</b>	SnmpCli command options	B-8
<b>C-1</b>	EPICenter Database Device Report View	C-1
<b>C-2</b>	EPICenter Database Interface Report View	C-4
<b>C-3</b>	EPICenter Database Event Log View	C-5
<b>C-4</b>	EPICenter Database Alarm Log View	C-7
<b>D-1</b>	SNMP Trap Events	D-1
<b>D-2</b>	EPICenter Events, Detected Through Polling	D-7
<b>E-1</b>	dbvalid Command Switches	E-3
<b>E-2</b>	Database Connection Parameters for dbvalid Utility	E-4
<b>E-3</b>	dbbackup Command Switches	E-5
<b>E-4</b>	Database Connection Parameters for dbbackup Utility	E-5



# Preface

---

This Preface provides an overview of this guide, describes guide conventions, and lists other useful publications.

## Introduction

This guide provides the required information to use the ExtremeWare EPICenter software. It is intended for use by network managers who are responsible for monitoring and managing Local Area Networks, and assumes a basic working knowledge of:

- Local Area Networks (LANs)
- Ethernet concepts
- Ethernet switching and bridging concepts
- Routing concepts
- The Simple Network Management Protocol (SNMP)



*If the information in the [ExtremeWare EPICenter SE Release Note and Quick Start Guide](#) shipped with your software differs from the information in this guide, follow the Release Note.*

## Terminology




When features, functionality, or operation is specific to the Summit, Alpine, or BlackDiamond switch family, the family name is used. Explanations about features and

operations that are the same across all Extreme switch product families simply refer to the product as the “Extreme device” or “Extreme switch.” Explanations about features that are the same for all devices managed by EPICenter (both Extreme devices and others) are simply refer to “devices.”

## Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

**Table 1:** Notice Icons

Icon	Notice Type	Alerts you to...
	Note	Important features or instructions.
	Caution	Risk of unintended consequences or recoverable loss of data.
	Warning	Risk of permanent loss of data.

**Table 2:** Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen .
<b>screen displays bold</b>	This typeface indicates how you would type a particular command.
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”

**Table 2:** Text Conventions (continued)

Convention	Description
[Key] names	<p>Key names appear in text in one of two ways. They may be</p> <ul style="list-style-type: none"> <li>■ referred to by their labels, such as “the Return key” or “the Escape key.”</li> <li>■ written with brackets, such as [Return] or [Esc].</li> </ul> <p>If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). For example:</p> <p style="padding-left: 40px;">Press [Ctrl]+[Alt]+[Del].</p>
Words in <b>bold</b> type	Bold text indicates a button or field name.
Words in <i>italicized</i> type	Italics emphasize a point or denote new terms at the place where they are defined in the text.

## Related Publications

The ExtremeWare EPICenter documentation set includes the following:

- The *ExtremeWare EPICenter SE User Guide* (the manual you are reading)
- *ExtremeWare EPICenter SE Release Note and Quick Start Guide*
- ExtremeWare EPICenter License Agreement

The two manuals and the Release Note can be found online in Adobe Acrobat PDF format, in the `docs` subdirectory of the EPICenter installation directory. You must have Adobe Acrobat Reader version 3.0 or later (available from <http://www.adobe.com> free of charge).

Other manuals that you will find useful are:

- *ExtremeWare Software User Guide*
- *ExtremeWare Quick Reference Guide*

For documentation on Extreme Networks products, and for general information about Extreme Networks, see the Extreme Networks home page:

- <http://www.extremenetworks.com>

Customers with a support contract can access the Technical Support pages at:

- <http://www.extremenetworks.com/support/database.htm>

The technical support pages provide the latest information on Extreme Networks software products, including the latest Release Notes, information on known problems, downloadable updates or patches as appropriate, and other useful information and resources.

Customers without contracts can still access manuals and patches at <http://www.extremenetworks.com/support/documentation.asp>



# EPICenter Overview

---

This chapter describes:

- Features of the ExtremeWare EPICenter™ SE software.
- EPICenter software components.
- Hardware and software requirements.

## Introduction

Today's corporate networks commonly encompass hundreds or thousands of systems, including individual end user systems, servers, network devices such as printers, and internetworking systems. Extreme Networks™ recognizes that network managers have different needs, and delivers a suite of ExtremeWare™ management tools to meet those needs.

EPICenter is a powerful yet easy-to-use application suite that facilitates the management of a network of Summit™ and BlackDiamond™ switches, as well as selected third-party switches. EPICenter makes it easier to perform configuration and status monitoring, create virtual LANs (VLANs), and implement policy-based networking in enterprise LANs with Extreme Networks switches. EPICenter offers a comprehensive set of network management tools that are easy to use from a workstation configured with a web browser and the Java plug-in.

EPICenter leverages the three-tier client/server architecture framework represented by Java applets, and can be accessed using Microsoft Internet Explorer or Netscape Navigator with Sun's Java Plug-in. The EPICenter application and database support two of the most



popular operating environments in the marketplace, Microsoft Windows NT and Sun Microsystems' Solaris. Integration with HP OpenView and other third-party network management software products provides additional flexibility.

## Summary of Features

In large corporate networks, network managers need to manage systems “end to end.” The EPICenter software is a powerful, flexible and easy-to-use application for centralizing the management of a network of Extreme switches and selected third-party devices, regardless of the network size. The EPICenter software provides the vital SNMP, HTML, and CLI-based tools you need for network-wide management of Extreme Networks Summit, Black Diamond, and Alpine switches.

- **Network Control.** The EPICenter software provides configuration and monitoring of Extreme Networks' switches and selected third-party devices anywhere on the network simultaneously.
- **Intelligent Management.** Extreme SmartTraps™ (patent pending) automatically gather switch configuration changes and forward them to the EPICenter server, thereby minimizing network management traffic. EPICenter separates its request “heartbeat” polling to assess a device's connectivity from its less frequent and more data-intensive status polling.
- **Hierarchical Displays.** Most information, including that found in EPICenter topology maps, VLAN management, configuration management, and real-time statistics, is dynamically presented in an easy-to-navigate hierarchical tree.
- **Multi-platform capability.** The EPICenter Server supports both Sun SPARC/Solaris and Intel/Windows NT 4.0 or Windows 2000. Clients running in browsers on either of these platforms can connect to servers on either platform.
- **Support for multiple users with security.** Users must log in to the application, and can be granted different levels of access to the application features.
- **Web-based clients.** EPICenter clients are web-based, requiring only a web-browser and Java plug-in to be installed on client machines.
- **Manage large numbers of devices.** The EPICenter server's scalability mode lets you manage up to about 2000 devices with a single installation of the EPICenter software.

Extreme Networks switches and many other MIB-2 compatible devices can be monitored and controlled from a central web-based interface, without exiting EPICenter to run a separate program or telnet session. Features such as SmartTraps and the EPICenter alarm

system further maximize network monitoring capability while maintaining network usage efficiency.

You can organize your network resources into groups (including groups made up of selected ports from multiple switches) that you can manage as a single entity. You can set VLAN configurations across the network without having to log into switches individually. You can search for individual IP addresses and identify their connections into the network. You can monitor the status of your network devices either visually, through the ExtremeView applet, or by setting alarms that will notify you about conditions or events on your network devices. You can get a high-level overview of the status of your network devices displayed as a hierarchical topology map.

These features and more are described in more detail in the following sections, and in the remaining chapters of this manual.

## Simple Inventory Management

EPICenter's Inventory Manager applet keeps a database of all the devices managed by the EPICenter software. Any EPICenter user can view status information about the switches currently known to the EPICenter database.

The EPICenter Inventory Management applet provides an automatic discovery function. Users with the appropriate access can use this feature to discover Extreme and other MIB-2 devices by specific IP address or within a range of IP addresses.

Network devices can also be added to the EPICenter database manually, using the Inventory Manager Add function. Once a network device is known to the EPICenter database, you can assign it to a specific device group, and configure it using the VLAN Manager, the Configuration Manager, or the ExtremeView tool.

## The Alarm System

The EPICenter Alarm System provides fault detection and alarm handling for the network devices monitored by the EPICenter software. This includes Extreme devices and some third-party devices—those that the EPICenter software can include in its Inventory database. The Alarm System also lets you define your own alarms that will report errors under conditions you specify, such as repeated occurrences or exceeding threshold values. You can specify the actions that should be taken when an alarm occurs, and you can enable and disable individual alarms.

Fault detection is based on SNMP traps, RMON traps, and some limited polling. The Alarm System supports SNMP MIB-2 and the Extreme Networks private MIB. When an

alarm occurs you can specify actions such as sending e-mail, forwarding a trap, running a program, running a script, or sounding an audible alert.

## The Configuration Manager

The EPICenter Configuration Manager applet provides a mechanism and a graphical interface for uploading and downloading configuration files to and from managed devices. It can also download ExtremeWare software images and BootROM images to Extreme Networks devices.

The Configuration Manager also provides a framework for storing the configuration files, to allow tracking of multiple versions. Configuration file uploads can be performed on demand, or can be scheduled to occur at regular times—once a day, once a week, or at whatever interval is appropriate.

## Interactive Telnet Applet

The ExtremeView Telnet feature includes a macro capability that lets you create and execute scripts of CLI commands repeatedly on multiple devices in one operation. You can save your macros for reuse at other times.

You can also use the interactive Telnet capability to view and modify configuration information for Cisco devices as well as for Extreme Networks devices.

## The Grouping Manager

One of the powerful features of the EPICenter software is its ability to take actions on multiple devices or resources with a single user action. The Grouping Manager facilitates this by letting you organize various resources into hierarchical groups, which can then be referenced in other applets. YOU can then take actions on a group, rather than having to specify the individual devices or ports that you want to affect.

You can also create or import named resources such as users and workstations, which can be mapped through the Grouping Manager to IP addresses and ports. This capability is especially important in relationship to the optional Policy Manager applet, which takes advantage of these types of resources to simplify the creation of QoS and Access List policies.

## The IP/MAC Address Finder

The IP/MAC Address Finder applet lets you search for specific network addresses (MAC or IP addresses) and identify the Extreme Networks switch and port on which the address resides. You can also use the IP/MAC Finder applet to find all addresses on a specific port or set of ports. You can export the results of your search to a file.

## ExtremeView Configuration and Status Monitoring

With ExtremeView, any Extreme Networks switch can be monitored and controlled from a central, web-based platform, without leaving the EPICenter client to invoke another program or Telnet session.

The ExtremeView applet displays detailed information about the status of Extreme switches in a number of categories. Any EPICenter user can view status information about these network devices known to the EPICenter database. Users with the appropriate access permissions can also view and modify configuration information for those switches using either the ExtremeWare Vista graphical user interface.

## Real-Time Statistics

The Real-Time Statistics feature of the EPICenter software provides a graphical presentation of utilization and error statistics for Extreme switches in real time. The data is taken from Management Information Base (MIB) objects in the etherHistory table of the Remote Monitoring (RMON) MIB. You can choose from a variety of styles of charts and graphs as well as a tabular display.

You can view data for multiple ports on a device, device slot, or within a port group, optionally limiting the display to the “top N” ports (where N is a number you can configure). You can also view historical statistics for an individual port. If you choose to view a single port, the display shows the value of the selected variable(s) over time, and can show utilization history, total errors history, or a breakdown of individual errors.

In addition, the Real-Time Statistics applet lets you “snapshot” a graph or table as a separate browser page. You can then save, print, or e-mail the page.

## Topology Views

The EPICenter software’s Topology applet allows you to view your network (EPICenter-managed devices and the links between devices) as a set of maps. These maps can be organized as a tree of submaps that allow you to represent your network as a

hierarchical system of campuses, buildings, floors, closets, or whatever logical groupings you want.

The Topology applet can automatically add device nodes to your map as devices are added to EPICenter software's device inventory. The EPICenter software will also add links that exist between the devices, and organize them into submaps as appropriate. You can customize the resulting maps by moving elements, adding new elements, such as links, "decorative" (non-managed) nodes, and text, and customizing the discovered nodes themselves.

Finally, from a managed device node on the map, you can invoke other EPICenter functions such as the alarm browser, telnet, real-time statistics, a front panel view, or ExtremeWare Vista for the selected device.

## Enterprise-wide VLAN Management

A virtual LAN (VLAN) is a group of location- and topology-independent devices that communicate as if they were on the same physical local area network (LAN).

The ExtremeWare EPICenter VLAN Manager is an enterprise-wide application that manages many aspects of VLANs on Extreme Network's Summit and BlackDiamond switches. Any EPICenter user can view status information about the VLANs currently known to EPICenter. Users with the appropriate access can create and delete VLANs, add and remove ports from existing VLANs, and create and modify the protocol filters used to filter VLAN traffic.

## The ESRP Manager

The Extreme Standby Router Protocol (ESRP) is a feature of ExtremeWare that allows multiple switches to provide redundant layer 3 routing services, as well as layer 2 redundancy, to users. The ESRP Manager displays the status of ESRP-enabled VLANs and the ESRP-enabled switches in those VLANs. You can view a summary status for all the ESRP-enabled VLANs being monitored by the EPICenter software. You can also view detailed information for an individual ESRP-enabled VLAN and the switches in those VLANs.

## Dynamic Reports

EPICenter Reports are HTML pages that can be accessed separately from the main EPICenter user interface, without logging in to the Java user interface. The Reports module

can also be accessed from the EPICenter Navigation toolbar. A Summary Report is also displayed on the main EPICenter “home” page that provides basic information on the status of EPICenter devices and alarms. From this report you can access other more detailed reports.

The EPICenter reports are HTML pages that do not require Java capability, and thus can be accessed from browsers that do not have the ability to run the full EPICenter user interface. This means reports can be loaded quickly, even over a dial-up connection, and it also provides the ability to print the reports.

The Reports capability provides a number of predefined HTML reports that present information from the EPICenter database. You can also create your own reports by writing Tcl scripts.

## Scalable Mode

As the number of devices in your network increases, the effort required on the part of the EPICenter server to monitor all those devices increases. At some point, EPICenter performance may become undesirably slow. For a network with a very large number of devices, therefore, you can run the EPICenter server in “scalable mode.” This lets you manage a very large number of devices (on the order of 2000 devices) at the expense of the availability of some of the EPICenter applets, and the ability to manage to the port level. The following applets are not available in Scalable Mode.

- ExtremeView
- Real-Time Statistics
- Topology
- VLAN Manager
- ESRP Manager
- Policy Manager (an optional, separately-licensed module)

Scalable Mode is implemented through a single property setting in the EPICenter Administration module.

## Security Management

In order to access EPICenter features, a user must log in with a user name and a password.

EPICenter provides three access levels:

- **Monitor**—users who can view status information only.
- **Manager**—users who can modify device parameters as well as view status information.
- **Administrator**—users who can create, modify and delete EPICenter user accounts as well as perform all the functions of a user with Manager access.

The EPICenter Admin applet enables configuration of EPICenter as a Remote Authentication Dial In User Service (RADIUS) server. As an alternative, it can be configured as a RADIUS client, or RADIUS authentication functionality can be disabled.

When EPICenter acts as a RADIUS server, it can be contacted by RADIUS clients (such as Extreme Networks switches) to configure access permissions for Extreme switches, and to authenticate user names and passwords. The use of the RADIUS server avoids the need to maintain user names, passwords, and access permissions in each switch, and instead centralizes the configuration in one location in EPICenter.

## EPICenter Stand-alone Utilities

The EPICenter software provides several stand-alone utilities or scripts that streamline the process of getting information into and out of the EPICenter database, or facilitate certain device troubleshooting functions. These are the following:

- The DevCLI utility lets you add devices to and remove devices from the EPICenter inventory database via command, and supports batch additions and deletions specified via a file.
- A set of Inventory Export scripts that enable you to export information from the EPICenter database about the devices that are being managed. The information is provided in a format suitable for import into other applications, such as a spreadsheet.
- The SNMPCLI utility provides SNMP Get, GetNext, and SNMP walk features that may be needed to obtain device MIB information for troubleshooting.

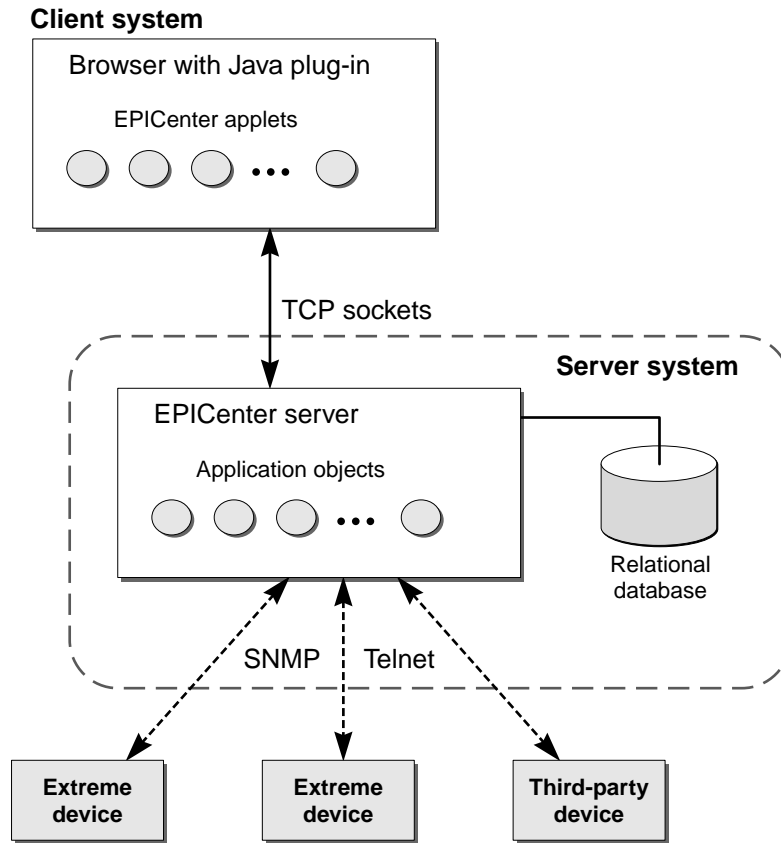
## EPICenter Components

The EPICenter software is made up of three major functional components:

- The EPICenter Server, which is based on the Tomcat Java server. The server is responsible for downloading applets, running servlets, managing security, and communicating with the database.

- A Relational Database Management System (RDBMS), Sybase Adaptive Server Anywhere, which is used as both a persistent data store and a data cache.
- The EPICenter client applications, which are Java applets that are downloaded from the server to a client machine on request and executed in a Java-enabled web browser. The Java Plug-in version 1.3.1 is required.

Figure 1-1 illustrates the architecture of the EPICenter software.



XM\_021

Figure 1-1: ExtremeWare EPICenter software architecture



## Extreme Networks Switch Management

The EPICenter software uses SNMP to monitor and manage the devices in the network. To avoid the overhead of frequent device polling, the EPICenter software uses a mechanism called SmartTraps to identify changes in Extreme device status and configuration.

When an Extreme switch is added to the EPICenter database, the EPICenter software creates a set of SmartTraps rules that define what events (status and configuration changes) the EPICenter server needs to know about. These rules are downloaded into the Extreme switch, and the EPICenter server is automatically registered as a trap receiver. Subsequently, whenever a status or configuration change takes place, the ExtremeWare software in the switch uses the SmartTraps rules to determine if the EPICenter server should be notified. These changes can be changes in device status, such as fan failure or overheating, or configuration changes made on the switch through the ExtremeWare CLI or ExtremeWare Vista.

The EPICenter server does a “heartbeat” check, by default every five minutes, of all the devices it is managing to determine if the devices are still accessible. It also does a full poll of each device at longer intervals. This interval for this less frequent status polling can be adjusted on each individual device. The EPICenter software also gives you the ability to gather device status at any time using the **Sync** feature in the Inventory Manager applet.

## Extreme Networks Device Support

Extreme Networks devices running the ExtremeWare software version 2.0 or later, are supported by most features in the EPICenter system, including the VLAN Manager and the graphical display features of the ExtremeView applet. Some features, such as ESRP, or the Policy Manager, require more recent versions of the ExtremeWare software.

See the *ExtremeWare EPICenter Release Note and Quick Start Guide* or the Extreme Networks web site for the most current information on device support in the EPICenter software.

## Third-Party Device Support

Any device running a MIB-2 compatible SNMP agent can be discovered by the EPICenter Inventory manager, and saved in the Inventory database. All devices in the database can also appear on a topology map. The EPICenter alarm system can handle SNMP traps from any device in the inventory database, including RMON traps from devices with RMON

enabled. The Real-Time Statistics module can display statistics for any device with RMON enabled, the IP/MAC Finder applet supports all devices running MIB-2 and the Bridge MIB, with the exception of user mapping, which is specific to Extreme devices.

In the Telnet applet, you can use the Telnet feature with any device that supports a Telnet interface. In the ExtremeView applet, all Extreme devices and selected third-party devices (including certain Cisco and 3COM devices) can display a device-specific front panel view in the Summary view. In addition, vendor-specific generic images are available for additional devices, such as Sun and Nortel, and a standard generic image can be displayed for all other “unknown” devices. New device images and configuration description files may be added over time—check the Extreme Networks web site for information on new device support.

## EPICenter Client Requirements

The EPICenter client requires a monitor that supports 1024x768 resolution, and at least 16-bit color. Your system Display Settings must be set for 65536 colors.

The client may also use large amounts of memory. 128 MB of RAM is recommended for best performance (256 MB is recommended if you plan to run the client on the same system as the EPICenter server).

The client can run using the following browsers:

- Microsoft Internet Explorer version 5.0 or version 5.5 with Service Pack 1 on Windows NT 4.0 or Windows 2000, with the Java Plug-in 1.3.1.
- Netscape Navigator version 4.7 under SPARC Solaris (2.6, 7, or 8) with the Java Plug-in version 1.3.1.



*See the ExtremeWare EPICenter Release Note and Quick Start Guide shipped with the software for the latest information about configuration requirements.*

# 2

## Installing the EPICenter Software

---

This chapter describes:

- Hardware and software requirements for the EPICenter server and client
- Procedure for obtaining an evaluation or permanent license key for the software
- Install the EPICenter Server software under either Windows NT or Windows 2000
- Set up Internet Explorer for use with the EPICenter client on a Windows system
- Install the EPICenter server software under the Solaris Operating Environment
- Set up Netscape Navigator for use with the EPICenter client on a Solaris system

### Installation Overview

The ExtremeWare EPICenter Standard Edition (SE) software includes a set of Java applications, a Web Server, and database software. The installation process installs all of these components on a Windows NT 4.0 or Windows 2000 system, or under Solaris 2.6, Solaris 7, or Solaris 8.

The EPICenter client runs within a web browser (Microsoft Internet Explorer under Windows or Netscape Navigator under Solaris) with the Java Plug-in version 1.3.1. The client does not require installation, you just point your browser to the EPICenter server.



*See the ExtremeWare EPICenter SE Release Note and Quick Start Guide for the most current information on installation requirements.*

The ExtremeWare EPICenter server installation process installs two components:

- The EPICenter Database Engine
- The EPICenter Web Server

Under Windows NT/2000 you can run these as services, or just as an application. Running them as services is recommended.

## Server Requirements

The ExtremeWare EPICenter Server can run under Microsoft Windows NT 4.0, Microsoft Windows 2000, or Sun Microsystems' Solaris Operating Environment, SPARC Platform Edition.

### Windows NT or Windows 2000

For installation under Windows NT or Windows 2000, the requirements are:

- Microsoft Windows NT 4.0 or Windows 2000 running on an Intel platform.
- 128 MB RAM (256 MB recommended, especially if you plan to run an EPICenter client on the same system).
- Disk space depends on the file system used on the disk as well as the number of items (devices, ports, alarms etc.) that the system must handle:
  - 130 MB of disk space for the server installation.
  - Up to 150-200 MB for runtime usage (log files, database, user-defined scripts, reports, and so on).
  - If the disk is using the FAT file system, the EPICenter server could use 30% of the disk (i.e 300MB on a 1 GB disk, 600 MB on a 2GB disk and so on). Installing on a FAT file system is not recommended.

You can tell the type of file system by looking at the disk properties. Right-click on the drive letter in the Windows Explorer or My Computer windows.

- 300 Mhz Pentium-compatible processor.
- CDROM drive (for installation).
- A network connection.

## Solaris

For installation under Solaris, the requirements are:

- Solaris Operating Environment 2.6, Solaris 7, or Solaris 8 with required patches already installed.
- 128 MB RAM (256 MB recommended, especially if you plan to run an EPICenter client on the same system).
- As much as 300 MB disk space:
  - 130 MB of disk space for the server installation
  - Up to 150-200 MB for runtime usage (log files, database, user-defined scripts, reports and so on)
- CDROM drive (for installation)
- A network connection

Both the Solaris 2.6 and Solaris 7 operating environments may require patches for EPICenter to function properly. Make certain these patches have been installed before you install the EPICenter server software. See Chapter 3 for more information on obtaining any needed patches.

For the most current information on required patches, see the *ExtremeWare EPICenter SE Release Note and Quick Start Guide* that accompanies your EPICenter software, or check the Extreme Networks web site at [www.extremenetworks.com](http://www.extremenetworks.com).

## Client Requirements

The EPICenter client requires a monitor that supports 1024 x 768 resolution, and at least 16-bit color. Your system Display Settings must be set for 65536 colors.

The client can also use large amounts of memory. 128 MB of RAM is recommended for best performance (256 MB is recommended if you plan to run the client on the same system as the EPICenter server).

The EPICenter client user interface is a Java-based application that runs within a web browser such as Microsoft Internet Explorer or Netscape Navigator.

- Under Windows NT 4.0 or Windows 2000, install Internet Explorer 5.0, or Internet Explorer 5.5 with Service Pack 1, and the Java 1.3.1 plug-in.

- On a Solaris system, install Netscape Navigator 4.7 or later, with the 1.3.1 Java plug-in.



See the ExtremeWare EPICenter Release Note and Quick Start Guide *shipped with the software for the latest information about configuration requirements.*

## EPICenter Software Licensing

In order to log in to the EPICenter server from an EPICenter client, the product must be configured with a valid license. Optional products such as the Policy Manager also require their own license keys.

An evaluation license allows you to run the product for 45 days. A permanent license has no time limit. You can install the software without a license key, but you will not be able to connect to it from an EPICenter client. (If you need to install the product without a license key, you can add the key at a later time using a license key upgrade utility.)

You must obtain both evaluation and permanent license keys from the Extreme Networks licensing web site. The license key should be sent to you as e-mail within minutes of submitting your request.

Both evaluation and permanent license keys are 14-character keys that start with EP and are followed by 12 additional characters that are a combination of upper- and lower-case alphabetic characters, numbers, and special characters such as “+”

If you have purchased the product, you should have received an activation key, found on the License Agreement included in your software package. This key starts with “AC,” and can be used to obtain a permanent license key. You do not need an activation key to obtain an evaluation license key.



See the ExtremeWare EPICenter Release Note and Quick Start Guide *shipped with the software for the latest information about obtaining a license key.*

## Obtaining an Evaluation License

To obtain an evaluation license key, use your browser to connect to the license page at <http://www.extremenetworks.com/go/epickey.htm>.

Select the option to obtain an evaluation license key. You will be asked to enter your name, company information, and other similar information, and an e-mail address to which your license key should be sent.

You license key will be sent to you by return e-mail.

## Obtaining a Permanent License

To obtain a permanent license key, use your browser to connect to the license page at <http://www.extremenetworks.com/go/epickey.htm>.

Select the option to obtain a permanent license key.

Fill in the requested information, and enter your activation key. The activation key is a 14-character key that starts with “AC” and is found on the License Agreement included with your software package.

Your permanent license key will be sent to you by return e-mail.

## Upgrading an Evaluation License

To update an evaluation license of the ExtremeWare EPICenter to a permanent license, use the `instlic` utility.

In Windows, run the `instlic` command using the **Run** command from the Windows Start menu, or from an MS-DOS command window. From Solaris, run the command from a command shell. The `instlic` utility is found in the EPICenter install directory, by default `epc3_1` in Windows, or `/opt/epc3_1` on a Solaris system.

Enter the command followed by the 14-character license key, as follows:

```
instlic <license_key>
```

See “Adding or Updating the License Key” on page 2-10 (for Windows) or “Adding or Updating a License Key” on page 2-17 (for Solaris) for further instructions.

## Adding a License for an Optional Product

When you purchase a product option such as the EPICenter Policy Manager, you receive a separate key to enable the optional module. If you purchase the optional module at the same time as the main ExtremeWare EPICenter software, you can use the use the optional module key when you do the EPICenter installation, and it will enable both the EPICenter software and the additional module.

However, if you purchase the additional module at a later time, you must update your license key to enable the new module.

To add a license key for an optional EPICenter product module, use the `instlic` utility.

In Windows, run the `instlic` command using the **Run** command from the Windows Start menu, or from an MS-DOS command window. From Solaris, run the command from a command shell. The `instlic` utility is found in the EPICenter install directory, by default `epc3_1` in Windows, or `/opt/epc3_1` on a Solaris system.

Enter the command followed by the 14-character license key, as follows:

```
instlic <license_key>
```

See “Adding or Updating the License Key” on page 2-10 (for Windows) or “Adding or Updating a License Key” on page 2-17 (for Solaris) for further instructions.

## Upgrading from a Previous Release

If you have the previous software release installed, the installation script can also migrate your database information to the new EPICenter software version. The installation process will upgrade only the previous release of the software—for the ExtremeWare EPICenter SE release 3.1, you can upgrade from ExtremeWare EPICenter 3.0, but not from any earlier versions of the ExtremeWare Enterprise Manager software. If you are running one of the older versions (ExtremeWare Enterprise Manager 1.0, 1.1, 2.0, or 2.1) you must do a new install of the EPICenter 3.1 software.

There is one caveat concerning the upgrade:

- Server-side configuration changes (specifically, edits you’ve made to `extreme.properties` file) are not copied. The `extreme.properties` file has been removed in EPICenter 3.1, and the server configuration settings are now handled through the EPICenter client in the Administration module. You must re-enter any configuration changes through the Server Properties page in the Administration applet.

## Installing on a Windows NT or Windows 2000 System

The following sections assume that Microsoft Windows NT 4.0 or Windows 2000 is already running.





*For information on installing and running Windows NT or Windows 2000, refer to the documentation supplied with your Microsoft Windows software.*

To install the EPICenter software components under Windows NT you must have Windows NT administrator privileges on that system.

If you have the previous software release installed, the installation script will also migrate your database information to the new EPICenter software version.



*If you are running an evaluation version of the EPICenter software, DO NOT REINSTALL the EPICenter software to upgrade to a permanent license if you want to retain the information in your EPICenter database. Using the license installation utility will preserve the contents of the database.*

To update an evaluation copy of the EPICenter server to a licensed copy without reinitializing the database, follow the update procedure described in “Adding or Updating the License Key” on page 2-10.

To install the ExtremeWare EPICenter server, follow these steps:

- 1 Close any open applications.
- 2 Insert the CDROM into the CDROM drive.
- 3 In most cases, the ExtremeWare EPICenter Welcome screen appears automatically. If it does not:
  - a Open **My Computer** or **Windows Explorer**, and go to your CDROM drive.
  - b Open the `nt` directory, and start `setup.exe`.The ExtremeWare EPICenter Welcome screen appears.
- 4 Follow the on-screen instructions to progress through the Welcome screen.
- 5 If you are running EPICenter 3.0, you are notified that the services will be stopped in order to install the EPICenter 3.1 software. If this is acceptable, click **Yes**.
- 6 Click **Yes** to accept the license agreement.
- 7 Enter your company information.
- 8 Enter your license key.

The license key is a case-sensitive string starting with “EP” and followed by 12 characters (a mixture of uppercase and lowercase letters, numbers, and special characters) that you obtained from the Extreme Networks web site.

The license key is NOT the same as the activation key, which starts with “AC,” and found on the License Agreement shipped with your purchased product. You use the

activation key to obtain a permanent license key from the Extreme Networks web site at <http://www.extremenetworks.com/go/epickey.htm>

See Chapter 1 of this manual or the *ExtremeWare EPICenter SE Release Note and Quick Start Guide* for details on obtaining an evaluation or permanent license key.

If you have purchased the EPICenter software and an additional module such as the Policy Manager, you can use the key you received for the optional module here. It will enable both the EPICenter software and the additional module.

If you do not yet have a key, you can still install the product, and then update the key later using the `instlic.exe` utility. See “Adding or Updating the License Key” on page 2-10.

- To skip entering a key, leave the field blank and click **Next**.
- A warning box pops up; click **OK** to continue.

**9** In the Destination dialog box, choose one of two options:

- Accept the default target drive and folder displayed in the Destination Directory box.
- Click **Browse** and select or enter a new folder, a new drive, or both.

If you are installing on a disk that uses the FAT file system rather than the NTFS file system, a warning message pops up when you click **Next**. This is because under the FAT file system, the EPICenter software can take up as much as 20% of your partition, regardless of the size of the partition.

**10** Accept the default program folder, EPICenter 3.1, or enter a different program folder name, and click **Next**.

**11** In the Database Server Information dialog box, enter a number into the **Port** field for the TCP port that the EPICenter Web Server will use to communicate with the database, or accept the default (2638). You can use any port number (a number between 1024 and 9999 is recommended) except a port number already in use by another process.

**12** In the Get HTTP Port dialog box, you are asked for two ports that the EPICenter Web Server will use:

- The HTTP Port for communication with clients (default 80).
- The Admin Port used by the EPICenter web server (default 8007).

Accept any or all of the default port numbers, or enter different port numbers. You can use any port number (a number between 1024 and 9999 is recommended) except:

- The port number you just entered for the database TCP port.
- Any port number already in use by another process.

- 13** If there are any ExtremeWare EPICenter or ExtremeWare Enterprise Manager servers running as services, a notice appears advising you that the services are being shut down. <

The installation software then copies the EPICenter program files from the CD to your system.

- 14** When the files have been copied, the Install as a Service dialog box asks if you want to install the ExtremeWare EPICenter database and web server components as Windows NT services.
- Click **Yes** to install the EPICenter components as services. This is strongly recommended. If the EPICenter components run as services, they will be started automatically on system boot, and will persist across user logins and logouts.



*You must have NT Administrator privileges to install the EPICenter components as services.*

*In addition, if you want to be able to import user and host information from a Windows NT Domain Controller, the EPICenter server must run with permissions that allow it to get user information from a Domain Controller.*

- Click **No** if you do not want to install the components as services.

- 15** If you are upgrading from the previous release of the EPICenter software, you are asked whether you want to copy the database and other persistent data to the new installation. Click **Yes** to copy the data, or **No** to continue without doing so.

If you answer **Yes**, an MS-DOS window will appear briefly while the database contents are dumped from the old database and loaded into the new database.



*For the EPICenter 3.1 release, this installation utility will upgrade the database from ExtremeWare EPICenter 3.0. Database upgrades from ExtremeWare Enterprise Manager versions are not supported.*

- 16** The installation procedure now installs the license key. An MS-DOS window will appear briefly while this occurs.

If the license key you entered is invalid, an error window pops up. If you did not enter a license key, a warning pops up. In either case, you can use the `instlic` utility to enter a valid license key after you have completed your installation.

- 17** In the final dialog box, EPICenter Setup Complete, you can do the following.

- Click the checkbox to indicate you want to view the Readme file
- If you have installed the EPICenter components as services, click the second checkbox to indicate you want your system to be restarted. If you choose not to

restart your system at this time, you must either restart the server or start the services manually before you can log in to the EPICenter server from a client.

- Click **Finish** to complete the installation process.

## Adding or Updating the License Key

To update an evaluation license of the ExtremeWare EPICenter to a permanent license, or to install a license key after the original installation is complete, use the `instlic` utility provided.



*DO NOT reinstall the software if you have any data or configurations of value in the EPICenter database. Re-installation will re-initialize the database.*

To update your license key, follow these steps:

- 1 Select **Run...** from the Start menu, or start an MS-DOS command window.



*Because you must enter the license key on the command line, you cannot run this utility from a Windows Explorer or My Computer window.*

- 2 Enter the command `<EPICenter_install_dir>\instlic <key>`

`<EPICenter_install_dir>` is the directory (path) where you installed the EPICenter components. If you installed in the default directory, the path is

`c:\EPC3_1\`

`<key>` is the 14-character license key, starting with “EP,” that you obtained from Extreme Networks. Type the key *exactly* as it is shown in the e-mail you received from Extreme Networks. The key is case sensitive.

For example: `c:\EPC3_1\instlic EP1a2B3c4D5+eF`

If the license update is successful, the message “License Installed” is displayed.

If the update is not successful, the message “Invalid argument key : `<key>`” is displayed. `<key>` is the license key you entered with the `instlic` command. Verify that you typed the key exactly as shown in the e-mail you received from Extreme Networks.

## Installing on a Solaris System

The EPICenter server software, version 3.1, is supported under Solaris 2.6, Solaris 7, and Solaris 8. See “Server Requirements” in Chapter 1 for the hardware requirements. Also,

check the *ExtremeWare EPICenter SE Release Note and Quick Start Guide* for any additional issues.

## Required Patches

Both the Solaris 2.6 and Solaris 7 operating environments require patches for the EPICenter software to function properly. Make certain these patches have been installed before you install the EPICenter server software.

For the most current information on required patches, see the *ExtremeWare EPICenter SE Release Note and Quick Start Guide* that accompanies your EPICenter software, or the Extreme Networks web site at [www.extremenetworks.com](http://www.extremenetworks.com).

Sun Microsystems makes these patches available on the Java download site in the form of tar files. They can be found at:

<http://www.sun.com/software/solaris/jre/download.html>

On this page, select Java 2 Standard Edition (J2SE) 1.3.0\_03 Production Release for Solaris, English, SPARC Edition. The patches listed for this release apply to the 1.3.1 Plug-in as well.

You must register or log in, and then you will be presented with the download page that includes Solaris patch bundles.

## Local Name Resolution

The Solaris system on which EPICenter is installed must be able to resolve both its own local name and its domain name. For example if you install EPICenter on a system named `system1`, then it must be able to resolve both `system1` and its domain name, such as `system1.company.com`. You can test for this by attempting to ping the system using both the local name and the domain name. If there are problems resolving either of these names, make sure the `etc/hosts` file contains the correct information.

## Installing the EPICenter Server

The instructions that follow assume that you are running in a command shell or Xterm window.

You can install the EPICenter components without being logged in as root, as long as you do not use port numbers less than 1024 (for example, port 80 for the EPICenter web server, which is the default).



*When you install the EPICenter Server, it initializes the database. If you attempt to re-install the server once you have installed it, the installation process reinitializes the database, and your existing data and configurations will be lost.*

*To update an evaluation copy of the EPICenter software to a licensed copy without reinitializing the database, follow the update procedure described in the section “Adding or Updating a License Key” on page 2-17.*

To install the EPICenter server software, follow these steps:

- 1 Insert the CDROM into the CDROM drive.
- 2 If you are running CDE, the contents of the CDROM are displayed in the File Manager. Go to the `sol` directory.

To run from an Xterm window:

```
cd /cdrom<x>/sol
```

where `<x>` is your CDROM drive number (e.g. `cdrom0`). The volume label of the installation CD is `epc31b<xx>`, where `<xx>` is the build number, for example `epc31b49`.

- 3 Run the installation script:

```
./install.sh
```

The EPICenter Welcome message appears as follows:

```
*****
```

```
Welcome to the Extreme Networks ExtremeWare EPICenter
install program. This program will install:
ExtremeWare EPICenter version 3.1.0 on this system.
```

```
*****
```

```
Please review the following software license terms
and conditions. You will need to accept this license
to continue the installation. Press space to page
through the license.
Press <enter> to view the license:
```

- 4** When you press [Enter], the text of the license is displayed. You can use the space bar to page through it. When you reach the end, you are asked:

```
Do you agree to the above conditions? (Y/N):
```

- 5** Enter **Y** if you agree and want to proceed. Enter **N** to terminate the installation process. This question does not have a default, you must enter Y or N.

- 6** Next, you are prompted for the directory where the EPICenter server software should be installed:

```
Please enter the directory in which the software will be installed.
The default directory is /opt/epc3_1, but the product may be installed
anywhere.
```

```
Install Directory [/opt/epc3_1]:
```

Enter the directory or accept the default (/opt/epc3\_1).

If you specify a directory that does not exist, you are asked whether it should be created:

```
/opt/epc3_1: No such directory. Do you wish to create it? (y/n)[y]
```

Assuming you want to create the directory, accept Y as the default. If you answer N, the script will assume the directory already exists.

- 7** The installation script now copies and installs the EPICenter files:

```
Installing EPICenter files...
```

After copying a number of files, the following message appears:

```
File copy complete.
Configuring Installation.
```

At this point additional files are copied and the EPICenter installation tree is created, and filled out. This will take several minutes.

When the files are complete, you are asked for a set of configuration information.

```
To configure EPICenter, we will need to ask you for some information.
In most case the default answers will work correctly.
```

- 8** First you are asked whether you want to upgrade from a previous installation of ExtremeWare EPICenter. You can upgrade from EPICenter 3.0.

```
*** Upgrade Parameters
```

```
If there is a previous installation of EPICenter installed,
you may import the database from the previous
```

installation. If there is no previous install, or you would like to start from scratch, select new installation.

Would you like to upgrade from a previous install? (Y/N) [N]:

Answer Y to upgrade.

If you answer **Yes**, the install script asks for the location of the previous version of ExtremeWare Enterprise Manager.

Old install directory [/opt/epc\_30]:

Accept the default or enter the actual location (full path name).

**9** Next, you are asked for a license key.

\*\*\* License Key

Please enter the license key for the product.

This will be a string starting with EP followed by 12 characters.

To obtain a license (evaluation or permanent) visit the web site

<http://extremenetworks.com/go/epickey.htm>

Refer to the product release notes for more information on obtaining a license key. Enter s to skip and install the license later.

Please enter the license key:

The license key is NOT the same as the activation key, which starts with “AC,” and is found on the License Agreement shipped with your purchased product. You use the activation key to obtain a permanent license key from the Extreme Networks web site at <http://www.extremenetworks.com/go/epickey.htm>

See Chapter 1 or the *ExtremeWare EPICenter SE Release Note and Quick Start Guide* for details on obtaining an evaluation or permanent license key.

If you do not yet have a key, you can still install the product, and then update the key later using the `instlic.exe` utility. See “Adding or Updating a License Key” on page 2-17.

If you have purchased the EPICenter software and an additional module such as the Policy Manager, you can use the key you received for the optional module here. It will enable both the EPICenter software and the additional module.

**10** Next, you are asked to enter a port for communication between the Web server and the database server:

\*\*\* Database Parameters

EPICenter will run an SQL database server on this machine. The database



needs the name of this machine and an unused port to listen on.

Please enter the port for the database: [2638]

Accept the default (2638) for the TCP port that the EPICenter Web Server will use to communicate with the database, or enter a different port number. You can use any port number (a number between 1024 and 9999 is recommended) except a port number already in use by another process.

## 11 You are now asked for three ports that the EPICenter Web Server will use.

\*\*\* Web Server Parameters

EPICenter runs as a web server and by default accepts HTTP requests on port 80. You may specify an alternative. Additionally EPICenter needs two other unused ports , one for a web administrative server and one for internal usage. If you are not sure what to enter, the defaults should be acceptable.

Please enter the http port for the web server: [80]

Please enter the http port for the admin web server: [8007]

Accept any or all of the default port numbers, or enter different port numbers. You can use any port number (a number between 1024 and 9999 is recommended) except:

- The port number you just entered for the database TCP port.
- Any port number already in use by another process.

## 12 Finally, you are asked to confirm the configuration parameters:

\*\*\* Configuration

Please review the following items.

Upgrade	= NO
License	= <the key you entered or "s">
Database Port	= <the port you entered or 2638>
HTTP Port	= <the port you entered or 80>
HTTP Admin Port	= <the port you entered or 8007>

Are these correct? (Y to accept / N to re-enter) [N]:

**13** If you accept the parameters by entering Y, the installation script will finish with the following messages:

```
Installing License...
License installed.
Done.
```

```
Updating ./extreme/WEB-INF/web.xml
```

```
Updating ./tomcat/conf/server.xml
```

If you are upgrading from an earlier version of ExtremeWare Enterprise Manager, you will also see the following:

```
*** Database Upgrade
```

```
Upgrading Database...
Upgrading from
```

```
Generating sql files...
Dumping data from tables in old database ...
Loading data into tables in new database ...
Database Upgrade Complete.
```

Next, the installation process creates a script and some symbolic links.

```
Adding EPICenter to /etc/init.d
Adding link from rc3.d to /etc/init.d/
Adding link from rc2.d to /etc/init.d/
```

**14** Finally, you are given the opportunity to have the EPICenter server started for you.

```
Would you like to start the server now? (Y/N): n
```

Answer **Yes** to start the server immediately, or **No** if you want to start it at a later time.

The final messages are:

```
The EPICenter software installation is complete.
```

```
Once the server is running, you can run the client in
a supported web browser with the following URL:
```

```
http://<host>:<port>/
```

INSTALL COMPLETE

`<host>` is the name of the system you've just installed on, and `<port>` is the HTTP port you entered (or 80 if you accepted the default).

## Adding or Updating a License Key

To update an ExtremeWare EPICenter evaluation license to a permanent license, or to install a license key after the original software installation is complete, use the `instlic` utility provided.



*DO NOT reinstall the software if you have any data or configurations of value in the EPICenter database. Re-installation will re-initialize the database.*

- ◆ Run the installation script found in the EPICenter installation directory:

```
<install_dir>/instlic <key>
```

`<install_dir>` is the directory (path) where you installed the EPICenter components.

`<key>` is the 14-character license key, starting with "EP," that you obtained from Extreme Networks. Type the key *exactly* as it is shown in the e-mail you received from Extreme Networks. The key is case sensitive.

For example, if you installed in the default directory, enter:

```
/opt/epc3_1/instlic EP1a2B3c4D5+eF
```

You must have write permission for the EPICenter install directory.

If the license update is successful, the message "License Installed" is displayed in the xterm or command window.

If the update is not successful, the message "Invalid argument key : `<key>`" is displayed. `<key>` is the license key you entered with the `instlic` command. Verify that you typed the key exactly as shown in the e-mail you received from Extreme Networks.

## Installing the EPICenter Client

In order to run the EPICenter client, web browser software must be installed. An EPICenter client can run on a system with a different operating system than the EPICenter server.

- Under Windows NT, or Windows 2000, install Microsoft Internet Explorer 5.0 with the Java Plug-in version 1.3.1, or Internet Explorer 5.5 with Service Pack 1 and the Java Plug-in.

To download the latest version of Internet Explorer, go to  
<http://www.microsoft.com/ie/>

- Under Solaris, install Netscape Navigator version 4.7x and the Java 1.3.1 plug-in. Navigator is included in Netscape Communicator, can be downloaded from Netscape Communications. Go to the Netscape web site at <http://home.netscape.com/browsers/> for more information. From there you can find links to download the Netscape 4.76 browser software.

If you do not have the required Java plug-in installed when you start the EPICenter client, you will be prompted to download it, and will be led through the brief installation process. This obtains the plug-in from the Sun Microsystems web site, and requires Internet access.

You can also install the Java Plug-in directly from the EPICenter client Start-up page. See Chapter 2 in the *ExtremeWare EPICenter SE Software User Guide* for details on starting the client and obtaining the plug-in, if needed.

## Uninstalling the EPICenter Server

To uninstall the EPICenter software, you must first shut down the server components (database and web server). Then you can remove the program components from your system.

### Uninstalling in Windows NT or Windows 2000

Under either of these Windows OPERating Systems versions, you can run the EPICenter server components as services, or as regular applications. The uninstall procedure is slightly different for these two situations.

To uninstall the EPICenter server software, do the following:

- 1 Shut down the EPICenter components if they are still running.

If they are **running as services**:

- a From the **Start** menu, highlight **Settings**, pull right, and click on the **Control Panel**. This displays the Control Panel folder.
- b Double-click on **Services** to display the Services Properties window.

- c Stop the EPICenter 3.1 Server.
- d Stop the EPICenter 3.1 Database Engine.

If they are **running as applications**:

- a Select **Run...** from the **Start** menu, or start an MS-DOS command window.
  - b Enter the command `<EPICenter_install_dir>\stopserv.exe`  
`<EPICenter_install_dir>` is the directory (path) where you installed the EPICenter components. If you installed in the default directory, the path is `c:\EPC3_1\`
- 2 Display the Control Panel folder if you have not already done so. From the **Start** menu, highlight **Settings**, pull right, and click on the **Control Panel**.
  - 3 From the Control Panel folder, double-click **Add/Remove Programs**. This displays the **Add/Remove Program Properties** window (**Add/Remove Programs** window under Windows 2000).
  - 4 From the list of installed programs, select **EPICenter 3.1** and click **Add/Remove** (or **Change/Remove** in Windows 2000). Follow the instructions to remove the component.
  - 5 If the Add/Remove utility is not able to remove all the files, it will inform you of that fact. You must delete them manually.

## Uninstalling in Solaris

To remove the EPICenter server software from a Solaris host, stop the server using the **stopserv** command, then remove the all the files in the installation directory.

To remove the EPICenter server software, follow these steps:

- 1 Run the **stopserv** command found in the root installation directory.  
 The installation directory is the directory (path) where you installed the EPICenter components.  
 For example, if you installed in the default directory, enter:  

```
/opt/epc3_1/stopserv
```

 This shuts down the EPICenter server if it is running.
- 2 Make the parent of the installation directory the current directory, and remove all files from the directory and its sub-directories.  
 For example, if you installed using the default directory path, `/opt/epc3_1`, enter:  

```
cd opt
```

**3** Remove all files from the installation directory tree.

For example, if you installed using the default directory path, enter:

```
rm -rf epc3_1
```

This removes all the EPICenter components, including the database, from the system.

**4** The EPICenter installation created a script, `EPICenter`, in the `/etc/init.d` directory, and links to `/etc/init.d` in the `/etc/rc2.d` and `/etc/rc3.d` directories. You should remove these as well:

```
cd /etc/init.d
rm EPICenter
```

```
cd /etc/rc2.d
rm K10EPICenter
```

```
cd /etc/rc3.d
rm S90EPICenter
```

The EPICenter software is now completely uninstalled.

# 3

## Starting ExtremeWare EPICenter

---

This chapter describes:

- Starting the ExtremeWare EPICenter Server.
- Launching an EPICenter Client.
- Navigating the EPICenter pages.

When you log in for the first time after installing the EPICenter server software, there are only two user accounts enabled—an Administrator account “admin,” and a user account “user” with Monitor access privileges. Neither account has a password. Follow the instructions in Chapter 15 to change the admin password and to create additional EPICenter user accounts.

### Running the EPICenter Software under Windows

The following instructions assume that the Windows NT operating system is already running, and that the ExtremeWare EPICenter server software is already installed.

If you have installed the EPICenter components as services under Windows NT, the EPICenter Server and database component will start automatically when you boot the server. This is the recommended method of installing EPICenter.

## Starting the EPICenter Server

If you have not installed the EPICenter server components as a service, you must start the server manually after you boot your server system. You can do this from the Windows NT **Start** menu.

The EPICenter Server consists of two components:

- The EPICenter Database Engine
- The EPICenter Web Server

Both components must be running in order to run the EPICenter client applets.

To start the EPICenter Server and database components, follow these steps:

- 1 Click **Start**.
- 2 Highlight **Programs** to display the Programs menu.
- 3 Highlight **EPICenter 3.1** in the Programs menu to display the EPICenter menu.
- 4 Click **EPICenter 3.1 Server**. This runs `runserv.exe`, a program that starts the two components in the required order.

Two windows are displayed briefly as the EPICenter Server starts up:

- Sybase Adaptive Server Anywhere. An icon representing this window is placed on the right side of the Windows task bar.
- A MS-DOS window that shows the processes being started.

## Shutting Down the EPICenter Server Components

There may be occasions when you need to shut down the EPICenter server, such as to upgrade a license key from an evaluation to a permanent license, or to add an optional module license.

If the EPICenter server components are **running as services**, follow these steps to shut them down:

- 1 From the **Start** menu, highlight **Settings**, pull right, and click on the **Control Panel**. This displays the Control Panel folder.
- 2 From the Control Panel folder, double-click **Services**. This displays the Services Properties window. You must have NT Administrator privileges to access this function.
- 3 From the list of installed programs select **EPICenter 3.1 Server** and click **Stop**.



#### 4 Repeat the same actions for the **EPICenter 3.1 Database Engine**.

If the EPICenter server components are **running as applications**, follow these steps to shut them down:

- 1 Select **Run...** from the Start menu, or start an MS-DOS command window.
- 2 Enter the command `<EPICenter_install_dir>\stopserv.exe`  
`<EPICenter_install_dir>` is the directory (path) where you installed the EPICenter components. If you installed in the default directory, the directory is `epc3_1`.

## Restarting the EPICenter Server Components as Services

If you have installed the EPICenter server components as services, follow these steps to restart them:

- 1 From the Start menu, highlight **Settings**, pull right, and click on the Control Panel. This displays the Control Panel folder.
- 2 From the Control Panel folder, double-click **Services**. This displays the Services Properties window. You must have NT Administrator privileges to access this function.
- 3 From the list of installed programs select **EPICenter 3.1 Database Engine** and click **Start**.
- 4 Repeat the same action for the **EPICenter 3.1 Server**
- 5 If you want to change the start-up parameters, click **Startup...** instead of **Start**.

One situation where you might want to do this is the following: in order to import users from an NT Domain Controller, the EPICenter 3.1 Web Server must be running with permissions that enable it to get user information from the Domain Controller. If you do not have those permissions as you are currently logged on, you can specify a different log on account for the Web Server as a start-up parameter:

- In the **Log On As:** section of the **Startup...** pop up window, enter the account name and password for a user that has the appropriate permissions to access the Domain Controller.

## Running the EPICenter Software under Solaris

The following instructions assume that you are using a command or Xterm window running the C shell.

## Starting or Restarting the EPICenter Server

To run the EPICenter Server:

- 1 Set the current directory:

```
cd <install_dir>
```

<install\_dir> is the directory (path) where you installed the EPICenter components.  
If you installed in the default directory, the path is /opt/epc3\_1.

- 2 Invoke `runserv` to start the two EPICenter components in the required order.

```
runserv &
```

## Shutting Down the EPICenter Server Components

To shut down the EPICenter Server:

- 1 Set the current directory:

```
cd <install_dir>
```

<install\_dir> is the directory (path) where you installed the EPICenter components.  
If you installed in the default directory, the path is /opt/epc3\_1

- 2 Invoke `stopserv` to shut down the EPICenter components in the required order.

```
stopserv &
```

This shuts down the EPICenter server if it is running.

## Launching the ExtremeWare EPICenter Client

The EPICenter client user interface is a Java-based application that runs within a web browser such as Microsoft Internet Explorer or Netscape Navigator.

- Under Windows NT 4.0 or Windows 2000, install Internet Explorer 5.0, or Internet Explorer 5.5 with Service Pack 1, and the Java 1.3.1 plug-in.
- On a Solaris system, install Netscape Navigator 4.7 or later, with the 1.3.1 Java plug-in.

To run the EPICenter client interface:

- 1 Launch your web browser.
- 2 Enter the following URL:

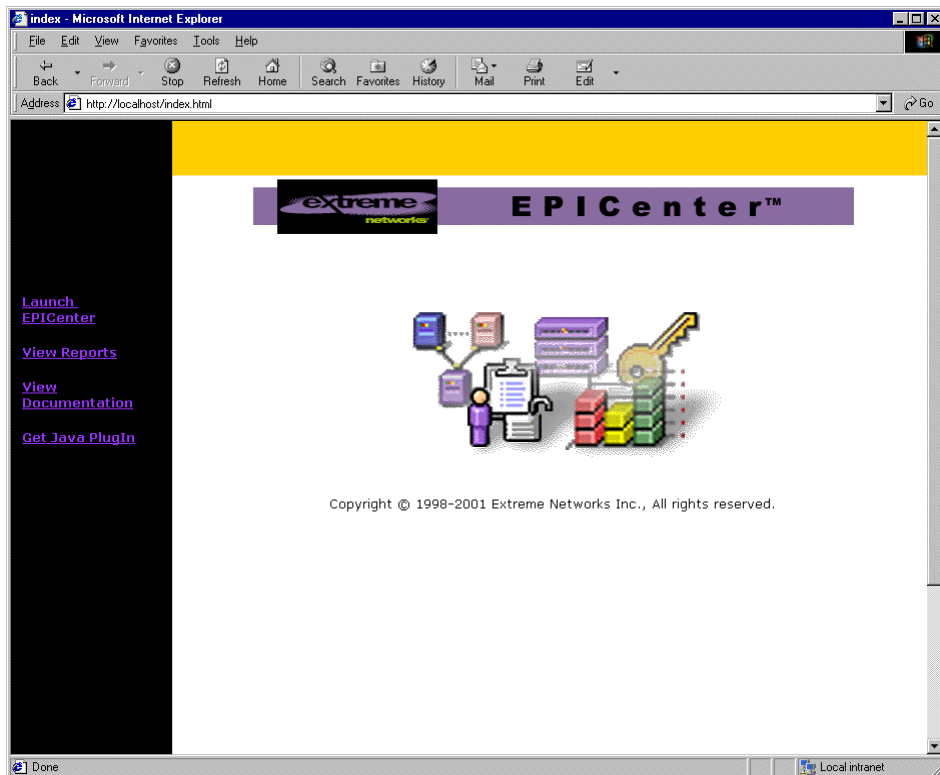
`http://<host>:<port>/`

In the URL, replace *<host>* with the name of the system where the EPICenter server is running. Replace *<port>* with the TCP port number that you assigned to the EPICenter Web Server during installation.



*If you used the default web server port, 80, you do not need to include the port number.*

The EPICenter Start-up page appears. Figure 3-1 shows the Start-up page in Internet Explorer under Windows NT. The Start-up page in Netscape Navigator looks similar.



**Figure 3-1:** EPICenter start-up page

From the Start-up page you can run the EPICenter client interface, view the online documentation, or log into the EPICenter reports module.

- To launch the EPICenter client interface, click the **Launch EPICenter** link. This requires that the Java Plug-in version 1.3.1 be installed in your browser.

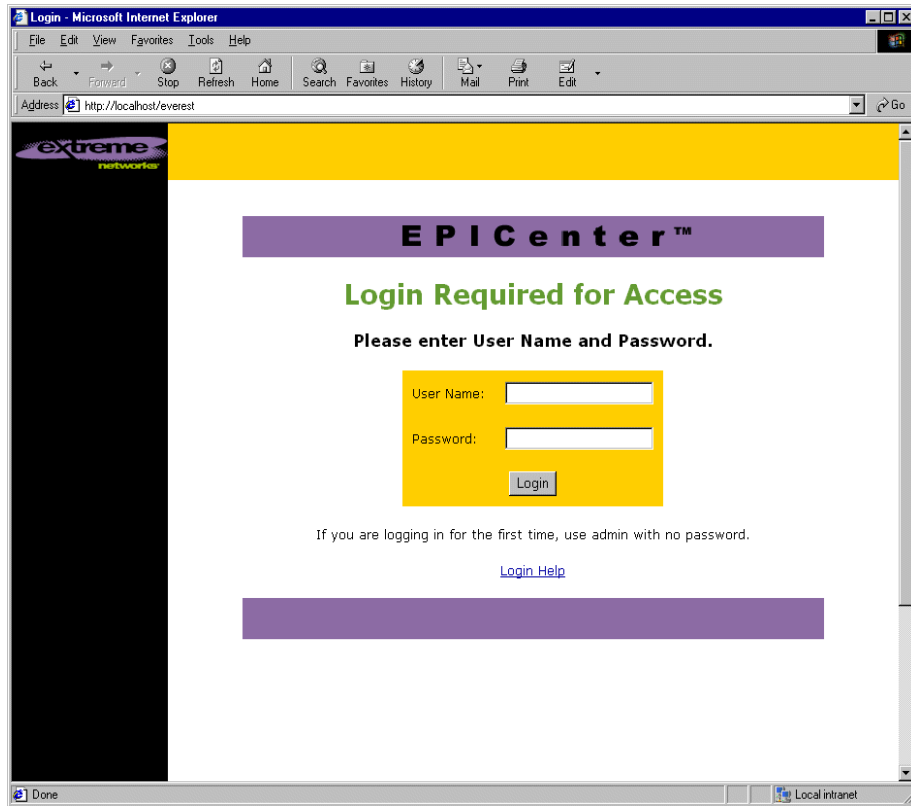
If the required version of the plug-in is not installed, you will be prompted to download it, and will be led through the brief installation process. This obtains the plug-in from the Sun Microsystems web site, and requires Internet access.

You can also install the Java Plug-in directly, if you know you do not have the correct version installed, or if you encountered problems downloading it. Click the **Get Java PlugIn** link, which will install the required version from the EPICenter server installation. This requires access to the system where the EPICenter server is installed, and does not require Internet access.

The EPICenter Login page appears, as shown in Figure 3-2.

- You can view a variety of reports about EPICenter devices and functions, without requiring the Java Plug-in. Click the **View Reports** link to log into the EPICenter Reports applet, which provides a number of HTML-based reports. See Chapter 12, “Viewing Dynamic Reports,” for more information on using these reports.
- Click the **View Documentation** link to display the online *ExtremeWare EPICenter Software User Guide*. This requires that you have a copy of Adobe’s Acrobat Reader (version 3.0 or later) installed.

If you do not have the Acrobat Reader installed, you can download it free of charge from Adobe’s web site, at <http://www.adobe.com>.



**Figure 3-2:** ExtremeWare EPICenter login page



*There are two default user accounts—the Administrator account “admin,” and the user account “user.” Initially, those accounts have no password. “User” has Monitor access privileges.*

*Chapter 15, “Administering EPICenter” describes how an EPICenter Administrator can create additional EPICenter user accounts.*

To log into EPICenter:

- 1** If you already have an EPICenter user account, type your EPICenter user name in the **User Name** field.
  - If you are the network administrator logging in to the EPICenter server for the first time since it has been installed, log in as “admin.”

You will be able to change the admin password (*strongly recommended*) and to create additional user accounts.

- If you are a new user without your own account on the EPICenter server, type “user” as the **User Name**. You will be able to view information in the various modules, but will not be able to change any configurations.

**2** Type your password in the **Password** field.

Both default names (“user” and “admin”) initially have no password, so you can leave the field blank.

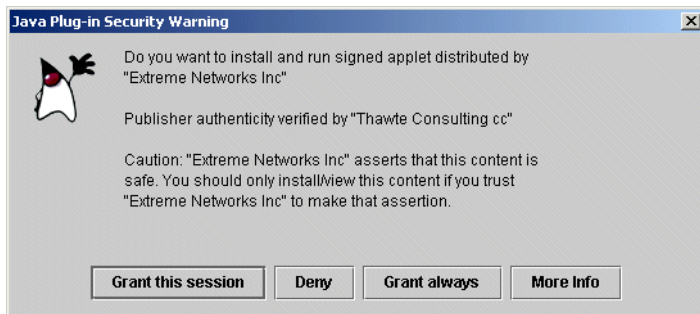
**3** Click **Login**.

If you are using an evaluation copy of the EPICenter, a dialog box appears notifying you how much longer the copy is valid.

Click **OK**.

The HTML **Network Summary Report** page appears.

**4** If you are loading the client for the first time, a **Java Plug-in Security Warning** pop-up will appear, as shown in Figure 3-3.



**Figure 3-3:** Java Plug-inSecurity Warning

This allows you to specifically accept loading of the EPICenter java applets on your system.



*If the browser appears to freeze after the Network Summary Report Page appears, but before any applet icons appear in the left-hand column, check to see if the security warning window is hidden behind the browser.*

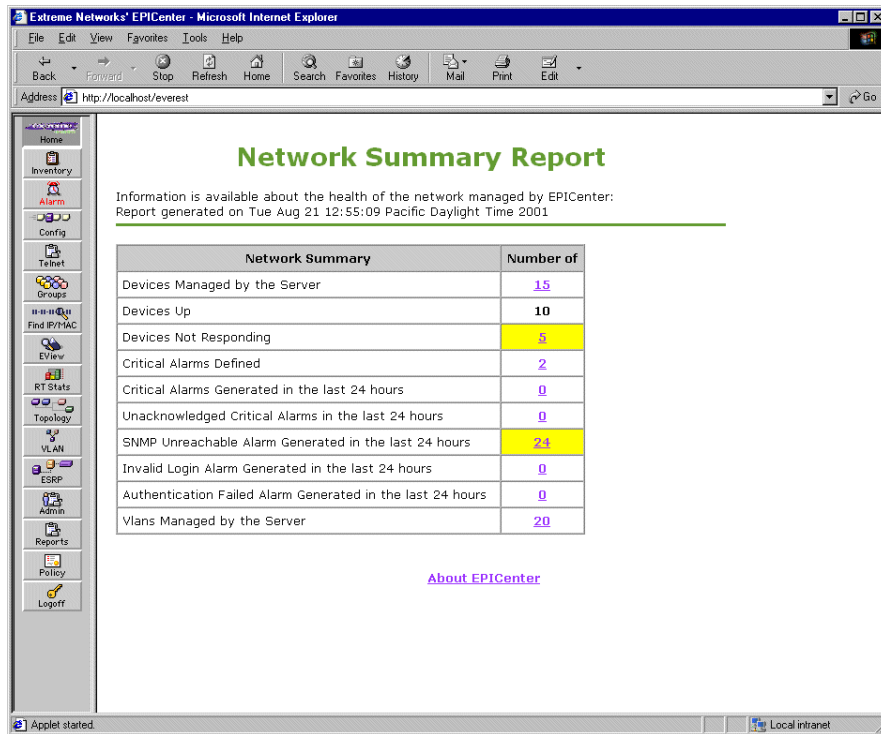
To allow the EPICenter applets to be loaded, click one of the Grant buttons:

- **Grant this session** will allow the installation of the applets for this browser session only. You will have to grant permission for every applet every time you run the client.
- **Deny** will prevent the EPICenter applets from being loaded. You will still be able to view the Network Summary Reports, but will not be able to access any EPICenter applets.
- **Grant always** indicates that you always want to load the EPICenter applets. This warning will not be displayed in the future.

Assuming you grant the session, the Navigation buttons for the EPICenter applets will appear in the left-hand panel alongside the Network Summary Report page, as shown in Figure 3-4.



*If you have problems with the client display the first time you try to run EPICenter after installing it, try clearing all browser cache (both memory and disk), then closing and re-opening the browser.*



**Figure 3-4:** The Network Summary Report page

This page displays a simple HTML report with some basic statistics on the status of your network. Click on the values in the right-hand column to display a detail report about a specific status item. From this summary report you can view the following reports:

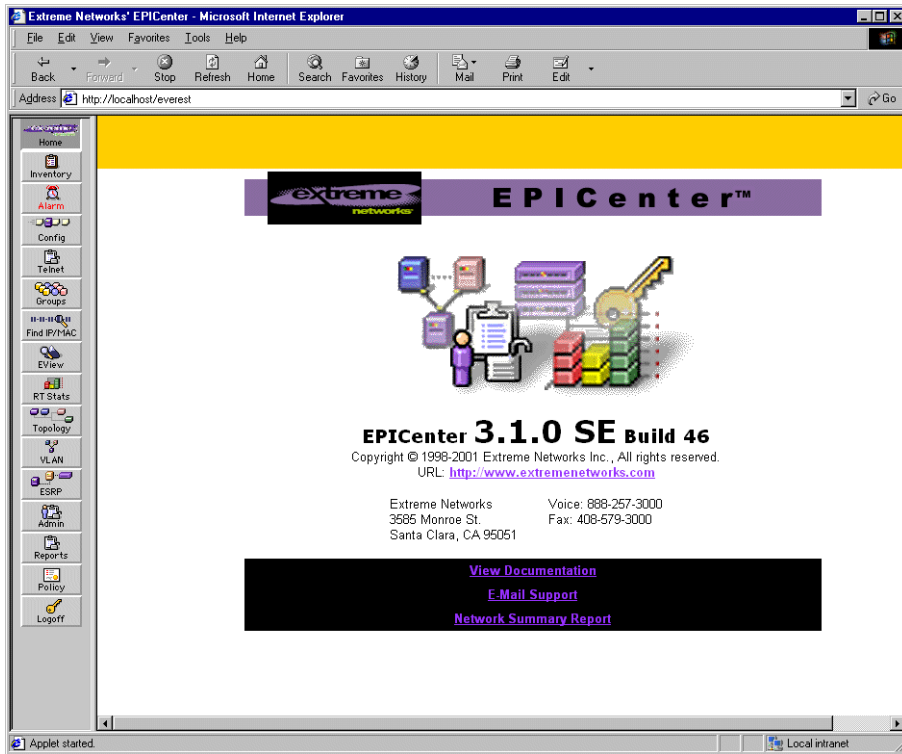
- Summary status of all the devices known to the EPICenter server.
- Summary status of the devices known to the EPICenter server that are not responding.
- A summary of alarm definitions that include severity levels of Critical or Major.
- A summary of critical alarms that have occurred in the last 24 hours.
- A summary of critical alarms in the last 24 hours that have not been acknowledged.
- A summary of SNMP Unreachable alarms that have occurred in the last 24 hours.
- A summary of Invalid Login alarms that have occurred in the last 24 hours.
- A summary of Authentication Failure alarms that have occurred in the last 24 hours.
- Summary information on all VLANs being managed by the EPICenter server.

The Network Summary Report can also be accessed from the Reports applet. See Chapter 16, “Dynamic Reports” for a more detailed discussion of these reports.

From the bottom of the Network Summary Report panel you can navigate to the **About EPICenter** page.

The **About EPICenter** page, shown in Figure 3-6, provides information about the version of EPICenter that you are running. This information may be needed if it becomes necessary for you to contact Extreme Networks’ Technical Support.





**Figure 3-5:** The About EPICenter page

From this page you can do the following:

- Access the online *ExtremeWare EPICenter Software User Guide*.
- Send e-mail to Extreme Networks' technical support organization.
- Return to the Network Summary Report page.

## Navigating the EPICenter Applications

The EPICenter client consists of two frames, as shown in Figure 3-6:

- The Navigation Toolbar, from which you can access the EPICenter applets
- The Main Applet frame, where the currently active applet runs.

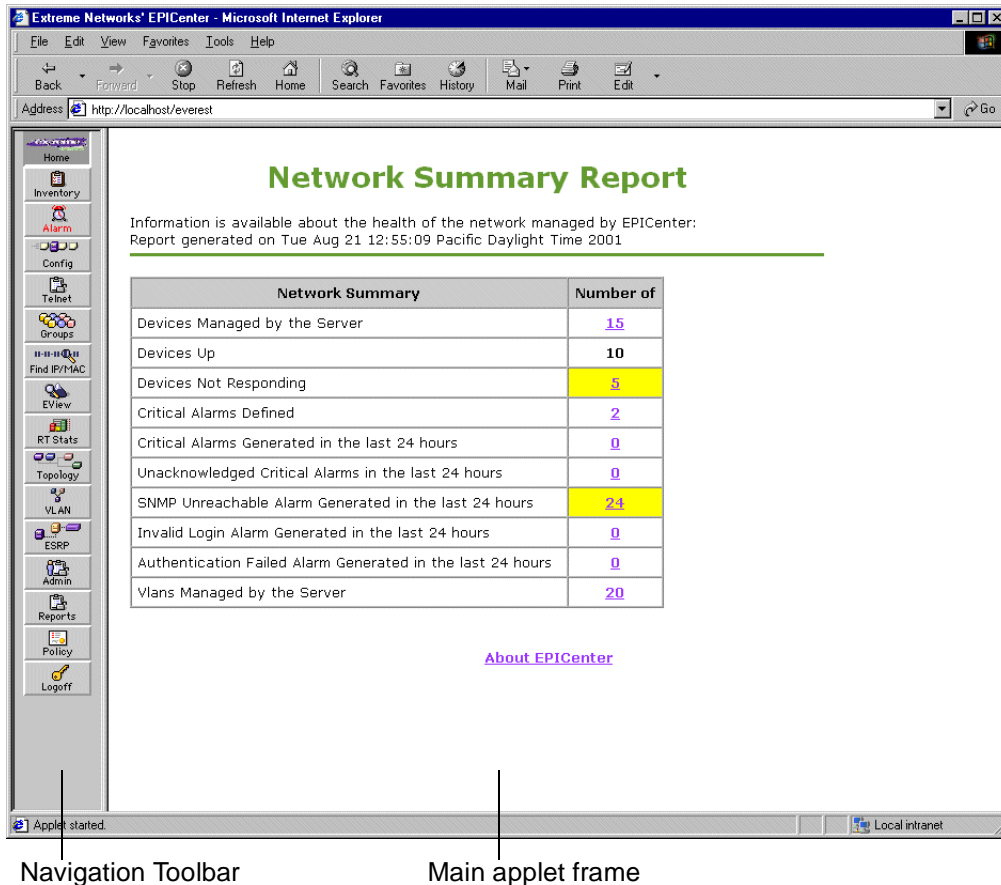


Figure 3-6: The EPICenter Home page

## The Navigation Toolbar

The Navigation Toolbar, on the left, displays a set of buttons you can use to access various EPICenter modules. The buttons that appear in this Toolbar may be a subset of those listed here, depending on whether you have licensed additional modules, such as the EPICenter Policy Manager, or are running in scalability mode, which disables certain modules.

- **Home** returns you to the Network Summary Report display shown in Figure 3-6. From this page, you can access the About EPICenter page.

- **Inventory** runs the Inventory Manager, where you can discover devices on your network, and set up device groups and port groups so you can manage network elements in sets rather than individually.
- **Alarm** runs the Alarm Manager, where you can view and browse alarms that have occurred on your network devices, as well as define alarms and the actions that should occur when an alarm happens. This button also indicates that a new alarm has been received by displaying its label in red text instead of black text.
- **Config** runs the Configuration Manager, where you can upload and download switch configuration files, and download ExtremeWare software to your switches.
- **Telnet** runs an interactive Telnet application where you can create and run command-line macros on multiple devices in one operation. You can also establish telnet sessions with individual switches, both Extreme Networks and third-party devices.
- **Group** runs the Grouping applet.
- **Find IP/MAC** runs the IP/MAC Address Finder applet, where you can search for the ports associated with one or more MAC or IP addresses, or identify the IP or MAC addresses connected to a set of ports.
- **EView** runs the ExtremeView applet, where you can view status and statistics about your managed devices, and do Extreme device configuration through Extreme Networks' interactive web-based device interface, ExtremeView Vista.
- **RT Stats** runs the Real Time statistics applet, that provides graphs of various device and port statistics. This applet is not available in scalability mode.
- **Topology** runs the Topology applet, which gives you a hierarchical, logical map-based view of your network topology. This applet is not available in scalability mode.
- **VLAN** runs the VLAN Manager, where you can set up and manage VLANs.
- **ESRP** runs the ESRP Manager, which lets your view the status of your ESRP-enabled switches and VLANs.
- **Admin** runs the Administration module, where a user with Administrator access can administer EPICenter user accounts and the RADIUS server. Other users can change their own password using this applet.
- **Reports** runs the Dynamic Reports module, where you can run a number of pre-defined HTML-based reports from data in EPICenter's inventory database. You can also define your own reports.
- **Logoff** ends your session and returns you to the Login display.



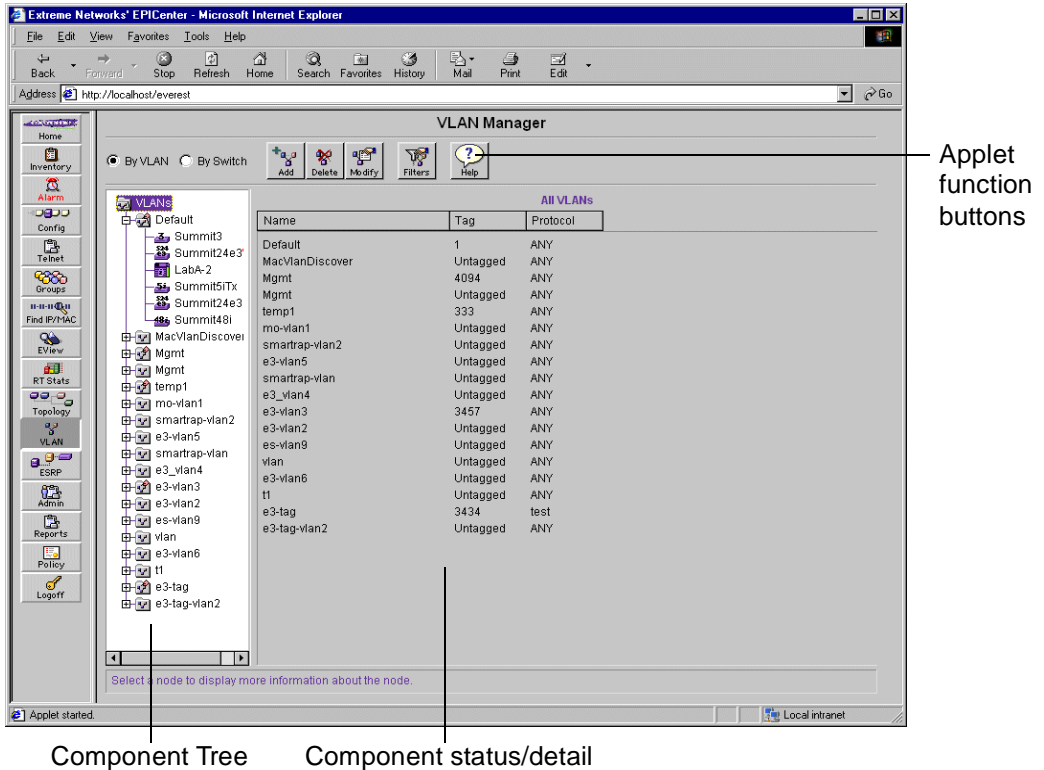
*Note that you must have Administrator or Manager access in order to use most of the functions of these applets. Users with Monitor access will be able to view status, statistics etc., but will not be able to set up or change EPICenter or device configurations.*

In addition to the applets described above, the Navigation Toolbar may include icons for other optional applications that have been integrated into the EPICenter server. These modules or products are typically purchased separately, and enabled via special license keys. Documentation for these modules is provided separately from the main EPICenter documentation. These include:

- **Policy** runs the EPICenter Policy Manager, where you can define QoS policies and access list rules for implementation on Extreme Networks and Cisco devices. This applet is an optional module that is licensed separately. It requires the installation of a separate license key.
- **ServiceWatch** runs the EPICenter ServiceWatch software within the EPICenter client browser. ServiceWatch is not an EPICenter module, but a separate product. You can enable the integration into the EPICenter Navigation Toolbar through the Server Properties pages in the EPICenter Administration applet.

## Main Applet Frame

The main applet frame is used to display the active EPICenter applet. For example, in Figure 3-7, the VLAN Manager is displayed in the main applet frame.



**Figure 3-7:** VLAN Manager applet running in a browser window

EPICenter applets use a two-panel display within the main applet frame. The two panels are:

- The Component Tree.
- A component status/detail information panel.

In addition, some applets provide an applet-specific set of buttons at the top of the main applet frame. These provide access to specific applet functions, such as adding, deleting, or configuring components managed by the applet.

## The Component Tree

The left side panel shows the Component Tree. The Component Tree is a nested tree that displays the components known to the EPICenter database that are relevant to the active module. The Component Tree displays different sets of components depending on which EPICenter module you are viewing.

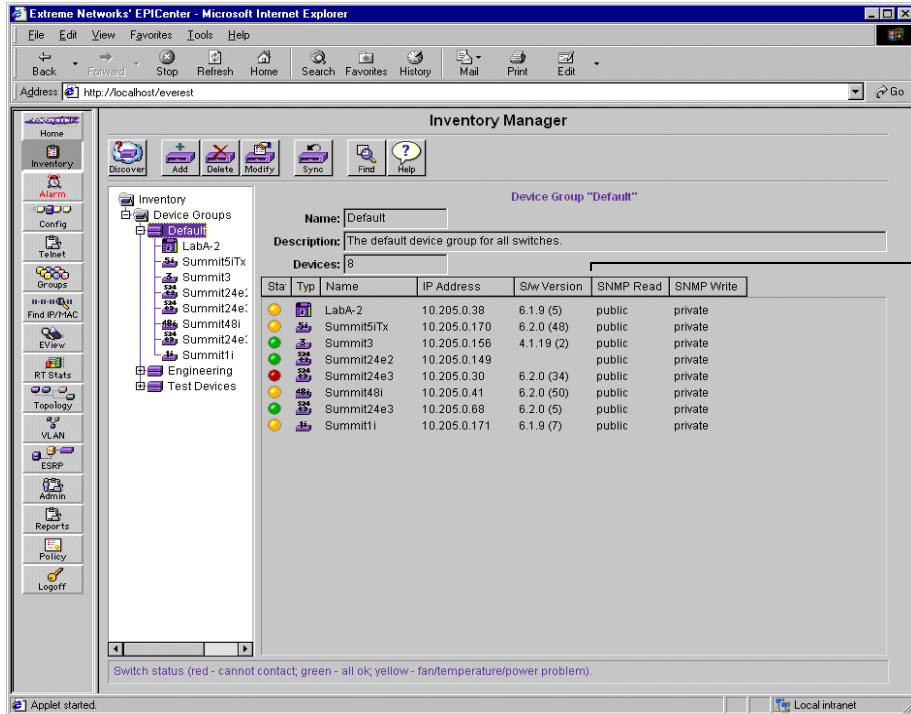
For example, in the Inventory Manager, the Component Tree shows all the Extreme and third-party devices known to the EPICenter. In the VLAN Manager, the Component Tree displays VLANs, as shown in Figure 3-7. In the Topology view, the Component Tree shows the nested maps within a topology view.

If a component in the tree has a plus sign to its left, that means there are subcomponents nested below it. For example, if the component is a VLAN, then it has Extreme switches as subcomponents. The switches, in turn, have ports as subcomponents.

- ◆ Click on the **plus** sign to display the nested subcomponents.  
The plus sign changes to a minus sign.
- ◆ Click on the **minus** sign to hide the subcomponent list.

## The Status/Detail Information Panel

The right side panel displays information about the component selected in the tree on the left. For example, Figure 3-8 shows the Inventory Manager applet, with basic information about the devices known to the EPICenter.



**Figure 3-8:** Inventory Manager applet

- ◆ Click on a component in the Component Tree to display information about that component.

In Figure 3-8, the selected component is the Default device group. The component status/detail panel displays summary status information about each device in this device group.

A red circle with the white “S” next to a device indicates that the device is not reachable through SNMP. This indicator may appear in any of the applets where a list of switches is displayed.

The buttons and frame contents change depending on which applet you are viewing, and also on the permissions associated with your user account.

## Moving the Component Tree Boundary

You can move the boundary between the Component Tree panel and the main applet panel by following these steps:

- 1 Place the cursor over the line separating the panels.
- 2 Click and hold the left mouse button to “grab” the panel separator.
- 3 Drag the separator until the panels are the desired widths.

## Resizing and Sorting Columns

In a wide columnar display such as shown in Figure 3-8, you can resize the widths of each column. To do this, follow these steps:

- 1 Place the cursor over the line separating the column you want to resize from the column to its right.
- 2 Click and hold the left mouse button to “grab” the column separator.
- 3 Drag the separator until the column is the desired width.

You can sort the rows of a columnar display according to the contents of any individual column.

- ◆ To sort the rows, click on the column heading you want to use as the sort criteria. Click once to sort in ascending order; click a second time to reverse the sort order.

In most applets, the column that is currently being used as the sort criteria is indicated with a small triangle in the cell with the column heading. The direction of the triangle (facing up or facing down) indicates whether the sort is ascending or descending.

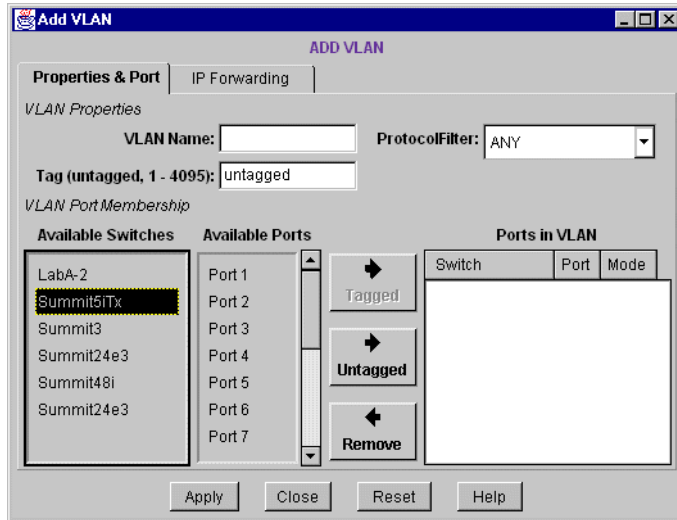
## Applet Function Buttons

For most EPICenter applets, stand-alone buttons at the top of the applet frame provide access to the functions provided by the current applet. Each button invokes a pop-up dialog box for the function, as shown in Figure 3-9.



*If you have Monitor access, some or all of the buttons in a given applet are not available to you. For example, in the VLAN Manager, a user with Monitor access can view information about the components in the Component Tree, but cannot Add, Delete, or Modify VLANs, or perform any port configurations.*





**Figure 3-9:** Pop-up dialog box for adding a VLAN in the VLAN Manager

A dialog box can contain the following types of fields:

- **Page tabs**, such as the **Properties & Port** and **IP Forwarding** tabs in Figure 3-9. These are used when there are multiple pages of settings for a specific function. Clicking a tab displays its page.
- **Text fields**, such as the **VLAN Name** field in Figure 3-9. Enter text or numbers by clicking in the field and then typing.

To clear a value from a text field, highlight the value with the cursor and press the Del or Backspace key on the keyboard. You can also highlight the value and just type a new value over the old one.

- **Drop-down menu fields**, such as the **Protocol Filter** field in Figure 3-9. Click in the field to drop down a menu of choices, then click on your selection to enter the value into the field.
- **List box fields**, such as the **Available Switches** field in Figure 3-9. Click to highlight a value in the field. Click again to unselect a value.

If there are more entries in the list than can be displayed in the box, a scrollbar is provided at the right side of the field.

Some list boxes allow multiple selections. Simply click on multiple items to select them. You can also use [Shift]-click to select the first and last items in a group of contiguous items; all the items between your first and last selection will be highlighted.

To have the settings you've entered take effect, many dialog boxes provide an **Apply** button. This saves the settings on the page you are viewing, but the dialog box remains open so you can make additional changes or change the settings on one of the other pages. For example, you can specify a new VLAN on the **Properties & Ports** page as shown in Figure 3-9, click **Apply** to commit those settings, then display the **IP Forwarding** settings and make changes on that page.

Other dialog boxes may provide a button that executes the function of the dialog, such as **Add**, or **Delete**. Like the **Apply** button, these often perform the function but leave the dialog box open so you can perform additional operations.

Most dialog boxes also provide a **Close** button you can use to exit the dialog box when you are finished.

In addition, most dialog boxes provide a **Reset** button. This typically restores the dialog box to the state it was in when it was invoked, clearing any selections on the screen and resetting the data to the current information from the EPICenter database.

## Printing from EPICenter

Printing is not supported in most of the EPICenter applets. The exceptions are the RT Stats and Topology applets, which each provide a print function, and the HTML-based reports (the Network Summary report and the Reports described in Chapter 15).

You can print the HTML reports using the browser print button. However, you should click in the panel where the report is displayed to ensure that only that panel will be printed. If you print without doing this, the Navigation Toolbar may not be refreshed, and you will need to refresh the client manually.

## Running the EPICenter Server in Scalable Mode

Scalable mode allows you to manage a very large number of devices using the EPICenter server while still maintaining reasonable response and performance. The trade-off is that some of the EPICenter applets described later in this chapter will not be available in Scalable Mode. These include:

- ExtremeView
- Real-Time Statistics
- Topology

- VLAN Manager
- ESRP Manager
- Policy Manager (an optional, separately-licensed module)

To set EPICenter into Scalable Mode, you must log into the client, set the Scalable Mode property to enable scalability (it is disabled by default), and then stop and restart the EPICenter server. The steps to do this are as follows:

- 1 Launch the ExtremeWare EPICenter client, following the instructions in the section “Launching the ExtremeWare EPICenter Client” on page 3-4.
- 2 Click the **Admin** button in the Navigation Toolbar to launch the Admin applet.
- 3 Click the **Server Properties** tab, then select **Scalability** from the pull-down menu (for more detailed instructions, see Chapter 15, “Administering EPICenter.”)
- 4 Click the checkbox to enable Scalable Mode.
- 5 From the Navigation Toolbar, click Logoff to exit the EPICenter client.
- 6 Follow the instructions in the sections earlier in this chapter on shutting down and restarting the EPICenter server.

For Windows NT or 2000, see “Shutting Down the EPICenter Server Components” on page 3-2 and “Starting the EPICenter Server” on page 3-2. If you are running the EPICenter server components as services, see “Restarting the EPICenter Server Components as Services” on page 3-3.

For Solaris, see “Shutting Down the EPICenter Server Components” on page 3-4 and “Starting or Restarting the EPICenter Server” on page 3-3.

When the EPICenter server restarts, it will be running in Scalable Mode, and the icons will be greyed out in the Navigation Toolbar for the applets that are not supported in Scalable Mode.

# 4

## Using the Inventory Manager

---

This chapter describes how to use the ExtremeWare EPICenter Inventory Manager applet for:

- Viewing the EPICenter device inventory
- Discovering network devices
- Adding network devices to the EPICenter database
- Modifying device contact parameters
- Deleting a device from the EPICenter database
- Updating device information in the database
- Finding specific network devices in the database

### Overview of the EPICenter Device Inventory

The Inventory Manager applet keeps a database of all the network devices managed by EPICenter. EPICenter can discover any devices running MIB-2 compatible agents. It can manage Extreme switches, and a number of third-party devices.

The EPICenter software provides an automatic discovery function. This feature can discover Extreme and MIB-2 compatible devices by specific IP address or within a range of IP addresses.

You can also add network devices to the EPICenter database manually, using the Inventory Manager **Add** function. Once a network device is known to the EPICenter database, you

can assign it to a specific device group, and configure it using the Inventory Manager, VLAN Manager, Configuration Manager, Interactive Telnet, ExtremeView, or the optional Policy Manager. You can receive alarms about faults on the device, and you can view a hierarchical topology layout of the devices known to the Inventory Manager.

Any EPICenter user can view status information about the network devices currently known to EPICenter. Users with Administrator or Manager access can run Discovery, and add devices to or delete devices from the list of managed devices in the database. These users can also explicitly refresh the information in the database related to the devices that the EPICenter is managing.

## Device Groups

Devices in the EPICenter are organized into one or more *device groups*. A device group is a set of network devices that have something in common, and that can be managed as a group. For example, devices might be grouped by physical location (Building 1, Building 2, first floor, second floor) or by functional grouping (engineering, marketing, finance) or by any other criteria that makes sense within the managed network environment.

An individual device must belong to one, and only one, device group. All devices become members of a device group when they are added to the EPICenter database, either through Add Devices or as a part of the Discovery process. By default, devices are added to the device group “Default,” if you do not specify otherwise. A device may then be moved to another device group as appropriate.

## Gathering Device Status Information

The EPICenter retrieves information about the devices it manages in several ways:

- EPICenter uses SNMP polling for the IP addresses specified in a Discovery request to retrieve the status information needed by the various EPICenter applets.
- When a switch is added manually to the EPICenter database, EPICenter uses SNMP to retrieve status information needed by the various EPICenter applets.
- Extreme switches send SmartTraps to EPICenter whenever a change occurs in a switch status variable in which the EPICenter has registered interest. These include changes to operating variables as well as configuration changes made through other management entities such as the switch command line interface or ExtremeWare Vista.

These traps are based on a set of SmartTraps rules that the Inventory Manager creates on the switch when it is added to the switch inventory. The rules tell the switch what events or changes EPICenter wants to be notified about. The rules are created on the

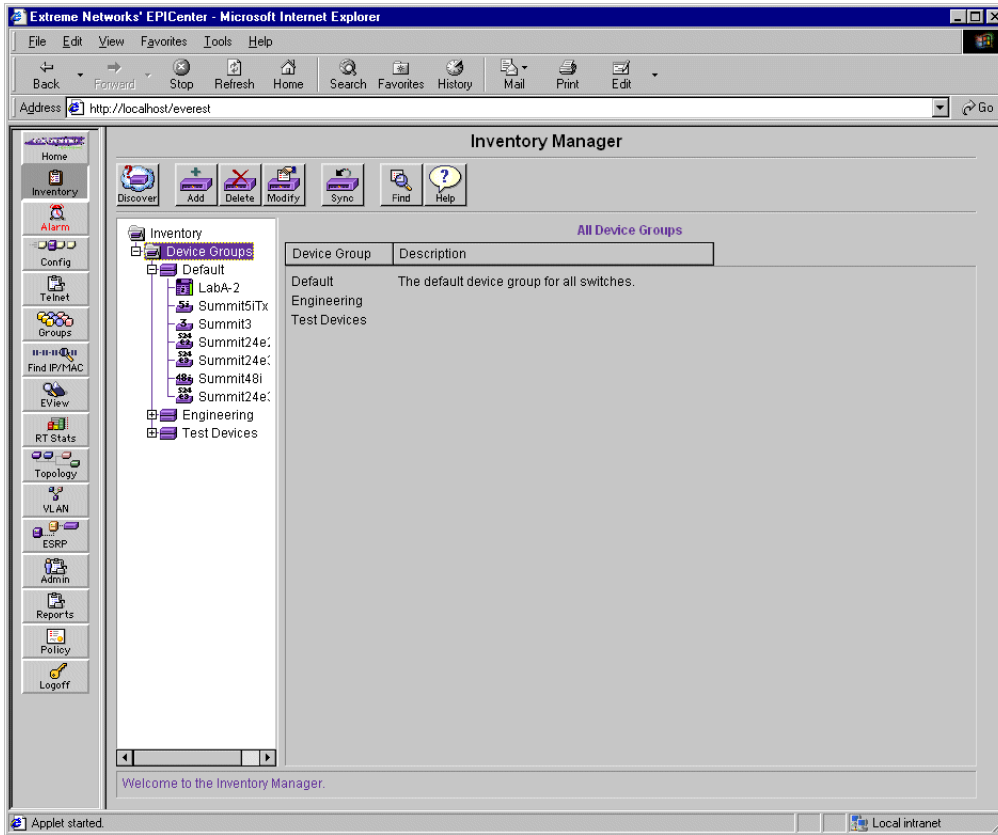
switch using SNMP. EPICenter also adds itself on the switch as a trap receiver. The switch uses the SmartTraps rules to determine what traps to send to EPICenter.

When EPICenter receives a trap from a switch, it then polls the switch for detailed status information.

- EPICenter polls every network device periodically (approximately every five minutes by default) to update basic switch status, which is a subset of the status and configuration information kept in the database. This poll interval is set globally for all devices being managed by the EPICenter server, and can be changed through the Server Properties settings in the Administration applet. See “Server Properties Administration” in Chapter 15.
- The EPICenter server polls each device periodically for detailed status information. This is done much less frequently than the basic status polling—by default, once every 30 minutes for core (chassis) devices, and once every 90 minutes for edge devices. This poll interval can be set individually for devices through the Modify Device interface in the Inventory applet (see the discussion “Modifying a Device” on page 4-18).
- A user with Administrator or Manager access can use the **Sync** command from the Inventory Manager. **Sync** is a manual update of the regular data gathering mechanisms, for use when the users believes that the device configuration or status is not correctly reported in EPICenter applets. **Sync** causes EPICenter to poll the switch and update *all* configuration and status information. During a **Sync** operation the SmartTraps rules are also reset in case the user has accidentally deleted the trap receiver or any SmartTrap rules.

## Displaying the Network Device Inventory

When you click the **Inventory** button in the Navigation Toolbar, the main Inventory Manager page appears as shown in Figure 4-1.



**Figure 4-1:** The Inventory Manager applet, main page



*You must add network devices to the database using Discovery or the Add Devices function in order to make them “known” to the EPICenter. Until this is done, no devices are displayed in the Inventory Manager.*

The Device Groups currently defined in the EPICenter database are displayed in the Component Tree in the left panel.

The panel on the right shows the All Device Groups page, a list of the currently defined device groups with their descriptions.

The first time you run EPICenter, there is only one device group, **Default**. You cannot delete or change the name of the Default device group.

Click on the plus sign to the left of a Device Group name to display the list of switches that are members of that group.

A red circle with a white “S” next to a device indicates that the device is not reachable through SNMP.

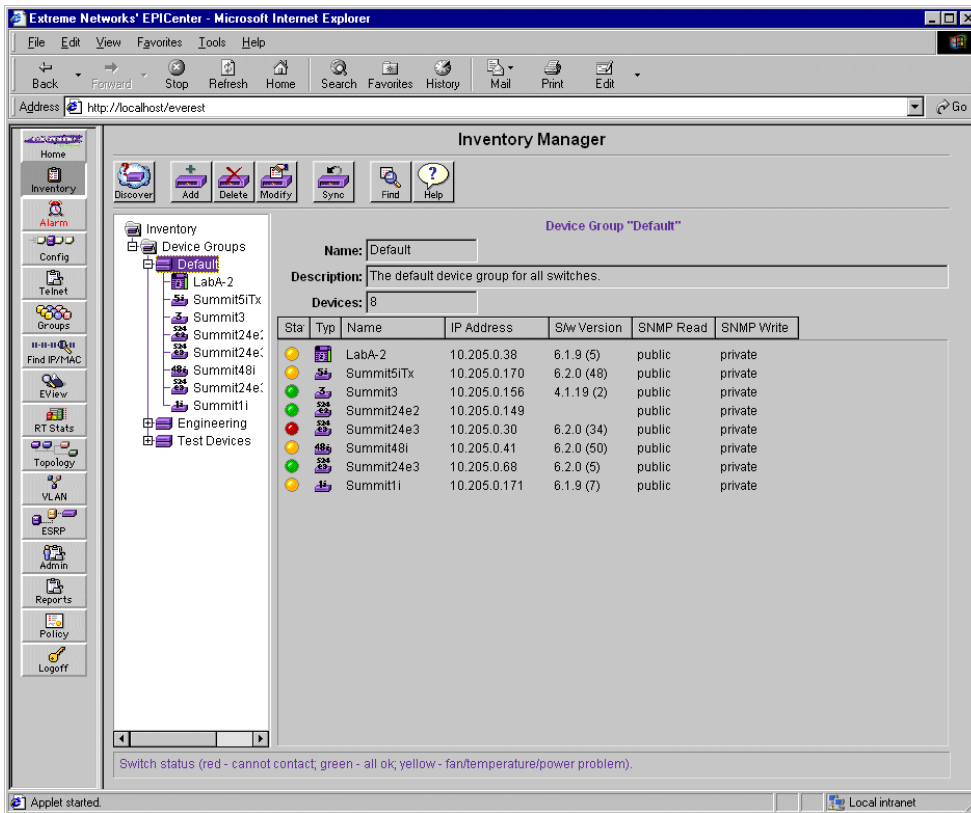
The buttons at the top of the page provide the following functions:

- **Discover** lets you find network devices by IP address or range of addresses
- **Add** lets you add individual devices and device groups to the database
- **Delete** removes a device or device group from the database
- **Modify** lets you change the members of a device group, or update a device’s contact parameters in the database
- **Sync** updates the EPICenter database with current device configuration and status information
- **Find** searches for devices by name, IP address, or device type, and returns information such as the device group to which the device belongs.
- **Help** displays an on-line help page for the Inventory Manager

## Viewing Device Status Information

When you select a device group in the Component Tree, the panel on the right displays a summary status of the devices in the selected device group (see Figure 4-2).





**Figure 4-2:** Inventory Manager device group summary status

- The status “lights” show the status of each device as detected by EPICenter.

**Table 4-1:** Inventory Manager Device Status Indicators

Status Light	Device Status
Green	Device is up and OK
Yellow	Device is responding, but reports an error condition such as a fan or power supply failure, or excessive temperature
Red	Device is not responding to EPICenter status queries. This may mean that the device is down, that it is unreachable on the network, or that the SNMP community strings have changed and EPICenter can no longer contact the switch.

- The name and type of the device are detected by EPICenter.
- The IP address and read/write community strings are also detected by the EPICenter discovery, or are those entered into the EPICenter database manually if the switch was added using the Add command.

Select a switch in the Component Tree on the left to display detailed configuration and status information, as shown in Figure 4-3. This display shows additional information that EPICenter has gathered from the switch agent.

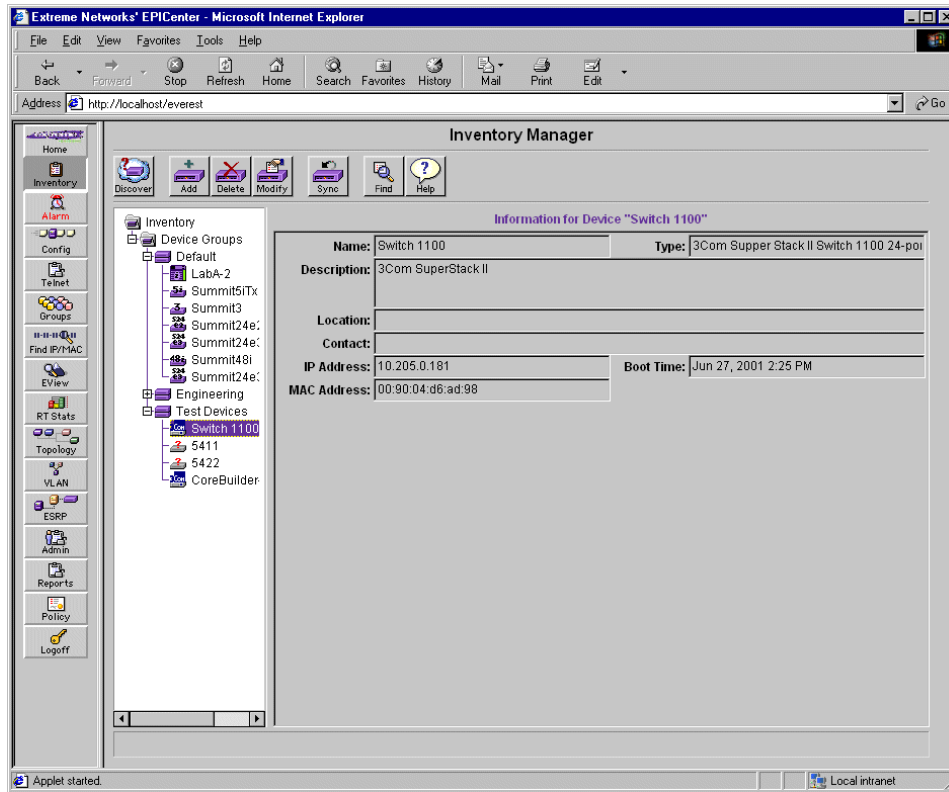
The screenshot shows the EPICenter Inventory Manager interface. On the left is a navigation pane with a tree view showing the hierarchy: Inventory > Device Groups > Default > LabA-2 > Summit51Tx. The main area displays 'Information for Device "Summit51Tx"'. The data is organized into several sections:

<b>Name:</b>	Summit51Tx	<b>Type:</b>	Extreme Summit 51 TX	
<b>Description:</b>	Summit51Tx- Version 6.2.0 (Build 48) by alin 08/03/0115:23:02			
<b>Location:</b>				
<b>Contact:</b>	support@extremenetworks.com, +1 888 257 3000			
<b>IP Address:</b>	10.205.0.170	<b>Boot Time:</b>	Aug 21, 2001 11:32 AM	
<b>Primary:</b>	6.1.5b20	<b>Secondary:</b>	6.2.0b48	
<b>Current:</b>	6.2.0 (48)	<b>OoS Mode:</b>	Ingress	
<b>Fans:</b>	fan 1 failed , fan 2 failed , fan 3 failed ; f		<b>Temperature:</b>	50 deg Centigrade
<b>MAC Address:</b>	00:01:30:6c:0d:00		<b>Power:</b>	power 2 present not ok
<b>System ID:</b>	800078-11-0035M02442		<b>Board ID:</b>	
<b>Other Board IDs:</b>				

At the bottom of the interface, there is a status bar with 'Applet started.' on the left and 'Local intranet' on the right.

**Figure 4-3:** Inventory Manager device status information

The information displayed in Figure 4-3 is for an Extreme switch. The ExtremeWare software running in the switch provides comprehensive status information through the Extreme MIB. Figure 4-4 show the information displayed for a Cisco device—a subset of the information available for an Extreme device.



**Figure 4-4:** Inventory Manager information for a 3Com device

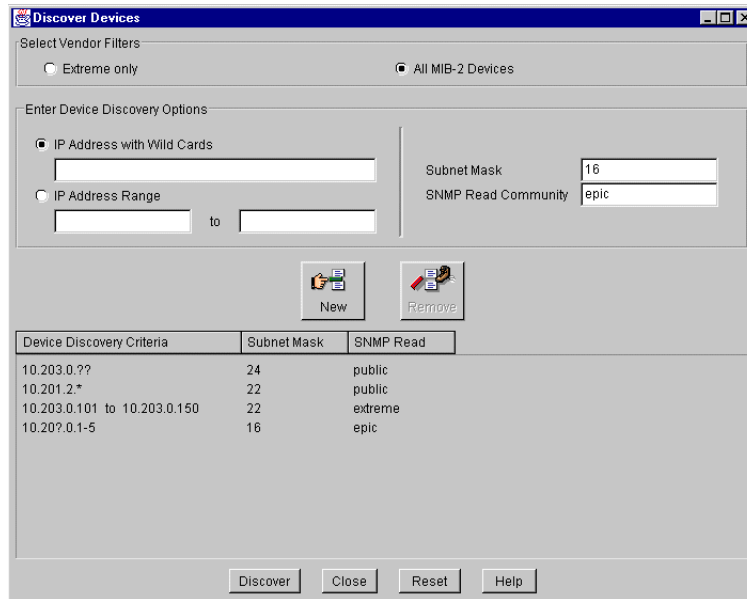
You can select a device group or a device in the Component Tree, then right-click to display a pop-up menu that contains the Modify, Delete, and Sync commands. These perform the same functions as the buttons at the top of the page, but with the appropriate device or device group displayed.

## Discovering Network Devices

EPICenter provides an automatic Discovery function that lets you discover network devices by IP address.

To discover network devices, do the following:

- 1 Click the **Discovery** button at the top of the Inventory Manager main window.  
The Discover Devices window, shown in Figure 4-5, is displayed.



**Figure 4-5:** Inventory Manager Device Discovery set up window

- 2 Click the appropriate boxes to select the types of devices you want to include in the discovery. You can discover Extreme devices only, or all devices with MIB-2 compatible agents.
- 3 Specify the device address range you want to discover. You may specify the range in one of two ways:

- As an **IP Address with Wildcards** (such as 10.203.10.\* or 10.203.?.??)

Valid wildcard characters are \*, ?, and - (dash):

- \* acts as a wildcard for the entire octet (0-255)

- ? is a wildcard for a single digit (0-9)

- lets you specify a range for any octet. You can use this in more than one octet



*You cannot combine the dash with another wildcard in the same octet.*

You can also use the IP Address with Wildcards field to specify a single IP address.

**Examples:**

<b>IP Address Specification</b>	<b>Addresses Generated</b>
10.203.0.*	polls 10.203.0.0 through 10.203.0.255
10.203.?.??	polls 10.203.0.0 through 10.203.9.99
0.203.0.1? or 10.203.0.10-19	both specify the same range: 10.203.0.10 through 10.203.0.19
10.203.0-2.10-30	polls 10.203.0.10 through 10.203.0.30 10.203.1.10 through 10.203.1.30 10.203.2.10 through 10.203.2.30

— As an **IP address Range** (such as 10.203.10.20 to 10.203.10.45)



*There are certain IP addresses that are reserved. You should not include these addresses in your discovery.*

- *Class A networks: 0 and 127 are reserved.*
- *Class D networks: 224 - 239 are reserved for multicasting.*
- *All addresses above 239 are reserved.*
- *255 is reserved for broadcast datagrams for either the host or network portion of the IP address.*

*In addition, certain host addresses may be interpreted as broadcast addresses, depending on the subnetting of your network.*

*IP addresses are processed prior to starting the discovery, and IP addresses that contain 255's in the host portion are eliminated. This is based on the IP address as well as the subnet mask.*

- 4** Specify (or verify) the **Subnet Mask** size as appropriate. The value in the Subnet Mask field is the number of bits to be masked, starting from the high-order (left-hand) octet. The default subnet mask of 24 will mask the three high-order octets.
- 5** Specify (or verify) the **SNMP Read Community** string so that EPICenter will be able to retrieve information from any devices it discovers.
- 6** Click the **New** button to add the range into the **Device Discovery Criteria** list.
- 7** Repeat steps 3 through 6 to specify any additional device addresses or ranges for the discovery.

- 8 If necessary, you can remove an address range from the Device Discovery Criteria list at any time before you initiate the discovery by selecting the range and clicking the **Remove** button.

You can remove all address ranges using the **Reset** button at the bottom of the page.

- 9 Click the **Discover** button at the bottom of the window to initiate the discovery.

If the discovery criteria results in a discovery of more than 1500 devices, a dialog appears informing you of the number of items in your search request, and asking you for confirmation. Click **Yes** to proceed or **No** to refine the discovery criteria.



*If a discovery request is too large, your browser may not have sufficient memory resources available to handle it. It is recommended that you break a large discovery task into multiple separate tasks.*

A Discovery Results window is displayed as soon as the discovery process begins, as shown in Figure 4-6. The panel at the bottom of the window shows the progress of the discovery and displays status messages for each device it finds as it works through the set of IP addresses you have specified.

The screenshot shows a window titled "Discovery Results" with a close button (X) in the top right corner. Below the title bar, there is a message: "Please select one or more devices from the list, then click the 'Add' button." Below this is a table with the following columns: Device Name, MAC Address, IP Address, SNMP Read, Device Type, and Status. The table contains 14 rows of data. Below the table is a progress bar showing 100% completion. Underneath the progress bar, it says "Total number of devices discovered is: 14". At the bottom of the window, there are five buttons: "Add", "Close", "Hide Details", "Reset", and "Help". Below the buttons, there is a text area with the following content: "Timeout on: 10.205.0.228", "Timeout on: 10.205.0.229", "Timeout on: 10.205.0.230", "Command was executed successfully.", "Select the devices listed above and click the 'Add' button to add them to the Inventory Manager.", and "You can also, change any device attributes by making modifications in the 'Modify' dialog."

Device Name	MAC Address	IP Address	SNMP Read	Device Type	Status
Summit48i	00:01:30:ca:83:10	10.205.0.41	public	Summit 48i	Added
MSM64	00:00:00:00:00:00	10.205.0.64	public	MSM64i	Error
Summit24e3	00:01:30:11:00:46	10.205.0.68	public	Summit 24e3	Added
Summit24e2	00:01:30:10:00:19	10.205.0.149	public	Extreme Summit 24e2	Already Managed
Summit3	00:e0:2b:03:3c:00	10.205.0.156	public	Summit 3	Already Managed
Summit3	00:e0:2b:05:30:00	10.205.0.161	public	Summit 3	Error
Summit5i	00:01:30:6c:4b:00	10.205.0.168	public	Summit 5i SX	Error
Summit5iTx	00:01:30:6c:0d:00	10.205.0.170	public	Summit 5i TX	Already Managed
Summit1i	00:01:30:6c:30:00	10.205.0.171	public	Summit 1i SX	Added
Summit48i	00:01:30:e7:f2:00	10.205.0.199	public	Summit 48i	Error

**Figure 4-6:** Results of a discovery, with details visible

- Click the **Hide Details** button at the bottom of this window to hide the detail display.

— Click **View Details** to re-display the discovery details.

When the discovery has completed, the set of discovered devices is listed in the top panel of the Discovery Results window.



*These devices are NOT automatically entered into the EPICenter database. You must explicitly select and add devices to the database.*

**10** To add devices to the ExtremeWare EPICenter database, select individual devices or a range of devices in the Results list, and click the **Add** button at the bottom of the window.



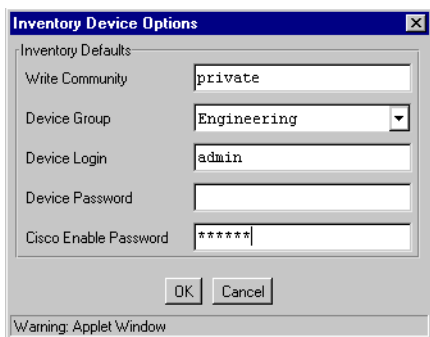
*If you select multiple devices, make sure the devices you select are similarly configured. As part of the Add process, you will be asked for a **single** password that will apply to all the selected devices. If the password is specified incorrectly for any of these devices, the add will fail for those devices.*

**11** A window pops up where you must set additional device options such as a write community string, the device group to which the devices should be added, and a default device login and password (see Figure 4-7). If there are Cisco devices among the set being added, you must also enter a Cisco enable password.

Enter or make changes to any of these fields. These options will apply to the entire set of devices you are adding.



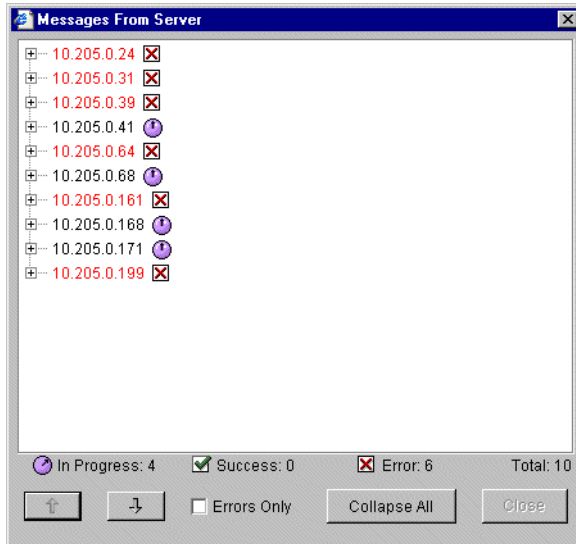
*Make sure the device passwords are correct for the selected devices. If you are adding multiple devices in one operation, make sure the passwords you specify are correct for each device. A device cannot be added if the password is not correct.*




**Figure 4-7:** Setting default device options for discovered devices



**12** Click **OK** to proceed with the Add process.

A message window (shown in Figure 4-8) pops up to show you the progress of the Add command.



**Figure 4-8:** Message window showing Add Device progress

Devices are listed followed by a small purple rotating clock icon  while the add function is in progress.

- When a device has been successfully added, the clock turns into a green checkmark .
- If the device cannot be added, the clock turns into a red X in the checkbox  and the device name is displayed in red.

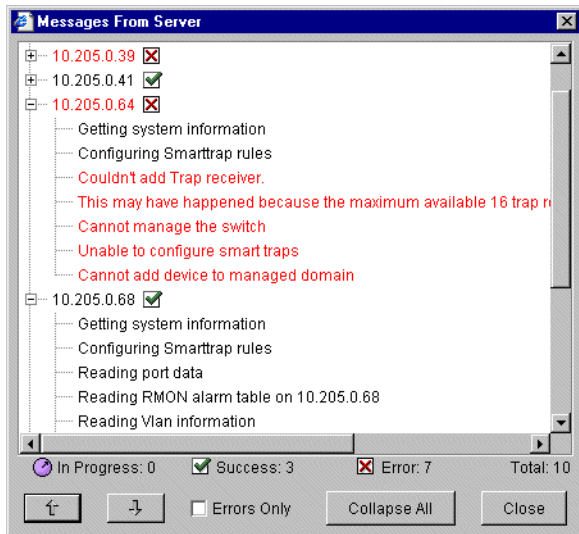
The indicators just below the tree area of the window show the number of devices currently in each state.

To see the messages related to an Add function (either successful or unsuccessful), select a device in the list. The messages related to the device are displayed as lines under the device node, as shown in Figure 4-9.

- Click the plus sign at the left of the device name to display server messages related to adding the device.
- Click the minus sign at the left of the device to hide the server messages.



- The up and down arrow buttons let you move up and down the device tree, displaying the server messages associated with each device.
- If you check the **Errors Only** box, the up and down arrow buttons will expand only devices that had errors.
- The **Collapse All** button collapses all the device nodes, hiding all the server messages.



**Figure 4-9:** Message window showing errors from the Add Device process



*If you close the Discovery Results window without adding devices, the results for devices not already in the ExtremeWare EPICenter database are lost. You must perform a discovery again to regenerate information on those devices.*

After the Add has finished, the Discovery Results window is re-displayed. You can select more devices and specify a different set of Inventory Device Options, and add those devices to the Inventory Manager.

## Adding Devices and Device Groups

Users with Administrator or Manager access can add devices to the EPICenter database, and create Device Groups. If you have Monitor access only, you may not use this function.

## Adding a Device

- 1 Click the **Add** button at the top of the Inventory Manager main window.

Select the appropriate tab to display the Add Device window, as shown in Figure 4-10.

The screenshot shows the 'Add Devices and Device Groups' window. The 'Device' tab is active. The 'Device Information' section includes the following fields:

- IP Address: 10.203.0.56
- SNMP Read: public
- SNMP Write: private
- Device Login: admin
- Device Password: \*\*\*\*\*
- Device Group: Default
- Cisco Enable Password: (empty)

Below the fields are 'New' and 'Remove' buttons. At the bottom of the window, there is a table with one row of data:

IP Address	SNMP Read	SNMP Write	Device Login	Device Group
10.203.0.41	public	private	admin	Default

At the bottom of the window are 'Add', 'Close', 'Reset', and 'Help' buttons.

**Figure 4-10:** Add Device window in the Inventory Manager

- 2 Enter the device IP address, community strings, device login and password into the appropriate fields. These are the parameters that EPICenter uses to access the switch. You may also enter a DNS-resolvable host name in place of the Switch IP address.
- 3 Select the device group to which this device should belong. It can belong to only one device group. **Default** is the default group for managed devices.
- 4 To clear the contents of the fields and reset them to their default values, click **Reset**.
- 5 To add the new device into the database, click **Add**.

When you click **Add**, the Inventory Manager adds the devices to the database. It makes a set of SNMP requests to retrieve data that is needed from the devices by EPICenter applets. If the device is an Extreme switch, it also creates a set of SmartTraps rules that tell the switch what status and configuration changes are of interest to EPICenter.

## Creating a Device Group

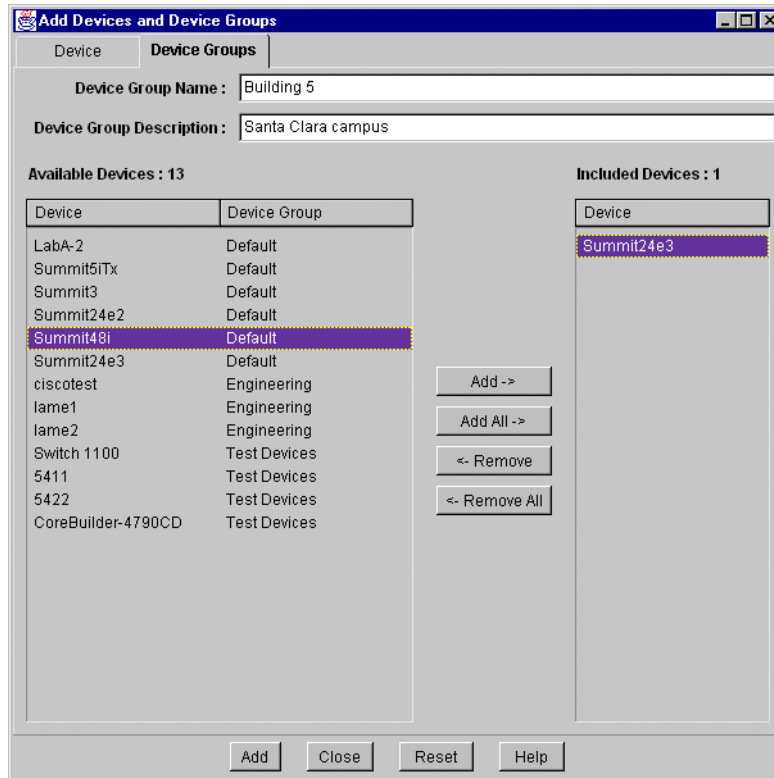
Device groups are sets of managed network devices that have something in common, and that can be managed as a group. For example, devices might be grouped by physical location (Building 1, Building 2, first floor, second floor), by department (engineering, marketing, finance), or by any other criteria that makes sense within the managed network environment.

Every device belongs to one, and only one, device group. All devices become members of a device group when they are added to the EPICenter database, either through Add Devices or as a part of the Discovery process. A device may then be moved to another device group as appropriate.

One device group may contain a maximum of 100 devices.

To create a new device group, follow these steps:

- 1 Click the **Add** button at the top of the Inventory Manager main window.  
Select the appropriate tab to display the Device Groups window, as shown in Figure 4-11.



**Figure 4-11:** Add Device Group window in the Inventory Manager

- 2 Type a name for the device group into the **Device Group Name** field, and a description (optional) into the **Device Group Description** field.
- 3 To add a device to the selected device group, select the device in the Available Devices list and click **Add ->**. To add all devices in the Available Devices list, click **Add All ->**.
- 4 To remove a device from the device group, select the device in the Included Devices list, and click **<- Remove**. The device will be moved from the selected device group to the Default device group. To return all devices in the Included Devices list to the Default device group, click **<- Remove All**.
- 5 Repeat steps 3 and 4 until you have included all the devices that should be members of this device group.
- 6 To add the list of newly created device groups to the database, click the **Add** button at the bottom of the window.

# Modifying Devices and Device Groups

You can use the Modify function to modify the access parameters for an individual device, or to add and delete members of a device group. Users with Administrator or Manager access can modify device contact information and device groups.

If you have Monitor access only, you cannot use this function.

## Modifying a Device

You can begin the modify function using the **Modify** button on the toolbar, or by selecting a device in the Component Tree, right-clicking to display the pop-up menu, and selecting Modify Device.

To modify the contact information for a managed device in the database, do the following:

- 1 Click the **Modify** button at the top of the Inventory Manager main page.

Select the appropriate tab to display the Modify Device window, as shown in Figure 4-12.

**Modify Devices and Device Groups**

Devices | Device Groups

Please select a device to modify its contact information.

Device Name	IP Address	Device Type	SNMP Read	SNMP Write	Device Login	Poll Interval
Summit48i	10.205.0.41	Extreme Summit 48i	public	private	admin	90
Summit24e3	10.205.0.68	Extreme Summit 24e3	public	private	admin	90
LabA-2	10.205.0.38	Extreme Alpine 3808	public	private	admin	30
Summit5iTx	10.205.0.170	Extreme Summit 5i TX	public	private	admin	90
Summit3	10.205.0.156	Extreme Summit 3	public	private	admin	90
ciscotest	10.205.0.50	Cisco 4500	public	private	jim	90
lame1	10.205.0.51	Generic Cisco	public	private	admin	90
lame2	10.205.0.52	Generic Cisco	public	private	admin	90
Summit24e2	10.205.0.149	Extreme Summit 24e2t	public	private	admin	90
Summit24e3	10.205.0.30	Extreme Summit 24e3	public	private	admin	90

Device IP Address: 10.205.0.68

SNMP Read Community String: public

SNMP Write Community String: private

Device Login: admin

Device Contact Password: \*\*\*\*\*

Device Poll Interval (minutes): 90

Cisco Enable Password:

Modify Close Reset Help

**Figure 4-12:** Devices tab of the Modify Devices and Device Groups window

- 2 Select the device for which you want to change contact information.
- 3 Enter the changed information in the appropriate fields.

The **Device Login** and **Device Contact Password** are the login and password needed in order to Telnet to the device or to use ExtremeWare Vista.

The **Device Poll Interval** lets you specify how frequently the EPICenter server should poll the for detailed device information, such as software version, bootrom version, and so on. This also includes EDP and ESRP information for non-"i" series devices. To avoid a potentially large amount of polling traffic, this detailed polling is only done every 30 minutes for core (chassis) devices, and every 90 minutes for edge devices. You can change this detailed polling interval by entering a different value in this field.



*Note that the Device Poll Interval set here is different from the global Poll Interval you can set in the Administration applet. The global poll interval controls the basic status polling needed to ensure SNMP reachability, and is typically done much more frequently than detailed device polling.*

- 4 Click **Modify** to add the changed information to the ExtremeWare EPICenter database.
- 5 Click **Cancel** to cancel the Modify process.



*If you change the community string for a device so that it no longer matches the string configured in the device, EPICenter will no longer be able to communicate with the device. For Extreme devices, EPICenter will display an error message, but it will not necessarily do so for third-party devices. To avoid this problem, change the community string on the device first, then change it in EPICenter.*

## Modifying a Device Group

Devices are always a member of a device group; devices not explicitly assigned to another device group are members of the Default device group. This has two effects related to modifying device groups:

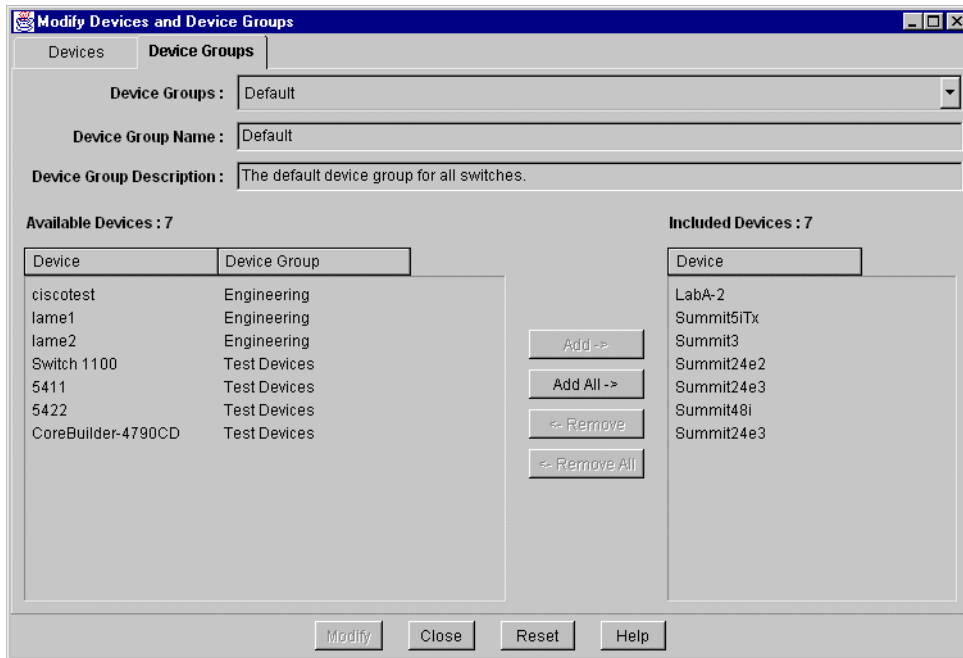
- When devices are removed from a device group, they are automatically added to the Default device group
- Devices cannot be removed from the Default device group using the Remove button in the Modify dialog. To remove a device from the default device group, you must add it to another device group.

You can begin the modify function using the **Modify** button on the toolbar, or by selecting a device group in the Component Tree, right-clicking to display the pop-up menu, and selecting Modify Device Group.

To add or remove devices in a device group, do the following:

- 1 Click the **Modify** button at the top of the Inventory Manager main page.

Select the appropriate tab to display the Modify Device Group window, as shown in Figure 4-13.



**Figure 4-13:** Device Groups tab of the Modify Devices and Device Groups window

- 2 Select the device group you want to modify. The Included Devices list displays the devices that are currently members of this group. The Available Devices list displays the other devices known to EPICenter, and their current device group membership.
- 3 To change the name or description of the group, type the new text into the **Device Group Name** and **Description** fields.
- 4 To add a device to the selected device group, select the device in the Available Devices list and click **Add ->**. To add all devices in the Available Devices list, click **Add All ->**.
- 5 To remove a device from the device group and return it to the Default device group, select the device in the Included Devices list, and click **<- Remove**. The device will be moved from the selected device group to the Default device group. To return all devices in the Included Devices list to the Default device group, click **<- Remove All**.

Because devices not otherwise assigned are members of the Default device group, you cannot remove devices from the Default device group. Devices are removed from the Default device group only when they are added to another device group.

- 6 Repeat steps 4 and 5 until you have included all the devices that should be members of this device group.

The **Reset** button will undo all your add and remove actions, and return both the **Available Devices** and **Included Devices** lists to the state they were in when you started the Modify command.

- 7 To replace the modified device group in the database, click the **Modify** button at the bottom of the window.

Moving a device from one device group to another requires two steps. First, remove it from its current device group (returning it to the Default group). Then select the new device group, and move the device from the Default device group to the new group.

## Deleting Devices and Device Groups from the Database

Users with Administrator or Manager access can delete devices and device groups from the EPICenter database. If you have Monitor access only, you cannot access this function.

### Deleting a Device

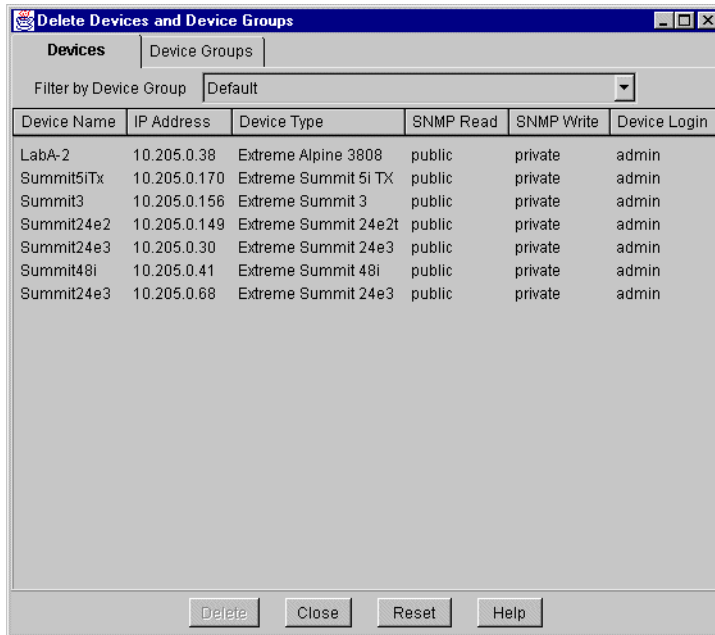
You can begin the delete function using the **Delete** button on the toolbar, or by selecting a device in the Component Tree, right-clicking to display the pop-up menu, and selecting Delete Device.

To delete a device from the EPICenter database, follow these steps:

- 1 Click the **Delete** button at the top of the Inventory Manager main page.

Select the appropriate tab to display the Delete Devices window (see Figure 4-14).





**Figure 4-14:** Devices tab of the Delete Devices and Device Groups window

- 2 To select a device from a specific device group, select the device group from the pull-down list in the **Filter by Device Group** field. Select **All** to view the list of all devices from all device groups.
- 3 Select one or more devices in the Devices list, and click **Delete**.
- 4 Click **OK** to confirm that you want to delete the device information from the database.

Deleting a device removes the information about the device from the EPICenter database. This means that the device can no longer be monitored and managed from the EPICenter application. If the device is an Extreme switch, deleting it removes any SmartTraps rules, both from the database and the switch change table. It also removes all information about VLANs, QoS Policy, and Virtual Chassis connections associated with this switch from the EPICenter database.



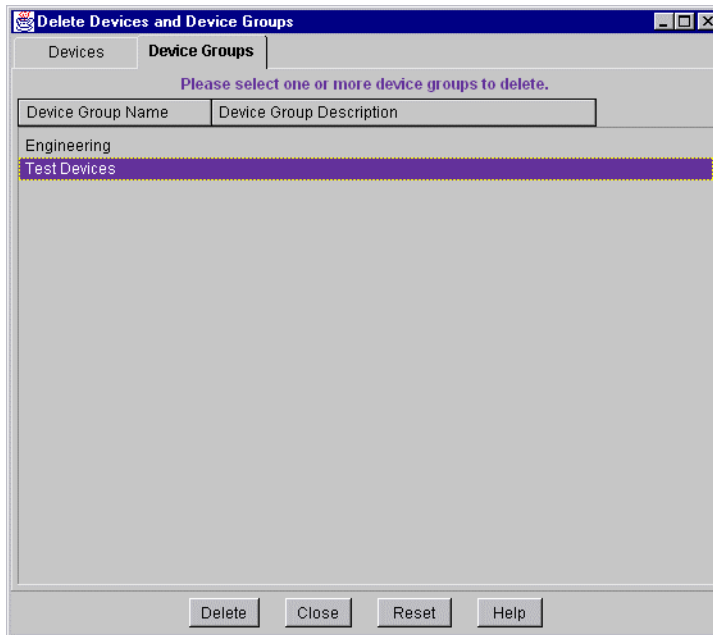
*Deleting a device from EPICenter has no effect on the configuration of the device itself.*

## Deleting a Device Group

You can begin the delete function using the **Delete** button on the toolbar, or by selecting a device in the Component Tree, right-clicking to display the pop-up menu, and selecting Delete Device Group.

To delete a device group from the EPICenter database, follow these steps:

- 1 Click the **Delete** button at the top of the Inventory Manager main page.  
Select the appropriate tab to display the Delete Device Groups window (see Figure 4-15).



**Figure 4-15:** Device Groups tab of the Delete Devices and Device Groups window

- 2 Select one or more device groups in the Device Groups list, and click **Delete**.
- 3 Click **OK** to confirm that you want to delete the device group information from the database.

The devices in the deleted device group automatically become members of the Default device group.

## Updating Device Information

Occasionally, you may want to update the configuration and status information for one or more devices in the EPICenter database. The **Sync** operation is a manual update you can use if you believe that the device configuration is not correctly represented in EPICenter applets. It updates all information for a selected set of devices, except for the contact information.

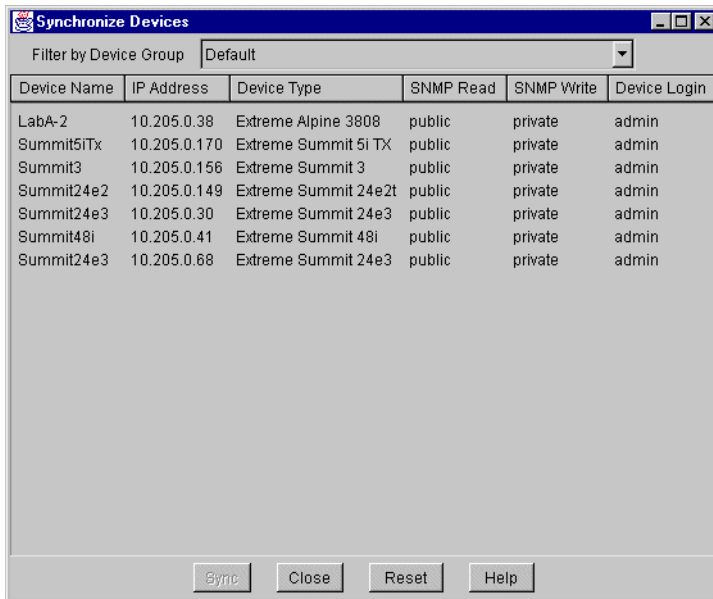
If you have Administrator or Manager access to EPICenter, you can perform a **Sync**. If you have Monitor access only, you can not use this function.

You can begin the synchronize function using the **Sync** button on the toolbar, or by selecting a device or device group in the Component Tree, right-clicking to display the pop-up menu, and selecting the Sync command.

To refresh the configuration and status information, follow these steps:

- 1 Click **Sync** at the top of the Inventory Manager page.

The Synchronize Devices dialog, shown in Figure 4-16, is displayed, listing the devices in the EPICenter database.



**Figure 4-16:** Synchronize Devices dialog

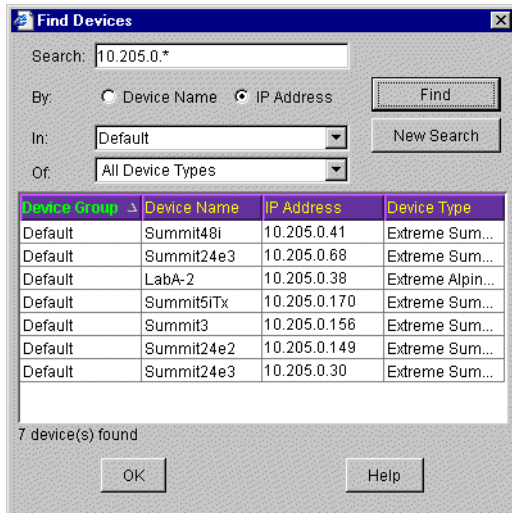
- 2 To select a device from a specific device group, select the device group from the pull-down list in the **Filter by Device Group** field. Select **All** to view the list of all devices from all device groups.
- 3 Select one or more devices in the Device list.
- 4 Click **Reset** at any time prior to initiating the Sync to deselect all device selections and start over.
- 5 Click **Sync** to initiate the synchronization process.  
The Inventory Manager uses SNMP to retrieve configuration and status information from each selected switch, and updates the database with that information.
- 6 The **Sync** function displays a dialog box with status or error information. Click **OK** to continue.

## Finding Devices

You can search for a device in the EPICenter database by name, by IP address, or by type of device. This may be useful if you have a large number of devices in your inventory.

To search for a device, follow these steps:

- 1 Click **Find** at the top of the Inventory Manager page.  
The Find Devices dialog, shown in Figure 4-17, is displayed.



**Figure 4-17:** Find Devices dialog

## 2 Enter your search criteria:

You can search for devices by name or by IP address. You can limit the search to a specific device group, or to a specific type of Extreme device. Search criteria can include:

- A device name. Click the **Device Name** button, and enter a complete or partial name in the **Search:** field.
- An IP address. Click the IP Address button and enter a complete or partial IP address in the **Search:** field. You can use the wild card characters \* or ? in your search criteria.
  - \* acts as a wildcard for an entire octet (0-255)
  - ? is a wildcard for a single digit (0-9)
- A device group. Select the device group from the drop-down menu in the device group field. If you do not specify a name or IP address in the Search field, all devices in the device group you select will be found.
- A device type. Select the device type from the drop-down menu in the type field. If you do not specify a name or IP address in the Search field, all devices of the type you select will be found.

- 3** Click **Find** to search for devices that meet the criteria you have specified. All devices found are listed in the center panel. Information includes the device group in which the device can be found, its name, IP address, and the type of device.
- 4** Double-click on a device in the results table to highlight the device in the Component Tree, and to display the associated status information for that device (see “Viewing Device Status Information” on page 4-5).
- 5** Click **New Search** to clear all search criteria.
- 6** Click **OK** to close the search window.

# 5

# The EPICenter Alarm System

---

This chapter describes how to use the ExtremeWare EPICenter Alarm System applet for:

- Viewing the alarms that have occurred
- Defining new alarms and modifying current alarm definitions
- Configuring RMON and CPU utilization trap conditions on devices
- Configuring EPICenter as a trap receiver

## Overview of the EPICenter Alarm System

The EPICenter Alarm System provides fault detection and alarm handling for the network devices monitored by EPICenter. This includes Extreme devices and some third-party devices—those that EPICenter can include in its Inventory database. The Alarm System provides a set of predefined, enabled alarms that will immediately report conditions such as authentication or login failures, device problems such as power supply or fan failures, reachability problems, or device reboots.

The Alarm System also lets you define your own alarms that will report errors under conditions you specify, such as repeated occurrences or exceeding threshold values. You can specify the actions that should be taken when an alarm occurs, and you can enable and disable individual alarms.

Fault detection is based on Simple Network Management Protocol (SNMP) traps, and some limited polling. The Alarm System supports SNMP Management Information Base-2 (MIB-2), the Extreme Networks private MIB, Remote Monitoring (RMON) traps, and

selected traps from other MIBs. When an alarm occurs you can specify actions such as sending e-mail, running a program, running a script, or sounding an audible alert.



*Extreme Networks devices are configured automatically by EPICenter to send traps to the EPICenter server. To receive traps from non-Extreme devices, you must manually configured the devices send traps to the EPICenter server.*

*Not all trap events are supported in older versions of the ExtremeWare software. Please refer to Appendix D for information on the switch software required for specific traps.*

## The Alarm Log Browser

Click the **Alarm** button in the Navigation Toolbar to run the Alarm System applet and view the Alarm Log Browser. If the **Alarm** button (icon) is displayed in red instead of black, it indicates that a new alarm has occurred.

You can also invoke the Alarm Log Browser from the Topology view.

The Alarm Log Browser page appears, as shown in Figure 5-1.



Predefined filters      Alarm System module tabs

New alarm indicator      Current filter definition      Alarm summary      Acknowledged alarms

ID	Name	Category	Severity	Source	Time	Message	Acked
9758	SNMP Unreacha...	Default	Minor	10.205.0.25	1:37:55 PM 8/8/2...	EPICenter SNMP ...	
9757	SNMP Unreacha...	Default	Minor	10.205.0.25	1:32:25 PM 8/8/2...	EPICenter SNMP ...	
9756	SNMP Unreacha...	Default	Minor	10.205.0.25	1:26:54 PM 8/8/2...	EPICenter SNMP ...	
9755	SNMP Unreacha...	Default	Minor	10.205.0.25	1:21:24 PM 8/8/2...	EPICenter SNMP ...	
9754	SNMP Unreacha...	Default	Minor	10.205.0.25	1:15:54 PM 8/8/2...	EPICenter SNMP ...	
9753	SNMP Unreacha...	Default	Minor	10.205.0.25	1:10:26 PM 8/8/2...	EPICenter SNMP ...	
9752	SNMP Unreacha...	Default	Minor	10.205.0.25	1:09:19 PM 8/8/2...	EPICenter SNMP ...	
9751	SNMP Unreacha...	Default	Minor	10.205.0.32	1:09:18 PM 8/8/2...	EPICenter SNMP ...	
9750	Device Reboot	Default	Warning	10.205.0.156	11:33:11 AM 8/8/2...	EPICenter Device...	
9749	Device Reboot	Default	Warning	10.205.0.171	11:29:27 AM 8/8/2...	EPICenter Device...	
9748	Device Reboot	Default	Warning	10.205.0.50	11:29:11 AM 8/8/2...	EPICenter Device...	
9747	Device Reboot	Default	Warning	10.205.0.32	11:28:42 AM 8/8/2...	EPICenter Device...	
9746	SNMP Unreacha...	Default	Minor	10.205.0.51	7:13:39 PM 8/6/2...	EPICenter SNMP ...	
9745	SNMP Unreacha...	Default	Minor	10.205.0.74	7:12:39 PM 8/6/2...	EPICenter SNMP ...	
9744	SNMP Unreacha...	Default	Minor	10.205.0.51	7:07:38 PM 8/6/2...	EPICenter SNMP ...	
9743	Device Reboot	Default	Warning	10.205.0.52	6:56:57 PM 8/6/2...	EPICenter Device...	
9742	SNMP Unreacha...	Default	Minor	10.205.0.51	6:56:33 PM 8/6/2...	EPICenter SNMP ...	
9741	SNMP Unreacha...	Default	Minor	10.205.0.32	6:47:33 PM 8/6/2...	EPICenter SNMP ...	
9740	SNMP Unreacha...	Default	Minor	10.205.0.50	6:45:03 PM 8/6/2...	EPICenter SNMP ...	
9739	SNMP Unreacha...	Default	Minor	10.205.0.156	6:43:33 PM 8/6/2...	EPICenter SNMP ...	
9738	SNMP Unreacha...	Default	Minor	10.205.0.171	6:42:50 PM 8/6/2...	EPICenter SNMP ...	
9737	Device Reboot	Default	Warning	10.205.0.32	6:39:32 PM 8/6/2...	EPICenter Device...	
9736	Device Reboot	Default	Warning	10.205.0.171	6:37:23 PM 8/6/2...	EPICenter Device...	
9735	Device Reboot	Default	Warning	10.205.0.50	6:37:02 PM 8/6/2...	EPICenter Device...	
9734	Device Reboot	Default	Warning	10.205.0.156	6:35:45 PM 8/6/2...	EPICenter Device...	
9733	Authen Failed	Default	Minor	10.205.0.74	5:58:14 PM 8/6/2...	Snmpp Trap Authe...	
9732	Authen Failed	Default	Minor	10.205.0.74	5:58:14 PM 8/6/2...	Snmpp Trap Authe...	
9731	Authen Failed	Default	Minor	10.205.0.74	5:54:09 PM 8/6/2...	Snmpp Trap Authe...	

**Figure 5-1:** The Alarm Log Browser page

The Alarm Log Browser page displays a summary of the alarms that have occurred, optionally filtered based on criteria you can specify. An alarm can be generated due to an SNMP or RMON trap, or based on the results of a poll.

By default, the Alarm System provides a set of predefined alarms that generate alarm log entries when the following events occur:

- Authentication failure (SNMP MIB-2 trap)

- Invalid login (Extreme proprietary trap)
- Redundant Power Supply alarm condition (Extreme proprietary trap)
- ESRP state change (Extreme proprietary trap)
- SNMP unreachable (EPICenter event)
- Configuration upload failure for an upload attempted from the EPICenter system (EPICenter event)
- Overheat (EPICenter event)
- Fan failure (EPICenter event)
- Device reboot (EPICenter event)

Therefore, you may see alarm log entries the first time you run the Alarm System, even if you have not defined any alarms of your own.

The Alarm Log Browser summary displays the following information for each alarm instance:

- **ID** (an integer number assigned by the EPICenter Alarm System based on the order in which the alarm occurred)
- **Name** (provided when the alarm is defined)
- **Category** (an optional user-defined classification that defaults to “Default”)
- **Severity** (the severity level associated with the alarm when it was defined)
- **Source** (the IP address of the device that generated the trap or responded to a poll)
- **Time** (the date and time at which the alarm was received)
- **Message** (the message generated by the alarm)
- **Acked** (a green check will be present if the alarm has been acknowledged)

The summary is initially sorted by ID in descending numerical order, so that the most recent alarm appears at the top of the list.

You can sort the display by the contents of any column by clicking on the column heading. Click the heading a second time to reverse the sort order based on that column.

## Acknowledging an Alarm

To acknowledge an alarm:

- 1 Select the alarm or alarms you want to acknowledge.

- 2 Click the Acknowledge (**Ack**) button at the top of the page.



Ack

This sets the state of the selected alarms to “acknowledged,” and places a green check in the **Acked** field of the selected alarm log entries.

When you acknowledge the most recent alarm, the state of the Alarm button in the EPICenter Navigation Toolbar also returns to black.

You can “unacknowledge” alarms, if needed, by selecting the alarms and clicking the



**Unack** button. Unack

## Deleting Alarms

To delete an alarm:

- 1 Select the alarm or alarms you want to delete.

- 2 Click the **Delete** button at the top of the page.




Delete

This removes the Alarm Log entry entirely from the ExtremeWare EPICenter database.

## Viewing Alarm Details

To view the details of an individual alarm:

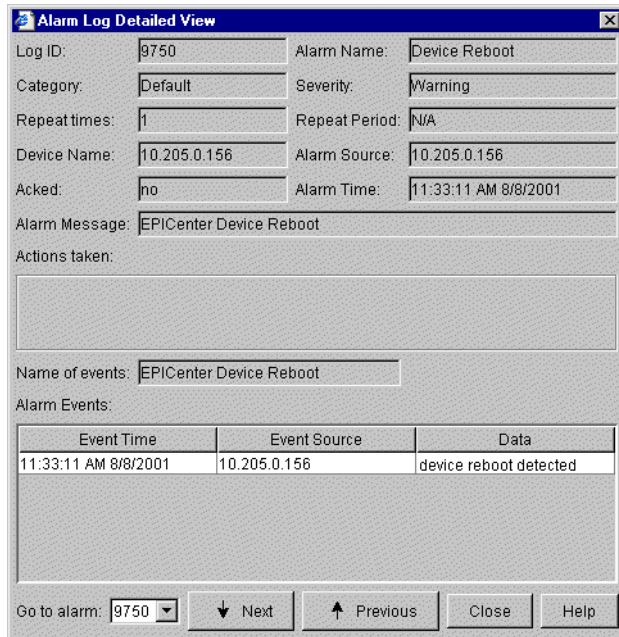
- 1 Select the alarm you want to view.

- 2 Click the **Detail** button at the top of the page,  or double-click on the alarm entry in the log.



Detail

The **Alarm Log Detailed View** is displayed, as shown in Figure 5-3.



**Figure 5-2:** Detailed view of an Alarm Log entry

This displays detailed information for the selected alarm.

From this window you can view details for other alarms:

- Enter or select an Alarm ID in the **Go to alarm** field.
- Click the **Next** button to view the next alarm down in the list (the next earlier alarm based on the default sorting order).
- Click the **Previous** button to view the next alarm higher in the list (the next later alarm based on the default sorting order).

## Filtering the Alarm Display

The alarms you see in the Alarm Log browser are displayed based on a filtering criteria you can set. The default criteria is to display the last 300 alarms from ExtremeWare EPICenter’s database (assuming you invoked the Alarm browser from EPICenter’s Navigation Toolbar). You can select a number of other filters from the pull-down field at

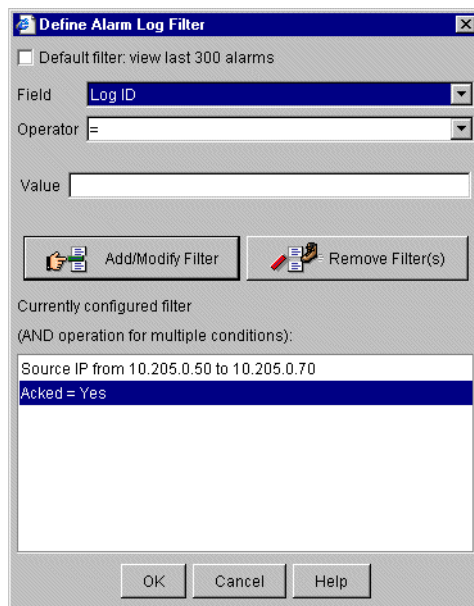
the top of the alarm summary display. The predefined filters are based on time: last one hour, last two hours, yesterday, and so on.

If you invoke the Alarm Browser from the Topology applet (using the pop-up menu for a specific node) the default filter is set to filter on the Source IP of the node you selected.

To specify your own filter, click the **Filter** button at the top of the page.



The Define Alarm Log Filter pop-up window is displayed, as shown in Figure 5-3.



**Figure 5-3:** Alarm Log filter definition pop-up window

To create your own filter, do the following:

- 1 If the “**Default Filter: view last 300 alarms**” check box is checked, the remaining fields will be greyed-out. Uncheck the check box to enable the other fields.
- 2 Select the parameter you want to use as a filter criterion from the pull-down menu in the **Field** field.
- 3 Select an operator using the pull-down menu in the **Operator** field.

- 4 Enter the value (or values) against which the parameter should be tested. If you have chosen the **Between** operator (available for Log ID, Source IP, and Port IfIndex) you will be asked to enter two values.

Some parameters (those that take text string values) provide a “Contains” operator, that lets you match against a portion of text that should be contained in the parameter value.

- 5 Click the **Add/Modify Filter** button to add this specification to the filter definition.

You can create a multi-criteria specification using more than one parameter, as shown in Figure 5-3, as long as each parameter is different. You cannot filter using multiple specifications of the same parameter.

For example, in order to find alarms for IP addresses 10.205.0.55 and 10.205.0.61, you must use the **Between** operator to test for any Source IP address between these two IP addresses. You cannot create a filter that includes both Source IP = 10.205.0.55 and Source IP = 10.205.0.61.

- 6 To remove an individual criteria, select it in the current filter list and click the **Remove Filter(s)** button. You can select and remove multiple filter criteria.
- 7 When your filter definition is complete, click OK.

To restore the default filter definition, click the **Default Filter: view last 300 alarms** check box and click OK.

## Defining Alarms

For convenience, the EPICenter Alarm System provides a number of predefined alarms. These alarms are enabled and will be active when you run the EPICenter server. These predefined alarms include:

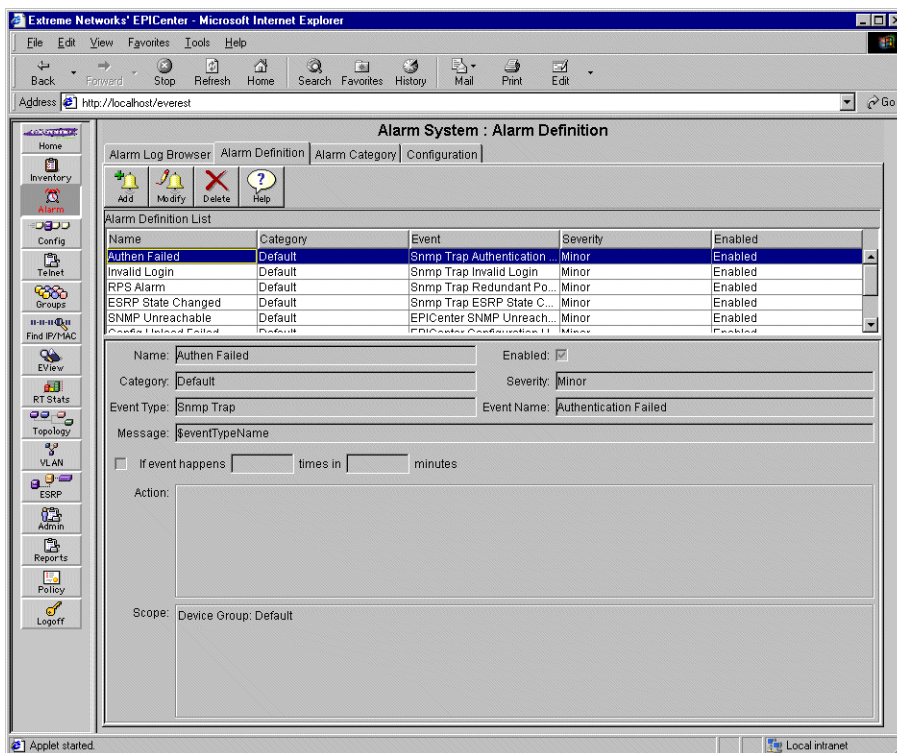
- Authentication failure (SNMP MIB-2 trap)
- Invalid login (Extreme proprietary trap)
- Redundant Power Supply alarm condition (Extreme proprietary trap)
- ESRP state change (Extreme proprietary trap)
- SNMP unreachable (EPICenter event)
- Configuration upload failure for an upload attempted from the EPICenter system (EPICenter event)
- Overheat (EPICenter event)
- Fan failure (EPICenter event)

- Device reboot (EPICenter event)

By default these alarms are all enabled, and will generate an alarm log entry upon occurrence. No other actions are specified in the predefined alarms.

You can define additional alarms based on a fairly large number of events.

To view the current alarm definitions, to create new definitions, or to modify existing definitions, click the **Alarm Definition** tab at the top of the page. The Alarm System: Alarm Definition page is displayed, as shown in Figure 5-4.



**Figure 5-4:** Alarm System: Alarm Definition page

To view the settings for an individual alarm, just select the alarm. Its definition will appear in the fields below the alarm list. For a definition of the fields in the top portion of the alarm definition, see the section “The Basic Alarm Parameters” on page 5-11.

**Alarm Actions:** Initially the predefined alarms have no actions defined for them. An *alarm action* is a specified function that the alarm system can execute when an alarm occurs, in addition to logging the occurrence of the alarm. Alarm actions can include sending e-mail, sounding an audible alert, running a program or executing a script. For the predefined alarms, an alarm event will create an entry in the Alarm Log, but no other actions will occur. You can define additional actions for any of these alarms.

**Alarm Scope:** The predefined alarms are all initially scoped to the Default device group. *Alarm scope* defines which devices can trigger an alarm. Thus, a trap occurring on any device in the Default device group will trigger the corresponding alarm. You can modify the scope of any of these alarms.

## Creating New Alarm Definitions



To create a new alarm, click the **Add** button at the top of the page.

The **New Alarm Definition** window appears, as shown in Figure 5-5, and displays the Basic page of the three-page alarm definition.

The screenshot shows a window titled "New Alarm Definition" with three tabs: "Basic", "Scope", and "Action". The "Basic" tab is selected. The window contains the following fields and controls:

- Name:** A text input field.
- Enabled:** A checked checkbox.
- Category:** A dropdown menu with "Default" selected.
- Severity:** A dropdown menu with "Normal" selected.
- Event Type:** A dropdown menu.
- Event Name:** A dropdown menu.
- Message:** A text input field containing "\$eventTypeName" and a "Variable..." button.
- Frequency:** A checkbox labeled "If event happens" followed by two input fields for "times in" and "minutes".
- Buttons:** "OK", "Cancel", and "Help" buttons at the bottom.

**Figure 5-5:** The New Alarm Definition window, Basic definition

There are three parts to an alarm definition: the Basic definition, the Scope definition, and the Action definition. Each is represented on its own page in the New Alarm Definition window.



Use the tabs at the top of the window to move between the three pages. When you are finished with your alarm definition, click OK, and the alarm will be entered into the Alarm Definition List.

## The Basic Alarm Parameters

On the **Basic** page, you define the event-related parameters of the alarm: its name, severity, the event that will trigger it, and so on. The fields in this window are defined as follows:

- **Name:** The name of the alarm as it will appear in the alarm log and (optionally) elsewhere. This defines the variable **alarmName**
- **Enabled:** Indicates whether the alarm is “turned on” or not. If you uncheck this box, the alarm will remain defined but will not be operational
- **Category:** The category assigned to this alarm. Select the category using the pull-down menu at the end of the field (see the section “Creating a New Alarm Category” on page 5-21 for more information). This defines the variable **alarmCategory**.
- **Severity:** The severity of the alarm. Select one of the five severity levels from the pull-down menu (normal, warning, minor, major, critical). This defines the variable **alarmSeverity**. The severity level also determines the sound that will be played as an audible alert.
- **Event Type:** The type of event (SNMP trap, RMON Rising trap, RMON Falling trap, or an EPICenter event). This determines the list of events you can select in the Event Name field.

An EPICenter event is generated by EPICenter based on the results of its periodic polling. In some cases, an EPICenter event may result from the same condition that could also generate an SNMP or other trap. An EPICenter event has the advantage that it guarantees that the condition will eventually be detected by polling even if the corresponding trap is missed.

See Appendix D for a description of the EPICenter and SNMP events from which you can choose.

Certain SNMP events require configuration on the switch in order to enable specific trap conditions.

You define RMON events and CPU Utilization events through the Event Configuration page of the EPICenter Alarm System. RMON events can only be configured on switches running ExtremeWare 6.1 or later. CPU Utilization rules can only be configured on switches running ExtremeWare 6.2 or later.

For certain other events, you must do the configuration on the switch using an SNMP configuration tool such as SNMPc. See “Configuring Other SNMP Trap Events” on page 5-38 for more information.

The event type is concatenated with the event name to define the variable **eventTypeName**.

- **Event Name:** The specific event (trap) that should trigger this alarm. Select the event from the pull-down list provided. For RMON Rising or RMON Falling trap types, the RMON rule name is used as the event name. The full-down list includes the configured RMON rule names. See Appendix D for a description of the EPICenter and SNMP events from which you can choose.

The event name is concatenated with the event type to define the variable **eventTypeName**.

- **Message:** A message you specify that will be transmitted whenever the alarm occurs. By default, this field contains the variable **eventTypeName**. You can delete this variable, add other variables as provided in the variable pop-up list, and add your own text.
- **Variables...:** A pop-up list that provides a list of variables you can select to include in the Message field. See Table 5-1 for a definition of the Alarm System variables you can use in the message field.
- **Repetitive occurrence specification:** The required number of repeated occurrences of the event that must occur before an alarm is generated. You can specify both the number of times the event must occur, and the time frame within which these events must occur. This lets you define alarms that will filter out short-lived or non-repeatable events, and will only take action if the triggering event occurs repeatedly within a sufficiently short time frame.

**Table 5-1:** EPICenter Alarm Variables

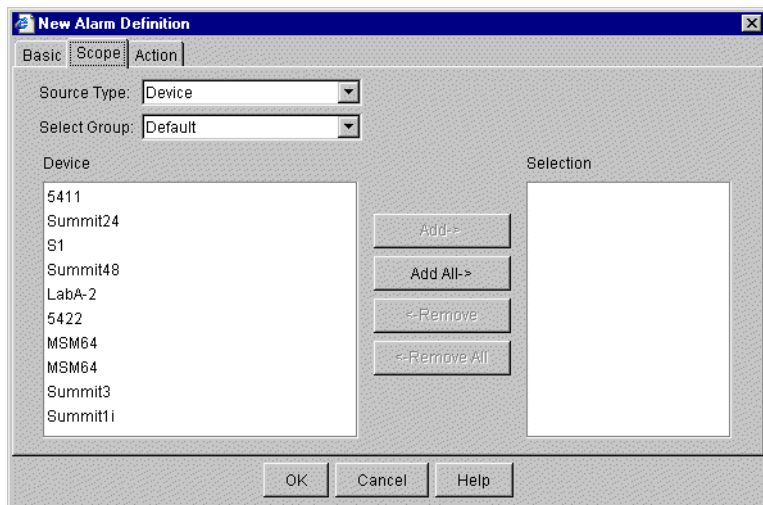
Variable Name	Description
alarmID	An integer number assigned by the EPICenter Alarm System based on the order in which the alarm occurred
alarmName	The name of the alarm as defined in the Name field
alarmCategory	The user-defined alarm category assigned to the alarm
alarmSeverity	The severity level assigned to the alarm
alarmRepeatTimes	The number of times the event must occur before an alarm is generated

**Table 5-1: EPICenter Alarm Variables**

<b>Variable Name</b>	<b>Description</b>
alarmRepeatPeriod	The time frame within which the repeated events must occur for the alarm to be generated
alarmSourceDeviceName	The name of the device on which the event(s) occurred (taken from the EPICenter database)
alarmSourceIP	The IP address of the device on which the event(s) occurred
alarmSourceIndex	The interface on the device on which the event(s) occurred
alarmGMTTime	The time at which the alarm occurred, in Greenwich Mean Time
alarmLocalTime	The time at which the alarm occurred, in local time
alarmMessage	The message defined for the alarm
alarmActions	The list of actions defined for the alarm
eventLogID	The ID of the alarm in EPICenter's event log
eventTypeName	The type of event (SNMP Trap, RMON Rising Trap, RMON Falling Trap, or EPICenter event) concatenated with the Event Name (the SNMP trap name, RMON rule name, or EPICenter event name).
eventGenericType	The SNMP Generic Type number of the trap
eventSpecificType	The SNMP Specific Type number for an enterprise-specific trap
eventTypeStr	The event description
eventEnterprise	The Enterprise portion of the Object ID (OID) of the event
eventData	The data associated with the trap

### The Alarm Scope

To define a scope for the alarm, click the Scope tab. The Scope definition page is displayed, as shown in Figure 5-6.



**Figure 5-6:** The New Alarm Definition window, Scope definition

In this window you define the scope of the alarm—the set of devices that can trigger the alarm. You can define the scope as a set of individual devices, one or more device groups, as a set of individual ports, or as one or more port groups.

To define the alarm scope, you select a Source Type (and Device Group, if appropriate), select individual devices, ports, device groups, or port groups, and add them to the Selections list.

The fields and buttons in this window are defined as follows:

- **Source Type:** The source of the scoping definition (Device, Device Group, Port, or Port Group). Select the type you want from the pull-down list.

Selecting Device Group or Port Group will scope the alarm on all members of the selected group. To scope the alarm on individual devices or ports, select Device or Port.

For events that originate from a device port (such as link down) the scope will determine whether the alarm will be generated based on an event from a single port, or on events from any port on a device, or from any port on any device in a device group.

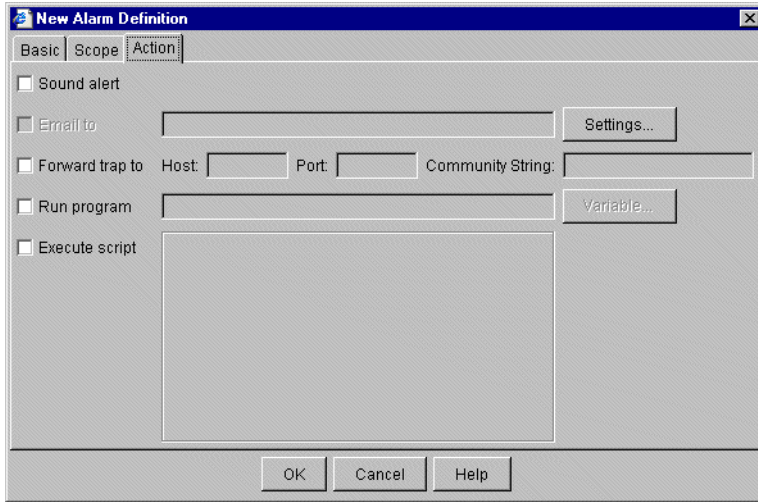
For example, if you want to define an alarm that is fired for any port on device A, you can scope the alarm as “Device,” select the appropriate device group, and select Device A. If you want to define the alarm only to be fired on selected ports on Device A, then you would scope the alarm as “Port,” select Device A, and then select the individual

ports. You could also define a port group for the specific ports of interest, the scope the alarm as Port Group and select the appropriate group.

- **Select Group:** If you select Device or Port as the Source Type, you must select a Device Group to indicate what set of devices (and ports) you want to see in the Source List.
- **Source list (Device/DeviceGroup/Port Group):** The list of components of the specified type. The field label changes based on the Source Type. It is labeled Device when you select either Device or Port as the Source Type.
- **ifIndex:** The list of ports available on the device selected in the Devices Source list. This list appears only if you have selected Port as the Source Type. Select a device from the Device list, and the appropriate set of ports for the device appears.
- **Selection:** The devices, ports, device groups, or port groups that are currently included in the scope.
- **Add->:** Adds the selected Device(s), Port(s), Device Groups or Port Groups to the Selections list, for inclusion in the scope of this alarm.
- **Add All->:** Adds all the components in the Source list to the Selection list.
- **<-Remove:** Removes the selected components from the Selection list.
- **<-Remove All:** Removes all the components from the Selection list.

## The Alarm Actions

To define actions for the alarm, click the **Actions** tab. The Action definition page is displayed, as shown in Figure 5-7.



**Figure 5-7:** The New Alarm Definition window, Action definition

In this window you define the actions for the alarm—the functions that should be performed when the alarm occurs. You can have the alarm perform any or all of the actions defined here.

The fields and buttons in this window are defined as follows:

- **Sound Alert:** Click the check box to have the alarm system play an audible alert on the client computer when the alarm occurs. The alarm will sound on all EPICenter clients currently connected to the EPICenter server. The sound that is played will depend on the severity level of the alarm.

The alert sound files are kept on the EPICenter server in the directory `<epicenter_installdir>\extreme`, and are named according to the severity level they represent (`normal.wav`, `warning.wav` and so on). `<epicenter_installdir>` is the directory where EPICenter is installed, by default `epc3_1` in the Windows operating environment, or `/opt/epc3_1` on a Solaris system.

- **Email to:** Click this check box to indicate that e-mail should be sent, then enter the e-mail address(es) of the recipients for the e-mail. E-mail addresses in a list can be separated by commas, semicolons, or spaces.



*If this box is greyed out, you must first configure your e-mail settings. See “Setting Up E-mail for the Alarm System” for details.*

- **Forward Trap to:** Click this checkbox to forward the trap event that caused this alarm. Specify the forwarding instructions in the fields to the right of the check box as follows:
  - **Host:** Enter the host name or host IP address of the system to which the trap should be forwarded.
  - **Port:** Enter the port on which the specified host receives traps.
  - **Community String:** Enter the community string for the specified host.
- **Run program:** Click the check box to have the Alarm System run a program when this alarm occurs. Enter the command string for the program you want to run. You can include Alarm System variables as arguments by clicking the **Variables...** button and selecting the variables you want.



*On a Windows NT or Windows 2000 system, if you are running the EPICenter server as a service, and you specify a program that does output to the desktop, that program will not run unless you specify that output to the desktop is allowed when you start the server service. You can solve this problem by restarting the EPICenter server and specifically allowing interaction with the desktop. Refer to the Alarm System section in Appendix A, Troubleshooting, for instructions on restarting the EPICenter server service with this option enabled. If you are running the EPICenter server as a regular program, this is not a problem.*



*If you want to specify a batch file that does output to the desktop, you must specify the “.bat” file within a DOS “cmd” command, as follows:*

```
cmd /c start <file.bat>
```

*where <file.bat> is the batch file you want to run.*

- **Execute script:** Click the check box to have the Alarm System execute a Tcl script when this alarm occurs. Enter the script commands into the window provided.

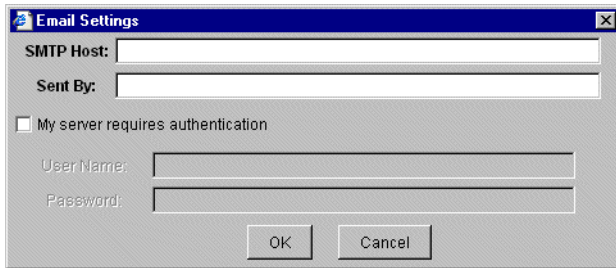
You can write your own scripts that access selected EPICenter database variables. See “Writing Tcl Scripts for Alarm Actions” on page 5-39 for more information.

## Setting Up E-mail for the Alarm System

Before you can use the e-mail action, you must configure the e-mail capability. Until you do so, the **Email To** field and check box will not be available. To configure the e-mail capability, do the following:

- 1 Click the **Settings...** button on the Action page.

This displays the **Email Settings** window, as shown in Figure 5-8.



**Figure 5-8:** Setting up E-mail for EPICenter alarm actions

- 2 Enter your outgoing mail server name (or IP address) into the **SMTP Host:** field.
- 3 Enter into the **Sent By:** field the e-mail address that should be used as the sender of the e-mail
- 4 If your mail server authenticates the user before sending out e-mail, check the **My server requires authentication** check box, and enter the user name and password of an account that the SMTP server will accept. Usually this will be the account you use to log into your network.

If you don't know whether your server requires authentication, you can go ahead and enter the authentication information—it will be ignored if it is not actually needed.

## Alarm Definition Examples

**Example 1:** Define an alarm that will page “Joe” at “4083236789@paging.com” if port 10 on device “switch8” goes down.

- 1 Bring up the **New Alarm Definition** dialog. On the **Basic** page, do the following:
  - a Type a name for the alarm (for example, **WAN Link Down**) in the **Name** field.
  - b Make sure the **Enabled** checkbox is checked.
  - c Select a category (e.g. “Default”) in the **Category** field.
  - d Select “SNMP Trap” in the **Event Type** field.
  - e Select “Link Down” in the **Event Name** field.
- 2 Click the **Scope** tab, and do the following:
  - a Select “Port” in the **Source Type** field.
  - b Select “switch8” from the **Device** list.
  - c Select “10” from the **ifIndex** list.



- d Click the **Add** button to add port 10 to the **Selection** list.
- 3 Click the **Action** tab, and do the following:
  - a Click the **Email to:** check box to turn on the check.
  - b Type 4083236789@paging.com in the text field next to the checkbox.
- 4 Click **OK** to finish the alarm definition.

**Example 2:** Define an alarm that will page “Joe” at “4083236789@paging.com” if any port on device “switch8” goes down.

- 1 Bring up the **New Alarm Definition** dialog. Fill in the fields on the Basic page just as you did in Example 1.
- 2 Under the **Scope** tab, do the following:
  - a Select “Device” in the **Source Type** field, instead of “Port.”
  - b Select “switch8” from the **Device** list as in Example 1.
  - c Click the **Add** button to add switch8 to the **Selection** list. No ifIndex list will be displayed.
- 3 Click the **Action** tab, and enter Joe’s paging information as you did in Example 1.
- 4 Click **OK** to finish the alarm definition.

**Example 3:** In a Windows NT environment (where both the EPICenter server and client are running under Windows), define an alarm that will pop up a message on the Windows client system “joe” if the port utilization on port 10 on device “switch8” exceeds 15 percent.

This alarm requires an RMON rule with a Rising Threshold of 15 percent for port utilization. You can define the RMON rule either before or after you define the alarm. See “RMON Rule Configuration Example” on page 5-34 for an example of how to create the RMON rule.

To create the alarm definition:

- 1 Bring up the **New Alarm Definition** dialog. On the **Basic** page, fill in the **Name** and **Category** fields, and check the **Enabled** checkbox, just as you did in Example 1.
  - a Select “RMON Rising Trap” in the **Event Type** field.
  - b Enter the RMON rule name in the **Event Name** field:

If you have already created the RMON rule, you can select it from the pull-down menu in the **Event Name** field. For example, if you named the rule “WAN Link 15%”, that name should appear in the pull-down menu.

If you have not yet created the RMON rule, type in a name for the rule (for example, “WAN Link 15%”). You will need to use this name for the rule when you create it.

See “RMON Rule Configuration Example” on page 5-34 for an example of how to create the RMON rule.

- 2 Click the **Scope** tab, and enter the port information as you did in Example 1:
  - a Select “Port” in the **Source Type** field.
  - b Select “switch8” from the **Device** list.
  - c Select “10” from the **ifIndex** list.
  - d Click the **Add** button to add port 10 to the **Selection** list.
- 3 Click the **Action** tab, and do the following:
  - a Click the **Run Program** checkbox to turn on the check.
  - b Type `net send joe "$alarmName"` in the text field next to the checkbox.



*This program is only available on the Windows NT platform.*

- 4 Click **OK** to finish the alarm definition.

## Modifying Alarm Definitions

To modify an alarm, select the alarm in the Alarm Definition List, and click the Modify



button at the top of the page. **Modify**

The Modify Alarm Definition window is displayed. This window, and its Basic, Scope and Action pages, are identical to the New Alarm Definition window, except that the current information for the alarm you selected is filled in.

To modify the alarm, make any changes you want, then click OK. For definitions of the various fields, see the section “Creating New Alarm Definitions.” on page 5-10.

## Deleting Alarm Definitions

To delete an alarm definition, select the alarm in the Alarm Definition List, and click the



Delete button at the top of the page. **Delete**

After you verify that you want to delete the alarm, the definition is removed from the Alarm Definition List and from ExtremeWare EPICenter's database. You must remove alarm definitions one at a time.

## Alarm Categories

Alarm categories are arbitrary collections of alarms that you can define as appropriate to your needs, and then assign to specific alarm definitions. For example, you might use categories to designate alarms from individual buildings, floors, or workgroups. An ISP might define categories for alarms from a specific customer's equipment.

By default, all alarms are assigned to the category named Default. This category can be renamed, but it cannot be deleted.

### Creating a New Alarm Category



To create a new alarm category, click the **Add** button at the top of the window.

A small pop-up window appears into which you can enter the name of the new category. Click **OK** to enter the new category into the Category List.

### Modifying an Alarm Category



To rename an alarm category, click the **Modify** button at the top of the window.

A small pop-up window appears and displays the current name of the category. Modify the name and click **OK** to enter the revised category into the Category List.

When an alarm category is renamed, all alarms assigned to that category are updated to use the new category name.

### Deleting an Alarm Category

To delete an alarm category, select the category from the Category List, then click the



**Delete** button at the top of the window.



*Deleting a category also deletes all the alarm definitions that are assigned to that category. If you do not want to delete those alarm definitions, you must first modify the alarm definitions to use a different alarm category before you delete the category.*

A warning message appears to let confirm that you want to delete the category and the alarm definitions that are assigned to it. Click **OK** to delete the category and the alarms from the EPICenter database.

The Default category cannot be deleted.

## Event Configuration

The Event Configuration page lets you define the conditions or rules that will cause certain trap events to occur, and specify the devices on which these rules should be configured. In EPICenter 3.1, you can use this page to define how RMON and CPU utilization events should be generated.

In the case of both RMON utilization and CPU utilization, events (traps) can be generated based on comparing a sample value to a threshold value. The rules you set up specify what these threshold values should be. Once these rules are in place, you can use them in your EPICenter alarm definitions to create alarms that will take actions when a sample value crosses one of the thresholds you've defined.

There are several other SNMP traps supported by the EPICenter Alarm System that also require conditions to be set on the switch to define when a trap should occur. See "Configuring Other SNMP Trap Events" on page 5-38 for additional information.

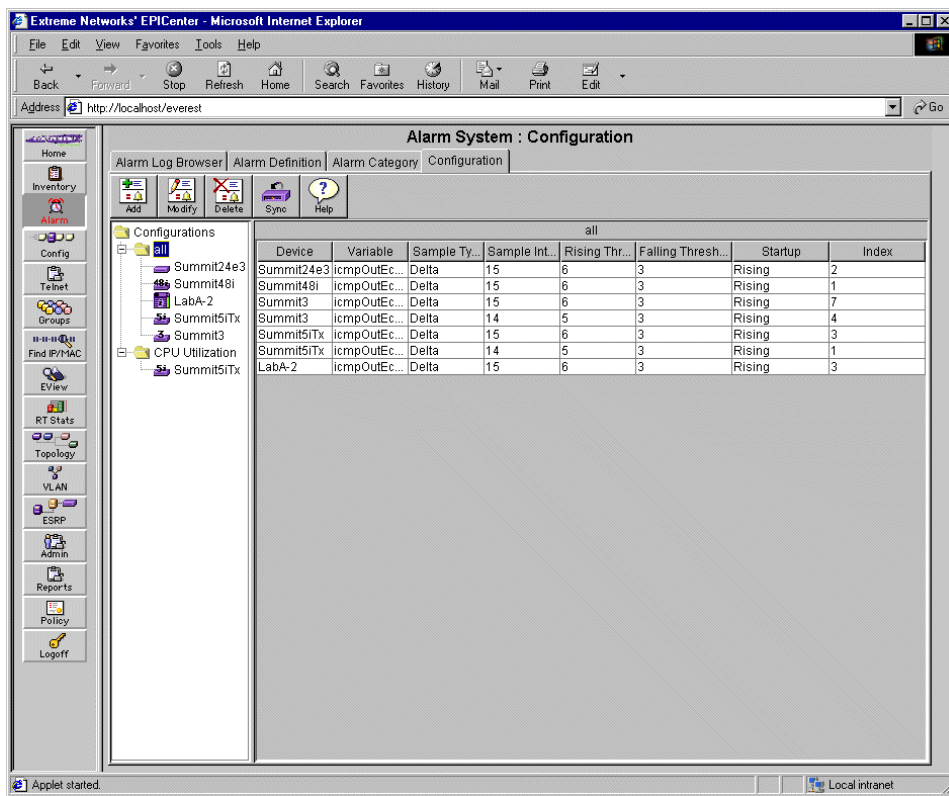
In addition to specifying the conditions under which trap events should be generated, you also use this page to define the target devices on which the event rules should be configured.



*Creating the rules that control trap (event) generation is only the first of the two steps required to create EPICenter alarms for these events. Even though you have set up these rules, the trap events generated as a result will be ignored by the Alarm System until you define alarms that take actions on those events. See "Defining Alarms" on page 5-8 for more information.*

To view the current RMON and CPU Utilization rules, and to create new rules or modify existing rules, click the **Configuration** tab at the top of the page. The Alarm System:

Configuration page is displayed. Figure 5-9 shows the Alarm System Configuration page as it appears when displaying RMON rules.



**Figure 5-9:** The event Configuration window showing RMON rules

The Configurations tree shows the existing RMON event definitions as nodes in the tree, with the devices to which they are applied shown as subnodes. The main panel shows the definition for the selected rule on each target device.

CPU Utilization rules are shown under a separate node. Devices on which a CPU utilization rule is configured are shown as subnodes of the CPU Utilization node. There can be only one CPU utilization rule per device.

Click the small plus next to an RMON Rule node or the CPU Utilization node to display in the tree the devices associated with that rule.

To display the definition of a rule click the rule node.

## RMON Rule Display

For RMON rules, the display shows the following for each device targeted by that rule:

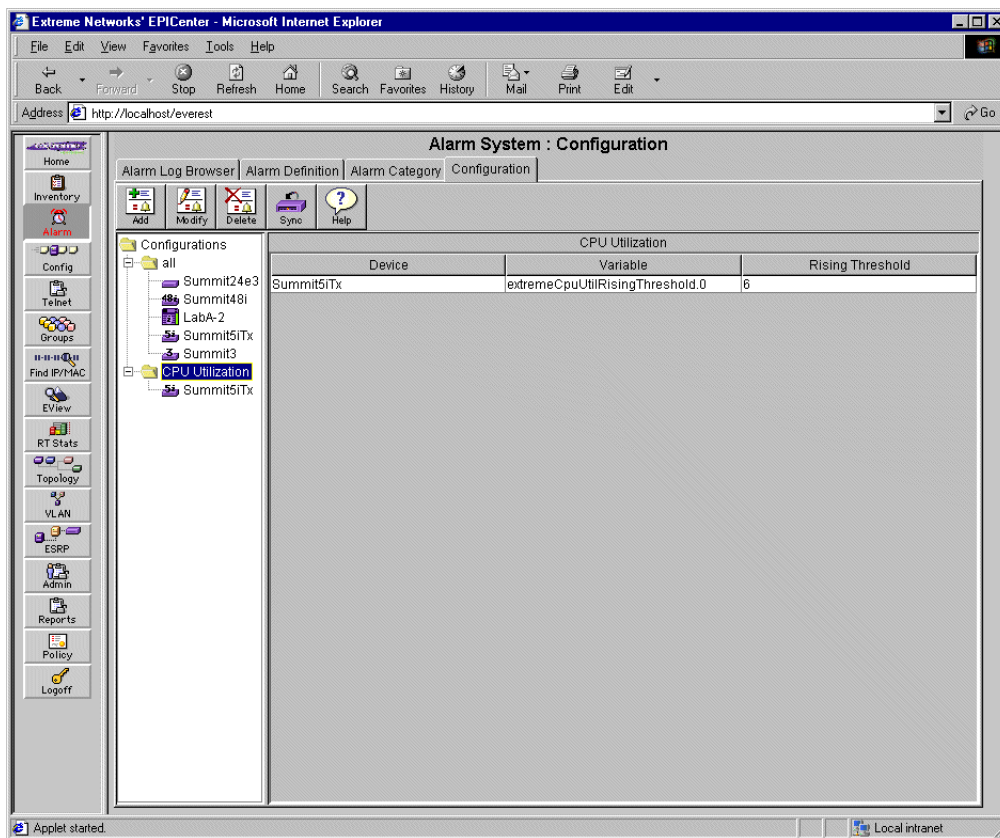
- **Device:** The name of the device
- **Variable:** The MIB variable being monitored
- **Sample Type:** Absolute or Delta
- **Sample Interval:** The time between samples, in seconds.
- **Rising Threshold:** A threshold value that will trigger an event when the value of the variable increments past this value.
- **Falling Threshold:** A threshold value that will trigger an event when the value of the variable decreases past this value.
- **Startup:** The condition that will cause the initial event (Rising, Falling, or RisingOrFalling).
- **Index,** the device index as obtained by the EPICenter server from the device.

For a detailed definition of these parameters, see “RMON Rule Configuration” on page 5-27.

## CPU Utilization Rule Display

To display the CPU Utilization rules, click the CPU Utilization node in the Configurations tree.

Figure 5-9 shows the Alarm System Configuration page as it appears when displaying CPU Configuration rules.



**Figure 5-10:** The event Configuration window showing CPU Configuration rules

For each device targeted by that rule, the CPU Utilization rule display shows the following:

- **Device:** The name of the device
- **Variable:** The MIB variable being monitored (always `extremeCpuUtilRisingThreshold.0`)
- **Rising Threshold:** A threshold value that will trigger an event when the CPU Utilization value (a percentage) increments past this value.

This value is also used to calculate a Falling Threshold value, which is to be 90% of the Rising Threshold value.

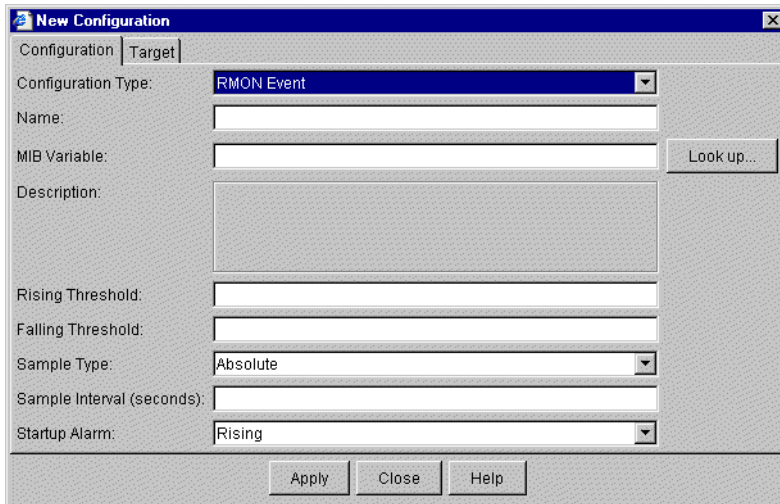
For a detailed definition of these parameters, see “CPU Utilization Rule Configuration” on page 5-31.

## Creating an Event Rule

To create a new event rule, click the **Add** button at the top of the page.



The **New Configuration Rule** window is displayed, as shown in Figure 5-11.



**Figure 5-11:** New Configuration window

There are two parts to an event rule; the rule configuration itself, and the association of the rule to its target devices.

The **New Configuration** window comes up with the Configuration page displayed.

In the **Configuration Type** field, select the type of rule you want to create (RMON Event or CPU Utilization) from the drop-down list.



*CPU Utilization is only supported on switches running ExtremeWare 6.2 or later.*

When you finish entering the configuration and target information, click the **Apply** button, and the new rule is added to the Configurations tree. For RMON rules, the rule name is included as a “folder” and each target device for the rule appears as a separate component under that rule. The rule name will also appear in the Event Name list.



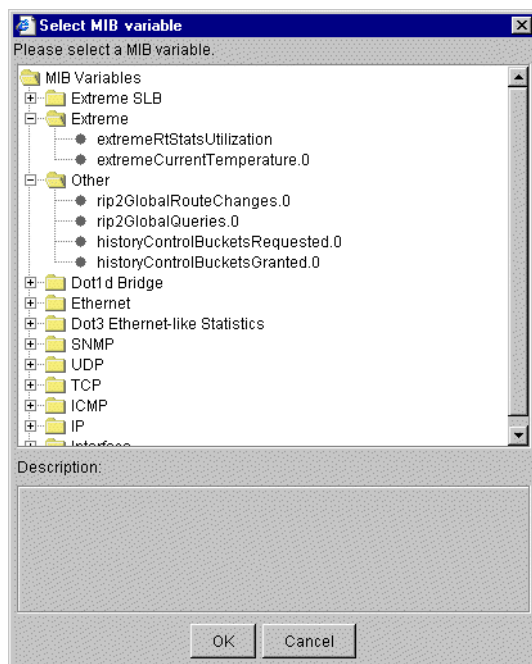
For CPU Utilization rules, each target device for a CPU utilization rule appears as a separate component under the CPU Utilization “folder” in the Configurations tree.

## RMON Rule Configuration

If you select RMON Event as the Configuration Type, the remaining fields and buttons in this window are defined as follows:

- **Name:** The name for this rule.
- **MIB Variable:** The MIB variable that the rule will monitor.

Type in the complete OID, or click the **Look Up...** button to bring up a list of variables that are available, organized by MIB groups, as shown in Figure 5-12.



**Figure 5-12:** A list of MIB variables available for use in RMON rules

Click on a variable group to display the individual variables within the group. You can use the up and down arrow keys to scroll the list.

You can also type the beginning of a variable name into the MIB Variable field, then type a space, and the Alarm System will attempt to match your typing to the variable list and auto-complete your entry.

MIB variables that apply to the entire device will have the suffix “.0” appended to them to create the complete OID. MIB variables that apply per port will be combined with the port ifIndex to generate the OID.



*The MIB variable list displays only the MIBs that were shipped with the EPICenter software. It does not display table variables if the table is indexed by an index other than (or in addition to) ifIndex.*

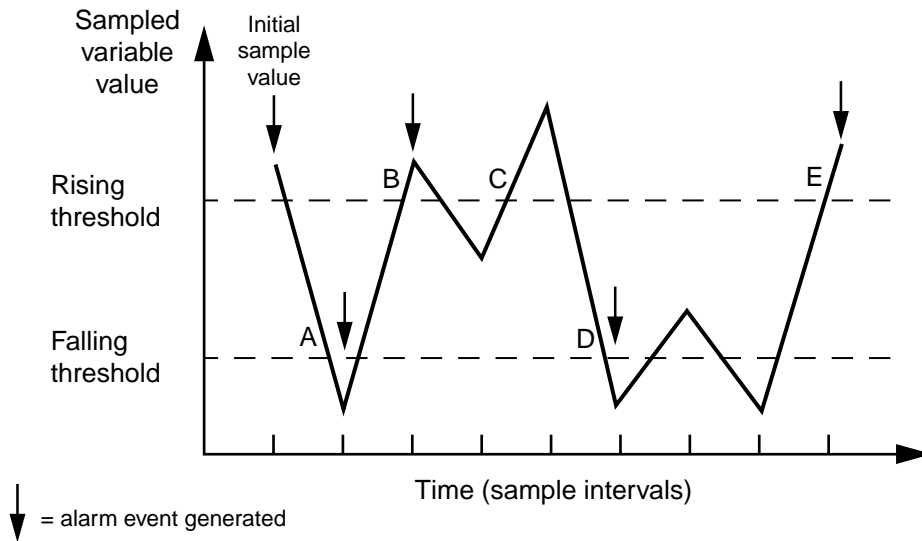
If the MIB variable you want to monitor does not appear in the MIB Variable lookup list, you can still use the variable by typing its complete OID into the MIB Variable field. Enter the OID in its numeric form, ending in .0 if it is a per device variable, or in the specific index if it is a per-port variable. If it is a table variable, you may need to enter each index and apply it to each target device one by one.

- **Description:** The description of the MIB variable. This description should specify the units of measure for the variable, needed in order to correctly specify the Rising Threshold and Falling Threshold values.
- **Rising Threshold:** A threshold value that will trigger an event when the value of the variable increments past this value. An event will be generated when the sample value meets the following conditions:
  - When the sample value becomes greater than or equal to the Rising Threshold for the first time after the alarm is enabled, if the Startup Alarm condition is set to Rising or RisingOrFalling
  - The first time the sample value becomes greater than or equal to the Rising Threshold, *after having become less than or equal to the Falling Threshold*
- **Falling Threshold:** A threshold value that will trigger an event when the value of the variable decreases past this value. An event will be generated when the sample value meets the following conditions:
  - When the sample value becomes less than or equal to the Falling Threshold for the first time after the alarm is enabled, if the Startup Alarm condition is set to Falling or RisingOrFalling
  - The first time the sample value becomes less than or equal to the Falling Threshold, *after having become greater than or equal to the Rising Threshold*
- **Sample Type:** The method used to compare the variable to the threshold. Specify the type as follows:
  - **Absolute** to use the actual sample value of the variable

- **Delta** to calculate the difference between the current sample value and the previous sample value of the variable, and use the difference in the comparison
- **Sample Interval (seconds):** The interval, in seconds, over which the data is sampled and compared to the rising and falling thresholds.
- **Startup Alarm:** The condition that should be met to cause the initial occurrence of this event. Select from the following:
  - **Rising:** an event will be generated the first time the sample value becomes greater than or equal to the Rising Threshold value. No events will be generated related to the Falling threshold until after this has occurred.
  - **Falling:** an event will be generated the first time the sample value becomes less than or equal to the Falling Threshold value. No events will be generated related to the Rising threshold until after this has occurred.
  - **RisingOrFalling:** an event will be generated the first time the sample value becomes either greater than or equal to the Rising Threshold value, or less than or equal to the Falling Threshold value.

It is important to understand that, except for the initial occurrence of the alarm, an RMON alarm event will be generated only when the sample value of the variable crosses one of the thresholds for the first time after having crossed the other threshold.

The following diagram, shown in Figure 5-13, shows how alarms are generated for an RMON rule using Delta values, where the startup alarm condition is set to “Rising” or “RisingOrFalling.”



XM\_022

**Figure 5-13:** RMON Alarm event generation

Because the initial sample value of the variable is greater than the value of the Rising threshold, an RMON rising threshold trap is generated. A second trap occurs at the next sample interval (point A) because the sample variable value is now less than the Falling Threshold. At point B the value again passes the Rising Threshold, and another trap event is generated. However, no trap occurs at point C, even though the value of the variable again becomes greater than the Rising Threshold, because the value has not yet become less than the Falling threshold. Another Rising threshold trap event cannot occur until after a Falling threshold alarm has occurred, as happens at point D.

Note that in order to have any of these trap events cause an alarm in the EPICenter Alarm System, you need to define an alarm that responds to a RMON Rising Threshold or RMON Falling Threshold event.

- If you define an alarm based on the RMON Rising Threshold event, then EPICenter alarms will occur at the initial sample, and at points B and E. Because the alarm is defined to respond to RMON Rising Threshold events, the falling threshold trap events that occur at points A and D do not trigger an EPICenter alarm.
- If you also define an alarm based on an RMON Falling Threshold event, then EPICenter alarms would also be generated at points A and D.

For a more detailed discussion of Remote Network Monitoring alarm behavior, refer to a book such as *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, Third Edition, by William Stallings (Addison-Wesley, 1999).

## CPU Utilization Rule Configuration



*CPU Utilization is only supported on switches running ExtremeWare 6.2 or later.*

If you select CPU Utilization as the Configuration Type, the remaining fields and buttons in this window are defined as follows:

- **Name:** CPU Utilization, the name for this rule. There can only be one rule of this type on a device, so the name is predefined.
- **MIB Variable:** `extremeCpuUtilRisingThreshold.0`, the MIB variable that this rule will monitor. This is also predefined.
- **Description:** The description of the `extremeCpuUtilRisingThreshold` MIB variable.
- **Rising Threshold:** A threshold value, in percent, that will trigger an event when the CPU utilization rises past this value. This value is also used to compute a falling threshold, which is defined as 90% of the rising threshold.



*Although you can define only a Rising Threshold value for CPU Utilization, you can define alarms for both CPU Utilization Rising Threshold events and CPU Utilization Falling Threshold events. The Alarm Definition process lets you create two separate alarms related to CPU Utilization, based on this one rule.*

If you define an alarm for CPU Utilization Rising Threshold events, an alarm will be generated each time the sample value meets the following conditions:

- When the sample value becomes greater than or equal to the Rising Threshold for the first time (including the initial sample) after the alarm is enabled.
- The first time the sample value becomes greater than or equal to the Rising Threshold, *after having become less than or equal to the Falling Threshold* (90% of the Rising threshold).

If you define an alarm for CPU Utilization Falling Threshold events, an event will be generated each time the sample value meets the following conditions:

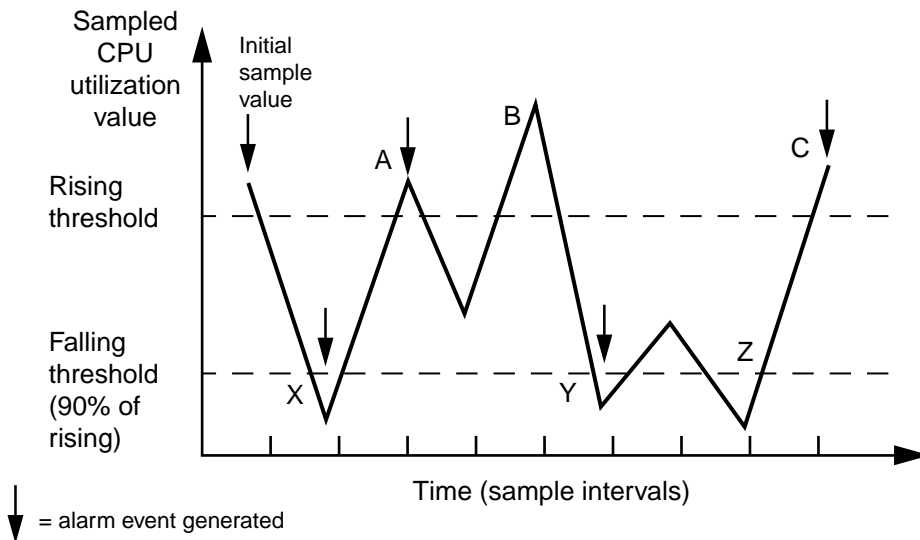
- The first time the sample value becomes less than or equal to 90% of the Rising Threshold, *after having become greater than or equal to the Rising Threshold*.

Several of the values you can set for an RMON event are predefined in the Extreme switch agent for CPU utilization. These are:

- **Startup Alarm:** The Startup condition is predefined to be **Rising**.
- **Sample Interval:** The sample interval for a CPU Utilization alarm is also predefined, and is set to 3 seconds.
- **Sample Type:** The sample value (a percentage) is always an absolute value.

It is important to understand that, except for the initial occurrence of a Rising Threshold alarm, a CPU Utilization alarm will be generated only when the sample value of the variable crosses the target threshold for the first time after having crossed the other threshold.

The diagram shown in Figure 5-14 illustrates how CPU Utilization trap events will occur once you have configured a CPU Utilization rising threshold. The startup condition for a CPU Utilization event is always predefined to be Rising.



XM\_023

**Figure 5-14:** CPU Utilization event generation

The first CPU Utilization trap occurs at the initial sample value, since the value is above the CPU Utilization Rising threshold. If the initial value were below the Rising threshold, no event would occur.

The second event occurs at point X, because the sample value has fallen below the falling threshold, which is defined as 90% of the rising threshold value. The third event occurs at point A because the sample value is again above the Rising Threshold after having fallen

below the Falling threshold. At point B the value again passes the Rising Threshold, but no alarm is generated because the value has not yet become less than the Falling threshold. Another Rising threshold alarm cannot occur until after a Falling threshold event has occurred, which happens at point Y. The next Rising threshold event happens at point C.

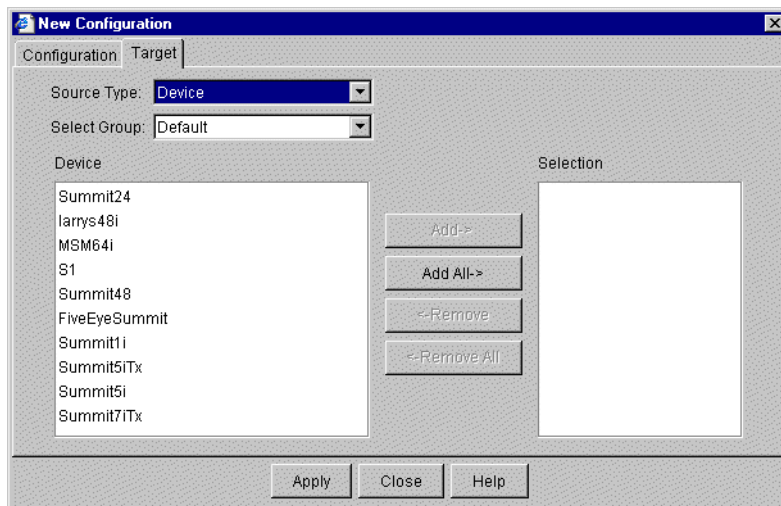
Note that in order to have any of these events cause an alarm in the EPICenter Alarm System, you need to define an alarm that responds to a CPU Utilization Rising Threshold or CPU Utilization Falling Threshold event.

- If you define an alarm based on the CPU Utilization Rising Threshold event, an EPICenter alarm will occur at the initial sample, and at points A and C. Because the alarm was defined to respond to CPU Utilization Rising Threshold events, the falling threshold trap events that occur at points X and Y do not trigger an EPICenter alarm.
- If you also define an alarm based on a CPU Utilization Falling Threshold event, then EPICenter alarms would be generated at points X and Y.

## Configuration Rule Target

Click the **Target** tab to display the New Configuration Target page, as shown in Figure 5-15.

This page lets you specify which devices should be configured to generate the event you have defined.



**Figure 5-15:** RMON target selection window

The fields and buttons in this window are defined as follows:

- **Source Type:** The source of the RMON rule targets (Devices, Device Groups, Ports, or Port Groups). Select the type you want from the pull-down list. The choices you have are determined by the variable you selected for the rule. For example, if the variable you have selected to monitor is applied per port, you will be able to select by Port or Port Group.
- **Source List (Device/DeviceGroup/Port Group):** The list of components (devices or groups) of the specified type. The field label changes based on the Source Type. It is labeled **Device** when you select either Device or Ports (a second Port field is provided for port selection).

Note that when you leave your cursor on a device for a moment, a pop-up displays the IP address of the device.

- **Source List (Port):** The list of ports available on the device selected in the Devices Source list. This list appears only if you've selected Ports as the Source Type. Select a device from the Device list, and the appropriate set of ports for the device appears.
- **Selection:** The devices, ports, device groups, or port groups that are currently targets for the RMON rule.
- **Add->:** Adds the selected Device(s), Port(s), Device Groups or Port Groups to the Selections list, for inclusion as a target for this rule.
- **Add All->:** Adds all the components in the Source list to the Selection list
- **<-Remove:** Removes the selected components from the Selection list.
- **<-Remove All:** Removes all the components from the Selection list.

## RMON Rule Configuration Example

**Example:** Create an RMON rule that will cause an RMON Rising Trap when port utilization on port 10 of device "switch8" exceeds 15%.



- 1 Bring up the **New Configuration** dialog. On the **Configuration** page, do the following:
  - a Type a name for the rule in the **Name** field (for example, "WAN Link 15%").  
If you have already created an alarm definition that will use this rule, make sure the name matches the name you entered in the alarm definition.
  - b Click the **Look up...** button to display the **Select MIB Variable** dialog.
  - c Expand the Extreme folder, select the `extremeRtStatsUtilization` variable, and click OK to enter it into the **MIB Variable** field.



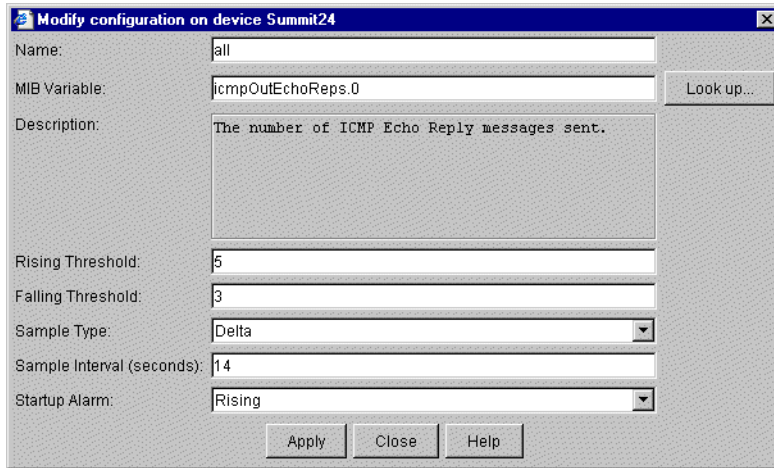
- d Type “1500” in the **Rising Threshold** field. Note that for this variable the value must be in hundredths of a percent.
  - e Type a smaller value, for example “1450” in the **Falling Threshold** field.
  - f Leave the **Sample Type** as “Absolute” and the **Sample Interval** at the default value (15).
  - g Select **Rising** for the **Startup Alarm** field.
- 2 Click the **Target** tab and do the following:
    - a Select Port as the **Source Type**
    - b Select “switch8” from the **Device** list
    - c Select 10 from the **ifIndex** list
    - d Click **Add** to add the port to the **Selection** list
  - 3 Click the **Apply** button to configure the rule on device switch8.  
A message window will appear with the device configuration results.
  - 4 Verify that no switch configuration errors have been reported, and click **OK** to dismiss the window.
  - 5 Click **Close** to dismiss the **New Configuration** dialog.

## Modifying a Rule

Once a set of RMON rules have been created, they must be modified individually. To modify a RMON rule do the following:

- 1 Select the rule folder or the individual rule name in the Configurations tree to display the rule details in the main panel of the window.
- 2 Select the individual rule you want to modify 
- 3 Click the **Modify** button at the top of the page. 

The **Modify Configuration** window is displayed for the target you selected.



**Figure 5-16:** Modify Configuration window

The window shows the same information as the Configuration page of the **New Configuration** window, but with the information for the current target filled in.


See “RMON Rule Configuration” on page 5-27 for a definition of the fields on this page.

Note that if you change the name of this rule, the new rule will be added as a “folder” in the Configurations tree, and this specific rule target will be moved under the new rule.

## Deleting a Rule

To delete an RMON or CPU Utilization rule, do the following:

- 1 Select the rule folder or the individual rule name in the Configurations tree to display the rule details in the main panel of the window.
- 2 Select the individual rule or rules you want to delete


- 3 Click the **Delete** button at the top of the window.  **Delete**

- 4 When the warning asking you to confirm that you want to delete is displayed, click **Yes** to delete the rule(s) or **No** to cancel the action.

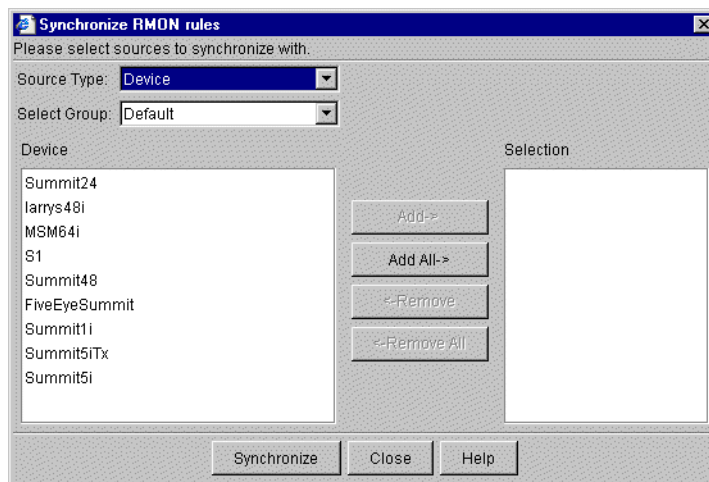
When you delete a rule, the alarm definition that references the rule is not deleted.

## Resynchronizing the RMON Rules

To resynchronize EPICenter's database with the RMON rules in place on a switch, do the following:

- 1 Click the **Sync** button at the top of the window. 

The **Synchronize RMON Rules** window is displayed, as shown in Figure 5-17.



**Figure 5-17:** The Synchronize RMON Rules window

You can resynchronize individual devices or all devices in a device group.

- 2 To select a device group, select Device Group from the pull-down list in the **Source Type** field. A list of device groups will be displayed.  
To select individual devices, select Devices in the **Source Type** field. A list is displayed showing all the Extreme Networks devices managed by EPICenter.
- 3 To add a device or device group to the Selection list, select the device or device group and click **Add ->**. To add all devices or device groups in the list, click **Add All ->**.
- 4 To remove a device or device group from Selection list, select the item and click **<- Remove**. To remove all devices or device groups, click **<- Remove All**.
- 5 Click **Synchronize** to initiate the synchronization process.

The Alarm Manager uses SNMP to retrieve configuration and status information from each selected switch, and updates the database with that information.

- 6 The **Synchronize** function displays a dialog box with status or error information. Click **OK** to continue.
- 7 Click **Close** to exit the **Synchronize RMON Rules** window.

## Configuring Other SNMP Trap Events

There are a number of SNMP events that require configuration on the switch before they can be used in EPICenter alarm definitions. If the configuration is not done on the switch, no trap events are generated, and therefore no EPICenter alarms for those events will occur. The Ping and OSPF traps fall into this category.

To configure the switch to send one of these traps, you must use a tool that allows you to set the value of the appropriate SNMP variable. Tools such as `SNMPC` can be used to perform this function. The following information assumes that you have a thorough understanding of SNMP and an appropriate SNMP utility.

Refer to the appropriate MIBs for details of the variable settings:

- Ping MIB: `pingmib.mib` (RFC 2925)
- OSPF v2 MIB: RFC 1850 or RFC 1850t

## Setting EPICenter as a Trap Receiver

When Extreme devices are added to the EPICenter inventory, they are automatically configured to send traps to the EPICenter server. However, third-party devices are not automatically configured to do so.

If you want alarms to function for third-party devices, you must manually configure the devices to send traps to the EPICenter server.

The information required to set up EPICenter as a trap receiver is the following:

- The IP address of the system where the EPICenter server is running.
- The EPICenter server trap port. By default this is 10550. (This is set in the properties file `extreme.properties`, found in the `<epicenter_installdir>/extreme` subdirectory).
- The EPICenter server community string. This is a string in the form:

`ST.<value of IP address>.<value of trap port>`

The value of the IP address is the decimal equivalent of the hex value of the IP address.

For example, if the IP address of the EPICenter server is 10.0.4.1, you would calculate the decimal equivalent by doing the following:

- a Convert each quad of the IP address to its hex equivalent:

Decimal	Hex
10	a
0	00
4	04
1	01

- b Convert the hex value a000401 into a decimal value, in this case 167773185

- c Put the three components together to form the community string:

```
ST.167773185.10550
```

You can find and verify the value of the community string by using Telnet to log into an Extreme Networks device that is being managed by ExtremeWare EPICenter, and using the ExtremeWare CLI command `show management` to display the list of trap receivers configured for that device. The EPICenter server, and its community string, should be included in this list.

To receive RMON traps, you need to ensure that RMON is enabled on the device. For Extreme devices, you can do this through the ExtremeWare CLI with the command `enable rmon`.

## Writing Tcl Scripts for Alarm Actions

An EPICenter alarm can call a Tcl function as an alarm action. This Tcl function can be a user-defined Tcl script that is executed in the EPICenter server.

There is an example script in the `<epicenter_install_dir>/user/alarms` directory called `example.tcl` that you can use as a guide to writing a Tcl function for an alarm action.

You can access the EPICenter alarm variables for use in your script, as demonstrated in the example script. These variables are defined in Table 5-1 on page 5-12.

## The Tcl Scripting Environment

The scripting environment for alarm actions is a fully operational Tcl environment. In this environment, a Tcl action script can save states across multiple alarms using global

variables, access alarm instance data, access event log data, and access other EPICenter server-side data. In order to protect the EPICenter server from malicious or erroneous alarm action scripts, the alarm script execution environment uses the “safe interpreter” ability of the Tcl system.

The safe interpreter is a slave of the main EPICenter server-side Tcl interpreter (master interpreter). The functions of the safe interpreter are restricted so that it cannot do harm to the overall EPICenter server. A safe interpreter creates a private “sandbox” in which the alarm action scripts executes. The master interpreter hides certain functions from the scripts inside the sandbox. The master interpreter performs some other functions on behalf of the slave interpreter. By performing functions for the slave, the master has a chance to check to see if the slave’s request is valid. If not, the master rejects the slave’s request.

The following table summarizes the Tcl commands that are deemed dangerous for use by a Tcl alarm action script. Some of these commands are removed entirely from the Alarm Tcl environment. Others are aliases so that the master interpreter can intercept the command call to provide restricted operations.

**Table 5-2:** Command Restrictions in EPICenter Tcl Safe Interpreter

Tcl Command	Hidden in Safe Interp	Explicit Hide by EPICenter	Alias in Master	Description
cd	✓			Not allowed
file	✓		✓	Only allow: attime, attributes (read-only), dirname, executable, exists, extension, isdirectory, isfile, join, lstat, mtime, native name, owned, pathtype, readable, readlink, rootname, size, split, stat, tail, type, volume, writable
pwd	✓			Not allowed
exec	✓			Not allowed
glob	✓		✓	Full functions
socket	✓		✓	No server-side socket, client socket is opened in async mode; the opened client socket is placed in nonblocking mode using the default buffer size; the number of open socket is restricted
exit	✓			Not allowed
load	✓			Not allowed

**Table 5-2:** Command Restrictions in EPICenter Tcl Safe Interpreter

source	✓		✓	Only from standard <code>\$tcl_library</code> and <code>user/alarm</code> directory, and subdirectories
configure	✓		✓	All channels are non-blocking by default, cannot set channel to blocking; cannot set channel buffer size
open	✓		✓	Can only open file in <code>user/alarm</code> and its subdirectories; file is opened in nonblocking mode using the default buffer size; number of open file is restricted
vwait	✓			not Allowed
encoding	✓		✓	Cannot change system encoding scheme
after		✓	✓	Cannot do “after ms”, which does not respond to events
puts			✓	puts data to stdout

The following table outlines the EPICenter server side commands that available in the slave through aliases.

EPICenter Command	Alias in Master	Description
extr::query	✓	<p>Retrieve server-side data from the database. Syntax:</p> <pre>extr::query {} ?-raw? sql ?arg arg ...?</pre> <p><b>{}</b>        The first argument must be {}. Using {} signals the command to retrieve data from the EEM server, in which the alarm action scripts are executing.</p> <p><b>-raw</b>     (Optional) If specified, the result of the query is returned unparsed as a string containing the data in the XML format.</p> <p><b>sql</b>       The sql query</p> <p><b>arg ...</b>   Arguments to the sql query for variable substitution</p>

extr::sendMail	✓	<p>Sends e-mail through the EPICenter server. Syntax:</p> <p><b>extr::sendMail toList from subject body ?smtpHost? ?login? ?password?</b></p> <p><b>toList</b> A list of recipient's email addresses</p> <p><b>from</b> The email address of the sender</p> <p><b>subject</b> The subject of the email</p> <p><b>body</b> The text of the email</p> <p><b>smtpHost</b> (Optional) The host ip address of the SMTP host. If not specified, use the default as defined in the alarm system.</p> <p><b>login</b> (Optional) The login name to the SMTP host</p> <p><b>password</b> (Optional) The password to the SMTP host</p>
extr::postEvent	✓	<p>Log an event to the server's event log. The event time is logged. Syntax:</p> <p><b>extr::postEvent message</b></p> <p><b>message</b> - the message of the event</p>





# 6 Configuration Manager

---

This chapter describes how to use the EPICenter Configuration Manager applet for:

- Uploading configuration settings from one or more devices to EPICenter, on demand or at a predefined (scheduled) time.
- Downloading configuration settings from EPICenter to a device.
- Downloading an incremental configuration to a device.
- Downloading a new ExtremeWare image to one or more devices.
- Downloading a BootROM image to one or more devices.
- Specifying an ExtremeWare software image as the “recommended” image. The Configuration Manager will compare the image currently running in a switch to determine if the switch is running the recommended or most current image.
- Specifying and configuring the TFTP server to be used for uploading and downloading configuration settings and software images.
- Searching for a specific device or group of devices.

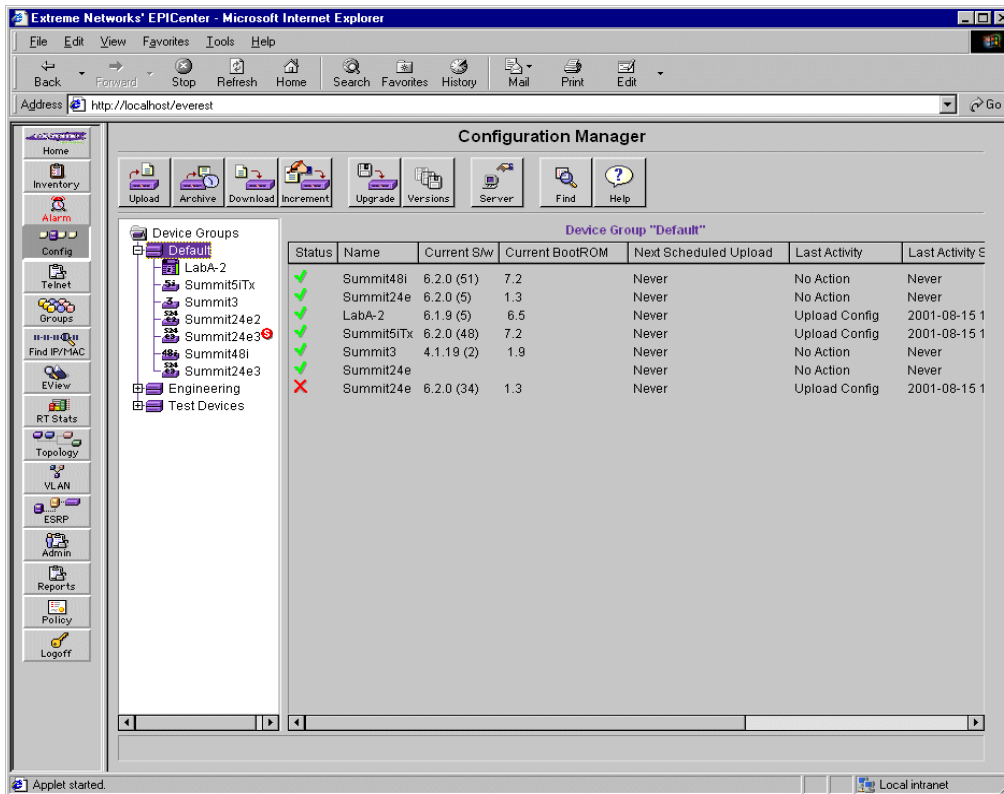
## Overview of the Configuration Manager

The EPICenter Configuration Manager applet provides a graphical interface for uploading and downloading files to and from managed devices. The Configuration Manager also provides a framework for storing the configuration files, to allow tracking of multiple versions. Configuration file uploads can be performed on demand, or can be scheduled to

occur at regular times—once a day or once a week. The Configuration Manager supports Extreme Networks and Cisco devices.



To start the Configuration Manager applet, click the **Config** button in the EPICenter Navigation Toolbar. The Configuration Manager applet appears (see Figure 6-1).

When the applet initially appears, it shows the status of the Device Group(s) defined in EPICenter. Click a device group name in the Component Tree to display the summary status for the devices in the group, as shown in Figure 6-1.

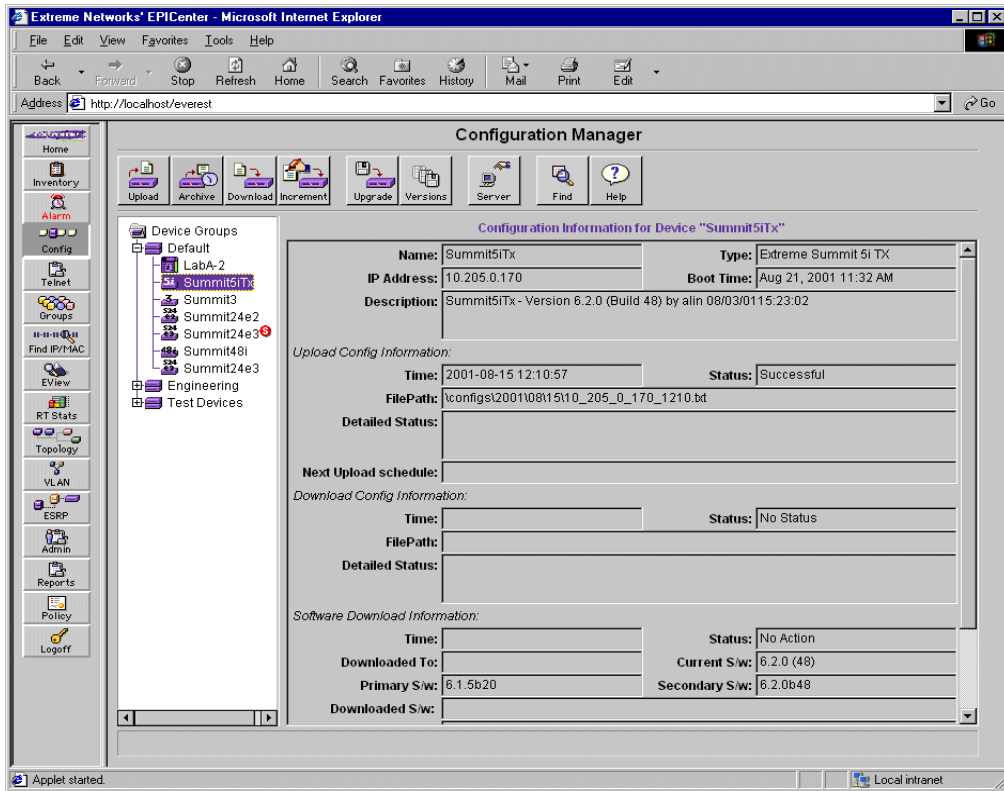


**Figure 6-1:** Configuration Manager showing summary device status

This display shows a summary of the upload and download activity for each managed device, as follows:

- **Status:** the status of the most recent configuration activity. A green check  indicates that the activity was successful. A red X  means that the activity (upload or download) did not complete successfully.
- **Name:** the device name.
- **Current S/w:** The version of the ExtremeWare software that is currently running in the device.
- **Current BootROM:** The version of the bootROM currently running in the device.
- **Next Scheduled Upload:** The date and time for the next Archival upload, if one is scheduled.
- **Last Activity:** The last activity (upload or download of a configuration file, software image, or BootROM) that has taken place through the EPICenter Configuration Manager for this device.
- **Last Activity Schedule:** The date and time that the activity occurred.
- **Last Activity FilePath:** The name and path of the configuration file or image file that was involved in the last activity.

You can display the upload and download status of the configuration information, software, and BootROM by clicking on an individual device in the Component Tree in the left-hand panel of the window. This displays a status window for the device similar to the one shown in Figure 6-2.



**Figure 6-2:** Configuration and Software status for an individual device

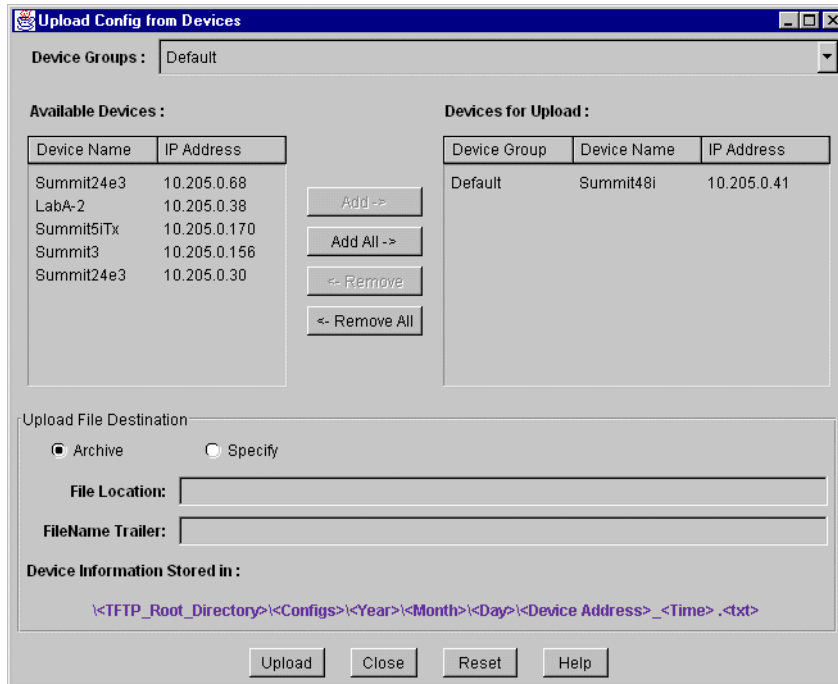
The device status window displays the following information:

- The success status, timestamp, and file name and location for configuration uploads and downloads. If archiving is scheduled, it also displays the time of the next scheduled archive.
- The success status, timestamp, and versions for software downloads, as well as version information for both the primary and secondary software stores.
- BootROM version information (at the bottom of the scrollable window, not visible in Figure 6-2).

# Uploading Configurations from Devices

To upload the configuration information from one or more devices, click the **Upload** button at the top of the window.

The **Upload config from devices** window appears, as shown in Figure 6-3.



**Figure 6-3:** The Upload Config window

To upload device configurations to EPICenter, do the following:

- 1 Select a Device Group in the **Device Groups** field. The devices that belong to this group are displayed in the **Available Devices** list.
- 2 From the **Available Devices** list, select the devices from which you want to upload configuration information, then click the **Add->** button.

If you want to upload from all the devices in the Device Group, click the **Add All->** button.

The devices you select will be moved to the **Devices for Upload** list.

To remove devices from the **Devices to Upload** list, select the devices and click the **<-Remove** button. This moves the selected devices back to the **Available Devices** list. Click **<-Remove All** to move all the devices in the **Devices for Upload** list back to the **Available Devices** list.

### 3 Specify where the uploaded information should be stored:

- a Select **Archive** to create files for each upload under the ExtremeWare EPICenter **Configs** directory, in a subdirectory hierarchy organized by year, month, and day. The form of the fully-qualified file names for these files is:

```
<tftp_root>\configs\<year>\<month>\<day>\<device_address>_<time>.txt
```

where *<tftp\_root>* is the location of your TFTP server. By default, *<tftp\_root>* is *<EPICenter\_install\_dir>\user\tftp*.

*<EPICenter\_install\_dir>* is the EPICenter installation directory, by default by default *epc3\_1*.

For example, a file uploaded from device Summit24 (10.205.0.25) on September 1, 2000 at 8:06 am, would be saved as follows:

```
EPC3_1\user\tftp\configs\2000\Sept\01\10.205.0.25_0806.txt
```



*If you have reconfigured your TFTP root directory (see “Configuring the TFTP Server” on page 6-16), the configs subdirectory will be found directly below (as a child of) your TFTP root directory.*

- b Select **Specify** to specify your own directory structure and file naming convention relative to the TFTP root’s *configs* subdirectory. The structure will be of the form:

```
<tftp_root>\configs\<file_location>\<device_address>_<filename_trailer>.txt
```

In the **File Location** field, specify the *<file\_location>* path where the files should be stored, starting from the *configs* subdirectory. **DO NOT** include *<tftp\_root>\configs* as part of the path; just include the remaining path.

In the **FileName Trailer** field, you can specify a string to be appended to the device address to create a file name. For example, if you specify a file name trailer of “week\_8\_backup” then the filename for the device Summit24 would be

```
10.205.0.25_week_8_backup.txt.
```

### 4 Click **Upload** to start the upload process.

The **Reset** button restores all the fields to their initial state.

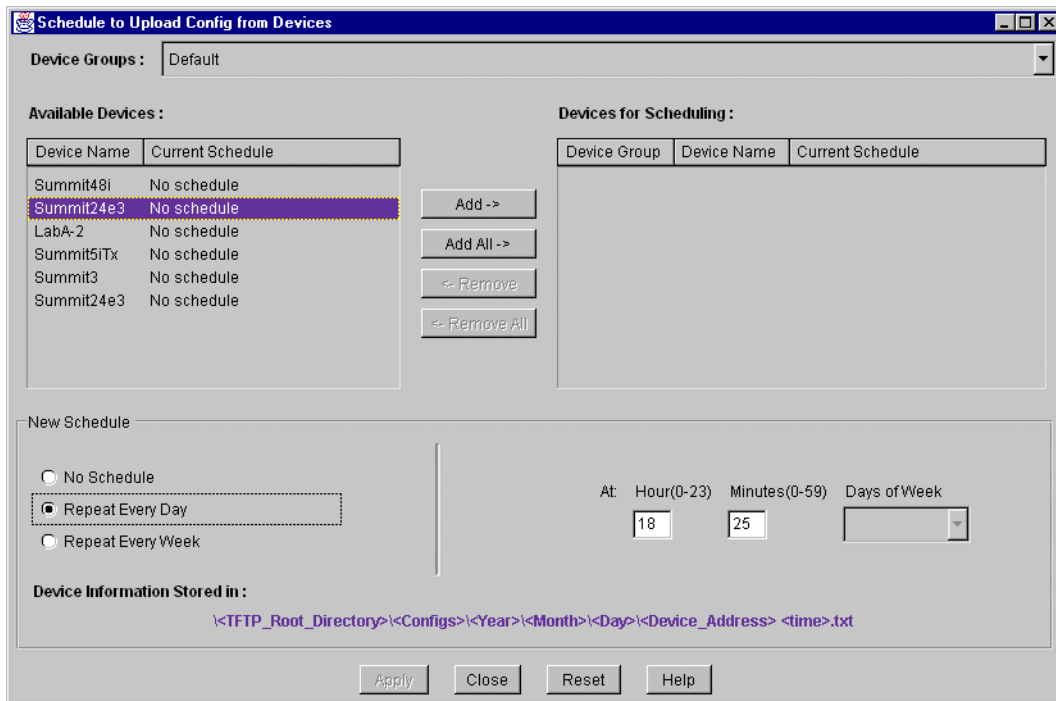
# Archiving Configuration Settings

You can schedule the uploading (archiving) of configuration information so that it is done automatically, either once a day or once a week.

A device, a set of devices, or one or more device groups can be scheduled for archive individually and independently of other device upload schedules.

To schedule device configuration archive uploads, click the **Archive** button at the top of the window.

The **Schedule Upload Config on devices** window appears, as shown in Figure 6-4.



**Figure 6-4:** Schedule Upload Config window

To schedule the upload of device configurations, do the following:

- 1 Select a Device Group in the **Device Groups** field. The devices that belong to this group are displayed in the **Available Devices** list.
- 2 From the **Available Devices** list, select the devices for which you want to schedule the upload of configuration information, then click the **Add->** button.

If you want to create the same schedule for all the devices in the Device Group, click the **Add All->** button.

The devices you select will be moved to the **Devices for Scheduling** list.

To remove devices from the **Devices to Scheduling** list, select the devices and click the **<-Remove** button. This moves the selected devices back to the **Available Devices** list. Click **<-Remove All** to move all the devices in the **Devices for Scheduling** list back to the **Available Devices** list.

- 3 Specify the schedule you want:

**No Schedule** will remove any schedule associated with the selected device(s).

**Repeat Every Day** indicates that the upload should be done every day at the specified time. When you select this option, you will be able to specify the time of day (the hour and minutes) at which the upload should be done.

**Repeat Every Week** indicates that the upload should be done every week at the specified day and time. When you select this option, you will be able to specify the time of day (the hour and minutes), and the day of the week at which the upload should be done.

- 4 Click **Apply** to have the upload schedule set for these devices.

Click the **Reset** button to return the schedule to its state when you initiated this window.

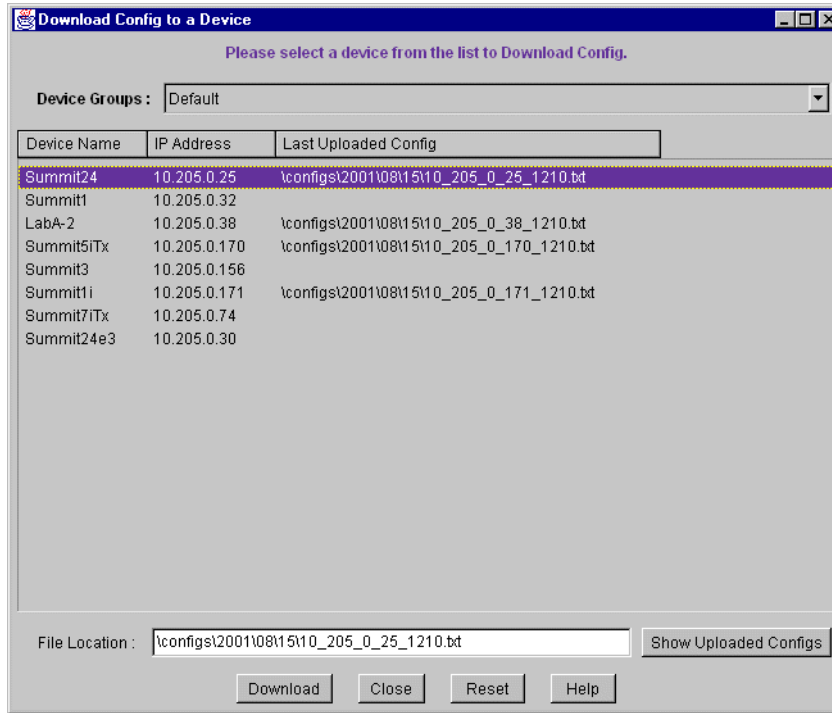
## Downloading Configuration Information to a Device

Downloading a configuration does a complete configuration download, resetting the current switch configuration and replacing it entirely with the new downloaded configuration. The switch will be rebooted automatically after the download has completed.

To download saved configuration information to a device, click the **Download** button at the top of the window.



The **Download Config to a device** window appears, as shown in Figure 6-5.



**Figure 6-5:** Download configuration window

To download a configuration to a device, do the following:

- 1 Select the device from the device list presented. You can only download to one device at a time.  
If configuration information has been uploaded from the device, the file where it was saved is listed in the **Last Uploaded Config** column.
- 2 In the **File Location** field, type the location and name of the file you want to download, or click the **Show Uploaded Configs** button and select the file to be downloaded.  
The Browse pop-up displays the list of uploaded files for the selected device.
- 3 To start the download, click the **Download** button.



*When the download completes, the switch will be rebooted.*

*The EPICenter software does not save the configuration on the device after the reboot. You can use the Telnet applet to open a telnet session on the affected devices and execute a save configuration command.*

## Downloading an Incremental Configuration to Devices

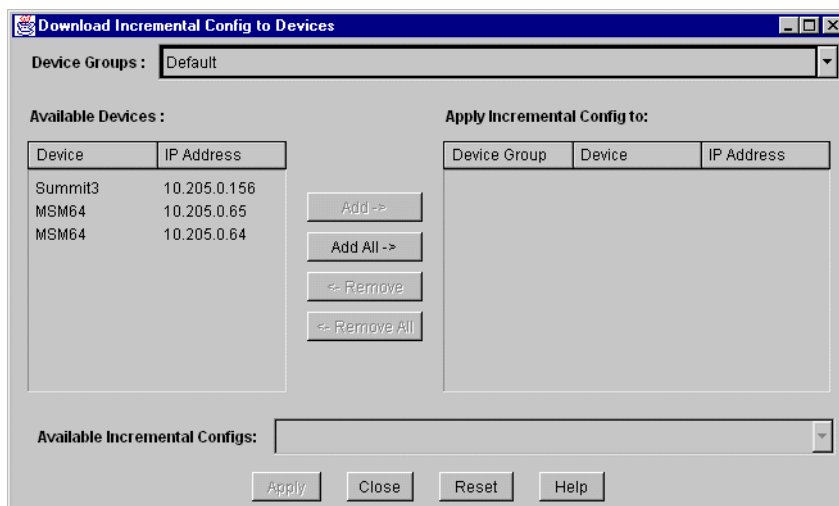
You can create or designate a set of configuration information to be used as a baseline configuration for devices running ExtremeWare 6.0 or later. Using an incremental download to execute a baseline configuration provides a known, “standard” configuration that you can use to ensure that devices are configured into a known state. For example, if you want to set a group of devices to the same basic configuration, you can first set individual IP addresses on each device, and then use the incremental configuration download feature to set all other configuration settings on all devices to a common state.

An incremental configuration download executes only the commands specified in the incremental download file. It does not reset the switch configuration or replace any other configuration settings that may exist in the device. No reboot is necessary. The EPICenter incremental download does not save the configuration; you must do so

Incremental downloads are supported on Extreme Networks devices running ExtremeWare 6.0 or later.

To download an incremental configuration to a device, click the **Incremental** button at the top of the window.

The **Download Incremental Config To Devices** window appears, as shown in Figure 6-6.



**Figure 6-6:** Download incremental configuration window

From this window, do the following:

- 1 Select a Device Group in the **Device Groups** field. The devices that belong to this group are displayed in the **Available Devices** list.
- 2 From the **Available Devices** list, select the devices for which you want to download the baseline configuration, then click the **Add->** button.

If you want to download the baseline configuration to all the devices in the Device Group, click the **Add All->** button.

The devices you select will be moved to the **Apply Incremental Config to:** list.

To remove devices from the **Apply Incremental Config to:** list, select the devices and click the **<-Remove** button. This moves the selected devices back to the **Available Devices** list. Click **<-Remove All** to move all the devices in the **Apply Incremental Config to:** list back to the **Available Devices** list.

- 3 Select the baseline configuration you want to download from the pull-down list in the **Available Incremental Configs** field.
- 4 Click **Apply** to start the baseline download to the selected device.



*The EPICenter software does not save the configuration on the device after the download. You can use the Telnet applet to open a telnet session on the affected devices and execute a save configuration command.*



*The Configuration Manager will display an error if you attempt an incremental download on a switch running a version of ExtremeWare prior to 6.0.*

## Creating an Incremental Configuration File

The purpose of an incremental configuration is to provide a set of known, standard configuration settings you can download to a device to restore it or initialize it to a known software state.

To create an incremental configuration, you can start with a configuration file you have uploaded, or one of the standard configurations. You can edit it, if needed, to reflect the basic configuration settings you want to use as your baseline configuration, and to remove settings you don't want changed.

Incremental configuration files must be stored in the `<tftp_root>\baselines` directory,

where `<tftp_root>` is the location of your TFTP server. By default, `<tftp_root>` is `<EPICenter_install_dir>\user\tftp`.

`<EPICenter_install_dir>` is the EPICenter installation directory, by default `epc3_1`. Thus, if you installed the EPICenter server under Windows NT using the default installation path, your incremental configurations must be in `epc3_1\user\tftp\baselines`, unless you have reconfigured your TFTP root directory.

You can name an incremental configuration file any way you want.



*If you have reconfigured your TFTP root directory (see "Configuring the TFTP Server" on page 6-16), the baselines subdirectory will be found directly below (as a child of) your TFTP server root directory.*

## Upgrading Device Software Images

The ExtremeWare software image contains the executable code that runs on the switch. An image comes pre-installed from the factory on every switch. You can upgrade this image by downloading a new version through the Configuration Manager. You can download the image into either the primary or secondary image, and specify whether the switch should be rebooted to use the new image.

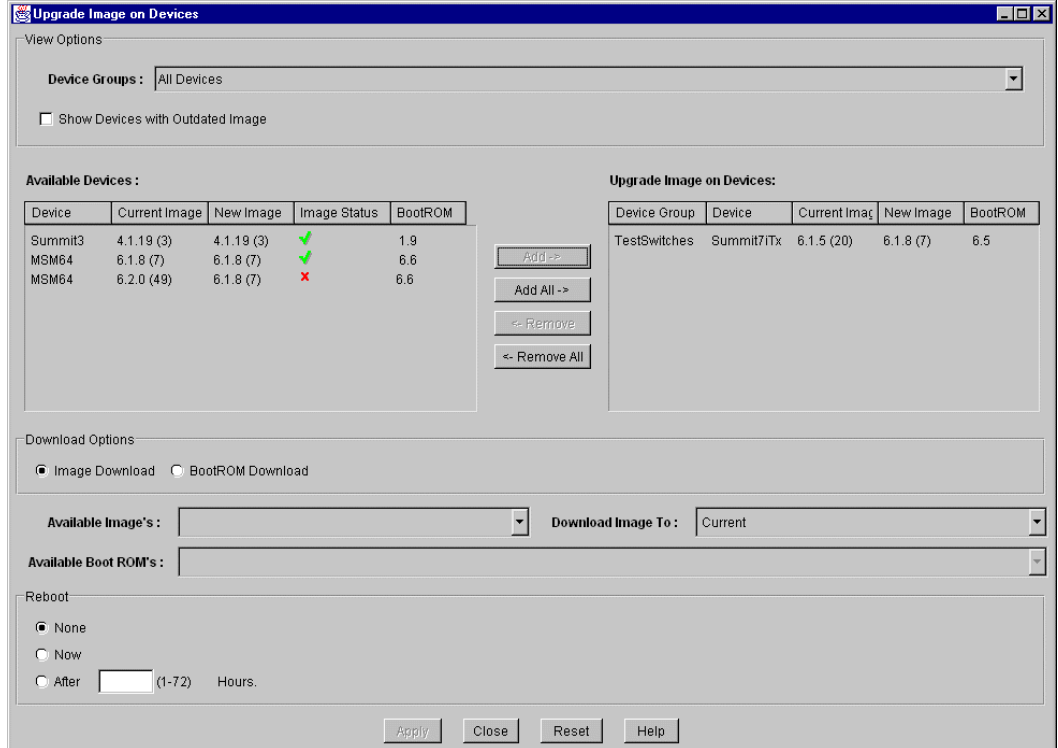
The BootROM software initializes certain important switch variables during the switch boot process.



If a BootROM upgrade does not complete successfully, it could prevent the switch from booting.

To download a new ExtremeWare software or BootROM image to an Extreme device, click the **Upgrade** button at the top of the window.

The **Upgrade Image on Devices** window appears, as shown in Figure 6-7.



**Figure 6-7:** Upgrade Image on Devices window



To download a new software image to one or more Extreme Devices, do the following:

- 1 Select a device group or **All Devices** from the drop-down menu in the **Device Groups** field.

The devices that belong to this group are displayed in the **Available Devices** list.

Click the **Show Devices with Outdated Images** button to show only devices with images that differ from the image you specified in the **Versions** window.

The entries in the **Current Image**, **New Image**, and **Image Status** columns let you determine which switches have outdated software images.

- The **Current Image** shows the image currently running in the device.
  - The **New Image** information comes from the information you provide in the **Versions** window for devices of this type (see “Specifying the Current Software Versions” on page 6-15). If you have not specified a software version in the Versions window, this will be blank.
  - **Image Status** shows the status of the image compared to the version shown in the New Image column. A green check  indicates that the version running in the device and the New Image version are the same. A red X  indicates that the image running in the device differs from the New Image version. The status is also shown as a red X if the New Images column is blank.
  - The **BootROM** column shows the version of the BootROM running on the device.
- 2** From the **Available Devices** list, select the devices you want to upgrade, then click the **Add->** button.

If you want to upgrade the images on all the displayed devices, click the **Add All->** button.

The devices you select will be moved to the **Upgrade Image on Devices** list.

To remove devices from the **Upgrade Image on Devices** list, select the devices and click the **<-Remove** button. This moves the selected devices back to the **Available Devices** list. Click **<-Remove All** to move all the devices in the **Upgrade Image on Devices** list back to the **Available Devices** list.

- 3** In the **Image Options** box select the type of upgrade you want to perform:
- Click the **Image Download** button to specify a software image upgrade.
  - Click the **BootROM Download** button to specify a BootROM upgrade.
- 4** For a software image upgrade do the following:
- a** Select the software image you want to download from the drop-down menu in the **Available Images** field.



*Note that there are different images for Summit devices and the “i” Series devices. If you try to download an incompatible image, you will receive an error message.*

Standard images as shipped by Extreme Networks are provided in the directory `<EPICenter_install_dir>\user\tftp\images` directory (by default `epc3_1\user\tftp\images` in the Windows operating environment, or `/opt/epc3_1/user/tftp/images` on a Solaris system).

You can check the Extreme Networks web site for the availability of newer software releases.

- b** Select the download target in the **Download Image To** field: Current, Primary, or Secondary.
- 5** For a BootROM upgrade, select the BootROM image you want to download from the drop-down menu in the **Available BootROMs** field.

Standard BootROM images are provided in the directory `<EPICenter_install_dir>\user\tftp\bootrom` directory (by default `epc3_1\user\tftp\bootrom` in the Windows operating environment, or `/opt/epc3_1/user/tftp/bootrom` on a Solaris system).

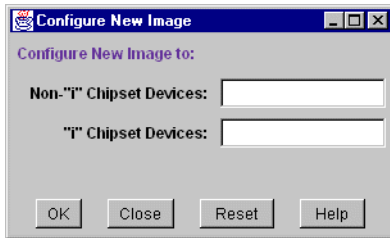
- 6** Indicate whether the devices should be rebooted:
  - Click **None** to indicate the devices should not be rebooted.
  - Click **Now** to indicate the devices should be rebooted immediately after the download.
  - Click **After** to indicate the devices should be rebooted at a later time, and enter the number of hours (up to 72) to wait before doing the reboot.
- 7** Click **Apply** to start the software download to the selected devices.  
Click **Reset** to return the window to its initial state (removing all devices from the **Upgrade Image on Devices** list, removing all image selections, and so on).
- 8** When the upgrade process has completed, click **Close** to close the **Upgrade Image on Devices** window.

## Specifying the Current Software Versions

The **Versions** window lets you specify the current version of the ExtremeWare software for pre-"i" Series devices (Summits/Black Diamonds) and "i" Series devices.

This information is used by the EPICenter software to determine whether an individual device is running the version you have specified as the "current version." This is the version that appears in the **New Image** column in the **Upgrade Image on Device** window.

Click the **Versions** button at the top of the window to display the **Configure New Image** window, as shown in Figure 6-8.



**Figure 6-8:** Configure New Image window

Enter the version information into the appropriate field. The version information is the version, release, and build number (in parentheses) associated with a specific ExtremeWare software release. For example, for a Summit device this could be a version such as 4.1.19 (2) or 5.0.4 (3). For the “i” chipset devices, it should be 6.1.5 (20) or later.



*You must specify the version exactly in its correct form, including periods, spaces, and parentheses. For example, version 6.1.5 b20 must be specified as “6.1.5 (20)”, with a space between the 5 and the “(“. The version names are always in the form #.#.#\_(#) where # is a numeric, and \_ indicates a space.*

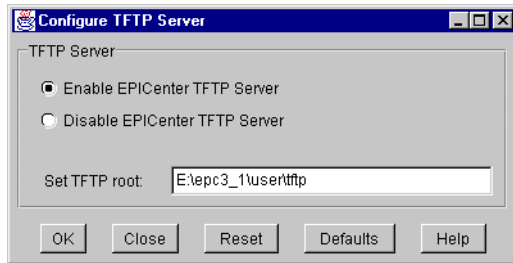
## Configuring the TFTP Server

If you already have a TFTP server installed on the system where the EPICenter server is running, you may choose to use that TFTP server instead of the one provided with EPICenter. This is the server that actually does the downloading and uploading from the devices.

The **Server** function lets you enable or disable the embedded TFTP server, and specify an alternate path for the location of the server.

Click the **Server** button at the top of the window to display the **Configure TFTP Server** window, as shown in Figure 6-9.





**Figure 6-9:** Configure TFTP Server window

By default, the embedded TFTP server is enabled.

- Click the **Disable EPICenter TFTP Server** button to disable the server. You can then provide a path in the Set TFTP Root field to the location of a different TFTP server.
- Click the **Enable EPICenter TFTP Server** button to enable the server.



*If you disable the server, you will not be able to upload or download configuration information or software to your devices, unless you provide a path to an alternate TFTP server.*

- To change the location of the TFTP server root, change the path in the **Set TFTP Root** field.

By default, the TFTP server is installed in `<epicenter_install_dir>\user\tftp` where `<epicenter_install_dir>` is the directory where the EPICenter server is installed. By default, the TFTP server is found in `epc3_1\user\tftp` in the Windows operating environment, or `/opt/epc3_1/user/tftp` on a Solaris system.

EPICenter will create four subdirectories (`baselines`, `bootrom`, `configs`, and `images`) as children of the directory you specify as the TFTP server root.



*If you plan to use this TFTP server with other software, such as the ExtremeWare CLI or for any other purpose, be aware of possible differences in the expected locations of the TFTP server and other components such as ExtremeWare software images or configuration files. See the ExtremeWare EPICenter SE Release Note and Quick Start Guide for information on any known issues.*

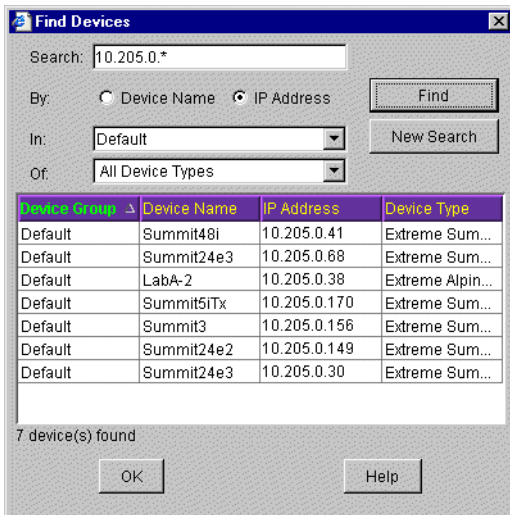
# Finding Devices

You can search for a device in the EPICenter database by name, by IP address, or by type of device. This may be useful if you have a large number of devices in your inventory.

To search for a device, follow these steps:

- 1 Click **Find** at the top of the Inventory Manager page.

The Find Devices dialog, shown in Figure 6-10, is displayed.



**Figure 6-10:** Find Devices dialog

- 2 Enter your search criteria:

You can search for devices by name or by IP address. You can limit the search to a specific device group, or to a specific type of Extreme device. Search criteria can include:

- A device name. Click the **Device Name** button, and enter a complete or partial name in the **Search:** field.
- An IP address. Click the **IP Address** button and enter a complete or partial IP address in the **Search:** field. You can use the wild card characters \* or ? in your search criteria.
  - \* acts as a wildcard for an entire octet (0-255)

**?** is a wildcard for a single digit (0-9)

- A device group. Select the device group from the drop-down menu in the device group field. If you do not specify a name or IP address in the Search field, all devices in the device group you select will be found.
  - A device type. Select the device type from the drop-down menu in the type field. If you do not specify a name or IP address in the Search field, all devices of the type you select will be found.
- 3** Click **Find** to search for devices that meet the criteria you have specified. All devices found are listed in the center panel. Information includes the device group in which the device can be found, its name, IP address, and the type of device.
  - 4** Double-click on a device in the results table to highlight the device in the Component Tree, and to display the configuration information for that device.
  - 5** Click **New Search** to clear all search criteria.
  - 6** Click **OK** to close the search window.

# 7

## Using the Interactive Telnet Application

---

This chapter describes how to use the Interactive Telnet application for:

- Configuring Extreme devices using Telnet and the ExtremeWare Command Line Interface (CLI)
- Configuring third-party devices using interactive Telnet

### Overview of the Interactive Telnet Applet

Users with Administrator or Manager access can view and modify configuration information for Extreme switches (Summit, Alpine, and Black Diamond switches) and third-party devices managed by EPICenter using Telnet and the ExtremeWare Command Line Interface (CLI). You can also use the interactive Telnet capability to view and modify configuration information for third-party devices being managed by EPICenter.

The Telnet application provides two usage modes:

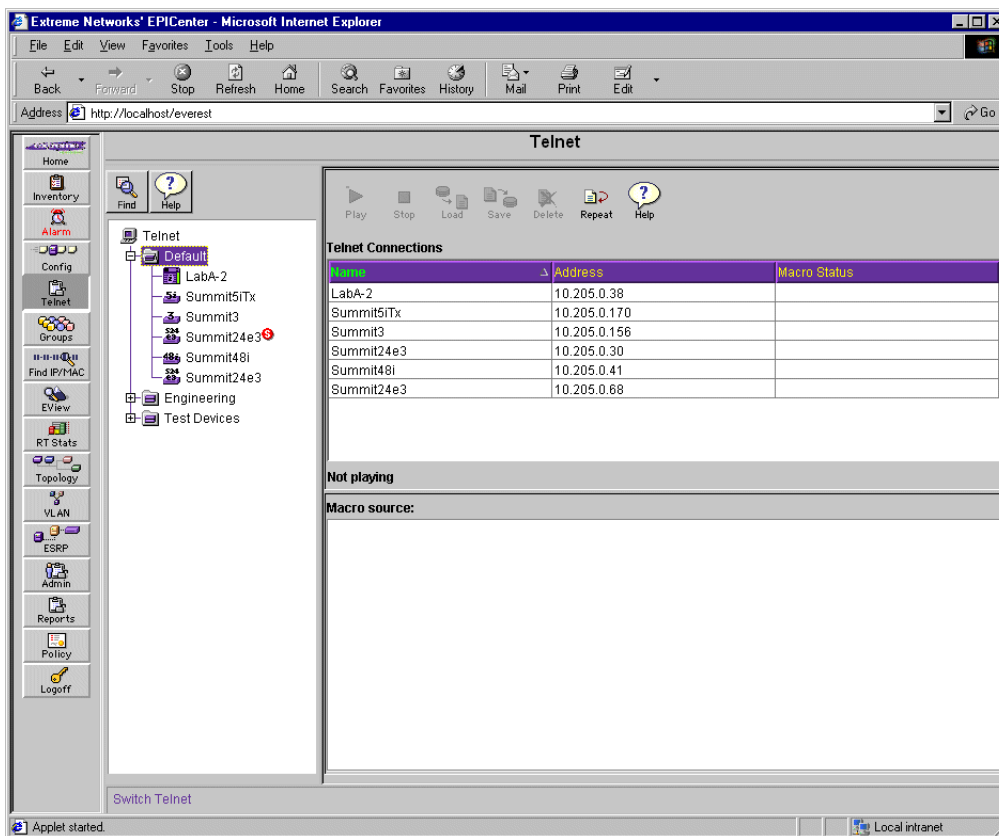
- A Macro View, where you can set up CLI command macros, and run them on multiple switches in a single operation. You set a macro to run repeatedly, and can save them in the EPICenter database for future use.
- An individual session mode, where you can open a session on an individual device, and execute commands just as you would from a standard Telnet interface.

# Using Telnet with Extreme Switches

The Telnet applet allows the scripting and playback of groups of CLI commands (macros) to a selection of Extreme switches. You can also use this applet to run an interactive Telnet session on an individual switch, including third-party switches.

Select **Telnet** from the Navigation Toolbar to display the Telnet module.

Select a device group in the Component Tree to display the Telnet Macro view for the devices in that device group, as shown in Figure 7-1.



**Figure 7-1:** The Telnet applet, macro interface

The **Telnet Connections** list displays the switches in the device group, and shows the status of any macros that have run or are being run on the switch. If macros are not supported on an individual switch (true of third party switches and a few Extreme switches) the Macro Status will be “Macros not supported.”



*If a switch is not supported by the EPICenter interactive Telnet feature, it will not appear in the Telnet Connections list, or in the Component Tree in this applet. The Summit24e2T and Summit24e2X are examples of devices that are not supported in the EPICenter Telnet applet.*

When a Telnet session is currently open on a switch, the switch name is highlighted in bold in the list of switches in the Component Tree.

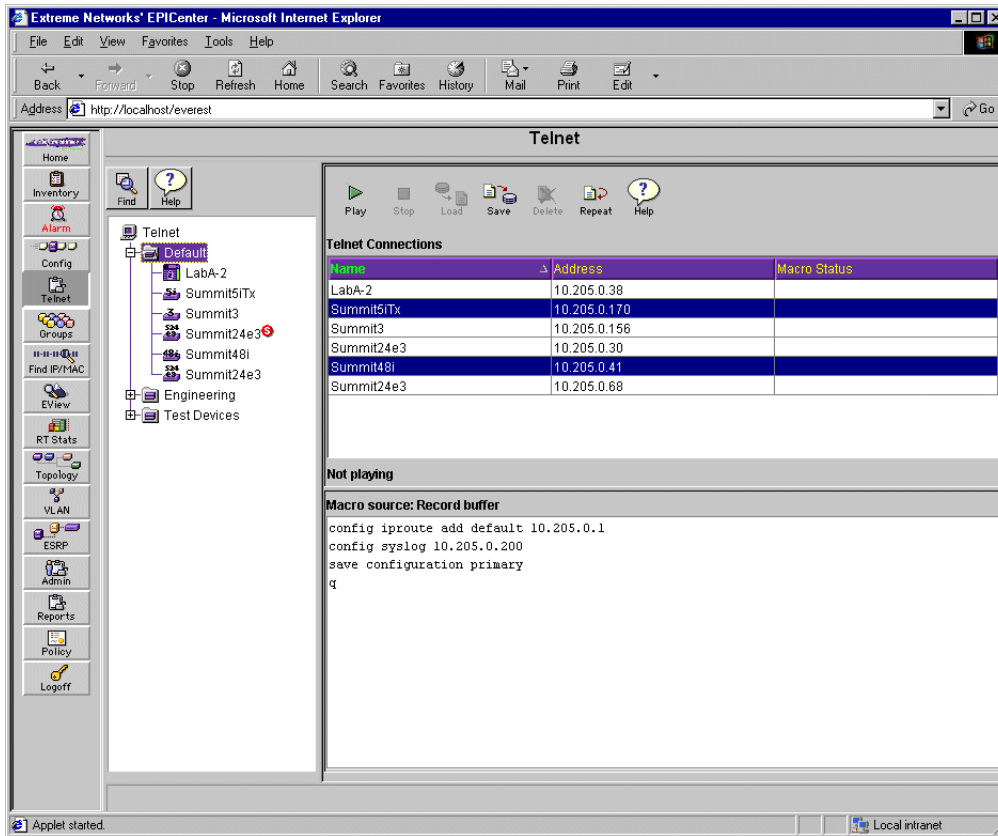


*If a switch displayed in the Component Tree has an “S” in a red circle along with the name, that means that the switch is not responding to SNMP requests. However, the switch may still respond to HTTP or Telnet requests.*

## Running ExtremeWare Command Macros

The lower half of the Macro view page contains the macro command buffer. You can enter a series of ExtremeWare commands into this buffer, which will form a script that can be played to the set of switches you select in the **Telnet Connections** list.

Figure 7-2 shows a command script entered into the buffer.



**Figure 7-2:** The Telnet record and play buffer

To create a macro for playback to a set of Extreme switches, follow these steps:

- 1 In the **Telnet Connections** list, select the set of switches where you want your command macro to run. The switches need not have a Telnet session already open—the macro play function will open a connection and log into the switch.

- 2 Enter a series of ExtremeWare commands into the macro buffer.

There are three ways to enter commands into the macro buffer:

- Type the commands directly into the buffer.
- Cut or copy commands from another location, either elsewhere in the buffer or from an external document, and paste them into the buffer.

Click the right mouse button anywhere in the macro buffer to display a pop-up edit menu which provides copy and paste functions. You can copy text from within the macro buffer using the copy function from the pop-up menu. From an external document, cut or copy text into the clipboard, then use the paste function from the pop-up edit menu.



*You cannot use the browser cut and paste functions for this purpose.*

— Load a saved macro (see “Saving a Macro in the EPICenter Database” on page 7-7).

The source of the commands in the macro buffer is indicated by the **Macro Source:** field at the top of the macro buffer panel.

There are four variables you can use in an ExtremeWare CLI command that will be expanded when the target switch is contacted. These are:

**Table 7-1:** ExtremeView Macro Variables

Variable	Definition
<NAME>	The name of the switch
<DATE>	The current date of the EPICenter server
<TIME>	The current time of the EPICenter server
<ADDRESS>	The IP address of the switch

For example, you can enter the command

```
upload config 45.1.12.101 extreme/<NAME>.cfg
```

and the macro substitutes the name of each switch on which it executes the macro.

These variables can only be used in macros, not in an interactive Telnet session.



*Because macros are intended for unattended, batch-type use, you should not use interactive commands in a macro. They may cause the command to run in a loop.*

- 3 To set the macro so that it plays back repeatedly at a specified interval, click the **Repeat** button to display the Macro Repeat pop-up window.
  - a Check the **Repeating** check-box.
  - b Enter an interval (in seconds) in the **Repeat Delay** field.
  - c Click **OK**.



- 4 Click **Play** to initiate playback of the macro on the selected switches. This opens a connection to the switch, logs in using the switch login and password as specified in the Inventory Manager, and runs the macro.

If the macro is a repeating macro, it will repeat sequentially on all selected switches until you click **Stop**.

You can execute just a portion of a macro by highlighting just the portion of the macro that you want to execute. Only the selected portion will execute when you initiate the playback. This will not affect saving the macro—the entire macro will be saved even if only a portion is highlighted.

The **Macro Status** column in the **Telnet Connections** table indicates the status of the macro as execution progresses on the selected switches. The states are:

- **Pending**—the macro is intended to run on this switch, but has not yet started.
- **Playing**—the macro is currently running.
- **Stopped**—the macro was stopped before it completed.
- **Complete**—the macro has completed running.
- **Macros Not Supported**—macros cannot be run on this device (may appear if you select a non-Extreme device or the Summit Px1 or Summit 24e2T/X devices).
- **Not Available**—macros cannot be run on this device (may appear if you select a non-Extreme device).
- **Failed**—a failure occurred when the macro was run. This is frequently due to an inability to connect to the switch.



*Macro play will be automatically stopped if you exit the Telnet applet (by selecting another applet or logging out) while a macro is running.*

The Telnet session is usually left open after the macros complete. However, EPICenter allows only five Telnet sessions to be open concurrently. Therefore, if you select more than five switches for macro playback, EPICenter will open five connections, then close the oldest (the first connection) in order to open a connection on the sixth switch, and so on. When macro playback has completed on all the selected switches, the Telnet sessions are left open on the last five switches. Open telnet sessions are indicated by displaying the switch name in bold in the Component Tree.

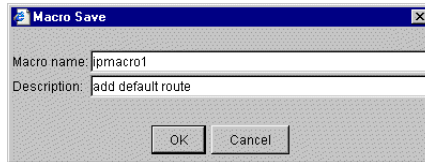
Any open Telnet sessions will be closed when you leave the Telnet applet to view a different EPICenter applet.

To view the results of the macro execution on a particular switch, select the switch in the Telnet switch list in the Component Tree. This displays the active Telnet session running on

the switch, and you can view the progress of the macro as the various ExtremeWare commands are executed.

### Saving a Macro in the EPICenter Database

To save a macro you've defined, click the **Save** button. This displays the **Macro Save** pop-up window (see Figure 7-3).

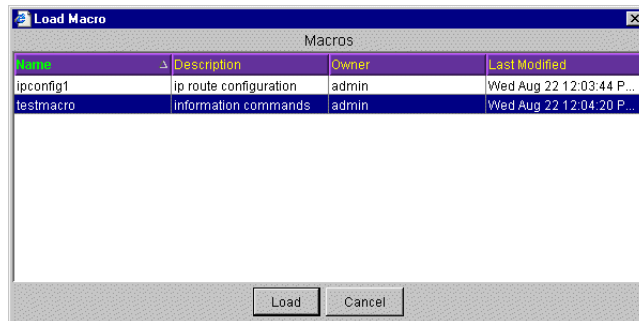


**Figure 7-3:** Saving a macro to the database

Enter a name for the macro, an optional description, and click **OK**.

All current contents of the macro buffer will be saved in the database under the name you specify. Selecting a portion of the macro (to playback only part of the macro) does not affect the save function.

To load a saved macro, click the **Load** button. This displays the **Load Macro** pop-up window (see Figure 7-4).



**Figure 7-4:** Loading a macro from the database

The pop-up window displays the names and descriptions of all saved macros, as well as the owner (EPICenter user) who created the macro, and the time at which it was last saved.

Select the macro you want to load and click **Load**. You can select only one macro to load at a time.

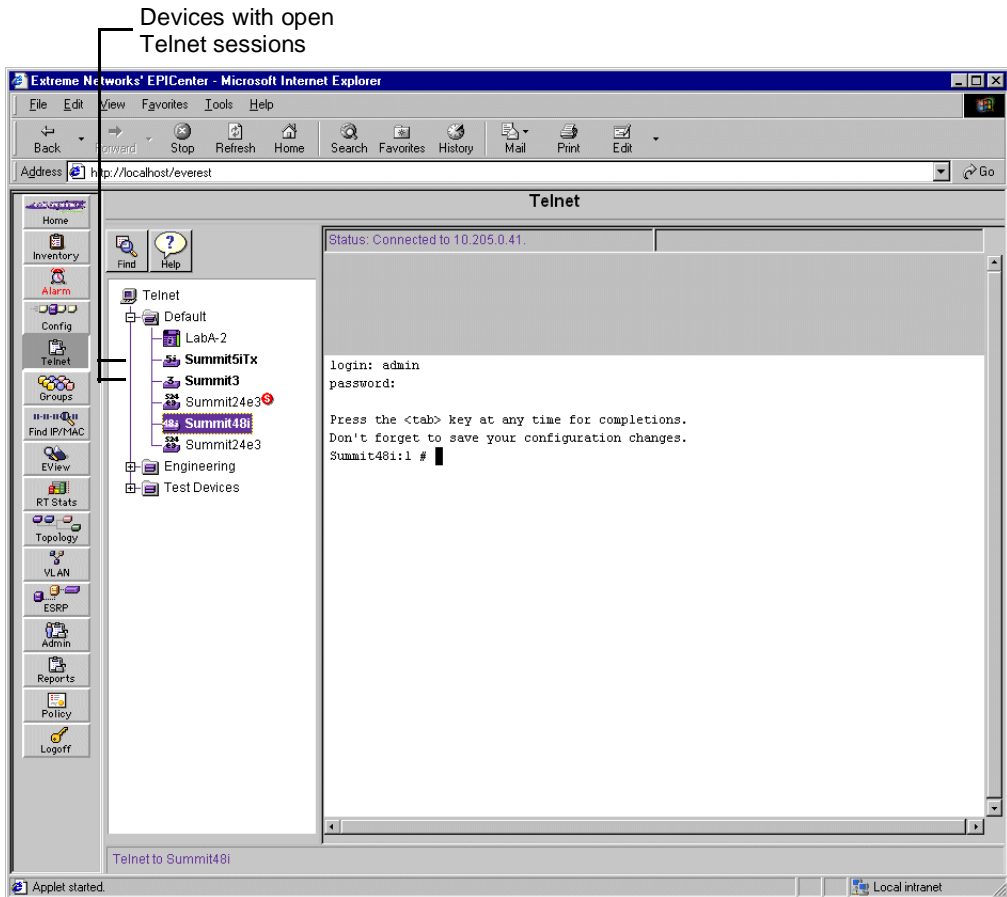
The contents of the saved macro will replace any previous contents in the macro buffer.

You can delete a saved macro by clicking the **Delete** button. A pop-up window similar to the Load Macro window appears. Select one or more macros to delete, then click **Delete**.

You will be asked to confirm the deletion.

## **Running a Telnet Session on an Individual Switch**

You can open a Telnet session on an individual switch by selecting the switch from the Telnet switch list in the Component Tree. This opens a Telnet session to the selected switch, and then waits for command input, just as with any other Telnet session.



**Figure 7-5:** A newly-opened Telnet session

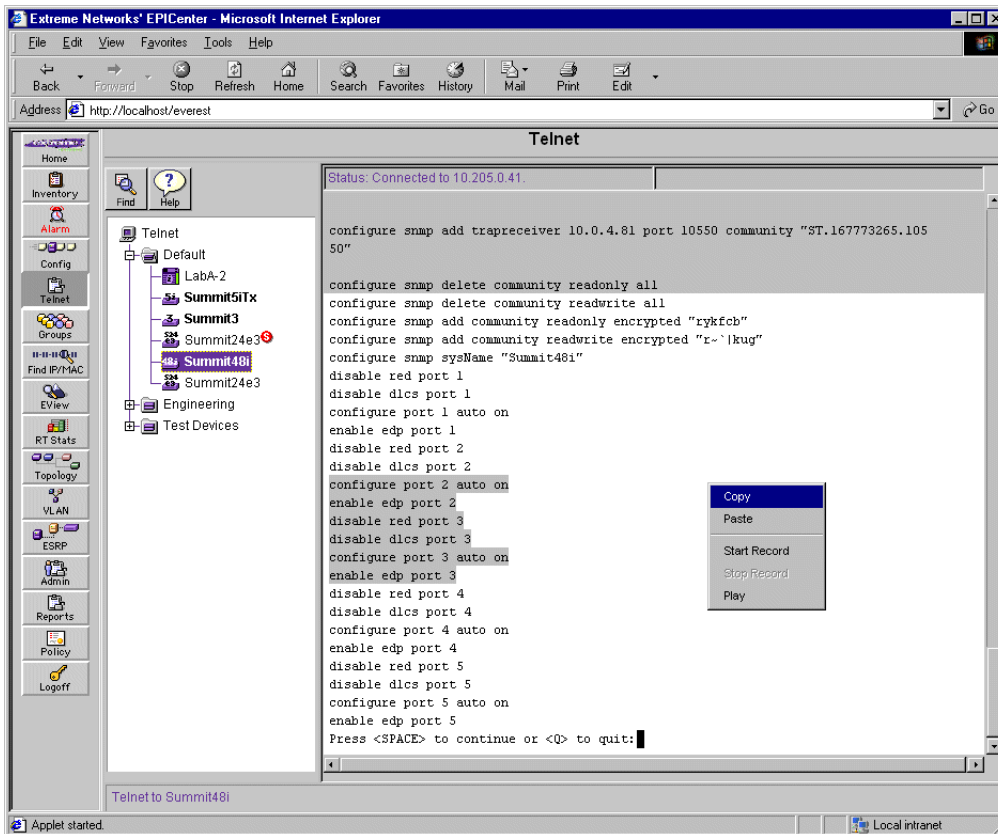
The Telnet session window is a two-tone window—the bottom of the window is white, the top is grey. The last 25 lines of Telnet commands and responses always appear in the white portion of the window. As output grows, the older lines scroll up into the grey portion of the screen. This makes it easy to tell whether you are viewing the most recent Telnet output.

The Telnet session window will display the commands and results from macros that are run on the switch. You can also type in commands individually.

You cannot use the macro variables (<NAME>, <DATE>, <TIME>, <ADDRESS>) in a command you enter interactively.

## Copy/Paste from an Interactive Telnet Session

A copy and paste function is available within an interactive Telnet session. Copy and paste let you copy from one interactive Telnet session into another interactive session or into the macro buffer. You can also paste commands from an external document into an interactive Telnet session. The copy and paste commands reside on a pop-up menu that you can display using the right mouse button (see Figure 7-6).



**Figure 7-6:** An open Telnet session showing the pop-up edit menu

- To copy from an interactive session, highlight the lines you want to copy, click the right mouse button and select **Copy** from the pop-up menu.
- To paste into an interactive Telnet session or into the macro buffer, place the cursor where you want the lines inserted, click the right mouse button and select **Paste** from the pop-up menu.



*You cannot use the browser cut and paste functions for this purpose.*

## Macro Recording and Playback from an Interactive Telnet Session

The record function creates a macro by echoing commands that you type in an interactive Telnet session, into the Macro Record/Play Buffer. The record function is controlled by commands from a pop-up menu displayed by using the right mouse button (see Figure 7-6).

- To start recording a macro, click the right mouse button and select **Start Record** from the pop-up menu  
Everything you type after this is copied into the macro Record/Play Buffer until you select **Stop Record** from the pop-up menu
- To stop recording a macro, click the right mouse button and select **Stop Record** from the pop-up menu
- To play back the macro to multiple switches, select **Telnet** in the Component tree, and play back the macro in the main Telnet page as discussed in the section Running ExtremeWare Command Macros on page 7-3
- To play the macro on an individual switch, select the switch in the Component Tree to display its interactive Telnet session, click the right mouse button, and select **Play** from the pop-up menu

## Using Interactive Telnet with Third-Party Devices

You can open an interactive Telnet session on a third-party device and execute commands interactively. Select the switch from the Telnet device list in the Component Tree. This opens a Telnet session to the selected switch, and waits for input as appropriate to the device's telnet interface. Unlike Telnet to an Extreme Networks switch, it does not log you in to the device. You must log in as required for the device.

You can enter and execute commands using the device's command line interface. The commands and any resulting output will be displayed in the session window just as if you were running a Telnet session on any other client.

The Telnet session window is a two-tone window—the bottom of the window is white, the top is grey. The last 25 lines of Telnet commands and responses always appear in the white portion of the window. As output grows, the older lines scroll up into the grey portion of

the screen. This makes it easy to tell whether you are viewing the most recent Telnet output.

The copy and paste feature, macros, and the macro variables (<NAME>, <DATE>, <TIME>, <ADDRESS>) are not supported for third-party devices.

To close the Telnet session, type the appropriate exit command on the command line. The session will be closed automatically when you exit the Telnet applet.

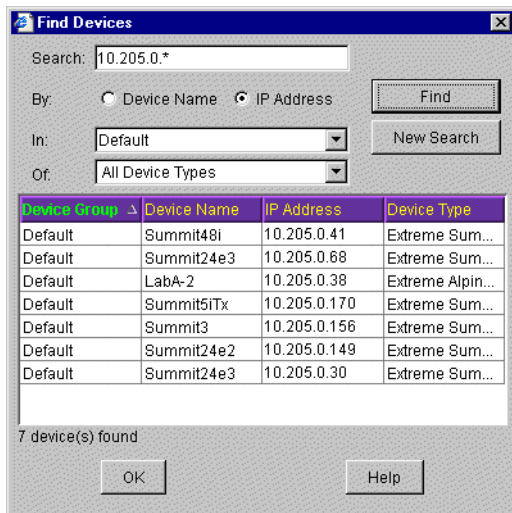
## Finding Devices

You can search for a device in the EPICenter database by name, by IP address, or by type of device. This may be useful if you have a large number of devices in your inventory.

To search for a device, follow these steps:

- 1 Click **Find** at the top of the Inventory Manager page.

The Find Devices dialog, shown in Figure 7-7, is displayed.



**Figure 7-7:** Find Devices dialog

- 2 Enter your search criteria:

You can search for devices by name or by IP address. You can limit the search to a specific domain, or to a specific type of Extreme device. Search criteria can include:

- A device name. Click the **Device Name** button, and enter a complete or partial name in the **Search:** field.
  - An IP address. Click the IP Address button and enter a complete or partial IP address in the **Search:** field. You can use the wild card characters \* or ? in your search criteria.
    - \* acts as a wildcard for an entire octet (0-255)
    - ? is a wildcard for a single digit (0-9)
  - A device group. Select the device group from the drop-down menu in the device group field. If you do not specify a name or IP address in the Search field, all devices in the device group you select will be found.
  - A device type. Select the device type from the drop-down menu in the type field. If you do not specify a name or IP address in the Search field, all devices of the type you select will be found.
- 3** Click **Find** to search for devices that meet the criteria you have specified. All devices found are listed in the center panel. Information includes the domain in which the device can be found, its name, IP address, and the type of device.
  - 4** Double-click on a device in the results table to highlight the device in the Component Tree, and to initiate a telnet session on the device (see “Running a Telnet Session on an Individual Switch” on page 7-8).
  - 5** Click **New Search** to clear all search criteria.
  - 6** Click **OK** to close the search window.





# The Grouping Manager

---

This chapter describes how to use the Grouping Manager to do the following:

- Create new groups.
- Create new user or host resources.
- Add resources or groups to a parent group.
- Define relationships between resources.
- Add attributes to a resource or a group.
- Searching for resources.
- Import users and hosts from Windows NT Domain Controller, NIS, an LDAP directory, or a file.

## Overview of the Grouping Manager

The Grouping Manager allows you to collect network “resources” (devices, ports, users, hosts, and VLANs) into groups that can be manipulated or managed as a single entity.

A **group** is a hierarchical collection of resources that have been grouped together for some common purpose. A group can contain individual resources as well as other (subordinate) groups. Groups (except for Device Groups) are not exclusive—a resource can be a member (child) of more than one group.

**Resources** are individual elements in your network, such as a device, port, host (end station), user, or VLAN. Device, port, and VLAN resources are defined externally to the

Grouping Manager, through the EPICenter discovery capability and the Inventory and VLAN applets. User and Host resources are defined within the Grouping module, either by importing the information from an external source (such as an LDAP directory, NT Domain Controller, NIS server, or a file) or by creating the resources within the grouping module. A group can also be considered a “resource” when it is used as an entity in the same way as an individual resource would be used—such as in a Policy definition within the ExtremeWare EPICenter Policy Manager, an optional, separately-licensed product.

With the exception of Device Groups and Port Groups, the group and resource definitions you create through the Grouping applet are primarily useful within the Policy Manager. For more information on how groups are used within that application, see the *ExtremeWare EPICenter Policy Manager Software User Guide*.

You can define groups and add resources to them to create an organizational structure that facilitates managing your network. The EPICenter software provides several predefined groups:

- Device Groups
- Hosts
- Import Sources
- Port Groups
- Users

You can define your own groups at the same hierarchical level as the predefined groups, or as subordinate groups (children) of an existing group. You can assign resources to your own user-defined groups and to the predefined groups, with the exception of Device Groups and Import Sources.

Three of the predefined groups—Hosts, Port Groups, and Users—initially have no members. Although these groups are provided to help you organize your host, user, and port resources, they can contain children of any resource type. You can create new groups as members of these groups, or add resources of any type directly to them.

- Port Groups may be used by the Real Time Statistics applet and the IP/MAC Address Finder applet. However, these applets do not support hierarchical groups—if you have subordinate groups within a port group, the subordinate layers are all collapsed into a single layer. Resources of types other than ports are ignored by these applets.

Port Groups, along with all the other types of groups and resources, may also be used by the optional Policy Manager module.

- The Hosts and Users groups (either the predefined groups or subordinate groups) may be used by the optional Policy Manager. This is also true of all user-defined groups. No other EPICenter applets currently support groups of these types.

In a group that contains resources of different types, the Policy Manager will ignore those resources that are not relevant to the purpose for which the group has been selected.

The other two predefined groups, the Device Groups group and the Import Sources group, are restricted in the way they can be used.

**Device Groups.** The “Device Groups” group contains the device groups and devices known to the EPICenter inventory database. Device groups are created within the EPICenter Inventory Manager applet, and devices are added or discovered, and are assigned to device groups, within that applet. All port resources are also defined in association with the devices known to the Inventory Manager.

- You cannot add resources to or remove resources from the Device Groups group through the Grouping Manager.
- You can add resources that are children of Device Groups group—device groups, devices, and ports—as members (children) of other groups.

**Import Sources.** The Import Sources group is used to contain resources imported from an external source, such as a file, NT Domain Controller, or LDAP directory. When you perform an import operation, the Grouping Manager creates a new group under the Import Sources group, and puts all the imported resources under that group.

- You cannot add groups or individual resources as children of the Import Sources group except by using the Import function.
- You cannot remove any of the members (including sub-groups) of an imported group. The imported group can only be deleted in its entirety, using the Destroy function.
- You can add resources that are children of an Import Sources group as members (children) of other groups.

## Resource Attributes

Attributes are name and value pairs that you can use for a variety of purposes. You can associate attributes with both groups and individual resources, including resources that are members of the Device Groups and Import Sources groups.

Some predefined resources, such as devices and imported resources, may also have predefined attributes. For example, device resources have their IP address as an attribute. Imported resources may bring with them sets of attributes determined by the content and configuration of the import source. Certain attributes, such as IP/subnet address and DLCID, are used by the optional Policy Manager applet to help it map between high-level named resources such as Users, and the information required to generate a QoS policy (IP address and port information).

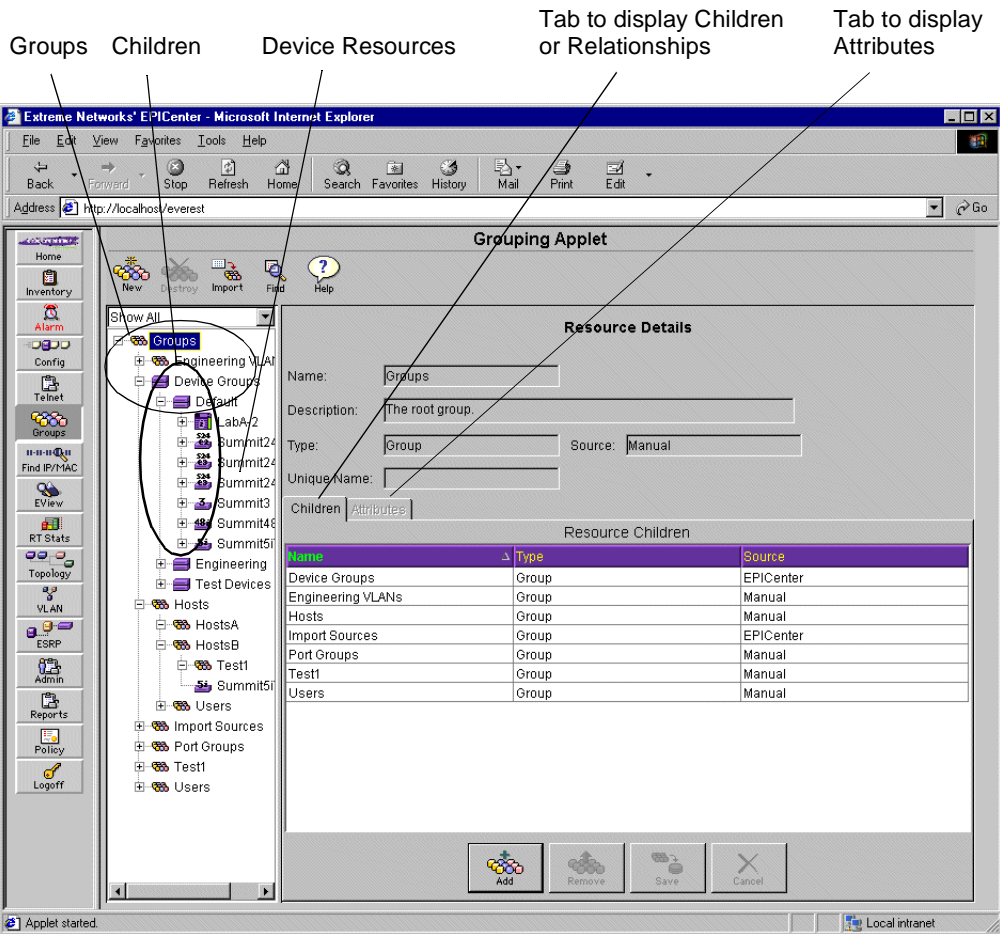
You can also define attributes of your own, and then use them as search criteria when you want to find sets of resources with common attributes.

## Relationships between Resources

The Grouping Manager also supports “relationships” between User, Host, and Port resources. These relationships are used by the optional Policy Manager applet, and help the Policy Manager generate specific QoS rules that it derives from high-level policy specifications that are given in terms of named objects such as users or hosts. See the *ExtremeWare EPICenter Policy Manager Software User Guide* for details.

## Displaying EPICenter Groups and Resources



When you click the **Groups** button in the Navigation toolbar, the main Grouping Manager window is displayed, showing Resource Details for the root-level group. Figure 8-1 shows the Grouping Manager window with a number of the groups expanded to show their children.



**Figure 8-1: Resource Details view**

The Component Tree on the left shows the currently-defined resources. Initially, this shows only the root-level group named “Groups.” Click on the plus sign to the left of a resource to display the children of that resource.

Children can be individual resources (devices, hosts, users, or ports) or groups. The icons indicate the type of resource:

-  indicates a general-purpose group.
-  indicates a device group.



indicates a host resource.



indicates a user resource.



indicates a VLAN resource.

Devices, slots, and ports are indicated by icons that vary based on the specific device model and port type. The icons are the same as are used in the Component Tree of the Inventory module and other EPICenter modules. Although slots appear in the Component Tree, they are not true resources, and cannot be children of groups within the Grouping Manager.

VLANs may appear as children in the Component Tree. However, unlike devices and Device Groups, VLANs will appear in this list only after they have been specifically added as children of a group. VLANs known to EPICenter but not used as children of a group will not appear in this list.

## Resource Details

The **Resource Details** display in the main panel shows the following information for the group (or resource) that is selected in the Component Tree on the left:

- **Name:** the name of the Resource.

For ports, the name of the port is the Device name followed by the port number. For example, S1 3 is the name of port 3 on the device named S1.

- **Description:** a description of the resource (optional for user-defined resources).
  - For Device Groups, this is the description entered for the group in the Inventory Manager.
  - For devices, this is the device description (`sysDescr` variable) if present in the agent.
  - For ports, this is the interface description (`ifDescr` variable) if present in the agent.
  - For VLANs, this contains the protocol and tag information.
- **Type:** the type of resource (Group, Device, Host, Port, User, VLAN).

Note that if you select a slot under a chassis device in the tree, the Resource Details window displays it as a “Slot” resource. However, a slot is not a true resources in that it cannot be added as a child of a group— its ports can be used as resources, but the slot as an entity cannot.

- **Source:** the origin of the resource. The source determines what actions are allowed relative to the resource, This can be one of the following:

- **EPICenter** indicates that the resource was defined by the EPICenter software: either by the Grouping Manager in the case of the predefined groups, or by another EPICenter applet in the case of device group, device, port, or VLAN resources. You cannot modify these resources or their children (if they are groups) through the Grouping Applet.
- **Manual** indicates that this is a user-defined resource, created within the grouping applet using the New button. These resources can be deleted from the Grouping Manager using the Destroy function. The exception is the three predefined groups, Hosts, Users, and Port Groups, which are considered Manual resources but cannot be destroyed. If the user-defined resource is a group, you can add and remove children as desired.
- Imported resources are assigned a source name as part of the Import process. See “Importing Resources” on page 8-28 for more information.

User-defined (Manual) resources can be deleted using the Destroy function. System-defined (EPICenter) and imported resources cannot be deleted, although they *can* be removed as children of other groups to which you have added them. See “Deleting Resources” on page 8-11 for more information on deleting resources, and “Removing A Child Resource from a Group” on page 8-15 for more information on removing resources from groups.

- **Unique Name:** a name that uniquely defines this resource within the Source scope. For user-defined resources (Source is Manual) this will always be blank.
  - For pre-defined resources, the Unique Name is the same as the Resource Name.
  - For device resources, the Unique Name is the device IP address.
  - For port resources, the Unique Name is the IP address of the device followed by the port number. For ports on a chassis device, the port number combines the slot number and the port number.
  - For resources imported from a file or LDAP directory, the Unique Name is specified in the input process, and may be different from the Resource Name.

Below these fields there are two tabbed pages whose contents depends on the type of resource being displayed.

- For Groups, you can view a list of **Children** of the group. This lists the resources (individual resources or subordinate groups) associated with the selected group. For each child, the list includes the resource name, its type, and its source.
- For User, Port and Host resources, you can view a list of **Relationships** for the resource. This displays a list of other resources related to the selected resource.

- For all types, you can view a list of the **Attributes** associated with the resource. The exception is the top level (root) node, “Groups,” which has no attributes.

## Resource Filtering

The field at the top of the Component Tree provides a drop-down menu from which you can select a filter to apply to the Component Tree display. This filter controls the types of resources that are displayed as subcomponents of the groups in the tree. This feature is useful when you have a large number of resources of various types, and lets you limit the display to resources of a specific type in which you are interested.

Groups are always displayed. The following filter choices determine the types of individual resources that will be displayed within the groups:

- **All** allows resource children of all types to be displayed.
- **Devices** shows only the Device resources within the groups.
- **Hosts** shows only Host resources within the groups.
- **Ports** shows only Device and Port resources within the groups.
- **Users** shows only User resources within the groups.
- **VLANs** shows only VLAN resources within the groups.

## Grouping Manager Functions

The buttons in the navigation bar at the top of the page provide the following functions:

- **New** lets you create a new Group, User, or Host resource.
- **Destroy** lets you delete a user-defined resource. This completely eliminates the resource from the EPICenter database, as well as removing it from all groups of which it was a member. This is not the same as removing a resource from an individual group. You cannot destroy system-defined resources or individual imported resources. You can only destroy imported resources by destroying the entire Import Source group.
- **Import** lets you import resources from an external source such as an NT Domain Controller, LDAP database, or a specially-formatted text file.
- **Find** lets you find a resource based on a set of search criteria that can include a resource name, description, type, source, or attribute value.
- **Help** displays on-line help for the Grouping Manager and the Resource Details display.

These functions are described in detail in the following sections.



## Creating a New Resource

You can create new groups and add new User and Host resources through the New Resource function. You can also associate attributes with the resource during this process.

This function creates a new resource. To add an existing resource to an existing group, see “Adding a Resource as a Child of a Group” on page 8-12.



*You cannot add resources of any type to the Device Groups or Import Sources groups, or any subgroups within those groups.*

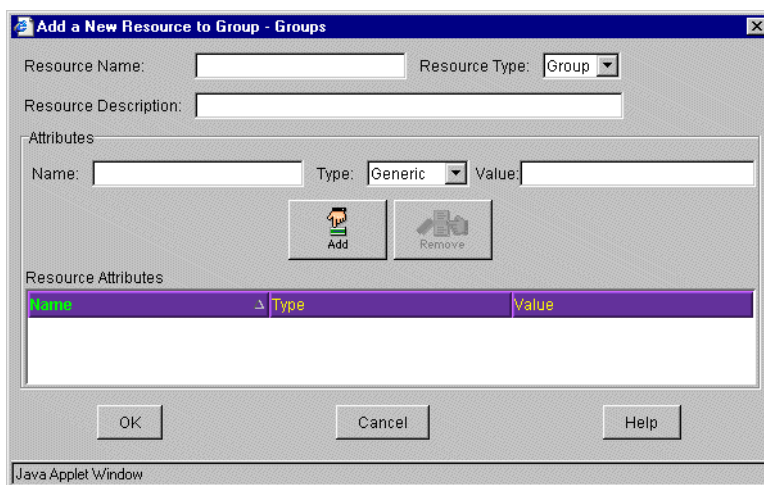
To add a new resource, do the following:

- 1 In the Component Tree, select the Group to which you want the resource added. To add a new group at the highest level, select the root “Groups” node. The new resource will be added as a child of the group you select.

If you plan to add User or Host resources, it is suggested that you add these initially to the User or Host groups, or to another group you have created, rather than to the root-level group. Once you’ve created a resource, you can add it as a child of other groups. For example, a User resource “Fred” can be a member of both the group “Marketing” and the group “Chicago.”

- 2 Click the **New** button at the top of the Grouping Manager window.

The **Add a New Resource to Group** window, as shown in Figure 8-2, is displayed.



**Figure 8-2:** Adding a new resource

**3** Enter identifying information in the fields at the top of the dialog:

- **Resource Name:** a name for the resource. The name can include any characters except a colon.
- **Resource Type:** select a type (Group, User, or Host) from the drop-down menu.

If you are creating this resource as a member of the Hosts group, the type defaults to Host. If you are creating it as a member of the Users group, the type defaults to User. Otherwise, the type is set to Group by default.

- **Resource Description:** an optional description of the resource

**4** Define any attributes that you want to associate with this resource. Attributes are name-value pairs that can be used as search criteria, and are used by the EPICenter Policy Manager. For a more detailed explanation of attributes, see “Adding and Removing Attributes” on page 8-19.

**a** Enter the name of the attribute in the Name field.

**b** Select an attribute type from the drop-down list in the Type field:

**Generic:** any attribute not specified as one of the other two types. The value is a string. You can use this attribute to classify your resources in any way you want, for search purposes.

**IP/Subnet:** this attribute specifies an IP address and subnet mask. For Host or User resources, this attribute may be used by the Policy Manager.

**DLCS ID:** this attribute specifies a DLCS ID (user ID or host ID) that can be detected by DLCS in the switch. DLCS ID attributes are most commonly created when a resource is imported from an external source such as an NT Domain Controller or NIS that contains user and host information.

For Host and User resources, this attribute may be used by the EPICenter Policy Manager. If DLCS is enabled on the switches in your network, attribute and relationship information (mappings between users, hosts, and IP addresses) for host and user resources with DLCS IDs, will be maintained automatically.

**c** Enter a value for the attribute:

For a Generic attribute, enter a string.

For an IP/Subnet attribute, fill in the fields provided, and edit the subnet mask specification as appropriate.

For a DLCS ID, enter a string. In order to be recognized correctly by the DLCS in Extreme switches, this should be the user name (login name) or host name as known within the network.

d To add this attribute to the list of attributes associated with this resource, click the

**Add Attribute to Resource** button



e To remove an attribute from the list of attributes, select the attribute in the list and

click the **Remove Attribute from Resource** button



5 When you have finished entering attributes, click the **OK** button to save your new resource definition.

To close this dialog without saving the resource definition, click the **Cancel** button.

## Deleting Resources

The **Destroy** button in the Grouping Manager toolbar lets you delete user-defined resources from the EPICenter database. The destroy function removes the resource from the database entirely, removing it from all groups where it exists as a child.



*You can only destroy resources whose source is “Manual” (except for the predefined groups) and the root groups of imported resources. You cannot destroy the predefined groups, system-defined resources (devices, device groups, or ports) whose source is EPICenter, or individual imported resources (where the source is a file, LDAP database etc.). If you select a resource you cannot delete, the Destroy button will not be available.*

To delete a user-defined resource do the following:

- 1 Select the resource in the Component Tree.
- 2 Click the **Destroy** button on the toolbar.

A confirmation dialog will be displayed. Click OK to confirm that you want to delete this resource.

If you delete a group, any orphaned children of the group (resources that are not members of any other group) are also deleted.

If you delete a Host or User, all relationships to other resources are also deleted.

To remove a resource as a child of a group, use the Remove function, see “Removing A Child Resource from a Group” on page 8-15. This just removes the parent-child relationship with the group, but does not delete the resource from the database.

## Adding a Resource as a Child of a Group

A group's children are individual resources or subordinate groups that will be manipulated or managed together. A resource is placed into a group as it is created—either the root-level group, or the group that was selected when it was created. However, because a resource can be a member of multiple groups, you may wish to add an existing resource to an additional group, or move it to a different group. To add a resource to a group, you select the resource from a list of the resources that are currently defined in the EPICenter database.

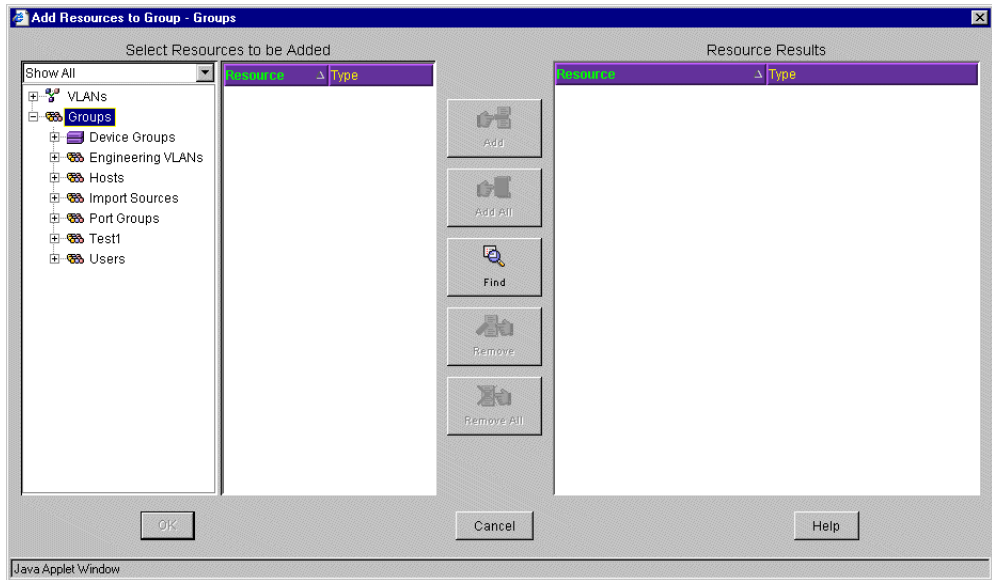
You can add individual resources as children of a group, or you can add groups as children. You cannot add an ancestor group as a child of one of its subordinate groups.

When you add a *group* as a child of another group, all members of the sub-group (its children) are considered members of the higher level (ancestor) group. As membership in the sub-group changes, so does the membership in the higher level (ancestor) group. This can have important effects when a group is used by another EPICenter module. For example, suppose you create group “A” that contains two groups of hosts “HostsA” and “HostsB”, and then use group A in defining access list policies through the Policy Manager. The Policy Manager will generate access list rules for traffic related to all the hosts in groups HostsA and HostsB. If you subsequently change the membership of HostsB, and auto-configuration of policies is enabled in the Policy Manager, the QoS rules that define the access lists will automatically be recomputed and reconfigured. (See the *ExtremeWare EPICenter Policy Manager Software User Guide* for more information on this optional module).

Adding resources to a group as individuals is a more static relationship—resources remain as children until they are explicitly removed from the group (or deleted from the EPICenter database).

To add a resource or group of resources to a higher-level group, do the following:

- 1 In the Component Tree, select the group to which you want to add the resource, so that the group's information is displayed in the Resource Details view.
- 2 Click the tab labeled **Children** to display the list of children belonging to this group.
- 3 Click the **Add** button at the bottom of the list of Children to display the **Add Resources to Group** pop-up dialog, as shown in Figure 8-3.



**Figure 8-3:** Adding Resources to a Group

This window has two parts:

- A display of the resources in the EPICenter database that are available to be added to the group.
- A list of the resources you've selected to add.

- 4 Select a resource from one of the lists in the **Select Resources to be Added** panel at the left hand side of the dialog window. You can make your selection from either side of the panel.

The **Select Resources to be Added** panel is split into two parts:

- The Component Tree in the left half of the panel displays the groups that contain resources of interest. It may include devices if you have filtering set to display port resources.

The drop-down menu field at the top of the Component Tree lets you select a filter to apply to the resource display. This filter controls the types of resources that are displayed as subcomponents of the groups in the tree.

Groups are always displayed. The following filter choices determine the types of individual resources that will be displayed within the groups:

**All** allows resource children of all types to be displayed.

**Devices** shows only Device resources within the groups.

**Hosts** shows only Host resources within the groups.

**Ports** shows only Device and Port resources within the groups.

**Users** shows only User resources within the groups.

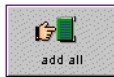
**VLANs** shows only VLAN resources within the groups.

— The resource list in the right half of the panel displays the resources available within the group you have selected in the Component Tree.

- 5 Select one or more resources from the list of individual resources, or select a resource group or device from the left-hand list.



- 6 Click the **Add** button to add your selections to the Resource Results list. You can select a group in the Component Tree or one or more groups or individual resources from the resource list.



Click the **Add All** button to add all the individual resources in the right-hand list to the Resource Results list.



*There is an important difference between adding individual resources as children of a group, and adding a group as a child of another group. Adding a group to the results list does **not** have the same effect as selecting the group in the Component Tree, and then adding its children using the **Add All** button.*

*When you add a group as a child of another group, all members of the subgroup (its children) are considered members of the higher level (ancestor) group. As membership in a subgroup changes, so does the membership in the higher level (ancestor) group. Resources added individually, on the other hand, remain as children until they are explicitly removed from the group (or deleted from the EPICenter database).*

To search for a resource using the Query function, click the **Find** button. You can add the results of your query directly into your Resource Results list by selecting the resources you want to add and clicking the **Add** button at the bottom of the Query window. See “Searching for a Resource” on page 8-23 for more information on the Find function.

- 7 You can remove resources from the Resource Results list if you change your mind about your selections.

Select one or more resources in the Resource Results list, and click the **Remove** button to remove the selected resources, and return them to the Resources to be Added list.

Click the **Remove All** button to clear the Resource Results list.

- 8 Click **OK** to add the resources in the Resource Results list to the list of children for this resource, or **Cancel** to cancel the Add function.
- 9 To save your changes to the EPICenter database, click the **Save** button at the bottom of the Grouping Manager window.

If you attempt to begin a different operation or leave the Grouping Manager applet without saving, the Grouping Manager will prompt you to save your changes. However, you can add and remove children and attributes to the group you've selected in multiple operations before you save.

Click the **Cancel** button at the bottom of the window to cancel the changes you've made to this group.

## Removing A Child Resource from a Group

If you have added a resource as a child of a group, you can remove the resource from that group using the Remove function. This removes the parent-child relationship between the resource and the group. This does not remove the resource from the EPICenter database, unless it is a user-defined resource and this is the only instance of the resource. (Removing all instances of a resource is the equivalent of destroying the resource.)

To remove a resource from a group, do the following:

- 1 Select the parent group in the Component Tree to display the group in the Resource Details window.
- 2 Select the **Children** tab to display the resources that are children of the group.
- 3 Select the resource you want to remove.
- 4 Click the **Remove** button at the bottom of the window.
- 5 To save your changes to the EPICenter database, click the **Save** button at the bottom of the Grouping Manager window.

If you attempt to begin a different operation or leave the Grouping Manager applet without saving, the Grouping Manager will prompt you to save your changes. However, you can add and remove children and attributes to the group you've selected in multiple operations before you save.

Click the **Cancel** button at the bottom of the window to cancel the changes you've made to this group.

Note that you can also remove resources by locating them using the Find function, and removing them using the search results list. See “Searching for a Resource” on page 8-23 for more information on the Find function.

Removing a resource from *all* groups of which it is a member is the equivalent of destroying the resource.

## Adding Relationships to a Resource

Individual resources cannot have children. However, certain types of resources (Hosts, Users, or Ports) can have relationships. Devices cannot have either relationships or children.

For example, a Host may have a relationship with a User, which indicates that the User is associated with the IP address of that Host. A Host may also have a relationship with a port, indicating that the host communicates over that port.

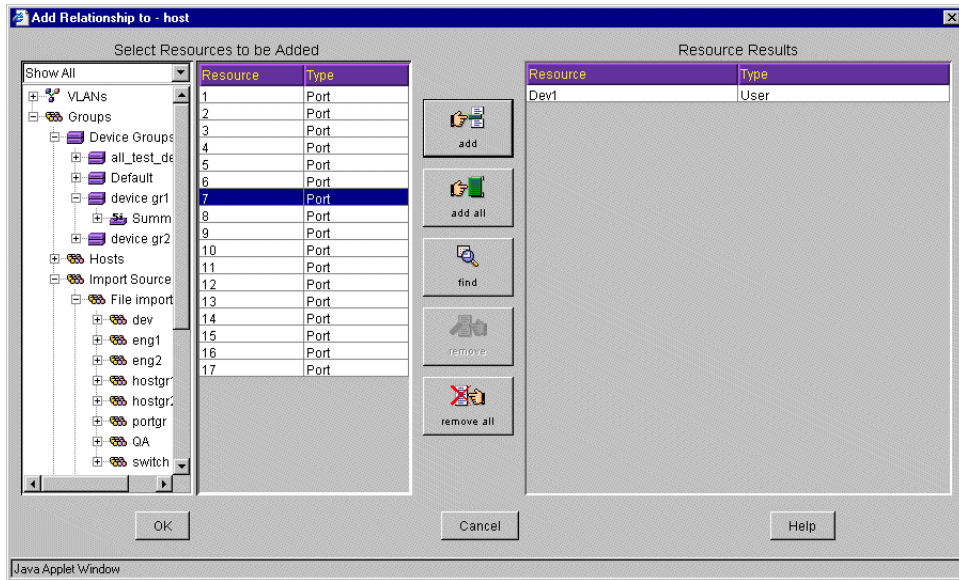
These relationships may be used by the Policy Manager applet to create low-level QoS policy rules based on named higher-level objects such as users and hosts. Relationships can be created between the following:

- Hosts and Users
- Hosts and Ports
- Users and Ports

These relationships are always reciprocal: when you create a relationship between two resources, it is added simultaneously to both resources.

- 1 In the Component Tree, select the resource to which you want to add a relationship, so that it is displayed in the Resource Details view.
- 2 Click the tab labeled **Relationships** to display the list of children belonging to this group.
- 3 Click the **Add** button at the bottom of the list of Children to display the **Add Relationship to Group** pop-up dialog, as shown in Figure 8-4.





**Figure 8-4:** Adding Relationships to a Resource

This window has two parts:

- A display of the resources in the EPICenter database that are eligible to be used in a relationship.
  - A list of the relationships you've selected to add to the resource.
- 4 Select a resource from one of the lists in the **Select Resources to be Added** panel at the left hand side of the dialog window. You can make your selection from either side of the panel.

The **Select Resources to be Added** panel is split into two parts:

- The Component Tree in the left half of the panel displays the groups that contain resources of interest.

The drop-down menu field at the top of the Component Tree lets you select a filter to apply to the resource display. You can filter the resources that will be presented as children of the groups in the tree.

**All** allows resource children of all types to be displayed.

**Devices** shows only Device resources. (However, devices cannot be used in relationships, so nothing is displayed if you select this filter.)


**Hosts** shows only Host resources.

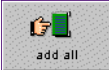
**Ports** shows only Device and Port resources.

**Users** shows only User resources.

**VLANs** shows only VLAN resources. (However, VLAN resources cannot be used in relationships, so nothing is displayed if you select this filter.)

- The resource list in the right half of the panel displays the resources available within the group you have selected in the Component Tree. It will display only the types of resources that are eligible to have relationships (host, users, and ports).

- 5 Select one or more resources in the list, and click the **Add** button  to add your selections to the Resource Results list. You can select a group in the Component Tree or one or more groups or individual resources from the resource list.

Click the **Add All** button  to add all the individual resources in the right-hand list to the Resource Results list.

To search for a resource using the Search function, click the **Find** button. You can add the results of your query directly into your Resource Results list by selecting the resources you want to add and clicking the Add button at the bottom of the Search window. See “Searching for a Resource” on page 8-23 for more information on the Find function.

- 6 You can remove resources from the Resource Results list if you change your mind about your selections.

Select one or more resources in the Resource Results list, and click the **Remove** button to remove the selected resources, and return them to the Resources to be Added list.

Click the **Remove All** button to clear the Resource Results list.

- 7 Click **OK** to add the resources in the Resource Results list to the list of relationships for this resource.
- 8 To save your changes to the EPICenter database, click the **Save** button at the bottom of the Grouping Manager window.

If you attempt to begin a different operation or leave the Grouping Manager applet without saving, the Grouping Manager will prompt you to save your changes. However, you can add and remove relationships and attributes in multiple operations on the resource you've selected before you save.

Click the **Cancel** button at the bottom of the window to cancel the changes you've made to this group.

## Removing Relationships from a Resource

To remove a relationship between two resources (Hosts, Users, or Ports) do the following:

- 1 In the Component Tree, select one of the resources that is involved in the relationship, so that the resource is displayed in the Resource Details window.
- 2 Select the **Relationship** tab to display the relationships for the resource.
- 3 Select the relationship you want to remove.
- 4 Click the **Remove** button at the bottom of the window. The relationship will be removed both from the resource you are viewing, and from the other resource involved in the relationship.

For example, if Host resource “HostB” has a relationship with user resource “Watson” the relationship will appear in the relationship list of both resources. If you display the relationships for resource HostB, and remove the relationship with user Watson, the relationship will be removed from the relationship lists of both HostB and Watson.

- 5 To save your changes to the EPICenter database, click the **Save** button at the bottom of the Grouping Manager window.

If you attempt to begin a different operation or leave the Grouping Manager applet without saving, the Grouping Manager will prompt you to save your changes. However, you can add and remove relationships and attributes in multiple operations on the resource you’ve selected before you save.

Click the **Cancel** button at the bottom of the window to cancel the changes you’ve made to this group.

Removing a relationship does not affect the group memberships of either resource.



*If you destroy a resource, any relationships with that resource will automatically be removed from the other resources involved.*

## Adding and Removing Attributes

Any resource (individual resources or groups) can have attributes. Attributes are simply name-value pairs that can be used for a number of purposes.

There are three types of attributes:

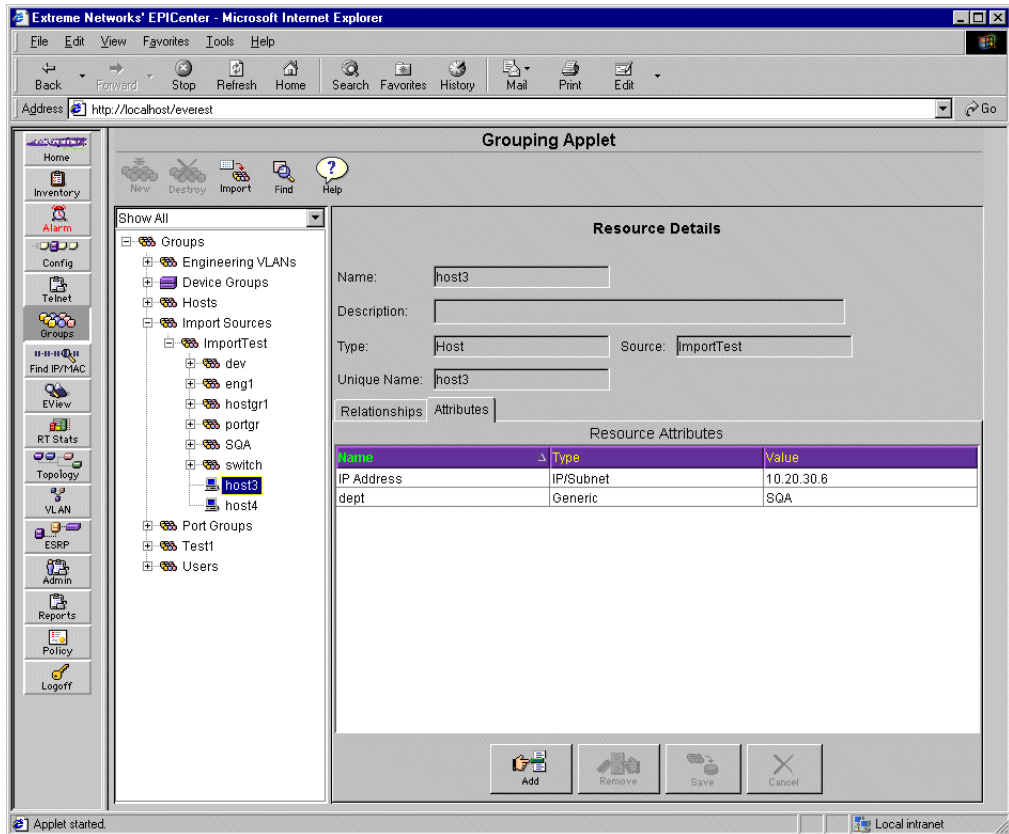
- **Generic:** a user-defined attribute not specified as one of the other two types. The value is a string. You can use this attribute to classify your resources in any way you want, for search purposes.

- **IP/Subnet:** an IP address and subnet mask. This attribute may be used by the Policy Manager to map a User or Host resource to an IP address.
- **DLCS ID:** this attribute specifies a DLCS ID (user ID or host ID) that can be detected by DLCS in the switch. DLCS ID attributes are most commonly created when a resource is imported from an external source such as an NT Domain Controller or NIS that contains user and host information.

For Host and User resources, this attribute may be used by the EPICenter Policy Manager. If DLCS is enabled on the switches in your network, attribute and relationship information (mappings between users, hosts, and IP addresses) for host and user resources with DLCS IDs, will be maintained automatically.

To view the attributes associated with a resource, do the following:

- 1 Select the resource in the Component Tree, so that it is displayed in the Resource Details view.
- 2 Click the **Attributes** tab. This will display the attributes (if any) associated with the resource, as shown in Figure 8-5.

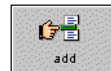


**Figure 8-5:** Resource attribute display

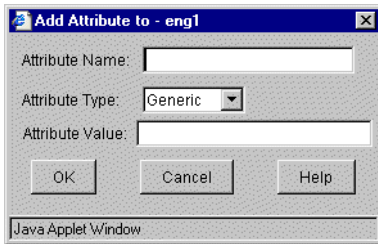
To add an attribute to the displayed resource, do the following:

- 1 Make sure the **Attributes** page is displayed. If it is not, the **Add Attributes** button will not be present.

- 2 Click the **Add Attribute to Resource** button



The Add Attributes pop-up dialog appears, as shown in Figure 8-6.



**Figure 8-6:** Adding attributes to a resource

**3** Enter the name of the attribute in the **Attribute Name** field.

**4** Select an attribute type from the drop-down list in the **Attribute Type** field:

**Generic:** any user-defined attribute other than an IP Address or DLCS ID.

**IP/Subnet:** an IP address and subnet mask.

**DLCS ID:** a User ID or Host ID as it will be detected by DLCS in the switch.

**5** Enter a value for the attribute:

For a Generic attribute, enter a string.

For an IP/Subnet attribute, fill in the fields provided, and edit the subnet mask specification as appropriate.

For a DLCS ID, enter a string. In order to be recognized correctly by DLCS in Extreme switches, this should be the user name (login name) or host name as known within the network.

**6** Click **OK** to enter the attribute into the attribute list.

**7** To save your changes to the EPICenter database, click the **Save** button at the bottom of the Grouping Manager window.

If you attempt to begin a different operation or leave the Grouping Manager applet without saving, the Grouping Manager will prompt you to save your changes.

However, you can add and remove relationships and attributes in multiple operations on the resource you've selected before you save.

Click the **Cancel** button at the bottom of the window to cancel the changes you've made to this group.

To remove an attribute from the list of attributes, do the following:

**1** Select one or more attributes you want to remove.

**2** Click the **Remove Attribute from Resource** button



- 3 To save your changes to the EPICenter database, click the **Save** button at the bottom of the Grouping Manager window.

Click the **Cancel** button at the bottom of the window to cancel the changes you've made to this group.

## Searching for a Resource

If you have a large number of resources defined in your EPICenter database, it may be cumbersome to find a specific resource in the Component Tree. In addition, you may want to be able to quickly identify all the resources that share a certain attribute. The Grouping Manager's Search function lets you find resources using any of the resource information fields as well as attributes as search criteria.

A search can be initiated either from the main toolbar, or by using the **Find** button in the Add Resource or Add Relationship pop-up windows. Setting up and executing the search is the same regardless of where you initiate the search; however, the actions you can take with the results differ depending on where you started from.

The Search Results provide you with the name of the resources that match your criteria, and the paths (group hierarchy) to where the resources reside within your search scope.

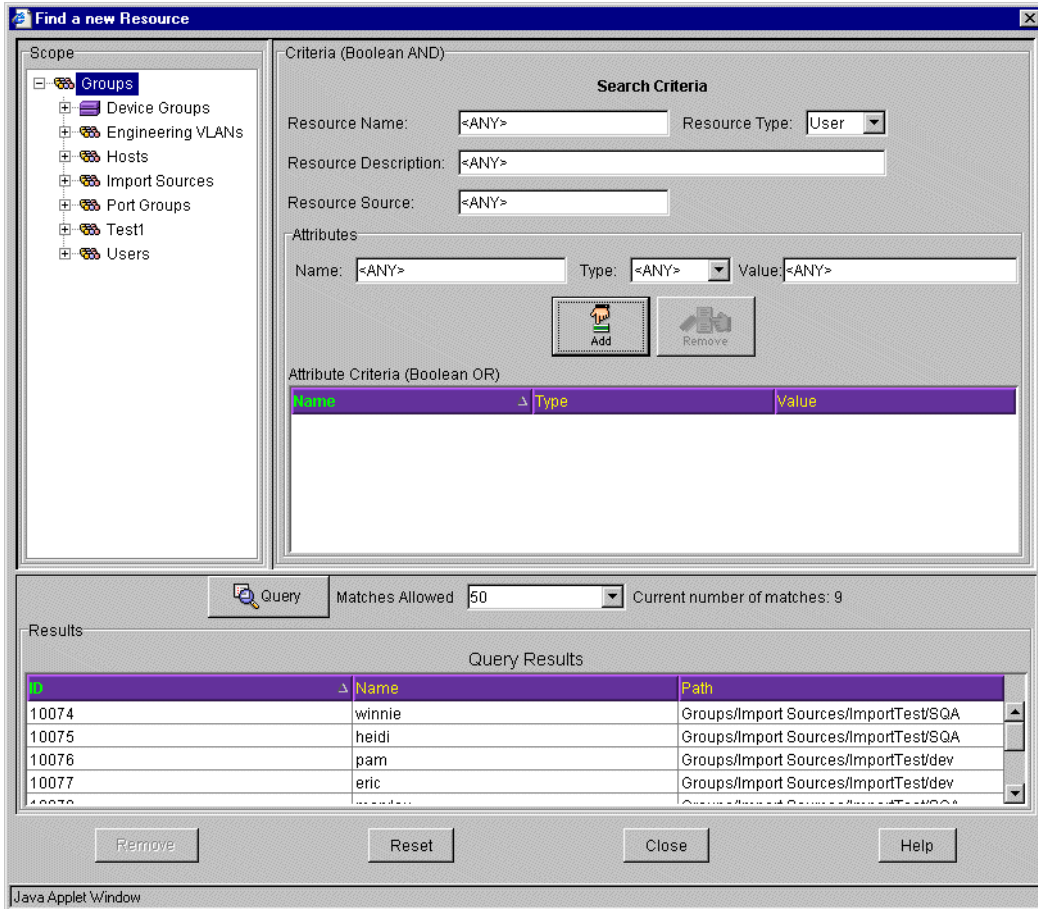
- If you initiate the Search from the main toolbar, you can select one or more resource in the result list, and remove them from their parent groups. See "Searching from the Main Toolbar" on page 8-26 for more information. You can double-click a resource in the results list to see where it is located in the Component Tree.
- If you initiate the search from an Add Relationship or Add Resource window, you can select one or more resources in the result list and add them to the Resource Results list in the Add Resource or Add Relationship window. See "Searching from the Add Resources or Add Relationship Window" on page 8-27 for more information.

## Setting up a Resource Search

To search for resources that match criteria you specify, do the following:

- 1 Click the **Find** button in the toolbar at the top of the main Grouping Manager window, or click the **Find** button in the Add Relationship or Add Resource pop-up windows.

The Search Criteria window is displayed, as shown in Figure 8-7.



**Figure 8-7:** Searching for a resource

The top half of the window is used to specify your search criteria. The Component Tree is used to define a scope for the search.

The bottom half of the window contains the results of the search. You can limit the number of results you want to receive in the case of a search that could yield a large number of matches.

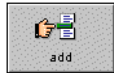
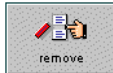
- 2 Enter your search criteria using the fields in the top part of the window. A resource will match the query if it meets *all* the criteria specified in this section:
  - <ANY> specifies a wildcard match, meaning that any and all values for this item will produce a match. There are also two other ways to indicate a wildcard match:



- The asterisk character \* used by itself.
- A blank field.
- For Resource Name, Resource Description, and Resource Source, enter a string to specify the value you want to match. You can specify a partial match using the wildcard characters \* and ?.
  - An \* indicates a wildcard match of unspecified length. Specifying a Resource Name as “A\*n” will find all Resources whose names start with “A” and end with “n.” This would include Ann, Alan, Allen, Allison, and so on. Using the \* by itself is the same as specifying <ANY>.
  - A ? indicates a single character wildcard. Specifying a Resource Name as “A?n” will find all Resources whose name start with “A”, and with “n” and having exactly one character in between. This would include Ann and Ayn, but not Alan, Allen or Allison.
- For Resource Type, select a specific type from the drop-down menu, or use <ANY> to match on all types.



*The values you enter into the search criteria fields are combined using a Boolean AND. This means a resource must match all the criteria you specify in these fields in order to be included in the search results.*

- 3 Enter any attribute specifications you want to use as search criteria. The process is similar to that used to add attributes to a resource. A resource will match the query if it matches any of the attributes specified in this section:
  - a Enter an attribute name or a partial name using the \* and ? wildcard characters.
  - b Select an attribute type from the drop-down list in the Type field, or select <ANY> to match all attribute types.
  - c Enter a value you want to match, or a partial match using the \* and ? wildcard characters.
  - d Click the **Add Attribute** button, , to add the attribute specification to the Attribute Criteria list.
  - e To remove an attribute search criteria you've added to the Attribute Criteria list, select the attribute and click the **Remove Attribute** button .



*Attributes used as search criteria are combined using a Boolean OR. This means that a resource that matches all the criteria specified in search criteria fields (in the top part of the window) and that matches any one (or more) of the attribute criteria, will be included in the search results.*

- 4 Specify a Scope for the search from the Component Tree at the left side of Search Criteria area. The scope will limit the search to the group you select, and its subordinate groups. By default the scope is set to the root-level group “Groups,” which means all groups will be searched.
- 5 To reset all the criteria to their defaults (<ANY>) and to clear the Attribute Criteria list, click the **Reset** button at the bottom of the window.
- 6 At the top of the Results portion of the window, select from the drop-down menu a limit for the number of matches you want to see. All indicates you want to see all matches. You can limit the results to 1, 10, 50, or 100 matches. The actual number of matches found will be displayed next to this field.
- 7 Click the **Query** button to initiate the search. The results will be displayed in the bottom portion of the window. The list will become a scrolling list if the number of results requires it.

For each match, the results will display the following:

- **Resource ID:** a unique internal number provided by the EPICenter software. This may be useful to distinguish between resources if you happen to have created several resources with the same name.
- **Resource Name:** the name of the resource
- **Path:** the path through the Group hierarchy to the location of the resource.

Note that an individual resource (i.e. the same Name and ID) may appear multiple times in this list if it is a child of multiple groups.

Once the list is complete, you can select resources in the Results list and take actions, depending on how you initiated the Find function. The buttons at the bottom of the window are slightly different depending on where you initiated the Find. See the following sections, “Searching from the Main Toolbar,” and “Searching from the Add Resources or Add Relationship Window” on page 8-27, for details on how you can use the results of the search.

## Searching from the Main Toolbar

When you initiate a search from the Main Toolbar, you can use the results to determine where a resource is used—i.e. to find out what groups it belongs to. Since a resource can be a child of multiple groups, this lets you identify all the parents of a particular resource. In particular, before you delete a resource from the EPICenter database, you may want to make sure that you know all the places it is being used to avoid problems when you remove it. Once you find a resource using the Find function from the main toolbar, you can remove instances of the resource directly from the Find window.

Setting up a search is the same regardless of where you initiate the Find function. This is describe in the section “Setting up a Resource Search” on page 8-23.

To remove resources you’ve identified with the Search function, do the following:

- 1 Select and highlight the resource or resources you want to remove.  
You can double-click on the resource and its location is highlighted in the Component Tree.
- 2 Click the **Remove** button to remove those resources from the locations specified in the Results entries you’ve selected.

The results list may present multiple entries for a given resource, if the resource is a child of multiple groups. You can remove a resource from specific groups on an individual basis without removing it from the EPICenter database.

The Remove function is subject to the same restrictions as removing resource children through the Resource Details window. If the resource is a system or imported resource (its source is EPICenter, a file, LDAP database etc.) you cannot remove the resource from it’s “home” group—the group in which it was initially created. If the function is a user-defined resource (source is “Manual”), removing it from all groups will delete it from the EPICenter database.

When you are finished, click the **OK** button to close the window.

## Searching from the Add Resources or Add Relationship Window

When you initiate a search from the Add Resources or Add Relationship window, you can identify resources with a common set of attributes, which can simplify the process of finding the attributes you want to include in a group. Once you find a set of resource using the Find function from the Add Resources or Add Relationship windows, you can add those resources directly from the Find window to the Resource Results list of the “Add...” window.

Setting up a search is the same regardless of where you initiate the Find function. This is describe in the section “Setting up a Resource Search” on page 8-23.



*When you do a search from the Add Resources or Add Relationship windows, the results will include only those resources that are relevant to the Add function you are performing.*

To add resources you've identified with the Search function to the Resource Results list of the Add Resources or Add Relationship windows, do the following:

- 1 Select and highlight the resource or resources you want to add.
- 2 Click the **Add** button to add those resources to the Resource Results list.

The selected resources are added to the list, and the Search window is closed.

To close the Search window without adding any resources, click the **Cancel** button.

## Importing Resources

The Import feature allows you to import user and host resource definitions, and groups containing those resources, from a source external to the EPICenter system. You can import from an NT Domain server, an NIS server, or an LDAP directory. You can also import host and user resource definitions from a tab-delimited text file.

- Importing from a text file requires a tab-delimited file in a very specific format.
- Importing from an LDAP directory requires an import specification file that defines how to map entries in the LDAP directory to resources and their attributes.
- Importing default domain information from an NT Domain server or an NIS server does not require any special preparation.



*If you import information from an LDAP server or NT Domain Controller, that information will become visible to all EPICenter users. If this is a security concern, you may want to consider exporting information from the NT Domain Controller or LDAP directory to a file, and using that to create an import file that contains only the information that you want to be visible through EPICenter Grouping Manager.*

Imported resources are placed under a group created in the Import Sources group (one of the pre-defined EPICenter groups). The name you specify in the Source field of the Import dialog will be used as the group name.

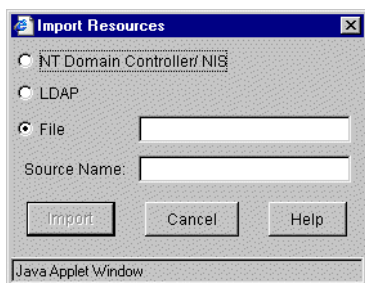
You can perform the same import operation (importing from the same source) multiple times. Once an import is complete, subsequent imports from the same source will act as an update:

- Existing resources will be left intact (including any attributes you may have added).
- New resources will be added.

- Resources that have been removed from the source will be deleted from the EPICenter database.
- Changes in group memberships and changes in relationships will be enacted.

To import resources from an external source, do the following:

- 1 Click the **Import** button in the toolbar at the top of the main Grouping Manager window. The Import Resources window is displayed (see Figure 8-8).



**Figure 8-8:** Importing resources

- 2 Select the type of source from which you want to import information.
  - Select **NT Domain Controller/NIS** to import information from the default Windows NT Domain Controller or NIS server. This will import information about users, hosts (stations), and user groups. See “Importing from an NT Domain Controller or NIS Server” on page 8-36 for more detailed information.
  - Select **LDAP** to import information from an LDAP directory.  
See “Importing from an LDAP Directory” on page 8-30 for information on modifying the file containing the LDAP import mapping specification.
  - Select **File** to import information from a tab-delimited text file.  
See “Importing from a File” on page 8-32 for information on creating the import text file.
  - In the **Source Name** field, enter a name that will identify the source of the imported resources. This name is used for two purposes:
    - It is used to create a group under which all the resources imported in this operation are placed. The group is created under the Import Sources group.
    - It appears in the Source field of the Resource Details view, or in the Source column when the resource is displayed as a child of group, for all resources imported from this source. It can be used as a search criteria in the Find function.

- 3 Click **Import** to begin the import process. The import button will not be enabled until you enter a source name.

Progress during the import will be displayed in a pop-up window, as shown in Figure 8-9.



**Figure 8-9:** Monitoring the progress of an Import function

- 4 When the process has completed, click **OK**.

If you are importing from a large source, the import process can take several minutes. The new group and resources will be available under the Import Sources group in the Component Tree.

If errors occur in the import process, it is possible that no data will be imported. This can result in an empty import group in the Import Sources tree. Once you fix the problems, you can rerun the import.

## Importing from an LDAP Directory

The EPICenter Grouping Manager supports importing groups, users, and hosts from a LDAP directory. The import process uses a TCL script to extract the requested data from the LDAP directory, and create a text file that specifies how the resources should be added to the EPICenter database. This file is in the same format as the import file discussed in “Importing from a File” on page 8-32.

The import process uses an import specification file that defines the following:

- The information you want to extract from the directory.

- How to map that data to groups, resources, and attributes in the EPICenter Grouping module.

The specification file must be named `LDAPConfig.txt`, and must reside in the EPICenter `user/import` directory.

You can use the `LDAPConfig.txt` file provided in the EPICenter `user/import` directory as a template.

You should only need to modify three lines in this file:

`host`: the name of the host where the directory resides.

`user`: the username, if required, to allow access to the directory.

`password`: the password, if required, to allow access to the directory.



*The information below is provided as an aid to importing data from LDAP directories with schemas that differ from the template provided. However, Extreme Networks cannot provide support for modifications to the template file other than the three changes mentioned above.*

If your LDAP directory is organized differently, you can modify the `LDAPConfig.txt` file to meet your individual needs. This requires that you understand the organizational structure of the directory from which you want to import data.

The `LDAPConfig.txt` file must include the following entries:

`base`: specifies the LDAP naming context. Leave this blank to use the default LDAP naming context. This is required.

`attributes`: specifies the attributes that you want to import into the EPICenter database from entries in the LDAP directory. By default, all imported attributes are considered type Generic. You can specify an EPICenter attribute type (Generic, IP/subnet, or DLCS ID) by enclosing both the attribute name and the EPICenter attribute type in curly brackets, as shown: `{uid {DLCS ID}}`. This is required.

`uniqueID`: specifies the attribute that should be used in the EPICenter database as the ID for this resource. This is required.

`scope`: the scope of the search (base, sub, one). This is required.

`groupBy`: the attribute that should be used to create EPICenter sub-groups within the imported group structure. This is optional.

`memberNameAttribute`: the attribute that should be used to define the child entry in a group.

`resourceName`: the attribute that should be used as the displayed name of the resource within the EPICenter Grouping Manager. This is required.

`filterList`: defines the search criteria. Because of the limits on the amount of data that a search will return in one operation, you may need to split your search into multiple operations, as is done in the example file. This is required.

`objectClassMapping`: this maps an LDAP entry to a Grouping Manager resource type based on the object class of the entry. You will need multiple entries of this type. The name-value pair contains the EPICenter resource type on the left, and either the LDAP object class specification or an EPICenter resource type of the right.

For example, the following line specifies that entries whose object class is “organizationalPerson” should be imported as user resources.

```
objectClassMapping: user=organizationalPerson person Top
```

The following line specifies that user resources can be group members.

```
objectClassMapping: groupmember=user
```

At least one mapping specification is required. You can comment out resource types that you don't need to use in the sample file, or leave them. They will be ignored if not defined.

## Importing from a File

To import data from a text file, you define the resources you want to import in a tab-delimited text file. The elements on each line are separated by tabs.

### The Import File Format

The simplest way to create this file is to enter it in a spreadsheet program such as Microsoft Excel, and then export it as tab-delimited text.

The elements on each line are separated by tabs.

### Format Definitions

The first three lines are required. They define the format of the following data.

```
#SYNTAX VERSION:1.0
Resource_UniqueName <tab>Resource_Type <tab> Resource_Name [ <tab>attribute ... ]
<tab> <tab> <tab> (<attribute_type>)[ <tab> (<attribute_type>)...]
```



The **first line** simply defines the version of the import syntax:

```
#SYNTAX VERSION:1.0
```

Enter this exactly as specified.

The **second line** defines the mapping of the data in the file to EPICenter resources:

```
Resource_UniqueName <tab>Resource_Type <tab> Resource_Name [ <tab>attribute... ]
```

- The first three items are required,
  - `Resource_UniqueName` specifies that the first field maps to the unique ID.
  - `Resource_Type` specifies that the second field defines the resource type (user, host, group, device, or port).
  - `ResourceName` specifies that the third field maps to the resource name. This is the name that will appear as the name of the resource in the Grouping Manager.
- The remaining items on the line define the attributes that can be included for each resource. The names you specify here will be used as the attribute names in the Grouping Manager.

The **third line** defines the type of each attribute (Generic, IP/subnet, or DLCS ID).

```
<tab> <tab> <tab> (<attribute_type>) [ <tab> (<attribute_type>)... ]
```

Each type specifier must be enclosed by parenthesis, and separated from the preceding type specifier by a tab. Three tabs must precede the first type specifier.

- The items in this line define the type of each attribute defined in line two. You must include a type specification for every attribute included in line two.
- The first three items in line two do not require a type (as they are predefined). You skip these by including the three tabs before the first type specifier.

## Resource Definitions

The remaining lines in the first section define the resources to be imported. Each resource must include the uniqueID, the resource type, and a name. Attribute values are optional, and will be assigned in the order presented on the line (separated by tabs). These lines are formatted as follows:

```
uniqueID1 <tab> <resource_type> <tab> resource_name1 <tab> { attribute <tab> ... }
uniqueID2 <tab> <resource_type> <tab> resource_name2 <tab> { attribute <tab> ... }
...
uniqueIDn <tab> <resource_type> <tab> resource_nameN <tab> { attribute <tab> ... }
```

- `uniqueID` will be used as the resource's unique name. It can be the same or different from the resource name. For a device, the `uniqueID` must be the device IP address. For a port it is the IP address of the device followed by the port number.
- `resource_type` can be `user`, `host`, `group`, `device`, or `port`.
- `resource_name` is the name that will be displayed as the name of the resource.
- `attribute` defines the value of the attribute that corresponds to this position in the list.

The combination of `uniqueID` and `resource_type` must be unique within this section. Duplicate definitions generate a warning.

For example, assume the following format definition at the beginning of the import file:

```
Resource_UniqueName Resource_Type Resource_Name Location Department RoomNo
```

To create a user resource named Judy Jones, with three attributes:

- Location, whose value is Denver
- Department, whose value is Sales
- RoomNo whose value is 3050

Enter a resource definition as follows:

```
judy user Judy Jones Denver Sales 3050
```

You cannot use the Import function to create new device or port resources. You *can* import attributes for device and port resources, and define relationships for them. The device and port resources must already exist in the EPICenter database, and the names you specify must match their names in the database.

See “Resource Details” on page 8-6 for more information on the components of a resource.

## Group and Relationship Definitions

The second part of the file defines the relationships between the resources—both group membership and relationships between the resources themselves (see “Adding Relationships to a Resource” on page 8-16 for more information about relationships).

The `#GROUPS#` specification is required, even if you do not define any groups.

```
#GROUPS#
```

Each line in this section has the following form:

```
<resource_type>:<resource_uniqueID> <tab> <resource_type>:<resource_uniqueID>
<resource_type>:<resource_uniqueID> <tab> <resource_type>:<resource_uniqueID>
```

- `resource_type` can be `user`, `host`, `group`, `device`, or `port`. A group that exists in the EPICenter database (and is not defined in the import file) can be specified as a child of an imported group, but the reverse is not supported.
- `resource_uniqueID` is the unique ID defined in the first part of the file (or known to exist already in the EPICenter database).

For creating group membership relationships, the first type:ID pair defines the parent, the second one defines the child. Thus, the first pair must always be a group. The second pair can be a group or an individual resource.

For defining peer-to-peer relationships, (user-host, user-port, and host-port relationships) either member of the relationship can be specified first.

## Example

The following is an example of an import file.

```
#SYNTAX VERSION:1.0
Resource_UniqueName Resource_Type Resource_Name IP Address DLCS OStype Dept
                    (IP/Subnet)(DLCS ID)(Generic)(Generic)
wendy                user          Wendy Lee                               NMS
heidi                user          Heidi Smith                              NMS
pam                  user          Pam Johnson                               SQA
eric                 user          Eric Wilson                              SQA
mary                 user          Mary Baker                               NMS

win2k                host          win2k      10.20.30.2    wlee windows NMS
host1                host          host1      10.20.30.4    HPUX   NMS
host2                host          host2      10.20.30.5    Solaris NMS
host3                host          host3      10.20.30.6    windows SQA
host4                host          host4      10.20.30.7    Solaris SQA

ugr1                 group         SQA
ugr2                 group         dev
hgr1                 group         hostgr1
dgr1                 group         eng1
switch              group         switch
portgr              group         portgr

#GROUPS#
group:ugr1          user:wendy
```

```
group:ugr1      user:heidi
group:ugr1      user:mary

group:ugr2      user:pam
group:ugr2      user:eric

group:hgr1      host:win2k
group:hgr1      host:host1
group:hgr1      host:host2

group:dgr1      host:host3
group:dgr1      host:host4

## Host to User Relation
user:wendy      host:win2k
user:heidi      host:host1
user:mary       host:host2
host:host3      user:pam
host:host4      user:eric
```

## Importing from an NT Domain Controller or NIS Server

Importing from an NT Domain Controller or NIS server is straightforward. The import is always done from the Domain Controller or NIS server that is serving the domain for the system running the EPICenter server. The type of system you are running will determine where the EPICenter server looks for the information.

In order to import information from an NT Domain Controller, the EPICenter server must be running with the appropriate user permissions in order to extract the information from the Domain Controller.



*If you import information from an NT Domain Controller, that information will become visible to all EPICenter user. If this is a security concern, you may want to consider exporting information from the NT Domain Controller to a file, and using that to create an import file that contains only the information that you want to be visible through EPICenter Grouping Manager.*

The import process imports the following information:

- For users: username, fullname, description.
- For hosts: hostname, description, Primary IP address.
- For groups (users only): name, description, usernames of members.

The import process creates a file, `import.txt`, in the `user/import` subdirectory.

# 9

## Using the IP/MAC Address Finder

---

This chapter describes how to use the IP/MAC Address Finder applet for:

- Creating search requests for locating specific MAC or IP addresses on the network, and determining the devices and ports where they are located.
- Creating search requests to identify MAC and IP addresses on specific devices and ports.

### Overview of the IP/MAC Finder Applet

Using the IP/MAC Address Finder applet you can specify a set of Media Access Control (MAC) or Internet Protocol (IP) network addresses, and a set of network devices to query for those addresses. The applet returns a list of the devices and ports associated with those addresses. You can also specify a set of devices and ports, and search for all MAC and IP addresses known those devices and ports.

The Search Tool lets you configure and start a search task, view the status of the task, and view the task results. The task specification and results are kept in the task list until you delete them, or until you log out of the EPICenter client.

When you click the **Find IP/MAC** button in the Navigation Toolbar, the main IP/MAC Address Finder page is displayed as shown in Figure 9-1. Initially there are no search requests displayed.

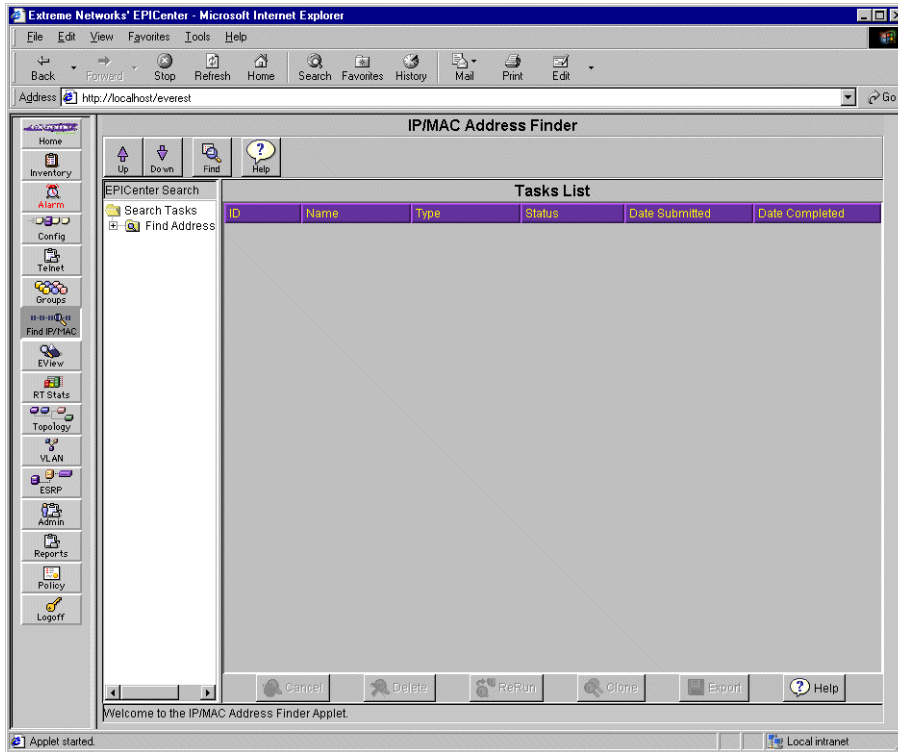
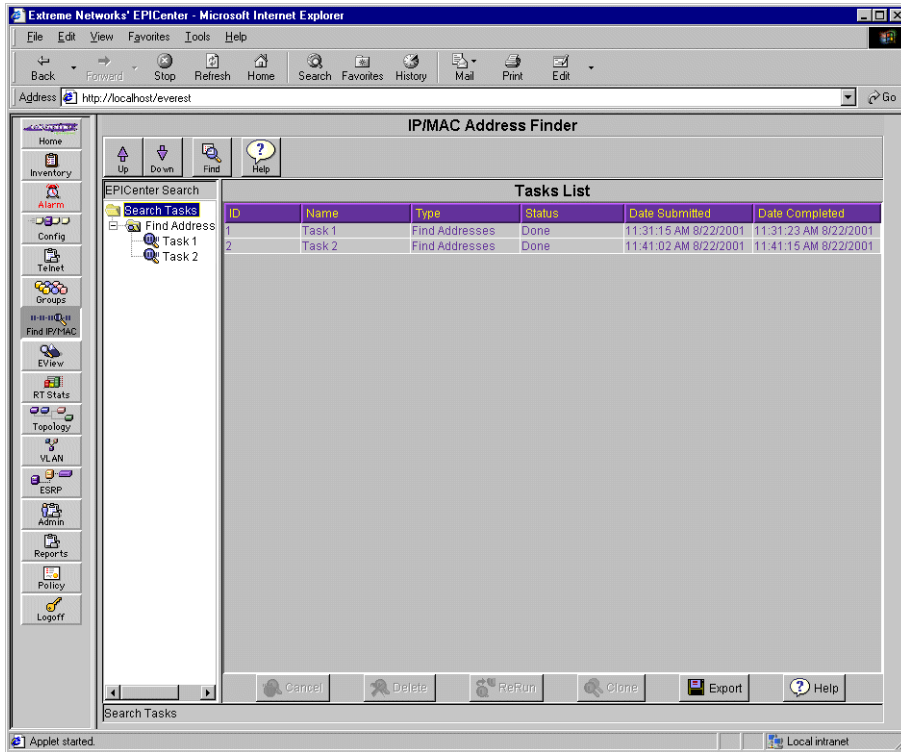


Figure 9-1: IP/MAC Address Finder main page

## Tasks List Summary Window

As search tasks are initiated, they are placed in the Find Address Tasks List in the Component Tree. Selecting the Find Address Tasks folder in the Component Tree displays a summary of the status of the tasks in the Task List (see Figure 9-2).



**Figure 9-2:** Tasks List summary

The Tasks List shows you basic information about the tasks you set up

- **ID** is automatically assigned by the EPICenter server
- **Name** is the name you gave the task when you created it. Giving a task a unique name is important to distinguish it from other tasks in the Tasks List
- **Type** is the type of search this will perform. In EPICenter release 3.0, this is always **Find Addresses**
- **Status** shows the status of the request
- **Date Submitted** shows the date and time the task was submitted
- **Date Completed** shows the date and time the task was finished



From the **Tasks List** you can perform the following functions:

- Select a Pending task and click **Cancel** to cancel the task before it has completed
- Select a task and click **Delete** to delete an individual task. This deletes the task specification as well as the task results. Once a task has completed, it cannot be rerun unless it is the most recent task completed
- Select a task and click **Clone** to bring up the **Find Addresses** window with the specifications of the selected task already displayed
- Select a task and click **ReRun** to execute the task again
- Select a task and click **Export** to export the search results to a text file. See “Exporting Task Search Results to a File” on page 9-9 for more information.



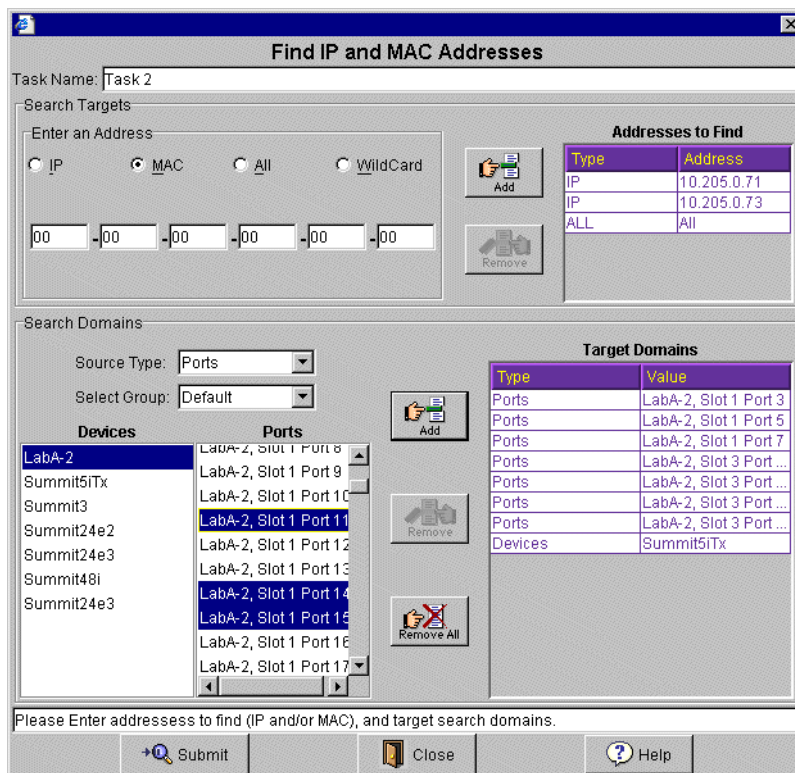
*The specified tasks and their search results persist as long as you are running the ExtremeWare EPICenter client, even if you leave the IP/MAC Address Finder applet and go to another EPICenter applet. However, when you exit the EPICenter client, all the task specifications and search results are deleted.*

## Creating a Search Task

To create a search task, click the **Find** button  in the tool bar at the top of the IP/MAC Address Finder page. This displays the Find Addresses window (Figure 9-3).



*If you have already submitted a task, the most recent task with its specifications is displayed in the Find Addresses window.*



**Figure 9-3:** Find Addresses window

To create a search task:

- 1 Enter the task name in the **Task Name** field. This name helps you identify the task in the Find Address Tasks List. Names of the form Task1, Task2 and so on are provided by default.
- 2 Define the search targets: in the **Enter an Address** group box, select either **IP** or **MAC** to determine the format of the address to search for, and enter the address into the fields provided. Click the **Add Address** button to add the address to the **Addresses to Find** list.
  - To find all addresses in the given search domain, click **All** in the **Enter an Address** group box, then click the **Add Address** button to add All to the **Addresses to Find** list

Note that **All** is added to the search list in addition to any individually-specified addresses. The **All** specification does overlap with the other target addresses. However, this allows the user to remove the **All** specification without losing the other addresses in the search list.

- Click the **Wildcard** button to search for a MAC address defined only by the first three hexadecimal tuples.
  - Click the **Remove Address** button to remove an address from the list
- 3** Define the search domain. The **Target Domains** list specifies the scope of the devices to be included in the search. Devices not included in this domain will not be searched.

You can define the search space in several ways:

- **Devices** lets you select individual devices to include in the search
- **Domains** lets you search all the devices in a specified device group
- **Ports** lets you select individual ports to include in the search
- **PortGroups** lets you search all the devices in a specified port group

You can create a target domain that includes a combination of these specifications.



*The IP/MAC Finder applet does not support hierarchical port groups. If you have created port groups in the Grouping Manager that include subgroups as members, the subgroups will not appear in the Target Domains list. Instead, any ports that are members of subgroups will be displayed directly under the top-level port group, as if they are members of the top-level group.*

- 4** If you select Devices or Ports as the Source Type, you must also select a Device Group from the **Select Group** field to define the list of devices that will appear in the Devices list. If you select Domains or PortGroups, this field will be inactive.
- 5** Select the Device, Port, Device Group, or Port Group that you want to search and click **Add Domain** to move it into the Target Domains list.
- To remove a member of the Target Domains list, select the item in the list and click **Remove Domain**. To clear the Target Domains list, click **Clear All**.
- 6** When you have completed your search specification, click the **Submit** button at the bottom of the window to initiate the search.

The IP/MAC Finder applet searches the IP Address Translation Table (the `ipNetToMediaTable`) in each device agent for IP addresses, and the Forwarding Database (FDB) for MAC addresses.



The IP/MAC Finder applet will not identify a device's own IP address when you search for IP addresses on that device. In other words, the applet will not find IP address 10.2.3.4 on the switch whose address is 10.2.3.4. It can only find addresses that are in the agent's IP Address Translation table, and a device's own address is not included in the table. The applet will find the address on the other switches that have connectivity to the switch with the target IP address, however.

## Detailed Task View

When you initiate a search, the task is placed in the Find Address Tasks list in the Component Tree. The main panel displays the Detailed Task View for the current search task (see Figure 9-4).

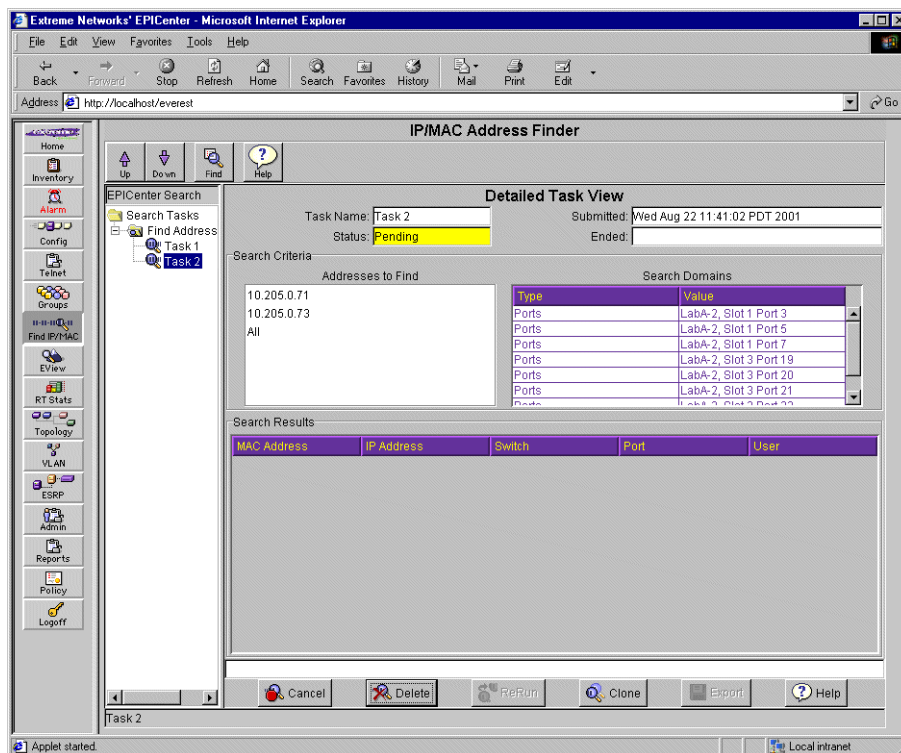
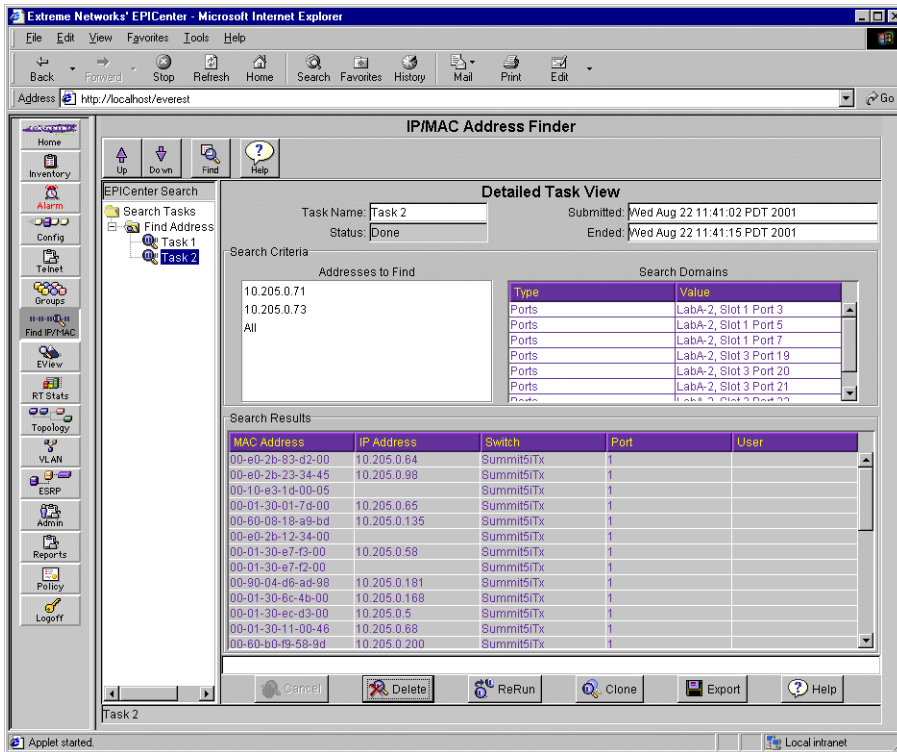


Figure 9-4: Search in progress

While the task is in progress, the window shows the status as **Pending**. When the search is complete, the **Detailed Task View** shows the results for the search (Figure 9-5).



**Figure 9-5:** Address search results in the Detailed Task view

The Detailed Task View shows the following information about your search.

- **Name** is the name you gave the task when you created it. Giving a task a unique name is important to distinguish it from other tasks in the Tasks List
- **Status** shows the status of the request
- **Date Submitted** shows the date and time the task was submitted
- **Date Completed** shows the date and time the task was finished

The Search Criteria areas shows:

- The list of IP or MAC addresses that were the object of the search

- The Search Domains where the search took place. The Search Domains lists shows the name and type (Device or Group) of the components of the domain specification

The Search Results list shows the results of the search. For every address successfully located, this list shows:

- Both the MAC address and the corresponding IP address.
- The switch and port to which the address is connected.
- The User (name) currently logged in at that address.

Once the search is complete, the search results will stay in the Tasks List until you explicitly delete them using the Delete Function from the Tasks List Summary View, or until you exit the EPICenter client.

From the Task Detail window you can do the following:

- Click **Delete** to delete this task. This deletes the task specification as well as the task results.
- Click **Clone** to bring up the **Find Addresses** window with the specifications of the selected task already displayed.
- Click **ReRun** to execute the task again.
- Click **Export** to export the search results to a text file.

## Exporting Task Search Results to a File

You can export a task's search results to a text file. You can do this from the Detailed Task View, or from the Task List.

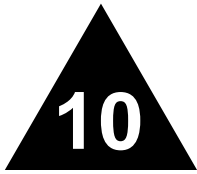
To export the search results to a file, do the following:

- 1 From the Detailed Task View, or from the Task List with the task selected, click the **Export** button.

This displays the Export pop-up dialog.

- 2 Enter a file name and subdirectory name in the fields provided, or accept the defaults provided by the EPICenter software.
  - Search Result files are save in the EPICenter `user/AddressFinderResults` directory, which is a subdirectory of the EPICenter installation directory. You can optionally specify a subdirectory within the AddressFinderResults directory by entering the subdirectory name into the **Directory** field.

- By default the exported file will be given a name created from the current date, time, and task name. For example, the results for task “Task 2” run on April 25, 2001 at 3:52 pm will be saved in a file named 2001\_4\_25\_1552\_Task 2.txt. You can change the file name by replacing the name in the File Name field.
- 3 Click the **Apply** button to save the results.  
Click **Reset** to clear all the fields.  
Click **Close** to close the dialog without saving the file.



# Using ExtremeView

---

This chapter describes how to use ExtremeView for:

- Viewing Extreme and third-party device status.
- Viewing and setting Extreme device configuration information using the ExtremeWare Vista graphical user interface.
- Viewing Extreme device statistics using the ExtremeWare Vista graphical user interface.

## Overview of the ExtremeView Application

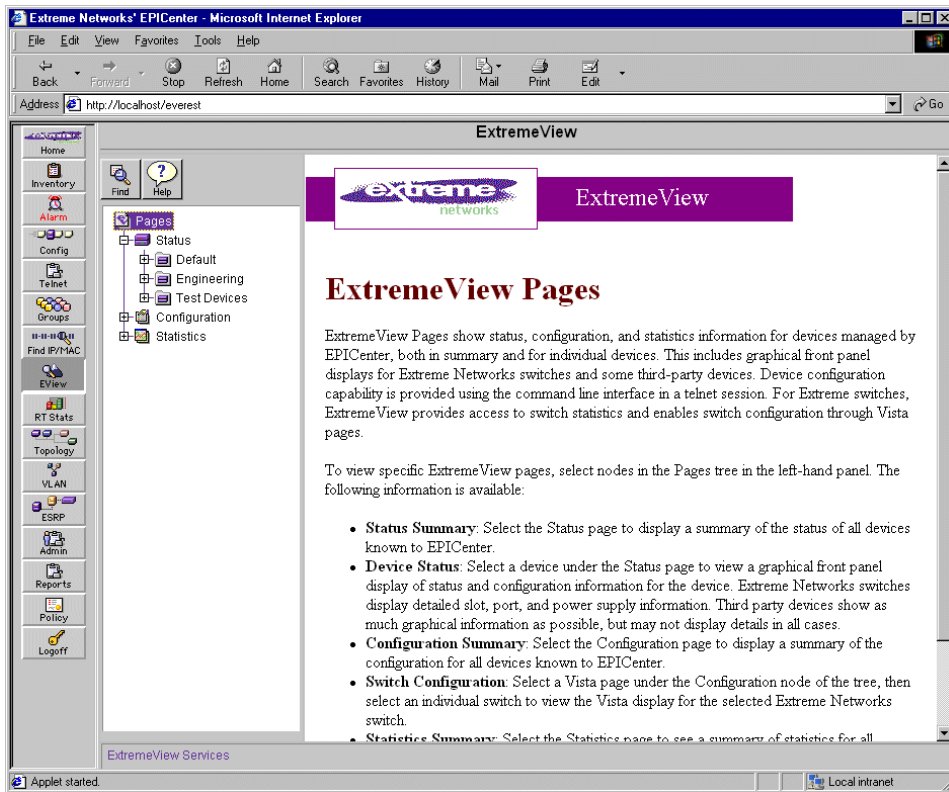
The ExtremeView applet displays information about the status of Extreme switches (Summit, Alpine, and Black Diamond switches) and third-party devices managed by EPICenter. Any EPICenter user can view status information about these network devices. Users with Administrator or Manager access can view and modify configuration information for those switches through the ExtremeWare Vista graphical user interface.

ExtremeWare Vista is device management software running in a Summit, Alpine, or Black Diamond switch. It allows you to access the switch over a TCP/IP network using a standard Web browser, and provides a set of pages for configuring and monitoring the Summit or Black Diamond switch.



*You must have a user account on the Extreme switch in order to run ExtremeWare Vista on the switch. A user account on a switch is separate from your EPICenter user account.*





**Figure 10-1:** The ExtremeView applet, main page

Use the nodes in the Component Tree as follows:

- **Status** displays status information for the devices known to EPICenter. You can view summary status for all network devices or for the devices within a device group. You can view status and configuration information for individual devices, slots, and ports through a front panel view accompanied by a table of configuration and status information. Select a device subnode under the Status node to view configuration information for the device.
- **Configuration** displays configuration information for Extreme Networks switches based on the configuration categories in ExtremeWare Vista. You can view summary configuration information for all devices in all device groups known to EPICenter, as well as detailed configuration information for individual Extreme Networks switches,

organized by ExtremeWare Vista configuration categories. Individual third-party devices cannot be accessed through this feature.

- **Statistics** displays monitoring results for Extreme Networks switches, also based on ExtremeWare Vista statistics monitoring categories. You can view summary statistics that include active and inactive port counters for all Extreme Networks devices known to EPICenter, or statistics for individual Extreme Networks switches. Individual third-party devices cannot be accessed through this feature.

## Viewing Device Status Information

Select **Status** in the Component Tree to display a summary status of all the devices known to EPICenter (see Figure 10-2).

The screenshot shows the ExtremeView applet in a Microsoft Internet Explorer browser window. The address bar shows `http://localhost/everest`. The main content area is titled "ExtremeView" and "Device Status". A table lists the following data:

Status	Name	Type	IP Address	Software	Last Reboot
Green	CoreBuilder-479	Generic 3Com	10.205.0.182	UNKNOWN	Jul 5, 2001 8:55 AM
Green	5422	Generic Compaq	10.205.0.145	UNKNOWN	Jul 17, 2001 3:24 PM
Green	5411	Compaq 5411	10.205.0.37	UNKNOWN	Aug 8, 2001 11:28 AM
Green	Switch 1100	3Com Supper Stack	10.205.0.181	UNKNOWN	Jun 27, 2001 2:25 PM
Green	Summit24e2	Extreme Summit 24e	10.205.0.149	UNKNOWN	Aug 21, 2001 10:25 AM
Green	lame1	Generic Cisco	10.205.0.51	12.0	Aug 16, 2001 10:44 AM
Green	ciscotest	Cisco 4500	10.205.0.50	12.0	Aug 8, 2001 11:27 AM
Green	Summit3	Extreme Summit 3	10.205.0.156	4.1.19 (2)	Aug 8, 2001 11:27 AM
Green	Summit24e3	Extreme Summit 24e	10.205.0.68	6.2.0 (5)	Aug 21, 2001 9:37 AM
Yellow	Summit5iTx	Extreme Summit 5i T	10.205.0.170	6.2.0 (48)	Aug 21, 2001 11:32 AM
Yellow	LabA-2	Extreme Alpine 380e	10.205.0.39	6.1.9 (5)	Jul 31, 2001 1:39 PM
Yellow	Summit48i	Extreme Summit 48i	10.205.0.41	6.2.0 (51)	Aug 21, 2001 5:35 PM
Red	Summit24e3	Extreme Summit 24e	10.205.0.30	6.2.0 (34)	Aug 13, 2001 12:11 PM
Red	lame2	Generic Cisco	10.205.0.52	11.3	Aug 6, 2001 6:54 PM

Figure 10-2: The ExtremeView applet, Status summary

Select a Device Group name to show summary status for the devices in the group.

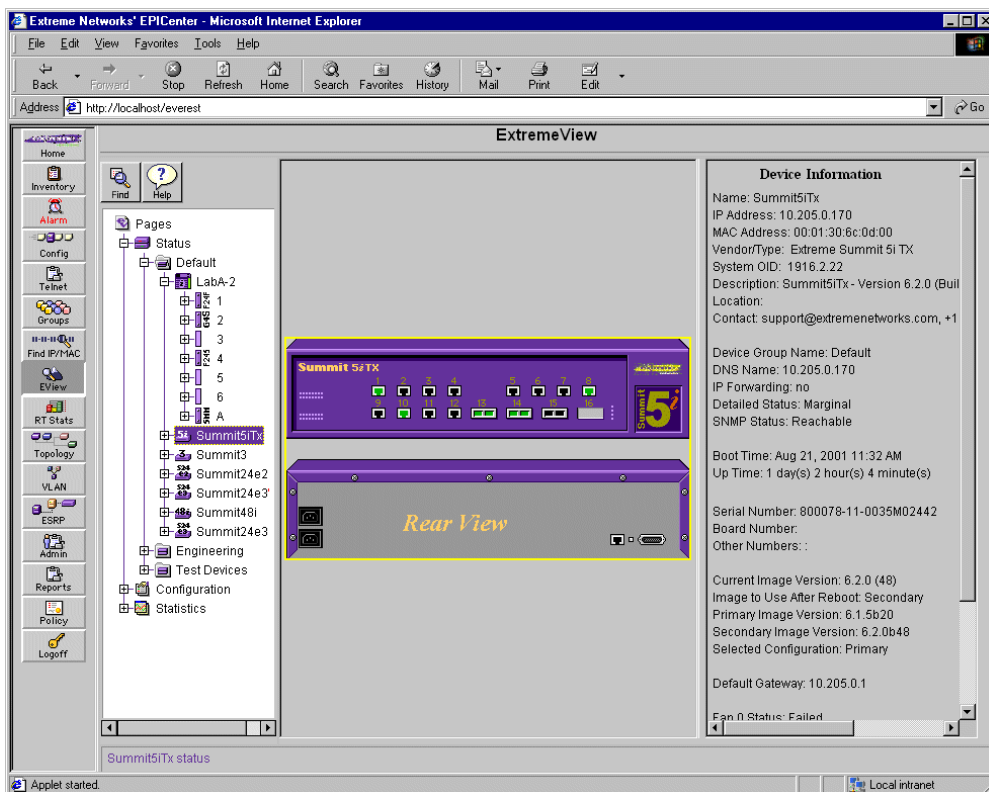
- The status “lights” show the status of the device as detected by EPICenter.

**Table 10-1:** ExtremeView Device Status Indicators

Status Light	Device Status
Green	Device is up and OK
Yellow	Device is responding, but reports an error condition such as a fan or power supply failure, or excessive temperature
Red	Device is not responding to EPICenter status queries. This may mean that the switch is down, that it is unreachable on the network, or that the SNMP community strings have changed and EPICenter can no longer contact the switch.

- The name, type of switch, IP address, the ExtremeWare software version, and the last reboot time are retrieved from the device by EPICenter.

Select a device in the Component Tree on the left to display detailed configuration and status information, as shown in Figure 10-3. This display shows additional information that EPICenter has gathered from the switch agent.

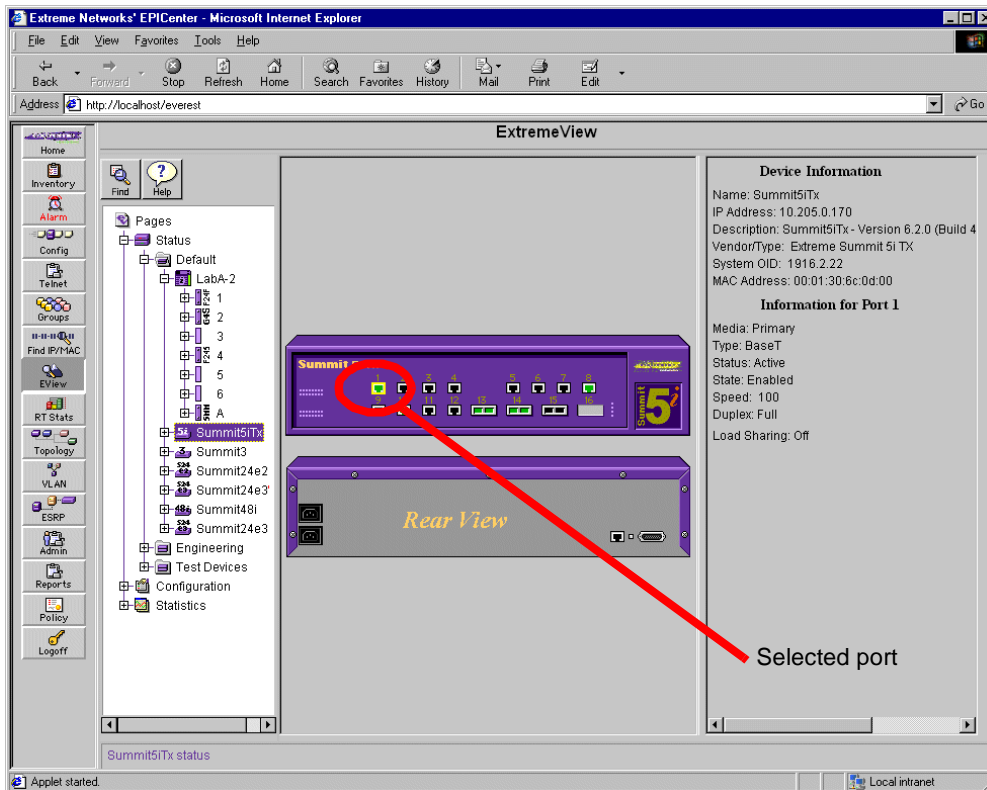


**Figure 10-3:** The ExtremeView applet, switch status

This view shows an active graphical display of the switch front panel, as well as a panel of status information.

You can view the status of individual modules (slots), ports, and power supplies (where shown), as shown in Figure 10-4, in two ways:

- Select the slot, port, or power supply by clicking the cursor on the item in the switch image.
- Display the list of slots or ports in the Component Tree, and select the element about which you want status information.



**Figure 10-4:** The ExtremeView applet, port status

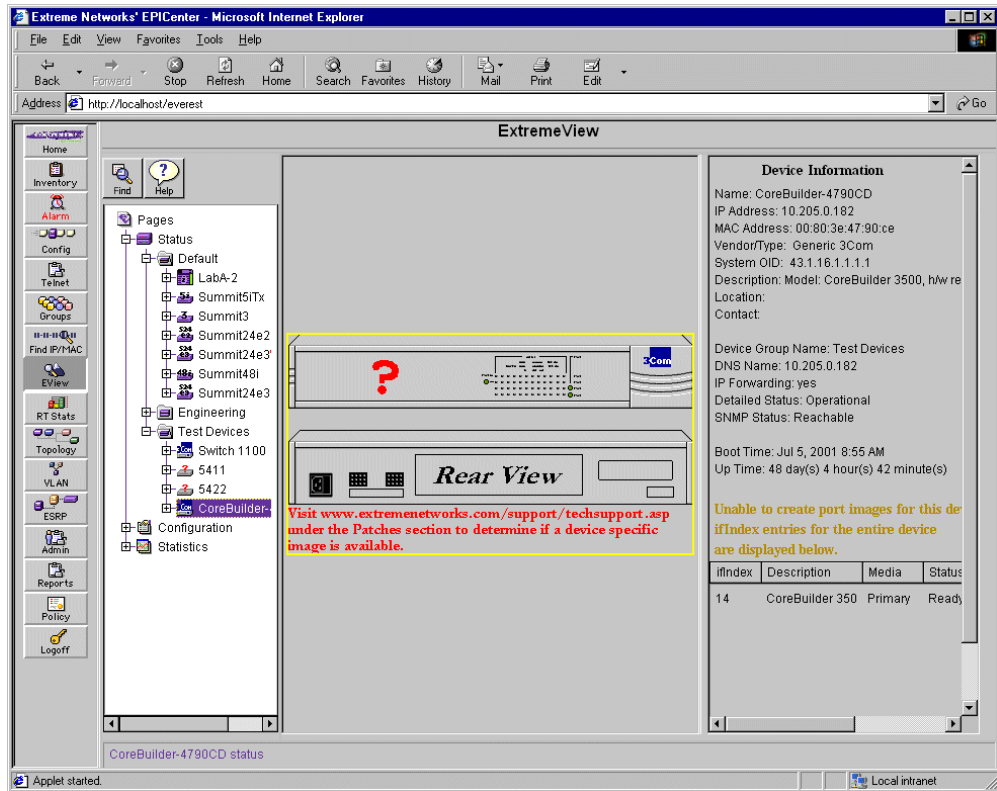
The right-hand panel displays status information about the selected port

There are a few Extreme devices, such as the Summit24e2T, Summit24e2X, and Summit Px1 switches, on which the ports are not selectable through ExtremeView. In these cases, the ifIndex entries for the device are displayed in the Device Information panel on the right.

### Third-party Device Status

If the device you select is a third-party device, and EPICenter does not have an image for the specific model, it displays a generic device image (a vendor-specific image if possible, but without model-specific details). If there is no configuration file for the device, and it is being managed by the EPICenter, the ifIndex entries for the entire device are displayed in

the Device Information panel on the right. Figure 10-5 shows a third-party device with an unknown configuration.



**Figure 10-5:** A third-party device with unknown configuration

The port type is ethernet-csmacd(6) by default. However, some devices may support other port types. For example, some 3Com devices support a layer 3 module which is of type other(1).

As Extreme Networks continues to develop additional device images, they will be made available on Extreme Networks' support web site at [www.extremenetworks.com/support/documentation.asp](http://www.extremenetworks.com/support/documentation.asp) under the Patches section. You can also contact your Extreme Networks sales representative or reseller if you would like help from Extreme's Professional Services organization for creating images or configuration files for specific devices.

## Viewing Switch Configuration Information

Select **Configuration** in the Component Tree to display a configuration summary for the Extreme switches known to the EPICenter software (see Figure 10-6).

Name	Type	IP Address	Mode	Config	Primary	Secondary
5411	Compaq 5411	10.205.0.37	Bridging	Secondary		
5422	Generic Compaq	10.205.0.145	Bridging	Secondary		
CoreBuilder	Generic 3Com	10.205.0.182	Routing	Secondary		
LabA-2	Extreme Alpine 3800	10.205.0.38	Routing	Primary	6.1.9b5	6.2.0b44
Summit24e2	Extreme Summit 24i	10.205.0.149	Routing	Secondary		Not Supported
Summit24e3	Extreme Summit 24i	10.205.0.30	Routing	Secondary	6.2.0b34	0.0e.0b2
Summit24e3	Extreme Summit 24i	10.205.0.68	Routing	Primary	6.2.0b5	6.2.0b329
Summit3	Extreme Summit 3	10.205.0.156	Routing	Primary	4.1.19b2	4.1.19b3
Summit48i	Extreme Summit 48i	10.205.0.41	Bridging	Primary	6.2.0b51	6.1.5b20
Summit5ITx	Extreme Summit 5i 7	10.205.0.170	Bridging	Primary	6.1.5b20	6.2.0b48
Switch 1100	3Com Supper Stack	10.205.0.181	Routing	Secondary		
ciscotest	Cisco 4500	10.205.0.50	Routing	Secondary		
lame1	Generic Cisco	10.205.0.51	Routing	Secondary		
lame2	Generic Cisco	10.205.0.52	Routing	Secondary		

**Figure 10-6:** The ExtremeView applet, Configuration summary

The sub-components under Configuration in the Component Tree are the categories of configuration information that are available through this applet. These correspond to pages from the ExtremeWare Vista application running on the switch.

- ◆ Select one of these categories to display a list of switches, then select a switch to view the configuration settings for that switch in the category you've chosen.

As shown in Figure 10-7, this displays the current switch configuration, and provides an interface through which you can change the configuration.

ExtremeView

Switch : Summit5iTx (10.205.0.170)

IP Interface Configuration

Vlan Name	IP Address	Unicast Forwarding	Broadcast Forwarding	Multicast Forwarding
Default	10.205.0.170	Disabled	Disabled	Disabled

Configure IP Interface Parameters

Vlan Name	Unicast Forwarding	Broadcast Forwarding	Multicast Forwarding
Default	Enable	Enable	Don't Change

Submit

Configure IP Forwarding on Summit5iTx

**Figure 10-7:** The ExtremeView applet, Configuration details

Enter your changes directly into the editable fields in the configuration display. When you have made the necessary configuration changes, click **Submit** to send these to the switch for implementation.



# Viewing Switch Statistics

Select **Statistics** in the Component Tree to display summary statistics for the Extreme switches known to the EPICenter (see Figure 10-8).

The screenshot shows the ExtremeView applet interface. On the left is a component tree with 'Statistics' selected. The main area displays a table of switch statistics.

Name	Type	IP Address	MAC Address	10/100 Active	10/100 Ready	10/100 Total	Gigabit Active	Gigabit Ready	Gigabit Total
5411	Compaq 5411	10.205.0.37	00:10:e3:1d:00:1e						
5422	Generic Compaq	10.205.0.145	00:10:e3:1d:00:05						
CoreBuilder-4	Generic 3Com	10.205.0.182	00:80:3e:47:90:ce						
LabA-2	Extreme Alpine 380	10.205.0.38	00:e0:2b:81:fc:00	0	48	48	2	63	65
Summit24e2	Extreme Summit 24	10.205.0.149	00:01:30:10:00:19						
Summit24e3	Extreme Summit 24	10.205.0.30	00:01:30:11:00:06	1	23	24	0	2	2
Summit24e3	Extreme Summit 24	10.205.0.68	00:01:30:11:00:46	2	22	24	0	2	2
Summit3	Extreme Summit 3	10.205.0.156	00:e0:2b:03:3c:00	6	18	24	0	1	1
Summit48i	Extreme Summit 4E	10.205.0.41	00:01:30:ca:83:00	1	47	48	0	2	2
Summit5ITx	Extreme Summit 5i	10.205.0.170	00:01:30:6c:0d:00	0	0	0	5	12	17
Switch 1100	3Com Supper Stacl	10.205.0.181	00:90:04:d6:ad:98						
ciscotest	Cisco 4500	10.205.0.50	00:e0:f7:25:e3:a8						
lame1	Generic Cisco	10.205.0.51	00:06:28:1b:b3:c0						
lame2	Generic Cisco	10.205.0.52	00:30:94:ab:10:80						

**Figure 10-8:** The ExtremeView applet, Statistics summary

The sub-components under Statistics in the Component Tree are the categories of statistical information that are available through this applet. These correspond to pages of information from the ExtremeWare Vista application running on the switch.

- ◆ Select one of these categories to display a list of switches, and select a switch to view the configuration settings for that switch in the category you've chosen.

This displays the selected set of statistics for the selected switch. For some types of statistics, you may be able to view the data in different ways through the use of view options or filters, such as the options shown in Figure 10-9.

ExtremeView

Switch : Summit51Tx (10.205.0.170)

IP Route Table

End of Route Table.

Destination	Gateway	Mtr	Flags	Use	Vlan	Origin
*10.205.0.0/24	10.205.0.170	1	U u	16866	Default	Direct
*127.0.0.1/8	127.0.0.1	0	U H um	0	Default	Direct
*Default Route	10.205.0.1	1	U G S um	38906	Default	Static

View Next Set

View Options

View all entries unfiltered  Show permanent

Show by VLAN

Show By IP Address  and Netmask

Configure View

Show IP Route statistics on Summit51Tx

Applet started. Local intranet

Figure 10-9: The ExtremeView applet, Statistics details

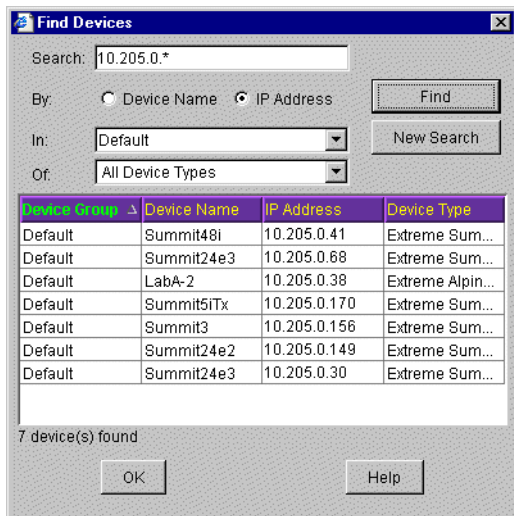
## Finding Devices

You can search for a device in the EPICenter database by name, by IP address, or by type of device. This may be useful if you have a large number of devices in your inventory.

To search for a device, follow these steps:

## 1 Click **Find** at the top of the Inventory Manager page.

The Find Devices dialog, shown in Figure 10-10, is displayed.



**Figure 10-10:** Find Devices dialog

## 2 Enter your search criteria:

You can search for devices by name or by IP address. You can limit the search to a specific domain, or to a specific type of Extreme device. Search criteria can include:

- A device name. Click the **Device Name** button, and enter a complete or partial name in the **Search:** field.
- An IP address. Click the IP Address button and enter a complete or partial IP address in the **Search:** field. You can use the wild card characters \* or ? in your search criteria.
  - \* acts as a wildcard for an entire octet (0-255)
  - ? is a wildcard for a single digit (0-9)
- A domain. Select the domain from the drop-down menu in the domain field. If you do not specify a name or IP address in the Search field, all devices in the domain you select will be found.
- A device type. Select the device type from the drop-down menu in the type field. If you do not specify a name or IP address in the Search field, all devices of the type you select will be found.

- 3** Click **Find** to search for devices that meet the criteria you have specified. All devices found are listed in the center panel. Information includes the domain in which the device can be found, its name, IP address, and the type of device.
- 4** Double-click on a device in the results table to highlight the device in the Component Tree, and to display the associated front panel view and status information for that device (see “Viewing Device Status Information” on page 10-3).
- 5** Click **New Search** to clear all search criteria.
- 6** Click **OK** to close the search window.

# 11

## Real-Time Statistics

---

This chapter describes how to use the Real-Time Statistics applet for:

- Viewing percentage utilization or total errors data for multiple ports in an Extreme Networks switch, a switch slot, or a port group.
- Viewing historical utilization, total errors, or individual errors data for a specific port on an Extreme Networks switch.

### Overview of Real-Time Statistics

The Real-Time Statistics feature of the EPICenter software enables you to view a graphical presentation of utilization and error statistics for Extreme Networks switches in real time. The data is taken from Management Information Base (MIB) objects in the etherHistory table of the Remote Monitoring (RMON) MIB. The Real-Time Statistics function is supported only for Extreme Networks switches.



*You must have RMON enabled on the switch in order to collect real-time statistics for the switch.*

You can view data for multiple ports on a device, device slot, or within a port group, and optionally limit the display to the “top N” ports (where N is a number you can configure). If you choose to view multiple ports, the display shows data for the most recent sampling interval for the selected set of ports. The display is updated every sampling interval.

You can also view historical statistics for a single port. If you choose to view a single port, the display shows the value of the selected variable(s) over time, based on the number of datapoints the MIB maintains in the etherHistory table.

You can choose from a variety of styles of charts and graphs as well as a tabular display.

You can view the following types of data:

- **Percent Utilization** for each port in the set (device, port group, or single port).  
Percent utilization reports the value of the **etherHistoryUtilization** MIB object. The MIB defines this variable as follows:

**Table 11-1:** Definition of RMON Utilization Variable Used in Port Utilization Displays

<b>etherHistoryUtilization</b>	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, graphed in percents.
--------------------------------	--

- **Total Errors** for each port in the set (device, port group, or single port).  
Total Errors is the sum of the six error variables shown in Table 11-2.
- **Individual Errors** for a single port.

An individual errors display shows the six variables shown in Table 11-2.

**Table 11-2:** Definition of RMON etherHistory Error Variables for Port Error Displays

<b>etherHistoryCRCAlignErrors</b>	The number of packets received during this sampling interval that had a length between 64 and 1518 octets, inclusive (excluding framing bits but including Frame Check Sequence (FCS) octets), but that had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
<b>etherHistoryUndersizePkts</b>	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
<b>etherHistoryOversizePkts</b>	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.

**Table 11-2:** Definition of RMON etherHistory Error Variables for Port Error Displays

<b>etherHistoryFragments</b>	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
<b>etherHistoryJabbers</b>	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
<b>etherHistoryCollisions</b>	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.

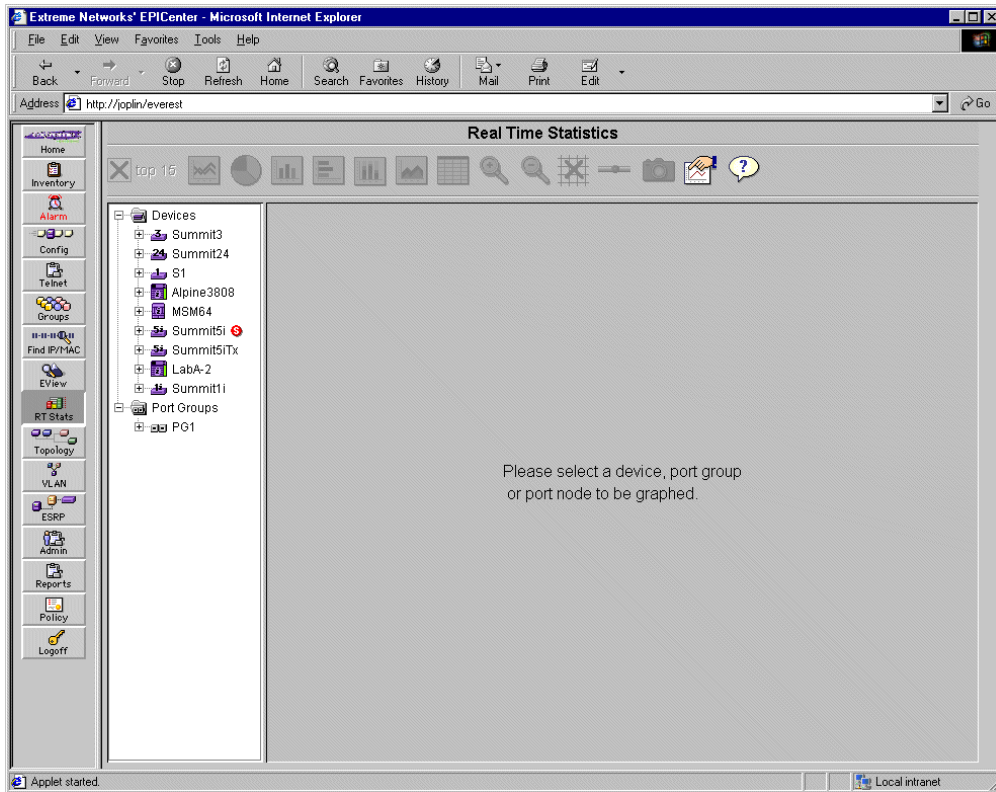
## Displaying Multi-port Statistics

When you click the **RT Stats** button in the Navigation Toolbar, the main Real-Time Statistics page is displayed, as shown in Figure 11-1. Initially, no data is displayed—you see a message asking you to select a device, device slot, or port group to be displayed.

The Component Tree displays the devices and port groups for which you can display statistics. An “S” in a red circle next to a device name indicates that the device is not responding to SNMP requests. A port group with a red-circled “S” indicates that the port group is empty.



*The Real-Time Statistics applet does not support hierarchical port groups. If you have created port groups in the Grouping Manager that include subgroups as members, the subgroups will not appear in the Component Tree of the Real-Time statistics applet. Instead, any ports that are members of subgroups will be displayed directly under the top-level port group, as if they are members of the top-level group.*



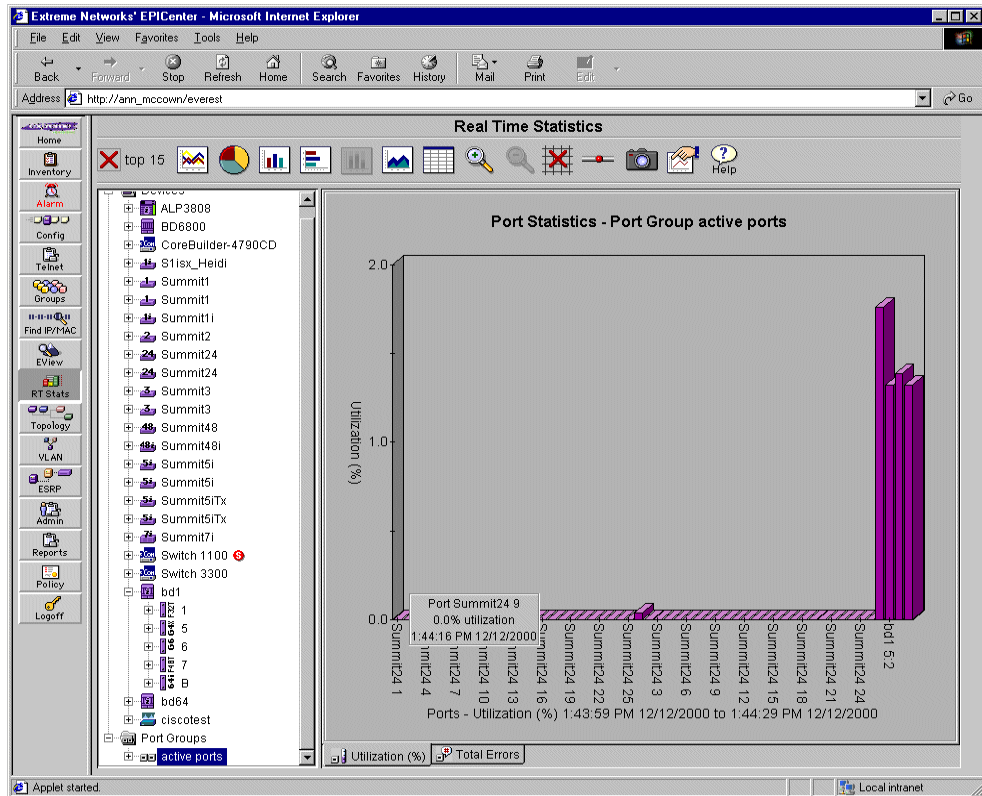
**Figure 11-1:** Real-Time Statistics main page

For an individual port, you can display individual errors in addition to utilization and total errors.

- ◆ Select a network device to display data for some or all ports on the device.
- ◆ Select a port group to display data for all ports in the port group.

You will first see a message saying “Please wait, loading data.” If the EPICenter server is successful in accessing the data, utilization data is displayed as shown in Figure 11-2.





**Figure 11-2:** Bar chart showing port statistics for a group of ports

If you place the cursor near a bar in the chart, a pop-up window shows the port number and device, actual data value, and the time stamp on the data sample.

You can use the mouse to change the depth and rotation of a 3-dimensional chart:

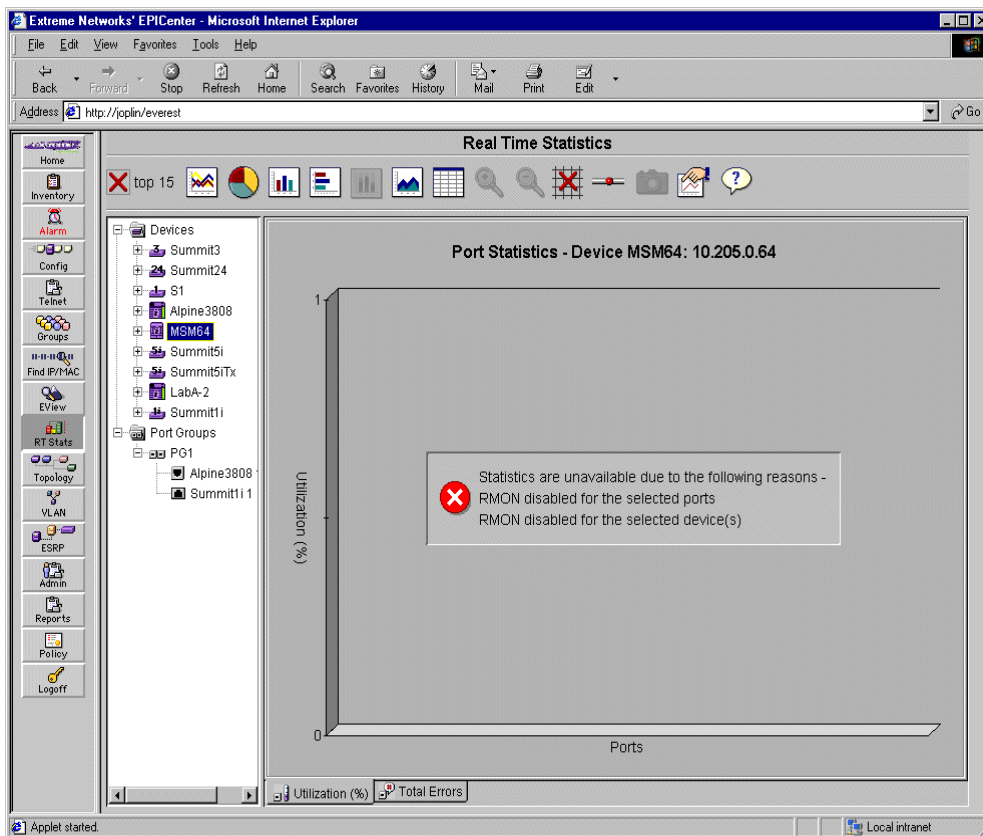
- Hold down the [Shift] key, press the left mouse button, and drag the cursor left or right to rotate the graph.
- Hold down the [Ctrl] key, press the left mouse button, and drag the cursor up or down to set the depth of the 3-dimensional view.

For any of the bar graphs, move the cursor and then wait to see the change take effect, which may take a few seconds.

There are cases where you may not see data for every port you expect in a multi-port display:

- You have selected the “top N” feature (top 15 by default), so only the “N” ports with the highest utilization or the highest total number of errors are displayed.
- RMON is disabled for some ports on the switch. If the switch as a whole can be reached and is reporting data, then individual ports that do not report data will be ignored. No error message appears in this case.

If the EPICenter server is *not* successful in loading data from the device, it displays a message similar to that shown in Figure 11-3.



**Figure 11-3:** Warning displayed when the EPICenter server cannot retrieve data

There are several reasons why the EPICenter server may not be able to display *any* device data:

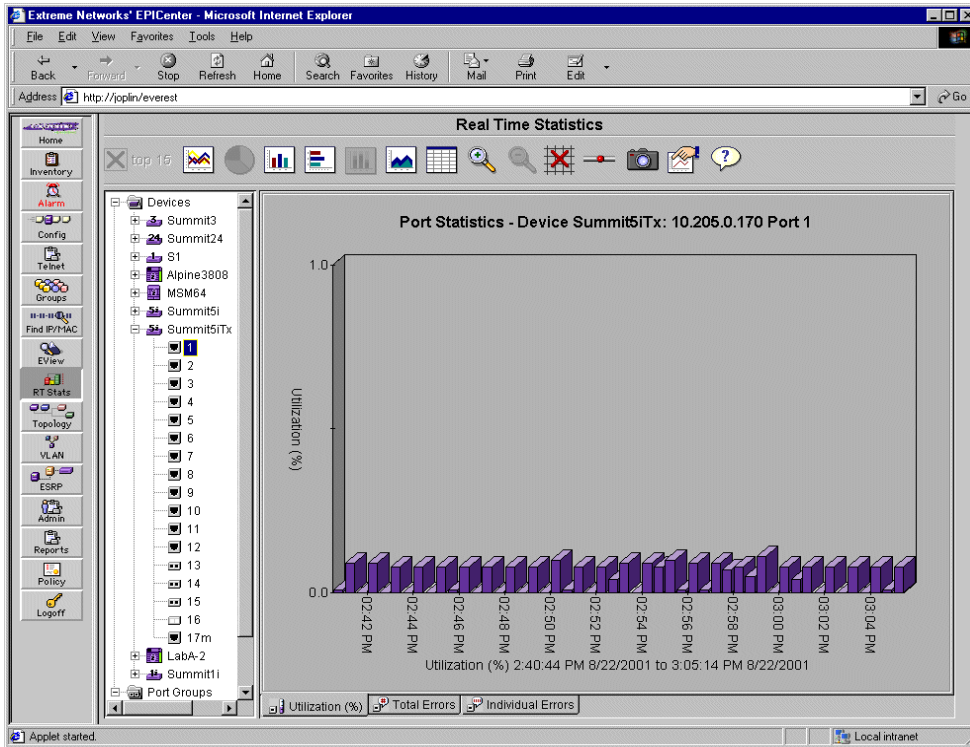
- The EPICenter server cannot communicate with the device (indicated by an “S” in a red circle next to the device name).
- The device does not have RMON enabled, or RMON was just recently enabled and no data samples exist yet.

## Displaying Statistics For a Single Port

In addition to displaying data for a set of ports, you can display historical data for an individual port. You can select a port in one of two ways:

- Double-click on the data point for an individual port in the device or port group statistics display (bar, data point, or pie slice in the respective chart, or row in a tabular display).
- Click on a device, device slot, or port group in the left-side Component Tree to list the ports it contains, then select a port.

A set of utilization statistics for the selected port is displayed, as shown in Figure 11-4.



**Figure 11-4:** Utilization data over time for an individual port on a device

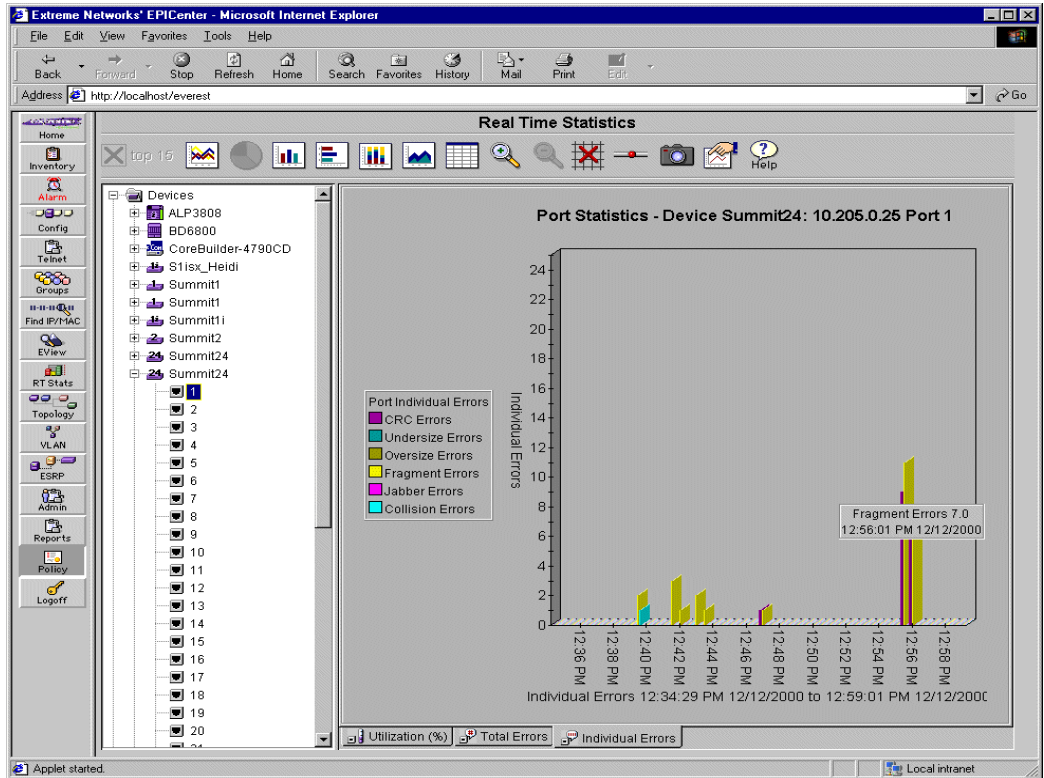
The number of data points displayed, and the sampling interval are user-configurable parameters, within the limitations of the device configuration. The defaults are:

- A 30-second sampling interval
- 50 data points displayed

However, in Figure 11-4, only 25 data points are displayed, because that is the maximum number of values the BlackDiamond switch stores as historical data.

For an individual port, you can display individual errors in addition to utilization and total errors.

- ◆ Select the tab at the bottom of the page to generate one of these displays. Figure 11-5 is an example.



**Figure 11-5:** Individual errors in a single-port chart

## Changing the Display Mode

The icons at the top of the page let you select the format of the statistical display, and control several other aspects of the display.

- top 15 Select this to determine whether the display for a device or port group will include all ports, or only the top N ports (where N is initially fifteen).
- top 15 Click the icon to toggle between the red X, which indicates the top N limitation is not in effect, and a green check, which indicates that the top N ports are being displayed. The top N ports are displayed in order from highest (largest percent utilization or largest total errors) to lowest. The number of ports (N) is a user-configurable setting. This option is available only for multi-port displays.



Select this to display the data as a line graph. This chart type is especially useful when displaying individual errors for a single port.



Select this to display the data as a pie chart. This chart type is available only when you are displaying statistics for multiple ports on a device, device slot, or in a port group. The maximum number of slices in the pie is a user-configurable setting. It is initially set to display 10 slices.



Select this to display the data as a bar chart. A 3D bar chart is the default for all chart displays. The 3D setting is also a user-configurable option.



Select this to display the data as a horizontal bar chart. This chart type by default displays in 3D. The 3D setting is also a user-configurable option.



Select this to display the data as a stacked bar chart. This chart type is only available when you are displaying individual errors for a single port.



Select this to display the data as an area chart. This chart type by default displays in 3D. The 3D setting is also a user-configurable option.



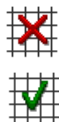
Select this to display the data as a table.



Select this to zoom in on (magnify) the size of the display. You can select this repeatedly to zoom up to three times the screen size.



Select this to zoom out (shrink) the size of the display. You can select this repeatedly until the chart is the desired size.



Determines whether grid lines are displayed on the background of the chart. Click the icon to toggle between the red X, which indicates that grid lines are turned off, and the green check, which indicates that grid lines are turned on.



Determines whether the graph data is updated automatically at every sampling interval. Click on the icon to toggle between continuous updates, indicated by the bar with the red dot (representing a traveling data packet), and the open palm, indicating that updates have been suspended.



Select this to take a “snapshot” of the graph or table view of the current real-time statistics data.



Select this to bring up the graph preferences pop-up window. You can change a variety of settings, such as graph and data colors, the sampling interval, or the number of ports in a top N display.

## Setting Graph Preferences

To change the graph settings used in this applet, click the **Set Graph Preferences** icon in the toolbar.

The Graph Preferences window is displayed, as shown in Figure 11-6.

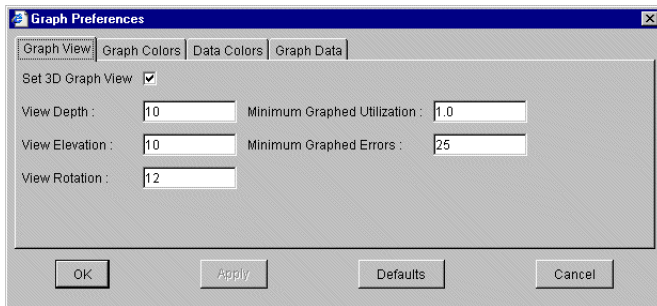
Use the tabs across the top of the window to select the type of setting you want to change. Each tab displays a page with a group of related settings. When you have changed any setting you want on a given page:

- Click **Apply** to put the changes into effect, but keep the Graph Preferences window open so you can make changes on another page.
- Click **OK** to put the changes into effect and close the Graph Preferences window.



*The Graph preferences settings are not persistent—if you move to another EPICenter applet, the settings will return to the defaults.*

**Graph View** (Figure 11-6) lets you change from 3D to 2D displays, and change the values for the 3D depth, elevation and rotation.

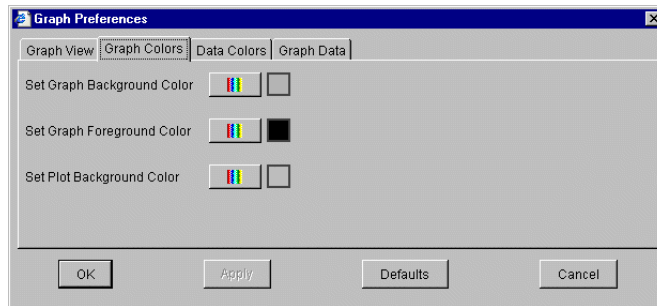


**Figure 11-6:** Setting 3D graph preferences

- To change to a 2D graph view, click the **Set 3D Graph View** box to remove the check mark.
- **View Depth** controls the depth of a bar. The default is 10, maximum is 1000.
- **View Elevation** controls the elevation (rise) from the front of the bar to the back, in degrees. The default is 10°, range is ±45°.
- **View Rotation** controls the angle of rotation of the bar, in degrees. The default is 12°, range is ±45°.
- **Minimum Graphed Utilization** specifies the minimum scale for the Y axis for utilization graphs. The default is 1.0 (1%), meaning that the Y axis will not show less than 1% as the top value of the Y axis.
- **Minimum Graphed Errors** specifies the minimum scale for the Y axis for error graphs. The default is 25, meaning that the Y axis will not show less than 25 errors as the top value of the Y axis.



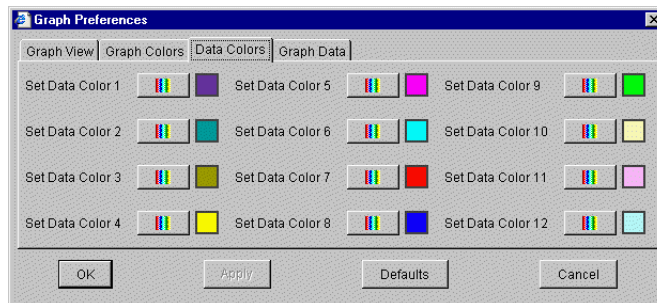
**Graph Colors** (Figure 11-7) lets you set the colors for the graph background and text (data and axis labels).



**Figure 11-7:** Setting graph color preferences

- To change a color, click on a button with the color bar icon. This displays a color selection window where you can select the color you want. You can select a color using color swatches, or by specifying HSB or RGB values.
- **Set Graph Background Color** sets the color of the background surrounding the graph.
- **Set Graph Foreground Color** sets the color of the text and bar outlines.
- **Set Plot Background Color** sets the color of the background behind the graph data.

**Data Colors** (Figure 11-8) lets you set the colors used for the various data sets in your graph.

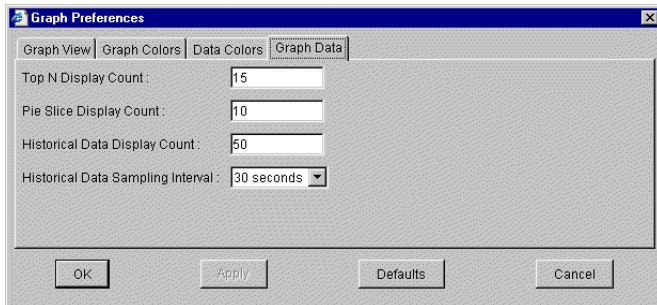


**Figure 11-8:** Setting data color preferences

- To change a color, click on a button with the color bar icon. This displays a color selection window where you can select the color you want. You can select a color using color swatches, or by specifying HSB or RGB values.

- **Data Color 1** is the color used for Utilization and Total Error graphs.
- Data colors 1 through 6 are used for the different errors in a individual errors chart.
- Data colors in order starting from 1 are used in a pie chart, for as many slices as you've specified. (If you specify more than 12 slices, the colors will repeat, with slice 13 using the same color as slice 1).

**Graph Data** (Figure 11-9) lets you set several miscellaneous graph parameters.

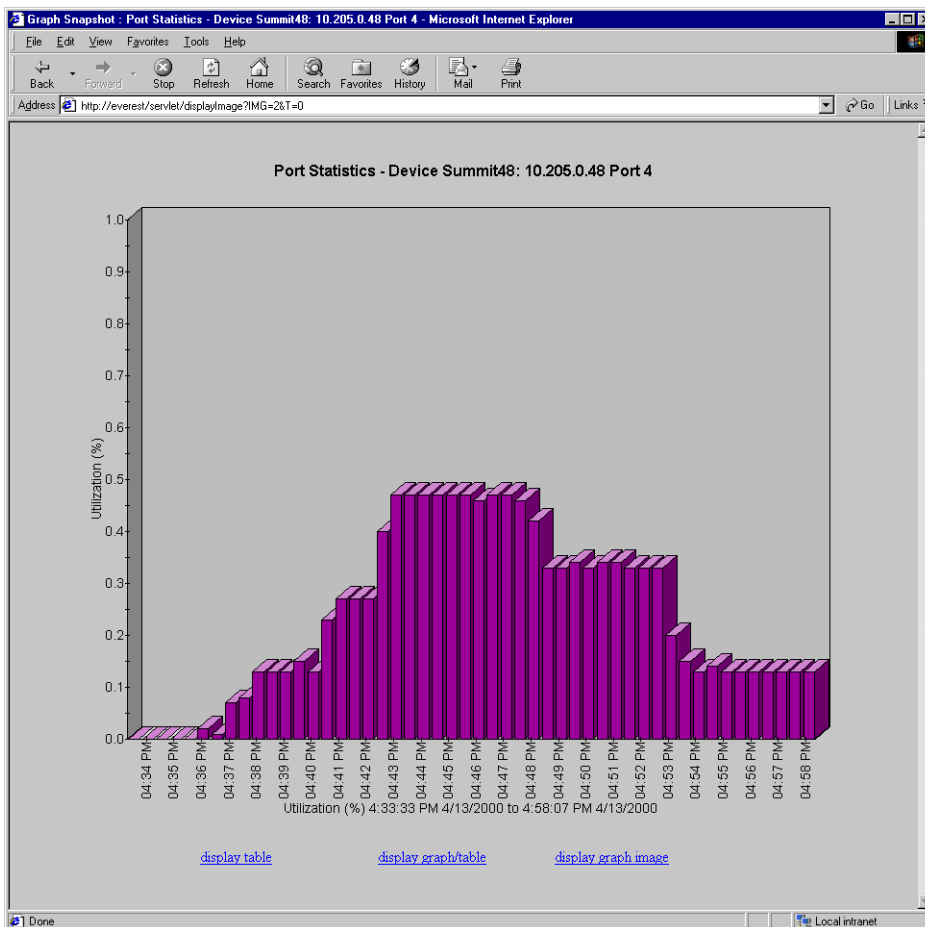


**Figure 11-9:** Setting other graph preferences

- **Top N Display Count** specifies the number of ports to include in a Top N display. The default is 15, maximum is 100.
- **Pie Slice Display Count** specifies the number of slices to display in a pie chart. The default is 10, maximum is 50.
- **Historical Data Display Count** specifies the number of historical data points to display in a graph for an individual port. The default is 50, the maximum value you can set is 100. However, the actual maximum number of data points you can get is determined by the SNMP agent running in the device from which you are getting data.
- **Historical Data Sampling Interval** is the sampling interval to use when displaying historical data. Select a choice from the pull-down list. The choices in the list are determined by the configuration of the device from which you are getting data.

## Taking Graph Snapshots

The Real-Time Statistics Snapshot feature lets you take a static image of a graph or table view of the current real-time statistics data. The snapshot generates a persistent HTML page that is displayed in a separate browser window (see Figure 11-10).



**Figure 11-10:** Snapshot of Real-Time Statistics graph display

To take a snapshot, click the camera icon located in the toolbar at the top of the RT Statistics applet window. The snapshot image will be displayed in a new browser window in the same form (graph or table) as it was in the RT Statistics applet. Graph images reflect the current display size and graph type (pie, bar, etc.).

From the browser window, the snapshot image can be saved as a file, printed, or sent by e-mail, just as with any other HTML page.

When a graph image is displayed in the browser window, you can click a link below the initial display to change the way the data is displayed:

- **display table** reformats the data as a table
- **display graph/table** displays both the graph and table formats on the same HTML page
- **display graph image** displays the data as a graph, in the style in which it was displayed when the snapshot was taken.



*Once you select “display graph image” you can no longer change the display format to a table or to a dual display. However, you can use the browser “Back” button to go to the previously displayed page.*

When you snapshot a table, you cannot change to a graph from within the snapshot image browser window.

The HTML page persists in a snapshot image cache until the EPICenter server is restarted, or until the image cache becomes full. When the image cache reaches its limit, older snapshot images will be deleted as needed to make room for new snapshot images.

# 12

## Network Topology Views

---

This chapter describes how to use the EPICenter Topology View applet for:

- Viewing EPICenter Topology maps
- Creating new topology views
- Adding, moving and deleting map elements (nodes and links)
- Modifying the layout of a topology map
- Displaying the alarm browser, telnet window, real-time statistics, a front panel view, or ExtremeWare Vista for a specific node on the map

### Overview of EPICenter Topology Views

EPICenter's Topology applet allows you to view your network (EPICenter-managed devices and the links between devices) as a set of maps. These maps can be organized into sets of submaps that allow you to represent your network as a hierarchical system of campuses, buildings, floors, closets, or whatever logical groupings you want. You can also create additional topology views (sets of maps) so you can create several different representations of your network for different purposes.

For views with the Auto Populate View option enabled, the Topology applet will automatically add device nodes that are added to EPICenter's device inventory, add links that exist between the devices, and organize them into submaps as appropriate. You can customize the resulting maps by moving elements, adding new elements, such as links, "decorative" (non-managed) nodes, and text, and customizing the device nodes themselves.

In addition, from a managed device node on the map, you can invoke other EPICenter functions such as the alarm browser, Telnet, real-time statistics, a front panel view, or ExtremeWare Vista for the selected device.

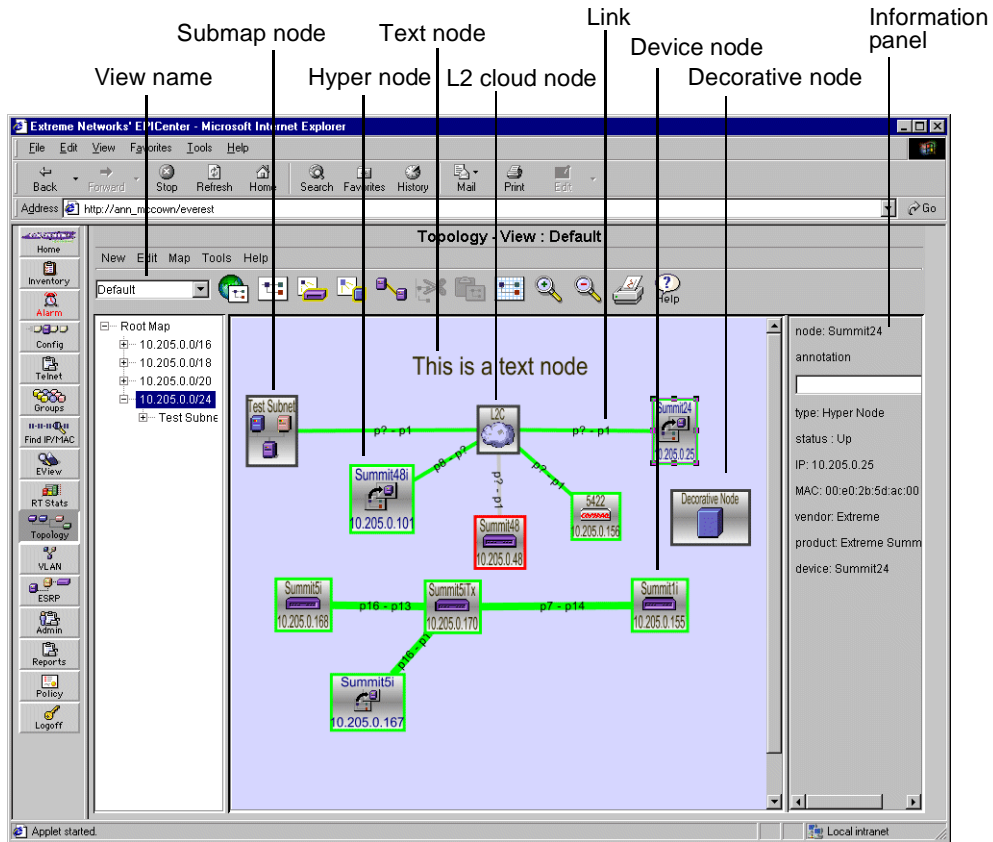
Maps are initially created in a default layout based on information in EPICenter's device inventory about the devices and their connectivity. You can customize the layouts into hierarchical views using drag and drop or cut and paste. You can also add and remove "decorative" nodes (nodes that aren't discovered or managed by EPICenter) and links.

## Displaying a Network Topology View

Click the **Topology** button in the EPICenter Navigation Toolbar to display the main Topology View page, as shown in Figure 12-1.



*If you have not yet performed a Discovery (i.e. there are no devices in EPICenter's Inventory database) the map will be blank.*



**Figure 12-1:** The Topology View

A **View** is a unique, named hierarchy of maps, consisting of a root map and optional submaps, depending on the topology of the network. The current View name is displayed in the pull down field at the left of the icon bar.

A **Map** is a collection nodes and links.

The **left-hand panel** displays the **Map Hierarchy Tree**. This starts at the root map and shows the hierarchy of submaps in the current topology view. The current map name is highlighted.

The **center panel** displays the **currently selected map** in the current topology view. Only one view and map can be displayed at a time.

The **right-hand panel** is the **Map Element Description** panel, that displays information about the currently selected map element (node or link) if one (and only one) is selected. Otherwise, the panel is empty.

When you do a Discovery or add a device in the Inventory applet, the newly added devices are placed into the default topology view, (named “Default”). If you have created other maps with the Auto Populate View feature enabled, those views will also be populated with the newly added devices. Device connectivity and the map hierarchy is determined by the information learned from the EPICenter database.

For views with the Auto Populate View option enabled, EPICenter places devices on the Root Map or into submaps based on the following criteria:

- Devices with IP Forwarding enabled are always placed on the Root Map
- Devices without IP Forwarding enabled are placed in submaps based on the subnet mask. In the Default view, submaps are named based on the subnet IP address plus the subnet mask: for example, 10.205.0.0/16, 10.205.0.0/24, and so on.

Both Extreme and third-party devices are placed using these rules. For Extreme devices, you can find the subnet mask and IP Forwarding status by looking at the device in the VLAN applet. For third-party devices, you must query the device itself if you want to determine these settings.

## Map Elements

The following elements can appear on a map:

**Device Nodes:** Device nodes represent the managed devices found in EPICenter’s Inventory data base.



**Figure 12-2:** Example of device nodes, including an unknown device type

A device node shows the following information:

- The name of the device as it is kept in the Inventory database
- An optional, user-supplied annotation for the node



- A small icon representing the specific device or device product line, if the device is of a known type, or an “unknown” device icon (a circle with a question mark) as shown in Figure 12-2
- The device’s IP address
- The device status, indicated by the color of the icon border
  - A green border indicates that the device is UP
  - A red border indicates that the device is DOWN

Each managed device known to EPICenter can only appear once in each topological view.

**Submap Nodes:** A submap node represents a child map of the current map.



**Figure 12-3:** Example of a submap node

The submap node icon shows the following information:

- The name of the node (submap), which can be edited. By default, it is given the subnet address/subnet mask as the name
- A submap icon, as shown in Figure 12-3

A submap node does not provide any status information.

**L2 Cloud Nodes:** An L2 cloud map node provides connectivity between devices when the details of the connectivity cannot be determined.



**Figure 12-4:** Example of an L2 cloud node

The L2 cloud node icon shows the following information:

- The name of the node (cloud), which can be edited. By default, it is named L2C
- A cloud icon, as shown in Figure 12-4

An L2 cloud node does not provide any status information.



*You cannot add L2 cloud nodes; they are placed automatically by EPICenter as required by device connectivity. You can remove them, but they may be replaced automatically by EPICenter if still needed.*

**Hyper Nodes:** A hyper node represents a link termination when the actual terminating node (device or cloud) is present on another map. Thus, a hyper node will show the same information as the node it represents (except for the optional node annotation):



**Figure 12-5:** Example of hyper node icons representing a device and an L2 cloud

A hyper node icon shows the following information:

- The name of the device or cloud node that this hyper node represents
- An optional, user-supplied annotation for a device hyper node. This is a different annotation than will appear in the device node that this hyper node represents
- A hyper node icon, as shown in Figure 12-5
- The device IP address, for a device hyper node
- The device status, for a device hyper node, as indicated by the color of the icon border:
  - A green border indicates that the device is UP
  - A red border indicates that the device is DOWN

An L2 cloud hyper node does not show any status information.



*You cannot add, cut, or delete hyper nodes; they are placed and removed automatically by EPICenter as required by device connectivity.*

**Decorative Nodes:** A decorative map node can be created by the user to represent any other type of node that is not discovered or managed by EPICenter, such as a server or workstation.



**Figure 12-6:** Example of a decorative node

A decorative node shows the following information:

- The name or description of the node, which can be edited
- A decorative node icon, as shown in Figure 12-6

**Text Nodes:** A text map node is a single-line text field that can be placed anywhere in a network map. It can be used to create a title for the map, additional annotations for other map elements, comments, and so on.

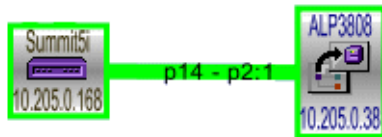
**Links:** A link represents connectivity between nodes in the map. When a link connects two devices on the same map, the link will be annotated with the port number or slot and port number for each of the endpoints, as shown in Figure 12-7. When an endpoint is not known (the link terminates in a L2 cloud) the unknown port is indicated with a question mark. The link also shows the following information:

The width of the link indicates the link type:

- A thick line indicates a gigabit link
- A thin line indicates a 10/100 link

The color of the link indicates the link status:

- A green line indicates that the link is UP
- A red line indicates that the link is DOWN
- A grey line indicates that the status is unknown



**Figure 12-7:** Example of a gigabit link showing endpoint connectivity and Up status

If RMON statistics are enabled for the map, then link utilization (as a percentage of link capacity) will be displayed for each port on a link between devices that have RMON enabled in the device. The utilization is updated at the nominal RMON rate as set in the switch—typically every 30 seconds. The default is that RMON statistics are not enabled for a map. To enable the display of RMON statistics, see “Setting Map Properties” on page 12-23.



*If RMON statistics are not enabled in the switch, then no statistics will be displayed, even if you enable the display of RMON statistics for the map.*

## Manipulating Map Elements

Map elements (nodes and links) can be resized, cut and pasted, and deleted, either using commands from the topology view menus, from the pop-menu enabled with a right-cursor click on the map background, using specific keyboard short cuts, or (under Windows NT or Windows 2000) through the regular Windows mouse and cursor actions and keyboard shortcuts.

For example, you can resize an individual node by selecting the node and doing one of the following:

- Using the cursor to grab one of the resize handles that appear when the node is selected, and dragging the handle to resize the node
- Selecting the Inflate Nodes or Deflate Nodes command from the Map Menu, or by using the keyboard shortcuts for those commands (see the sections “Inflating the Map Nodes” and “Deflating the Map Nodes” on page 12-21).

## Map Element Description Panel

When you select a map node or link with the cursor, a panel on the right-hand side of the window displays information about the node or link.

For map nodes the information panel displays the following:

- Node name (an editable name for all but device nodes and device hyper nodes)
- Node annotation field (for device nodes and device hyper nodes only)
- Node type (Device, Submap Node, L2 Cloud, Decoration Node, Text Node, or Hyper Node)
- Status (Up, Down, or None)
- IP (IP address for a Device node, n/a for any other node type)
- MAC (MAC address for a Device node, n/a for any other node type)
- Vendor (Device vendor name for a Device node, n/a for any other node type)
- Product (Product name for a Device node, n/a for any other node type)
- Device (Device name obtained from the sysName variable for a Device node, n/a for any other node type)

For links, the information panel displays the following for each link endpoint:

- The name of the node

- The device represented by the endpoint node
- The device port or slot and port to which the link connects, if known
- The utilization percentage, if RMON is enabled on the device *and* if RMON statistics are enabled for this map. The default is that RMON statistics are not enabled for a map. This is updated regularly, typically every 30 seconds
- The total errors, if RMON is enabled on the device and if RMON statistics are enabled for this map. This is updated regularly, typically every 30 seconds

In addition, for the link itself, the following information is displayed:

- The status of the link: UP, DOWN, or NONE
- The link type (speed): 10/100, 1000, or unknown
- Whether the link is load shared: yes or no

## Manipulating Map Views

You can create new topology views or move elements around on existing maps in a number of ways. The Topology View applet provides a number of ways to invoke the various commands and functions:

- A series of pull-down menus. All commands and functions can be accessed from these menus
- A set of icons that represent a commonly-used subset of the functions available
- A pop-up menu you can invoke by clicking the right mouse button on any unoccupied area of the map background
- A pop-up menu you can invoke by right-clicking on a Device map node
- Keyboard shortcuts for some functions

The various methods you can use to perform a command are described under each command or function.


### Creating a New View or a New Map

The Default map contains all the network devices known to EPICenter, arranged based on EPICenter's internal algorithms (see the discussion on page 12-4 in the section "Displaying a Network Topology View"). However, it is often convenient to create views based on other criteria, such as physical location, departmental organization, and so on. The

Topology applet lets you create additional views that organize your network elements in any way you wish.

## Creating a New View

You can create a new view (and its Root Map) by doing one of the following:

- Select **New View** from the **New** menu
- Click the “Create new view” icon on the icon bar: 

A pop-up window appears where you can enter the name of the view.

When you click **OK**, a new, blank root map is displayed. The new view name appears in the **View** field at the left of the icon bar.


If you select the **Auto populate view** option, as new devices are added to EPICenter, they will also be added to the view, and submaps, L2 clouds and hyper nodes will be created as needed. If you do a Discovery after you have created a view with the auto populate option enabled, all new discovered devices will be added to the view.

You can display the Default view or any other views you have created by selecting the View name from the pull down list in the **View** field.

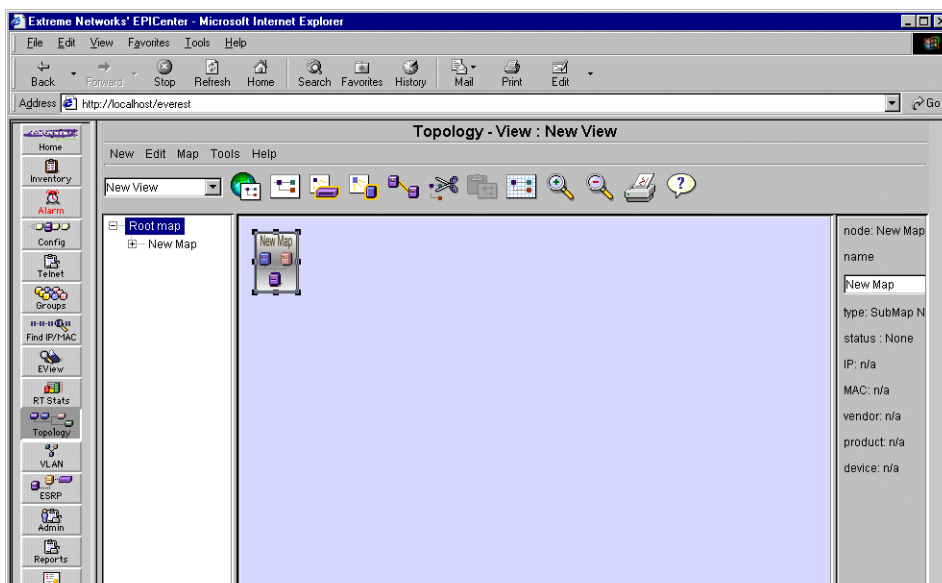
You can rename the view by clicking in the **View** field and typing over the view name. Click away from the View field to commit the change.

## Creating a New Submap

You can create a new map by doing one of the following:

- Select **New Map** from the **New** menu
- Click the “Create new map” icon on the icon bar: 

A new submap node appears on the map, and a New Map entry appears in the map hierarchy tree, as shown in Figure 12-8.



**Figure 12-8:** Adding a new map

To give the submap a different name, select the submap node, and change the name in the name field in the right-hand panel (the Information panel). The change will take effect when you click away from the submap node.

You can also change the name of any map (including the Root Map) by clicking slowly twice on the name in the Map Tree Hierarchy. This puts you into an edit mode where you can change the name.

When editing the map name in either location, you can cancel the edit with the [Esc] key, as long as you have not yet committed it.


You can commit the change with the [Enter] key, or by clicking in a different panel from the one where you are editing.

## Adding Elements to the Map

You can add a variety of elements to your map: device nodes, submap nodes, links, decorative nodes, and text “nodes”.

## Adding a Device Node

You can add device nodes to your map by doing one of the following:

- Select **New Device Map Node** from the **New** menu
- Click with the right mouse button on the map background to display the pop-up menu, then select **New Device Map Node**
- Click the “Create new device map” node icon on the icon bar: 

A pop-up window appears with a list of all devices currently known to ExtremeWare EPICenter, that are not already used somewhere in this view. Select the devices you want to add and click OK. The device node will appear on the map, identified by the information from EPICenter’s inventory database.

If the device has known links to other devices already on the map, or on other submaps within the same view, those links will also be placed on the map. An L2 cloud node or a hyper node, may also be placed on the map, if required for connectivity between the devices.


If all devices known to EPICenter are already placed in this view (on any of the maps in the view) the pop-up window will inform you of that fact.

## L2 Cloud Nodes and Hyper Nodes

You cannot add L2 cloud nodes and you cannot add or remove hyper nodes to or from your map; they are added automatically if the connectivity between device nodes requires it.

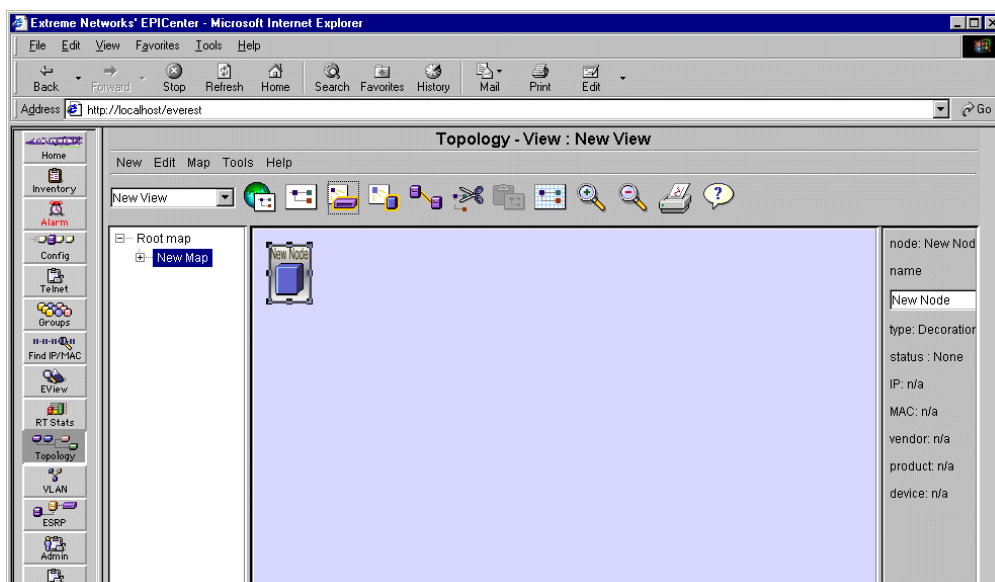
## Adding a Decorative Node

You can add a decorative node to your map by doing one of the following:

- Select **New Decorative Map Node** from the **New** menu
- Click with the right mouse button on the map background to display the pop-up menu, then select **New Decorative Map Node**
- Click the “Create new decorative map node” icon on the icon bar 

A decorative map node is a node that can be used to represent any component of your network that is not recognized or managed by ExtremeWare EPICenter.





**Figure 12-9:** Adding a decorative node to the map

You can change the node name by selecting the node, and editing the contents of the name field in the right-hand panel (the Information panel). The change will take effect when you click away from the submap node.

### Adding a Text Node

You can add a text node to your map by doing one of the following:

- Select **New Text Map Node** from the **New** menu
- Click with the right mouse button on the map background to display the pop-up menu, then select **New Text Map Node**

A text map node can be used to annotate your map, such as to create a title for the map.

### Adding a Map Link

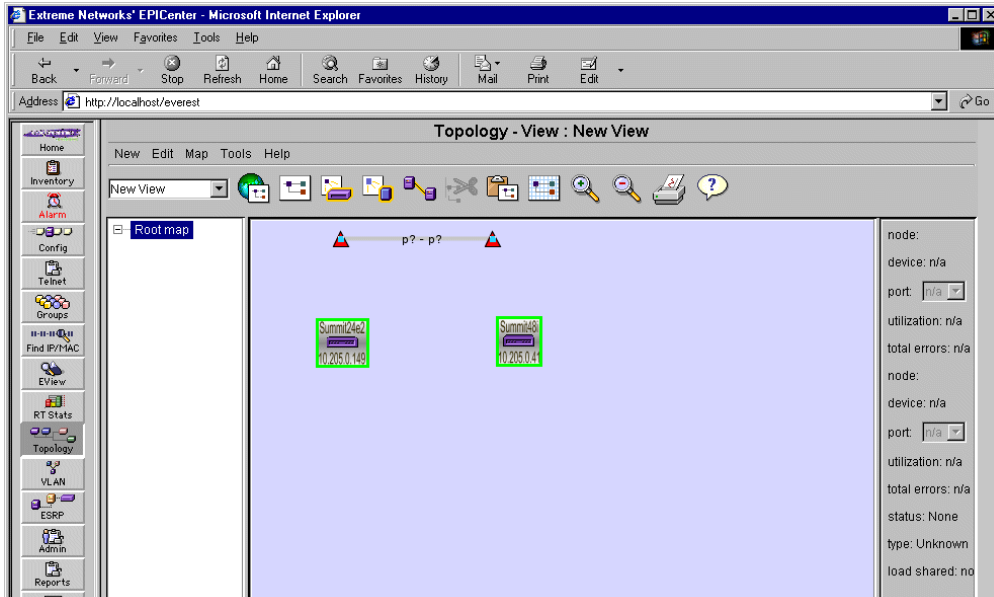
You can add a link between nodes on your map by doing one of the following:

- Select **New Map Link** from the **New** menu
- Click with the right mouse button on the map background to display the pop-up menu, then select **New Map Link**

- Click the “Create new map link” icon on the icon bar



A link is added to your map, as shown in Figure 12-10.



**Figure 12-10:** Adding a link to your map

To attach the link between two map nodes, follow these steps:

- 1 Select one of the red triangles, then wait until a move cursor appears
- 2 Drag and drop one end of the link onto one of the node you want to connect
- 3 Do the same with the other end of the link

After the link is connected, you can specify endpoint for the link. To specify the end points, follow these steps:

- 1 Select the link
- 2 In the right-hand information panel, select the port for the endpoint from the list in the **Port** field for first device
- 3 Select the port for the other endpoint from the list in the **Port** field for second device, as shown in Figure 12-11

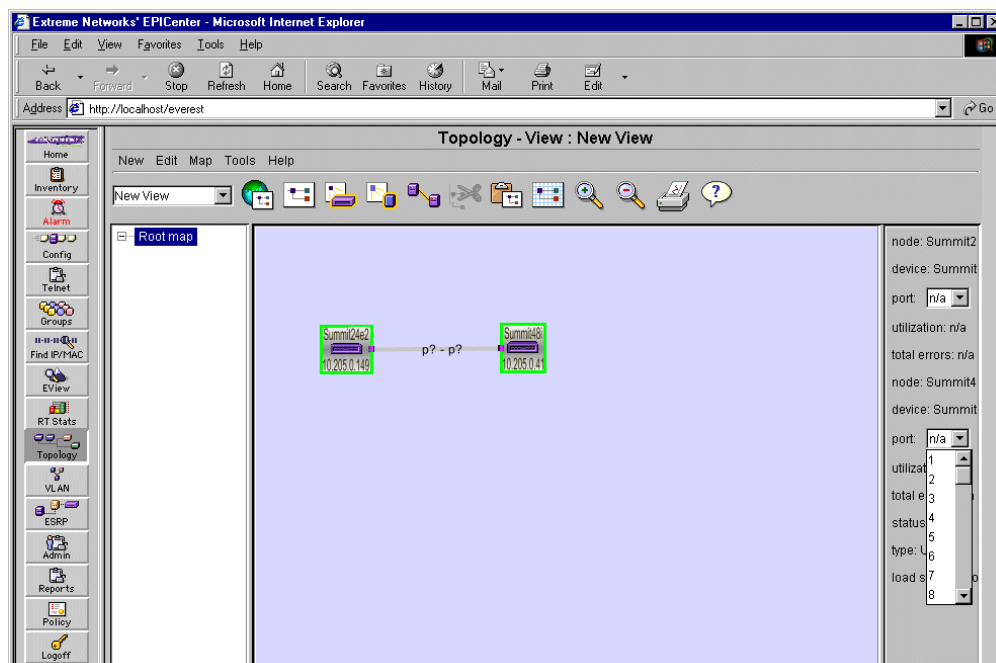


Figure 12-11: Specifying ports for a new link connection

## Discovering Links Between Devices

EPICenter will eventually rediscover links between devices if they are real existing links, even if you have deleted the links from your map. However, if you want to have EPICenter discover new links immediately, instead of waiting for the next polling cycle, you can use the Discover Links command.

To have EPICenter rediscover all existing links between devices, do the following:

- Select **Discover Links** from the **New** menu

EPICenter will add or update the links that exist between the devices on your map.

## Editing the Map

You can edit your topology views in a number of ways, including changing the names of the views and maps, and cutting, pasting, or deleting map elements.

## Renaming a Topology View

You can change the name of a view (including the Default view) by doing one of the following:

- Select **Rename View** from the **Edit** menu
- Click once on the view name in the view name field

Either of these actions puts you into an edit mode where you can directly change or replace the contents of the field.

## Renaming a Map

You can change the name of the current map by doing one of the following:

- Select **Rename Map** from the **Edit** menu
- Click twice on the Map name in the Map Hierarchy Tree

Either of these actions puts you into an edit mode where you can change or replace the name in the Map Hierarchy Tree.

You can also change the name of the map in the Map Properties window, as discussed in “Setting Map Properties” on page 12-23.

## Deleting a View

To delete the entire current view, select **Delete View** from the **Edit** menu. You will be asked to confirm that you want to delete the entire view. This function deletes the currently displayed view, including all of its maps.

Once the view is deleted, the next remaining view is displayed, if there are any other views.



*You can use this command to delete the Default view. However, if you do this, it will be difficult to recreate the view and its submaps.*

## Deleting a Submap

To delete a submap, you must first display the submap you want to delete, and delete all the elements on the map. You can then delete the submap by selecting **Delete Map** from the **Edit** menu. You can also delete a submap by clicking the submap node on its parent map.

You will be asked to confirm that you want to delete the map.



*A submap must be empty before you can delete it.*

You cannot use the **Delete Map** command to delete the Root Map.


To delete the Root map you must delete the entire View with the **Delete View** command.

## Cutting Map Nodes

You can cut selected device, decorative, or text nodes from the map in order to paste them in another location.

- You can cut a submap node as long as it is empty
- You cannot cut a hyper node. A hyper node will be removed automatically as appropriate, if all nodes on the current map that have links to that node, are removed
- L2 cloud nodes can be cut, but cannot be pasted.

To cut one or more nodes, do the following:

- 1 Select the nodes you want to cut. You can select multiple nodes by dragging the cursor to rubber-band the selection, or by using Shift-click (hold down the shift key while clicking the cursor on the nodes you want to select).
- 2 Then, cut the nodes by doing one of the following:
  - Select **Cut Map Nodes** from the **Edit** menu
  - Click the “Cut nodes from map” icon on the icon bar 
  - Enter [Alt]+X from the keyboard




*You will NOT be asked to confirm this action: if you cut a node by mistake, you will just need to paste it back again to the map.*

To remove nodes from the map without provision for pasting them, use the **Delete Map Nodes** command.

## Pasting Nodes onto a Map

Once you have cut one or more nodes, you can paste them onto another map by doing one of the following:

- Select **Paste Map Nodes** from the **Edit** menu

- Click the “Paste nodes into map” icon on the icon bar 
- Enter [Alt]+V from the keyboard

These commands will only be available if there are cut nodes currently on the clipboard.

If nodes are pasted partially or completely on top of one another, you can use the **Layout Map** command (see page 12-19) to rearrange them.



*Cutting and pasting multiple nodes will not preserve manually-created links between the nodes. Links that are automatically discovered will be recreated after the nodes are pasted, but links that were created manually must be recreated manually.*



*If an L2 cloud node was among those you selected to cut, it will not necessarily be pasted with the other nodes. It will be placed automatically on a submap, if necessary, as determined by EPICenter.*

## Deleting Nodes from the Map

You can delete selected device, decorative, or text nodes from the map, as opposed to cutting them for later pasting.

- You can delete a submap node as long as it is empty
- You cannot delete hyper nodes. A hyper node is deleted automatically when the actual node it represents is deleted
- L2 cloud nodes are deleted when they are no longer needed. You can also delete them manually

To delete one or more nodes, do the following:

- 1 Select the nodes you want to delete. You can select multiple nodes by using Shift-click (hold down the shift key and click the cursor on the node you want to select).
- 2 Select **Delete Map Nodes** from the **Edit** menu to delete the node or nodes.



*You will NOT be asked to confirm that you want to delete the nodes. If you delete nodes accidentally, you will need to add them again to the map.*

## Deleting Links from the Map

You can remove one or more links from the map using the **Delete Map Links** command.

To delete one or more links, do the following:

- 1 Select the links you want to delete. You can select multiple links by using Shift-click (hold down the shift key and click the cursor on the link you want to select).
- 2 Select **Delete Map Links** from the **Edit** menu to delete the link or links. You will be asked to confirm that you want to delete these links.



*Active links that were created automatically by EPICenter will be recreated automatically on the next polling cycle as long as the endpoints they linked are still present on the map. The only links that can be permanently deleted are manually-created links or links that cease to exist.*



*Links that have been deleted cannot be pasted. Manual links must be recreated manually.*

## Selecting All Nodes in a Map

You can select all the nodes in a map by doing one of the following:

- Select **Select All Map Nodes** from the **Edit** menu
- Enter [Alt]+A from the keyboard



*To move a multiple-node selection as a group, hold down the shift key while dragging to preserve the multiple-node selection.*

## Map Viewing Functions

ExtremeWare EPICenter's Topology applet provides a number of ways to view and manipulate the layout of a topology map.

The size and layout of map nodes is saved at every map operation (except for the map zoom level).

### Map Layout

You can drag map nodes around on the map yourself, or you can have EPICenter lay out the map nodes for you. To have ExtremeWare EPICenter do the map layout, do one of the following:

- Select **Layout Map** from the **Map** menu

- Click the "Layout" icon on the icon bar 

- Click with the right mouse button on the map background to display the pop-up menu, then select **Layout Map**
- Enter [Alt]+L from the keyboard

You can use the **Expand Map** and **Compress Map** commands to increase the space between nodes in the map. You can also move map nodes by selecting them and dragging them to the location where you want them placed.

## Expanding the Map

The Expand Map function increases the length of the links between map nodes without changing the size of the nodes. To expand the current map, do one of the following:

- Select **Expand Map** from the **Map** menu
- Enter [Alt]+E from the keyboard

Because this command affects map links, nodes that do not have links are not moved.

## Compressing the Map

The Compress Map function decreases the length of the links between map nodes without changing the size of the nodes. To compress the current map, do one of the following:

- Select **Compress Map** from the **Map** menu
- Enter [Alt]+S from the keyboard

Because this command affects map links, nodes that do not have links are not moved.

## Inflating the Map Nodes

The Inflate Nodes function increases the size of some or all of the nodes on the current map, without changing the spacing between the nodes.

By default (if you do not select any specific nodes) the command will inflate all nodes on the current map. If you select one or more nodes, the command will inflate just the nodes you've selected. You can select multiple nodes by using Shift-click (hold down the shift key and click the cursor on the node you want to select).

To inflate the selected nodes, do one of the following:

- Select **Inflate Nodes** from the **Map** menu
- Enter [Alt]+I from the keyboard



## Deflating the Map Nodes

The Deflate Nodes function decreases the size of some or all of the nodes on the current map, without changing the spacing between the nodes.


By default (if you do not select any specific nodes) the command will deflate all nodes on the current map. If you select one or more nodes, the command will deflate just the nodes you've selected. You can select multiple nodes by using Shift-click (hold down the shift key and click the cursor on the node you want to select).

To deflate the selected nodes, do one of the following:

- Select **Deflate Nodes** from the **Map** menu
- Enter [Alt]+D from the keyboard

## Zooming In


The **Zoom In** function expands the entire map, both the size of the nodes as well as the spacing between them. To zoom in the current map, do one of the following:

- Select **Zoom Map In** from the **Map** menu
- Click the “Zoom map in” icon on the icon bar 
- Enter [Alt] and the [Plus] from the numeric keypad on the keyboard

Unlike the other map manipulation commands, the zoom level is not saved with the map.

## Zooming Out

The Zoom Out function shrinks the entire map, both the size of the nodes as well as the spacing between them. To Zoom Out the current map, do one of the following:

- Select **Zoom Map Out** from the **Map** menu
- Click the “Zoom map out” icon on the icon bar 
- Enter [Alt] plus the [Minus] from the numeric keypad on the keyboard

Unlike the other map manipulation commands, the zoom level is not saved with the map.

## Unzooming the Map

The Unzoom Map function restores the map to the size it was prior to any Zoom In or Zoom Out actions. To “unzoom” the map, do one of the following:

- Select **Unzoom Map** from the **Map** menu
- Enter [Alt]+R from the keyboard

## Undoing Your Map Edits


You can undo your last ten map layout and sizing actions one by one using the **Undo Map Edit** function. Each **Undo Map Edit** action undoes your previous editing action. To undo the most recent edit, do one of the following:

- Select **Undo Map Edit** from the **Map** menu
- Enter [Alt]+U from the keyboard

This command does *not* undo delete, cut or paste of map elements. It stores only the last ten map layout and sizing actions.

## Printing a Map

You can print the current map using the Print Map function. To print a map, display the map you want to print and then do one of the following:

- Select **Print Map** from the **Map** menu
- Click the “Print map” icon on the icon bar 
- Enter [Alt]+P from the keyboard

Printing a large map can be very memory-intensive, and can take a significant amount of time.

## Finding a Map Node

If your map has a large number of nodes, it may be difficult to quickly find a specific node you’re interested in seeing. The Find Map Node function lets you select a node from the list of all nodes in the current view, and will then find and “select” that node.

To find a node, do one of the following:

- Select **Find Map Node...** from the **Map** menu
- Click with the right mouse button on the map background to display the pop-up menu, then select **Find Map Node...**
- Enter [Alt]-F from the keyboard

You are presented with a list of all the nodes in the current view (see Figure 12-12). The list includes the name of the node, the IP address, the node type, and the map where it can be found.



The screenshot shows a window titled "Find Map Node" with a sub-header "Map Nodes". Below the header is a table with four columns: "Node Name", "IP Address", "Node Type", and "Parent Map". The table contains 18 rows of data. At the bottom of the window are four buttons: "Find", "Refresh", "Close", and "Help".

Node Name	IP Address	Node Type	Parent Map
10.205.0.0/16		SubMap Node	Root Map
10.205.0.0/24		SubMap Node	Root Map
5411	10.205.0.37	Device	10.205.0.0/16
5422	10.205.0.145	Device	10.205.0.0/24
ciscotest	10.205.0.50	Device	Root Map
CoreBuilder-4790...	10.205.0.182	Device	Root Map
hn	10.205.0.68	Hyper Node	10.205.0.0/24
hn	10.205.0.30	Hyper Node	10.205.0.0/24
hn	10.205.0.156	Hyper Node	10.205.0.0/24
L2C		L2 Cloud	10.205.0.0/24
LabA-2	10.205.0.38	Device	Root Map
Summit24e2	10.205.0.149	Device	Root Map
Summit24e3	10.205.0.68	Device	Root Map
Summit24e3	10.205.0.30	Device	Root Map
Summit3	10.205.0.156	Device	Root Map
Summit48i	10.205.0.41	Device	10.205.0.0/24
Summit5ITx	10.205.0.170	Device	10.205.0.0/24
Switch 1100	10.205.0.181	Device	Root Map

**Figure 12-12:** Finding a node in the current view

- ◆ To find a node, select the node and click the **Find** button.

This will display the appropriate submap, if necessary, and highlight the node you have selected.

The **Find Map Node** window will continue to be displayed until you dismiss it with the **Close** button. You can move around among different maps and views while the **Find Map Node** window is displayed.

If you change views while the **Find Map Node** window is displayed, the list of devices will no longer be correct. To update the list to reflect the current view, click the **Refresh** button.

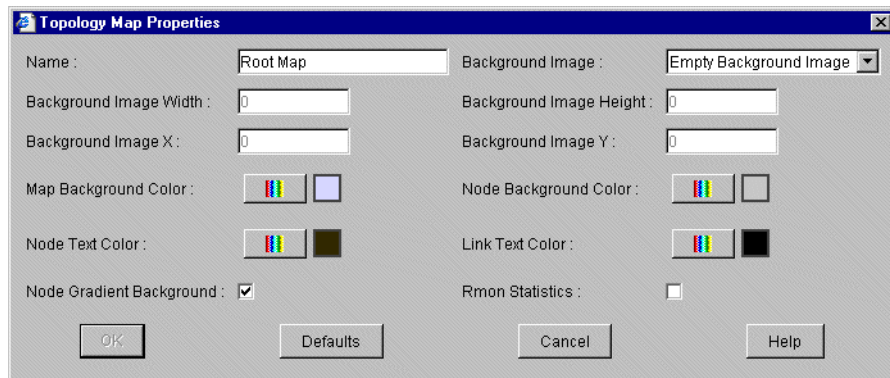
## Setting Map Properties

There are a number of properties you can set for the current map, such as the background color or image, node background color and style, node and link text color, and whether RMON statistics should be enabled for the devices on this map.

To display the Map Properties window, do one of the following:

- Select **Map Properties...** from the **Map** menu
- Click with the right mouse button on the map background to display the pop-up menu, then select **Map Properties...**

The Topology Map Properties window will appear, as shown in Figure 12-12.



**Figure 12-13:** Setting Map Properties for the current map

In this window you can do the following:

- To change the name of the map, modify the name in the **Name** field
- To select a background image for the map, select the image you want from the drop-down list in the **Background Image** field
- To change the height and width (in pixels) for the background image, enter the number of pixels in the **Background Image Width** or **Background Image Height** field
- To select the coordinates (in pixels) where the upper left hand corner of the background image should be placed, enter the number of pixels in the **Background Image X** or **Background Image Y** field
- To change the map background color, click the color bar icon labeled **Map Background Color**. This displays a color selection window where you can select the color you want. You can select a color using color swatches, or by specifying HSB or RGB values. The current color is displayed in the small box to the right of the color bar icon.
- To change the node background color, click the color bar icon labeled **Node Background Color**. This displays a color selection window where you can select the color you want. You can select a color using color swatches, or by specifying HSB or

RGB values. The current color is displayed in the small box to the right of the color bar icon.

- To set the color used to label nodes, click the color bar icon labeled **Node Text Color**. This displays a color selection window where you can select a color by using color swatches, or by specifying HSB or RGB values. The current color is displayed in the small box to the right of the color bar icon.
- To set the color of the text used to label links, click the color bar icon labeled **Link Text Color**. This displays a color selection window where you can select a color using color swatches, or by specifying HSB or RGB values. The current color is displayed in the small box to the right of the color bar icon. The default is black.
- To use a gradient node background color (the color is shaded from light to dark to light), click the checkbox labeled **Node Gradient Background**. To turn the gradient off, so that the node background will be a uniform solid color, click in the checkbox to remove the check mark. The default is to use a gradient background.
- To select whether RMON statistics should be enabled for this map, click the checkbox labeled **Rmon Statistics**. When RMON statistics are on for a map, the percent utilization will be displayed for links.

RMON statistics can be enabled separately for each map in the view. The default is to have RMON statistics disabled for the map.



*It is possible to disable RMON statistics for the Topology applet as a whole, so that the Rmon Statistics checkbox will not have any effect. This is done setting RMON properties on the Server Properties page of the Administration applet.*

## Adding Map Background Images

You can add images of your own to use as background images for topology maps by placing them in the `BackgroundImages` directory in the EPICenter server installation.

Both `.gif` and `.jpg` image types are supported.

Background images are kept in the directory

`<epicenter_install_dir>\extreme\gifs\topology.BackgroundImages`

where `<epicenter_install_dir>` is the root directory of your EPICenter server

installation (by default `epc3_0\extreme\gifs\topology.BackgroundImages` in the Windows operating environment, or

`/opt/epc_30/extreme/gifs/topology.BackgroundImages` on a Solaris system).

## Device Information Views

You can view a variety of information about the devices represented by the nodes on the map. By selecting a function from the Tools menu, or from the Device pop-up menu, you can invoke displays of information kept by ExtremeWare EPICenter for the selected device.

All these views can be run either by selecting the command from the Topology Tools menu, or by right-clicking on a Device map node to bring up the Device node pop-up menu.

### Device Alarms

The Device Alarms function runs the ExtremeWare EPICenter Alarm System and displays the Alarm Browser function to show the alarms for the selected device.

To view the Device Alarms display for a selected node, select the node and do one of the following:

- Select **Device Alarms...** from the **Tools** menu
- Click with the right mouse button on the Device map node, then select **Device Alarms...** from the pop-up menu that appears

This starts the Alarm System applet in a new browser window. The Alarm System displays the Alarm Log Browser and displays the alarms for the device associated with the selected Device map node.

See Chapter 5, “The EPICenter Alarm System” for details on using this feature.

### Device Browse

The Device Browse function runs the ExtremeWare Vista switch management interface for the selected device.

To run ExtremeWare Vista for a selected node, select the node and do one of the following:

- Select **Device Browse...** from the **Tools** menu
- Click with the right mouse button on the Device map node, then select **Device Browse...** from the pop-up menu that appears

This starts the ExtremeWare Vista login page in a new browser window.

Refer to the *ExtremeWare Software User Guide* for details on using ExtremeWare Vista.

## Device Statistics

The Device Statistics function runs the ExtremeWare EPICenter Real-Time Statistics applet, and displays port statistics for the selected device.

To view the Device Statistics display for a selected node, select the node and do one of the following:

- Select **Device Statistics...** from the **Tools** menu
- Click with the right mouse button on the Device map node, then select **Device Statistics...** from the pop-up menu that appears

This starts the Real-Time Statistics applet in a new browser window, and displays port statistics for the device associated with the selected Device map node.

See Chapter 11, “Real-Time Statistics” for details on using this feature.

## Device Telnet

The Device Telnet function opens an EPICenter telnet window that is connected to the selected device.

To open a telnet session for a selected device, select the appropriate device node and do one of the following:

- Select **Device Telnet...** from the **Tools** menu
- Click with the right mouse button on the Device map node, then select **Device Telnet...** from the pop-up menu that appears

This starts a telnet session for the device in a new browser window.

See Chapter 10, “Using ExtremeView” for details on using this feature.

## Device View

The Device View function runs the ExtremeWare EPICenter ExtremeView applet, and displays the device front-panel image and device information for the selected device.

To view the Device View for a selected node, select the node and do one of the following:

- Select **Device View...** from the **Tools** menu
- Click with the right mouse button on the Device map node, then select **Device View...** from the pop-up menu that appears

This starts the ExtremeView applet in a new browser window and displays the front-panel image and information for the device associated with the selected Device map node.

See Chapter 10, “Using ExtremeView” for details on using this feature.



# 13

## Using the VLAN Manager

---

This chapter describes how to use the VLAN Manager for:

- Viewing enterprise-wide, tagged and untagged VLAN information for Extreme (Summit and BlackDiamond) switches managed by the EPICenter software
- Adding new tagged or untagged VLANs to Extreme devices, adding ports to those VLANs, and modifying IP addresses
- Deleting VLANs
- Modifying VLANs
- Adding and deleting protocol filters

### Overview of Virtual LANs

A Virtual LAN is a group of location- and topology-independent devices that communicate as if they were on the same physical local area network (LAN). Extreme Networks switches have a VLAN feature that enables you to construct broadcast domains without being restricted by physical connections.

The VLAN Manager creates and manages VLAN for Extreme Networks devices only. It does not handle other third-party devices, even though third-party devices can be managed through the Inventory Manager.

If you run the EPICenter client with Administrator or Manager access, you can:

- Create and delete VLANs
- Add or remove ports from existing VLANs
- Modify a VLAN's IP address
- Enable/disable IP Forwarding
- Create and modify the protocol filters used to filter VLAN traffic

Extreme Networks switches support a maximum of 3000 VLANs. VLANs on Extreme Networks switches can be created according to the following criteria:

- Physical port
- 802.1Q tag
- Protocol sensitivity using Ethernet, LLC SAP, or LLC/SNAP Ethernet protocol filters
- A combination of these criteria

In the EPICenter system, a VLAN is defined uniquely by the following:

- Name
- 802.1Q tag (if defined)
- Protocol filters applied to the VLAN

As a result, multiple switches are shown as members of the same VLAN whenever all the above are the same.

For a more detailed explanation of VLANs, see the *ExtremeWare Software User Guide*.

## Displaying a VLAN

When you click the VLAN icon in the EPICenter Navigation Toolbar, the VLAN Manager window is displayed, as shown in Figure 13-1.

The screenshot shows the 'VLAN Manager' applet in a Microsoft Internet Explorer browser window. The address bar shows 'http://localhost/everest'. The interface is divided into a left sidebar with navigation icons (Home, Inventory, Alarm, Config, Telnet, Groups, Find IP/MAC, EView, RT Stats, Topology, VLAN, ESRP, Admin, Reports, Policy, Logoff) and a main content area. The main area has a 'By VLAN' radio button selected and a 'By Switch' radio button. Below these are icons for 'Add', 'Delete', 'Modify', 'Filters', and 'Help'. The 'VLANs' tree on the left shows a hierarchy starting with 'Default', containing several switches like 'Summit3', 'Summit24e3', 'LabA-2', etc. The table on the right, titled 'All VLANs', displays the following data:

Name	Tag	Protocol
Default	1	ANY
MacVlanDiscover	Untagged	ANY
Mgmt	4094	ANY
Mgmt	Untagged	ANY
temp1	333	ANY
mo-vlan1	Untagged	ANY
smartrap-vlan2	Untagged	ANY
e3-vlan5	Untagged	ANY
smartrap-vlan	Untagged	ANY
e3_vlan4	Untagged	ANY
e3-vlan3	3457	ANY
e3-vlan2	Untagged	ANY
es-vlan9	Untagged	ANY
vlan	Untagged	ANY
e3-vlan6	Untagged	ANY
t1	Untagged	ANY
e3-tag	3434	test
e3-tag-vlan2	Untagged	ANY

**Figure 13-1:** VLAN Manager applet, showing devices organized by VLAN

The VLANs currently known to the EPICenter database are displayed in the Component Tree on the left. The panel on the right shows summary information about each VLAN. Note that in the example shown in Figure 13-1, there are two VLANs with the same name, but differing in the protocol filters applied.



*You must add switches to the EPICenter database through Discovery or by using the Add function in the Inventory Manager. Until you add a switch to the database, you cannot create any VLANs on that switch.*

Information about VLAN configurations is obtained when a switch is added to the database.

The VLAN Manager can display information either by VLAN (showing all the switches with ports that are members of a specific VLAN) or by switch (showing the VLANs that have members on a specific switch).

- Select the **By VLAN** button to display VLANs at the first level of the Component Tree. Listed under each VLAN is every switch that has the VLAN defined on it (see Figure 13-1).

Select an individual VLAN to view a summary of the configuration of the switches and ports that are members of that VLAN.

- Select the **By Switch** button to display switches at the first level of the Component Tree. Listed under each switch is every VLAN that is defined on the switch, as shown in Figure 13-2.

The screenshot shows the Extreme Networks EPICenter interface in a Microsoft Internet Explorer browser window. The address bar shows <http://localhost/everest>. The main window is titled "VLAN Manager" and has two radio buttons: "By VLAN" (unselected) and "By Switch" (selected). Below these are buttons for "Add", "Delete", "Modify", "Filters", and "Help".

The left sidebar contains a tree view of the network topology. Under "Switches", "Summit24e3" is selected and highlighted in red. The tree shows a hierarchy: LabA-2 > Summit51Tx > MacVlanDisc > Mgmt > Default > Summit3 > Summit24e3 > Summit48i > Summit24e3 > MacVlanDisc > vlan > t1 > e3-tag-vlan2 > Default > es-vlan9 > e3-vlan6 > e3-tag.

The main area displays a table titled "All VLANs on Switch 'Summit24e3'". The table has the following columns: Name, Tag, Protocol, VLAN IP Addr, VLAN IP Mask, and Ports.

Name	Tag	Protocol	VLAN IP Addr	VLAN IP Mask	Ports
MacVlanDiscover	Untagged	ANY			
vlan	Untagged	ANY			
t1	Untagged	ANY			
e3-tag-vlan2	Untagged	ANY			
Default	1	ANY	10.205.0.68	255.255.255.0	Untagged: 1-9
es-vlan9	Untagged	ANY			
e3-vlan6	Untagged	ANY			
e3-tag	3434	test	11.22.33.44	255.255.255.0	Untagged: 23-24

The status bar at the bottom indicates "Applet started." and "Local intranet".

**Figure 13-2:** VLAN topology shown by switch

You can display details about the component ports of a VLAN by selecting the VLAN or switch in the tree on the left. The panel on the right displays detailed information about the selected component, as shown in Figure 13-3 and Figure 13-4.

Figure 13-3 presents details about the ports in a VLAN on the selected switch.

The screenshot shows the Extreme Networks EPICenter web interface in a Microsoft Internet Explorer browser window. The address bar shows `http://localhost/everest`. The main content area is titled "VLAN Manager" and displays a tree view on the left and a table of member ports on the right.

The tree view on the left shows a hierarchy of VLANs under "Default". The selected switch is "Summit48i".

The table of member ports is titled "Member Ports in Switch 'Summit48i' for VLAN 'Default'". It has the following columns: #, Type, Speed, Duplex, State, Status, and Tagging.

#	Type	Speed	Duplex	State	Status	Tagging
1				Enable	Ready	Untagged
2				Enable	Ready	Untagged
3				Enable	Ready	Untagged
4				Enable	Ready	Untagged
5				Enable	Ready	Untagged
6				Enable	Ready	Untagged
7				Enable	Ready	Untagged
8				Enable	Ready	Untagged
9		100	Full	Enable	Active	Untagged
10				Enable	Ready	Untagged
11				Enable	Ready	Untagged
12				Enable	Ready	Untagged
13				Enable	Ready	Untagged
14				Enable	Ready	Untagged
15				Enable	Ready	Untagged
16				Enable	Ready	Untagged
17				Enable	Ready	Untagged
18				Enable	Ready	Untagged
19				Enable	Ready	Untagged
20				Enable	Ready	Untagged
21				Enable	Ready	Untagged
22				Enable	Ready	Untagged

Below the table, the following information is displayed:

```

On Summit "Summit48i", VLAN "Default" has:
802.1Q Tag: 1   IP: 10.205.0.41/255.255.255.0
Protocol: ANY
  
```

Figure 13-3: VLAN member ports on a selected switch

Figure 13-4 presents details about the ports on a given switch that are found in the selected VLAN.

The screenshot shows the Extreme Networks EPICenter web interface. The browser address bar shows `http://localhost/everest`. The main content area is titled "VLAN Manager" and has two radio buttons: "By VLAN" (selected) and "By Switch". Below these are buttons for "Add", "Delete", "Modify", "Filters", and "Help".

The left sidebar contains a tree view of the network hierarchy. Under "Switches", "Summit481" is selected, and its "Default" VLAN is highlighted.

The main area displays a table titled "Member Ports in VLAN 'Default' on Switch 'Summit481'":

#	Type	Speed	Duplex	State	Status	Tagging
1				Enable	Ready	Untagged
2				Enable	Ready	Untagged
3				Enable	Ready	Untagged
4				Enable	Ready	Untagged
5				Enable	Ready	Untagged
6				Enable	Ready	Untagged
7				Enable	Ready	Untagged
8				Enable	Ready	Untagged
9		100	Full	Enable	Active	Untagged
10				Enable	Ready	Untagged
11				Enable	Ready	Untagged
12				Enable	Ready	Untagged
13				Enable	Ready	Untagged
14				Enable	Ready	Untagged
15				Enable	Ready	Untagged
16				Enable	Ready	Untagged
17				Enable	Ready	Untagged
18				Enable	Ready	Untagged
19				Enable	Ready	Untagged
20				Enable	Ready	Untagged
21				Enable	Ready	Untagged
22				Enable	Ready	Untagged

Below the table, it states: "On Summit 'Summit481', VLAN 'Default' has: 802.1Q Tag: 1 IP: 10.205.0.41/255.255.255.0 Protocol: ANY".

Figure 13-4: Switch member ports for a selected VLAN

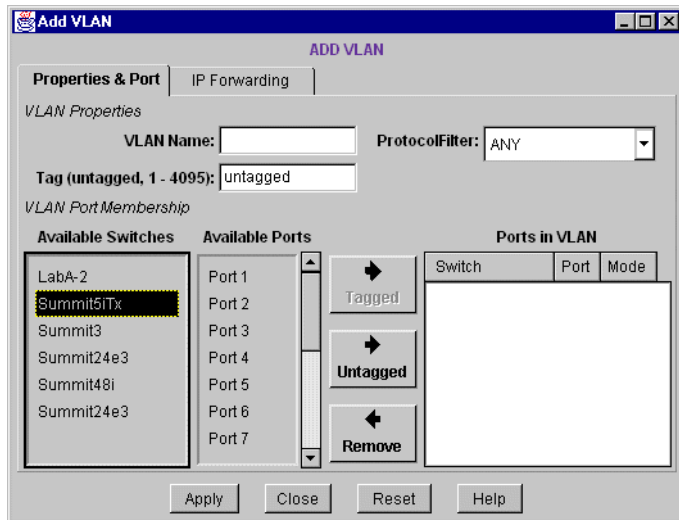
## Adding a VLAN

Users with Administrator or Manager access can create VLANs on the Extreme Networks switches managed by the EPICenter software. If you have Monitor access only, you can not use this function.

To add a new VLAN, do the following:

- 1 Click the **Add** button in the VLAN Manager panel.

The Add VLAN dialog box, Properties & Ports page is displayed, as shown in Figure 13-5.



**Figure 13-5:** Add VLAN dialog, Properties and Ports page

- 2 Enter a descriptive name for the VLAN. The name must begin with a letter followed by up to 31 characters. See the *ExtremeWare Software User Guide* for details on VLAN naming.
- 3 Select an entry from the pull-down **Protocol Filter** list. This selection determines what protocol (if any) is used to determine membership in this VLAN. If you do not want to specify a protocol, select **ANY**. This means the filtering rules will match all unfiltered protocols.
- 4 If the VLAN is to be tagged, enter a 802.1Q tag value in the **Tag** field. The tag value can be a number between 2 and 4095. By entering a tag number, you enable tagging for this VLAN. Enter the text “untagged” or 0 (zero) to indicate that the VLAN is to be untagged.
- 5 To add a port to the VLAN, first select the switch from the **Available Switches** list. This displays a list of ports on the switch that are available to be included in the VLAN.



*The **Available Ports** list does not include ports in SummitLink™ mode, or ports configured as slave load sharing ports.*

- 6 Select one or more ports from the **Available Ports** list.
- 7 Click **Tagged** to add the port as a tagged port. Click **Untagged** to add the port as an untagged port.



*If this is an untagged VLAN, you are not able to add a tagged port.*

When you add an untagged port to a VLAN, it is automatically removed from any other VLAN which uses the same protocol as the new VLAN, and where the port is an untagged member.

You can add a switch to a VLAN as a unit—just select the switch without selecting any ports, and click **Tagged** or **Untagged** to add the switch to the VLAN.

- 8 To remove a port from the VLAN, select the port from the Ports in VLAN list, and then click **Remove**.
- 9 When you have finished adding ports to the VLAN, click **Apply** to implement the changes.

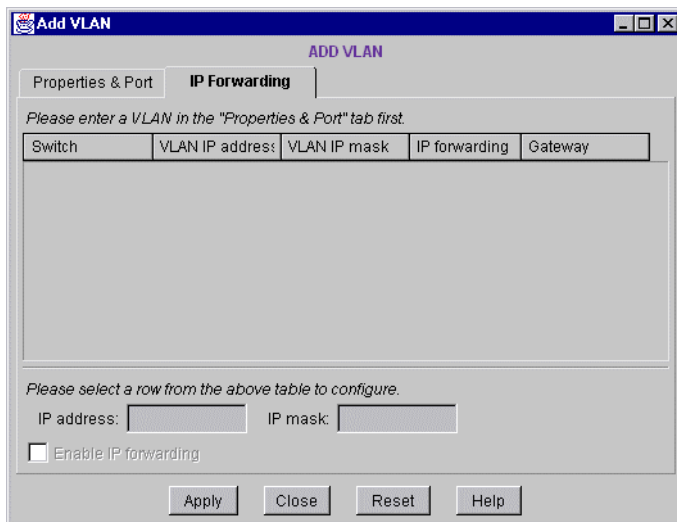
The VLAN is created on the switches whose ports are members of the new VLAN.

Once you have added a VLAN, you can specify an IP address and mask for the VLAN on each switch, and also enable or disable IP Forwarding.

- 1 Select the **IP Forwarding** tab at the top of the Add VLAN window.

The IP Forwarding page is displayed, as shown in Figure 13-6.





**Figure 13-6:** Add VLAN dialog, IP Forwarding page

- 2 Select a switch from the table of switches.
- 3 Enter an IP address and IP mask. Click the Enable IP Forwarding check box if you want to enable IP forwarding for this VLAN on the switch.
- 4 Click **Apply** to implement the changes.
- 5 Click **Close** to exit the window.

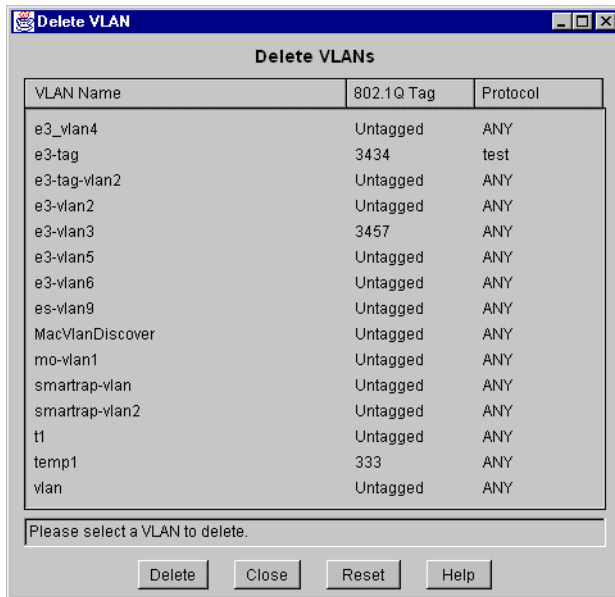
## Deleting a VLAN

Users with Administrator or Manager access can delete VLANs from Extreme Networks switches managed by the EPICenter software. If you have only Monitor access, you cannot use this function.

To delete a VLAN, follow these steps:

- 1 Click the **Delete** button in the VLAN Manager panel.

The Delete VLAN dialog is displayed, as shown in Figure 13-7.



**Figure 13-7:** The Delete VLAN page

- 2 Select the VLAN you want to delete.
- 3 Click **Delete**.

The VLAN is deleted from all the switches on which it exists.

- 4 Click **Close** to exit the window.

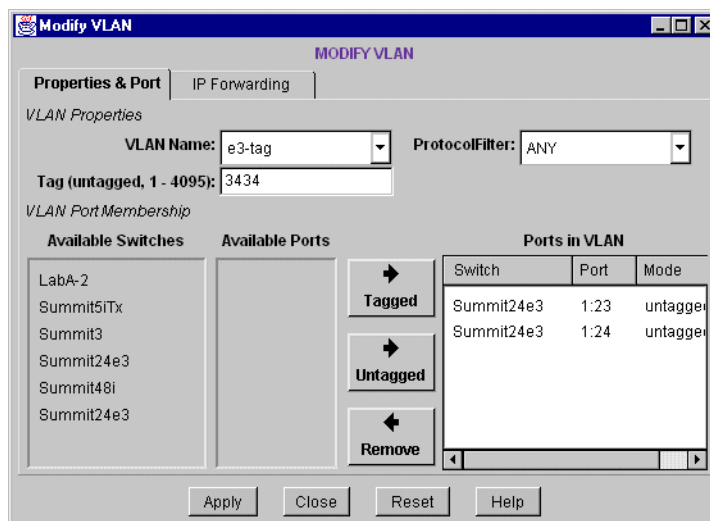
## Modifying a VLAN

Users with Administrator or Manager access can modify the properties of a VLAN, and add and remove ports from the VLAN. If you have only Monitor access, you can not use this function.

To modify a VLAN, follow these steps:

- 1 Click the **Modify** button in the VLAN Manager panel.

The Modify VLAN dialog, Properties & Ports page is displayed, as shown in Figure 13-8.



**Figure 13-8:** The Modify VLAN dialog, Properties and Ports page

- 2 Select a VLAN from the drop-down list in the **VLAN Name** field.

The current values for the VLAN are displayed.



*The **Ports in VLAN** list does not display SummitLink ports, because you cannot modify them.*

- 3 To change the Protocol Filter selection, select a different entry from the pull-down **Protocol Filter** list.
- 4 To change the VLAN tag, type a new value into the **Tag** field.  
To disable tagging for the VLAN, type “untagged” or 0 (zero) into the **Tag** field.
- 5 To remove a port from the VLAN, select the port in the **Ports in VLAN** list, and click **Remove**.
- 6 To add a port to the VLAN, first select the switch from the **Available Switches** list. This displays a list of ports on the switch that are available to be included in the VLAN.



*The **Available Ports** list does not include ports in SummitLink mode, or ports configured as slave load sharing ports.*

- 7 Select a port from the **Available Ports** list.

- 8 Click **Tagged** to add the port as a tagged port. Click **Untagged** to add the port as an untagged port.



*If this is an untagged VLAN, you cannot add a port as a tagged port.*

If a port is added as an untagged port, it is automatically removed from any other VLAN which uses the same protocol as the new VLAN, and where the port is an untagged member.

You can add a switch to a VLAN as a unit—just select the switch without selecting any ports, and click **Tagged** or **Untagged** to add the switch to the VLAN.

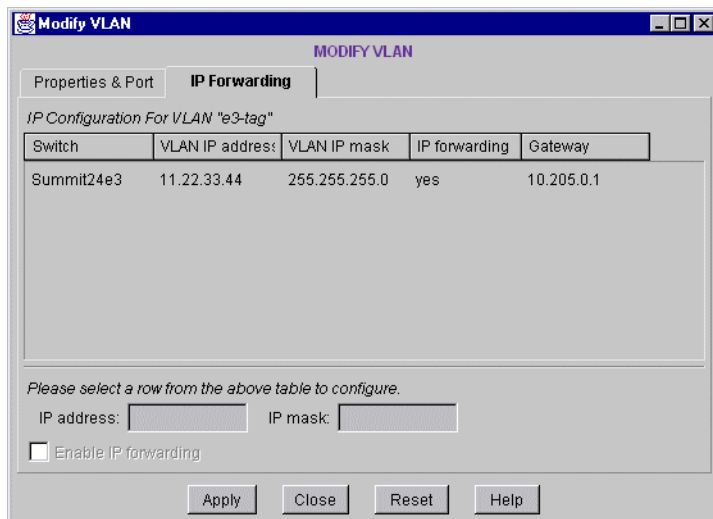
- 9 When you have finished adding and removing ports, click **Apply** to implement the changes.

If all ports of a switch are removed from the VLAN, the VLAN is deleted from that switch.

If a port on a new switch is added to the VLAN, then the VLAN is created on that switch.

- 10 To modify the IP address and mask for a VLAN on a switch, and to enable or disable IP Forwarding, select the **IP Forwarding** tab at the top of the Add VLAN window.

The IP Forwarding page is displayed, as shown in Figure 13-6.



**Figure 13-9:** The Modify VLAN dialog, IP Forwarding page

- 11 Select a switch from the table of switches.

- 12 Change the IP address and IP mask as appropriate. Click the Enable IP forwarding check box to enable or disable IP forwarding for this VLAN on the switch.
- 13 Click **Apply** to implement the changes.
- 14 Click **Close** to exit the window.

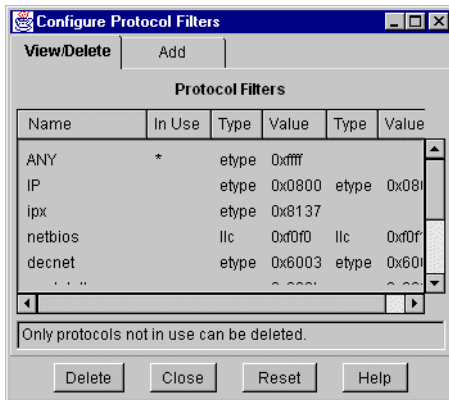
## Adding and Deleting Protocol Filters

Users with Administrator or Manager access can view, add, and delete protocol filter definitions. If you have Monitor access, you can view filter definitions, but not add or delete them.

To view, delete, or add protocol filter definitions, do the following:

- 1 Click **Protocol Filters** in the VLAN Manager.

The View/Delete page of the Protocol Panel dialog box is displayed, as shown in Figure 13-10.



**Figure 13-10:** Protocol Panel dialog box, View/Delete page

This page shows all the protocol filters configured within the EPICenter database. Any filters that are in use by a VLAN are indicated with an asterisk (\*) in the In Use column.

- 2 To delete a protocol filter, select a filter in the list, and click **Delete**.

This deletes the protocol filter from all Extreme Networks switches managed by the EPICenter software, as well as from the EPICenter database.



*If a filter is in use by a VLAN, you cannot delete it.*

- 3 Click **Close** to exit the window.

To add a protocol filter, follow these steps:

- 1 Click the **Add** tab at the top of the Protocol Panel dialog box to display the Add Protocol page, as shown in Figure 13-11.

ADD Protocol	
Protocol Name: <input type="text"/>	
Protocol Definition:	
type	value
<input type="text"/>	0x <input type="text"/>
<input type="text"/>	0x <input type="text"/>
<input type="text"/>	0x <input type="text"/>
<input type="text"/>	0x <input type="text"/>
<input type="text"/>	0x <input type="text"/>
<input type="text"/>	0x <input type="text"/>

**Figure 13-11:** Protocol Panel dialog box, Add Protocol page

- 2 Enter a descriptive name for the Protocol. The name must begin with a letter followed by up to 31 characters. See the *ExtremeWare Software User Guide* for details on naming.
- 3 Select a protocol type from the pull-down list in the **type** column.
- 4 Type a corresponding four-digit hexadecimal filter value in the **value** field.
- 5 Repeat steps 3 and 4 to enter up to six type-value pairs.
- 6 When you have finished entering the definition, click **Add** to add the new protocol filter to the EPICenter database.



*The protocol filter is now available to be used on any switch, but is not created on any switches at this time. The protocol filter is created on a switch only when you create or modify a VLAN to use the new protocol filter on that switch. The database acts as a collective store for network data without needing to replicate it on every switch.*

- 7 Click **Close** to exit the window.

# 14

## The ESRP Manager

---

This chapter describes how to use the ExtremeWare EPICenter ESRP Manager applet for:

- Viewing the status of ESRP-enabled VLANs and the ESRP-enabled switches in those VLANs

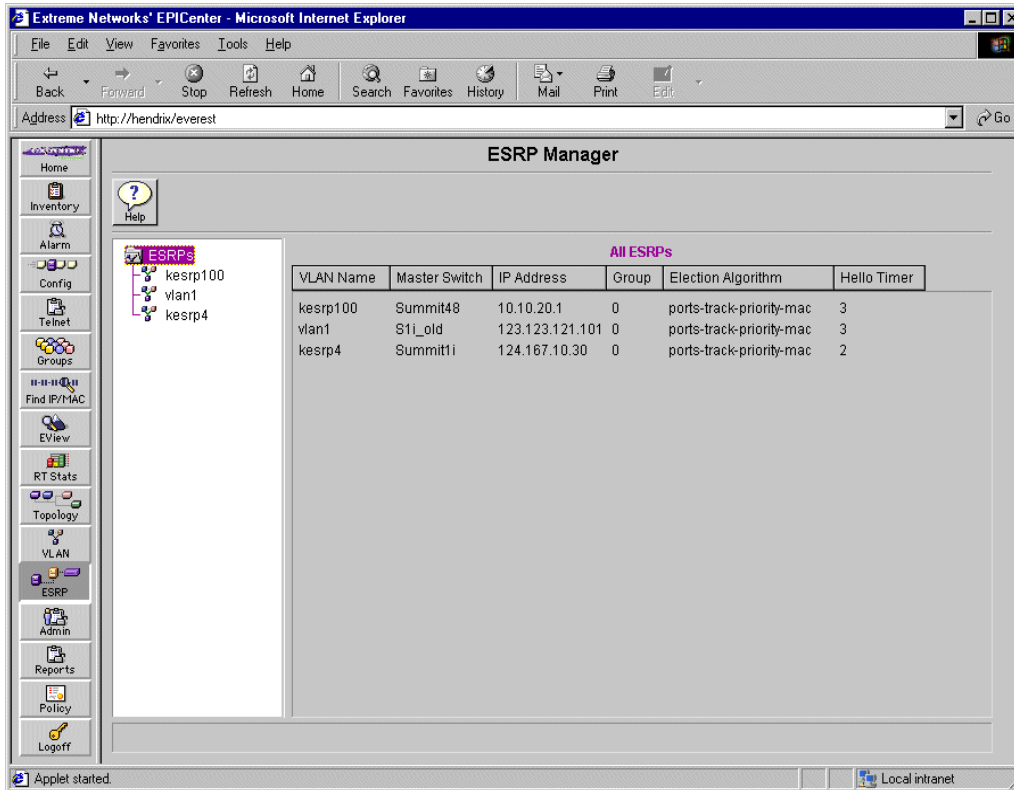
### Overview of the ESRP Manager

The Extreme Standby Router Protocol (ESRP) is a feature of ExtremeWare that allows multiple switches to provide redundant layer 3 routing services, as well as layer 2 redundancy, to users. The ESRP Manager displays the status of ESRP-enabled VLANs and the ESRP-enabled switches in those VLANs. You can view a summary status for all the ESRP-enabled VLANs being monitored by EPICenter. You can also view detailed information for an individual ESRP-enabled VLAN and the switches in those VLANs.



*This chapter does not discuss ESRP functionality in any detail. For more information about ESRP, see the ExtremeWare Software User Guide, versions 6.0 or later.*

To start the ESRP Manager applet, click the **ESRP** button in the ExtremeWare EPICenter Navigation Toolbar. The ESRP Manager applet appears, initially displaying a summary status of the ESRP-enabled VLANs known to EPICenter, as shown in Figure 14-1.



**Figure 14-1:** ESRP Manager showing summary ESRP-enabled VLAN status

This display shows a summary of the ESRP configuration for each ESRP-enabled VLAN.

The information displayed is as follows:

- **Name:** The name of the ESRP-enabled VLAN
- **Master Switch:** The name, if known, or MAC address of the switch currently designated as the Master switch. If this switch is being managed by EPICenter (is included in EPICenter's Inventory database) the name will appear. If the switch is not known to EPICenter, the MAC address will appear.
- **IP Address:** The IP address of the ESRP-enabled VLAN. If the master switch is not known to EPICenter, this will be "N/A."



- **Group:** The ESRP group to which this ESRP-enabled VLAN belongs, in a broadcast domain that contains multiple instances of ESRP (multiple ESRP groups). The names of the ESRP-enabled VLANs participating in the same group must be identical.
- **Election Algorithm:** The ESRP election algorithm in use for this VLAN. The election algorithm determines the order of precedence of the election factors used to determine the ESRP Master. The election factors are:
  - Ports: the number of active ports (the switch with the highest number takes priority)
  - Track: whether the switch is using ESRP tracking (a switch using tracking has priority)
  - Priority: a user-defined priority number between 0 and 254 (a higher number has higher priority)
  - MAC: the switch MAC address (a higher-number address has priority)

The election algorithm can be one of the following:

- `ports_track_priority_mac` (the default): This algorithm considers active ports first, then tracking, then priority, then the MAC address to determine the ESRP Master. This is the only algorithm supported for ExtremeWare releases prior to version 6.0
- `track_ports_priority_mac`
- `priority_ports_track_mac`
- `priority_track_ports_mac`
- `priority_mac_only`: only considers priority and the MAC address

See the *ExtremeWare Software User Guide*, version 6.1, for details.



*The ESRP election algorithm must be identical on all switches in an ESRP group. If it is not, serious problems may arise.*

- **Hello Timer:** This is the interval, in seconds, for exchanging keep-alive packets between the ESRP switches for this ESRP-enabled VLAN. Also known as the ESRP timer. The default is 2 seconds.

## Viewing ESRP Detail Information

You can display detailed ESRP information for the switches in an individual ESRP-enabled VLAN by clicking on the VLAN name in the Component Tree in the left-hand panel of the window. This displays a status window similar to the one shown in Figure 14-2.

The screenshot shows the EPICenter ESRP Manager interface in a Microsoft Internet Explorer browser window. The address bar shows the URL `http://hendrix/everest`. The main content area is titled "ESRP Manager" and displays "Detailed ESRP Information of 'Vlan1'". A table lists the following data:

Switch Name	MAC	State	Priority	To Master	To Slave	Active Ports	Tracked Ports	Tracked Rout	Tracked Pir
s11	00:01:30:00:8b:00	Slave	0	2	3	1	0	0	0
S11_old	00:e0:2b:81:6f:00	Master	0	25	25	1	1	0	0

The interface also includes a left-hand navigation menu with options like Home, Inventory, Alarm, ESRPs, Config, Telnet, Groups, Find IP/MAC, EView, RT Stats, Topology, VLAN, ESRP, Admin, Reports, Policy, and Logout. The status bar at the bottom indicates "Applet started." and "Local intranet".

**Figure 14-2:** ESRP detail for an individual ESRP-enabled VLAN

ESRP trap events will also be recorded in the EPICenter Event Log, which you can view using the EPICenter Event Log Report (see Chapter 16, “Dynamic Reports”). ESRP state change traps will be recorded in the EPICenter Alarm Log (see Chapter 5, “The EPICenter Alarm System”).



*ESRP Traps are not implemented in ExtremeWare versions 4.x or 5.x. Thus, for switches running those versions of ExtremeWare, state changes and other ESRP updates will only be reflected after the next ESRP polling interval.*

Note that an ESRP-enabled VLAN can be monitored by EPICenter as long as at least one of its ESRP-enabled switches is managed by EPICenter (i.e. is included in EPICenter’s device database). If there are other ESRP-enabled switches in that VLAN, their ESRP status will also be displayed in the ESRP Manager, even if they are not being managed by EPICenter.

The Detailed ESRP Information view displays the following information:

- **Switch Name:** The name of the switch, if known. (If the switch is not being managed by EPICenter, this field will contain “N/A”)
- **MAC:** The MAC address of this switch
- **State:** The current state of the switch—Master or Slave
- **Priority:** A user-defined value, between 0 and 254, which can be used by the ESRP election algorithm in determining which switch is the Master switch. The default is 0
- **ToMaster:** The number of times this switch has transitioned to become a Master
- **ToSlave:** The number of times this switch has transitioned to become a Slave



*The number of Master and Slave transitions cannot be obtained from versions of ExtremeWare prior to version 6.1.6. For switches running earlier versions of ExtremeWare, the display defaults to “N/A.”*



*If some of the ESRP-enabled switches in an ESRP-enabled VLAN are not managed by EPICenter, the **ToMaster** and **ToSlave** values for those switches will not be updated until the next ESRP polling interval.*

- **Active Ports:** The number of active ports in this ESRP-enabled VLAN
- **TrackedActivePorts:** The number of tracked ports that are currently active
- **TrackedIPRoutes:** The number of tracked IP routes that are currently active
- **TrackedPings:** The number of tracked ping responders that are responding successfully.



*The number of Tracked Pings cannot be obtained from versions of ExtremeWare prior to version 6.1.6. For switches running earlier versions of ExtremeWare, the display defaults to zero.*

# 15

## Administering EPICenter

---

This chapter describes how to use the Administration applet for the following:

- Changing your own user password, for users without Administration access
- Adding and deleting EPICenter users
- Setting and modifying user permissions for both the EPICenter and ExtremeWare software
- Configuring the EPICenter server as a RADIUS client or a RADIUS server for user authentication
- Modifying EPICenter server properties to change settings such as polling rates, time-outs, port assignments and other similar settings
- Setting the EPICenter server into Scalable mode or back to regular mode

### Overview of User Administration

In order to log in to the EPICenter server and use its management features, you must have a user name and password. An EPICenter administrator can create and modify EPICenter user accounts, passwords, and account permissions through the Administration applet. Individual users, regardless of their access permissions, can change their own password using the Administration applet.

The EPICenter server and its Remote Authentication Dial In User Service (RADIUS) server can be used for user authentication, both for EPICenter server access and Extreme Networks switch access. The Administration applet provides an interface for configuring the RADIUS server.

Finally, the Administration applet provides an interface that allows an EPICenter administrator to modify a number of properties that affect the performance and configuration of the EPICenter server. These properties are stored in the EPICenter database along with other EPICenter data.

## Controlling EPICenter Access

The EPICenter server provides three levels of access to EPICenter functions:

- Monitor—users who can view status information and statistics.
- Manager—users who can modify device parameters as well as view status information and statistics.
- Administrator—users who can create, modify and delete user accounts as well as perform all the functions of a user with Manager access.

The EPICenter server provides two default users:

- “admin” with Administrator access
- “user” with Monitor access

The two default users do not initially have passwords. All other user names must be added and enabled by an Administrator user.

Regardless of your access level, you can run the Administration applet and change your own password. Users with Administrator access can add and delete users and assign user access levels.



*The EPICenter user accounts are separate from the Extreme switch user accounts. You can configure both through the EPICenter software, or you can have switch access independently of the EPICenter software.*

## ExtremeWare Software Access

Through the EPICenter software, two levels of access to Extreme switches can be enabled:

- User—users who can view device status information and statistics, but cannot modify any parameters.
- Administrator—users who can modify device parameters as well as view status information and statistics.

These permissions enable access to Extreme Networks switches through Telnet or ExtremeWare Vista. The use of the RADIUS server avoids the need to maintain user names, passwords, and access permissions in each switch, and instead centralizes the configuration in one location in the EPICenter server.

## The EPICenter RADIUS Server

The EPICenter software incorporates a basic RADIUS server for user authentication. RADIUS provides a standard way for the EPICenter software and Extreme Networks switches to handle user authentication, permitting the unification of the Extreme Networks CLI, ExtremeWare Vista, and EPICenter user authentication.

ExtremeWare versions 4.1 and later support the RADIUS server for authentication and can act as RADIUS clients.

## Setting EPICenter Server Properties

The server properties interface allows an EPICenter administrator to modify a number of parameters that affect server performance and function. These include communication parameters such as polling intervals, time-outs, port usage, number of retries, setting Scalability mode, and a number of other parameters.

## Starting the EPICenter Client for the First Time

The two default users, admin and user, do not initially have passwords.

It is strongly recommended that you log in the first time with the user name admin, and immediately change the admin password. You can then add other users with Manager, Monitor, or Administrator access.

To run the EPICenter client interface for the first time:

- 1 Launch your Web browser.
- 2 Enter the URL:

```
http://<host>:<port>/
```

In the URL, replace *<host>* with the name of the system where the EPICenter server is running. Replace *<port>* with the TCP port number that you assigned to the EPICenter Web Server during installation.



*If you used the default web server port, 80, you do not need to include the port number.*

The EPICenter Start-up page appears.

**3** Launch the EPICenter client.

The EPICenter Login page appears.

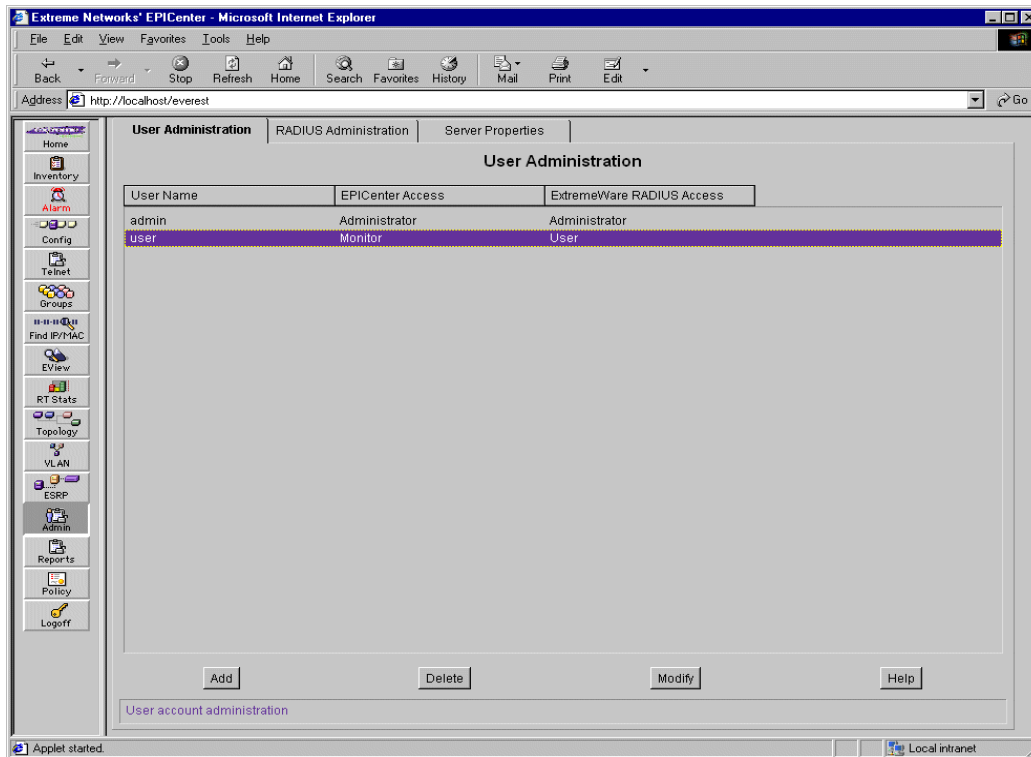
**4** Type the user name **admin** in the User field.

**5** Leave the Password field empty.

**6** Click **Login**. The About EPICenter window appears.

**7** Click **Admin** to access the Administration functions of the EPICenter server.

The User Administration page appears, as shown in Figure 15-1. The only users are “admin” and “user.”



**Figure 15-1:** User Administration window

## Changing the Admin Password

To change the Admin password:

- 1 Click the tab at the top of the page to display the User Administration page, if necessary.
- 2 Select the user **admin** in the User list.
- 3 Click **Modify**.

The Edit User window appears, as shown in Figure 15-2.

**Figure 15-2:** Edit User window

- 4 Type a new password in the **Password** field.
- 5 Type the password again in the **Verify Password** field.
- 6 Click **OK**.

The new admin password is stored in the EPICenter database. You cannot change the ExtremeWare EPICenter access level for this user.

You can, however, change the ExtremeWare account access. The default for the ExtremeWare EPICenter user “Admin” is Administrator. See the information under



“Adding or Modifying User Accounts” for details on the ExtremeWare account access levels.

## Adding or Modifying User Accounts

To add users to the EPICenter database, or to modify ExtremeWare EPICenter user account access, follow these steps:

- 1 Login to the ExtremeWare EPICenter as a user with Administrator access.
- 2 Click **Admin** in the Navigation Toolbar.
- 3 Click the User Administration tab at the top of the page to display the User Administration page, if necessary.
- 4 To add a user, click **Add**. To change a user’s access or password, select the user name and click **Modify**.

The New User window (or Edit User window) appears (Figure 15-3).

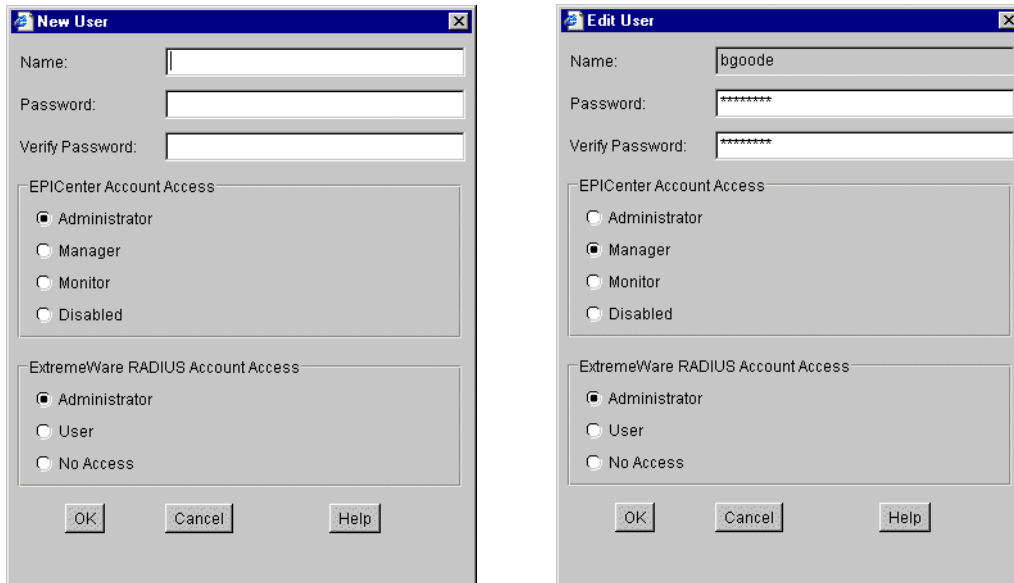


Figure 15-3: New User and Edit User windows

- 5 For a new user, type a user name into the **Name** field.

- 6 Type a new password into the **Password** field.
- 7 Type the password again into the **Verify Password** field.
- 8 Select the appropriate EPICenter Account Access level:
  - **Administrator** access allows the user to add, edit and delete user accounts, as well as view status information and statistics and modify device parameters.
  - **Manager** access allows the user to view status information and statistics and modify device parameters.
  - **Monitor** access allows the user to view status information and statistics.
  - **Disabled** provides no access privileges (the user will not be able to log in to the EPICenter), but keeps the user account information in the EPICenter database.
- 9 Select the appropriate ExtremeWare Account Access level:
  - **Administrator** access allows the user to modify device parameters as well as view status information and statistics.
  - **User** access allows the user to view device status information and statistics, but cannot modify any parameters.
  - **No Access** provides no access privileges, but keeps the user account information in the EPICenter database.
- 10 Click **OK**.

The new user information is stored in the EPICenter database.



*A change to a user account does not take effect until the next time the user logs in.*

## Deleting Users

To delete a user, follow these steps:

- 1 Log in to the ExtremeWare EPICenter as a user with Administrator access.
- 2 At the About ExtremeWare EPICenter window, click **Admin** in the Navigation Toolbar.  
The User Administration page appears.
- 3 Click the User Administration tab at the top of the page to display the User Administration page, if necessary.
- 4 Select the user name you want to delete and click **Delete**.



*You cannot delete the user name **admin**.*

A confirmation window appears.

**5 Click Yes.**

This removes all information about this user account from the EPICenter database.



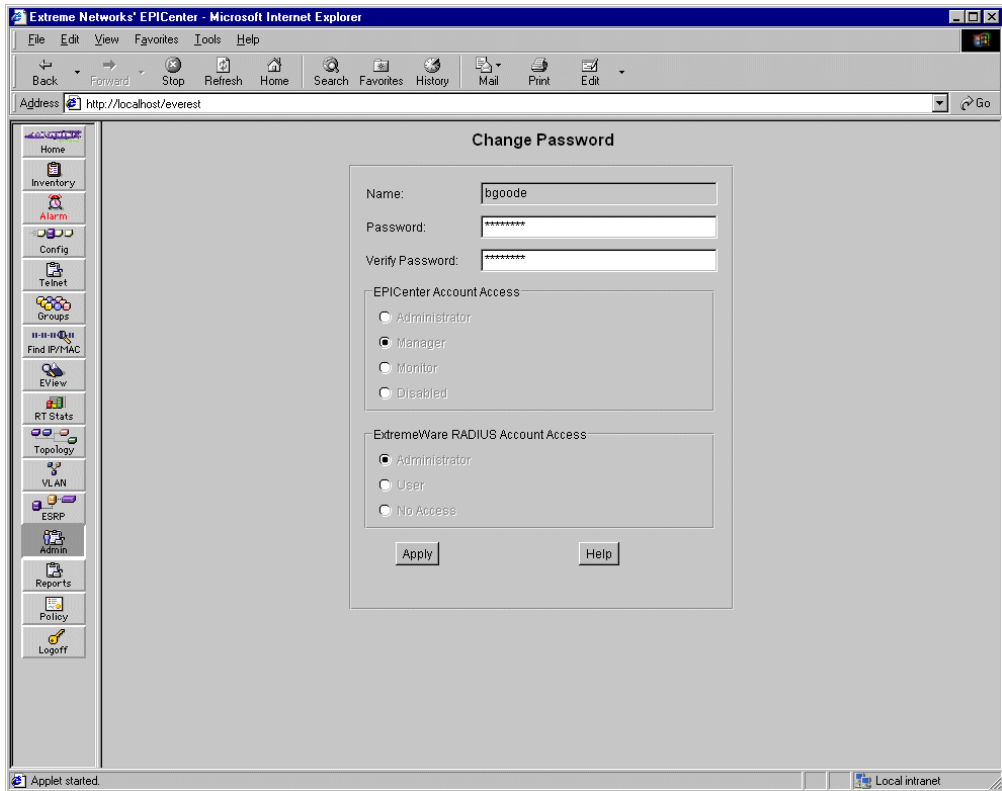
*To remove all access privileges for a user **without** removing the user account from the EPICenter database, use the Modify User function and change the Account Access to Disabled.*

## Changing Your Own User Password

If you are a user with Manager or Monitor access, you can change your own password at any time after you have logged in to the ExtremeWare EPICenter. To do so, follow these steps:

**1 Click Admin** in the Navigation Toolbar.

The Change Password window appears, as shown in Figure 15-4.



**Figure 15-4:** Change Password window

The window shows your user name, and your EPICenter and RADIUS Account Access levels, but you cannot change them.

- 2 Type your new password in the **Password** field.
- 3 Type the password again in the **Verify Password** field.
- 4 Click **Apply**.

Your new password is stored in the EPICenter database.



*The change does not take effect until the next time you log in.*

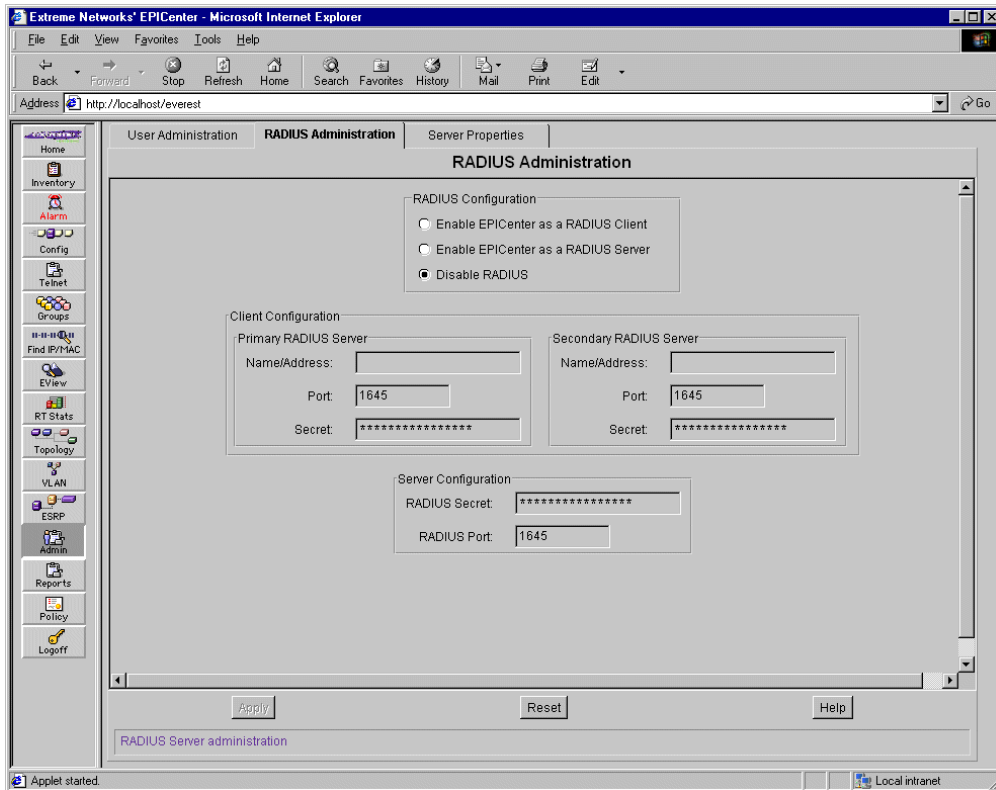
# RADIUS Administration

If you have Administrator access, you can enable or disable the RADIUS server, and change its port or the RADIUS secret.

To configure EPICenter as a RADIUS server, follow these steps:

- 1 Click the **RADIUS Administration** tab at the top of the page.

The RADIUS Administration page appears, as shown in Figure 15-5.



**Figure 15-5:** Radius Administration page

- 2 Click the **Enable EPICenter as a RADIUS Server** button in the **Radius Configuration** panel at the top of the page.

This enables the fields in the **Server Configuration** panel.

- 3 Enter the RADIUS server's shared secret in the **RADIUS Secret** field.

This string is basically a shared key by which the RADIUS server and its clients recognize each other, and which they use for secure transmission of user passwords.



*If you change the secret in the RADIUS server, you must also change it in any of the RADIUS clients (Extreme switches) that use the RADIUS server for user authentication.*

- 4 The default port used for the RADIUS server is 1645. To change the server port, enter the port number in the **RADIUS Port** field.



*If you change the RADIUS server port, you must make sure that the ports used in any RADIUS clients (Extreme switches that use this RADIUS server for user authentication) match the port you enter for the server.*

To enable EPICenter as a RADIUS client, do the following:

- 1 Click the **RADIUS Administration** tab at the top of the page.
- 2 Click the **Enable EPICenter as a RADIUS Client** button at the top of the page.

This enables the fields in the **Client Configuration** panel.

- 3 Fill in the fields (server name or IP address, port, and shared secret) for the primary and secondary RADIUS servers as appropriate.

It is recommended, but not required, that both a primary and a secondary RADIUS server be available for authentication.

- 4 Click **Apply** to have the configuration changes take effect.
- 5 To enable or disable the RADIUS server, click the appropriate button.

Enabling the RADIUS server means that Extreme switches can act as RADIUS clients, authenticating users against the RADIUS server's database of users, as administered through the EPICenter. Thus, even if a user accesses the switch directly through Telnet or a browser, the RADIUS server will provide the authentication service.

Disabling the RADIUS server means that it will not be available for authenticating users. In this case, each Extreme switch must maintain its own list of users and access permissions, and users will need to remember a (possibly different) login and password for every switch.

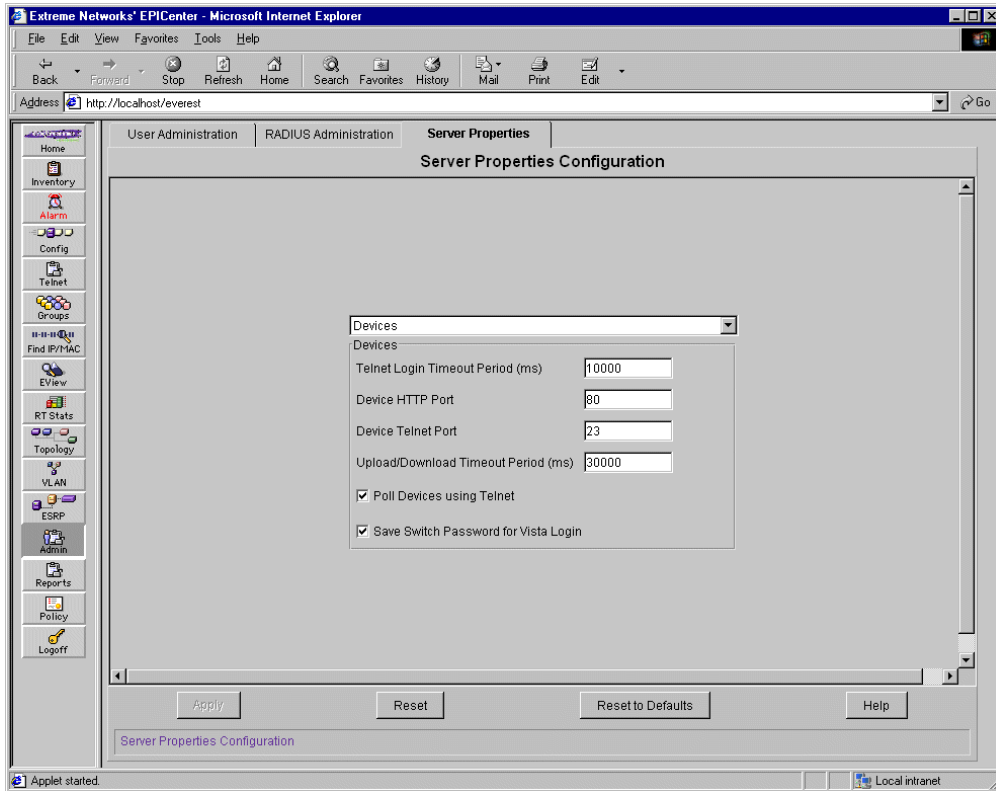
If you have enabled the EPICenter RADIUS server, authentication activity is logged to the file `radius_log.txt`, found in the EPICenter root install directory.

# Server Properties Administration

If you have Administrator access, you can modify the values of a number of properties that affect the function and performance of the EPICenter server.

- 1 Click the **Server Properties** tab at the top of the page.

The Server Properties Configuration page appears, as shown in Figure 15-6.



**Figure 15-6:** Server Properties Configuration page, initial properties list

- 2 Select a set of properties from the drop-down menu field at the top of the central panel. You can select among five sets of properties:
  - Devices
  - Scalability

- SNMP
- Topology
- Other

The Server Properties Configuration page displays the properties in that set.

- 3 Type a new value into the field for the property you want to change, or click a check-box to turn on or off an option. The specific properties and their meanings are discussed in the following sections.

- 4 Click the **Apply** button to cause your changes to take effect.

You can undo your changes in one of two ways:

- Click the **Reset** button to restore the values that the displayed properties held when you first entered this page.
- Click the **Reset to Defaults** button to restore the values to the EPICenter server default values (the values in effect immediately after installation).

- 5 For some changes, you will need to restart the EPICenter server for the changes to take effect. A pop-up dialog will let you know that this is necessary.

Click **OK** to dismiss the dialog box, and then shut down and restart the EPICenter server.

See Chapter 2, “Starting ExtremeWare EPICenter” for information on how to shut down and restart the EPICenter server.

## Devices Properties

When you select Devices from the drop-down menu field at the top of the properties panel, you can set the following properties:

- **Telnet Login Timeout Period:** Length of time, in milliseconds, after which a CLI/Telnet login request to a switch should time out. The default is 10000 milliseconds (10 seconds), the range is 1 to 30 seconds (1000 to 30000 ms).
- **Device HTTP Port:** the port that the EPICenter server will use to communicate with an Extreme switch’s web server to run ExtremeWare Vista. Default is port 80.
- **Device Telnet Port:** the port that the EPICenter server will use to telnet to a switch. Default is port 23.
- **Upload/Download Timeout Period (ms):** Length of time, in milliseconds, after which a configuration upload or download operation should time out. If some devices have a large number of VLANs, the timeout may need to be increased to allow an upload or download operation to complete successfully without timing out.



- **Poll Devices Using Telnet** (checkbox): This enables or disables regular CLI/Telnet polling of ExtremeWare 4.1 devices. It disables ESRP polling as well as EDP polling. The default is enabled.
- **Save Switch Password for Vista Login** (checkbox): Enables ExtremeView to save the switch password in the EPICenter database when you log into a switch using ExtremeWare Vista. If you disable this property, you will be required to login to each switch in order to view Configuration and Statistics information in the ExtremeView applet. The default is enabled (passwords will be saved).

## Scalability Properties

Select Scalability from the drop-down menu field at the top of the properties panel to set the EPICenter server into Scalable mode (or reset it into regular mode).

- **Scalable Mode** (checkbox): A check in the box indicates that Scalability mode is turned on. When the box is blank, the EPICenter server is in regular mode. Click the checkbox to add or remove the check. The default is regular mode.

You must restart the EPICenter server after changing from regular to Scalable Mode or back to regular mode. When you click Apply after changing this setting, a pop-up confirmation dialog will warn you that you must restart the server.

Scalable Mode allows the EPICenter server to manage up to approximately 2000 devices. However, not all applets are available in this mode. In particular, the following applets are NOT available in Scalable Mode:

- ExtremeView
- Real-Time Statistics
- Topology
- VLAN Manager
- ESRP Manager
- Policy Manager (an optional module)

## SNMP Properties

When you select SNMP from the drop-down menu field at the top of the properties panel, you can set the following properties:

- **Poll Interval:** the interval, in seconds, between SNMP polls of a switch to fetch basic device status information. The default is 300 seconds (five minutes). The range is 5 to

3600 seconds (one hour). You can disable all SNMP polling by setting this property to zero.



*Note that this Poll Interval is different from the Device Polling Interval you can set through the Inventory Manager. The Device Polling Interval controls the frequency of polling for detailed device information such as software version, bootrom version, and so on. The polling interval set in the Administration applet controls only the basic SNMP status information necessary to ensure SNMP reachability, and is typically performed relatively frequently.*

- **Timeout Period:** The length of time to wait for an SNMP poll request to complete, in seconds, before timing out. The default is 2 seconds. The range is 1 to 10 seconds.

This setting determines the time-out interval only for the first unsuccessful SNMP request; once a request times out, subsequent requests will time out more slowly, based on an exponential time-out back-off algorithm, until it reaches the maximum number of retries.

- **Number of Retries:** the number of SNMP requests that should be attempted before giving up, for a request that has timed out.
- **EPICenter Trap Receiver Port:** the port on which EPICenter expects to receive traps. Default is port 10550.

## Topology Properties

Select Topology from the drop-down menu field at the top of the properties panel to set properties that affect the collection and display of RMON statistics in the Topology applet.

- **Enable RMON Display** (checkbox): This enables the collection of RMON statistics in the Topology applet. The default is enabled, which means that RMON statistics will be collected for all devices that have RMON enabled in the device.
- **Default Map RMON Statistics** (checkbox): This specifies the default state of the RMON statistics display checkbox in the Topology Map Properties pop-up. If this is checked, then the RMON Statistics option in the Map Properties window will be enabled by default, meaning that RMON statistics will be displayed on the links in the map. To disable the RMON statistics display for a map, you must disable the option in the Map Properties pop-up for that map. The default is that the option is disabled.

## Other Properties

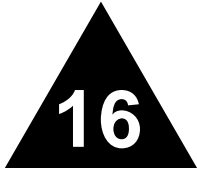
When you select Other from the drop-down menu field at the top of the properties panel, you can set the following properties:

- **DNS Lookup Timeout Period:** The time-out period, in milliseconds, when performing DNS lookup operations for hosts found through DLCS or when importing (in the Grouping applet) from an NT Domain Controller. The default is 1000 milliseconds (one second).
- **Session Timeout Period:** The non-activity time-out period, in milliseconds, after which the user is required to re-login to the EPICenter server. The default is 600,000 milliseconds (ten minutes). You can disable the time-out by setting the property to -1.
- **ServiceWatch URL:** The URL for accessing ExtremeWare ServiceWatch, to allow it to be launched from the EPICenter navigation toolbar, and to run in the main EPICenter applet window.

For example, if ServiceWatch is running on a system named “tampico” at port 2000, you would enter `http://tampico:2000` as the ServiceWatch URL. You must then restart the EPICenter server to activate the ServiceWatch integration.

- **IP QoS Rule Precedence:** The starting value that the EPICenter server will use for setting precedence in the Policy Manager applet. This is an integer between 1 and 25,600. The default value is 10,000.

Setting this value lets you ensure that policies created by EPICenter will have higher precedence than policies created through the ExtremeWare CLI. It is also useful in distinguishing between policies created through the CLI and those created through the EPICenter Policy Manager applet.



# Dynamic Reports

---

This chapter describes how to use the ExtremeWare EPICenter Reports capability for:

- Viewing predefined Network Summary Reports from the Home EPICenter page
- Viewing predefined EPICenter status reports from the Dynamic Reports
- Creating new reports by writing Tcl scripts

## Overview of EPICenter Reports

The EPICenter software provides several sets of HTML-based reports that provide information about the devices managed by the EPICenter server. There are two types of these reports:

- A Network Summary Report, available on the main EPICenter “Home” page, displayed when you first log in through the EPICenter client.
- EPICenter Dynamic Reports, available separately from the main EPICenter client, or as an applet accessed from the client.

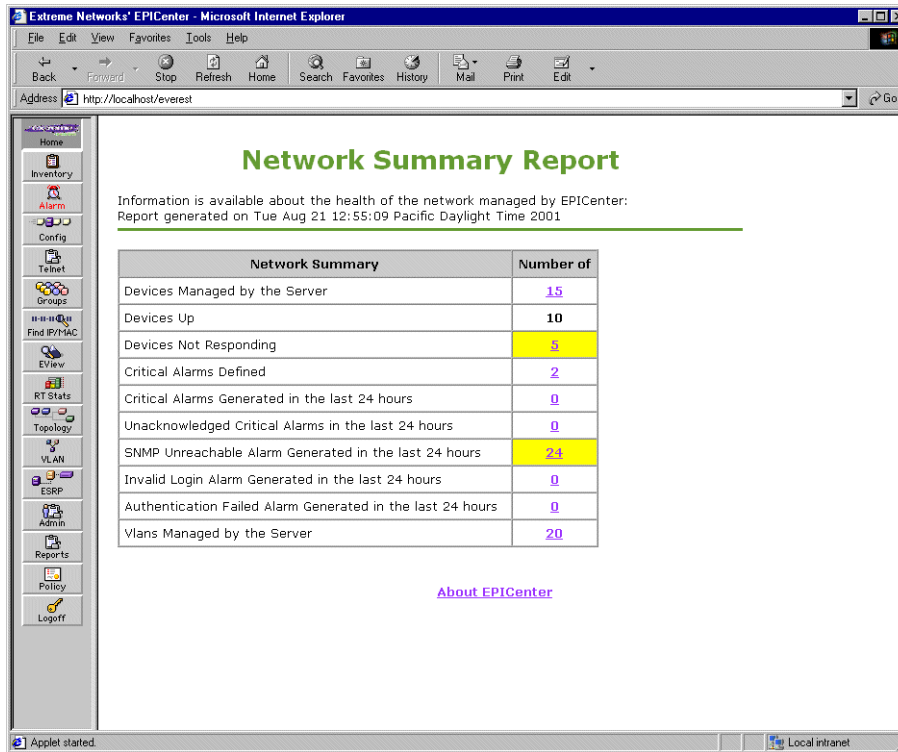
The Network Summary Report provides summary statistics about the status of the devices being managed by the EPICenter server. This report can also be accessed from the Dynamic Reports Main page.

EPICenter Dynamic Reports are a separate feature from the main EPICenter user interface, and can be accessed directly from the initial EPICenter Start-up page without logging in to the Java client interface. The Reports module can also be accessed from the EPICenter Navigation toolbar.

The EPICenter dynamic reports are HTML pages that do not require Java capability, and thus can be accessed from browsers that do not have the ability to run the full EPICenter user interface. This means reports can be loaded quickly, even over a dial-up connection, and it also provides the ability to print the reports.

## Network Summary Report

The Network Summary Report provides an at-a-glance summary of the status of the devices the EPICenter server is monitoring. The main report page, as shown in Figure 16-1, appears when you first log into the EPICenter client, and when you click the **Home** button at the top of the Navigation Toolbar.



The screenshot shows a Microsoft Internet Explorer browser window displaying the EPICenter Network Summary Report. The browser's address bar shows the URL `http://localhost/everest`. The page content includes a navigation toolbar on the left with buttons for Home, Inventory, Alarms, Config, Telnet, Groups, Find IP/MAC, EView, RT Stats, Topology, VLAN, ESRP, Admin, Reports, Policy, and Logoff. The main content area features the report title, a brief description, and a table of network statistics.

Network Summary	Number of
Devices Managed by the Server	15
Devices Up	10
Devices Not Responding	5
Critical Alarms Defined	2
Critical Alarms Generated in the last 24 hours	0
Unacknowledged Critical Alarms in the last 24 hours	0
SNMP Unreachable Alarm Generated in the last 24 hours	24
Invalid Login Alarm Generated in the last 24 hours	0
Authentication Failed Alarm Generated in the last 24 hours	0
Vlans Managed by the Server	20

Below the table, there is a link labeled [About EPICenter](#). The status bar at the bottom of the browser window shows 'Applet started.' and 'Local intranet'.

Figure 16-1: Network Summary Report page

If there are statistics that indicate problems (such as devices not responding, or alarms generated within the last twenty-four hours) the cell containing that statistic is displayed in yellow.

To view a detail report for a particular summary statistic, click the number in the right hand column of the summary display.

For example, you can click the value in the right-hand column of the **Devices Managed by the Server** row to display a **Device Reports** summary listing, showing the device groups currently configured in the EPICenter server.

From the Device Reports summary you can click one of the Device Group names to display a Device Summary report similar to that shown in Figure 16-2.

The screenshot shows the EPICenter Dynamic Reports interface in Microsoft Internet Explorer. The main content area displays a "Device Summary" report for a selected device group. The report is generated on Tue Aug 14 17:20:38 Pacific Daylight Time 2001. The report contains a table with the following data:

Group	IP Address	Name	Status	Boot Time (GMT)	MAC	S/w version	Serial Number
Default	<a href="#">10.205.0.25</a>	Summit24	operational	2001-07-08 19:14:02	00:e0:2b:5d:ac:00	4.1.19 (7)	800025-05-9920M00675
Default	<a href="#">10.205.0.32</a>	Summit1	not responding	2001-08-08 18:28:31	00:e0:2b:0c:cf:00	4.1.19 (2)	800002-20-9918F02415
Default	<a href="#">10.205.0.38</a>	LabA-2	operational	2001-07-31 20:39:34	00:e0:2b:81:fc:00	6.1.9 (5)	9942a00059
Default	<a href="#">10.205.0.170</a>	Summit5ITx	operational	2001-08-08 21:33:23	00:01:30:6c:0d:00	6.2.0 (48)	800078-11-0035M02442
Default	<a href="#">10.205.0.156</a>	Summit3	operational	2001-08-08 18:27:37	00:e0:2b:03:3c:00	4.1.19 (2)	800003-13-9804A07307
Default	<a href="#">10.205.0.171</a>	Summit1i	operational	2001-08-10 16:08:53	00:01:30:6c:30:00	6.1.9 (7)	0029M01563
Default	<a href="#">10.205.0.74</a>	Summit7ITx	not responding	2001-08-06 19:21:52	00:e0:2b:81:ae:00	6.1.5 (20)	6
Default	<a href="#">10.205.0.149</a>	Summit24e2T	operational	2001-08-06 16:39:57	00:01:30:10:00:19	UNKNOWN	
Default	<a href="#">10.205.0.30</a>	Summit24e3	not responding	2001-08-13 19:11:59	00:01:30:11:00:06	6.2.0 (34)	800096-01-0126M00933

Below the table, there is a link: [Back to Device Reports](#)

Figure 16-2: Network Summary Detail report

The only statistic in the Network Summary Report that does not provide its own detail report is the **Devices Up** statistic.

This report illustrates a number of features that are common to all the Summary Detail reports. In these reports, you can do the following:

- Click a column heading to sort on the contents of that column. For example, to sort by IP address, click on the Device IP Address link at the top of the first column. When you sort on a column, a small arrow in a box indicates whether the column is sorted in ascending or descending order.
- Click a link at the bottom of the report page to view additional report information or return to the main Network Summary Report.

Most of the Network Summary Reports provide additional detailed reports.

- To return to the main Network Summary Report from any of the detail reports, click the **Home** button at the top of the Navigation Toolbar.

The following sections describe the reports available from the Network Summary Report.

## Devices Managed by the Server

This report provides a summary status of all the devices known to the EPICenter server, organized by device group. This is also known as the **Device Inventory Report**, and can be accessed from the **Device Inventory** link on the main Reports pages, or from the **Device Inventory Reports** link on the **Devices Not Responding** report. See “Device Inventory Report” on page 16-13.

When you click the number in the right-hand column, a **Device Reports** summary is displayed. This shows the following information:

- **Group:** Device group name
- **Description:** Description (optional) associated with the device group
- **Devices:** Number of devices that belong to this device group

Select a Device Group to display the Device Summary report for the devices in the group.

The **Device Summary** report displays the following information about each device:

- **Group:** EPICenter Device Group to which it belongs
- **IP Address:** IP address of the device

Click the IP address to display a table with detailed configuration and status information. This is the same information you can view in the Inventory applet.

- **Name:** Device name from the `sysName` variable
- **Status:** Device status (operational or not responding)
- **Boot Time (GMT):** Time when the device was last booted
- **MAC:** MAC address of the device
- **S/w version:** Software version currently running on the device, if known
- **Serial Number:** Device serial number

Click the heading of a column to sort on the contents of that column.

Click the link **Back to Device Reports** to return to the Device Reports summary to select a different Device Group.

## Devices Not Responding

This report provides a summary status of the devices known to the EPICenter server that are currently not responding. It shows the following information for each device:

- **Device IP Address:** IP address of the device
- **Device Name:** Device name from the `sysName` variable
- **Device Description:** Device description from the `sysDescr` variable
- **Device Location:** Device location from the `sysLocation` variable
- **Device Status:** A red or yellow status “light”

Red indicates the device is not responding the EPICenter polls.

Yellow indicates the device is responding but is reporting a fan or power supply error.

Click the **To Device Inventory Reports** link at the bottom of the page to view Device Inventory Reports. See “Device Inventory Report” on page 16-13 for more information.

Click the **To Device Status Reports** link at the bottom of the page to view Device Status Reports. See “Device Status Report” on page 16-14 for more information.



## Critical Alarms Defined

This report provides a summary of alarms defined as having a severity level of Critical or Major. It shows the following information for each alarm:

- **Alarm Name:** Name of the alarm
- **Category:** Alarm category of which this alarm is a member
- **Enabled:** Whether the alarm is currently enabled or disabled
- **Severity:** Severity level of the alarm (Critical or Major)

See Chapter 5 for more information on alarm definitions, categories, and other alarm topics.

## Critical Alarms for Last 24 Hours

A summary of critical alarms that have occurred in the last 24 hours. It shows the following information.

- **Alarm Name:** Name of the alarm
- **Category:** Category that the alarm is classified under
- **Source IP:** IP address of the device that generated the alarm
- **Time (GMT):** Time the alarm occurred (Greenwich Mean Time)
- **Event #:** Event ID of the alarm (assigned by the EPICenter server when the alarm is received)
- **Severity:** Severity level of the alarm

You can view the complete Alarm Log report, showing all EPICenter alarms, from the Reports module. See “Alarm Log Report” on page 16-17.

See Chapter 5 for more information on alarm definitions, categories, and other alarm topics.

## Unacknowledged Critical Alarms

A summary of critical alarms that have occurred in the last 24 hours that have not been acknowledged. It shows the following information.

- **Alarm Name:** Name of the alarm

- **Category:** Category that the alarm is classified under
- **Source IP:** IP address of the device that generated the alarm
- **Time (GMT):** Time the alarm occurred (Greenwich Mean Time)
- **Event #:** Event ID of the alarm (assigned by the EPICenter server when the alarm is received)
- **Severity:** Severity level of the alarm

You can view the complete Alarm Log report, showing all EPICenter alarms, from the Reports module. See “Alarm Log Report” on page 16-17.

See Chapter 5 for more information on alarm definitions, categories, and other alarm topics.

## SNMP Unreachable Alarms

A summary of SNMP Unreachable alarms that have occurred in the last 24 hours. It shows the following information.

- **Alarm Name:** the name of the alarm.
- **Category:** the category that the alarm is classified under.
- **Source IP:** the IP address of the device that generated the alarm.
- **Time (GMT):** the time the alarm occurred (Greenwich Mean Time).
- **Event #:** the event ID of the alarm (assigned by the EPICenter server when the alarm is received).
- **Severity:** the severity level of the alarm.

You can view the complete Alarm Log report, showing all EPICenter alarms, from the Reports module. See “Alarm Log Report” on page 16-17.

See Chapter 5 for more information on alarm definitions, categories, and other alarm topics.

## Invalid Login Alarms

A summary of Invalid Login alarms that have occurred in the last 24 hours. It shows the following information.

- **Alarm Name:** Name of the alarm
- **Category:** Category that the alarm is classified under
- **Source IP:** IP address of the device that generated the alarm
- **Time (GMT):** Time the alarm occurred (Greenwich Mean Time)
- **Event #:** Event ID of the alarm (assigned by the EPICenter server when the alarm is received)
- **Severity:** Severity level of the alarm

You can view the complete Alarm Log report, showing all EPICenter alarms, from the Reports module. See “Alarm Log Report” on page 16-17.

See Chapter 5 for more information on alarm definitions, categories, and other alarm topics.

## Authentication Failure Alarms

A summary of Authentication Failure alarms that have occurred in the last 24 hours. It shows the following information.

- **Alarm Name:** Name of the alarm
- **Category:** Category that the alarm is classified under
- **Source IP:** IP address of the device that generated the alarm
- **Time (GMT):** Time the alarm occurred (Greenwich Mean Time)
- **Event #:** Event ID of the alarm (assigned by the EPICenter server when the alarm is received)
- **Severity:** Severity level of the alarm

You can view the complete Alarm Log report, showing all EPICenter alarms, from the Reports module. See “Alarm Log Report” on page 16-17.

See Chapter 5 “The EPICenter Alarm System” for more information on alarm definitions, categories, and other alarm topics.

## VLANs Report

Summary information on all VLANs being managed by the EPICenter server. This report is the same as the VLAN Summary Report you can access from the Reports module. See “VLAN Summary Report” on page 16-15 for a description of this report.

## Dynamic Reports

A number of predefined reports present information from the EPICenter software database. The predefined reports include:

- Network Summary Report (described in the previous section)
- Server State Summary Report
- Device Inventory Report
- Device Status Report
- VLAN Summary Report
- Interface Report
- Resources by Attribute
- User to Host Mapping
- Alarm Log Report
- Event Log Report
- Configuration Management Log Report

The content for the first three reports (Device Inventory, Device Status, and VLAN Summary) are generated by Tcl scripts. The remaining four reports (Device Interface, Alarm Log, Event Log, and Configuration Management Log) are generated by Java-based code.

The Java-based reports can be sorted, filtered, and paginated, but they cannot be customized. The Tcl-based reports can be customized, and can serve as models for new reports. You can create your own reports by writing Tcl scripts that generate HTML code. See “Creating New Reports” on page 16-21 for details.

You can access the EPICenter software Dynamic Reporting capability in one of two ways:

- By clicking the **Reports** icon in the EPICenter software Navigation Toolbar

- By logging in directly from the EPICenter Start-up page

To log in directly from the EPICenter software Start-up page, follow these steps:

- 1 Launch your Web browser.
- 2 Enter the following URL:

`http://<host>:<port>/`

In the URL, replace `<host>` with the name of the system where the ExtremeWare EPICenter server is running. Replace `<port>` with the TCP port number that you assigned to the ExtremeWare EPICenter Web Server during installation.



*If you used the default web server port, 80, you do not need to include the port number.*

The EPICenter Start-up page appears.

- 3 Click **View Reports** in the left-hand panel of the Start-up page.

The ExtremeWare EPICenter Login page appears.

- 4 Enter your user name and password, and click **Login**. Use the same user name and password as you use to log in to the EPICenter system.

The Dynamic Reports module is displayed. The main page includes a brief description of the predefined reports that are available.

## Viewing Predefined EPICenter Reports

To view a predefined report, click the appropriate link in the left-hand navigation panel.

To go to the main ExtremeWare EPICenter user interface, click the “**About EPICenter**” link at the top of the list. This displays the **About ExtremeWare EPICenter** page.

To exit from ExtremeWare EPICenter, click the Logout link in the left-hand panel. This returns you to the ExtremeWare EPICenter Start-up page.

## Report Filtering

Four of the reports provide a filtering capability that lets you select the information that should appear in the report. This filtering capability lets you construct a two-part

conditional statement based on the values of relevant variables in the ExtremeWare EPICenter database.

The following reports provide filtering:

- Interface Report
- Alarm Log
- Event Log
- Config Mgmt Log

These reports provide a set of fields at the bottom of the report similar to the ones shown in Figure 16-3.

**Figure 16-3:** Report filter specification

To create a filter, follow these steps:

- 1 In the first field, select the variable to use in the filter. The variables from which you can choose are based on the column headings in the report, and depend on the type of report you are viewing.
- 2 In the second field, select a comparison operator. You can choose from the following comparison operators:
  - > (greater than)
  - < (less than)
  - <= (greater than or equal)
  - >= (less than or equal)
  - != (not equal)
  - = (equal)

If the variable values are strings, then the comparisons are taken to indicate alphabetic order, where greater than indicates later in later in the alphabet (for example, the letter B is greater than A).

- 3 In the third field, select the value you want to compare the variable against. If the variable takes a string as its value, enter a string. If the variable is numeric, enter an integer.



*You can use the browser Copy and Paste functions to copy a specific value from the current report into the comparison field.*

- 4 In the fourth field, you can indicate whether the second condition should be used. To use a second condition to your filter, choose one of the logical operators **And** or **Or**. Specify **And** to include a row in the report only if both conditions are true. Select **Or** to include the row if either one (or both) of the conditions are true.

If you do not want to include a second condition, select **NIL** to indicate that the second clause should be ignored.

- 5 Click **Filter** to generate the report based on the filter you have specified.

Click **Remove Filter** to remove the filter definition and generate an unfiltered report.

## Server State Summary Report

The Server State Summary Report displays statistics about SNMP activity, database activity, and the ports used by the EPICenter server. The report provides the following information.

The first table in the report provides the number of operations that have occurred in the last minute, the last hour, and the last day (24 hours) for the following operations:

- **SNMP Queries:** Number of SNMP queries performed by the EPICenter server
- **Database Commits:** Number of database commits performed by the EPICenter server
- **Client Requests:** Number of data requests to the EPICenter server performed by all connected clients
- **Trap Requests:** Number of trap PDUs received by the EPICenter server

The second table in the report shows the ports currently in use by the EPICenter server.

- **Web Server Port:** Port currently used by the EPICenter web server.
- **Trap Receiver Port:** Port currently used by the EPICenter server to receive traps

- **Radius Port:** Port currently used by the RADIUS server
- **Telnet Port:** Port currently used for Telnet
- **Database Port:** Port currently used for EPICenter database communication

The Web Server, Trap Receiver, Radius and Telnet ports can be changed through the Administration applet, if you have administrator-level access to EPICenter. See Chapter 15, “Administering EPICenter,” for more information.

If you are running under Windows NT or WIndows 2000, you can use the Port Configuration Utility, accessible from the Programs menu, to change the database port. See Appendix B “EPICenter Utilities” for details on the utility.

There are no further detailed reports available from this report.

## Device Inventory Report

To view a Device Inventory Report, click the **Device Inventory** link in the left-hand panel.

The Device Inventory Report displays basic status and identification information for the devices known to ExtremeWare EPICenter. The initial display presents a summary at the Device Group level. This includes the following information:

- **Group:** Device Group name
- **Description:** Description of the group as kept in the EPICenter device inventory
- **Devices:** Number of devices in the group

Select a Device Group to display the Device Summary report for the devices in the group.

The Device Summary report displays the following information about each device:

- **Group:** EPICenter Device group to which it belongs
- **IP Address:** IP address of the device  
Click the IP address to display a table with detailed configuration and status information. This is the same information you can view in the Inventory applet.
- **Name:** Device name from the `sysName` variable
- **Status:** Device status
- **Boot Time (GMT):** Time when the device was last booted
- **MAC:** MAC address of the device
- **S/w version:** Software version currently running on the device, if known



- **Serial Number:** Device serial number

Click the heading of a column to sort on the contents of that column.

## Device Status Report

To view a Device Status Report, click the **Device Status** link in the left-hand panel. This displays the device status and failure log for all devices known to EPICenter.

The initial display presents a summary at the Device Group level. This includes the following information:

- **Group:** Device Group name
- **Description:** Description of the group as kept in the EPICenter device inventory
- **Alarms Defined:** Total alarms for all devices in the device group
- **Devices Up:** Number of devices in the group that are up
- **Devices Not Responding:** Number of devices in the group that are not responding

Select a Device Group to display the Device Status Report for the devices in the group.

The Device Status report displays the following information:

- **Device Name:** Name of the device from the **sysName** variable
- **IP:** IP address of the device
- **Status:** A green, yellow, or red status “light”  
Green indicates the device is up and OK.  
Yellow indicates the device is responding but is reporting fan, temperature, or power supply errors.  
Red indicates that the device is unreachable.
- **Last Failure (GMT):** Time at which the most recent device failure occurred
- **Down Period (d:h:m:s):** Length of time the device was unreachable, reported in *days:hours:minutes:seconds*
- **Boot Time (GMT):** Time when the device was last booted
- **Alarms in last 24 hours:** Number of alarms in the last 24 hours from this device  
If the number of alarms is greater than zero, you can click on the number to display a summary of the alarms that have occurred for this device.

If the number of alarms for a device is greater than zero, you can click the number to view a summary of the alarm information for that device.

## VLAN Summary Report

To view a VLAN Summary Report, click the **VLAN Summary** link in the left-hand panel. This displays a report of the VLANs known to ExtremeWare EPICenter. The information reported includes:

- **VLAN Name:** Name of the VLAN
- **Tag:** 802.1Q tag, if any
- **Protocol:** Protocol used to filter packets for this VLAN
- **QoS Profile:** QoS profile configured for this VLAN
- **Device (DNS) List:** IP addresses of devices with ports that are members of this VLAN

See Chapter 13 “Using the VLAN Manager” for more information on VLANs.

## Interface Report

To view a device interface report, click the **Interface Report** link in the left-hand panel. This displays a report on the status of every port known to ExtremeWare EPICenter. The information reported for each interface includes:

- **IP Address:** IP address of the interface
- **Port:** Port number of the interface
- **AdminStatus:** Interface administrative status (enabled/disabled)
- **OperStatus:** Operational status of the interface (ready/active)
- **Configured speed/type:** Nominal (configured) speed of the interface
- **Actual speed/type:** Actual speed of the interface

Since the EPICenter server may be aware of many hundreds of ports, the interface information is displayed in groups of 25 ports per page. You can navigate among the pages using any of the following methods:

- Clicking the **Previous** and **Next** links
- Selecting a page number from the at the top of the report
- Clicking the **First** or **Last** links to display the first or last page in the report

The list of ports is sorted initially by IP address. Click the heading of a column to sort the report based on the contents of that column. For example, to sort by operational status, click on the **OperStatus** heading.

You can filter the ports that are displayed by constructing a conditional filter using the fields at the bottom of the page. This lets you construct a two-clause filter statement in the form shown in Figure 16-4.

**Filter Report on Device Ports With**

AdminStatus is = disabled And Actual Speed/Type is = 10BaseT

Filter RemoveFilter

**Figure 16-4:** Device Ports filter specification

You can filter on any of the variables shown in the report.

## Resource to Attribute Mapping Report

The Resource to Attribute Mapping Report displays a list of all the resources that include the specified attribute. Click the **Resource to Attribute Mapping** link in the left-hand panel to display the attribute selection field. Then select an attribute from the pull-down list, as shown in Figure 16-5.

### View resources for an attribute

View resources for: IP Submit

- IP
- UDP Any
- TCP Any
- TCP Permit-Established Any
- IP Any
- L4 port
- IP Address
- dept
- type

**Figure 16-5:** Attribute specification for Resource to Attribute Mapping report

The pull-down list shows a set of system-defined attributes used by the Policy Manager, along with any attributes you've added to resources through the Grouping Manager.

The system-defined attributes (IP, UDP Any, TCP Any, TCP Permit-Established Any, IP Any, and L4 Port) have static definitions and are used internally by the EPICenter Policy Manager.

User-defined attributes are created within the Grouping Manager, either by adding them to a resource through the user interface, or by importing them.

For the attribute you select in the pull-down menu, the report displays the following information:

- **Resource Type:** Type of the resource (such as device, user, host, or group)
- **Resource Name:** Name of the resource that includes the selected attribute
- **Attribute Value:** Value of the attribute associated with the resource

## User to Host Mapping Report

The User to Host Mapping Report displays a list of any user and host mappings that are currently defined, along with the primary IP address of the host. User-host mappings can be created in the Grouping Manager, and can also be created automatically if the Dynamic Link Context System (DLCS) is enabled on your Extreme devices. Click the **User to Host Mapping** link in the left-hand panel to display the attribute selection field.

The report displays the following information:

- **User Name:** User name
- **Host Name:** Name of the host mapped to the user
- **Host IP Address:** Primary IP address of the host

## Alarm Log Report

To view an Alarm Log Report, click the **Alarm Log** link in the left-hand panel. This displays a report of all the entries in the EPICenter Alarm Log. The information reported includes:

- **Time (GMT):** time the alarm occurred (Greenwich Mean Time)
- **Name:** Name of the alarm
- **Severity:** Severity level of the alarm

- **Source:** IP address of the device that generated the alarm
- **Category:** Category that the alarm is classified under
- **Ack'd** (acknowledged): Whether the alarm has been acknowledged (true or false)
- **Event #:** Event ID of the alarm (assigned by the EPICenter server when the alarm is received)
- **Message:** Message associated with the alarm

The alarm information is displayed in groups of 25 alarm events per page. You can navigate among the pages using any of the following methods:

- Clicking the **Previous** and **Next** links.
- Selecting a page number from the at the top of the report.
- Clicking on the **First** or **Last** links to display the first or last page in the report.

The report is sorted initially by the Time that the alarm occurred. Click the heading of a column to sort on the contents of that column.

You can filter the alarms that are displayed by constructing a conditional filter using the fields at the bottom of the page. This lets you construct a two-clause filter statement in the form shown in Figure 16-6.

The screenshot shows a web form titled "Filter Alarm Log With". It contains two filter clauses. The first clause is "Severity is > Minor", where "Severity" is a dropdown menu, "is" is a text label, ">" is a dropdown menu, and "Minor" is a text input field. The second clause is "Source is = 205.0.50", where "Source" is a dropdown menu, "is" is a text label, "=" is a dropdown menu, and "205.0.50" is a text input field. Below the clauses are two buttons: "Filter" and "RemoveFilter".

**Figure 16-6:** Alarm Log filter specification

You can filter on any of the variables shown in the report.

For more details on the meaning of these variable, see the Chapter 5 “The EPICenter Alarm System.”

## Event Log Report

To view an Event Log Report, click the **Event Log** link in the left-hand panel. This displays a report of all the entries in the EPICenter Event Log. The information reported includes:

- **Event #:** Event ID of the alarm (assigned by the EPICenter server when the alarm is received)
- **Time (GMT):** Time the alarm occurred
- **Source:** IP address of the device that generated the alarm
- **Type:** Event type (for example, SNMP Trap)
- **Varbinds:** Variable data transmitted with a trap

The event information is displayed in groups of 25 events per page. You can navigate among the pages using any of the following methods:

- Clicking the **Previous** and **Next** links
- Selecting a page number from the at the top of the report
- Clicking the **First** or **Last** links to display the first or last page in the report

Click the heading of a column to sort on the contents of that column.

You can filter the events that are displayed by constructing a conditional filter using the fields at the bottom of the page, as shown in Figure 16-7. This lets you construct a two-clause filter statement.

Filter Event Log With

Time(GMT) is > 2000-10- And Type is = SNMP T

Filter RemoveFilter

**Figure 16-7:** Event Log filter specification

You can filter on any of the variables shown in the report.

You can use the browser Copy and Paste functions to copy a specific value from the current report into the comparison field. This is particularly useful if you want to filter on a specific Varbinds value.

## Configuration Management Log Report

To view a Configuration Management Log Report, click the **Config Mgmt Log** link in the left-hand panel. This creates a report of all the entries in the Configuration Management Log. The information displayed includes the following:

- **Time(GMT):** Time (Greenwich Mean Time) when the activity occurred.
- **Device:** IP Address of the device.
- **Activity:** Activity that occurred, such as uploading a configuration file, updating a software image, and so on. The actual entries will be abbreviated in form similar to “Get Cfg From Device” or “Put Cfg To Device.”
- **Status:** Status of the activity (Success or Failed).
- **File:** Name of the file involved in the upload or download.
- **Descr:** Description of the problem for a failed activity.

Click the heading of a column to sort on the contents of that column.

You can filter the management activity events that are displayed by constructing a conditional filter using the fields at the bottom of the page, as shown in Figure 16-8. This lets you construct a two-clause filter statement.

The screenshot shows a filter specification interface with the following elements:

- Title: Filter Config Management Activity Log With
- Field 1: Activity (dropdown) is = (dropdown) download (text input)
- Operator: And (dropdown)
- Field 2: Time(GMT) (dropdown) is >= (dropdown) 12:00 (text input)
- Buttons: Filter (button), RemoveFilter (button)

**Figure 16-8:** Configuration Management Log filter specification

You can filter on any of the variables in the report.

## Printing EPICenter Reports

Unlike the other EPICenter applets, you can print EPICenter reports using your browser’s print function. To print a report, place the cursor in the pane where the report is displayed,

and use the browser's Print button, or the Print command from the File menu, to initiate the print.

## Creating New Reports

The EPICenter software allows you to customize the existing EPICenter dynamic reports, and to define new reports. Because the reports use HTML and Tcl, you can incorporate the new or modified reports into the running EPICenter server without requiring a restart. In addition, the EPICenter software includes features that aid in debugging user changes.

All the files needed to create or modify reports can be found in the directory `<epicenter_install_dir>/user/reports`, where `<epicenter_install_dir>` is the directory where the EPICenter software resides (by default `epc3_1` in the Windows operating environment, or `/opt/epc3_1` on a Solaris system). There are two subdirectories under the `reports` directory:

- The `html` directory contains the HTML files displayed by the EPICenter server. The HTML files in the reports directory have the following functions:
  - `index.html` sets up the various frames for the browser display. It references `menu.html` to define the menu on the left-hand side, and `body.html` for the content in the main panel of the window.
  - `menu.html` defines the menu items for the predefined reports, and includes links to the `html` files that generate the reports. This is a generated file.
  - `body.html` defines the content that appears in the main panel of the window when the Reports feature is requested, either from the EPICenter software Start-up window, or from the icon on the Navigation Toolbar. Modify this file if you want to change or add to the list of Reports and their descriptions.
  - `color1.html` defines the color of the bar at the top of the main content window.
  - `epistylesheet.css` contains the style definitions used in the menu and main body frames.
  - `reportstylesheet.css` contains the style definitions used in the reports themselves. To change the look of all reports, you can modify this stylesheet.
  - The remaining files, such as `device_summary.html`, and `vlan_summary.html`, define a number of the actual reports available from the Reports module.

Note that some of the reports (the Interface Report and the four Log reports) are not user-modifiable, and are not included in the HTML directory.



- The `tcl` directory contains the following:
  - The Tcl methods available for creating new reports
  - The source code for the existing reports

The information presented in the remainder of this chapter assumes you have a reasonably thorough understanding of both HTML and Tcl scripting.

## Creating or Modifying a Report

You can modify an EPICenter report HTML file in any HTML editor, such as Microsoft FrontPage.

You can modify the existing HTML files to change the look and feel of the report, your icons, etc. The `device_summary.html` file is a good example.

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN">
<html>

<head>
<meta http-equiv="Content-Type"
content="text/html; charset=iso-8859-1">
<meta name="GENERATOR" content="Microsoft FrontPage 2.0">
<title>Simple Report</title>
<LINK REL="STYLESHEET" HREF="reportstylesheet.css" TYPE="text/css">
</head>

<BODY bgcolor="#ffffff" marginwidth="20" marginheight="0" leftmargin="20"
topmargin="0">

<TABLE border="0" cellspacing="0" cellpadding="0" height="120px">
<TR valign="bottom"><TD>
<H2>Device Reports</H2>
</TD></TR>

<TR valign="top"><TD>
Reports are available for the following devices in EPICenter.<br>
Report generated on <extr>clock format [clock seconds]</extr></TD></TR>

<TR valign="bottom"><TD><P></P>
</TD></TR>
</TABLE>
```

```

<BR>
<!-- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx -->

<p><font size="3"><extr>ShowDeviceSummaryList</extr></font></p>

<p><font size="3"></font>&nbsp;</p>

<p><font size="3"></font>&nbsp;</p>
</body>
</html>

```

The `device_summary.html` file is just like a standard HTML file with one exception: it has a new pair of tags, `<extr> ... </extr>` which are specific to the EPICenter report server. The EPICenter report server treats everything defined between these tags as Tcl code. The report server executes this code dynamically when it generates the report (upon a user request through the browser).

You can use any standard Tcl constructs between these tags, and you can also use methods defined in the “`extr`” package (`extr.tcl`). `extr.tcl` defines a set of methods to obtain information from the EPICenter software database. Appendix C “EPICenter Database Views,” defines a number of database views that contain information that may be useful in creating reports.

In addition, you can define new methods in any Tcl file in the `<epicenter_install_dir>/user/reports/tcl` directory, and use those methods inside the HTML file within the `<extr>` and `</extr>` tags.

A number of reports have been defined for use as examples. Look at the various HTML files to understand how `<extr>` tags are used within HTML files.

Look at the methods defined in the file `user/reports/tcl/examples.tcl` for details on using these methods to generate the data that will become a part of the generated report. Some utility methods have been provided in `commands.tcl` to help parse the result that comes back from the EPICenter software API.

In general, the Tcl methods defined here will generate well-formatted HTML. Everything between the `<extr>` and `</extr>` tags is replaced by HTML code generated by the embedded Tcl code. Using this method, you can generate lots of new reports quickly, and without disrupting the EPICenter software server.

## Adding a User-Defined Report to the Reports Menu

To add a new user-defined report to the report menu, simply place the HTML file into the `<epicenter_install_dir>/user/reports/html/userdefined` directory. The EPICenter server automatically creates a link on the Reports menu for files in the userdefined directory. It will use the report file names as the report names. They will appear below the heading **User Defined Reports** at the bottom of the left-hand panel of the Reports page.

The file names must conform to two restrictions:

- They must use `.html` as the extension. `.htm` is not supported.
- The file name may not contain spaces.

If you want to create a set of hierarchical reports, you can create a subdirectory under the userdefined directory to contain subordinate HTML files that should not have a direct link from the Reports menu.



*If you put files into the `userdefined` directory that were originally in the `<epicenter_install_dir>/user/reports/html` directory, be sure you also copy the report stylesheet (`reportstylesheet.css`) into the `userdefined` directory.*

## Debugging

The EPICenter software provides a mechanism that you can use to debug any Tcl procedures you write.

Debugging is done in the Tcl shell that is shipped with the EPICenter software. You do not need to view your reports through a browser to debug them.

To debug Tcl code you have created or modified, follow these steps:

- 1 Run `<epicenter_install_dir>/tcl/bin/tclsh83d.exe` to invoke the Tcl shell.
- 2 Change to the `<epicenter_install_dir>/user/reports/tcl` directory.
- 3 Execute the command `source extrdebug.tcl` within the Tcl shell.

This sets up the Tcl packages required, and also establish a connection with the database using the EPICenter software external API.

- 4 Now, run the command `extr: :ExecuteExtrCommand` which parses your Tcl code and displays the resulting HTML file.

`ExecuteExtrCommand` takes the following arguments:

- The name of the HTML file that will generate the report.

- A string containing the parameter that should be available to the HTML file. The values for the parameters can be obtained in the various Tcl methods using `extr::GetSessionParam`

You must ensure that the appropriate environment variables are set to allow access to Tcl. These should be set as follows:

For Windows NT, set variables as follows:

```
TCL-LIBRARY=<epicenter_install_dir>/tcl/lib/tcl8.3
PATH=$PATH:<epicenter_install_dir>/tcl/bin
```

For Solaris, set the `LD_LIBRARY_PATH` variable as follows:

```
LD_LIBRARY_PATH=<epicenter_install_dir>/tcl/lib/tcl8.3
```

## Useful Methods for Debugging

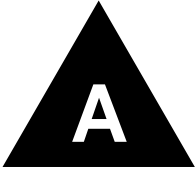
The `GetFromDB`, `ExecuteExtrCommand` and `GetSessionParam` methods are defined as follows:

```
#####
# extr::GetFromDB
#     Used to make any SQL query to the database through the
#     Epicenter server. The result is a SQL result table,
#     formatted within HTML tags.
#
# Arguments
#     A string representing an SQL query.
#
# Returns
#     The result table of an SQL query embedded in HTML tags.
#
#####

#####
# extr::ExecuteExtrCommand
#     This is the public method typically used during debugging.
#     When a user wants to run an HTML file through the reporting
#     engine, to generate dynamic html, s/he calls this method.
#     Users will need to use this method only during debugging.
#
# Arguments
```

```
#      filePath  This is the fully specified path of where to
#                find the HTML file that has embedded <extr> tags.
#      params    A string containing params and their values that
#                should be available to the procedures in the HTML files.
#                The parameters are specified as in HTML. i.e. the param
#                is a string of type "param1=value1&param2=value2"
#
# Returns
#      The result of executing the command. Typically this is parsed HTML.
#
#####

#####
# extr::getSessionParam
#      Used in reports to get the value of a specific parameter
#      that was passed into the reporting system.
#      This method, along with GetFromDB form the two most
#      commonly used routines by users of the reporting system.
#      The params passed into ExecuteExtrCommand are available
#      through this method.
#
# Arguments
#      param     A param name. This should be one of the params
#                that was passed into ExecuteExtrCommand.
# Returns
#      The value of the parameter. Returns "" if param was not defined.
#
#####
```



# Troubleshooting

---

This appendix describes how to:

- Resolve problems you may encounter that are related to the EPICenter server
- Resolve problems you may encounter while using the EPICenter client application

## Troubleshooting Aids

If you are having problems with EPICenter, there are several things you can do to help prevent or diagnose problems.

### Enable the Java Console

To facilitate problem diagnosis, you can attempt to duplicate the problem with the Java Console enabled. To enable the Java Console, do the following:

- 1 From the Windows **Start** menu, select **Programs**, then **Java Plug-in Control Panel** and launch the Control Panel.  
Under Solaris, run `controlPanel1`, which resides in the `netscape/j2pi` directory.
- 2 On the **Basic** page, click the **Show Java Console** check box.
- 3 Click **Apply**.

The next time you launch the EPICenter client, the Java Console will start automatically.



*Running with the Java Console displayed may affect the performance of the EPICenter client.*

There is limited space for Java Console messages; once the console log file is filled, no more messages will be recorded. If you are trying to duplicate a problem, clear the Java Console log file periodically by clicking the **Clear** button at the bottom of the window.

You can close the Java Console by clicking the **Close** button at the bottom of the window. However, once it is closed, it can only be restarted by closing and restarting the browser.

### **Restart the Browser and Clear Browser Cache**

If you have experienced problems with an EPICenter applet, restarting the browser is recommended to ensure that conditions are re-initialized. In addition, it is a good idea to clear the browser's cache.

## **EPICenter Client Initialization**

**Problem: Browser is unable to connect to the EPICenter server.**

Verify that the EPICenter Server process is running.

Verify that the server is running on the specified port. You can use the Port Configuration utility to determine the port on which the EPICenter server is running.

To run the Port Configuration utility, run the program from the Windows **Start** menu: Select **Programs**, then **EPICenter 3.1**, then **Port Configuration**.

For more information on this utility, see Appendix B, "EPICenter Utilities."

**Problem: Browser does not bring up the Login page.**

Verify the version of the browser you are using. See the system requirements in Chapter 1 or see the *ExtremeWare EPICenter SE Release Note and Quick Start Guide* shipped with the software.

**Problem: Client software loads and allows login, but data is missing or other problems arise.**

Clear your browser's cache, exit the browser, and restart it. This frequently clears up miscellaneous start-up problems in the client.

In Internet Explorer, clear cache by selecting **Internet Options** under the **Tools** Menu, then clicking **Delete Files** under the Temporary Internet Files section of the **General** tab.

In Netscape, clear cache by selecting **Preferences** under the **Edit** menu, then click on **Advanced**, and select **Cache**. Click each of the separate buttons for clearing memory cache and disk cache.

**Problem: After running for a while, the display disappears in some applets.**

Under some conditions the Java Plug-in can run out of memory. If you are running with the Java Console enabled, you may see "Out of Memory" errors recorded in the console log file. To alleviate this problem, you can grant the plug-in more memory through the Java Plug-in Control Panel.

**1 From the Windows Start menu, run the Java Plug-in Control Panel.**

Under Solaris, run `ControlPanel`, which resides in the `netscape/j2pi` directory.

The Plug-in Control Panel should appear with the **Basic** page displayed.

**2 In the Java RunTime Parameters field, enter the following without any embedded spaces:**

**`-Xmxnnnm`**

*nnn* is the maximum number of megabytes of virtual memory available to the plug-in.

For example, entering `-Xmx128m` allows the plug-in to use up to 128 MBytes of virtual memory, and should prevent out-of-memory problem.



*For Solaris, due to a bug in the Control Panel, you must enter the command **without** the initial **x**, and **with a space** between the small **x** and the memory specification, as follows:*

**`-mx nnnm`**

*Note that Sun could fix this problem at any time. Check with Sun Microsystems or look at the Extreme Networks web site to determine whether the problem has been fixed.*



**Problem: Colors in client interface are incorrect (Windows NT or Windows 2000).**

The Color Palette must be set for 65536 colors (or True Color). If your display is set for only 256 colors, the colors in the left-hand panel (the Navigation Toolbar) and the EPICenter applets themselves may be incorrect.

To change the color palette, double-click the **Display** icon in the **Control Panel**, select the **Settings** tab, and use the drop-down list in the **Color Palette** field to select the appropriate setting.

**Problem: No prompt is given for the plug-in upgrade when a Netscape client is started, and the plug-in is not installed.**

When starting a Netscape 4.76 client for the first time, the upgrade prompt may not appear even though the Java 1.3.1 Plug-in is not installed. As a result, an error message will be displayed in the panel where the Navigation Toolbar icons should appear.

This may occur if the environment variable `NPX_PLUGIN_PATH` is set, even if it points to a previous version of the plug-in. You can unset the variable, restart the browser, and the prompt will appear. You can also download the plug-in by returning to the EPICenter start-up page and selecting **Get Java PlugIn**.

## EPICenter Server Issues

**Problem: Cannot talk to a specific switch.**

Verify that the switch is running ExtremeWare software version 2.0 or later.

Ping the switch's IP address to verify availability of a route. Use the `ping` command from a MS DOS or Solaris command shell.

Verify that the read and write community strings used in the EPICenter match those configured on the switch.

**Problem: ExtremeWare CLI or ExtremeWare Vista changes are not reflected in EPICenter.**

Verify that the switch is running ExtremeWare software version 2.0 or later.

From the Inventory Manager, click **Sync** to update the information from the switch. This refreshes the switch specific data, validates the SmartTrap rules, and ensures that the EPICenter server is added as a trap receiver (Extreme switches only).

If the problem persists, verify that the EPICenter workstation has been added in the list of trap destinations on the given switch:

- 1 Telnet to the switch.
- 2 Log in to the switch.
- 3 Type `show management` to verify that the system running the EPICenter is a trap receiver.

An Extreme switch can support a maximum of 6 trap destinations in ExtremeWare 2.0, and up to 16 trap destinations with ExtremeWare 4.1 or greater. If EPICenter is not specified as a trap destination, then no SmartTraps are sent, and the data is not refreshed. If you need to remove a trap receiver, use the command:

```
config snmp delete trapreceiver <ipaddress>
```

For details, see the *ExtremeWare Software User Guide*.

**Problem: Need to change polling interval, SNMP request time-out, or number of SNMP request retries.**

You can change the default values for the SNMP polling interval, the SNMP request time-out, or the number of SNMP request retries, through the Administration applet, Server Properties page. You must stop and restart the EPICenter server to have your changes take effect.

See Chapter 15 for information on the EPICenter Administration applet. See Chapter 3 for instructions on stopping and starting the EPICenter server.

**Problem: Need to change the Telnet or HTTP port numbers used to communicate with managed devices.**

You can change the port numbers for all managed switches through the Administration applet, Server Properties page. You must stop and restart the EPICenter server to have your changes take effect.

See Chapter 15 for information on the EPICenter Administration applet. See Chapter 3 for instructions on stopping and starting the EPICenter server.

**Problem: Telnet polling messages can fill up a device's syslog file.**

For switches running older versions of ExtremeWare (prior to 6.0), the EPICenter server uses telnet polling to get EDP topology and ESRP information. However, each telnet login and logout message is logged to the switch's log file, and will eventually fill up the log.

You can disable EDP and ESRP logging through the EPICenter Administration applet, Server Properties page. This will also avoid the syslog messages.

See Chapter 15 for information on the EPICenter Administration applet. See Chapter 3 for instructions on stopping and starting the EPICenter server.

**Problem: Traps may be dropped during a trap "storm."**

The EPICenter server limits its processing of traps in order to be able to reliably handle trap storms from a single or multiple devices. EPICenter limits its trap processing to 21 traps every 28 seconds from an individual device, and a total of 275 traps every 55 seconds system-wide. Any traps that occur beyond these limits will be discarded, but will be noted in the log.txt file.

This situation is rare and should be considered abnormal behavior in the managed devices. If it does occur, the managed devices should be diagnosed and corrected.

## VLAN Manager

**Problem: Multiple VLANs have the same name.**

A VLAN is defined by the name, its tag value, and its protocol filter definition. EPICenter allows multiple VLANs of the same name if one of the defining characteristics of one VLAN is different from the other.

**Problem: Multiple protocols have the same name.**

EPICenter allows multiple protocols of the same name if one of the defining characteristics of one protocol is different from the other.

**Problem: Created a new protocol in VLAN Manager, but the protocol does not appear on any switch.**

When a new protocol is created, it is stored in the EPICenter database. EPICenter only creates the protocol on a switch when the new protocol is used by a VLAN on that switch.

**Problem: Can only access one of the IP addresses on a VLAN configured with IP multinetting.**

EPICenter does not currently support IP multinetting.

**Problem: Configuration fails when attempting to configure a VLAN with a modified protocol definition.**

EPICenter does not have a mechanism to modify protocols. When a VLAN is configured through EPICenter to use a protocol that does not exist on the switch, the protocol is first created on the switch. However, if a protocol with the same name but a different definition already exists on the switch, the operation will fail.

**Problem: An untagged port has disappeared from its VLAN.**

Check to see if the port has been added as an untagged port to a different VLAN. In EPICenter, adding an untagged port to a VLAN automatically removes the port from its previous VLAN if the port was an untagged port, and the new and old VLANs used the same protocol. This is different behavior from the ExtremeWare CLI, where you must first delete the port from the old VLAN before you can add it to the new VLAN.

## Alarm System

**Problem: Device is in a fault state that should generate a trap, and an alarm is defined to detect it, but the alarm does not appear in the EPICenter Alarm Log.**

There are several possible reasons this can occur. Check the following:

- Make sure that the alarm is enabled.
- Check that the device is in your alarm scope.
- Check that SNMP traps are enabled on the device.

- For a non-Extreme device, make sure you have set EPICenter as a trap receiver on the device (see Chapter 8).
- For an RMON alarm, make sure you have RMON enabled on the device.

**Problem: The “Email to:” field is greyed-out in the Actions tab of the New Alarm Definition dialog**

You need to specify an e-mail server in order to send e-mail. Click the **Settings...** button next to the **Email to** field to set up your mail server.

**Problem: An RMON rule is defined to monitor a counter variable, and to cause an alarm when the counter exceeds a certain value. The counter has exceeded the threshold value but no alarm has occurred.**

There are several things to check:

- Make sure the RMON rule and the alarm definition are set up correctly
- If the value of the counter was already above the threshold value when you set up the RMON rule, and you have the Sample Type set to Absolute, no alarm will ever be generated. This because the value must fall below the Falling Threshold value before the before another Rising Threshold trap will be sent, and this will never occur. You should consider using the Delta Sample Type instead.

**Problem: When creating an RMON rule in the RMON Rule Configuration window, the MIB variable I want to use is missing from the list of variables displayed when I click “Lookup...”**

The MIB Variable list displays only the MIBs shipped with the EPICenter software. In addition, within those MIBs the variable list will not display variables that are indexed by an index other than (or in addition to) ifIndex. You can still use variables that do not appear in the Lookup... list, but you must type the complete OID into the MIB Variable field, in numeric notation. If the variable is a table variable, you will need to append the specific index and apply the variable to each target device, one at a time.

**Problem: A program specified as an action for an alarm (in the Run Program field) does not get executed. It includes output to the desktop among its functions.**

If you are running the EPICenter server as a service, you must specifically tell it to allow output to the desktop. To do this you must stop and restart the EPICenter server, as follows:

- 1 In the Services properties window, select **EPICenter 3.1 Server** and click **Stop**. (To find the Services window, from the Start menu select Settings, then Control Panel, the double-click the Services icon).
- 2 When the **EPICenter 3.1 Server** service has been stopped, select it again and click the **Startup....** This displays a pop-up window where you can specify start-up options.
- 3 In the lower part of the window, in the **Log On As:** area, click the box labeled **Allow Service to Interact with Desktop**. Then click **OK**.

After the EPICenter server restarts, the program you have specified as an alarm action should execute correctly.

## ESRP Manager

**Problem: None of the member VLANs of an ESRP group are appearing in the ESRP Manager applet.**

Make sure that all members of the ESRP group use the same election algorithm. If there is an election algorithm mismatch between any of the ESRP-enabled switches in any of the ESRP-enabled VLANs in the ESRP group, this causes a misconfiguration scenario, and ESRP will not function. As a result, none of the members of the ESRP group will appear in the ESRP Manager applet.

**Problem: Some of the switches in an ESRP-enabled VLAN are missing from the ESRP Manager applet.**

Make sure that the Hello Timer (ESRP Timer) is set to the same interval for all ESRP-enabled switches. If there is a timer mismatch, ESRP will not function correctly, and the ESRP Manager applet will not be able to detect ESRP switch neighbors that are not being managed by the EPICenter software.

## Inventory Manager

**Problem: Discovery hangs if a large number of addresses is specified.**

A very large discovery can cause the discovery process to hang because there is insufficient memory available to the browser to process the number of addresses. This is a limitation of the browser.

To recover, restart the browser. Then split your discovery request into multiple requests that involve a smaller number of addresses. Discovery displays a warning if your request involves more than 1500 IP addresses. The actual number of addresses you can successfully poll will depend on the amount of memory available at that time in your browser (browser memory is shared among the various running applets).

**Problem: Multiple switches have the same name.**

This is because the sysName of those switches is the same. Typically, Extreme Networks switches are shipped with the sysName set to the type of the switch “Summit48,” “Summit1i,” “Alpine3808,” and so on, depending on the type of switch. You should change these names to unique names using the ExtremeWare CLI or ExtremeWare Vista.

**Problem: Discovery does not display MAC address for some devices in discovery results list. In addition, may not add the device to inventory (primarily happens with workstations).**

If the MAC address is not found in the first instance of ifPhysAddress, it is not displayed in the discovery results table. However, when the device is selected to be added to the EPICenter inventory, the Inventory applet searches all the ifPhysAddress entries for the device, and will use the MAC address found in this manner. If no MAC address is found in any ifPhysAddress entry, the device will not be added to the EPICenter database.

**Problem: Attempted to add a switch in the Inventory Manager after rebooting the switch, and received an “SNMP not responding” error.**

If a switch has recently been powered on, it may take some time (a number of minutes) before the device is completely initialized. This will be especially true of chassis devices with many blades, or devices with a large number of VLANs configured on the device. If the device has not completed its initialization, the Inventory Add process may return an error. You can simply wait until the device has finished initializing and try the Add function again.

# ExtremeView

**Problem: For a device selected under Status, the Device Information panel shows incorrect information, and the device image is not displayed correctly.**

This can be caused by a device IP address that is in conflict with another device on the network (a duplicate IP address). Remove the problem device from the EPICenter inventory, and add it in again with the correct IP address.

**Problem: While looking at a device in ExtremeView, the device view was suddenly replaced by the top-level ExtremeView page.**

This will happen if another EPICenter user removes the device from the database while you are viewing it. If you are running with the Java Console enabled you may see an error message indicating the device has been removed (as long as your console log has not been filled up).

**Problem: When device information is not displayed completely (for example, only a generic image is displayed) no messages explaining the problem seems to appear.**

These types of messages for ExtremeView are displayed as error messages in the Java Console error log. These messages are really informational errors, but must be displayed as errors in order to appear under the normal Java Console settings. To see these messages, you must be running the Java Console (see “Enable the Java Console” on page A-1). Also, there must still be room left in the console log, as it stops displaying messages when it fills up.

**Problem: After initiating a switch reboot from the switch configuration page in ExtremeView, the browser times out with an error.**

You can initiate a switch reboot from the Switch configuration page in the ExtremeView applet. However, because the switch is rebooting, it does not respond to the browser’s forms submission, and the browser will time out and report an error (Error: 504) instead of refreshing the configuration page. Once the switch has successfully finished rebooting, you can select it again in the Component Tree and the page will refresh correctly.



# Grouping Manager

## **Problem: Cannot import users from NT Domain Controller**

The ExtremeWare EPICenter Server must be running with permissions that enable it to get user information from a Domain Controller. To verify and change permissions for the Web Server, do the following:

- 1 From the **Start** menu, highlight **Settings**, pull right, and click on the **Control Panel**. This displays the Control Panel folder.
- 2 Double-click on **Services** to display the Services Properties window.
- 3 Highlight “EPICenter 3.1 Server” in the list of services, and click the **Startup...** button.
- 4 In the “Log On As:” section of the pop-up window, enter the account name and password for a user who has the appropriate permissions to access the Domain Controller.
- 5 Stop and restart the Web Server service to have the new user logon take effect.

# Printing

## **Problem: When printing a topology map or a report, the browser can appear to freeze.**

Printing a report or a topology map can cause the browser utilization to become very high (approaching 100%) and can spool a very large amount of memory. There is no current solution other than to wait, and the process will eventually finish.

## **Problem: After printing an HTML report, the Navigation Toolbar is not refreshed.**

Although printing from the browser is not supported in most EPICenter applets, you can print the HTML reports using the browser print button. However, you should first click in the panel where the report is displayed to ensure that only that panel will be printed. If you print without doing this, the Navigation Toolbar may not be refreshed. If this happens you will need to refresh the browser manually.

# Topology

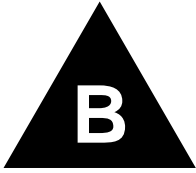
**Problem: Created a new view with the Auto Populate option turned on. However, no devices are placed on the map.**

The Auto Populate option causes new devices to be added to your view, on the appropriate map, when they are added to the EPICenter inventory database. Therefore, if you create a new view *after* you have added devices to the inventory, any devices already in inventory are not added to the map.

Note that if you updated from an earlier version of the EPICenter software (or ExtremeWare Enterprise Manager 2.0 or 2.1) this means that none of devices that were already in the old database are added to the map.

**Problem: Links get “stuck” when nodes are dragged to new positions on the map.**

Normally when you drag a node to a new position on the map, the link is repositioned to run directly as a straight line between the nodes it connects. However, very infrequently (due to a toolkit error) the links may get “stuck” at the node’s previous position, causing the link to turn into a two-part angled line instead of a straight line. You can eliminate this problem by closing and restarting your browser.



# EPICenter Utilities

---

This appendix describes several utilities and scripts shipped with the ExtremeWare EPICenter software:

- The DevCLI utility, that can be used to add and delete devices from the EPICenter database using the `devcli` command
- The Inventory Export scripts, that can be used to extract information from the EPICenter inventory and output it to the console or to a file
- The SNMPCLI utility, that can be used to inspect the contents of device MIBs
- The Port Configuration utility, a Windows-only utility you can use to change the ports used by the EPICenter server

## The DevCLI Utility

The DevCLI utility allows you to add devices to and remove devices from an EPICenter database using a command line statement, rather than through the EPICenter client user interface. You can add devices individually or in groups, and can specify arguments such as community strings and login and passwords for both the EPICenter server and the devices. You can specify a list of devices in a file and have them added in a single operation.

The DevCLI is useful for updating the EPICenter inventory database quickly when large numbers of devices are added or removed, or if changes occur frequently. It can also be useful when you want to duplicate the device inventory across multiple installations of the EPICenter server.

## Using the DevCLI Commands

The utility is located in the root EPICenter install directory, by default `\epc3_1` or `/opt/epc3_1` (in a UNIX environment).

The DevCLI utility supports the following two commands:

- `devcli add <options>` to add a device.

For example, to add device 10.205.0.99 to the EPICenter database on the local host, using the default device user name and password, enter the following command at the prompt:

```
devcli add -a 10.205.0.99
```

- `devcli del <options>` to remove a device.

For example, to remove the same device from the EPICenter database, enter the command:

```
devcli del -a 10.205.0.99
```

These commands support a set of options for specifying device information such as passwords and community strings, as well as information about the EPICenter server, such as host name or IP address, port, and user name and password. You can also specify multiple IP addresses in a file to have them added or removed as a group, as long as they all use the same user name, password, and community strings.

Table B-1 specifies the options you can use with these commands:

**Table B-1:** DevCli command options

Option	Value	Default
-a	Device IP address. This option can be specified more than once.	None
-c	Cisco enable password.	""
-d	Device password.	""
-f	Input file name. This specifies an ascii file that contains a list of IP addresses, one per line. No other information can be included in this file.  This option can be specified more than once.	None
-g	Device group to which devices should be added. Case sensitive. The device group must already exist.	Default

**Table B-1:** DevCli command options

Option	Value	Default
-l	(Letter l) User name to use for device login	admin
-n	EPICenter server port number	80
-p	EPICenter user password	""
-r	Read community string (only needed for adding devices; not needed for deleting them).	public
-s	EPICenter server hostname or IP address	localhost
-u	EPICenter user name	admin
-w	Write community string (only needed for adding devices; not needed for deleting them).	"private"

Options such as the user login names and passwords and community strings, apply to all devices specified in the command. You can specify multiple devices in one command as long as they use the same options. If you have devices with different access parameters, you must add or delete them in separate commands. The exception is when removing devices, you don't need to specify community strings, so you can remove multiple devices in a single command even if their community strings are different.

Most options default to the values equivalent to those used by default on Extreme Networks devices or in the EPICenter software.

You can specify only one EPICenter server (database) in a command. If you want to add the same devices to multiple EPICenter databases, you must use a separate command for each server. The command by default adds or removes devices from the EPICenter database running on the local host at port 80.

## DevCLI Examples

The following examples illustrate the usage of these commands.

- To add a device with IP address 10.205.0.99 to the EPICenter database running on server `snoopy` on port 81, with EPICenter login "master" and password "king," enter the following command:

```
devcli add -a 10.205.0.99 -s snoopy -n 81 -u master -p king
```

- To add two devices (10.205.0.98 and 10.205.0.99) to the EPICenter database on the local host, with read community string “read” and write community string “write,” enter the following command:

```
devcli add -a 10.205.0.98 -a 10.205.0.99 -r read -w write
```

- To delete a set of devices specified in the file “devList.txt” with device login “admin2” and password “purple,” enter the following command:

```
devcli del -f devList.txt -l admin2 -d purple
```

The file `devList.txt` must be a plain ASCII text file containing only IP addresses, such as:

```
10.205.0.95  
10.205.0.96  
10.205.0.97
```

## Inventory Export Scripts

There are three scripts you can run to export information about the devices or occupied slots known to the EPICenter inventory. The scripts let you export information on devices known to a single EPICenter installation, on slots known to a single EPICenter installation, or on devices known to multiple EPICenter servers. The information will be output in comma-separated (CSV) format suitable for importing into a spreadsheet.

- For a device report, the information reported includes the device name and type, IP address, location, serial and board numbers. If you use the multi-server version of this report, the name of the EPICenter server that manages the device will also be included.
- For a slot report, it includes the device name and IP Address, slot number, slot name and slot type, and the serial number of the blade in the slot.

## Using the Inventory Export Scripts

The three scripts are located in the EPICenter `user\scripts\bin` directory under the EPICenter install directory (by default `\epc3_1` under Windows, or `/opt/epc3_1` under Solaris). You must have the `user\scripts\bin` directory as your current directory in order to run these scripts.

There are three inventory export scripts you can use:

- `inv.bat <options>` exports device information from the EPICenter database.

For example, to export device information to file `devinfo.csv`, enter the following commands at the prompt:

```
cd epc3_1\user\scripts\bin
inv.bat -o devinfo.csv
```

- `slots.bat <options>` exports slot information from the EPICenter database.

For example, to run the command as user “user1,” and export slot information to file `slotinfo.csv`, enter the command:

```
cd epc3_1\user\scripts\bin
slots.bat -u user1 -o slotinfo.csv
```

- `msinv.bat <options>` exports device information from the databases of multiple EPICenter servers. You must provide a list of EPICenter servers in a file.

For example, the following command exports device information from the databases of EPICenter servers listed in file `servers.txt` (in the `scripts\config` directory) to file `alldevinfo.csv`, without prompting for a password:

```
cd epc3_1\user\scripts\bin
msinv.bat -d -o alldevinfo.csv -s ..\config\servers.txt
```

The server file defaults to the file `servers.txt` in the `user\scripts\config` directory. You can edit this file to include the names or IP addresses of the servers where the EPICenter server and databases are running. You can also provide your own file. The format of the file entries are:

```
<servername or IP>:<port>
```

For example:

```
iceberg:80
10.2.3.4:81
```

Table B-2 specifies the options you can use with these commands:

**Table B-2:** Inventory script command options

Option	Value	Default
-d	None If present, the command will use the default EPICenter password (“”) and will not prompt for a password.	If -p option not present, prompts for password
-o	Name of file to receive output. If you don’t specify a path, the file will be placed in the current directory ( <code>user\scripts\bin</code> ).	output written to console (stdout)

**Table B-2:** Inventory script command options

Option	Value	Default
-p	EPICenter user password	""
-u	EPICenter user name	admin
-s	For the <b>msinv.bat</b> command only: Name (and path) of file containing EPICenter server list	<epc_install_dir>\user\scripts\config\servers.txt

## Inventory Export Examples

The following examples illustrate the usage of these commands.

- To export slot information to the file `slotinventory.csv` from the EPICenter database whose login is “admin123” and password is “sesame” enter the following command:

```
slots.bat -u admin123 -p sesame -o slotinventory.csv
```

This will not prompt for a password, and will output the results to the specified file.

- To export device information to the console, after prompting for a password, enter the following command:

```
inv.bat
```

This command will login with the default user name (admin), will prompt for the password, and will output the results to the console.

- To export device information to the console, using the default login and default password, enter the following command:

```
inv.bat -d -o output.csv
```

This command will login using the default user name (admin) and the default password, and will output the results to the file `output.csv` in the `user\scripts\bin` directory.

- To export device information from the EPICenter databases on the multiple servers, edit the `servers.txt` file in the `user\scripts\config` directory, then enter the following command:

```
msinv.bat -d -o devices.csv -s serverlist2.txt
```

This command logs in to each of the EPICenter servers specified in the file `serverlist2.txt`, using the default login and password, and output the device information from these servers to the file `devices.csv`. The `devices.scv` file is created in the `user\scripts\bin` directory.



## The SNMPCLI Utility

The SNMPCLI utility provides three basic SNMP query capabilities, that can be used to access the values of MIB objects kept by the SNMP agents of the devices you are managing. Accessing these variable may be helpful in diagnosing problems with a device or its configuration, if its behavior as seen through the EPICenter software is not as expected.

Use of this utility assumes you are familiar with SNMP MIBs, and can determine the OID the variable you want to retrieve, as well as the meaning of the results that are returned.

## Using the SNMPCLI Utility

The three scripts are located in the EPICenter `user\scripts\bin` directory under the EPICenter install directory (by default `\epc3_1` under Windows, or `/opt/epc3_1` under Solaris). You must have the `user\scripts\bin` directory as your current directory in order to run these scripts.

The SNMPCLI utility supports the following three commands:

- `snmpcli snmpget <options>` returns the value of a specified OID.

For example, to get the value of the object (the variable `extremePrimaryPowerOperational` in the Extreme Networks MIB) whose OID is `.1.3.6.1.4.1.1916.1.1.1.10.0` on the device at `10.205.0.99`, enter the following command:

```
snmpcli snmpget -a 10.205.0.99 -o .1.3.6.1.4.1.1916.1.1.1.10.0
```

- `snmpcli snmpnext <options>` returns the value of the next OID (subsequent to the OID you specify) in the MIB tree.

For example, you can use this command to get the value of the object whose OID is `.1.3.6.1.4.1.1916.1.1.1.10.0` on the device at `10.205.0.99`, by entering the following command:

```
snmpcli snmpnext -a 10.205.0.99 -o .1.3.6.1.4.1.1916.1.1.1.10
```

- `snmpcli snmpwalk <options>` returns the value of the entries in a table.

For example, to get the value of the entries in the `extremeFanStatusTable`, which is OID `.1.3.6.1.4.1.1916.1.1.1.9` on the device at `10.205.0.99`, enter the following command:

```
snmpcli snmpget -a 10.205.0.99 -o .1.3.6.1.4.1.1916.1.1.1.9
```

Table B-3 specifies the options you can use with these commands:

**Table B-3:** SnmpCli command options

Option	Value	Default
-a	Device IP address. This option can be specified more than once. This option is required.	None
-o	Object Identifier (OID) of the MIB object whose value you want to retrieve, or that is the starting point for the values you want. This option is required.	None
-r	Read community string	public
-t	Timeout value for SNMP request, in milliseconds.	500 ms

## SNMPCLI Examples

The following examples illustrate the usage of these commands.

- To retrieve the values of the `extremePrimaryPowerOperational` and `extremeRedundantPowerStatus` variables for the Extreme Networks device with IP address 10.205.0.99, with read community string “purple” and a timeout of 1000 ms, enter the following command:

```
SnmpCli snmpget -a 10.205.0.99 -r purple -t 1000 -o
.1.3.6.1.4.1.1916.1.1.1.10.0 -o .1.3.6.1.4.1.1916.1.1.1.11.0
```

This returns the following:

```
IP Address: 10.205.0.99
Read community string: purple
Timeout(ms): 1000
OUTPUT:
OID: .1.3.6.1.4.1.1916.1.1.1.10.0 ; VALUE: 1
OID: .1.3.6.1.4.1.1916.1.1.1.11.0 ; VALUE: 1
```

- To retrieve the values from the `extremeFanStatusTable` variables for the Extreme Networks device with IP address 10.205.0.99, with the default read community string (public) and a default timeout, enter the following command:

```
SnmpCli snmpwalk -a 10.205.0.99 -o .1.3.6.1.4.1.1916.1.1.1.9
```

This returns the following:

```
IP Address: 10.205.0.99
Read community string: public
```

```

Timeout(ms) : 500
OUTPUT:
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.1.1 ; VALUE: 1
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.1.2 ; VALUE: 2
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.1.3 ; VALUE: 3
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.2.1 ; VALUE: 2
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.2.2 ; VALUE: 2
OID: .1.3.6.1.4.1.1916.1.1.1.9.1.2.3 ; VALUE: 2

```

## Port Configuration Utility

The Port Configuration utility is a stand-alone utility that runs on the Windows NT 4.0 or Windows 2000 platform.

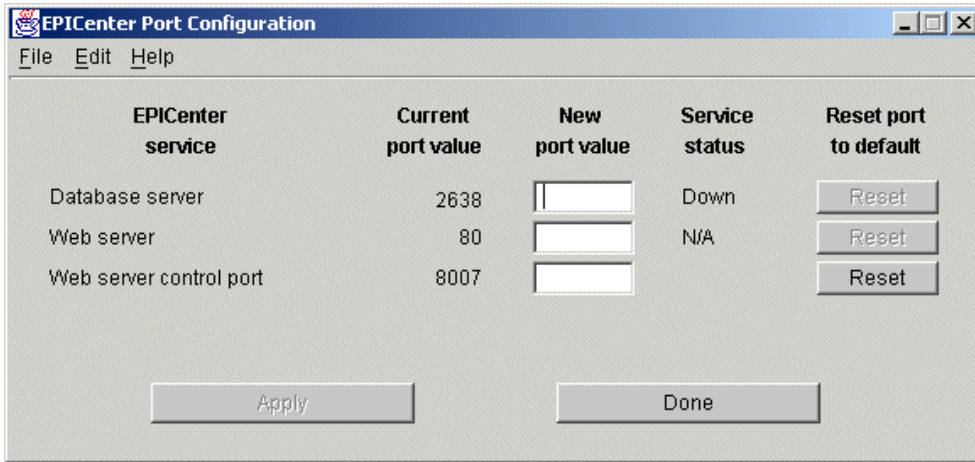
The EPICenter Port Configuration utility provides a way for an EPICenter administrator to change some of EPICenter's logical TCP/IP port numbers, in the event that there are conflicts between these port numbers and those used by other software products running on the same system. Because these port conflicts may prevent EPICenter from running, the port configuration capability needs to be accessible outside of EPICenter. The Port Configuration application runs on the same system as the EPICenter Database Server and Web Server.

You can run the utility from the **Programs** menu. You do not need to shut down the ExtremeWare EPICenter services (Web Server or database) in order to change the port configurations. However, the new configurations will not take effect until you restart the affected server(s).

To run the Port Configuration utility, do the following:

- 1 Run the program from the Windows **Start** menu:  
Select **Programs**, then **EPICenter 3.1**, then **Port Configuration**.

The EPICenter Port Configuration window appears, as shown in Figure B-1.



**Figure B-1:** ExtremeWare EPICenter Port Configuration Utility

- 2 Type in new port values for the ports you want to change.

You can use the standard Windows Cut, Copy, and Paste functions from the Edit menu, or use the keyboard shortcuts ([Ctrl]+X, [Ctrl]+C, and [Ctrl]+V) to move values among the fields.

The **Apply** button is enabled when there is text in some edit field.

- 3 Click **Apply** to record the settings you have entered.

Click the **Reset** button for a specific port to reset that port to its default value. The **Reset** button for a field is enabled when the corresponding values in the “Current port value” field is something other than the default.

Click **Done** when you have finished making and applying changes. Any new text in the edit fields, that has not been applied, is discarded.

The utility checks to see if it can open the requested new port number(s). If the new port number is in use, the utility reports this fact and asks if you want to keep the new value anyway.

- 4 To have the new port settings take effect, restart the server(s) whose ports you have changed.

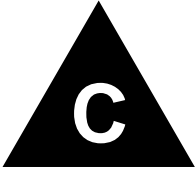
Changes do not take effect until the corresponding service is stopped and restarted.

However, after applying the new values, the entries under “Current port value” are updated. This information can be misleading if you have not yet restarted the corresponding services. In particular, if you dismiss and re-run the Port Configuration

utility before you restart the affected services, the “Current port value” fields will reflect the changed values which are not yet in effect.

If the servers are running as system services, you can restart your system, or stop and restart the servers using the Services utility from the Windows Control Panel.

If the EPICenter servers are not running as NT system services, you must manually stop and restart the servers.



# EPICenter Database Views

This appendix describes the most useful views in the EPICenter database for the purpose of creating Tcl scripts for use in Reports or as Alarm actions.

The variables in these views can be accessed using the methods defined in the file `extr.tcl` found in the `<epicenter_install_dir>/user/reports/tcl` directory, where `<epicenter_install_dir>` is the directory where the EPICenter software resides. They can also be used by external applications.

## Device Report View

**Table C-1:** EPICenter Database Device Report View

<b>Extreme_Device_Report</b>		
Extreme_Device_Report is a database view that has one row for each device that is being managed by the EPICenter server. Some of the columns in the view contain Extreme specific information. If a device is not an Extreme device, the Extreme specific columns contain empty values, such as an empty string.		
<b>Column Name</b>	<b>Column Type</b>	<b>Description</b>
device_id	integer	A database unique id identifying a device. (This column can be used as the primary key.)
enterprise_oid	integer	The enterprise id, e.g. 1916 for extreme networks.

<b>Column Name</b>	<b>Column Type</b>	<b>Description</b>
system_oid	string	The partial system oid, e.g. "1916.2.7" for Summit 24.
device_group_name	string	The EPICenter device group name of the device group in which this device belongs to.
ip	string	The IP address of the device, e.g. "10.205.0.1".
mac	string	The MAC address of the device, e.g. "00:e0:2b:00:5e:00".
sysName	string	The sysName of the device.
sysDescription	string	The sysDescription of the device.
sysLocation	string	The sysLocation of the device.
sysContact	string	The sysContact of the device.
read_write_community	string	The read/write SNMP community string.
read_only_community	string	The read-only SNMP community string.
clilogin	string	The CLI/Telnet login name of the device.
clipassword	string	The CLI/Telnet password for the above login.
status	string	The status of the device: "operational", "marginal", or "not responding".
boot_time	string	The boot time of the device in GMT, e.g. "2000-11-13 21:05:28".
hardware_id	string	The vendor specific hardware id of the device (not all device have a hardware id).
reserved	string	Reserved field, only used by a Cisco device to store Cisco specific information.
ip_forwarding	string	"true" if the device is a router, "false" otherwise.
current_software	string	The software version of the device.
<i>the following columns are Extreme specific</i>		
primary_image	string	The primary software image version on the device, e.g. "4.1.9 (2)".

<b>Column Name</b>	<b>Column Type</b>	<b>Description</b>
secondary_image	string	The secondary software image version on the device, e.g. "6.1.5b20".
image_after_reboot	string	The image to use after a switch reboot: "primary", "secondary", "neither", or "unknown".
board_number	string	The hardware board number.
other_numbers	string	Other hardware board numbers.
serial_numbers	string	The serial number of the device.
fan_status	string	The status of all fans on the device, e.g. "fan 1 OK; fan 2 OK; fan 3 OK".
selected_configuration	string	The currently selected configuration on the device: "primary" or "secondary".
power_status	string	The status of the primary power supply of the device: "fan/temperature alarm", "not present", "OK", "failed", or "unknown".
rps_status	string	The status of the redundant power supply of the device: "fan/temperature alarm", "not present", "OK", "failed", or "unknown".
voltage	string	The voltage of the power supplied to the device: "110 AC", "220 AC", "48 DC", or "unknown".
temperature	integer	The current operating temperature of the device in centigrade, e.g. 48.
default_gateway	string	The default gateway of the device, e.g. "10.205.0.1".



# Interface Report View

**Table C-2:** EPICenter Database Interface Report View

<b>Extreme_Interface_Report</b>		
<p>Extreme_Interface_Report is a database view that has one row for each interface that is being managed by the EPICenter server. Some of the columns in the view contain Extreme specific information. For interface that is not on an Extreme device, the Extreme specific columns are empty, such as an empty string.</p>		
<b>Column Name</b>	<b>Column Type</b>	<b>Description</b>
device_id	integer	A database unique id identifying a device. (This column and the ifIndex column below can be used as the primary key.)
ifIndex	integer	The ifIndex of the interface. (This column and the device_id column above can be used as the primary key.)
ifType	integer	The ifType of the interface.
ifPhysicalAddress	string	The ifPhysicalAddress (MAC address) of the interface.
ifDescription	string	The ifDescription of the interface.
conigured_media	string	The configured media information of the interface, e.g. "100BaseTX, full duplex".
actual_media	string	The actual media information of the interface, e.g. "10BaseTX, half duplex".
auto_negotiation	string	The status of auto negotiation of the interface: "true" or "false".
admin_status	string	The admin status of the interface: "enabled" or "disabled".
operation_status	string	The operational status of the interface: "active", "ready", or "failed".
<i>the following columns are Extreme specific</i>		
IP_Address	string	The IP address of the device, to which this interface belongs to, e.g. "10.205.0.31".

<b>Column Name</b>	<b>Column Type</b>	<b>Description</b>
port_number	string	The Extreme specific representation for the interface, e.g. "1:3" or "12".
redundant_media	string	Specify which media is active, for interfaces without any redundant media, the value is always "primary". For interfaces with redundant media, the value can be either "primary or redundant".
algorithm	string	When the interface is in load-sharing mode, specify the port sharing algorithm: "none", "port based", "address based", "round robin", or "unknown".
member_port_number	string	When the interface is in port sharing mode, specify all members of the port sharing group, e.g. "1:1, 2:1, 2:2, 2:3".
unsignedIPInt	integer	The IP address number of the device, to which the interface belongs. This is the same IP address as in the IP_Address column, except that the address is represented using a unsigned 32-bit integer: e.g. the IP Address "10.205.0.1" is represented as 181207041.

## Database Event Log View

**Table C-3:** EPICenter Database Event Log View

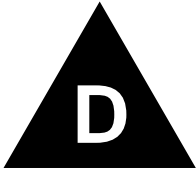
<b>Event_Log_View</b>		
Event_Log_View is a database view that shows the EPICenter alarm event log, but making the data from each column into a human readable format.		
<b>Column Name</b>	<b>Column Type</b>	<b>Description</b>
event_log_id	integer	An unique id for the event log entry. (This column can be used as the primary key.)
event_timeticks	integer	The time when the event happened. This time is shown as milliseconds since 1970-01-01 00:00:00 GMT.

<b>Column Name</b>	<b>Column Type</b>	<b>Description</b>
event_time	string	The time when the event happened. This is the same time as the event_timeticks column except that the time is shown as a string. E.g. "2000-10-21 14:20:21 GMT"
event_source	string	The IP (and the ifIndex, if appropriate) of the source, from which the event is generated. E.g. "10.205.0.31", "10.205.0.31, port 2:1", or "10.205.0.2, ifIndex 10".
event_type	string	The type of the event, e.g. "SNMP Trap: Cold Start"
event_ip	string	The IP address of the source, from which the event is generated. E.g. "10.205.0.31"
event_generic	integer	For SNMP trap based event, this is the generic field of the trap.
event_specific	integer	For SNMP trap based event, this is the specific field of the trap.
event_enterprise	string	For SNMP trap based event, this is the enterprise field of the trap.
event_varbinds	string	For SNMP trap based event, this is the varbinds of the trap.
unsignedIPInt	integer	The IP address number of the device, from which the event originates. This is the same IP address as in the event_ip column, except that the address is represented using a unsigned 32-bit integer: e.g. the IP Address "10.205.0.1" is represented as 181207041.

# Database Alarm Log View

**Table C-4:** EPICenter Database Alarm Log View

<b>Alarm_Log_View</b>		
Alarm_Log_View is a database view that shows the EPICenter alarm log, but making the data from each column into a human readable format.		
<b>Column Name</b>	<b>Column Type</b>	<b>Description</b>
alarm_time	integer	The time when the event happened. This time is shown as milliseconds since 1970-01-01 00:00:00 GMT. This time is unique for all alarm logs. (This column can be used as the primary key.)
alarm_name	string	The name of the alarm definition, to which this alarm instance belongs.
alarm_category	string	The alarm category as defined in the alarm definition.
source	string	The IP (and the ifIndex, if appropriate) of the source, from which the event that triggered the alarm is generated. E.g. "10.205.0.31", "10.205.0.31, port 2:1", or "10.205.0.2, ifIndex 10".
severity	string	The severity of the alarm as defined in the alarm definition.
msg	string	The alarm message as defined in the alarm definition.
acked	byte	A byte value in hexadecimal representation specifying whether the alarm is ack'ed or not, 00 – not ack'ed; 01 – ack'ed.
event_log_id	integer	The event log id of the event that triggers the alarm.
unsignedIPInt	integer	The IP address number of the device, from which the event that triggers the alarm originates. This is the same IP address as in the event_ip column, except that the address is represented using a unsigned 32-bit integer: e.g. the IP Address "10.205.0.1" is represented as 181207041.



# Event Types for Alarms

---

This appendix describes the events that can be detected through the EPICenter Alarm System:

- SNMP traps
- RMON Rising and Falling traps
- EPICenter events

## SNMP Trap Events

**Table D-1:** SNMP Trap Events

<b>Event</b>	<b>Definition</b>	<b>ExtremeWare Version</b>
Cold Start	This trap indicates that the device is rebooted by power recycling. Extreme switches always send out this trap after a reboot.	All
Warm Start	Trap indicates that the device has been rebooted without power recycling. An Extreme switch never sends out this trap.	All
Link Up	This trap indicates that a port becomes active from previous inactive state.	All
Link Down	This trap indicates that a port becomes inactive from previous active state.	All

**Table D-1: SNMP Trap Events**

<b>Event</b>	<b>Definition</b>	<b>ExtremeWare Version</b>
Authentication Failed	This trap indicates that a SNMP request with an invalid community string is issued to the device.	All
Overheat	Extreme Networks proprietary trap.  This trap indicates that the on board temperature sensor has reported an overheat condition. This indicates the temperature has reached the Overheat threshold. The switch will continue to function until it reaches its shutdown threshold. The system will then shutdown until the unit has sufficiently cooled such that operation may begin again. A cold start trap will be issued when the unit has come back on line. This trap is sent repetitively every 30 seconds until the temperature goes back to normal.	All
Fan Failed	Extreme Networks proprietary trap.  This trap indicates one or more of the cooling fans inside the device has failed. A fan OK trap will be sent once the fan has attained normal operation. This trap is sent repetitively every 30 seconds until all the fans are back to normal condition.	All
Fan OK	Extreme Networks proprietary trap.  This trap indicates that a fan has transitioned out of a failure state and is now operating correctly.	All
Invalid Login	Extreme Networks proprietary trap. This trap indicates that a user attempted to login to console or by telnet but was refused access due to incorrect user name or password. The trap is issued after three consecutive failure of log in.	All
Power Supply Failed	Extreme Networks proprietary trap. This trap indicates that one or more sources of power have failed. Presumably a redundant power-supply has taken over. This trap is sent repetitively every 30 seconds until all the power supplies are back to normal condition.	All
Power Supply OK	Extreme Networks proprietary trap. This trap indicates that one or more previously bad sources of power have come back to life without causing the device to restart.	All

**Table D-1: SNMP Trap Events**

<b>Event</b>	<b>Definition</b>	<b>ExtremeWare Version</b>
Redundant Power Supply Failed	Extreme Networks proprietary trap. This trap indicates that the attached redundant power supply device is indicating an alarm condition. This trap is sent repetitively every 30 seconds until the redundant power supply is back to normal condition.	All
Redundant Power Supply OK	Extreme Networks proprietary trap. This trap indicates that the attached redundant power supply device is no longer indicating an alarm condition.	All
ESRP State Changed	Extreme Networks proprietary trap. This trap indicates that the ESRP state (master or slave) of a VLAN has changed on the device.	6.0 or later
EDP Neighbor Added	Extreme Networks proprietary trap. A new neighbor has been discovered through the Extreme Discovery Protocol (EDP).	6.1 or later
EDP Neighbor Removed	Extreme Networks proprietary trap. No EDP updates have been received from this neighbor within the configured timeout period, and this neighbor entry has been aged out by the device.	6.1 or later
BGP Established	The BGP Established event is generated when the BGP FSM enters the ESTABLISHED state.	6.1.9 or later
BGP Backward Transition	The BGPBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.	6.1.9 or later
Ping Probe Failed	Generated when a probe failure is detected when the corresponding pingCtlTrapGeneration object is set to probeFailure(0) subject to the value of pingCtlTrapProbeFailureFilter. The object pingCtlTrapProbeFailureFilter can be used to specify the number of successive probe failures that are required before this notification can be generated.	6.1.9 or later
Ping Test Failed	Generated when a ping test is determined to have failed when the corresponding pingCtlTrapGeneration object is set to testFailure(1). In this instance pingCtlTrapTestFailureFilter should specify the number of probes in a test required to have failed in order to consider the test as failed.	6.1.9 or later
Ping Test Completed	Generated at the completion of a ping test when the corresponding pingCtlTrapGeneration object is set to testCompletion(4).	6.1.9 or later

**Table D-1: SNMP Trap Events**

<b>Event</b>	<b>Definition</b>	<b>ExtremeWare Version</b>
OSPF Interface State Change	An ospflfStateChange trap signifies that there has been a change in the state of a non-virtual OSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup).	6.1.9 or later
OSPF Virtual Interface State Change	An ospfVirtIfStateChange trap signifies that there has been a change in the state of an OSPF virtual interface. This trap should be generated when the interface state regresses (e.g., goes from Point-to-Point to Down) or progresses to a terminal state (i.e., Point-to-Point).	6.1.9 or later
OSPF Neighbor State Change	An ospfNbrStateChange trap signifies that there has been a change in the state of a non-virtual OSPF neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full). When an neighbor transitions from or to Full on non-broadcast multi-access and broadcast networks, the trap should be generated by the designated router. A designated router transitioned to Down will be noted by ospflfStateChange.	6.1.9 or later
OSPF Virtual Neighbor State Change	An ospfVirtNbrStateChange trap signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).	6.1.9 or later
OSPF Interface Config Error	An ospflfConfigError trap signifies that a packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. Note that the event optionMismatch should cause a trap only if it prevents an adjacency from forming.	6.1.9 or later
OSPF Virtual Interface Config Error	An ospfVirtIfConfigError trap signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. Note that the event optionMismatch should cause a trap only if it prevents an adjacency from forming.	6.1.9 or later



**Table D-1: SNMP Trap Events**

<b>Event</b>	<b>Definition</b>	<b>ExtremeWare Version</b>
OSPF Interface Authentication Failure	An ospflfAuthFailure trap signifies that a packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	6.1.9 or later
OSPF Virtual Interface Authentication Failure	An ospfvirtlfAuthFailure trap signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	6.1.9 or later
OSPF Interface Receive Bad Packet	An ospflfRxBadPacket trap signifies that an OSPF packet has been received on a non-virtual interface that cannot be parsed.	6.1.9 or later
OSPF Virtual Interface Receive Bad Packet	An ospfvirtlfRxBadPacket trap signifies that an OSPF packet has been received on a virtual interface that cannot be parsed.	6.1.9 or later
OSPF TX_Retransmit	An ospfTxRetransmit trap signifies than an OSPF packet has been retransmitted on a non- virtual interface. All packets that may be retransmitted are associated with an LSDB entry. The LS type, LS ID, and Router ID are used to identify the LSDB entry.	6.1.9 or later
OSPF Virtual Interface TX Retransmit	An ospfvirtlfTxRetransmit trap signifies than an OSPF packet has been retransmitted on a virtual interface. All packets that may be retransmitted are associated with an LSDB entry. The LS type, LS ID, and Router ID are used to identify the LSDB entry.	6.1.9 or later
OSPF Originate LSA	An ospfOriginateLsa trap signifies that a new LSA has been originated by this router. This trap should not be invoked for simple refreshes of LSAs (which happens every 30 minutes), but instead will only be invoked when an LSA is (re)originated due to a topology change. Additionally, this trap does not include LSAs that are being flushed because they have reached MaxAge.	6.1.9 or later
OSPF Max_Age LSA	An ospfMaxAgeLsa trap signifies that one of the LSA in the router's link-state database has aged to MaxAge.	6.1.9 or later
OSPF LSDB Overflow	An ospfLsdbOverflow trap signifies that the number of LSAs in the router's link-state database has exceeded ospfExtLsdbLimit.	6.1.9 or later

**Table D-1: SNMP Trap Events**

<b>Event</b>	<b>Definition</b>	<b>ExtremeWare Version</b>
OSPF LSDB Approaching Overflow	An ospfLsdbApproachingOverflow trap signifies that the number of LSAs in the router's link-state database has exceeded ninety percent of ospfExtLsdbLimit.	6.1.9 or later
Health Check Failed	Extreme Networks proprietary trap. The CPU HealthCheck has failed	6.1.5 or later
CPU Utilization Rising Threshold	Extreme Networks proprietary trap. CPU Utilizations Rising trap is generated when the value of extremeCpuAggregateUtilization touches/crosses extremeCpuUtilRisingThreshold.	6.2 or later
CPU Utilization Falling Threshold	Extreme Networks proprietary trap. CPU Utilization Falling Trap is generated when the extremeCpuAggregateUtilization falls below 80% of the extremeCpuUtilRisingThreshold.	6.2 or later

## RMON Rising Trap Events

This trap indicates that the value of the MIB variable being monitored has risen to or above the rising threshold value. RMON rules need to be configured on a device for it to send out this trap. See “Event Configuration” in Chapter 5 for more information.

## RMON Falling Trap Events

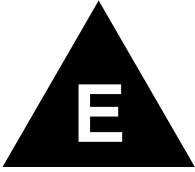
This trap indicates that the value of the MIB variable being monitored has fallen to or below the falling threshold value. RMON rules need to be configured on a device for it to send out this trap. See “Event Configuration” in Chapter 5 for more information.

## EPICenter Events

An EPICenter event is generated by the EPICenter server based on the results of its periodic polling. In some cases, an EPICenter event may result from the same condition that could generate an SNMP or other trap. An EPICenter event has the advantage that it guarantees that the condition will be detected (by polling) even if the corresponding trap is missed.

**Table D-2:** EPICenter Events, Detected Through Polling

Event	Definition
SNMP Unreachable	The EPICenter server generates this event when it fails to communicate with a device following a previously successful communication. In other words, this event is generated when the state of communication with the device transitions from reachable to unreachable.
SNMP Reachable	The EPICenter server generates this event when the state of communication with the device transitions from unreachable to reachable.
Configuration Upload Failed	The EPICenter server generates this event when it fails to upload configuration information from a device. This event occurs <b>ONLY</b> when the upload is attempted from EPICenter, not if it was attempted from Telnet, ExtremeWare Vista or any other method.
Configuration Upload OK	The EPICenter server generates this event when it successfully uploads configuration from a device. This event occurs <b>ONLY</b> when the upload is done from EPICenter, not from Telnet, ExtremeWare Vista or any other method.
Overheat	For Extreme Networks devices only. The EPICenter server generates this event for an Extreme device when it detects a transition from normal temperature to overheat condition on the device. Unlike the SNMP overheat trap event, this event is based on a state transition, and will be generated only once. As an alternative, you can detect an Overheat condition by using the SNMP Overheat trap, which will be generated every 30 seconds until the condition is corrected.
Fan Failed	For Extreme Networks devices only. The EPICenter server generates this event for an Extreme device when it detects, via polling, a transition from fan OK to fan failed condition on the device. Unlike the SNMP Fan Failed trap event, this event is generated only once, based on a state transition. As an alternative, you can detect a Fan Failed condition by using the SNMP Fan Failed trap, which will be generated every 30 seconds until the condition is corrected.
Device Reboot	The EPICenter server generates this event for a device when it detects a device reboot (cold start or warm start). Unlike the cold start or warm start SNMP trap, EPICenter generates this event by polling the device.



# EPICenter Backup

---

This chapter describes the following:

- The EPICenter Alarm Log and Event Log backup files
- The DBVALID command-line database validation utility
- The DBBACKUP command-line database backup utility

## EPICenter Log Backups

Both the EPICenter Event Log and Alarm Log files are kept in tables in the EPICenter database. These tables can contain approximately 50,000 entries.

The EPICenter server checks once every 24 hours to determine if either of these logs has reached its maximum size. When one reaches its maximum, EPICenter moves the oldest 10% of the entries to a backup file, and clears those entries from the table.

The backup files are created in the directory `<install_dir>/user`, where `<install_dir>` is the root directory of the EPICenter install, by default `epc3_1`.

- The Alarm Log is backed up to the file `Alarm_Log.txt`
- The Event Log is backed up to the file `Event_Log.txt`

Each primary backup file is in turn backed up to a secondary file when it reaches its maximum size of approximately 30MB.

- `Alarm_Log.txt` is backed up to the file `Alarm_Log.sav`

- `Event_Log.txt` is backed up to the file `Event_Log.sav`

The primary file is then emptied.

When the primary file becomes full for the second time, the secondary backup file will be overwritten with the new contents of the primary backup file.

If you want to maintain a complete set of log file backups over time, you should save the `*_Log.txt` and `*_Log.sav` files periodically.

## Database Utilities

Sybase database validation and backup utilities are shipped with the ExtremeWare EPICenter software.

The Validation utility validates all indexes and keys on some or all of the tables in the database. The Validation utility scans the entire table and looks up each record in every index and key defined on the table. This utility can be used in combination with regular backups to give you confidence in the security of the data in your database.

The Backup utility makes a backup copy of all data in the database, except for user names and passwords, which are kept in separate files. Backing up your database regularly will ensure that you will not need to re-enter or recreate all the switch, VLAN, Topology, and Alarm information in the event that the database is corrupted or destroyed.

Both database utilities are found in the `<install_dir>\database` directory. `<install_dir>` is the directory where you installed the EPICenter software. Substitute the name of the actual directory for `<install_dir>` when you run these commands.



*In the Solaris environment, you must ensure that the EPICenter database path is set in the `LD_LIBRARY_PATH` environment variable. This should be set to `<install_dir>/database` where `<install_dir>` is the root directory of the EPICenter install, for example `opt/epc3_1`.*

## The Validation Utility

The Validation utility validates all indexes and keys on some or all of the tables in the database. Access the Validation utility from the MS DOS or Solaris command line using the

`dbvalid` command. This convention also allows incorporation into batch or command files.

## Using the DBVALID Command-line Utility

To validate the EPICenter database running under Windows NT, use the command:

```
<install_dir>\database\dbvalid -c "uid=dba;pwd=sql;dbf=<install_dir>\basecamp.db"
```

Under Solaris, use the command:

```
<install_dir>/database/dbvalid -c "uid=dba;pwd=sql;dbf=<install_dir>/basecamp.db"
```

This example assumes a database user ID of `dba`, with password `sql`. These are the defaults used when the database server is installed through the EPICenter installation process. If you have changed your database user ID and password, substitute your actual user ID and password in the command.

`<install_dir>` is the directory where the EPICenter software is installed. Substitute the actual directory name in the command.

This operation should report no errors. If there are errors, the system should be stopped and a backup database copied into place. See “Installing a Backup Database” on page E-6. If there are no backups, the EPICenter software must be re-installed.

**Syntax:**            `dbvalid [switches]`

**Table E-1:** dbvalid Command Switches

Switch	Description
<code>-c "keyword=value; ..."</code>	Supply database connection parameters

## Database Connection Parameters

These are the parameters for the `-c` command-line switch. If the connection parameters are not specified, connection parameters from the `SQLCONNECT` environment variable are used, if set.

**Table E-2:** Database Connection Parameters for `dbvalid` Utility

<code>uid=&lt;user name&gt;</code>	The user name used to login to the database. Default is <b>dba</b> . The user ID must have DBA authority.
<code>pwd=&lt;password&gt;</code>	The password used to login to the database. Default is <b>sql</b> .
<code>dbf=&lt;database_file&gt;</code>	The name of the file that stores the data. This is the file to be validated.

The connection parameters are separated by semicolons, and the entire set must be quoted. For example, under Windows NT, the following validates the EPICenter, connecting as user ID **dba** with password **sql**:

```
<install_dir>\database\dbvalid -c "uid=dba;pwd=sql;dbf=<install_dir>\basecamp.db"
```

## The Backup Utility

The Backup utility makes a backup copy of all data in the database, except for user names and passwords. Access the Backup utility from the MS DOS or Solaris command line using the `dbbackup` command. This convention also allows incorporation into batch or command files.

### The DBBACKUP Command-line Utility

To back up the EPICenter database running under Windows NT, use the command:

```
<install_dir>\database\dbbackup -c  
"uid=dba;pwd=sql;dbf=<install_dir>\basecamp.db" <backup_dir>
```

Under Solaris, use the command:

```
<install_dir>/database/dbbackup -c  
"uid=dba;pwd=sql;dbf=<install_dir>/basecamp.db" <backup_dir>
```

This example assumes a database user ID of `dba`, with password `sql`. These are the defaults used when the database server is installed through the EPICenter installation process. If you have changed your database user ID and password, substitute your actual user ID and password in the command.

`<install_dir>` is the directory where the EPICenter software is installed. Substitute the actual directory name in the command.

`<backup_dir>` is the directory where the backup copy of the database should be stored. Substitute an actual directory name in the command.

This command generates a backup of the database in the specified backup directory. The backup consists of two files, `basecamp.db` and `basecamp.log`. All database files are backed up. These files should be saved so they can be used to replace the original files in the event of a problem.

**Syntax:** `dbbackup [switches] directory`

**Table E-3:** dbbackup Command Switches

Switch	Description
<code>-c "keyword=value; ..."</code>	Supply database connection parameters
<code>-y</code>	Replace files without confirmation

## Database Connection Parameters

These are the parameters for the `-c` command-line switch. If the connection parameters are not specified, connection parameters from the `SQLCONNECT` environment variable are used, if set.

**Table E-4:** Database Connection Parameters for dbbackup Utility

<code>uid=&lt;user name&gt;</code>	The user name used to login to the database. Default is <code>dba</code> . The user ID must have DBA authority.
<code>pwd=&lt;password&gt;</code>	The password used to login to the database. Default is <code>sql</code> .
<code>dbf=&lt;database_file&gt;</code>	The name of the file that stores the data. This is the file to be backed up.



The connection parameters are separated by semicolons, and the entire set must be quoted. For example, under Windows NT, the following backs up the EPICenter database `basecamp.db`, connecting as user ID **dba** with password **sql**:

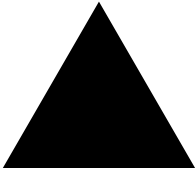
```
<install_dir>\database\dbbackup -c  
"uid=dba;pwd=sql;dbf=<install_dir>\basecamp.db" c:\tmp
```

## Installing a Backup Database

The backup database is named `basecamp.db`, and is kept in the directory you specified when you ran the `dbbackup` command (`c:\tmp` in the example).

To replace a damaged database with the backup copy, follow these steps:

- 1 Shut down the EPICenter software following the instructions for your operating system in the *ExtremeWare EPICenter Software Installation and User Guide*.
- 2 Move or delete the old copy of `basecamp.db` found in the EPICenter installation directory.
- 3 Copy the backup copy of `basecamp.db` to the EPICenter installation directory.
- 4 Restart the EPICenter software following the instructions in the *ExtremeWare EPICenter Software Installation and User Guide* for your operating system environment.



# Index

---

## Numerics

802.1Q tag 13-2, 13-7

---

## A

access levels 1-7, 15-2

Ack button 5-5

### actions

E-mail 5-16

execute script 5-17

for alarms 5-15

run program 5-17

sound alert 5-16

activation key 2-5, 2-8, 2-14

Active Ports (ESRP) 14-5

### Add All button

in Add Relationship to Group 8-18

in Add Resources 8-14

Add Attribute to Resource button 8-11

### Add button

in Add Attribute to Resource 8-21

in Add Relationship to Group 8-18

in Add Resource 8-14

in Alarm Category 5-21

in Alarm Definition 5-10

in Discovery 4-12

in Event Configuration 5-26

in Grouping Manager 8-12, 8-16

in Grouping Manager search 8-25

in Inventory Manager 4-5, 4-15

in VLAN Manager 13-7

Add/Modify Filter button 5-8

### adding

alarm category 5-21

alarm definition 5-10

CPU Utilization rule 5-26

devices 4-14

map background images 12-25

nodes to a map 12-12

protocol filters 13-14

relationships to resource 8-16

resource as child 8-12

RMON rule 5-26

user accounts 15-6

VLANs 13-6

### address ranges

in discovery 4-9

Admin button 3-13

Admin Port 2-8

Administration page 15-4

### Administrator

adding users 15-6

changing password 15-5

default password 15-3

deleting a user account 15-7

ExtremeWare 15-2

modifying users 15-6

Administrator access level 1-8

Enterprise Manager 15-2

### Alarm Browser

from topology map 12-26

Alarm button 5-2

### buttons

Alarm 3-13

Alarm Definition tab 5-9

### alarm events

Extreme proprietary traps 5-4, 5-8

from EPICenter 5-4, 5-8

from SNMP traps 5-8

SNMP traps 5-3

Alarm Log Browser	5-3	Add (Discovery)	4-12
Alarm Log report	16-17	Add (Event Configuration)	5-26
alarm scope		Add (Grouping Manager search)	8-25
select group	5-15	Add (Grouping Manager)	8-12, 8-16
source type	5-14	Add (Inventory Manager)	4-5, 4-15
alarms		Add (Relationship to Group)	8-18
acknowledging	5-5	Add (VLAN Manager)	13-7
actions	5-15	Add All (Add Resources)	8-14
Basic parameters	5-11	Add All (Relationship to Group)	8-18
categories	5-21	Add Attribute to Resource	8-11
creating a filter	5-7	Add/Modify Filter	5-8
Default category	5-21	Admin	3-13
defining	5-8	Alarm	5-2
definition examples	5-18	Archive (Configuration Manager)	6-7
deleting	5-5	Config	3-13
detail view	5-5, 5-6	Config (Configuration Manager)	6-2
E-mail alarm action	5-16	Configure (Inventory Manager)	4-5
execute script action	5-17	Create new decorative map node	12-12
filtering	5-6	Create new device	12-12
predefined	5-3, 5-8	Create new map	12-10
run program action	5-17	Create new map link	12-14
scope	5-13	Create new view	12-10
setting up e-mail	5-17	Cut nodes from map	12-17
sound alert action	5-16	Delete (Alarm Category)	5-21
unacknowledging	5-5	Delete (Alarm Definition)	5-20
variables	5-12	Delete (Alarm System)	5-5
All Device Groups page	4-4	Delete (Event Configuration)	5-36
All ESRPs view	14-2	Delete (Inventory Manager)	4-5
architecture		Delete (VLAN Manager)	13-9
Enterprise Manager software	1-9	Destroy	8-8, 8-11
Archive button (Configuration Manager)	6-7	Detail	5-5
archiving configuration settings	6-7	Discover	4-5
Attribute Name field	8-22	Download (Configuration Manager)	6-8
Attribute Type field	8-22	ESRP	3-13, 14-1
attributes of resources	8-8	EView	3-13
DLCS ID type	8-10, 8-20, 8-22	Filter	5-7
generic type	8-10, 8-19, 8-22	Find (Grouping Manager)	8-8, 8-14, 8-23
IP/subnet type	8-10, 8-20, 8-22	Find IP/MAC	3-13
Attributes tab	8-20	Group	3-13
Authentication Failure Alarms report	16-8	Home	3-12, 16-2
Auto populate view	12-10	Import	8-8, 8-29
placement algorithm	12-4	Incremental (Configuration Manager)	6-10
		Inventory	3-13
		Layout	12-19
		Logoff	3-13
		Modify (Alarm Category)	5-21
		Modify (Alarm Definition)	5-20
		Modify (Event Configuration)	5-35
		Modify (Inventory Manager)	4-5, 4-18
		New	8-8, 8-9
		Paste nodes into map	12-18
		Print map	12-22
		Query	8-26
		Remove (Add Attribute)	8-22
		Remove (Add Resources)	8-14
		Remove (Grouping Manager)	8-15, 8-19
		Remove (Relationship from Group)	8-18
<hr/>			
<b>B</b>			
background map image	12-24		
baseline configuration			
creating	6-12		
Basic Alarm parameters	5-11		
button			
Groups	8-4		
buttons	3-18		
Ack	5-5		
Add (Add Attribute)	8-21		
Add (Add Resources)	8-14		
Add (Alarm Category)	5-21		
Add (Alarm Definition)	5-10		

Remove All (Add Resources)	8-15
Remove All (Relationships from Group)	8-18
Remove Attribute from Resource button	8-11
Remove Filter(s)	5-8
Reports	3-13
Reset (Grouping Manager search)	8-26
RT Stats	3-13, 11-3
Save	8-15, 8-18, 8-19, 8-22
Server (Configuration Manager)	6-16
Settings... (Alarm Definition)	5-17
Sync (Event Configuration)	5-37
Sync (Inventory Manager)	4-5, 4-24
Telnet	3-13
Topology	3-13, 12-2
unack	5-5
Upgrade (Configuration Manager)	6-13
Upload (Configuration Manager)	6-5
Variables... (Alarm Definition)	5-17
Versions (Configuration Manager)	6-15
VLAN	3-13
Zoom map in	12-21
Zoom map out	12-21

## C

categories for alarms	5-21
changing password	
for Administrator	15-5
user	15-8
children of resource	8-7
Children tab	8-12
Cisco device requirements	1-10
client	
browser requirements	1-11, 2-3
installation	2-17
starting	3-5
starting for first time	15-3
columns	
sorting	3-18
community string	
in Discovery	4-10
Component Tree	3-15, 3-16
moving the boundary	3-18
Compress Map menu selection	12-20
Config button	3-13
Config button (Configuration Manager)	6-2
configuration files	
archiving	6-7
download incremental	6-10
downloading	6-8
Configuration Management Log report	16-20
Configuration tab	5-22
Configure button	4-5
conventions	
notice icons, About This Guide	xxiv
text, About This Guide	xxiv
copy (Telnet)	7-5, 7-10

CPU Utilization	
alarm event generation	5-32
event configuration rules	5-23
MIB variable	5-31
Rising Threshold	5-31
rule definition	5-31
rule display	5-24
Sample Type	5-32
Startup Alarm	5-32
Create new decorative map node button	12-12
Create new device button	12-12
Create new map button	12-10
Create new map link button	12-14
Create new view button	12-10
creating	
device groups	4-16
new device node (Topology)	12-12
new topology map	12-10
new topology view	12-10
port groups	4-18
resources	8-9
search task (IP/MAC Finder)	9-4
VLANs	13-6
Critical Alarms Defined report	16-6
Critical Alarms report	16-6
Cut Map Nodes menu selection	12-17
Cut nodes from map button	12-17
cutting map nodes	12-17

## D

database backup utility	E-4
database validation utility	E-2
dbbackup utility	E-4
dbvalid utility	E-2
decorative node	12-6
Default alarm category	5-21
Default device group	4-4
Deflate Nodes menu selection	12-21
Delete button	
in Alarm Category	5-21
in Alarm Definition	5-20
in Alarm System	5-5
in Event Configuration	5-36
in Inventory Manager	4-5
in VLAN Manager	13-9
Delete Map Links menu selection	12-19
Delete Map menu selection	12-16
Delete Map Nodes menu selection	12-18
Delete View menu selection	12-16
deleting	
a user account	15-7
alarm category	5-21
alarm definition	5-20
alarms	5-5
device groups	4-23
Event configuration	5-36

map elements	12-18	setting up for alarms	5-17
map links	12-18	Enterprise Manager	
map view	12-16	architecture	1-9
protocol filters	13-13	client	2-17
submaps	12-16	components	1-8
VLANs	13-9	logging in	3-7
Destroy button	8-8, 8-11	server components	2-2, 3-2
Detail button	5-5	EPICenter telnet	
Detailed ESRP Information view	14-5	from topology map	12-27
Detailed Task View (IP/MAC Finder)	9-7	ESRP	
device		active ports	14-5
download incremental configuration	6-10	All ESRPs view	14-2
download saved configuration	6-8	detailed information view	14-5
modifying information	4-18	election algorithm	14-3
scheduled configuration upload	6-7	Hello timer	14-3
uploading configuration from	6-5	Master switch	14-2
Device Alarms... menu selection	12-26	priority	14-5
Device Browse... menu selection	12-26	state	14-5
Device Discovery set up window	4-9	ToMaster	14-5
device group	8-2	ToSlave	14-5
device groups	4-2	TrackedActivePorts	14-5
creating	4-16	TrackedIPRoutes	14-5
default	4-4	TrackedPings	14-5
deleting	4-23	ESRP button	3-13, 14-1
modifying	4-19	evaluation copy	
Device Inventory r	16-4	updating to full license	2-10
Device Inventory report	16-13	event configuration	5-22
device node	12-4	CPU utilization rule display	5-24
Device Statistics... menu selection	12-27	CPU utilization rules	5-23
device status		other SNMP traps	5-38
Inventory Manager	4-6	RMON rule example	5-34
Device Status report	16-14	RMON rules	5-23
Device Summary report	16-3, 16-4	rule target	5-33
Device Telnet... menu selection	12-27	Event Configuration page	5-22
Devices Not Responding report	16-5	Event Log report	16-19
dialog boxes	3-19	EView button	3-13
Discover button	4-5	Execute script alarm action	5-17
Discovery	1-3, 4-2, 4-8	Expand Map menu selection	12-20
Add button	4-12	Extreme switch	
address range	4-9	updating status	4-24
community string	4-10	Extreme switch requirements	1-10
subnet mask	4-10	ExtremeView	1-5
Discovery Results window	4-11	from topology map	12-27
display mode, real-time statistics	11-9	switch configuration information	10-8
download		switch statistics	10-10
ExtremeWare software image	6-13	switch status	10-3
incremental configuration	6-10	Telnet	1-4
saved device configuration	6-8	ExtremeWare software image	
Download button (Configuration Manager)	6-8	downloading to device	6-13
		specifying current version	6-15
		ExtremeWare Vista	
		from topology map	12-26
<hr/>			
<b>E</b>			
EEM 2.x			
upgrading from	2-3		
election algorithm (ESRP)	14-3		
E-mail			
alarm action	5-16		
<hr/>			
		<b>F</b>	
		Falling Threshold	5-28
		file import	8-29

Filter button	5-7
filtering	
in reports	16-10
resources	8-8, 8-13
Find button	
in Grouping Manager	8-8, 8-14, 8-23
Find IP/MAC button	3-13
Find Map Node... menu selection	12-22

---

## G

group	8-1
Group button	3-13
Groups button	8-4

---

## H

heartbeat check	1-10
Hello Timer (ESRP)	14-3
Home button	3-12, 16-2
host	8-2
HTTP port	2-8
hyper node	12-6
caveats	12-12

---

## I

Import button	8-8, 8-29
import resources	
from NT Domain controller	8-29, 8-36
import source	8-2, 8-3
importing resources	8-28
from file	8-29
from LDAP directory	8-29, 8-30
from NIS	8-29, 8-36
Incremental button (Configuration Manager)	6-10
individual errors graph	11-2
Inflate Nodes menu selection	12-20
installing the client	2-17
installing the server	
as a service (Windows NT)	2-9
under Solaris	2-11
Interface report	16-15
Invalid Login Alarms report	16-7
Inventory button	3-13
Inventory Manager	1-3
adding devices	4-14
Discovery	4-8
Inventory Manager page	4-3
IP address	
modifying for a VLAN	13-12
IP forwarding	13-8
disabling	13-12
enabling	13-12
IP/MAC Address Finder	1-5
IP/MAC Finder	

creating search task	9-4
search results	9-8
tasks list	9-4

---

## L

L2 cloud node	12-5
caveats	12-12
Layout button	12-19
Layout Map menu selection	12-19
LDAP directory, importing from	8-29, 8-30
license key	2-7, 2-14
activation key	2-5
licensing	
obtaining a permanent license	2-5
obtaining an evaluation license	2-4
link (topology)	12-7
deleting	12-18
logging in	3-7
Login page	3-7, 15-4
Logoff button	3-13

---

## M

macros (Telnet)	
Play command	7-11
record/play	7-3
Start Record command	7-11
Stop Record command	7-11
variables	7-5
Manager access level	1-8, 15-2
Map	12-3
auto populate	12-4, 12-10
creating	12-10
map element description panel	12-4, 12-8
map elements	
decorative node	12-6
device node	12-4
hyper node	12-6
L2 cloud node	12-5
link	12-7
submap node	12-5
text node	12-7
map hierarchy tree	12-3
map nodes	
adding	12-12
cutting	12-17
deleting	12-18
laying out	12-19
map properties	12-24
background image	12-24
link text color	12-25
map name	12-24
node gradient background	12-25
node text color	12-25
RMON statistics	12-25

Map Properties... menu selection	12-24
Master switch	14-2
Modify button	
in Alarm Category	5-21
in Alarm Definition	5-20
in Event Configuration	5-35
in Inventory Manager	4-5
in VLAN Manager	13-10
Modify button (Inventory Manager)	4-18
modifying	
alarm category	5-21
alarm definition	5-20
device groups	4-19
device information	4-18
Event Configuration	5-35
IP address for VLAN	13-12
map properties	12-24
user accounts	15-6
VLANs	13-10
Monitor access level	1-8, 15-2

## N

Navigation Toolbar	3-12
Network Summary report	16-2
New button	8-8, 8-9
New Decorative Map Node menu selection	12-12
New Device Map Node menu selection	12-12
New Map Link menu selection	12-13
New Map menu selection	12-10
New Text Map Node menu selection	12-13
New View menu selection	12-10
NIS, importing from	8-29, 8-36
NT Domain Controller, importing from	8-29, 8-36

## P

passwords	
changing for Administrator	15-5
default	15-3
users changing	15-8
paste (Telnet)	7-5, 7-10
Paste Map Nodes menu selection	12-17
Paste nodes into map button	12-18
Play command (Telnet)	7-11
polling	4-3
Port Configuration utility	B-9
port group	8-2
port groups	
creating	4-18
ports	
changing configuration	B-9
correcting conflicts	B-9
removing from VLAN	13-8, 13-11
predefined alarms	5-3, 5-8
Print map button	12-22

Print Map menu selection	12-22
Priority (ESRP)	14-5
protocol filters	13-2, 13-7
adding	13-14
changing in VLAN	13-11
deleting	13-13

## Q

Query button	8-26
--------------	------

## R

RADIUS server	15-3
administering	15-10
changing shared secret	15-11
disabling	15-11
enabling	15-11
Real Time Statistics	1-5
Real-Time Statistics	11-1
from topology map	12-27
graph preferences	11-9, 11-11
individual errors graph	11-2
total errors graph	11-2
utilization graph	11-2
related publications, About This Guide	xxv
Relationship tab	8-19
relationships of resources	8-7
Relationships tab	8-16
Release Notes	xxiii
Remote Authentication Dial In User Service (RADIUS)	1-8
Remove All button	8-15
in Add Relationship to Group	8-18
Remove Attribute from Resource button	8-11
Remove button	
in Add Attribute to Resource	8-22
in Add Relationship to Group	8-18
in Grouping Manager	8-19
remove children from a group	8-15
remove resource from results list	8-14
Remove Filter(s) button	5-8
removing a child resource	8-15
Rename Map menu selection	12-16
Rename View menu selection	12-16
report	
Invalid Login Alarms	16-7
reports	
Alarm Log report	16-17
Authentication Failure Alarms report	16-8
Configuration Management Log report	16-20
creating user-defined	16-21
Critical Alarms Defined report	16-6
Critical Alarms report	16-6
Device Inventory report	16-4, 16-13
Device Status report	16-14

Device Summary report	16-3, 16-4	resynchronize	5-37
Devices Not Responding report	16-5	Rising Threshold	5-28
Event Log report	16-19	rule definition	5-27
filtering	16-10	rule display	5-24
Interface report	16-15	Sample Type	5-28
Network Summary report	16-2	Startup Alarm	5-29
printing	16-20	traps	5-1, 5-3
Resource to Attribute Mapping report	16-16	utilization on map links	12-25
Server State Summary report	16-12	RMON Statistics (Topology)	12-25
SNMP Unreachable Alarms report	16-7	RT Stats button	3-13, 11-3
Unacknowledged Critical Alarms report	16-6	rule	
User to Host Mapping report	16-17	CPU utilization event configuration	5-31
VLAN Summary report	16-15	RMON configuration example	5-34
VLANs report	16-9	RMON event configuration	5-27
Reports button	3-13	target	5-33
Reset button		Run program alarm action	5-17
in Grouping Manager search	8-26	running the client	3-5
resizing			
columns in status display	3-18		
Component Tree	3-18		
resource	8-1	<b>S</b>	
adding as child	8-12	Sample Type (CPU Utilization)	
adding relationships	8-16	Absolute	5-32
attributes	8-3, 8-8	Delta	5-32
children	8-7	Sample Type (RMON)	
Children tab	8-12	Absolute	5-28
creating	8-9	Delta	5-28
deleting	8-11	Save button	8-15, 8-18, 8-19, 8-22
filtering	8-8	scheduled configuration upload	6-7
importing	8-28	scope	
relationships	8-4, 8-7	for alarms	5-13
Relationships tab	8-16	search results	
removing as a child	8-15	Grouping Manager query	8-26
resource details display	8-6	search results (IP/MAC Finder)	9-8
Resource Results list	8-14	search task	
searching for	8-23	creating	9-4
Select Resource to be Added panel	8-13	Searching for a resource	8-23
Resource Results list	8-14	Select All Map Nodes menu selection	12-19
Resource to Attribute Mapping report	16-16	Select Resources to be Added panel	8-13, 8-17
resources		Server button (Configuration Manager)	6-16
description	8-6, 8-10	server installation	
DLCS ID attribute type	8-10, 8-20, 8-22	under Solaris	2-11
filtering	8-13	Server State Summary report	16-12
generic attribute type	8-10, 8-19, 8-22	setting	
IP/subnet attribute type	8-10, 8-20, 8-22	graph preferences (RT Stats)	11-11
name	8-6, 8-10	setting root directory path	6-16
source	8-6	Settings... button (Alarms)	5-17
type	8-6, 8-10	SmartTraps	1-10, 4-2
unique name	8-7	SNMP	4-2
resynchronize (RMON)	5-37	configuring trap events	5-38
Rising Threshold	5-28, 5-31	traps	5-1, 5-3
RMON		SNMP Unreachable Alarms report	16-7
alarm event generation	5-30	software architecture	1-9
configuration	5-22	software components	1-8
event configuration rules	5-23	software licensing	
Falling Threshold	5-28	licensing	2-4
MIB variables for rules	5-28	Solaris	
		server installation	2-11



starting the server	3-4	device node	12-4
stopping the server	3-4	hyper node	12-6
uninstalling the server	2-19	L2 cloud node	12-5
sorting columns	3-18	link	12-7
sound alert alarm action	5-16	map	12-3
Source Name field	8-29	map element description panel	12-4, 12-8
source of resource	8-6	map hierarchy tree	12-3
Start Record (Telnet)	7-11	submap node	12-5
starting the server		text node	12-7
under Solaris	3-4	view	12-3
under Windows NT	3-2	Topology button	3-13, 12-2
Startup Alarm (CPU Utilization)	5-32	Topology views	12-1
Startup Alarm (RMON)	5-29	ToSlave (ESRP)	14-5
State (ESRP)	14-5	total errors graph	11-2
statistics		TrackedActivePorts (ESRP)	14-5
display mode, real-time	11-9	TrackedIPRoutes (ESRP)	14-5
graph preferences (RT Stats)	11-11	TrackedPings (ESRP)	14-5
in ExtremeView	10-10	traps	
individual port real-time	11-7	Extreme proprietary	5-4, 5-8
multi-port real-time	11-3	RMON	5-1, 5-3
real-time	11-1	setting EPICenter to receive	5-38
Status/Detail Information panel	3-16	SNMP	5-1, 5-3
Stop Record (Telnet)	7-11		
stopping the server		<hr/>	
under Solaris	3-4	<b>U</b>	
under Windows NT	3-2	Unack button	5-5
submap node	12-5	Unacknowledged Critical Alarms report	16-6
subnet mask		Undo Map Edit menu selection	12-22
in Discovery	4-10	uninstalling the server	
switch configuration information (ExtremeView)	10-8	under Solaris	2-19
switch polling	4-3	under Windows NT	2-18
switch statistics (ExtremeView)	10-10	unique name of resource	8-7
switch status (ExtremeView)	10-3	untagged ports	13-8
Sync button	4-3, 4-5, 4-24	Unzoom Map menu selection	12-22
in Event Configuration	5-37	updating switch information	4-24
		Upgrade button (Configuration Manager)	6-13
		upgrading	
		from a previous release	2-3, 2-6
		license (evaluation to permanent)	2-5
		upload	
		device configuration	6-5
		scheduled	6-7
		Upload button (Configuration Manager)	6-5
		User	
		ExtremeWare	15-2
		user	8-2
		User Administration page	15-4
		User to Host Mapping report	16-17
		user-defined reports	16-21
		users, adding	15-6
		users, modifying	15-6
		utilities	
		database backup	E-4
		database validation	E-2
		utilization graph	11-2
<hr/>			
<b>T</b>			
tagged ports	13-8		
Telnet	1-4		
copy	7-5, 7-10		
macro variables	7-5		
macros	7-3		
paste	7-5, 7-10		
third-party devices	7-11		
Telnet button	3-13		
terminology, About This Guide	xxiii		
text node	12-7		
TFTP server	6-16		
enabling/disabling	6-16		
Third-Party Device Requirements	1-10		
third-party device support			
Telnet	7-11		
ToMaster (ESRP)	14-5		
topology			
decorative node	12-6		

---

## V

Variables... button (Alarms)	5-17
Versions button (Configuration Manager)	6-15
view (topology)	12-3
viewing	
alarm details	5-5
Virtual LANs. <i>See</i> VLANs	
VLAN button	3-13
VLAN Manager	1-6
VLAN Manager page	13-3
VLAN Summary report	16-15
VLANs	1-6
adding	13-6
adding protocol filters	13-14
adding tagged ports	13-8
adding untagged ports	13-8
criteria	13-2
deleting	13-9
deleting protocol filters	13-13
disabling IP forwarding	13-12
displaying	13-4
enabling IP forwarding	13-12
modifying	13-10
modifying IP address	13-12
remove a port	13-8
removing a port	13-11
VLANs report	16-9

---

## W

wildcards	
in Discovery addresses	4-9
Windows NT	
starting the server	3-2
stopping the server	3-2
uninstalling the server	2-18

---

## Z

Zoom map in button	12-21
Zoom Map In menu selection	12-21
Zoom map out button	12-21
Zoom Map Out menu selection	12-21