Net-Net® EMS
User Guide
Release Version 6.0 4000

Acme Packet, Inc.
71 Third Avenue
Burlington, MA 01803 USA
t 781-328-4400
f 781-425-5077
www.acmepacket.com

Last updated: July 16, 2008
Document Number: 400-0065-60 Rev. 1.0.0

Notices

Contents

About this Guide

The *Net-Net® EMS User Guide* provides the information you need to use Net-Net EMS to manage network elements (NEs) for Acme Packet's Net-Net session border controller. Acme Packet's Net-Net EMS supports all the necessary configuration, fault, performance, and security management functions through a browser-based graphical user interface.

Who is Acme Packet?

Acme Packet enables service providers to deliver trusted, first class interactive communications—voice, video and multimedia sessions—across IP network borders. Our Net-Net family of session border controllers satisfy critical security, service assurance and regulatory requirements in wireline, cable and wireless networks. Our deployments support multiple applications—from VoIP trunking to hosted enterprise and residential services; multiple protocols—SIP, H.323, MGCP/NCS and H.248; and multiple border points—interconnect, access network and data center.

Established in August 2000 by networking industry veterans, Acme Packet is a public company trading on the NASDAQ and headquartered in Burlington, Massachusetts.

Customer Questions, Comments, or Suggestions

Acme Packet is committed to providing our customers with reliable documentation. If you have any questions, comments, or suggestions regarding our documentation, please contact your Acme Packet customer support representative directly or email support@acmepacket.com.

Contact Us

Acme Packet
71 Third Avenue
Burlington, MA 01803 USA
t 781 328 4400
f 781 425 5077
www.acmepacket.com

1 Getting Started

Overview

This chapter contains information you should review before you get started using Net-Net EMS.

Before You Start

This section contains the information you should review before you start the installation process.

Net-Net EMS and Net-Net 4000 SBC Compatibility

You should ensure that the version of Net-Net EMS you are using is compatible with the version of software on the Net-Net 4000 SBCs you plan to manage. The following table lists the released versions of Net-Net 4000 SBC software and indicates compatibility with the Net-Net EMS releases.

	Net-Net EMS Versions										
Net-Net SBC	**1.3**	**2.0**	**2.1**	**2.1.1**	**4.0**	**4.1**	**4.2**	**4.3**	**5.0**	**5.1**	**6.0**
1.00	N	N	N	N	N	N	N	N	N	N	N
1.1.0	N	N	N	N	N	N	N	N	N	N	N
1.2.0	N	N	N	N	N	N	N	N	N	N	N
1.2.1	N	N	N	N	N	N	N	N	N	N	N
1.3.0	Y	N	N	N	N	N	N	N	N	N	N
1.3.1	N	N	N	N	N	N	N	N	N	N	N
2.0.0	N	Y	N	N	Y	Y	Y	Y	Y	Y	Y
2.0.1	N	N	N	N	Y	Y	Y	Y	Y	Y	Y
2.1.0	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y
2.1.1	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
2.2.0	N	N	N	N	Y	Y	Y	Y	Y	Y	Y
4.0	N	N	N	N	Y	Y	Y	Y	Y	Y	Y
4.1	N	N	N	N	N	Y	Y	Y	Y	Y	Y
4.1.1	N	N	N	N	N	Y	Y	Y	Y	Y	Y
4.1.4	N	N	N	N	N	N	N		Y	Y	Y
5.0	N	N	N	N	N	N	N		Y	Y	Y
5.1	N	N	N	N	N	N	N	N	N	Y	Y

	Net-Net EMS Versions										
Net-Net SBC	**1.3**	**2.0**	**2.1**	**2.1.1**	**4.0**	**4.1**	**4.2**	**4.3**	**5.0**	**5.1**	**6.0**
5.1.1	N	N	N	N	N	N	N	N	N	N	Y
5.2	N	N	N	N	N	N	N	N	N	N	Y

Contact your Acme Packet representative if you have questions about compatibility between Net-Net EMS and Net-Net 4000 SBCs.

Minimum Net-Net SBC Configuration

The Net-Net SBCs you plan to manage using Net-Net EMS must have the following information configured in order to be discovered. To verify the minimum configuration for Net-Net SBCs you plan to manage, see the following documentation:

- *Net-Net EMS 4000 Configuration Guide* for details about configuring a Net-Net SBC using the Acme Command Line Interface (ACLI)
- *Net-Net ACLI Reference Guide* to refer to all ACLI commands.

Boot Parameters

Boot parameters specify the information your Net-Net SBC system uses at boot time when it prepares to run applications. The Net-Net SBC system's boot parameters include the Net-Net SBC system's IP address for the management interface (wancom0) and the target name.

Net-Net EMS uses the target name to uniquely identify a Net-Net SBC from among the list of Net-Net SBCs in its Active configuration area. You need to ensure that all Net-Net SBCs you plan to manage, thus discover, with Net-Net EMS have unique target names. Otherwise, a list of Net-Net SBCs, all with the default name acmesystem would appear in the list.

Ensure the following boot parameters have been configured:

- wancom0 IP address and mask
- target name is set to a unique name (do not use the default name acmesystem)

System Configuration Element

You need to ensure the **system-config** element has been configured. This element establishes general system information and settings, for example:

- Contact information for this Net-Net SBC system for SNMP purposes
- Identification of the Net-Net SBC system for SNMP purposes
- Physical location of the Net-Net SBC system for SNMP purposes
- Whether SNMP is enabled on the system
- Whether traps are enabled
- default gateway

For complete details about system configuration, see the *Net-Net 4000 Configuration Guide* and the *Net-Net ACLI Reference Guide*.

SNMP Community Element

You need to ensure the **snmp-community** element is configured. This element defines the NMSes from which the Net-Net SBC system will accept SNMP requests. Specifically, you need to ensure:

- IP address list contains the address of the host upon which EMS server is running. IP address(es) for SNMP communities for authentication purposes.
- Access mode is read-only

Trap Receiver Element

You need to ensure the **trap-receiver** element is configured. This element defines the NMSes to which the Net-Net SBC system sends SNMP traps for event reporting. Specifically, you need to ensure the following:

- IP address is that of the Net-Net EMS server
- Filter level is set to All
- Community name matches the name in the SNMP community element

Instructions Based on Mozilla Firefox 1.06

The instructions in this document are based on Mozilla Firefox 1.06 The instructions are the same for Internet Explorer, except where noted. For example, when connecting to the Net-Net EMS server using the secure login, additional security messages appear.

All screen examples are those from Mozilla Firefox 1.06.

2 Using Net-Net EMS

Introduction

This chapter explains how to use the Net-Net EMS Graphical User Interface (GUI). It explains how to logon to Net-Net EMS, the relationship between Net-Net EMS and the Acme Command Line Interface (ACLI), and contains descriptions of the GUI itself.

About the Relationship with ACLI

The Net-Net EMS provides a a GUI-based approach to managing Net-Net SBCs. It provides the ability to configure and monitor standalone Net-Net SBCs and HA pairs. The ACLI is an administrative interface that communicates with other components of the Net-Net system. The ACLI is a single DOS-like, line-by-line entry interface that you can use to configure and monitor your Net-Net family of products.

You can use the Net-Net EMS to perform almost all the same configuration and monitoring functions that can be performed using the ACLI. (See the *Net-Net ACLI Reference Guide* for more information about using the ACLI.) You can use both interfaces to work with Net-Net SBCs; even switching from Net-Net EMS to login to a Net-Net SBC and use the ACLI.

Basic Workflow

The basic provisioning cycle includes the following:

- Discover a Net-Net SBC configuration.
- Copy the discovered Net-Net SBC configuration to the Inactive configurations area to edit it.
- Edit the inactive copy of the Net-Net SBC configuration.
- Save the edited Net-Net SBC configuration and activate it.

Accessing the Net-Net EMS GUI

You can access the Net-Net EMS GUI by HTTP or HTTPS login, using the following address formats:

http://<*EMS server IP address*>:9090

https://<*EMS server IP address*>:8443

Note: If you want to connect to EMS servers overs a SSL connection, you must have administrator privileges on the client system.

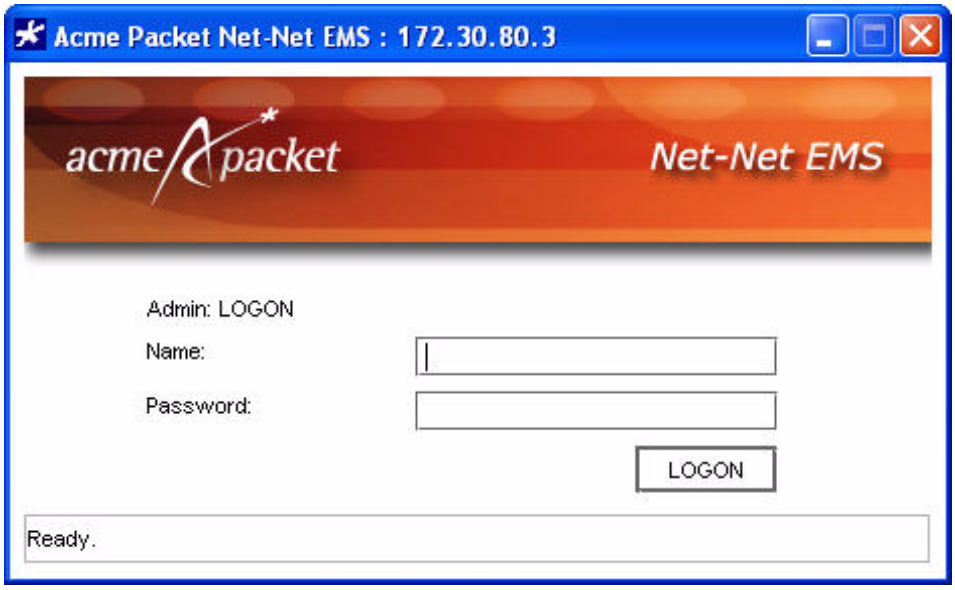
HTTP Login

To access the Net-Net EMS GUI:

1. Open a Web browser.
2. Connect to the Net-Net EMS server using one of the following address formats:

   http://<*EMS server IP address*>:9090

   The Login screen appears.



3. Enter your user name and password and click **LOGON**. (The default username is `admin`, with a default password of `admin`.)

   Go to the *After You Login* section to continue.

HTTPS Login Using Microsoft Internet Explorer 6.0

The process for a secure login using Microsoft Internet Explorer 6.0 includes first accepting or rejecting the security certificate.

To login using Microsoft Internet Explorer 6.0:

1. Open Microsoft Internet Explorer 6.0.
2. Connect to the Net-Net EMS server using the following address format:

   https://<EMS server IP address>:8443

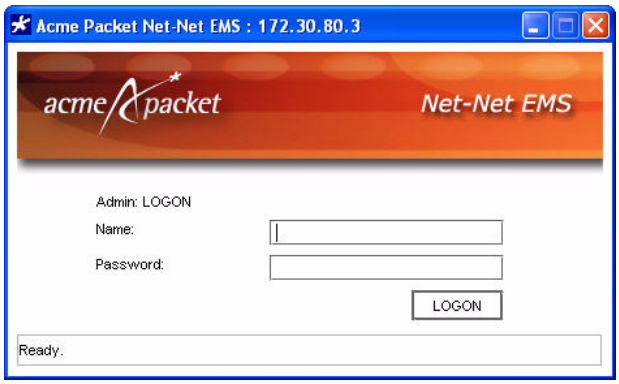
A Security Alert screen appears:

3. Click **Yes** to continue. The Warning - Security screen appears:

4. Click one of the following:

   - `Yes` to accept the security certificate for this session only and to access the Login screen.
   - `No` if you want to reject the security certificate and discontinue the login process.
   - `Always` to permanently accept the security certificate, prevent this screen from appearing, and access the Login screen.
   - `More Details` for more information.

   If you choose `Yes` or `Always`, the Login screen appears.



5. Enter your user name and password and click **LOGON**. (The default username is `admin`, with a default password of `admin`.)

   Go to the *After You Login* section to continue.

HTTPS Login Using Mozilla Firefox 1.0

The process for a secure login using Mozilla Firefox 1.0 includes first accepting or rejecting the security certificate.

To login using Mozilla Firefox 1.0:

1. Open Mozilla Firefox 1.0.
2. Connect to the Net-Net EMS server using the following address format:

   https://<EMS server IP address>:8443

   A Website Certified by an Unknown Authority screen appears:

3. Click one of the following options and click **OK**:
   - `Accept the certificate permanently`
   - `Accept the certificate temporarily for the session` (this window will appear each time you connect to the Net-Net EMS server)
   - `Do not accept the certificate and do not connect to the Web site`

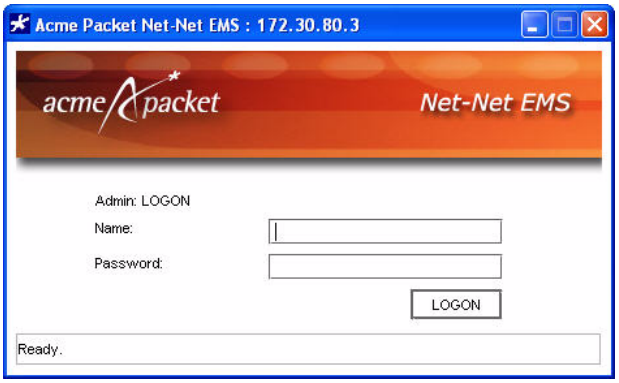
   If you choose to accept the certificate permanently or temporarily, the Security Warning appears:

4. Ensure the checkbox is marked if you want this warning to appear each time you view an encrypted page. If you deselect the checkbox, this warning will not appear again.
5. Click **OK** to clear the Security Warning. The Opening WebNMS.jnlp window appears:

6. Click `Open it with the default application (JNLPFile)` and `Always perform this action when handling files of this type`. This popup will not appear next time you connect.
7. Click **OK**. The Warning - Security screen appears:

8. Click one of the following:
   - `Yes` to accept the security certificate for this session only and to access the Login screen.
   - `No` if you want to reject the security certificate and discontinue the login process.
   - `Always` to permanently accept the security certificate, prevent this screen from appearing, and access the Login screen.
   - `More Details` for more information.

   If you choose `Yes` or `Always`, the Login screen appears.

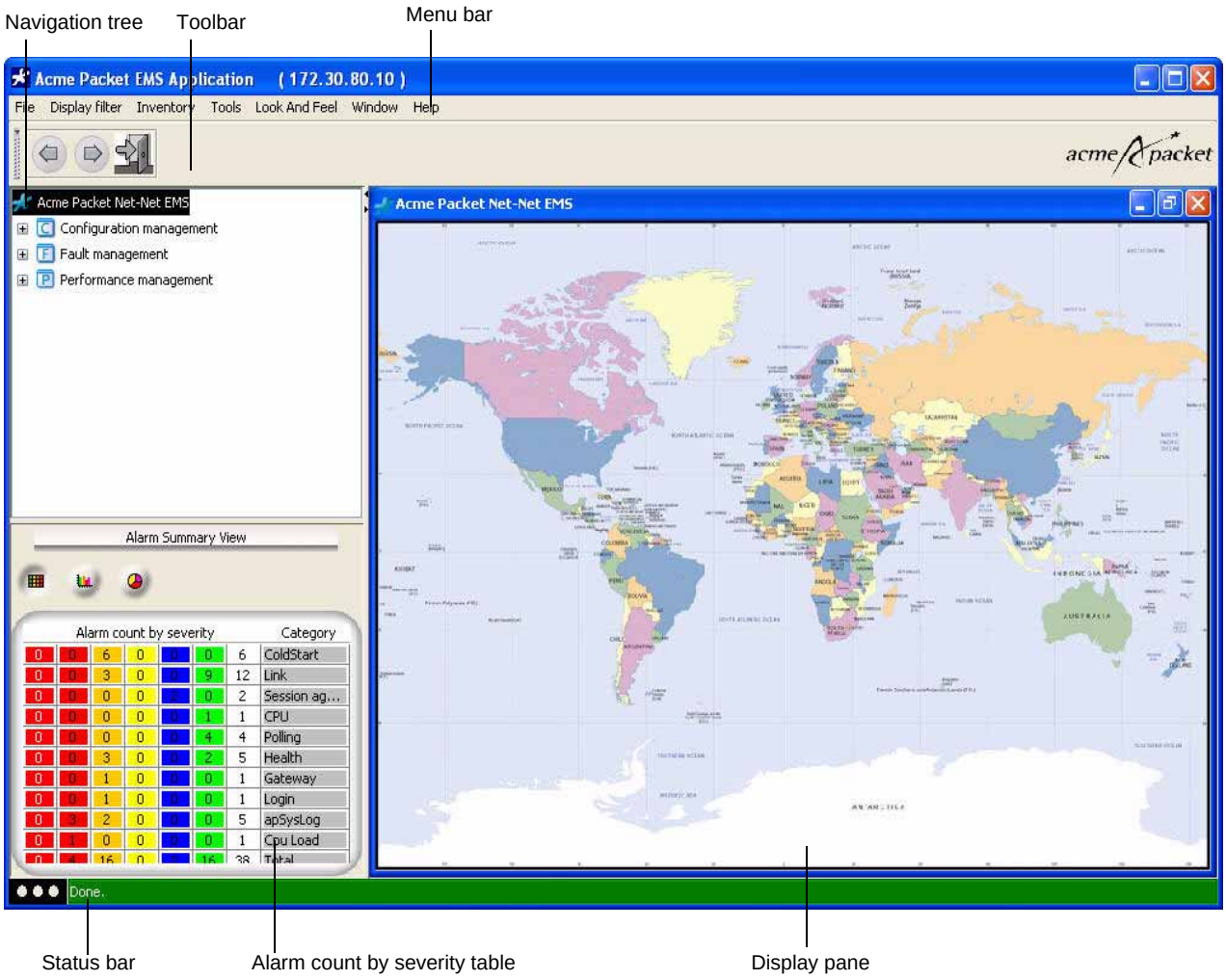


9. Enter your user name and password and click **LOGON**. (The default username is `admin`, with a default password of `admin`.)

   Go to the *After You Login* section to continue.

After You Login

The Acme Packet splash screen appears displaying a progress bar while contacting Net-Net EMS. Next, the top-level Net-Net EMS screen appears:



Overview of Net-Net EMS GUI

The top-level screen is divided into the following areas:

- Menu bar across the top of the window
- Toolbar located under the menu bar
- Navigation tree in the upper left pane
- Alarm count by severity table in the lower left pane
- Display pane on the right side of the window
- Status bar across the bottom of the screen

Menu Bar

The menu bar across the top of the screen contains sets of functions you can perform organized into different categories (menus). You click a menu to access a list of options, from which you then select the function you want to perform. (Many of these functions are also available when you right-click objects in the Navigation tree.)

The menu bar differs from screen to screen based on the functions being performed and on your privileges as a user. For example, the Active configurations module has the additional menu item called Add domain. Other menu items remain constant, such as File, Tools, Look And Feel, Window, and Help.

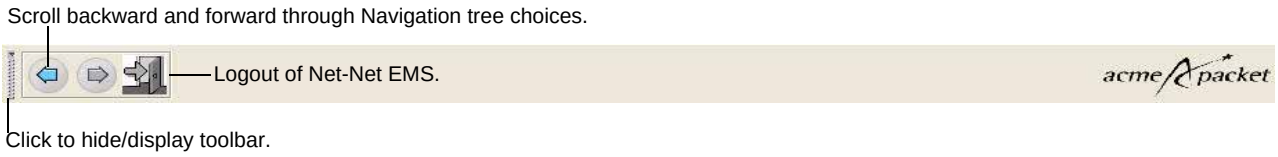
The following table lists the menus and their options; including a brief description

Menu	Menu Item	Description
File	Broadcast message	Send messages to clients connected to the server
	Logout	Exit Net-Net EMS
Save all (Inactive configurations)	Save All	Not currently supported
SD system	Save config	Saves the current configuration to the Net-Net system's last-saved configuration, stored in flash memory
	Activate config	Activates the current configuration on the Net-Net SBC to make it the running configuration
	Save and Activate config	Saves and then activates the configuration
	Copy for Edit	Copies an active configuration to the Inactive configuration area for editing purposes
	Create offline config	Copy an existing active or inactive configuration and modify the existing parameters offline
	Create SD HA node	Create an HA node with two Net-Net SBC configurations
	Configuration Search	Allows you to search for, view, and edit top-level objects

Menu	Menu Item	Description
	Replicate	Replicates selected configuration data from one inactive Net-Net SBC configuration copy to another. Data includes: • account configuration • authentication • capture receiver • SIP manipulation • SNMP community • NTP configuration • session agents • session agent groups • routes • trap receiver
Display filter	Syslog filter	View existing syslog filters and create new filters to apply to the syslog view
Inventory	Inventory details	Access the Inventory window from which you can choose the different standalone Net-Net SBCs or Net-Net SBC pairs for which you want to review inventory data.
Tools	View license	Monitor the number of Net-Net SBCs and the total number of concurrent sessions under management by the Net-Net EMS server
	Runtime administration	Currently not supported by Net-Net EMS
	Security administration	Access the Security Administration tool. Users who have administration privileges can control the different security levels of Net-Net EMS.
	Audit logs	View the audit log. The audit log provides information about the changes made to the copies of Net-Net SBCs while using the Net-Net EMS.
	Client log level	Configure the client log levels. See *Configuring External Trap Receivers* for details about configuring logs.
	Change password	Change the password used to login to Net-Net EMS
	Login Banner	Add text to the login screen as a banner that is displayed when you login to Net-Net EMS
	Task Administration	Access the task administration console
	Operation Administration	Access the operation administration console
Look and Feel	Metal	Apply Metal look to GUI appearance
	CDE/Motif	Apply CDE/Motif look to GUI appearance
	Windows	Apply Windows look to GUI appearance
Window	Show toolbar	Display or hide the toolbar
Help	Help Topics	Access the Net-Net EMS online help
	About Acme Packet EMS	Access Acme Packet version and contact information

Toolbar

The toolbar displays a collection of actions, commands, or control functions. It is placed below the menu bar and consists of various tools for different nodes. A tool tip indicates the operation performed by each tool.

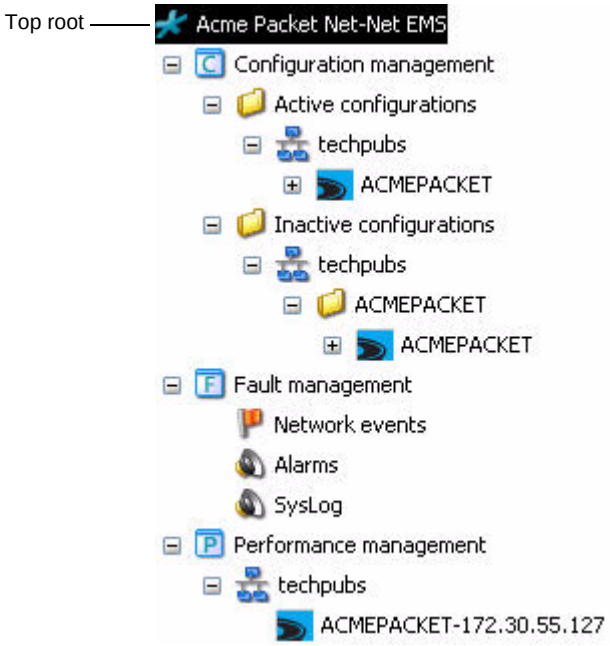


Note: The Show toolbar option located on the Windows menu is not currently supported by Net-Net EMS.

Navigation Tree

The upper section of the left pane is called the Navigation tree. The Navigation tree is divided into three categories under the top node or root (Acme Packet Net-Net EMS). Each category contains objects called nodes, each of which represents a Net-Net SBC data item. Those nodes in turn can contain additional data items.

The following example shows a Navigation tree with all categories fully expanded to display all the nodes:



The Navigation tree contains the following three functions:

- `Configuration management`: where you discover and configure a Net-Net SBC.

  The Active configurations area contains a list of all discovered Net-Net SBCs and reflects the current configuration each of them. You cannot modify these configuration values. You need to make a copy of the Net-Net SBC in this area, which is placed in the Inactive configurations area, in order to make configuration changes.

- `Fault management`: where you monitor alarms, events, and syslog.
- `Performance management`: which displays real-time, on-demand performance statistics for monitoring performance and utilization. For example, system,

session agent-, and realm-based session information. You can export this information to .CSV format.

Alarm Count by Severity Table

The lower left pane displays the Alarm count by severity table:

Alarm count by severity							Category
0	0	6	0	0	0	6	ColdStart
0	0	3	0	0	9	12	Link
0	0	0	0	2	0	2	Session ag...
0	0	0	0	0	1	1	CPU
0	0	0	0	0	4	4	Polling
0	0	3	0	0	2	5	Health
0	0	1	0	0	0	1	Gateway
0	0	1	0	0	0	1	Login
0	3	2	0	0	0	5	apSysLog
0	1	0	0	0	0	1	Cpu Load
0	4	16	0	2	16	38	Total

The Alarm count by severity table displays a summary of all alarms generated, by alarm severity and by category. The summary displays the number of alarms that are generated under various categories and severity levels. This table is automatically refreshed when alarms arrive at the Net-Net EMS server.

Each row in the Alarm count by severity table corresponds to a specific category of alarms. The number of rows correspond to the number of alarm categories. The last row provides the total number of alarms for each severity level.

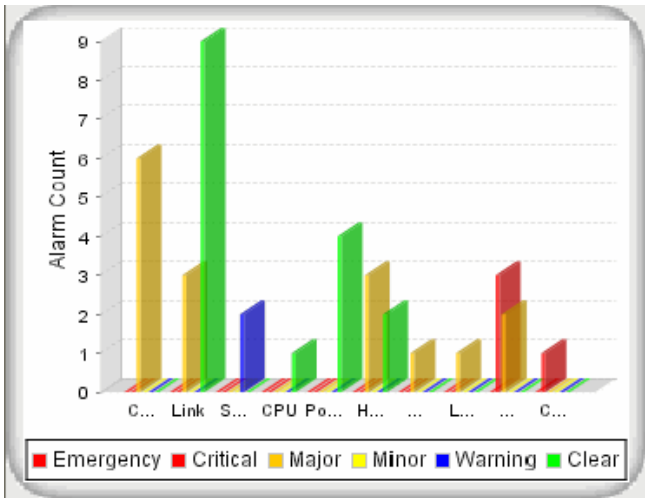
See *Viewing Alarm Information* in the *Fault Management* chapter for details.

Changing the Alarm Table Presentation

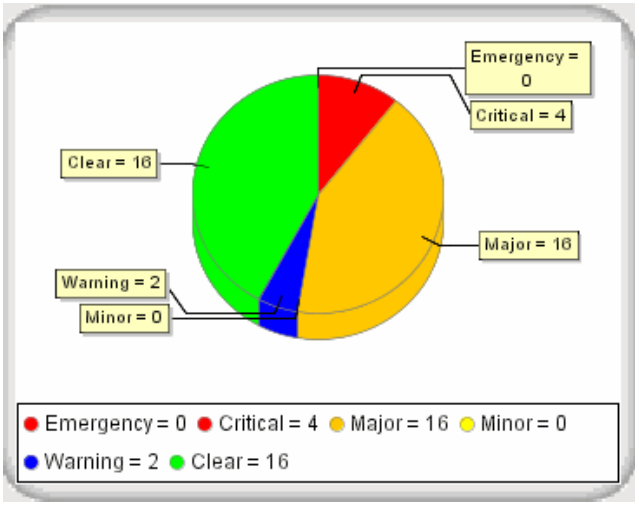
You can change the presentation of the alarm summary information by clicking the following buttons.

-  displays the alarm information by severity and category in the table

-  displays the alarm information by severity and category in a stack chart



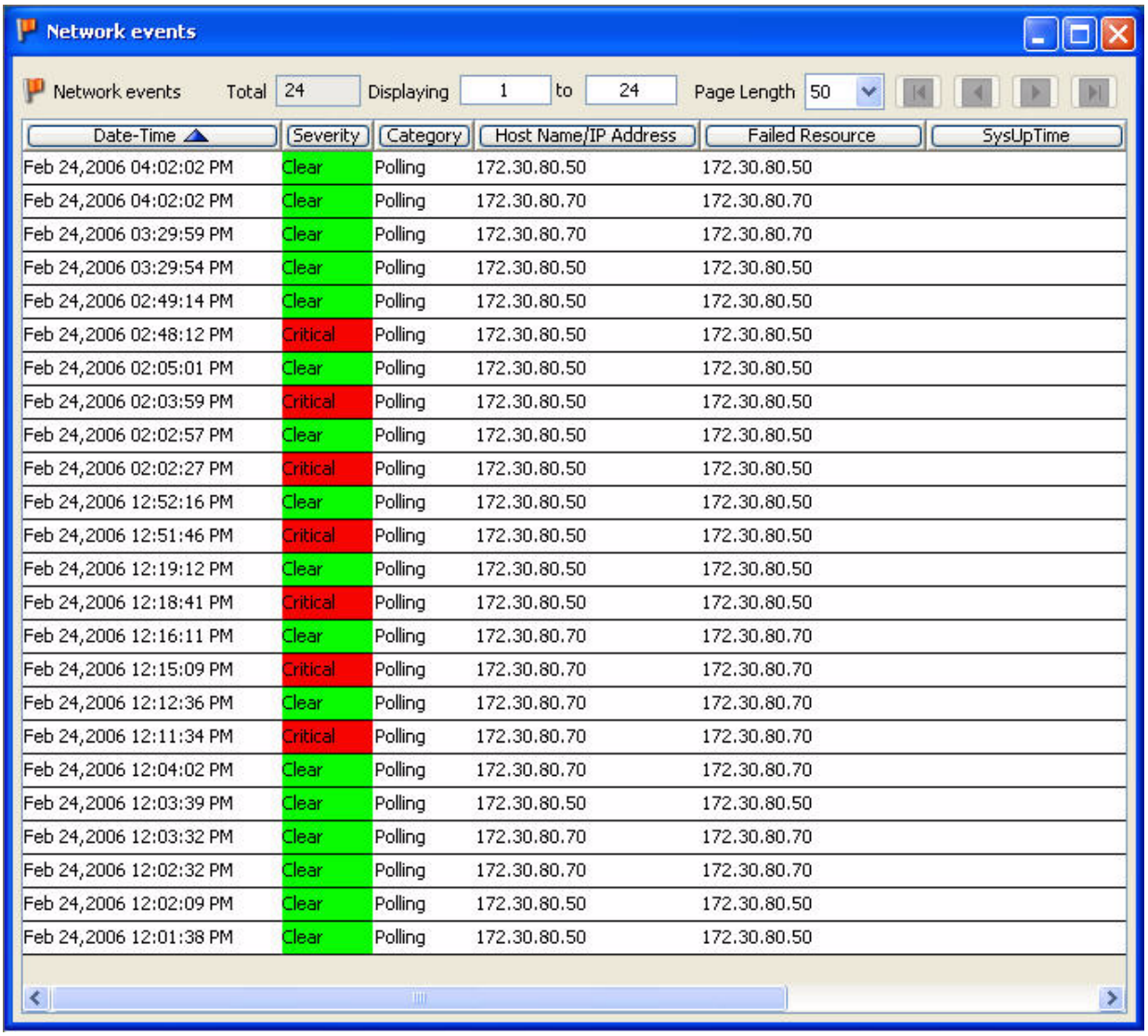
-  displays the alarm information by severity in a pie chart



Display Pane

The Display pane is displayed on the right side of the Net-Net EMS GUI and contains a map of the world when you first access Net-Net EMS. When you select an option from the Navigation tree, the result of the choice appears in the Display pane.

For example, if you choose Network events from the Fault management category, a list of network events appears in the Display pane:



Date-Time	Severity	Category	Host Name/IP Address	Failed Resource	SysUpTime
Feb 24,2006 04:02:02 PM	Clear	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 04:02:02 PM	Clear	Polling	172.30.80.70	172.30.80.70	
Feb 24,2006 03:29:59 PM	Clear	Polling	172.30.80.70	172.30.80.70	
Feb 24,2006 03:29:54 PM	Clear	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 02:49:14 PM	Clear	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 02:48:12 PM	Critical	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 02:05:01 PM	Clear	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 02:03:59 PM	Critical	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 02:02:57 PM	Clear	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 02:02:27 PM	Critical	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 12:52:16 PM	Clear	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 12:51:46 PM	Critical	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 12:19:12 PM	Clear	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 12:18:41 PM	Critical	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 12:16:11 PM	Clear	Polling	172.30.80.70	172.30.80.70	
Feb 24,2006 12:15:09 PM	Critical	Polling	172.30.80.70	172.30.80.70	
Feb 24,2006 12:12:36 PM	Clear	Polling	172.30.80.70	172.30.80.70	
Feb 24,2006 12:11:34 PM	Critical	Polling	172.30.80.70	172.30.80.70	
Feb 24,2006 12:04:02 PM	Clear	Polling	172.30.80.70	172.30.80.70	
Feb 24,2006 12:03:39 PM	Clear	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 12:03:32 PM	Clear	Polling	172.30.80.70	172.30.80.70	
Feb 24,2006 12:02:32 PM	Clear	Polling	172.30.80.70	172.30.80.70	
Feb 24,2006 12:02:09 PM	Clear	Polling	172.30.80.50	172.30.80.50	
Feb 24,2006 12:01:38 PM	Clear	Polling	172.30.80.50	172.30.80.50	

Status Bar

The Status Bar is located at the bottom of the screen.

It indicates the status of the current discovery or rediscovery process by displaying text and changing from green to blue. When the process completes, the final status of indicating whether the process is successful is displayed.

For example, if rediscovery has been initiated the message appears and the background color of the status bar changes from green to blue.

When rediscovery has completed successfully, a message appears. For example:

Right-Click Mouse Functions

You can right-click in both the Active and Inactive configuration areas to access pop-up lists of functions. To choose a function, click the function name.

Active Configuration Category

Right-click the Active configuration category to access the following function.

Function	Description
Create domain	Create a new domain

Active Domain

Right-click a domain in the Active configuration area to access the following functions:

Function	Description
Rename	Rename the selected domain
Delete	Delete the selected domain

Active Net-Net SBC Configuration

Right-click a Net-Net SBC configuration in the Active configuration area to access the following functions:

Function	Description
Rediscovery	Rediscover this Net-Net SBC
Reboot	Reboot this Net-Net SBC
Set offline (Net-Net 4000 only)	Take this Net-Net SBC offline
Move	Move this Net-Net SBC configuration to another domain
Copy for edit	Copy this Net-Net SBC configuration to the Inactive configuration area

Function	Description
Create offline configuration	Create an offline configuration based on the selected Net-Net SBC configuration. You can then edit the offline configuration's parameters.
Delete	Delete this Net-Net SBC configuration from the Net-Net EMS navigation tree
Inventory Details	Access details about the hardware, software, and licenses associated with this Net-Net SBC
Telnet to SD System	Open a Telnet session to this Net-Net SBC
SSH to device	Open a Secure Shell session to this Net-Net SBC. You need a username and password for SSH authentication
HDR operations(G)	Access HDR reporting operations
Registration Cache	Access Registration cache details for this active configuration
Lock	Lock the configuration node to prevent other users from performing any configurations on the same node
Unlock	Unlock the configuration node
Search configuration	Allows you to search for, view, and edit top-level objects
Configuration inventory	Access configuration inventory details for this active configuration

Active SD HA Pair

Right-click an HA pair to access the following functions in addition to those in the active Net-Net SBC configuration table:

Function	Description
Switch HA Role	Switch the role of the active node to standby. The standby node becomes the active one.
Reboot Active	Reboot the active Net-Net SBC
Reboot Standby	Reboot the standby Net-Net SBC

Inactive Configuration Category

Right-click the Inactive configuration category to access the following functions:

Function	Description
Save all	Not currently supported

Inactive Domain

Right-click the Inactive domain to access the following functions:

Function	Description
Rename	Rename the domain
Delete	Delete the domain
Create offline SD configuration	Create a new offline standalone Net-Net SBC configuration associated with this domain

Function	Description
Create offline SD HA configuration	Create a new offline Net-Net SBC HA configuration associated with this domain
Save all	Not currently supported

Offline configuration lets you create configurations for devices that are not currently available. Using offline configuration lets you create a Net-Net SBC node that is not associated with a specific Net-Net SBC until you save the configuration to one.

Inactive Configuration Node

Right-click an inactive configuration node to access the following functions:

Function	Description
Rename	Rename the configuration node
Delete	Delete the configuration node
Lock	Lock the configuration node to prevent other users from performing any configurations on the copy of the node configuration
Unlock	Unlock the configuration node

Inactive Net-Net SBC Configuration

Right-click a Net-Net SBC configuration in the Inactive configuration areas to access the following functions:

Function	Description
Save config	Saves the current configuration to the Net-Net system's last-saved configuration, stored in flash memory
Activate config	Activates the current configuration on the Net-Net SBC to make it the running configuration
Save and Activate config(Z)	Saves and then activates the configuration
Copy for edit	Copy an inactive configuration for edit
Create offline configuration	Copy an existing active or inactive configuration and modify the existing parameters offline
Create SD HA node	Create an HA node with two Net-Net SBC configurations
Replicate	Replicates selected configuration data from one inactive Net-Net SBC configuration copy to another. Data includes: • session agents • session agent groups • routes
Search configuration	Allows you to search for, view, and edit top-level objects
Configuration inventory	Access configuration inventory details for this inactive configuration

Inactive SD HA Pair

Right-click an HA pair to access the following functions:

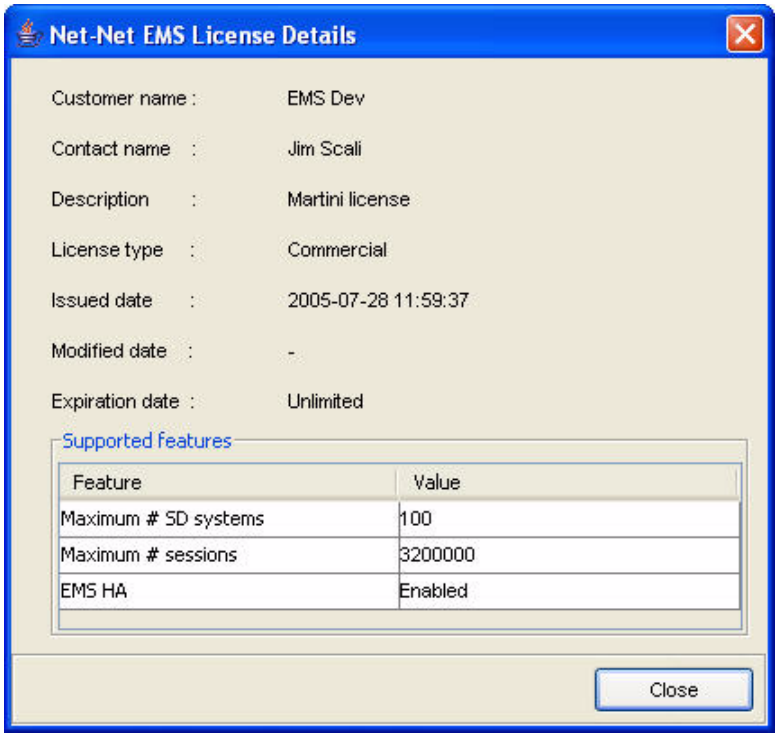
Function	Description
Save and Activate Config	Saves the current configuration to the Net-Net system's last-saved configuration, stored in flash memory and activates it to make it the running configuration
Create offline configuration	Copy an existing active or inactive configuration and modify the existing parameters offline
Rename	Rename the configuration node

Viewing Net-Net EMS License Information

This section explains how to view the Net-Net EMS license information.

To view license information:

1. From the Tools menu, choose `View license`. The Net-Net EMS License Details window appears:



About the License Data

The following table defines the data displayed by Net-Net EMS for a standalone Net-Net SBC or for the Net-Net SBCs that belong to an HA pair:

Data	Description
Customer name	Name of customer licensed to use Net-Net EMS
Contact name	Name of the contact person
Description	Descriptive text that describes the license
License type	Type of license issued: • Commercial: indicates Net-Net EMS is licensed for commercial use • Evaluation: indicates Net-Net EMS is licensed for evaluation purposes and beta deployments
Issued date	Date the Net-Net EMS license was issued in the format: yyyy-mm-dd hh:mm:ss
Modified date	Date modifications were made to the license in the format: yyyy-mm-dd hh:mm:ss

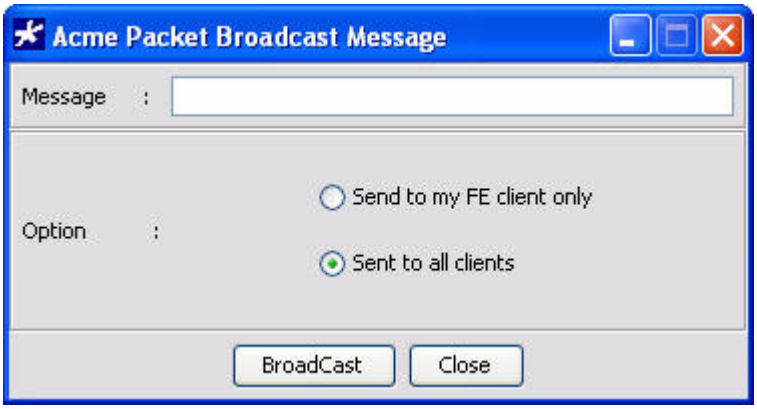
Data	Description
Expiration date	Date the Net-Net EMS license expires. Values are: • Unlimited for a Commercial license only • Specific date in the format: yyyy-mm-dd hh:mm:ss
Supported features	
Maximum # SD systems	Maximum number of Net-Net SBCs allowed in the Active configurations area. (The number in the Inactive configurations area does not count.) When the maximum number is exceeded, you cannot discover additional systems, apply offline configuration, or save to an offline Net-Net SBC. You must delete the excess number of Net-Net SBCs to proceed. Note: Net-Net SBC HA pair is considered a single system.
Maximum # sessions	Informational only
EMS HA	Whether EMS HA functionality is enabled

Sending Broadcast Messages

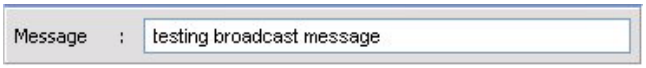
This section explains how to send (broadcast) messages to all the clients connected to the server.

To broadcast a message:

1. From the File menu, choose `Broadcast Message`. The Broadcast Message dialog box appears:



2. **Message**—Type the message to be broadcast in the Message field. For example:



3. Select the delivery option:
   - `Send to my FE client only`: The message is sent to all the clients connected to that specific Net-Net EMS server.
   - `Send to all clients`: The message is sent to all the clients connected to different Net-Net EMS servers.
4. Click **Broadcast**.

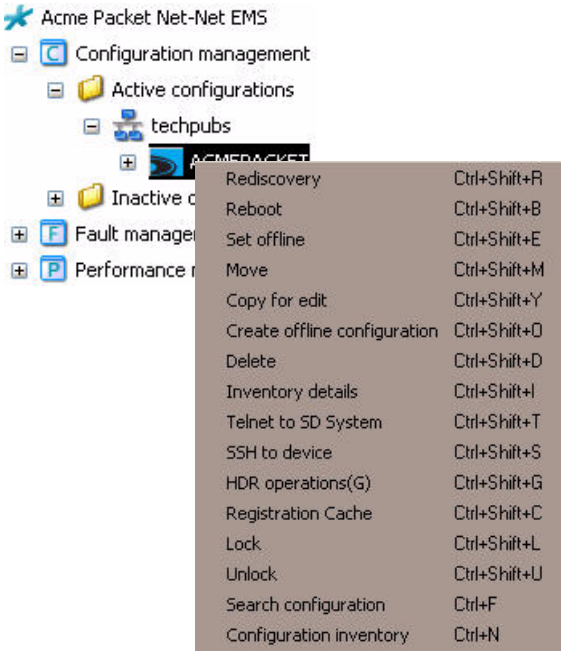
   The message is delivered to intended clients that are connected to the Web NMS Server and is displayed on the status bar.

Connecting Using Telnet

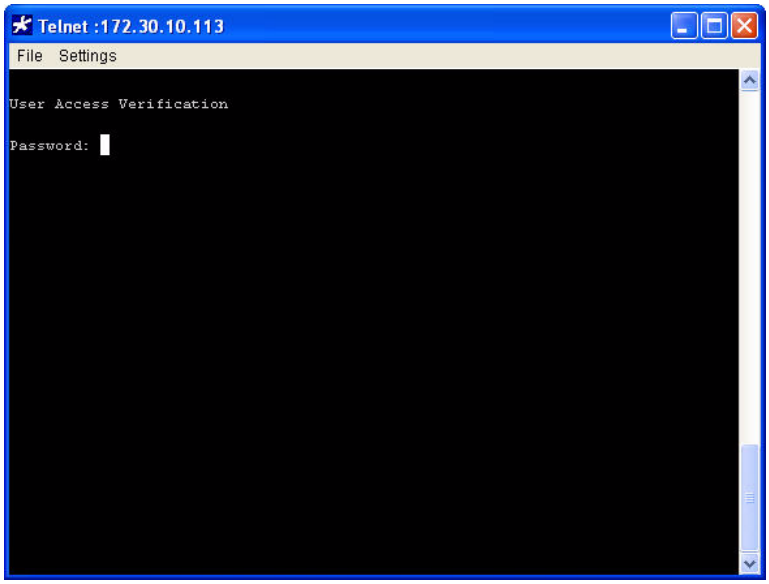
If you want to switch from configuring Net-Net SBCs in the Net-Net EMS to using the ACLI, you can connect through Telnet to the Net-Net SBC. You can then login in to continue working using the ACLI.

To connect using Telnet:

1. In the `Active configurations` area, right click the name of the Net-Net SBC. A list of options appears:



2. Click `Telnet to SD system`. The Telnet window appears:



3. Login to the Net-Net SBC. See the *Net-Net ACLI Reference Guide* for details about logging in and using the ACLI. See the *Net-Net EMS Configuration Guide* for details about configuring a Net-Net SBC using the ACLI.
4. Save the configuration to the Net-Net SBC to activate it.

Offline Configuration

Offline configuration lets you create configurations for devices that are not currently available. Using offline configuration lets you create a Net-Net SBC node that is not associated with a specific Net-Net SBC until you save the configuration to one.

> **Note:** See the *Net-Net Configuration Guide* for details about creating offline configurations.

You can create an offline configuration using one of the following methods:

- Copy an existing active or inactive configuration and modify the existing parameters
- Create an original configuration

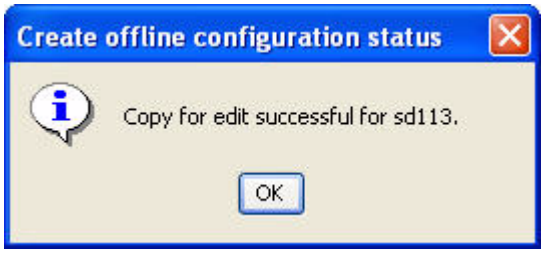
Copying a Configuration

To copy an existing configuration:

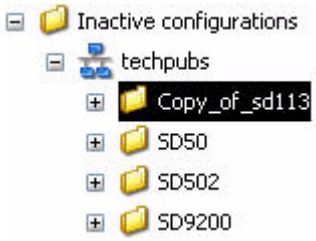
1. In the `Active configurations` or `Inactive configurations` area, right-click the Net-Net SBC to access the popup menu. (You can also select an existing offline configuration.)
2. Click `Create offline configuration`. The Create offline configuration dialog box appears:

3. **Configuration name**—Edit the name of the copy if you do not want to retain the default.
4. Click **OK**. A status message appears indicating the request has been sent to the server.

   When the process completes, the following message appears:



The copy appears under the Inactive configuration category of the Net-Net EMS navigation tree.



Refer to the *Net-Net EMS Configuration Guide* for details about configuring a Net-Net SBC.

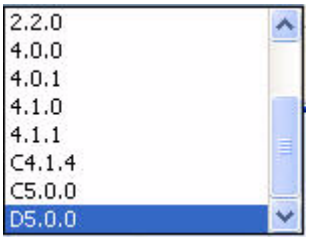
Creating an Original Configuration

To create an original configuration:

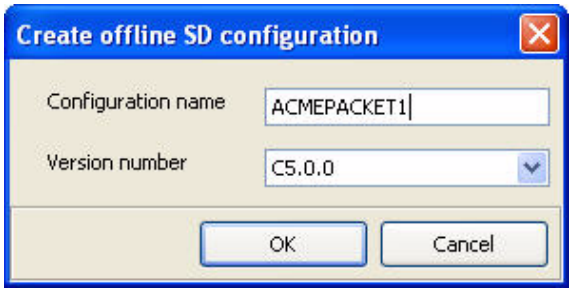
1. Click the domain to which you want to associate the new configuration under Inactive configurations.
2. Right-click the domain name to access the pop-up menu.
3. Click one of the following options:
   - Standalone Net-Net SBC: `Create offline SD configuration`

     The Add offline SD configuration dialog box appears:
   - HA Net-Net SBC pair: `Create offline SD HA configuration`

     The Add offline SDHA configuration dialog box appears:
4. **Configuration name**—In either dialog box, enter a name for this configuration.
5. Click the down arrow to access a drop-down list of versions.

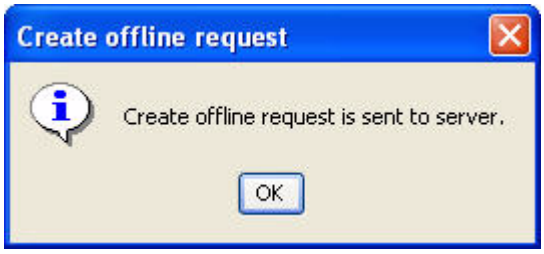


6. **Version number**—Click the version number to select it. For example:



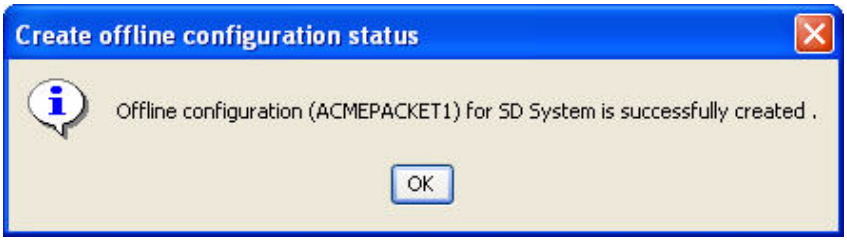
7. Click **OK**.

A message appears indicating the request has been sent to the server:



8. Click **OK** to clear the message.

   When the process completes, the following message appears:



   Refer to the *Net-Net EMS Configuration Guide* for details about configuring a Net-Net SBC.

Replicating Selected Configuration Elements

If you have the privilege to configure an SBC, you can replicate configuration information for the following elements from one inactive configuration copy to another:

- account configuration
- authentication
- capture receiver
- NTP configuration
- session agents
- session agent groups
- routes
- SIP manipulation
- translation rules
- translation profiles
- SNMP communities
- trap receivers

You need to ensure that all the configuration records referenced by the elements you are replicating have corresponding counterparts in the target configuration.

The target you choose for the data you are replicating must have a matching platform (4000 or 9000), a matching configuration (standalone, HA, or PAC), and a matching version of SBC software (6.0, 9000).

> **Note:** The existing configuration information on the target will be deleted and replaced by the replicated configuration data.

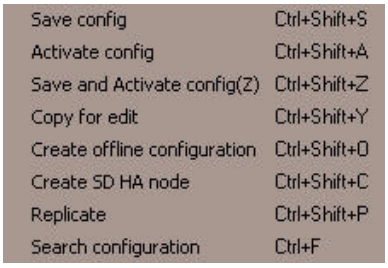
Record Validation

Net-Net EMS validates that all records referenced by the data being replicated in the source configuration have corresponding records in the destination copy. For example, all realm IDs that appear as source realm values in routes being copied must already exist with the same realm ID in the destination configuration.

Replicating Data

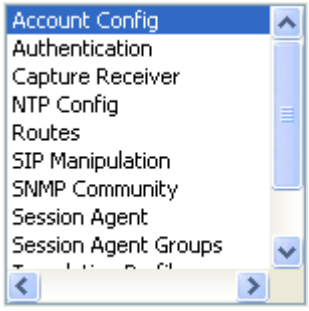
To replicate data:

1. In the Inactive configurations area, right click the Net-Net SBC from which you want to replicate data. A pop-up menu appears.
2. Click **Replicate**. The Selective Configuration Replication console appears.



3. **Target Configuration**—Select the target configuration from the drop-down list.

4. **Targeted groups**—Click **Add**. The Selective Configuration Replication selector window appears.
5. Click a group name in the Available Groups list to select it.



6. Click > to move the group name to the Selected Groups list.
   - You can select multiple non-contiguous group names by holding down the CTRL key and clicking the different group names. Click > to move the multiple group names to the Selected Groups list.
   - You can move all groups from the Available Groups list to the Selected Groups list by clicking >>.
7. Click **OK** to save your selections and close the Selective Configuration Replication selector window. The group names you chose appear in the Targeted groups list.

8. Click **Start** to begin the replication. A warning message appears about existing data in the target configuration being deleted.

9. Click **OK** to proceed. The icon at the top of the window changes to indicate replication is in progress.

Net-Net EMS validates all records in the source configuration that are associated with the set of data being copied have corresponding records in the destination copy. For example, all realm IDs that appear as source realm values in routes being copied must already exist with the same realm ID in the destination configuration.

```
06/27/2007 10:58:01 : Request for replication submitted.
--------------------------------------------------------------------------------
06/27/2007 10:58:01 : Started replication processing for thread : Thread-594
--------------------------------------------------------------------------------
06/27/2007 10:58:01 : Replication started from source : SD50 to target :SD50
--------------------------------------------------------------------------------
Operation       Status  Element Name                    Object Name
--------------------------------------------------------------------------------
Validation      true    SessionAgentGroup               N/A
Validation      false   SessionAgent                    h323-sa
Validation      false   SessionAgent                    sip-sa
Validation      false   SessionAgentCarriers            hong-carr1
Validation      false   SessionAgentCarriers            hong-carr3
```

Validations for all elements are listed in the Replication log area. If validation fails, you can see which records were invalid, as well as the specific parameters within those records that cause the failure. Replication is cancelled and the target configuration is restored to it's original state.

If validation fails, a message appears in the Replication log area.

```
Validation      false   SessionAgent                    N/A
Validation      false   LocalPolicySourceRealm          access1
Validation      false   LocalPolicySourceRealm          access3
Validation      false   LocalPolicyAttribute            RP5
Validation      false   LocalPolicyAttribute            RP1
Validation      false   LocalPolicyMediaProfiles        hong1-media
Validation      false   LocalPolicyMediaProfiles        hong3-media
Validation      false   LocalPolicy                     N/A
--------------------------------------------------------------------------------
06/27/2007 10:58:01 : Validation failed for target : SD502
06/27/2007 10:58:01 : Exception thrown for thread : Thread-5945. Reason : Ab
06/27/2007 10:58:01 : Replication aborted for thread Thread-5945.
06/27/2007 10:58:01 : Replication process completed for thread Thread-5945.
```

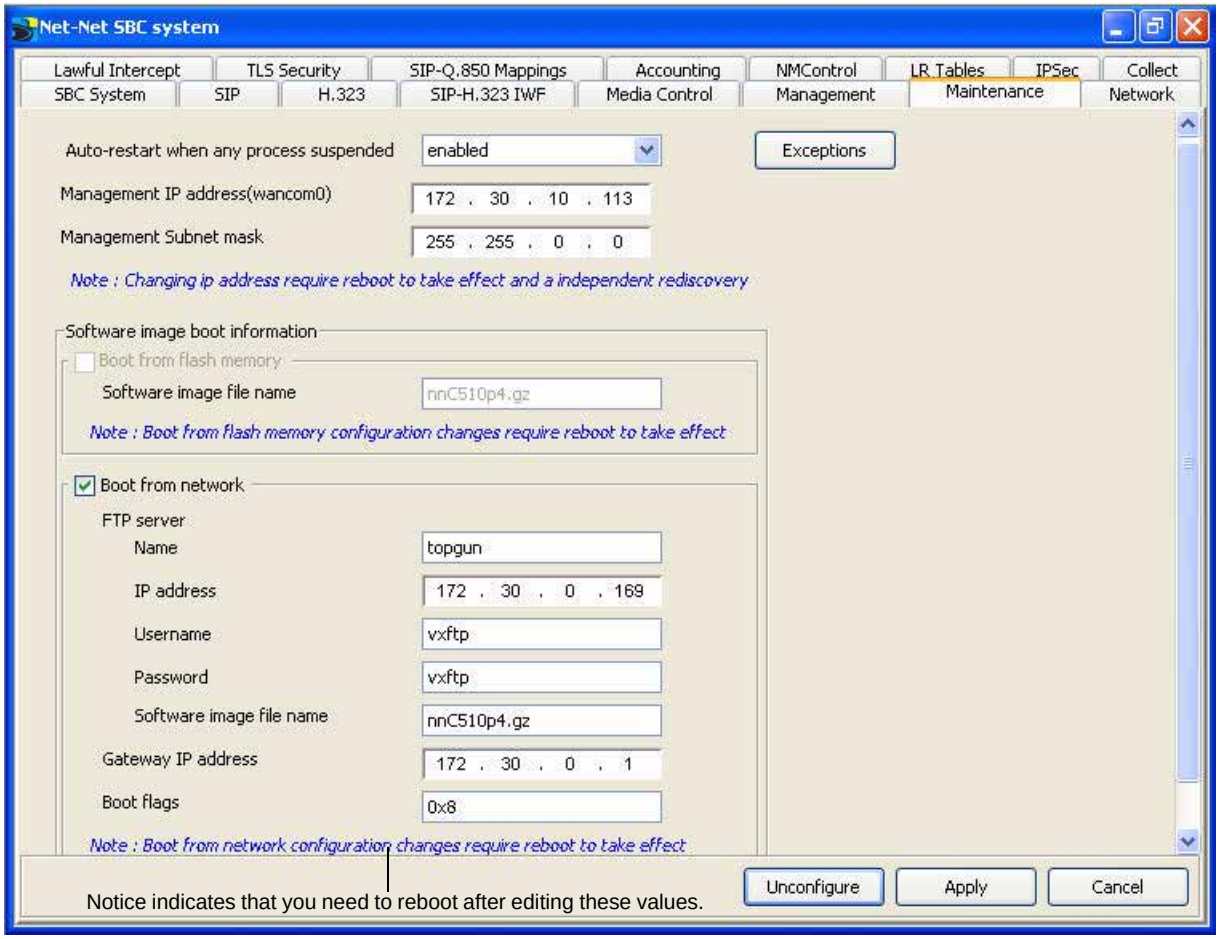
If validation is successful, all session agent, route, and route policy records are deleted from the target configuration and replaced with duplicates of the source configuration records. A message appears indicating replication was successful.

```
Replicate       routes          Route 8         Success
Replicate       routes          Route 9         Success
Replicate       routes          Route 10        Success
--------------------------------------------------------------------------------
Commit Transaction @ 06/01/2007 14:35:05
Transaction completed successfully @ 06/01/2007 14:45:05
--------------------------------------------------------------------------------
Replication completed successfully @ 06/01/2007 14:45:40
```

10. Click **Save** log if you want to save the replication log information to a file.
11. Click **Close** to exit the Selective Configuration Replication console.

Reboot Notices

Some Net-Net SBC configuration parameters require a reboot of the system if the values are changed. On-screen notifications about the need to reboot the Net-Net SBC are included where required. For example if managing Net-Net 4000:



Configuring External Trap Receivers

This section describes the Net-Net EMS traps contained in the Acme Packet EMS MIB and the configuration of the external trap receivers. Net-Net EMS generates traps when it detects the following:

- Failure to discover or rediscover a Net-Net SBC configuration
- Failure to save a Net-Net SBC configuration
- Failure to activate a Net-Net SBC configuration
- Missing components when validating a Net-Net SBC configuration
- Node status change from reachable to unreachable

You need to configure an external server as the receiver for these traps.

About Net-Net EMS Traps

Net-Net EMS generates the following traps.

Trap	Description
apEMSDiscoveryFailure	Generated when Net-Net EMS fails to discover or rediscover a Net-Net SBC configuration. The trap is generated from any discovery or rediscovery failure initiated by the SOAP XML API, Net-Net EMS, or system processing. The trap contains the Net-Net SBC's node ID, the start and end time of the discovery or rediscovery operation, and the user who initiated the operation.
apEMSSaveFailNotification	Generated when Net-Net EMS fails to save a configuration. The trap is generated by a save failure whether initiated by the SOAP XML API or Net-Net EMS GUI for the save/activate, save, or offline save operations. The trap contains the Net-Net SBC node ID, the start and stop time of the save configuration attempt, and the user initiating the save operation.
apEMSActivateFailNotification	Generated when Net-Net EMS fails to activate a configuration, whether initiated from the SOAP XML API or the Net-Net EMS GUI for the save/activate or activate operations
apEMSInvalidConfigDiscoveredNotification	Generated when Net-Net EMS validates a discovered Net-Net SBC's configuration (for example, confirms each referenced realm is configured) and detects missing components. The trap contains the time and the Net-Net SBC node ID.
apEMSNodeUnreachableNotifcation	Generated when a node's status changes from reachable to unreachable. The trap contains the Net-Net SBC's node ID and the time of the event.
apEMSNodeUnreachableClearNotification	Clearing condition trap. Generated when a node's status changes from unreachable to reachable. The trap contains theNet-Net SBC's node ID and the time of the event.

Notification Objects

The Acme Packet EMS MIB also lists the following notification objects, the information for which is contained in the generated traps.

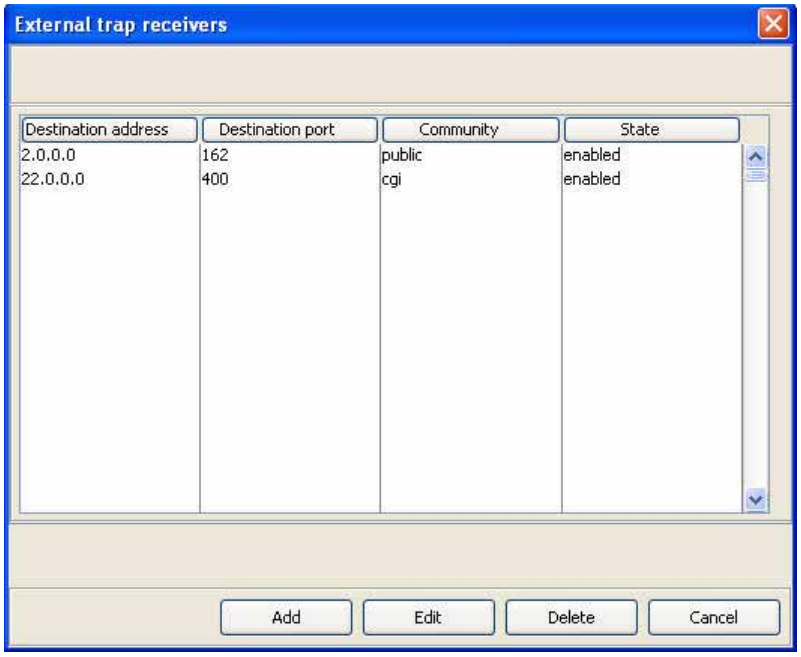
Notification Objects	Description
apEMSDiscoveryMode	Discovery mode values: unknown(0) discovery(1) reDiscovery(2)
apEMSNodeID	Identifier for a Net-Net EMS node that appears on the navigation tree in the Active configuration area on the Discovery table in the Host Name/IP Address column
apEMSStartTime	Time as configured on the EMS server when an event occurs
apEMSDateTime	Time as configured on the EMS server when an event completes
apEMSUser	User initiating the function. If the function was automatically initiated by the Net-Net EMS application, the user is system.
apEMDeviceAddress	Address for a device being managed

Configuring External Trap Receivers

An external trap receiver is a server that you use as the trap destination, instead of the server where Net-Net EMS is installed. When you configure the external trap receiver, you enter its address and port. The combination of IP address and port must be unique for each configured trap receiver.

To configure external trap receivers:

1. Login to Net-Net EMS.
2. From the Tool menu, choose `External trap receiver`. The External trap receivers table appears:



3. Click **Add**. The Add external trap receivers dialog box appears.
4. **Destination address**—Enter the IP address of the server receiving the traps.
5. **Destination port**—Enter the port number for the server receiving the traps or retain the default value of `162`.
6. **Community**—Enter the name of the SNMP community to which the server receiving traps belongs or retain the default value `public`.
7. **State**—Retain the default value `enabled`.

8. Click **OK**.

   A validation is performed on the destination address and port. If either or both cannot be validated the following message appears.

   A validation is also performed on the community name. If left blank, the following message appears.

9. If necessary, click **OK** to clear the error message.

   The new trap receiver appears in the External trap receivers table.

You can edit an existing trap receiver to change its SNMP community name and state; you cannot edit the destination address and port.

Using Net-Net EMS Client Logs

This section explains how to use Net-Net EMS client logs. Client logs contain messages about the following Net-Net EMS client-side processes:

- Discovery
- Configuration
- Fault
- Miscellaneous (all other processes that do not fall under the first three categories)

To view the messages, you need to enable the Java console and set the client log levels. Messages are then written to the Java console and you can review them online, save them to a file, or both.

Enabling the Java Console

You enable the Java console by configuring the Java Web Start application.

To enable the Java console:

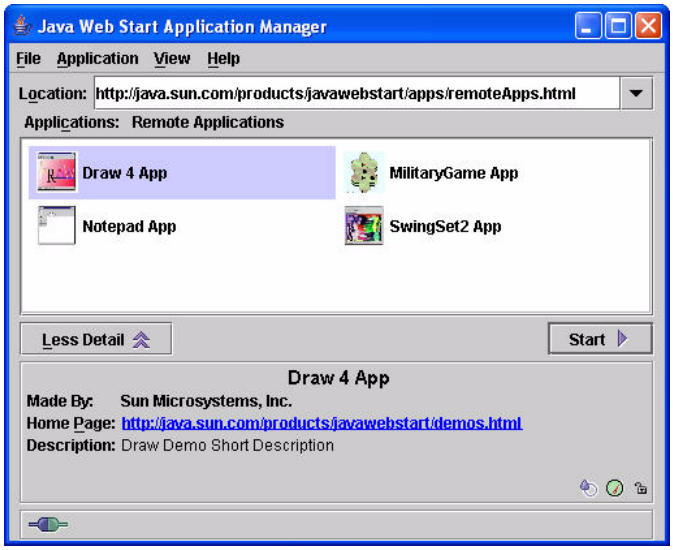
1. Click `Start`, then `All Programs`, and choose `Java Web Start` from the list.

   or

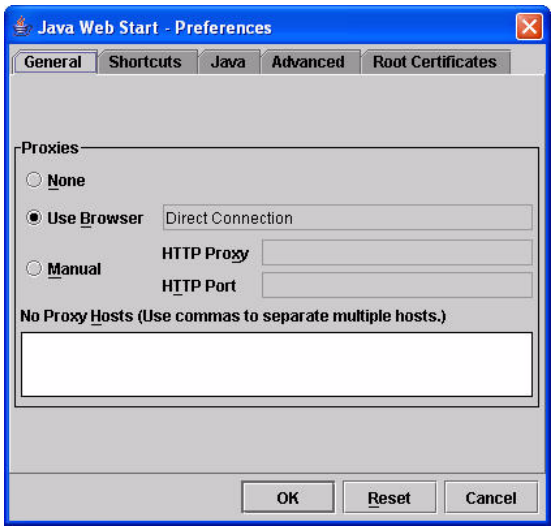
   Double-click 

   on your desktop (if present).

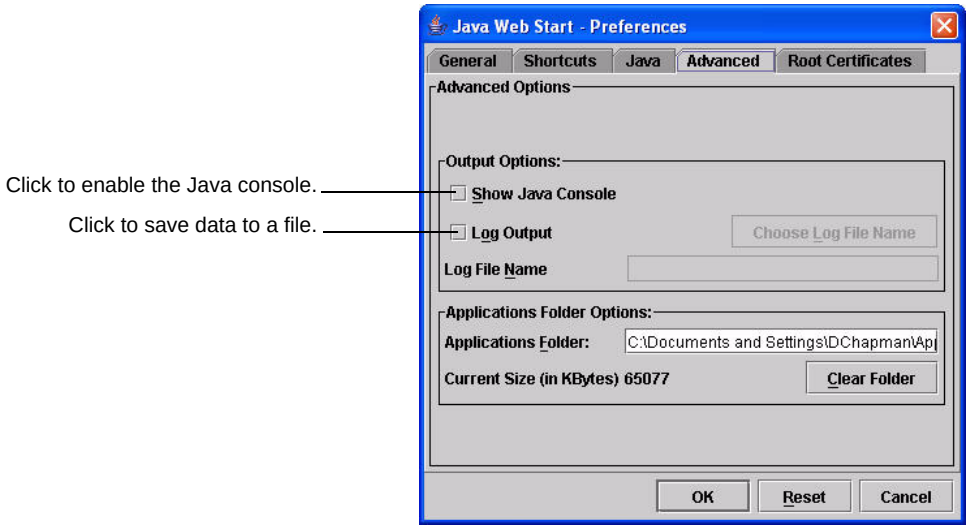
   The Java Web Start Application Manager appears:



2. Choose `Preferences` from the File menu. The Java Web Start Preferences window appears:



3. Click the Advanced tab. The Advanced Options appear:



Note: You can choose to view the data online, save the data to a file, or do both.

4. To view the data online, click `Show Java Console` to enable the display of the Java console. The Java console will start after you connect to the Net-Net EMS. It appears along with the Login screen.

   If you want to review the Java console logs online, go to step 7. If you want to save the data to a file, continue to the next step.

5. **Log Output**—To save the Java console logs to a file, click `Log Output` to activate the `Log File Name` textbox:

6. **Log File Name**—Enter a name for the file (for example, emsclientlog.txt) or click `Choose Log File Name` to browse to file you want to use.

   Data is written to the file you name when the Java console starts. If you have also chosen to enable the Java console display, the same data appears in the Java console.

7. Click **OK** to return to the Java Web Start Application Manager window.

8. Exit the Java Web Start Application Manager.

Starting the Java Console

To start the Java console:

1. Ensure you have enabled the Java console display in the Java Web Start application.

2. Connect to the Net-Net EMS server using the following address format:

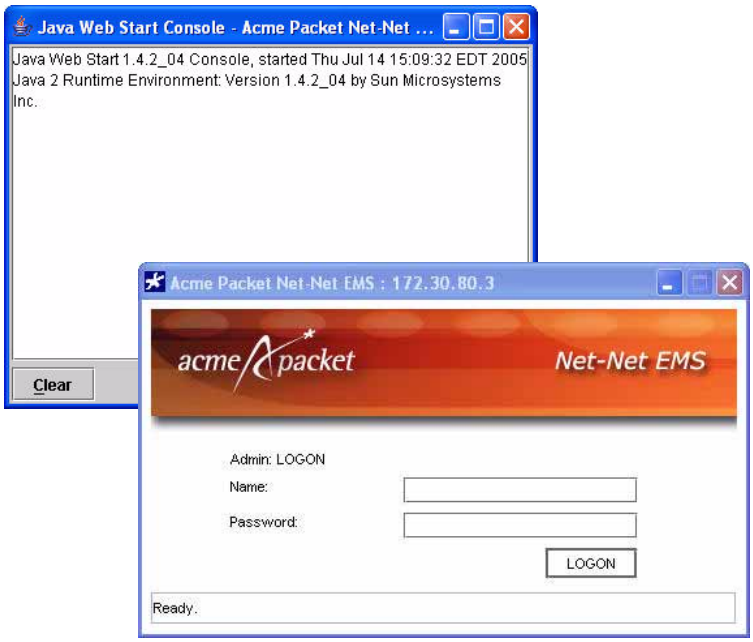
   http://<EMS server IP address>:9090

   Note: If your system has been configured for HTTPS login, you need to use the following address format to connect:

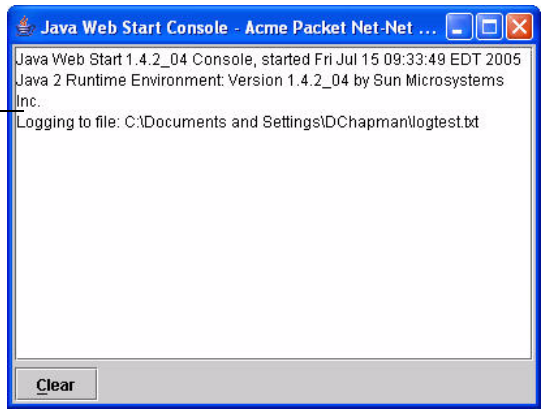
   https://<EMS server IP address>:8443

   See *HTTPS Login Using Microsoft Internet Explorer 6.0* or *HTTPS Login Using Mozilla Firefox 1.0* for details about the security windows that appear when you connect using HTTPS.

   Because you have enabled the Java console, it appears along with the Login screen:



If you also chose to save data to a file, the Java console displays the complete path and filename:



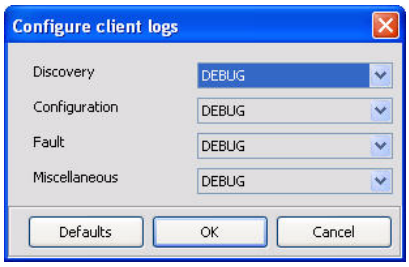
You can minimize the Java console and continue with the Net-Net EMS login. See *Accessing the Net-Net EMS GUI* for details. After you login to Net-Net EMS, you can configure the client log levels for the current session.

Configuring the Client Log Levels

When you configure the client log levels, you are configuring them for the current session. If you logout and login again, you have started a new session and the log levels have reverted to the default values.

To configure the client log levels for the current session:

1. Login to Net-Net EMS.
2. From the Tool menu, choose `Client log level`. The Configure client log levels window appears:



Note: Acme Packet recommends you use either NONE or DEBUG for log levels. Set the client log levels to NONE if you do not need to log information for the current session. Retain the DEBUG level if you need to log error information for diagnostic purposes.

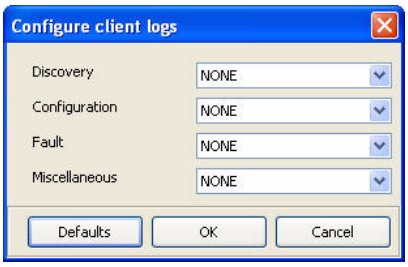
For example, if an Acme Packet representative asks you to provide a log of client process information, you set the level to DEBUG and enable the Java console to save the data to a file. See "Enabling the Java Console"on page 48 for details.

Although there are several other log levels available, INTERMEDIATE_DETAIL, SUMMARY, and VERBOSE, NONE and DEBUG should provide the information you need.

3. Retain the default value DEBUG for each category for which you want to log the current session's error information. All error information is logged.

   or

Click **Defaults** to set all categories to the log level `NONE` if you do not plan to log messages for the current session.



Note: When you set the log level to NONE, you might find some error information is still logged.

4. Click **OK** to apply your changes and close the Configure client logs window.

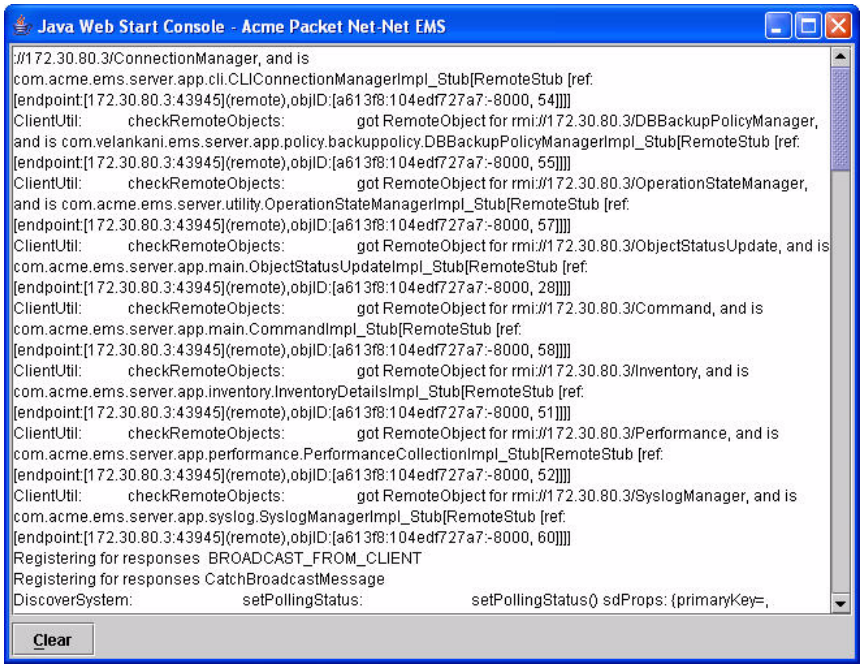
   You can now maximize the Java console and view log data.

Viewing Log Data Online

To view Java console logs online:

1. Start or maximize the active Java console.
2. Perform the process for which you want to view data, if you have set the log level for a specific process. For example if you have set the log level for the Discovery process, perform a discovery and view the data online in the Java console.

   Information is written to the screen in real-time:



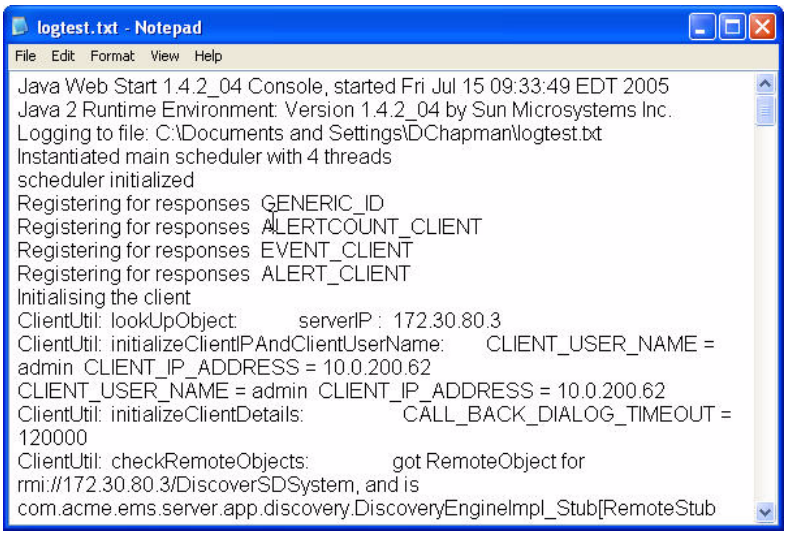
3. Click **Clear** to clear the data from the screen.

Viewing the Java Console Log File

If you chose to write the log messages to a file, you can access that file to view the data.

To view the log file:

1. Open the log file that you named in the Java Web Start application. The logged data appears. For example:



3 Discovering Net-Net SBCs

Overview

This chapter explains how to discover the Net-Net SBCs you want to manage using Net-Net EMS. You can discover a single Net-Net SBC, a single Net-Net SBC high availability (HA) pair, PAC, or multiple single and HA pair systems.

Discovery is the process of identifying Net-Net SBCs in the network using the IP address and collecting inventory data about the devices to store in the Net-Net EMS database. Discovery discovers devices in the network and gathers resource information about the devices for use with data collection, report generation, and queries.

Discovery establishes a connection with the Net-Net SBC, PAC, or HA pair, checks the state of a PAC or HA pair, obtains the system's details, and adds the Net-Net SBC, PAC, or HA pair to the Net-Net EMS navigation tree.

There is also a rediscovery process that occurs when a Net-Net SBC's configuration has been updated, after the reboot of the system. The reboot causes the rediscovery to occur automatically.

Minimum Net-Net SBC Configuration

The Net-Net SBCs you plan to manage using Net-Net EMS must have the following information configured in order to be discovered. To verify the minimum configuration for Net-Net SBCs you plan to manage, see the following documentation:

- *Net-Net EMS 4000 Configuration Guide* for details about configuring a Net-Net SBC using the Acme Command Line Interface (ACLI)
- *Net-Net ACLI Reference Guide* to refer to all ACLI commands.

Boot Parameters

Boot parameters specify the information your Net-Net system uses at boot time when it prepares to run applications. The Net-Net system's boot parameters include the Net-Net system's IPv4 address for the management interface (wancom0) and the target name of the Net-Net SBC.

Net-Net EMS uses the target name to uniquely identify a Net-Net SBC from among the list of Net-Net SBCs in its Active configuration area. You need to ensure that all Net-Net SBCs you plan to manage, thus discover, with Net-Net EMS have unique target names. Otherwise a list of Net-Net SBCs, all with the default name `acmesystem`, would appear in the list.

Ensure the following boot parameters have been configured:

- wancom0 IP address and mask
- target name is set to a unique name (do not use the default name acmesystem)

System Configuration Element

You need to ensure the `system-config` element has been configured. This element establishes general system information and settings, for example:

- Contact information for this Net-Net system for SNMP purposes
- Identification of the Net-Net system for SNMP purposes
- Physical location of the Net-Net system for SNMP purposes
- Whether SNMP is enabled on the system
- Whether traps are enabled

For complete details about system configuration, see the *Net-Net EMS Configuration Guide* and the *Net-Net ACLI Reference Guide*.

SNMP Community Element

You need to ensure the `snmp-community` element is configured. Specifically, you need to ensure:

- IP address list contains the address of the host upon which EMS server is running. IP address(es) for SNMP communities for authentication purposes
- Access mode is READ-ONLY

Trap Receiver Element

You need to ensure the `trap-receiver` element is configured. Specifically, you need to ensure

- IP address is that of the Net-Net EMS server
- Filter level is set to All.
- Community name matches the name in the SNMP community element

About Configuring the Discovery

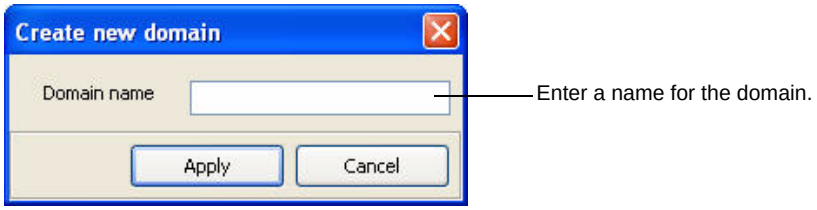
You need to create a domain in the Active configuration area before performing a Discovery. When configuring the Discovery, you choose the domain in which to store the discovered Net-Net SBCs.

Creating a New Domain

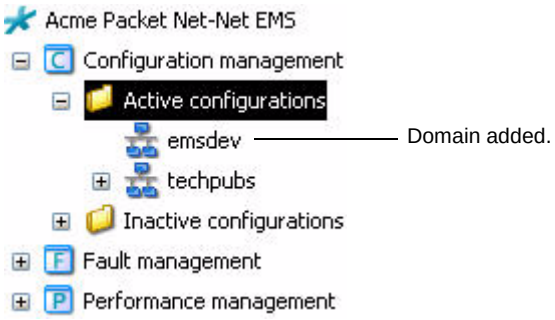
This section explains how to create a new domain. The Net-Net SBCs you discover are placed in a domain you define in the Active configurations area.

To add a domain:

1. Right-click Active configuration. The `Create domain` option appears. (You can also choose `Create domain` from the toolbar at the top of the window.)
2. Click the `Create domain` option to select it. The Create new domain dialog box appears. For example:



3. Enter the name for the domain you want to add and click **Apply**. A status message window appears.
4. Click **OK**. The domain name appears under the Active configuration heading. In the following example the domain named emsdev has been added:



The domain is also automatically added to the Inactive configurations area.

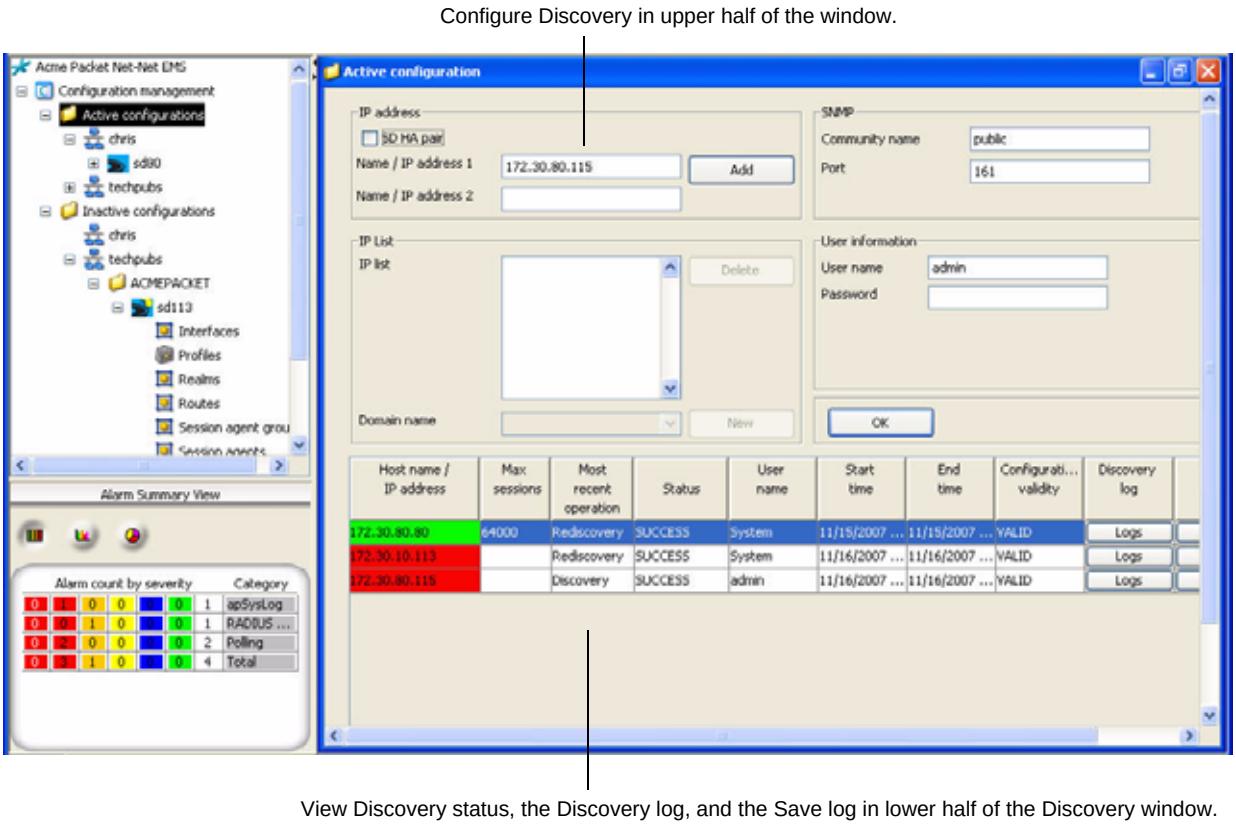
Accessing the Discovery Window

This section explains how to access the Discovery window. You use the Discovery window to enter the discovery configuration information and to view the discovery progress.

To access the Discovery window:

1. Click Active configurations in the Net-Net EMS navigation pane to display the Discovery window in the right pane.

   For example:



   You enter the Discovery configuration information in the section at the top of the window. The lower part of the window contains a Discovery table, see the following section for more information.

About the Discovery Table

The Discovery table contains information about the Discovery process. It also includes a Save log you can access to view information about saving a configuration. The following table lists the information contained in the Discovery table:

Option	Description
Host name/IP address	Host name or IP address for the standalone Net-Net SBC (or for both Net-Net SBCs in an HA pair) being discovered. This cell is color coded to indicate whether the Net-Net is reachable (status updated by the polling mechanism). • green: device is reachable • turquoise: device is not managed • red: device is unreachable (standalone or both Net-Net SBCs in an HA pair) • yellow: one of the Net-Net SBCs in an HA pair is unreachable
Max sessions	Maximum number of licensed sessions supported by the Net-Net SBC or by the active system in an HA pair
Most recent operation	Most recent operation that has occurred for the Net-Net SBC. The operations include: • Discovery • Rediscovery • Save
Status	Status of the discovery or rediscovery • In-progress: discovery or rediscovery is in progress • SUCCESS: discovery or rediscovery succeeded • FAILED: discovery or rediscovery failed
User name	Name of the user who invoked the discovery operation
Start time	Time the discovery or rediscovery operation started
End time	Time the discovery or rediscovery operation ended
Configuration validity	Indicates whether the Net-Net SBC's configuration is valid
Discovery log	Access the Discovery log to view information about the Discovery process
Save log	Access the Save log to view information about the Save process

About the Save Log

You can view information about Save configuration operations by viewing the Save log accessed from the Discovery table. For information about saving configurations, refer to the *Net-Net EMS Configuration Guide*.

Configuring the Discovery

This section explains how to configure a discovery. The discovery process identifies the Net-Net SBC in the network and collects configuration data that it stores in the Net-Net EMS database. You can configure discoveries for the following:

- standalone Net-Net SBC
- Net-Net SBC HA pair
- multiple systems (standalone and/or HA pairs) that have the same SNMP community name and port number, and the same ACP port.

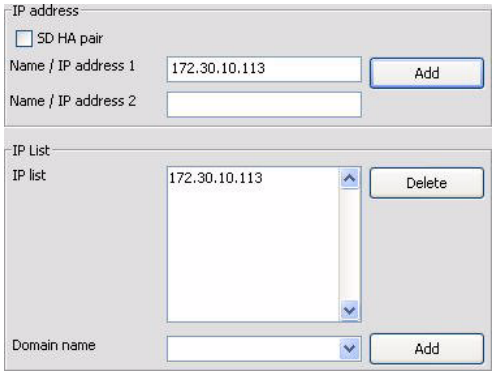
Entering the Net-Net SBC Addresses

You can enter a single address for a standalone Net-Net SBC, two addresses for an HA pair, or multiple addresses for a multi system discovery.

Standalone Net-Net SBC

To enter the address:

1. In the Discovery window, enter the IP address for the Net-Net SBC.
2. Click **Add**. The address appears in the IP list:



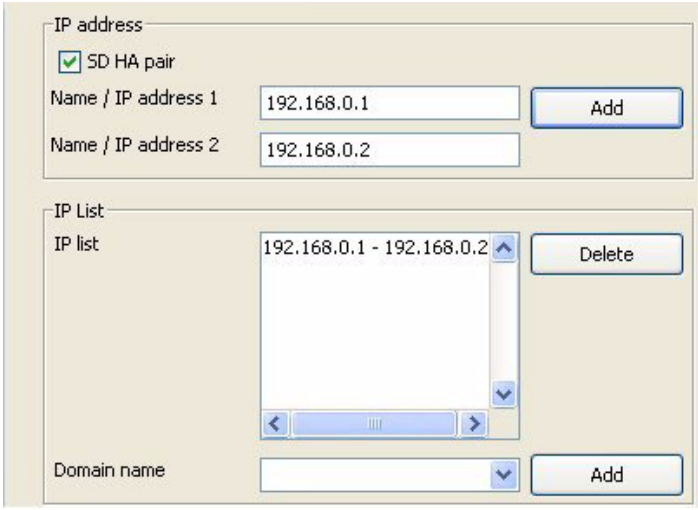
3. Complete the configuration by following the steps in *Completing the Configuration*.

Net-Net SBC HA Pair

To enter the addresses:

1. In the Discovery window:
   - **SD HA pair**—Click the checkbox.
   - **Name / IP address 1**—Enter the IP address for one of the Net-Net SBCs in the HA pair in the textbox.
   - **Name / IP address 2**—Enter the IP address for the second Net-Net SBC of the pair in the textbox.

2. Click **Add**. The addresses appear in the IP list:



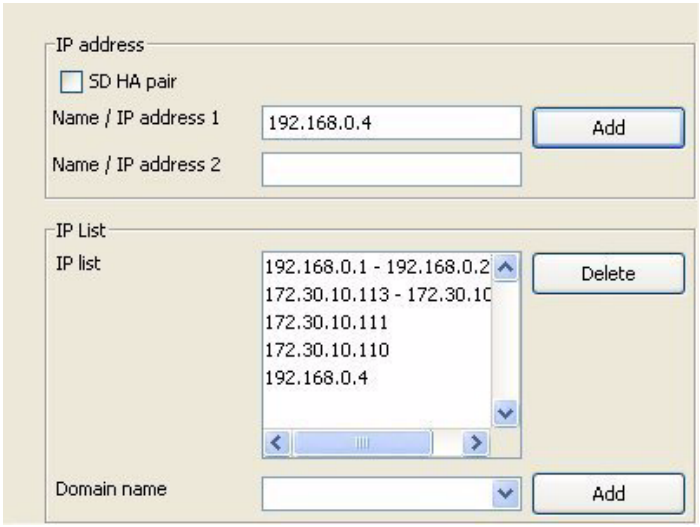
3. Complete the configuration by following the steps in *Completing the Configuration*.

Multiple Net-Net SBCs

To enter addresses:

1. In the Discovery window:
   - Enter the IP address for a standalone Net-Net SBC. See *Standalone Net-Net SBC* for details.
   - **SD HA pair**—Click the checkbox.
   - **Name / IP address 1**—Enter the IP address for one of the Net-Net SBCs in the HA pair in the textbox.
   - **Name / IP address 2**—Enter the IP address for the second Net-Net SBC of the pair in the textbox. See *Net-Net SBC HA Pair* for details.
2. Click **Add**. The address appears in the IP list.
3. Repeat steps 1 and 2 until you have added all IP addresses.

For example:



4. Complete the configuration by following the steps in *Completing the Configuration*.

Completing the Configuration

If discovering multiple Net-Net SBCs, the SNMP community name and port number, and the ACP port must be the same for all systems.

To complete the configuration:

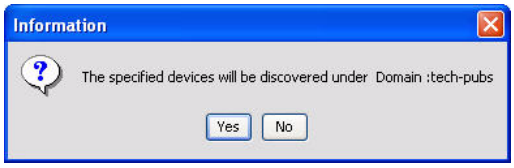
1. Enter a domain name by clicking the `Domain name` text box or down arrow to pick from a list of existing domains. For example:

   Or you can click **Add** to add a new domain. See *Creating a New Domain* for details.

2. Edit the default SNMP community name and port number if necessary. The SNMP community name is the name of an active community where this Net-Net SBC can send or receive SNMP information. Net-Net SBC events are reported to Net-Net EMS.
3. Edit the default Acme Control Protocol (ACP) port if necessary. The ACP port enables the Net-Net SBC to respond to ACP requests and is required for Net-Net EMS use.
4. Edit the user name if necessary.
5. Enter the password associated with the user name. All other areas are filled in for you. Valid user names and passwords include:
   - user and <login password> (for example: user and acme)
   - admin and <enable password> (for example: admin and packet)

   Note: Perform the discovery as the admin user if you plan to save the configuration.

6. Click **OK**. The following message appears:



7. Click **Yes** to clear the message and continue the discovery.

   The discovery process starts. A row is added to the Discovery table and the Status column shows the discovery is in progress:

Host name / IP address	Max sessions	Most recent operation	Status	User name	Start time	End time	Discovery log	Save log
172.30.10.114 - 172....	32000	Rediscovery	SUCCESS	admin	06/30/2005 12:34:07	06/30/2005...	Logs	Logs
172.30.10.75		Rediscovery	FAILED	System	06/30/2005 14:00:06	06/30/2005...	Logs	Logs
172.30.80.40		Rediscovery	FAILED	admin	06/30/2005 12:38:05	06/30/2005...	Logs	Logs
172.30.80.41		Rediscovery	In-progress	System	06/22/2005 13:40:04	-	Logs	Logs
172.30.10.113		Discovery	In-progress	admin	06/30/2005 14:09:11	-	Logs	Logs

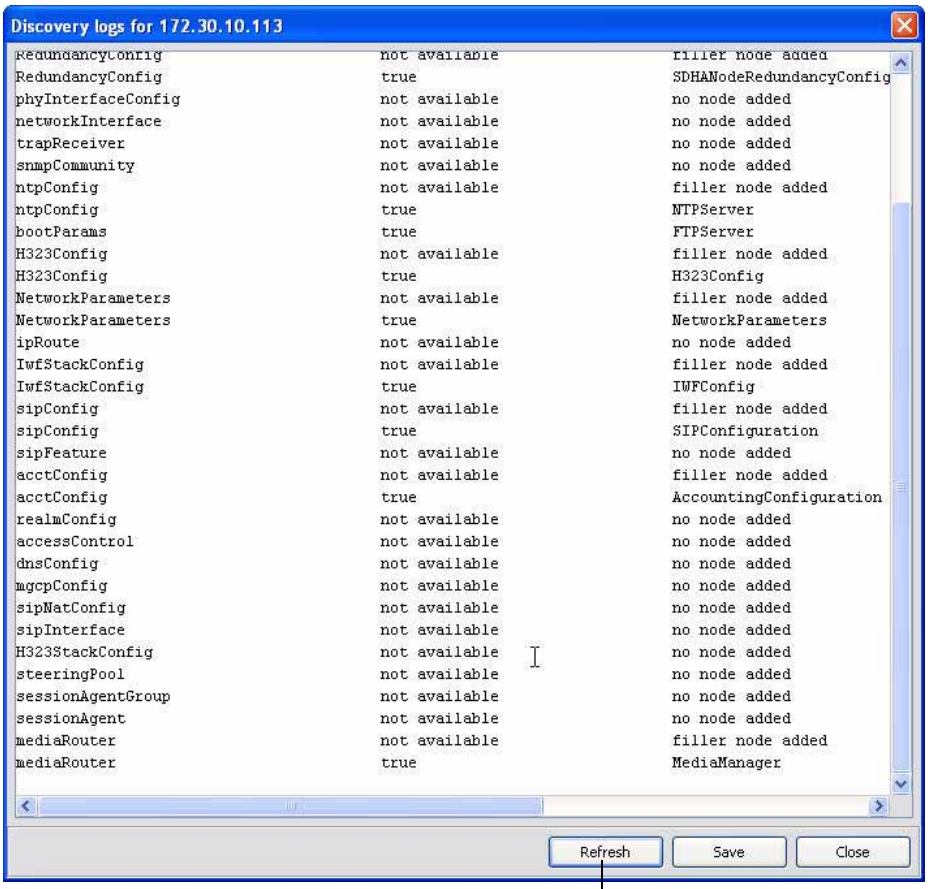
Color indicates status of IP host.

Status indicates Discovery is in progress.

The color of the cells in the first column indicate the status of the IP host:

- green: host is reachable
- turquoise: host is not managed
- red: host is unreachable (standalone or both Net-Net SBCs in an HA pair)
- yellow: one of the Net-Net SBCs in an HA pair is unreachable

8. In the Discovery log column, click **Logs** to access the Discovery log for the host you are discovering. The Discovery log for that host appears. For example:



9. Click **Refresh** to update the information displayed in the log.

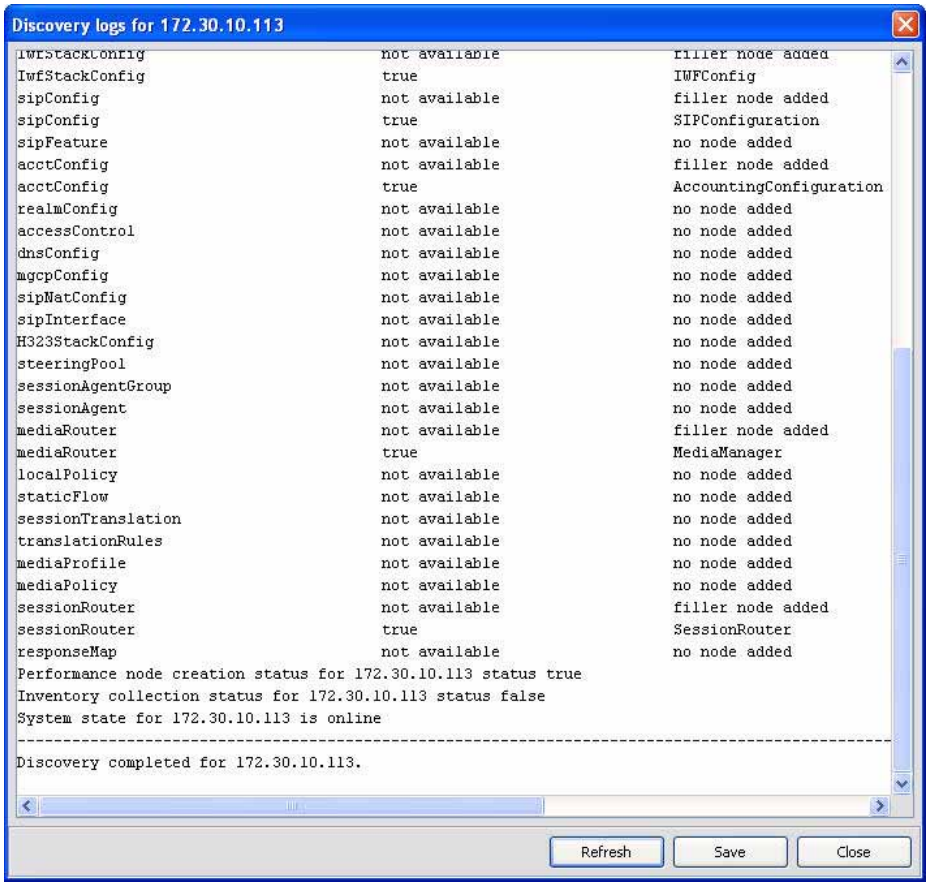
After the Discovery process is finished, the Discovery table is updated to display the status of the Discovery, Failed or Success:

Host name / IP address	Max sessions	Most recent operation	Status	User name	Start time	End time	Discovery log	Save log
172.30.10.114 - 172....	32000	Rediscovery	SUCCESS	admin	06/30/2005 12:34:07	06/30/2005...	Logs	Logs
172.30.10.75		Rediscovery	FAILED	System	06/30/2005 14:00:06	06/30/2005...	Logs	Logs
172.30.80.40		Rediscovery	FAILED	admin	06/30/2005 12:38:05	06/30/2005...	Logs	Logs
172.30.80.41		Rediscovery	In-progress	System	06/22/2005 13:40:04	-	Logs	Logs
172.30.10.113		Discovery	SUCCESS	admin	06/30/2005 14:20:58	06/30/2005...	Logs	Logs

Color indicates whether IP host can be reached.

Status indicates Discovery is successful.

The Discovery log displays the final data and results of the Discovery. For example:



10. Click **Close** to exit the Discovery log. Or to save the log data, click **Save**. The Save window appears displaying the default filename for the saved log in the format:

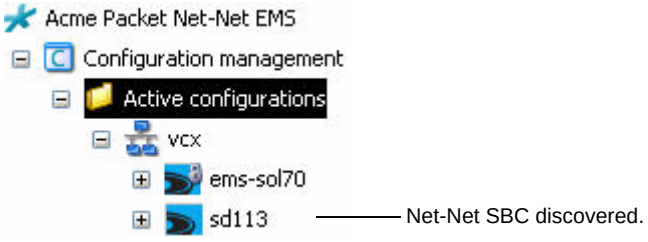
    <Host IP address>-Discovery.txt

    For example:

    172.30.10.113-Discovery.txt

11. Click **Save** to save the log.
12. Click **Close** to close the log window.

Upon completion of Discovery, the Net-Net SBC appears under the network name. The name of the Net-Net SBC is the same as that of the target name set in the boot parameters. For example:



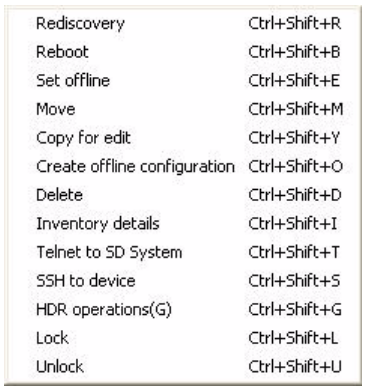
From here, you make a copy of the Net-Net SBC that goes under the Inactive configurations heading. You can then modify the configuration before saving it back to the Net-Net SBC.

Moving the Discovered Net-Net SBC

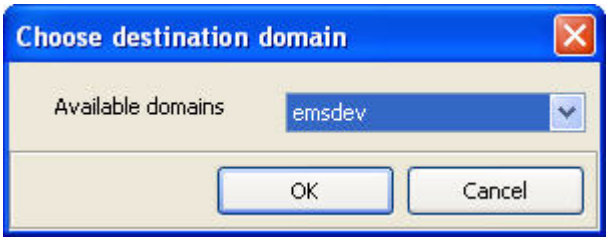
You can move the discovered Net-Net SBC to a different domain.

To move the discovered Net-Net SBC:

1. In the Active configurations area, right-click the name of the Net-Net SBC you want to move.
2. From the list of options, choose `Move`:



The Choose destination domain window appears:



3. Click the down arrow next to `Available domains` to access the list of destinations:

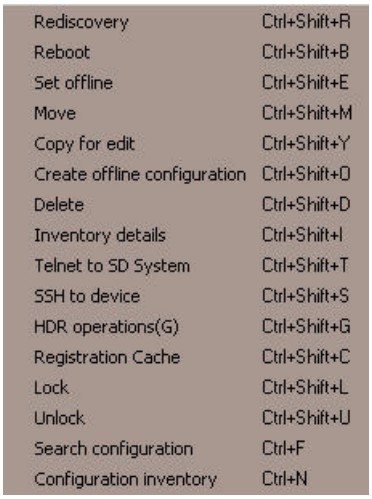
4. Select the target domain's name from the list.
5. Click **OK**. A confirmation message appears.
6. Click **Yes** to continue with the move. The Net-Net SBC is moved to the new domain. If you have saved a copy of this Net-Net SBC to the Inactive configurations area, it also gets moved to the new domain.

Rediscovering Net-Net SBCs

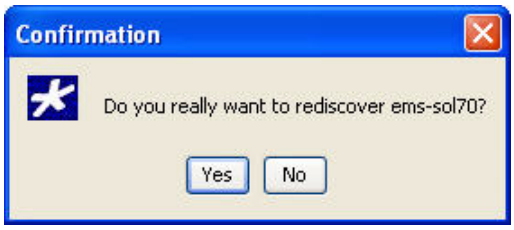
This section explains how to rediscover Net-Net SBCs. You can manually perform a rediscovery to collect updated inventory data to store in the Net-Net EMS database. Rediscovery is also automatically performed when the node is activated or rebooted.

To rediscover a Net-Net SBC:

1. In the Active configuration area, right-click the name of the Net-Net SBC you want to rediscover. A list of options appears:

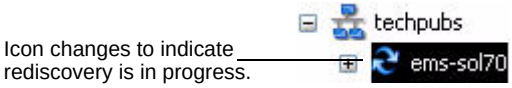


2. Choose `Rediscovery`. The following confirmation message appears:



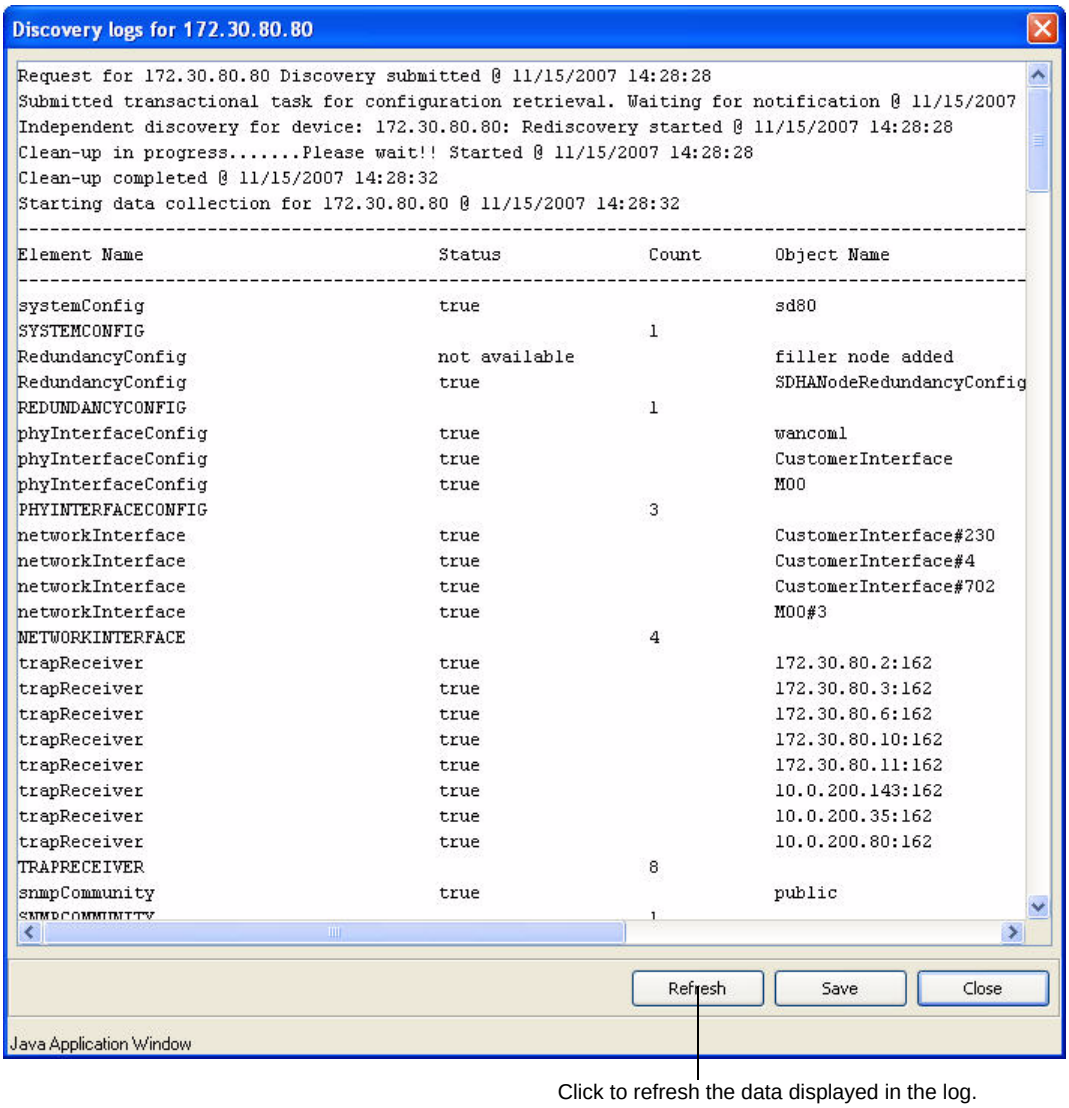
3. Click **Yes** to continue. The following message appears:

4. Click **OK** to clear the message. The rediscovery process begins. The icon for the Net-Net SBC in the Active configuration area changes to indicate rediscovery is occurring:



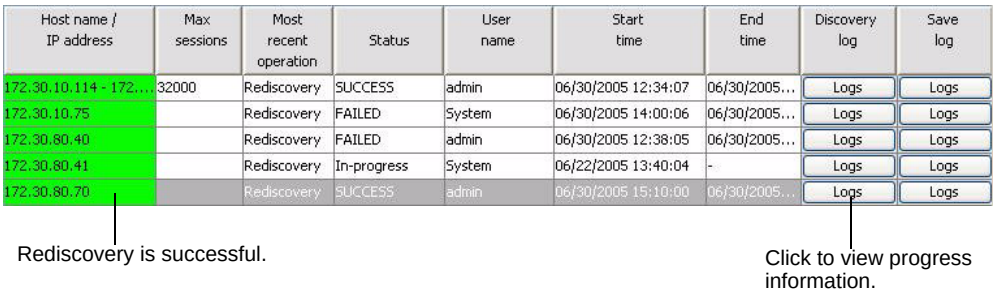
5. Click `Active configuration` to display the Discovery table. It will display the status of the rediscovery as being In Progress.

6. In the Discovery log column, click **Logs** to access the Discovery log for the host you are discovering. The Discovery log for that host appears displaying data about the rediscovery progress. For example:

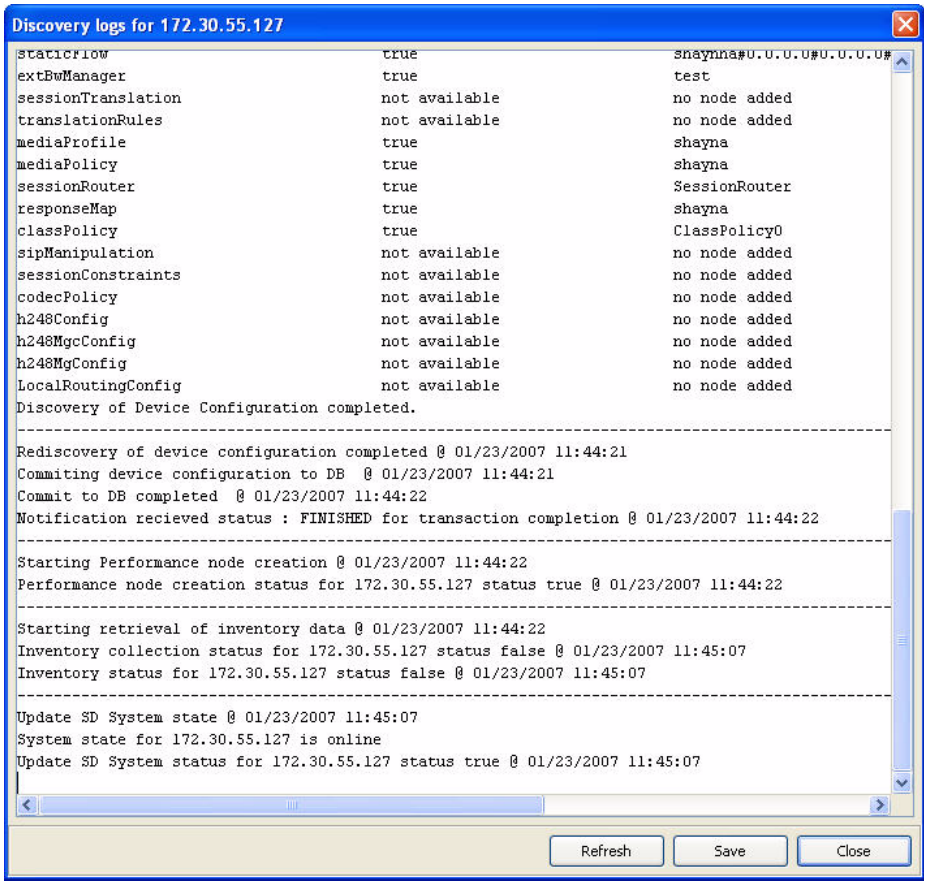


7. Click **Refresh** to update the information displayed in the log.

   After the rediscovery finishes, the status is updated in the Discovery table:



The Discovery log displays the final data and results of the rediscovery. For example:



8. Click **Close** to close the window. Or to save the log data, click **Save**. The Save window appears displaying the default filename for the saved log in the format:

   <Host IP address>-Discovery.txt

   For example:

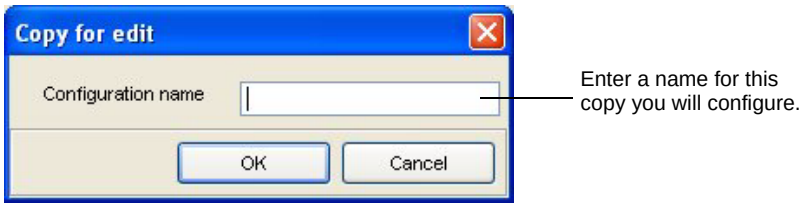
   172.30.80.70-Discovery.txt

9. Click **Save** to save the log.
10. Click **Close** to close the log window.

Copying the Net-Net SBC

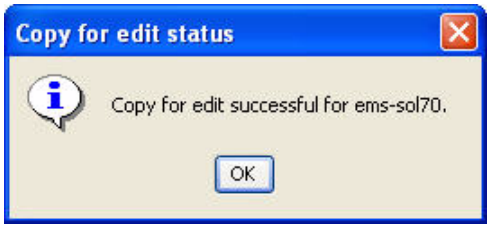
To copy the Net-Net SBC configuration to edit:

1. Click the newly discovered Net-Net SBC to select it.
2. Right-click to access the popup menu of options. (You can access the same list from the `SD system` option on the toolbar across the top of the screen.)
3. Click `Copy for edit` to select it. The Copy for edit screen appears. For example:

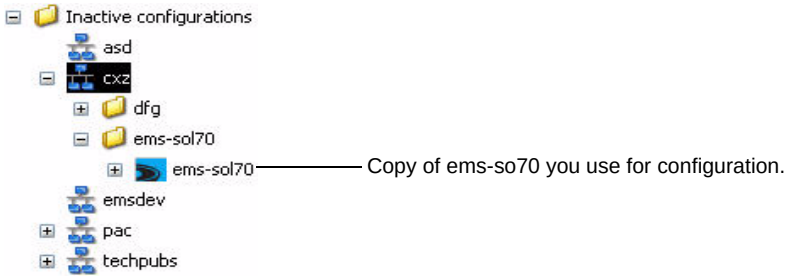


4. Enter a name for this Net-Net SBC copy which you will configure and click **OK**. You can use a descriptive name to indicate this is a copy. For example, ems-so70_Updated. (You cannot use spaces when naming the copy.)

   A progress message appears, followed by a status message:



5. Click **OK** to clear the message. A copy of the Net-Net SBC was placed under the Inactive configurations area:



   You can now edit the copy of the Net-Net SBC and save the changed configuration to the Net-Net SBC. Refer to the *Net-Net EMS Configuration Guide* for details about configuring, saving, and activating a Net-Net SBC.

   After the configuration is saved and activated, the Net-Net SBC notifies Net-Net EMS that its configuration has changed. Net-Net EMS automatically initiates a rediscovery process for the Net-Net SBC in the background. The progress bar at the bottom of the screen turns blue as the rediscovery begins. The icon in the left pane changes.

   When the rediscovery is complete, the Net-Net SBC in the Active configurations list reflects the newly activated configuration and the icon returns to its original form. The Most recent operation column in the Discovery window lists Rediscovery for that Net-Net SBC.

Renaming the Net-Net SBC Configuration Copy

You can rename the copy of the Net-Net configuration located in the Inactive configurations area.

To rename the Net-Net SBC configuration:

1. Right-click the copy of Net-Net-SBC.
2. Choose `Rename`. The Rename node window appears. For example:

3. **New node name**—Enter the new name.
4. Click **OK**.

4 Configuring Net-Net SBCs

Configuring SBCs

The *Net-Net EMS User Guide* does not include detailed information about configuring Net-Net SBCs. You can refer to the *Net-Net EMS Configuration Guide* for complete details about configuring Net-Net SBCs

This section does provide an overview of the Net-Net SBC configuration process and contains information about Net-Net EMS GUI features that relate to configuring Net-Net SBCs.

Configuration Overview

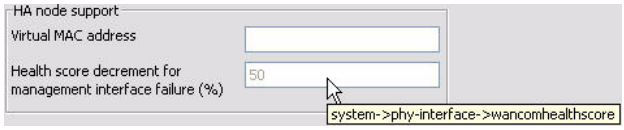
When you configure a Net-Net SBC, you follow a specific order. The recommended configuration order consists of the following:

- physical layer
- network interface
- realm and steering pool/media manager
- signaling services (SIP, H.323, MGCP)
- session agents
- routes

Tool Tips

If you are familiar with using the ACLI to configure Net-Net SBCs, you will notice that the Net-Net EMS organizes the configuration information differently from the ACLI organization, although for the most part the content is identical.

While configuring a Net-Net SBC, you can position your cursor over a parameter field or checkbox to view a tool tip. A tool tip displays the complete path to the corresponding ACLI parameter:



If no tool tip is available, the following message appears:

Locking Your Configuration

You can mark a configuration in either the Active or the Inactive configuration list as locked, which prevents other users from modifying that Net-Net SBC configuration using Net-Net EMS. While locked, you can make your edits to the configuration but no other user can modify it nor perform any operations such as copy it for edit, save it, activate it, and so on. Locking the active node ensures that only one user can provision the node by performing all right-click operations, except for the inventory function.

The lock state is saved to the database and is preserved across standalone server restarts and HA failovers. An audit trail entry is logged for the node locking and unlocking operations.

Locking active and inactive configuration nodes in Net-Net EMS applies only to the nodes maintained in Net-Net EMS. It has no impact on the Net-Net SBC itself or on the users of the Acme Packet command line interface (ACLI).

Lock Privileges

The node locking feature is available to users with the SD system configuration and Admin privileges. In addition, the Admin user can override any user's lock to unlock a node. This privilege is enabled by default for the Admin user. See the *Net-Net EMS Administration Guide* for more information about permissions. If you try to lock a node already locked by another user, the error message that appears contains the name of that other user.

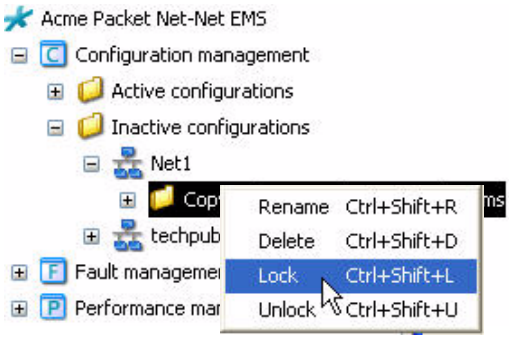
Locking and Unlocking an Inactive Configuration

When you lock your copy of a Net-Net SBC configuration in the Inactive configuration area, all nodes below that configuration node are also locked to prevent other users from modifying them. Only the user who locks the configuration can modify it. The configuration only becomes available to other users after it is unlocked.

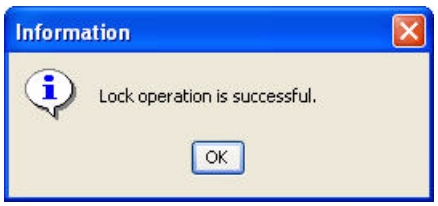
Only the user who locked the node can unlock it, with the exception of the user with Admin privileges. The Admin user can always override any user's lock by unlocking a node.

To lock an inactive configuration:

5. Right-click the configuration in the Inactive configuration area.

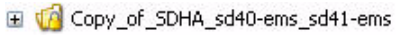


6. Choose **Lock** from the pop-up list of options. A confirmation message appears.



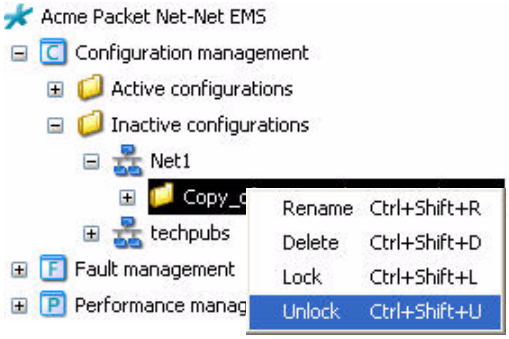
7. Click **OK** to clear the message.

   The Net-Net SBC icon in the navigation pane changes to indicate it is locked.

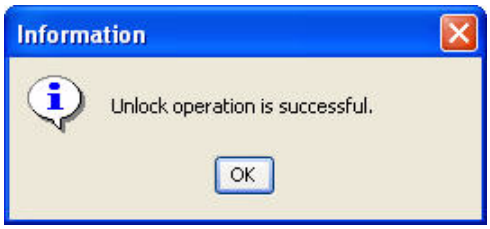


Unlocking an inactive configuration:

1. Right-click the configuration in the Inactive configuration area.



2. Choose **Unlock**. A confirmation message appears.



3. Click **OK** to clear the message. The Net-Net SBC icon in the navigation pane no longer displays a lock.

Locking and Unlocking an Active Configuration

When you lock an active node, only you will be able to perform the right-click operations:

- Rediscovery
- Reboot
- Set offline
- Move
- Copy for edit
- Create offline configuration
- Delete

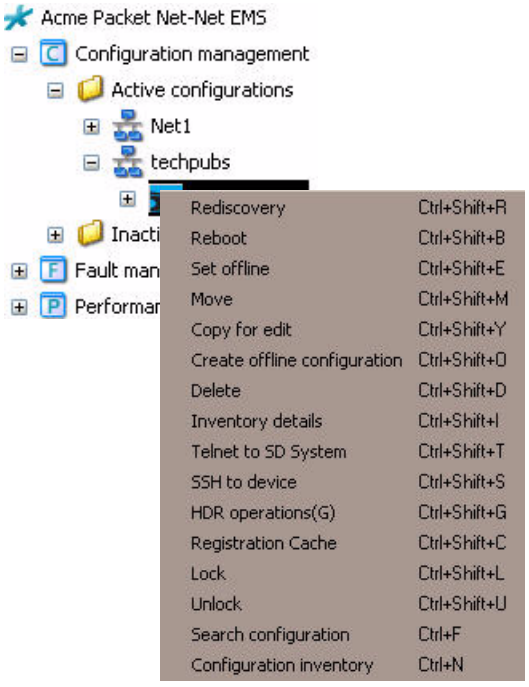
- Inventory details
- Telnet to System
- SSH to device
- HDR Operations (G)
- Registration Cache
- Lock
- Unlock
- Search configuration
- Configuration inventory

  Note: Because the Rediscovery operation is locked-out, automatic rediscovery of the Net-Net SBC is blocked. Automatic rediscovery occurs when a configuration on the Net-Net SBC is activated or the Net-Net SBC is rebooted. The user who locked the node has to manually perform a Rediscovery after saving and activating changes to a locked node.

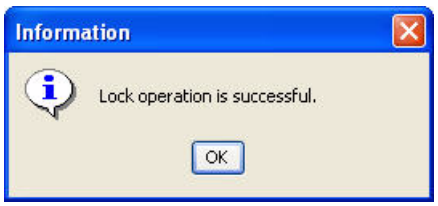
When you lock an active node, you lock the inactive copies associated with that node. All operations for those inactive copies are blocked. Any inactive configuration copies made by other users prior to the active node being locked cannot be applied to the Net-Net SBC while the active node is locked.

To lock an active configuration:

1. Right-click the configuration in the Active configuration area.

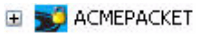


2. Choose **Lock** from the pop-up list of options. A confirmation message appears.



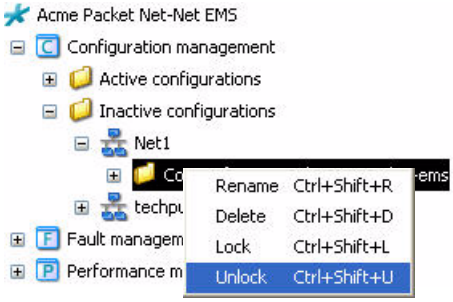
3. Click **OK** to clear the message.

   The Net-Net SBC icon in the navigation pane changes to indicate it is locked.

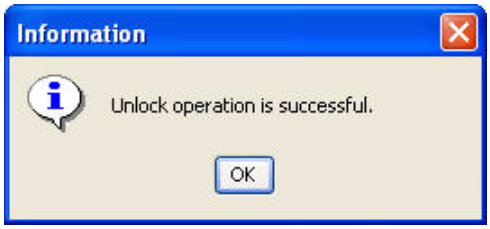


Unlocking an inactive configuration:

1. Right-click the configuration in the Inactive configuration area.



2. Choose **Unlock**. A confirmation message appears.



3. Click **OK** to clear the message. The Net-Net SBC icon in the navigation pane no longer displays a lock.

Configuration Search

You can search for and view top-level objects (for example, sip-interface, SIP manipulation) within an **active** node or **inactive** copy node by typing the Net-Net EMS label or the corresponding ACLI parameter name.

Once you access the configuration object, double-click it to view the details. A window appears and displays the valid settings. You can edit these settings from this window.

> **Note:** Active nodes and nodes locked by another user can only be viewed. Inactive and unlocked nodes can be viewed and edited if the user has the appropriate privileges.

Caveats

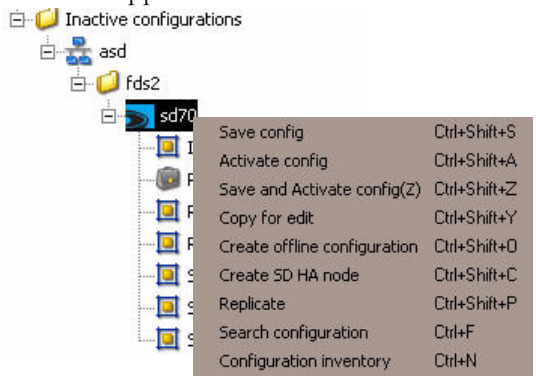
Certain types of configuration objects are not supported:

- Single-instance configuration elements, such as IWF and media manager configuration
- Configuration sub elements that do not lend themselves to viewing outside of the context of their parent element (for example, SIP header rules and element rules)

Searching for Configuration Objects

To use the search configuration function:

1. Right-click a Net-Net SBC Active or Inactive configuration. A pop-up list of functions appears.



2. Click Search configuration. The Select an object to search window appears.
3. Choose a configuration object by either:
   - Clicking the down arrow to scroll through the list. Click on the desired object to select it.
   - Typing the object name in the text field. If the name is found in the list, it will auto-complete once enough of the word is typed to distinguish it from others in the list.

   Several configuration objects may share similar names, for example, media policy, media profile, and media router. In these instances, you can type "media" and then click the desired object in the list, or keep typing until the object populates the text field. Typing "media po" will populate with "media policy."

For unique object names, you can type as little as one letter to locate the desired configuration object. For example, when you type "P" the field is populated with "Physical interface."

The following table lists a brief explanation of top-level objects. You can search for these top-level objects using the Net-Net EMS label or the corresponding ACLI parameter names. See the *ACLI Reference Guide* for parameter names.

Top-Level Object	Description
Access control	Accesses the Edit Access control window. See the *Security* chapter in the *Net-Net EMS Configuration Guide* for more information.
Account servers	Accesses the Edit Account servers window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
Alarm threshold	Accesses the Edit Alarm threshold window. See the *RADIUS Accounting Management* chapter in the *Net-Net Accounting Guide* for more information.
Authentication radius server	Accesses the Edit Authentication radius server window. See the *Getting Started* chapter in the *Net-Net EMS Configuration Guide* for more information.
CODEC policy	Accesses the Edit CODEC policy window. See the *Transcoding* chapter in the *Net-Net EMS Configuration Guide* for more information.
Certificate record	Accesses the Edit Certificate record window. See the *Using Net-Net EMS* chapter in the *Net-Net EMS User Guide* for more information.
DNS config	Accesses the Edit DNS config window. See the *Realms and Nested Realms* chapter in the *Net-Net EMS Configuration Guide* for more information.
ENUM config	Accesses the Edit ENUM config window. See the *Session Routing and Load Balancing* chapter in the *Net-Net EMS Configuration Guide* for more information.
Enforcement profile	Accesses the Edit Enforcement profile window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
External bandwidth manager	Accesses the Edit External bandwidth manager window. See the *Performance Management* chapter in the *Net-Net EMS User Guide* for more information.
External policy server	Accesses the Edit External policy server window. See the *Admission Control and Quality of Service Reporting* chapter in the *Net-Net EMS Configuration Guide* for more information.

Top-Level Object	Description
H323 service	Accesses the Edit H323 service window. See the *H323 Signaling Services* chapter in the *Net-Net EMS 4000 Configuration Guide* for more information.
H323 stack	Accesses the Edit H323 stack window. See the *H323 Signaling Services* chapter in the *Net-Net EMS 4000 Configuration Guide* for more information.
HMR	Accesses the Edit HMR window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
Host routes	Accesses the Edit Host routes window. See the *System Configuration* chapter in the *Net-Net EMS Configuration Guide* for more information.
Interface	Accesses the Edit Interfaces window. See the *System Configuration* chapter in the *Net-Net EMS Configuration Guide* for more information.
IPSec security association	Accesses the Edit IPSec security as so cation window. See the *Security* chapter in the *Net-Net EMS 4000 Configuration Guide* for more information.
IPSec security policy	Accesses the Edit IPSec security policy window. See the *Security* chapter in the *Net-Net EMS 4000 Configuration Guide* for more information.
LR tables	Accesses the Edit LR tables window. See the *IMS Support* chapter in the *Net-Net EMS Configuration Guide* for more information.
Local policy	Accesses the Edit Local policy window. See the *Session Routing and Load Balancing* chapter in the *Net-Net EMS Configuration Guide* for more information.
Local response map	Accesses the Edit Local response map window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
Local routing	Accesses the Edit Local routing window. See the *IMS Support* chapter in the *Net-Net EMS Configuration Guide* for more information.
MGCP config	Accesses the Edit MGCP config window. See the *MGCP/NCS Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
Management interface access list	Accesses the Edit Management interface access list window. See the *Security* chapter in the *Net-Net EMS 4000 Configuration Guide* for more information.
Media policy	Accesses the Edit Media policy window. See the *Realms and Nested Realms* chapter in the *Net-Net EMS Configuration Guide* for more information.
Media profile	Accesses the Edit Media profile window. See the following chapters for more information: *H.323 Signaling Services*, *IWF Services, Session Routing and Load Balancing*, or *External Policy Server*, all found in the *Net-Net EMS Configuration Guide*.

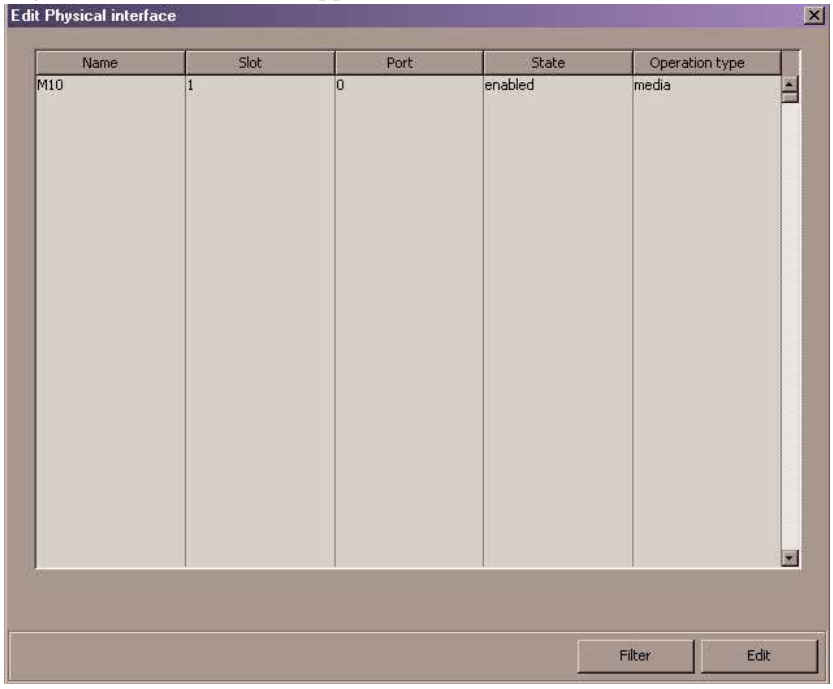
Top-Level Object	Description
Media router	Accesses the Edit Media route window. See the *Realms and Nested Realms* chapter in the *Net-Net EMS Configuration Guide* for more information.
NM control	Accesses the Edit NM control window. See the *Admission Control and Quality of Service Reporting* chapter in the *Net-Net EMS Configuration Guide* for more information.
Net management control	Accesses the Edit Net management control window. See the *Admission Control and Quality of Service Reporting* chapter in the *Net-Net EMS Configuration Guide* for more information.
Network interface	Accesses the Edit Network interface window. See the *System Configuration* chapter in the *Net-Net EMS Configuration Guide* for more information.
Physical interface	Accesses the Edit Physical interface window. See the *System Configuration* chapter in the *Net-Net EMS Configuration Guide* for more information.
Q850 SIP map	Accesses the Edit Q850 SIP map window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
QoS marking profile	Accesses the Edit QoS marking profile window. See the *Realms and Nested Realms* chapter in the *Net-Net EMS Configuration Guide* for more information.
RPH Policy	Accesses the Edit RPH Policy window. See the *Security* chapter in the *Net-Net EMS Configuration Guide* for more information.
RPH Profile	Accesses the Edit RPH Profile window. See the *Security* chapter in the *Net-Net EMS Configuration Guide* for more information.
Radius server	Accesses the Edit Radius server window. See the *Getting Started* chapter in the *Net-Net EMS Configuration Guide* for more information.
Realm	Accesses the Edit Realm window. See the *Realms and Nested Realms* chapter in the *Net-Net EMS Configuration Guide* for more information.
Realm media access	Accesses the Edit Realm media access window. See the *Realms and Nested Realms* chapter in the *Net-Net EMS Configuration Guide* for more information.
Route	Accesses the Edit Route window. See the *Session Routing and Load Balancing* chapter in the *Net-Net EMS Configuration Guide* for more information.
SIP NAT	Accesses the Edit SIP NAT window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
SIP Q850 map	Accesses the Edit SIP Q850 map window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
SIP Q850 mappings	Accesses the Edit SIP Q850 mappings window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.

Top-Level Object	Description
SIP enforcement	Accesses the Edit SIP enforcement window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
SIP feature	Accesses the Edit SIP feature window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
SIP interface	Accesses the Edit SIP Services window. {SIP Services includes SIP interface, SIP Nat interface, and SIP Option tag.} See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
SIP manipulation	Accesses the Edit SIP manipulation window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
SIP option tag	Accesses the Edit SIP option tag window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
SIP response map	Accesses the Edit SIP response map window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
SNMP community	Accesses the Edit SNMP community window. See the *System Configuration* chapter in the *Net-Net EMS Configuration Guide* for more information.
Security association	Accesses the Edit Security association window. See the *Security* chapter in the *Net-Net EMS Configuration Guide* for more information.
Security policy	Accesses the Edit Security policy window. See the *Security* chapter in the *Net-Net EMS Configuration Guide* for more information.
Session agent	Accesses the Edit Session agent window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
Session agent group	Accesses the Edit Session agent group window. See the *SIP Signaling Services* chapter in the *Net-Net EMS Configuration Guide* for more information.
Session constraints	Accesses the Edit Session constraints window. See the *Admission Control and Quality of Service Reporting* chapter in the *Net-Net EMS Configuration Guide* for more information.
Session group	Accesses the Edit Session group window. See the *Admission Control and Quality of Service Reporting* chapter in the *Net-Net EMS Configuration Guide* for more information.
Session translation	Accesses the Edit Session translation window. See the *Address Translation* chapter in the *Net-Net EMS Configuration Guide* for more information.
Static flow	Accesses the Edit Static flow window. See the *Static Flows* chapter in the *Net-Net EMS Configuration Guide* for more information.

Top-Level Object	Description
Steering pools	Accesses the Edit Steering pools window. {Steering pools may also be invoked using the Net-Net EMS label, Realm media address.} See the *Realms and Nested Realms* chapter in the *Net-Net EMS Configuration Guide* for more information.
Surrogate agent	Accesses the Edit Surrogate agent window. See the *IMS Support* chapter in the *Net-Net EMS Configuration Guide* for more information.
Syslog servers	Accesses the Edit Syslog servers window. See the *System Configuration* chapter in the *Net-Net EMS Configuration Guide* for more information.
System access list	Accesses the Edit System access list window. See the *Security* chapter in the *Net-Net EMS Configuration Guide* for more information.
TLS profile	Accesses the Edit TLS profile window. See the *Security* chapter in the *Net-Net EMS Configuration Guide* for more information.
Translation profile	Accesses the Edit Translation profile window. See the *Address Translation* chapter in the *Net-Net EMS Configuration Guide* for more information.
Translation rules	Accesses the Edit Translation rules window. See the *Address Translation* chapter in the *Net-Net EMS Configuration Guide* for more information.
Trap destination	Accesses the Edit Trap destination window. See the *System Configuration* chapter in the *Net-Net EMS Configuration Guide* for more information.
Trap receiver	Accesses the Edit Trap receiver window. See the *System Configuration* chapter in the *Net-Net EMS Configuration Guide* for more information.

4. Click **OK**. Net-Net EMS searches for and displays the configuration screen for the object.

For example, if you had chosen the Physical interface top-level object, the Edit Physical interface window appears.



From here, refer to the *Net-Net EMS Configuration Guide*, or the *Net-Net EMS Accounting Guide* for configuration instructions.

5 Viewing the Audit Log

Overview

This chapter explains how to view the audit log. The audit log provides information about the changes made to the copies of Net-Net SBCs using the Net-Net EMS. The audit log contains audit trails. Each audit trail contains information about an activity performed on the Net-Net SBC copy when using the Net-Net EMS. Audit trails enable you to view all operations that have been performed, the time they were performed, whether they were successful, and who performed them.

About the Information Logged

Information is logged for the following operations:

- Adding domains
- Discovering Net-Net SBCs
- Copying Net-Net SBCs for edit
- Creating an offline copy
- Creating Net-Net SBC HA pairs
- Creating Net-Net SBC HA pairs from offline configuration
- Creating standalone Net-Net SBCs from offline configuration
- Saving edits to a Net-Net SBC
- Deleting objects
- Rediscovering Net-Net SBCs
- Rebooting
- Switching HA pair roles
- Saving configurations
- Activating configurations
- Saving and activating configurations
- Rebooting and activating configurations

About the Audit Trail Information

Audit trails include the following information:

- User who performed the operation
- What operation was performed by the user
- When the operation was performed by the user
- Whether the operation performed by the user was successful or failed

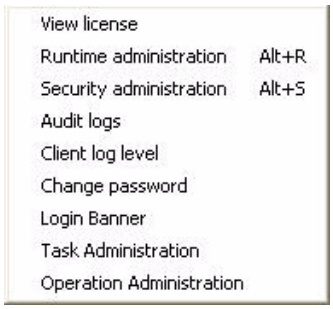
Viewing Audit Logs

This section explains how to view audit log's audit trail data. All users can access the Audit logs from the Tool menu, located in the Net-Net EMS toolbar. If you have the appropriate privileges, you can also access audit trail information from the Security Administration window. See *Security Administration* for details.

Accessing Audit Logs

To access audit logs:

1. From the Tool menu, choose `Audit logs`. For example:



The Audit log window appears:

From here you can choose the criteria you want to apply to the display of data. You can display audit trails by the following:

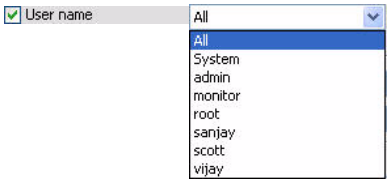
- user name
- date-time range
- user name and date-time range

If you do not choose the date-time range criterion, Net-Net EMS still limits the time to one day (24 hours). The 24 hours counts from the time you click View back 24 hours.

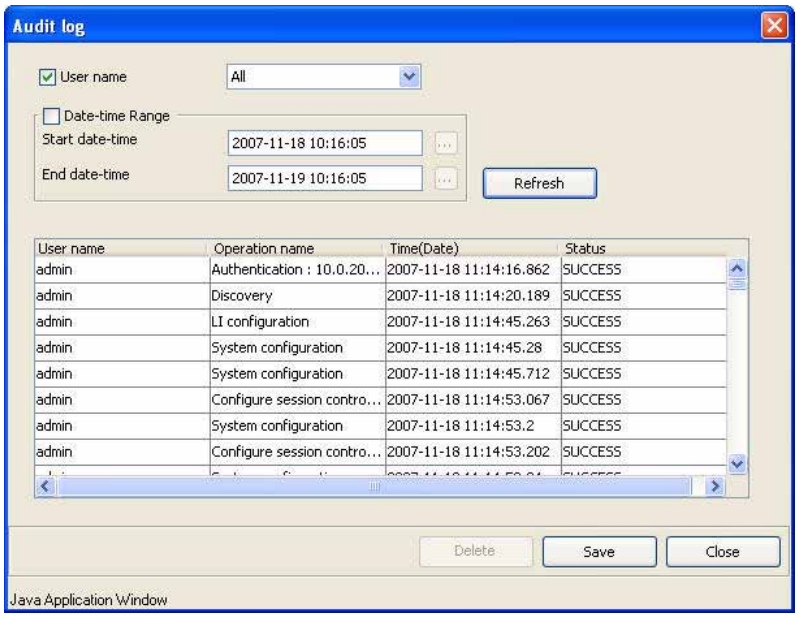
Displaying Audit Trails by User Name

To display audit trails by user name:

1. **User name**—Click the checkbox.
2. Click the down arrow next to the textbox to display the list of all users configured for this Net-Net SBC.



3. Click the user name to select it.
4. Click **View** to display the data. The Audit log window appears and the View button toggles to the Refresh button. For example, the following data is displayed for the user named admin:

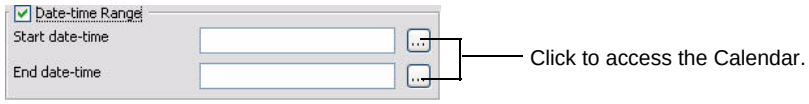


From here you can delete one or more audit trails displayed in the Log window and save the data to the file. See *Deleting Audit Trails* and *Saving Data* for details.

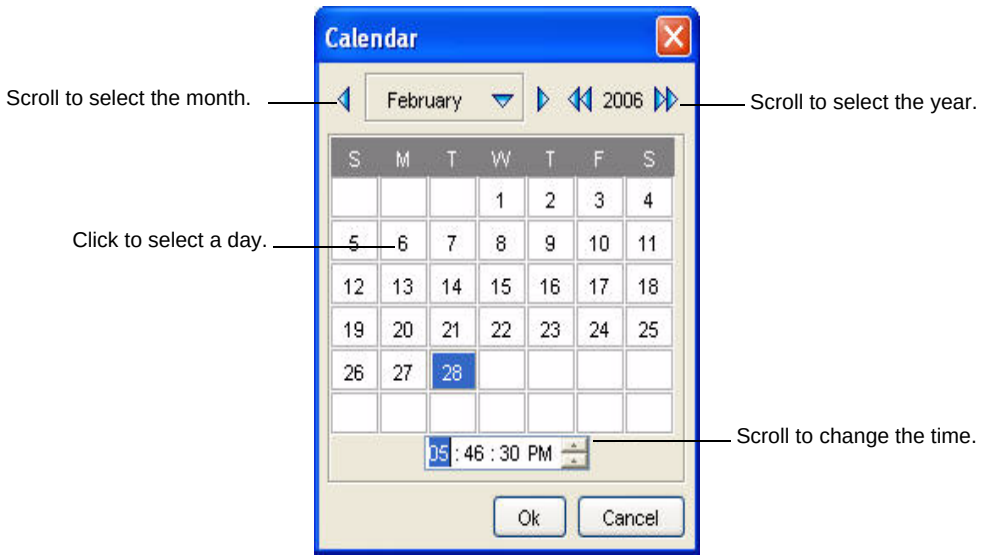
5. Click **Close** to exit the window.

Displaying Audit Trails by Date-Time Range

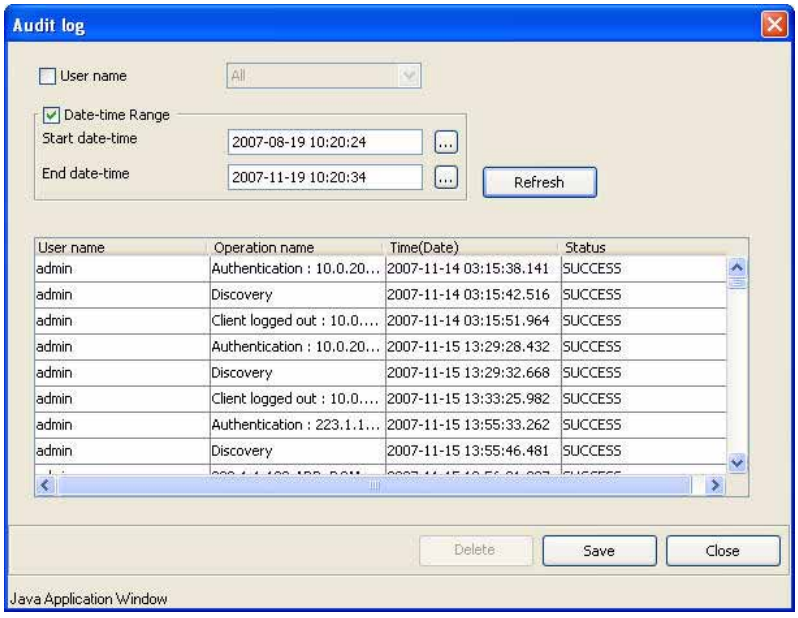
1. **Date-time Range**—Click the checkbox. The `Start date-time` and `End date-time` options are activated.



2. For the `Start date-time` and `End-date time`, click [...] to access the Calendar:



3. Choose the month and the year by using the arrows to scroll to the needed options.
4. Choose the day by clicking the appropriate cell.
5. Choose the time by scrolling up or down in the time textbox.
6. Click **OK** to exit the Calendar and apply the values.
7. Click **View** to display the data. The Audit log window appears and the View button toggles to the Refresh button:



From here you can delete one or more audit trails displayed in the Log window and save the data to the file. See *Deleting Audit Trails* and *Saving Data* for details.

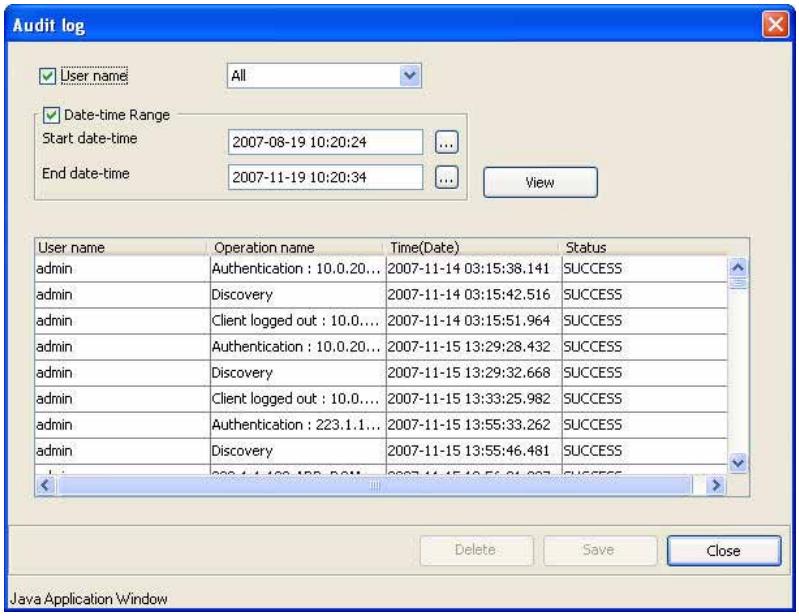
8. Click **Close** to exit the window.

Display Audit Trails by User Name and Date-Time Range

To display audit trails by user name and date-time range:

1. **User name**—Click the checkbox and choose the appropriate value.
2. **Date-time Range**—Click the checkbox and choose the appropriate values for `Start date-time` and `End date-time`.

3. Click **View** to display data. The Audit log window appears and the View button toggles to the Refresh button:



From here you can delete one or more audit trails displayed in the Log window and save the data to the file. See *Deleting Audit Trails* and *Saving Data* for details.

4. Click **Close** to exit the window.

About the Audit Trail Data

The following table defines the audit trail data displayed by Net-Net EMS:

Data	Description
User name	Name of the user associated with this audit trail. For example: • admin • system • monitor
Operation name	Description of the operation performed. The operation description can include the following information: • IP address of the origin of the request. For example, Authentication: 10.0.200.40 • Type of operation. For example, user authentication, user logout, adding new objects (OBJ_ADD), Net-Net SBC rediscovery and so on

Data	Description
Time(Date)	Date and time the operation occurred
Status	Final status of the operation. Values are: • SUCCESS • FAILED

Refreshing Audit Trail Data

You can update the audit trail data currently displayed in the Audit log window.

To refresh the data:

1. With audit trail data displayed in the Audit log window, click **Refresh**. The data currently displayed is updated.

Deleting Audit Trails

The Admin user can delete one or more audit trails displayed in the Log window.

To delete audit trails:

1. Click the row of the audit trail(s) you want to delete. You can select multiple contiguous rows by pressing Shift+click or multiple non-contiguous rows by pressing Ctrl+click.
2. Click **Delete**.

   A confirmation message appears:

3. Click **Yes** to delete the audit trail(s).

Saving Data

You can save the data displayed on each screen to a text file in comma separated format.

To save data to a file:

1. With the data displayed, click **Save**.

   A Save window appears.
2. Enter a name for the file and choose the location where you want to save the file.
3. Click **Save.**

6 Generating HDR Reports

Introduction

Historical data recording (HDR) refers to a group of management features that let you configure the Net-Net SBC to collect statistics about system operation and function, and then send those records to designated servers. System statistics, defined in detail below, are saved to a comma-separated value (CSV) file, which are then sent to the designated server(s).

Information types are grouped so that you can refer to a set of statistics by simply invoking their group name. Within each group, there are several metrics available.

Configuring Net-Net EMS for HDR Collection

You enable HDR by first turning on the system's collection function, then choosing the records you want to capture, and finally setting up server(s) to which you want records sent.

The main collect configuration (found within the main system configuration) allows you to create global settings that:

- Turn the HDR function on and off
- Set the sample rate in seconds, or the time between sample individual collections
- Set the time in seconds in between individual pushes to designated servers (configured in the push receiver configuration accessed via the collect configuration)
- Set the time you want the collect to start and stop; time is entered in year, month, day, hours, minutes, and seconds

You also configure setting for each group of data you want to collect, and the push receiver (server) to which you want data sent.

For complete details about configuring Net-Net EMS for HDR collection, see *Configuring HDR* in the *Net-Net EMS Decomposed SBC Essentials Guide*.

Group Record Types

In the group-name parameter for the group-settings configuration, you can enter any one of the groups record type defined in the following table. You specify the collection object, and then all metrics for these groups are sent.

Collection Object	Metrics Included
General system statistics (system)	• CPU utilization • Memory utilization • Health score • Redundancy state • Current signaling sessions • Current signaling session rate (CPS) • CAM utilization media • CAM utilization ARP • I2C bus state • License capacity
Interface statistics (interface)	• Interface index • Name/description • Type • MTU • Speed • Physical address • Administrative status • Operational state • In last change • In octets • In unicast packets • In non-unicast packets • In discards • Out errors • Out octets • Out unicast packets • Out non-unicast packets • Out discards • Errors
Combined session agent statistics (session-agent)	• Hostname • System name • Status • Inbound active sessions • Inbound session rate (CPS) • Outbound active sessions • Outbound session rate (CPS) • Inbound sessions admitted • Inbound sessions not admitted • Inbound concurrent sessions high • Inbound average session rate (CPS) • Outbound sessions admitted • Outbound sessions not admitted • Outbound concurrent sessions high • Outbound average session rate (CPS) • Max burst rate (in and out) (CPS) • Total seizures • Total answered sessions • Answer/seizure ratio • Average one-way signaling latency (ms) • Maximum one-way signaling latency (ms)

Collection Object	Metrics Included
Session realm statistics (session-realm)	• Realm name • Inbound active sessions • Inbound session rate (CPS) • Outbound active sessions • Outbound session rate (CPS) • Inbound sessions admitted • Inbound sessions not admitted • Inbound concurrent sessions high • Inbound average session rate (CPS) • Outbound sessions admitted • Outbound sessions not admitted • Outbound concurrent sessions high • Outbound average session rate (CPS) • Max burst rate (in and out) (CPS) • Total seizures • Total answered sessions • Answer/seizure ratio • Average one-way signaling latency (ms) • Maximum one-way signaling latency (ms)
Environmental voltage statistics (voltage)	• Voltage type • Description • Current voltage (mv)
Environmental fan statistics (fan)	• Fan type • Description • Speed
Environmental temperature statistics (temperature)	• Type • Description • Value (Celsius)
SIP status statistics (sip-sessions)	• Sessions • Subscriptions • Dialogs • Call ID map • Rejections • ReInvites • Media sessions • Media pending • Client transaction • Server transaction • Response contexts • Saved contexts • Sockets • Requests dropped • DNS transactions • DNS sockets • DNS results • Session rate • Load rate

Collection Object	Metrics Included
SIP error/event statistics (sip-errors)	• SDP offer errors • SDP answer errors • Drop media errors • Transaction errors • Media expiration events • Early media expirations • Early media drops • Expired sessions • Multiple OK drops • Multiple OK terminations • Media failure drops • Non-AXK 2XX drops • Invalid requests
SIP policy/routing (sip-policy)	• Local policy lookups • Local policy hits • Local policy misses • Local policy drops • Agent group hits • Agent groups misses • No routes found • Missing dialog • Inbound SA constraints • Outbound SA constraints • Inbound REG SA constraints • Outbound REG SA constraints • Requests challenged • Challenge found • Challenge not found • Challenge dropped
SIP server transaction (sip-server)	• All states • Initial • Trying • Proceeding • Cancelled • Established • Completed • Confirmed • Terminated
SIP client transactions (sip-client)	• All states • Initial • Trying • Calling • Proceeding • Cancelled • EarlyMedia • Completed • SetMedia • Established • Terminated
SIP ACL status (sip-ACL-status)	• Total entries • Trusted • Blocked
SIP ACL operations (sip-ACL-oper)	• ACL requests • Bad messages • Promotions • Demotions

Collection Object	Metrics Included
SIP session status (sip-status)	• Sessions initial • Sessions early • Sessions established • Sessions terminated • Dialogs early • Dialogs confirmed • Dialogs terminated
MGCP task state (mgcp-state)	• MGCP sessions • CA endpoints • GW endpoints • Media sessions • Client transactions • Server transactions • Pending MBCD • MGCP ALGs
MGCP transactions (mgcp-trans)	• Requests received • Responses sent • Duplicates received • Requests sent • Responses received • Retransmissions sent
MGCP media events (mgcp-media-events)	• Calling SDP errors • Called SDP errors • Drop media errors • Transaction errors • Media expiration events • Early media expiration • Expiration media drops
MGCP ACL status (mgcp-ACL)	• Total entries • Trusted • Blocked
ACL operation (mgcp-oper)	• ACL requests • Bad messages • Promotions • Demotions
H.323 statistics (h323-stats)	• Incoming calls • Outgoing calls • Connected calls • Incoming channels • Outgoing channels • Contexts • Queued messages • TPKT channels • UDP channels

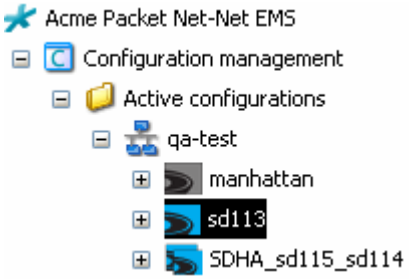
Configuring HDR Reporting Operations

You configure the HDR reporting operations to start and stop collection, to generate reports, and to purge HDR data from a Net-Net SBC.

Accessing HDR Operations

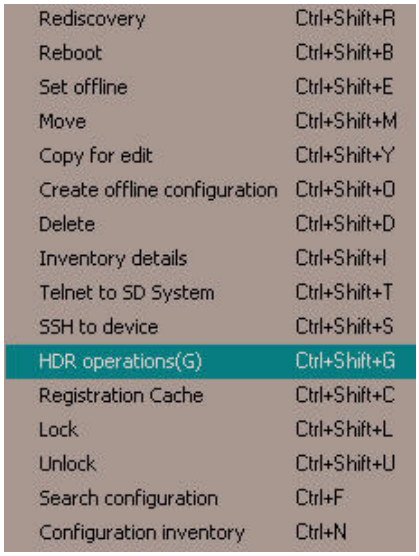
To access HDR operations:

1. In the Active configurations area, right click a Net-Net SBC.



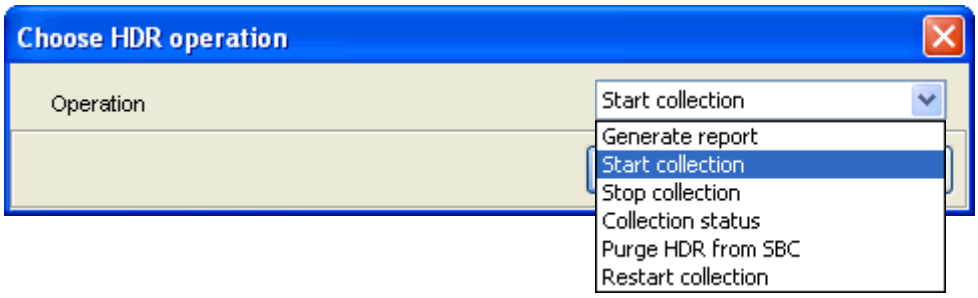
   A list of options appears.

2. Click HDR operations(G) to select it.



   The Choose HDR operation dialog box appears.

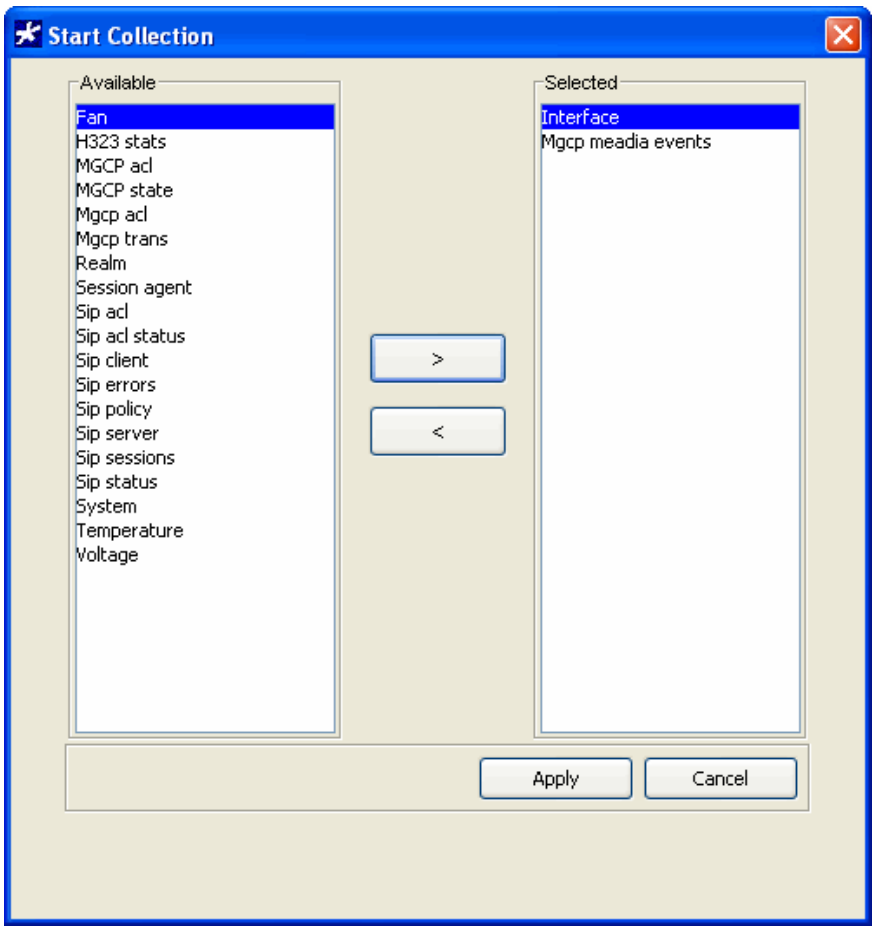
3. **Operation**—Choose the operation you want from the drop-down list.



Starting Data Collection

To start data collection:

1. Choose Start collection from the Choose HDR operation drop-down list.
2. Click **OK** to close the dialog box. The Start Collection window appears.
3. Click the collection group for which you want to start collection in the Available list.
4. Click >>> to move the collection group to the Selected list.



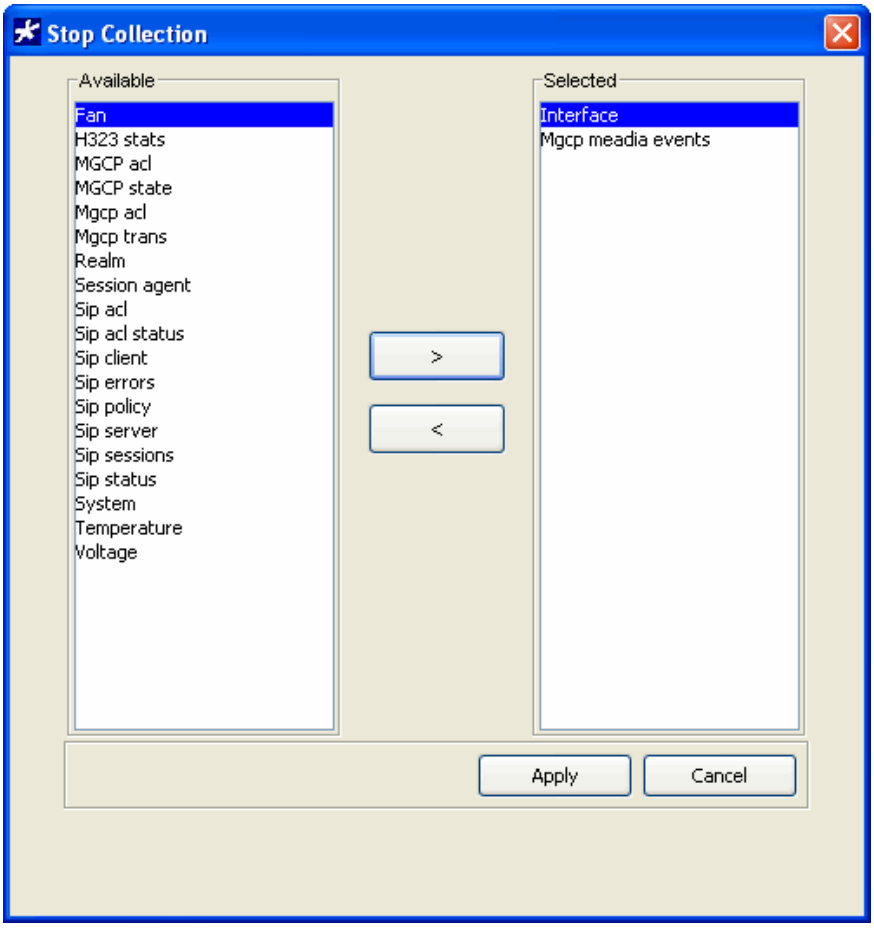
5. Repeat steps 3 and 4 for each collection group for which you want to start collection.
6. Click **Apply**. A Start collection is successful message appears.
7. Click **OK** to clear the message.

Stopping Data Collection

To stop collection:

1. Choose Stop collection from the Choose HDR operation drop-down list.
2. Click **OK** to close the dialog box. The Stop Collection window appears.
3. Click the collection group for which you want to stop collection in the Available list.

4. Click >>> to move the collection group to the Selected list.



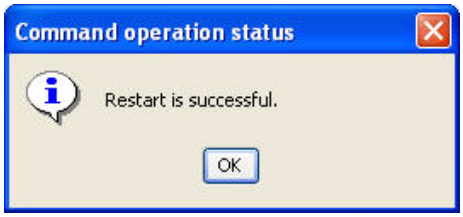
5. Repeat steps 3 and 4 for each collection group for which you want to stop collection.
6. Click **Apply**. A Stop collection is successful message appears.
7. Click **OK** to clear the message.

Restarting Collection

To restart collection:

1. Choose Restart collection from the Choose HDR operation drop-down list. A message appears that the restart is in progress.

   When the restart concludes a message appears stating restart is successful.

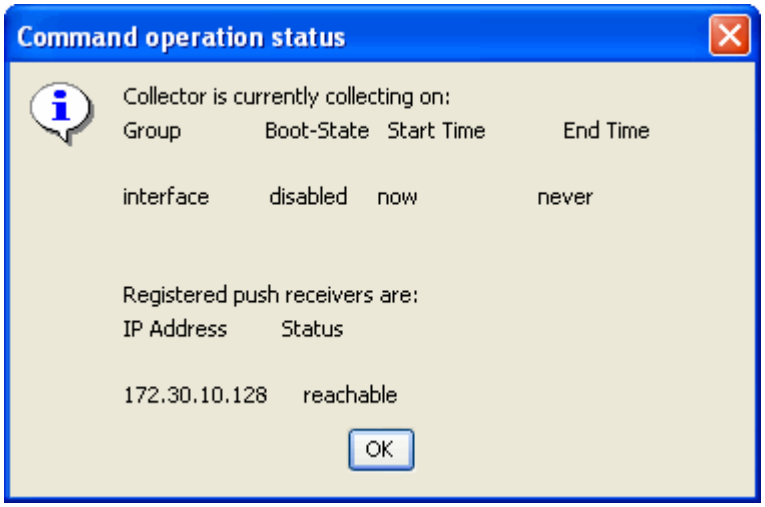


2. Click **OK** to close the dialog box.

Checking Collection Status

To check the status of the collection:

1. Choose Collection status from the Choose HDR operation drop-down list.
2. Click **OK** to close the dialog box. A message appears. Then the Command operation status window appears indicating the current collection status.



3. Click **OK** to close the status window.

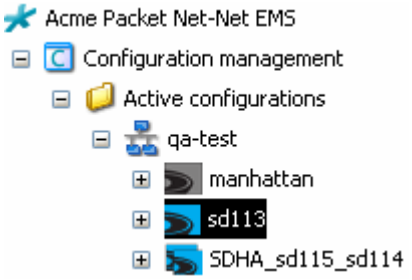
Generating Reports

You can generate HDR data reports by choosing the HDR operations(G) option in the right-click menu and then selecting your report criteria and report style.

Accessing the Report Generation Operation

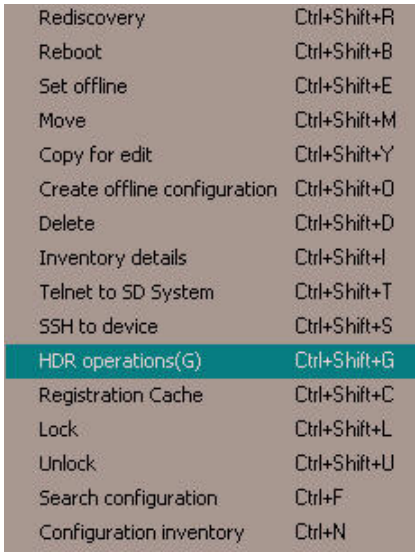
To access the report generation operation:

1. In the Active configurations area, right click a Net-Net SBC.



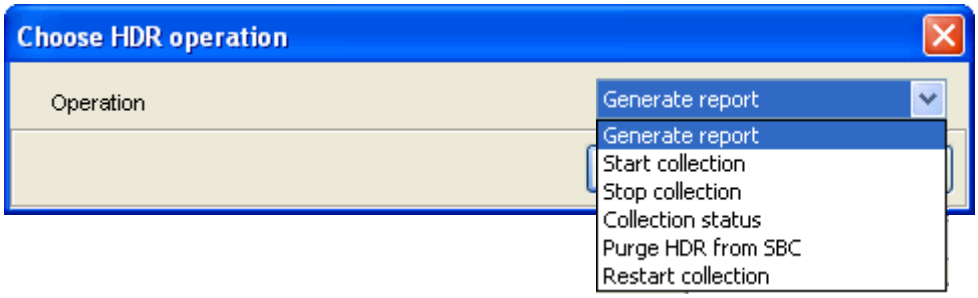
A list of options appears.

2. Click HDR operations(G) to select it.



The Choose HDR operation dialog box appears.

3. **Operation**—Choose the Generate report from the drop-down list.



The Report generation window appears.

Choosing Reporting Criteria

The process of generating the different reports is the same. You choose:

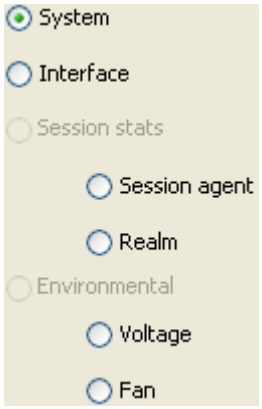
- Group on which you want to report
- Type of report you want to generate
- Start and end date and time of the reporting period
- Data you want to report on

  If generating an interface report, you need to choose the interface instance.

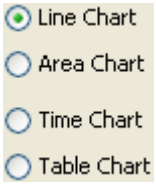
The following instructions show how to generate a line chart for system data. You use the same procedure for generating each type of report.

To generate system reports:

1. **Groups**—Click **System**.

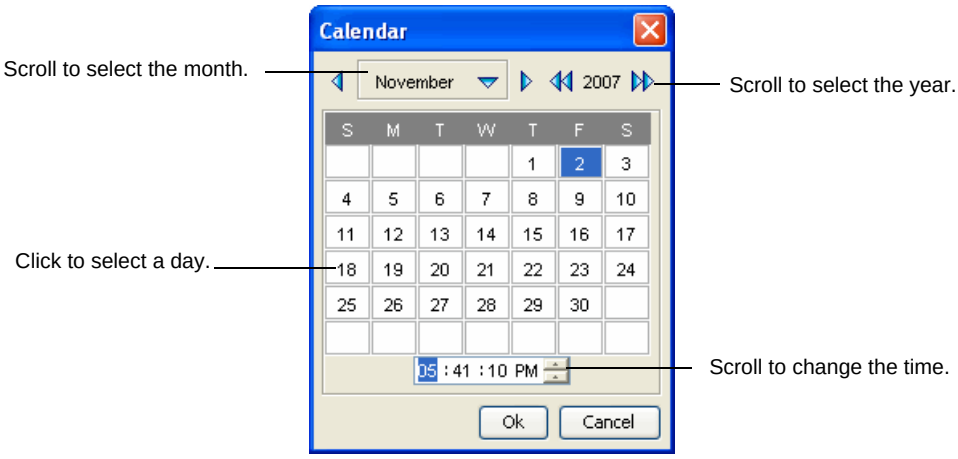


2. **Report Style**—Click the type of report you want. For example:



3. **Start date time**—Click the button with the three dots to access a calendar. Choose the exact date and time (for your local timezone) you want the reporting period to start.
4. **End date time**—Click the button with the three dots to access a calendar. Choose the exact date and time (for your local timezone) you want the reporting period to end.

The Calendar appears:

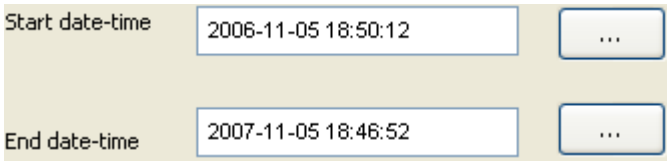


4a. Choose the month, and the year, for the date by scrolling to the month and year you need.

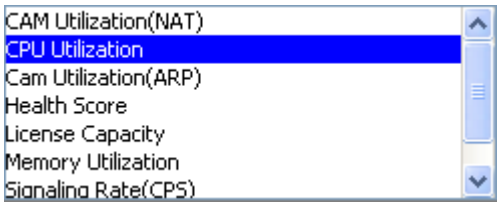
4b. Choose the day by clicking the appropriate cell.

4c. Choose the time by scrolling up or down in the time textbox.

5. Click **OK** to close the Calendar. The start and end dates and time for the reporting period appear in the Date/Time area.

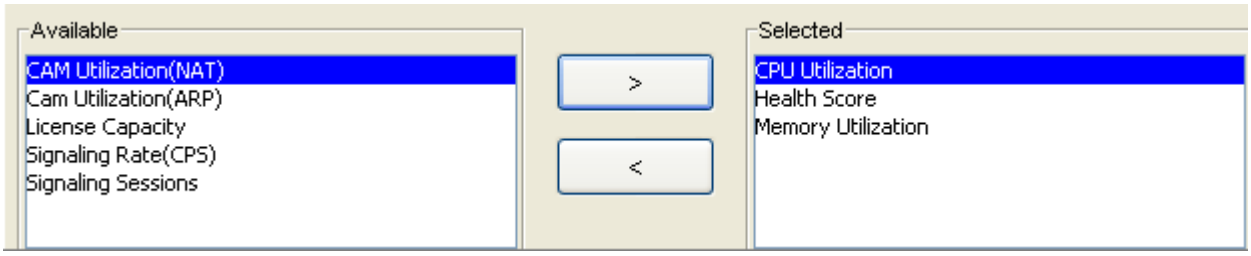


6. Choose the data upon which you want to report from the Available list.

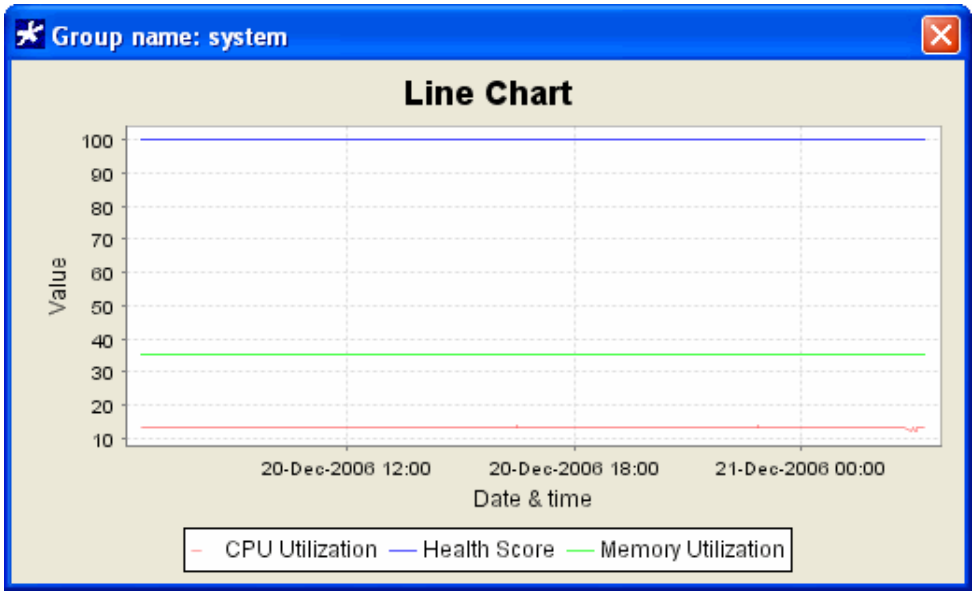


7. Click  to move the data to the Selected list.

8. Repeat steps 6 and 7 to choose the data upon which to report. For example:



9. Click **Apply**. The report you configured appears.



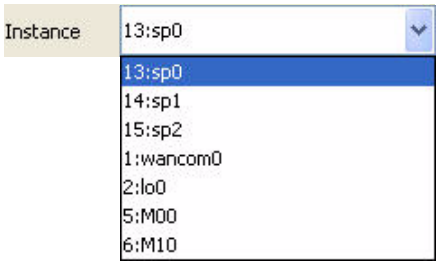
You can change the report type for this data by checking a different type and clicking **Apply** again.

Choose an Interface Instance

If you are generating a report on an interface, you need to choose the interface instance. When you choose Interface in the Groups section and enter the start and end date and time, the Instance parameter and Lookup button are activated in the Report Period section.

To choose the interface instance:

1. Click **Lookup**. The Instance parameter is populated with a list of instances.
2. Choose an instance from the Instance drop-down list.



3. Continue to configure the remaining reporting criteria.
4. Click **Apply** to generate the report.

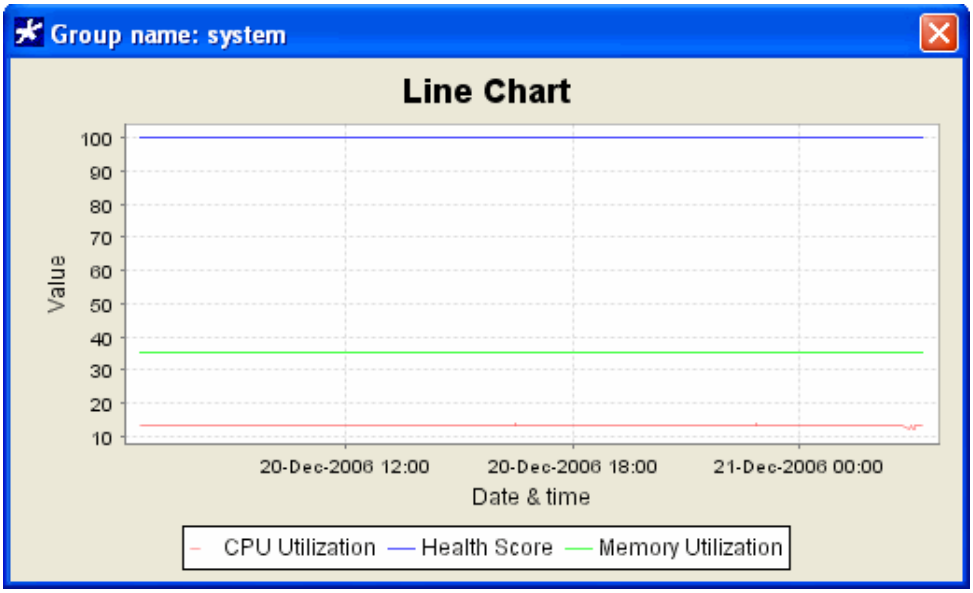
Examples of Report Styles

You can generate four different types of reports (charts):

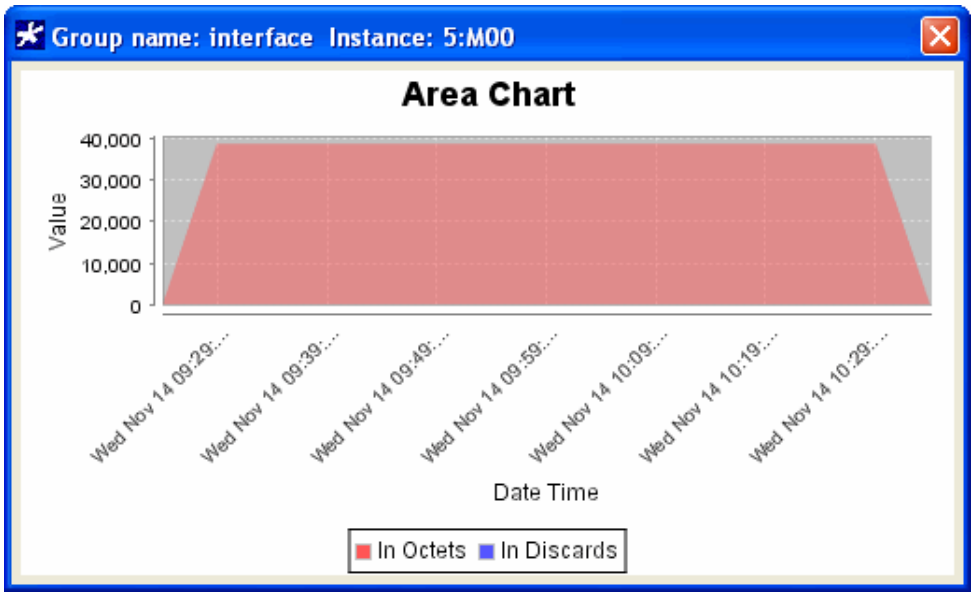
- Line
- Area
- Time
- Table

Line Chart

.



Area Chart



Time Chart

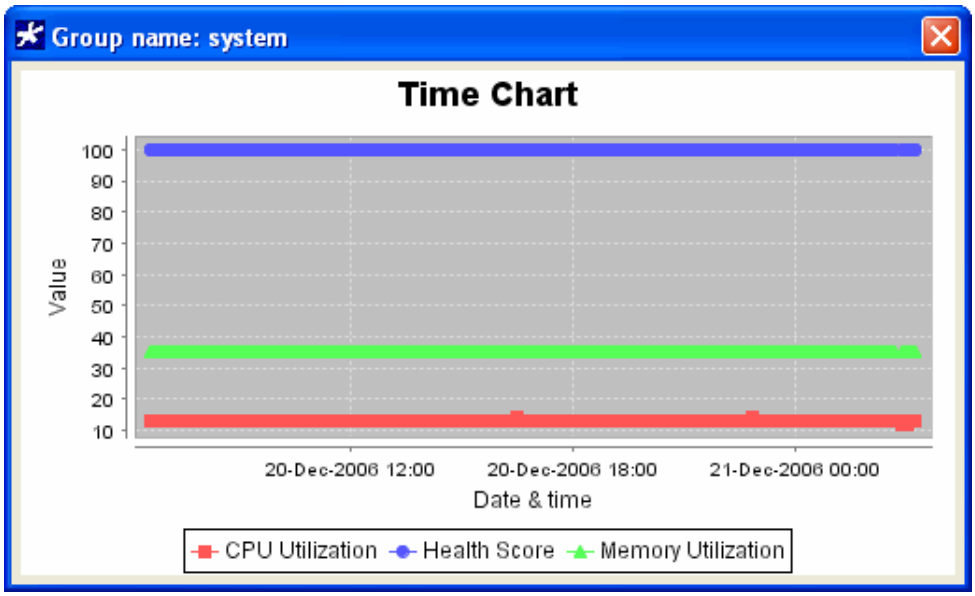


Table Chart

Group name: system

Date Time	CPU Utilization	Health Score	Memory Utilization
Wed Dec 20 06:36:...	13.0	100.0	35.0
Wed Dec 20 06:37:...	13.0	100.0	35.0
Wed Dec 20 06:38:...	13.0	100.0	35.0
Wed Dec 20 06:39:...	13.0	100.0	35.0
Wed Dec 20 06:40:...	13.0	100.0	35.0
Wed Dec 20 06:41:...	13.0	100.0	35.0
Wed Dec 20 06:42:...	13.0	100.0	35.0
Wed Dec 20 06:43:...	13.0	100.0	35.0
Wed Dec 20 06:44:...	13.0	100.0	35.0
Wed Dec 20 06:45:...	13.0	100.0	35.0
Wed Dec 20 06:46:...	13.0	100.0	35.0
Wed Dec 20 06:47:...	13.0	100.0	35.0
Wed Dec 20 06:48:...	13.0	100.0	35.0
Wed Dec 20 06:49:...	13.0	100.0	35.0
Wed Dec 20 06:50:...	13.0	100.0	35.0
Wed Dec 20 06:51:...	13.0	100.0	35.0
Wed Dec 20 06:52:...	13.0	100.0	35.0
Wed Dec 20 06:53:...	13.0	100.0	35.0
Wed Dec 20 06:54:...	13.0	100.0	35.0
Wed Dec 20 06:55:...	13.0	100.0	35.0
Wed Dec 20 06:56:...	13.0	100.0	35.0
Wed Dec 20 06:57:...	13.0	100.0	35.0
Wed Dec 20 06:58:...	13.0	100.0	35.0
Wed Dec 20 06:59:...	13.0	100.0	35.0
Wed Dec 20 07:00:...	13.0	100.0	35.0

7 Inventory Management

Introduction

This chapter describes the Net-Net EMS inventory management component. Each time Net-Net EMS does a discovery or rediscovery of a Net-Net SBC system, the inventory information for that system is retrieved and stored in the database. The results of each new discovery/rediscovery overwrites the existing inventory contents of the database.

Inventory data is maintained for all the nodes and Net-Net SBCs present in the Active configuration area. If a device is deleted from Active configuration, its inventory data is deleted from the database.

Inventory Data Collected

Inventory information is collected on the following Net-Net SBC components:

- hardware components and versions
- software components, which includes software images (current image and other loaded images - includes version) and configuration files (current file and other loaded files)
- software license key

Accessing Inventory Information

This section explains how to access the Inventory management information.

Accessing Inventory Data

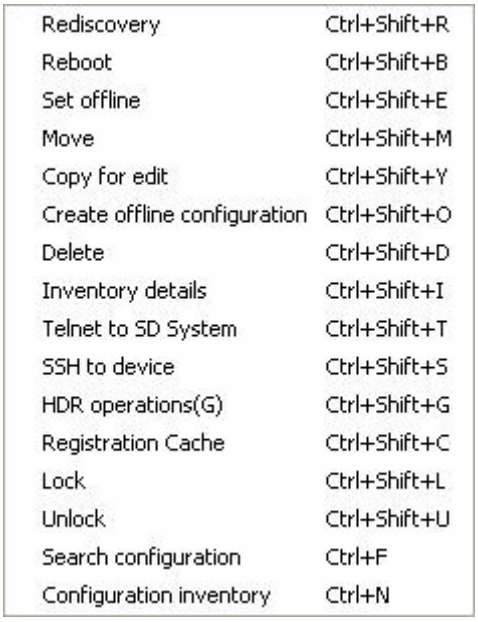
You can use the following methods to access inventory information:

- Right-click a specific Net-Net SBC listed under Active configuration and select Inventory details. The Inventory window only displays the details for that Net-Net SBC. (You cannot choose another from the Inventory window.)
- Choose Inventory details from the Inventory option located in the menu bar across the top of the Net-Net EMS screen. You then choose the Net-Net SBC for which you want to view data from the Inventory window. (You can make different choices while in the Inventory window.)

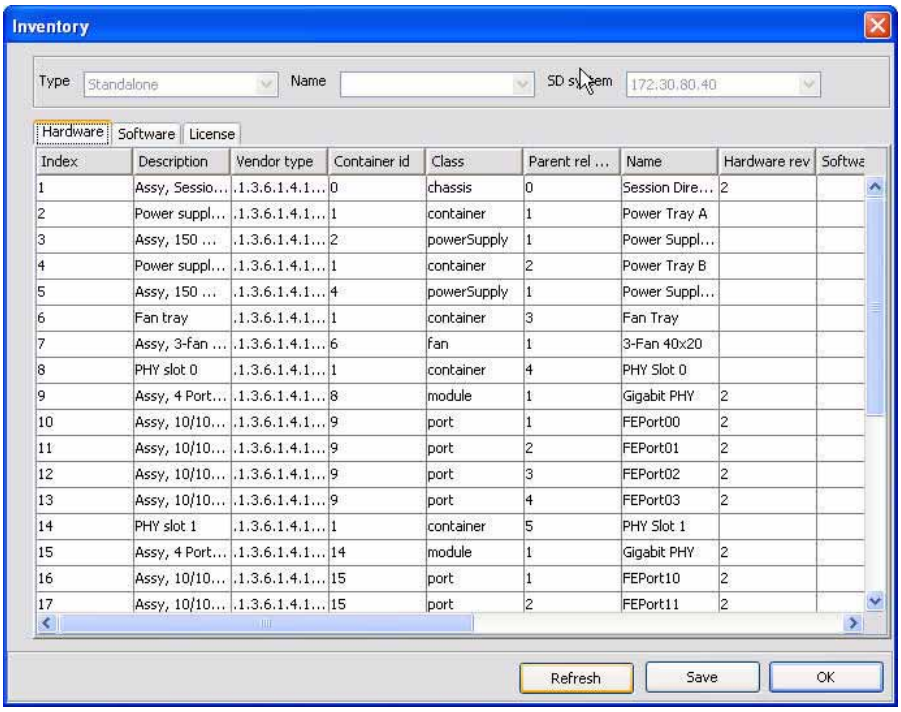
Accessing Data for a Specific Net-Net SBC

To access inventory management information:

1. Under the `Active configuration` category, right-click the name of the Net-Net SBC for which you want to view inventory data. A list of options appears:



2. Click `Inventory details` to select it. The Inventory window opens, with data for the specific Net-Net SBC displayed:



Index	Description	Vendor type	Container id	Class	Parent rel ...	Name	Hardware rev	Softwa
1	Assy, Sessio...	.1.3.6.1.4.1...	0	chassis	0	Session Dire...	2	
2	Power suppl...	.1.3.6.1.4.1...	1	container	1	Power Tray A		
3	Assy, 150 ...	.1.3.6.1.4.1...	2	powerSupply	1	Power Suppl...		
4	Power suppl...	.1.3.6.1.4.1...	1	container	2	Power Tray B		
5	Assy, 150 ...	.1.3.6.1.4.1...	4	powerSupply	1	Power Suppl...		
6	Fan tray	.1.3.6.1.4.1...	1	container	3	Fan Tray		
7	Assy, 3-fan ...	.1.3.6.1.4.1...	6	fan	1	3-Fan 40x20		
8	PHY slot 0	.1.3.6.1.4.1...	1	container	4	PHY Slot 0		
9	Assy, 4 Port...	.1.3.6.1.4.1...	8	module	1	Gigabit PHY	2	
10	Assy, 10/10...	.1.3.6.1.4.1...	9	port	1	FEPort00	2	
11	Assy, 10/10...	.1.3.6.1.4.1...	9	port	2	FEPort01	2	
12	Assy, 10/10...	.1.3.6.1.4.1...	9	port	3	FEPort02	2	
13	Assy, 10/10...	.1.3.6.1.4.1...	9	port	4	FEPort03	2	
14	PHY slot 1	.1.3.6.1.4.1...	1	container	5	PHY Slot 1		
15	Assy, 4 Port...	.1.3.6.1.4.1...	14	module	1	Gigabit PHY	2	
16	Assy, 10/10...	.1.3.6.1.4.1...	15	port	1	FEPort10	2	
17	Assy, 10/10...	.1.3.6.1.4.1...	15	port	2	FEPort11	2	

From here you can navigate through the different categories of inventory data by clicking the Hardware, Software, or License tab. You can save the displayed data to a text file. See the following sections for details.

Note: You cannot select a different Net-Net SBC from the Inventory window. See *Accessing Data for All Discovered Net-Net SBCs* for information about choosing from among multiple systems.

No Available Data

An error message appears when there is no Inventory data for a Net-Net SBC, which can occur if the Net-Net SBC is not properly configured for SNMP or if the discovery process was interrupted.

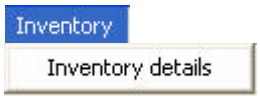
- Standalone: Clear the error message and choose a different system under the Active configuration area
- HA pair: Clear the error message. From the Inventory window, click the down arrow next to SD system and choose the other Net-Net SBC in the pair. If no data is available for it, close the Inventory window and select another HA pair from under the Active configuration area.

Accessing Data for All Discovered Net-Net SBCs

You can access the Inventory window once, then choose the different standalone Net-Net SBCs, or Net-Net SBC pairs, for which you want to view inventory data.

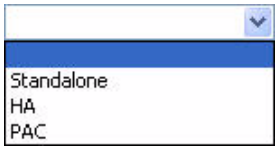
To view inventory data for all discovered systems:

1. From the Inventory toolbar option, choose `Inventory details`:



   The Inventory window appears.

2. In the Inventory window, click the down arrow next to the `Type` textbox to display the type of Net-Net SBCs. For example:



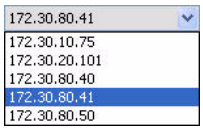
   Note: The PAC option is not supported in this release of Net-Net EMS.

3. Choose either `Standalone` or `HA` from the list. See the instructions in the following sections for more details.

Viewing Standalone Data

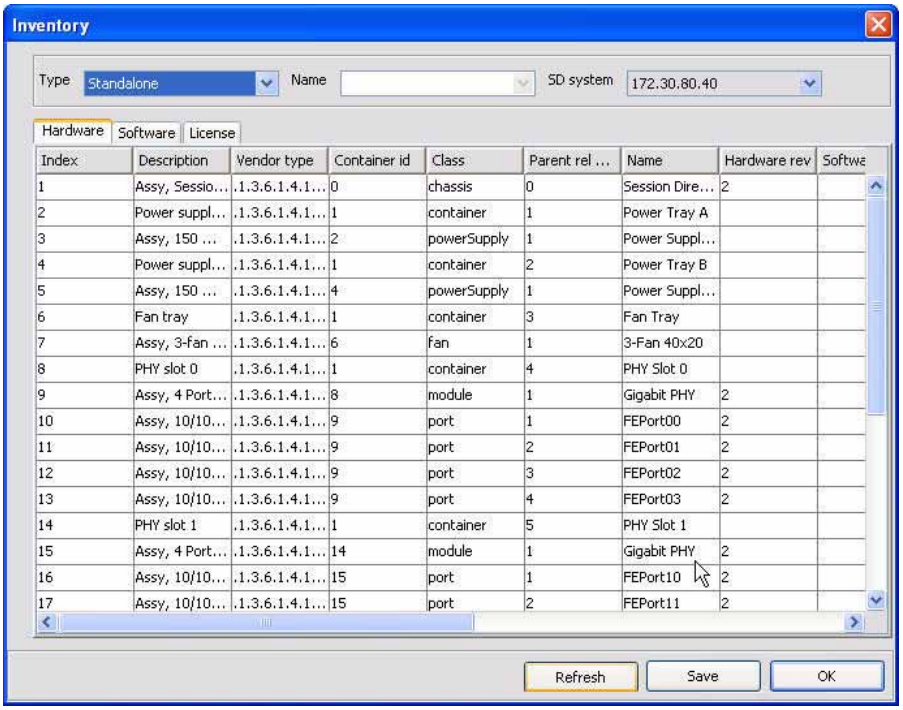
To view standalone data:

1. From the Type dropdown list, click `Standalone`.
2. Click the down arrow next to the `SD system` textbox to display all currently discovered standalone systems. For example:



3. Click the name of the system for which you want to view data.

4. The Inventory window appears with data displayed. By default, the hardware data for the Net-Net system you chose is displayed (if any data is available). For example:



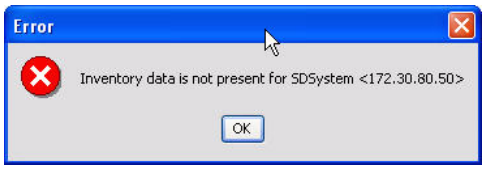
Index	Description	Vendor type	Container id	Class	Parent rel ...	Name	Hardware rev	Softwa
1	Assy, Sessio...	.1.3.6.1.4.1...	0	chassis	0	Session Dire...	2	
2	Power suppl...	.1.3.6.1.4.1...	1	container	1	Power Tray A		
3	Assy, 150 ...	.1.3.6.1.4.1...	2	powerSupply	1	Power Suppl...		
4	Power suppl...	.1.3.6.1.4.1...	1	container	2	Power Tray B		
5	Assy, 150 ...	.1.3.6.1.4.1...	4	powerSupply	1	Power Suppl...		
6	Fan tray	.1.3.6.1.4.1...	1	container	3	Fan Tray		
7	Assy, 3-fan ...	.1.3.6.1.4.1...	6	fan	1	3-Fan 40x20		
8	PHY slot 0	.1.3.6.1.4.1...	1	container	4	PHY Slot 0		
9	Assy, 4 Port...	.1.3.6.1.4.1...	8	module	1	Gigabit PHY	2	
10	Assy, 10/10...	.1.3.6.1.4.1...	9	port	1	FEPort00	2	
11	Assy, 10/10...	.1.3.6.1.4.1...	9	port	2	FEPort01	2	
12	Assy, 10/10...	.1.3.6.1.4.1...	9	port	3	FEPort02	2	
13	Assy, 10/10...	.1.3.6.1.4.1...	9	port	4	FEPort03	2	
14	PHY slot 1	.1.3.6.1.4.1...	1	container	5	PHY Slot 1		
15	Assy, 4 Port...	.1.3.6.1.4.1...	14	module	1	Gigabit PHY	2	
16	Assy, 10/10...	.1.3.6.1.4.1...	15	port	1	FEPort10	2	
17	Assy, 10/10...	.1.3.6.1.4.1...	15	port	2	FEPort11	2	

From here you can chose the category of information you want to view. You can save the inventory data to a file.

Note: If Net-Net EMS displays an error message instead of data, proceed to the next section.

No Data is Available

If no inventory data is available for the chosen Net-Net SBC, the following error message appears:



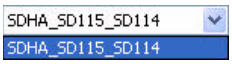
1. Click **OK** to clear the error message.
2. Choose a different Net-Net SBC from the `SD system` list or exit the Inventory window.

Viewing HA Data

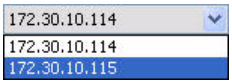
To view HA data:

1. From the `Type` dropdown list, click `HA`.

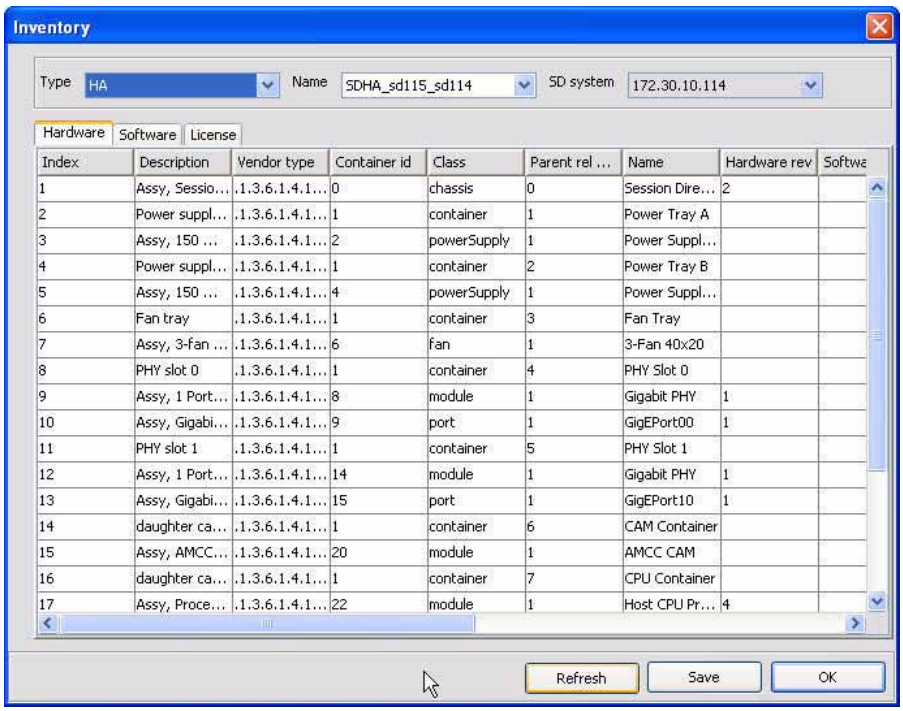
2. Click the down arrow next to the **Name** textbox to display all currently discovered HA pairs. For example:



3. Click the name of the system for which you want to view data.
4. Click the down arrow next to the **SD system** textbox to display the Net-Net SBCs that belong to that pair. For example:



5. Click the Net-Net SBC for which you want to view inventory data. The Inventory window displays the hardware data for that system by default:

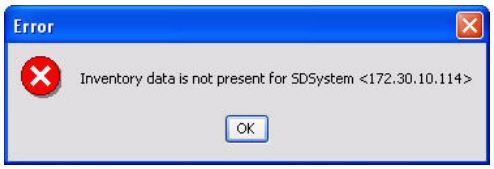


From here you can chose the category of information you want to view. See the following sections for details.

Note: If Net-Net EMS displays an error message instead of data, proceed to the next section.

No Data is Available

If no inventory data is available for the chosen Net-Net SBC, the following error message appears:



1. Click **OK** to clear the error message.
2. Choose the other Net-Net system that belongs to the pair from the `SD system` list, choose a different HA pair from the `Name` list, or exit the Inventory window.

Saving Data

You can save the data displayed on each screen to a text file in comma separated format.

To save data to a file:

1. With the data displayed, click **Save**.

   A Save window appears.
2. Enter a name for the file and choose the location where you want to save it.
3. Click **Save.**

Net-Net SBC Configuration Integrity

Net-Net EMS maintains s a configuration inventory for each active and inactive Net-Net SBC configuration. This inventory is used to check whether there are discrepancies between the Net-Net SBC's configuration as seen by Net-Net EMS and as seen by the device itself. The record information is retrieved from the Net-Net SBC during each save and discover operation and matched against the information in Net-Net EMS.

Configuration Record Counting

During the discovery phase, Net-Net EMS compares the record count advertised by the Net-Net SBC to the data read by Net-Net EMS. This process confirms that the configuration was correctly discovered from the managed device before being stored in the Net-Net EMS database.

Discovery

If you initiate discovery or rediscovery, Net-Net EMS retrieves the inventory list to obtain the list of objects configured at the Net-Net SBC. Net-Net EMS sets up a list of counters, one for each object in the inventory list. As elements are retrieved, Net-Net EMS increments the corresponding counter. When the discovery or rediscovery finishes, the retrieved counter list is compared to the inventory list. If they do not match, the discovery or rediscovery fails.

When you copy a configuration for edit, the record count is propagated. If elements are added or deleted the corresponding count is updated.

Save

The Net-Net EMS process for saving a configuration involves deleting the current elements at the managed device and re-creating each element stored in the Net-Net EMS database at the managed device, one at a time. After the elements are created, a save command instructs the managed device that the configuration is complete and to save the configuration to persistent storage.

With this feature, Net-Net EMS maintains its own inventory list for an inactive configuration. When that inactive configuration is saved to the Net-Net SBC, the managed device's inventory maintained by the Net-Net SBC is compared to the Net-Net EMS inventory. If they match, the save command is issued.

If the inventories do not match, the Net-Net EMS save fails and an error message appears. Net-Net EMS does not move to the save or the activate configuration phase. The user can perform a manual activate at this point to re-activate the last saved configuration.

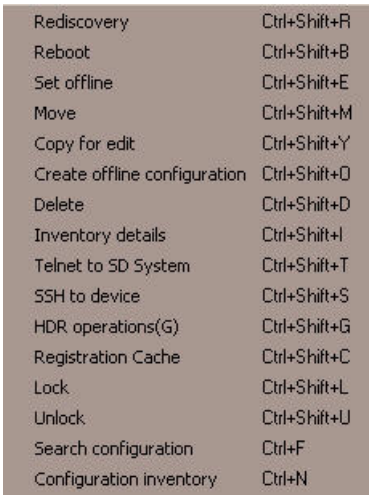
Accessing the Configuration Record Count

You can access the record count for a Net-Net SBC configuration and save it to a file.

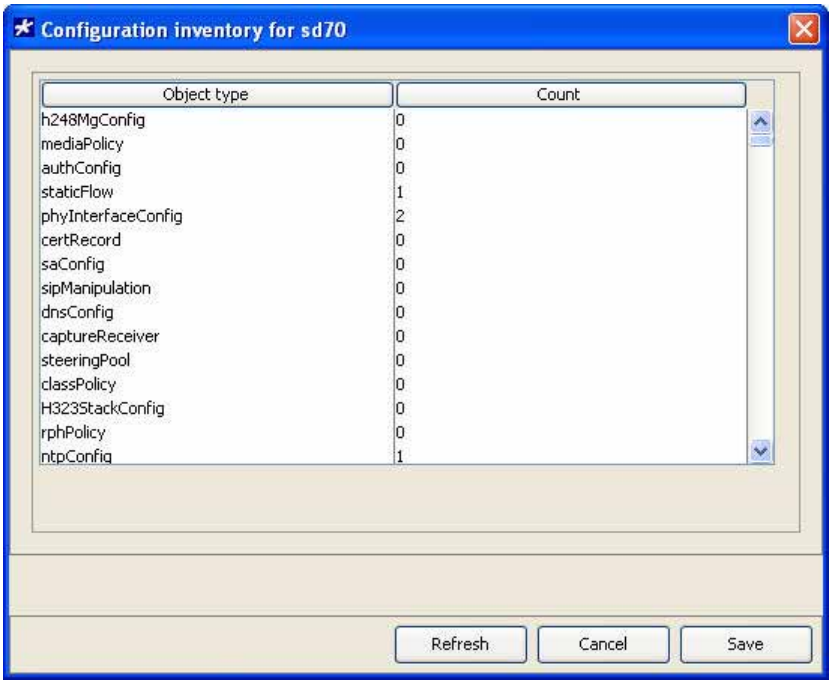
To check configuration record counts:

1. You can check the record count for an active or inactive configuration by accessing the Configuration inventory right-click option.

For example, under the `Active configuration` category, right-click the name of the Net-Net SBC for which you want to view inventory data. A list of options appears:



2. Click `Configuration inventory` to select it. The Configuration Inventory window appears.



You can review the list of configuration objects and their associated counts. At the bottom of the display, a total count of all records is displayed.

3. *Optional.* Save the record count to a file.

Saving Record Counts

You can save the data displayed to a text file in comma separated format.

To save data to a file:

1. With the data displayed, click **Save**.
   A Save window appears.
2. Enter a name for the file and choose the location where you want to save it.
3. Click **Save.**

Viewing Hardware Information

This section explains the inventory data displayed by the Net-Net EMS for the following hardware components:

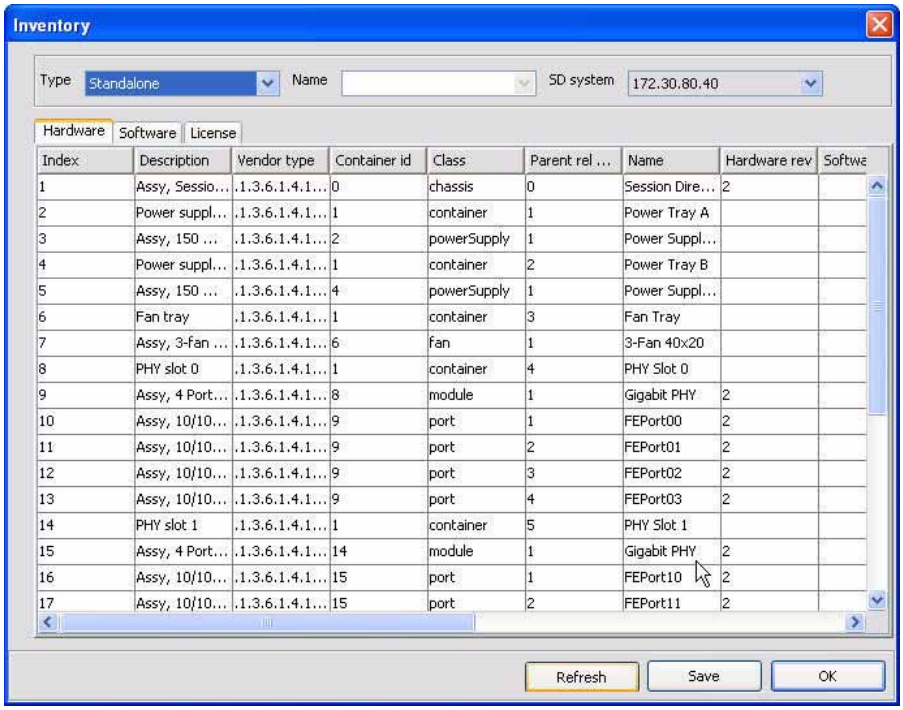
- chassis (main system board)
- CPU
- memory
- network processor
- fans
- packet-processing CAM
- environmental sensors
- network interface
- physical interface cards
- power supplies

Accessing Hardware Data

To access hardware data:

1. In the Inventory window, ensure the Hardware tab is selected.
2. Choose the type of Net-Net SBC by clicking `Standalone` or `HA`. The data for your choice appears in the Inventory window. The same information is displayed for either type of Net-Net SBC.

   The following example shows the data for a standalone Net-Net SBC:



Index	Description	Vendor type	Container id	Class	Parent rel ...	Name	Hardware rev	Softwa
1	Assy, Sessio...	.1.3.6.1.4.1...	0	chassis	0	Session Dire...	2	
2	Power suppl...	.1.3.6.1.4.1...	1	container	1	Power Tray A		
3	Assy, 150 ...	.1.3.6.1.4.1...	2	powerSupply	1	Power Suppl...		
4	Power suppl...	.1.3.6.1.4.1...	1	container	2	Power Tray B		
5	Assy, 150 ...	.1.3.6.1.4.1...	4	powerSupply	1	Power Suppl...		
6	Fan tray	.1.3.6.1.4.1...	1	container	3	Fan Tray		
7	Assy, 3-fan ...	.1.3.6.1.4.1...	6	fan	1	3-Fan 40x20		
8	PHY slot 0	.1.3.6.1.4.1...	1	container	4	PHY Slot 0		
9	Assy, 4 Port...	.1.3.6.1.4.1...	8	module	1	Gigabit PHY	2	
10	Assy, 10/10...	.1.3.6.1.4.1...	9	port	1	FEPort00	2	
11	Assy, 10/10...	.1.3.6.1.4.1...	9	port	2	FEPort01	2	
12	Assy, 10/10...	.1.3.6.1.4.1...	9	port	3	FEPort02	2	
13	Assy, 10/10...	.1.3.6.1.4.1...	9	port	4	FEPort03	2	
14	PHY slot 1	.1.3.6.1.4.1...	1	container	5	PHY Slot 1		
15	Assy, 4 Port...	.1.3.6.1.4.1...	14	module	1	Gigabit PHY	2	
16	Assy, 10/10...	.1.3.6.1.4.1...	15	port	1	FEPort10	2	
17	Assy, 10/10...	.1.3.6.1.4.1...	15	port	2	FEPort11	2	

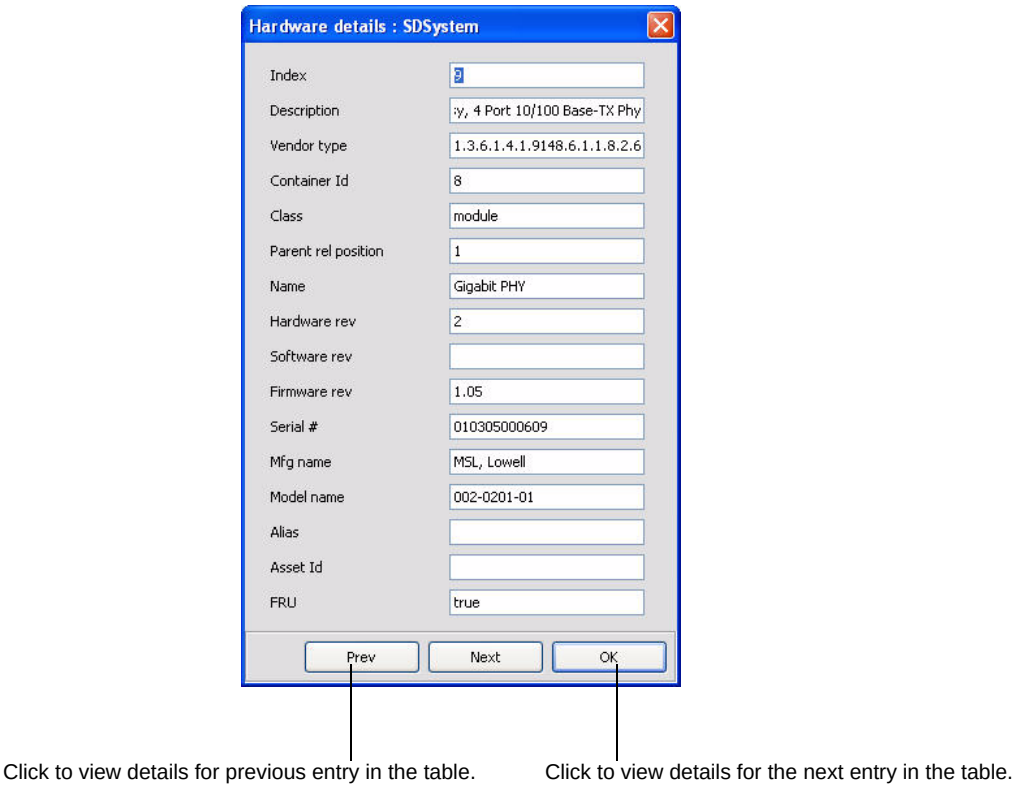
The following table defines the data displayed by Net-Net EMS for a standalone Net-Net SBC or for the Net-Net SBCs that belong to an HA pair:

Data	Description
Index	Number that represents the physical entity
Description	Textual description of the physical entity
Vendor type	Vendor-specific hardware type of the physical entity. (This value is different from the definition of MIB-II"s sysObjectID.)
Container id	Value of the entPhysicalIndex for the physical entity that *contains* this physical entity
Class	Enumerated value that indicates the general hardware type of this physical entity
Parent rel pos	Relative position of this *child* component among all its *sibling* components
Name	Textual name of this physical entity. Name of the component as assigned by the local device
Hardware rev	Vendor-specific hardware revision string for the physical entity
Software rev	Vendor-specific software revision string for the physical entity
Firmware rev	Vendor-specific firmware revision string for the physical entity
Serial #	Vendor-specific serial number string for the physical entity
Mfg name	Name of the manufacturer of this physical entity
Model name	Vendor-specific model name identifier string associated with this physical entity
Alias	Alias name for the physical entity as specified by a network manager. It provides a non-volatile *handle* for the physical entity.
Asset ID	User-assigned asset tracking identifier for the physical entity as specified by a network manager. It provides non-volatile storage of this information.
FRU	Whether this physical entity is considered a field replace unit (FRU) by the vendor

Viewing the Details

To view the details:

1. In the Hardware table, double-click the row of the hardware component for which you want to view details. The Hardware details window appears:



2. Click Prev and Next to scroll forward and backward through all the Hardware table entry details.
3. Click **OK** to close the window.

Viewing Software Information

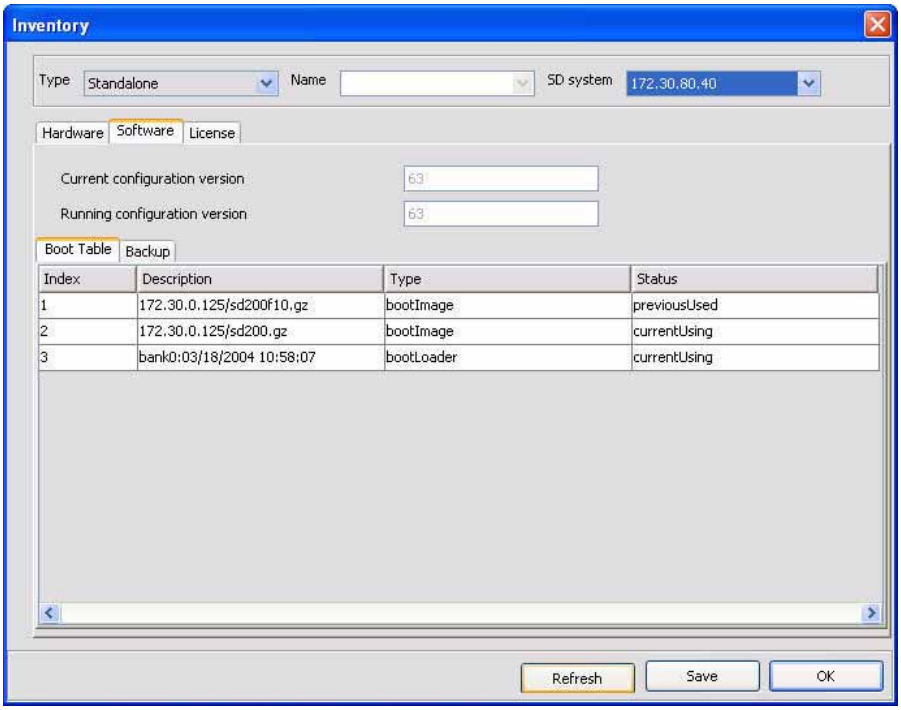
This section explains how to view the inventory data for the following software components:

- Software images: current software image as well as other loaded images, including the version.
- Configuration files: current file as well as other loaded files

Accessing Software Data

To access software data:

1. Select either a standalone Net-Net SBC or an HA pair.
2. In the Inventory window, click the Software tab. By default, the Boot Table software inventory data appears:



About the Configuration Versions

The top section of the screen displays both the current configuration version and the running configuration version.

- Current configuration version: Saved version number of the current configuration
- Running configuration version: Saved version number of the configuration currently running on the Net-Net SBC

About the Boot Table Data

Boot parameters specify what information your Net-Net system uses at boot time when it prepares to run applications. The Net-Net system's boot parameters:

- Determine what software image the Net-Net SBC is using and from where it boots that image: an external device or internal flash memory

- Type of software entity being booted
- Status of that software entity

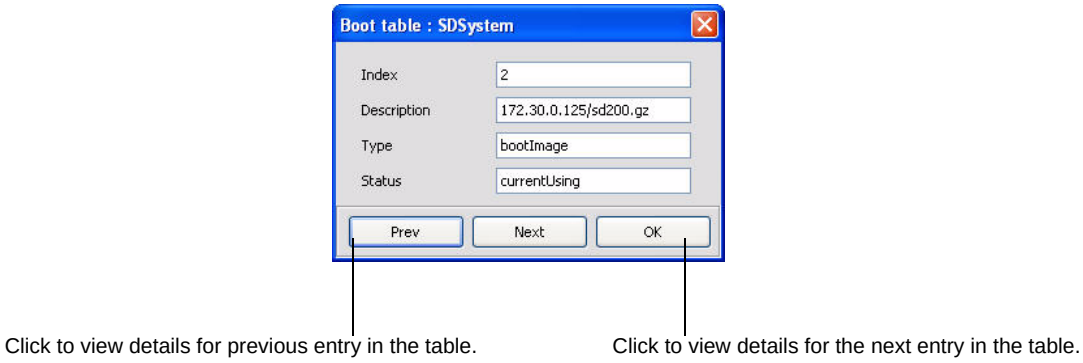
The following table defines the boot table data displayed by Net-Net EMS for a standalone Net-Net SBC or for the Net-Net SBCs that belong to an HA pair:

Data	Description
Index	Number that represents the physical entity
Description	Textual description that uniquely identifies the software image. Filename, date and time image was built, or other unique identifier can be used. For example: • *host address*/*image name* (boot image) 10.0.1.12/sd121p3.gz • *boot from flash0*/*image name* (boot image) /tffs0/sd121p3.gz • bank0:*date time* (boot loader) bank0:06/13/2005 10:58:25
Type	Software entity type. Values are: • bootImage • bootLoader
Status	Software entity status. Values are: • previousUsed • currentUsing

Viewing Boot Table Details

You can view the details of a software component.

1. In the Boot Table display, double-click the row of a specific software component. The Boot table details window appears:



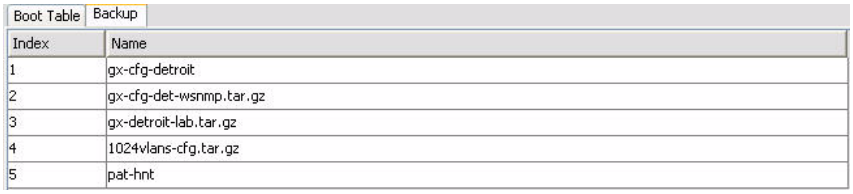
2. Click Prev and Next to scroll forward and backward through all the Boot table entry details.
3. Click **OK** to close the window.

Viewing Backup Information

The Net-Net SBC can save an existing configuration into a single backup file. Backups are created as gzipped tar files in a .tar.gz format. They are stored in the `/code/bkups` directory on the Net-Net SBC.

To view backup data:

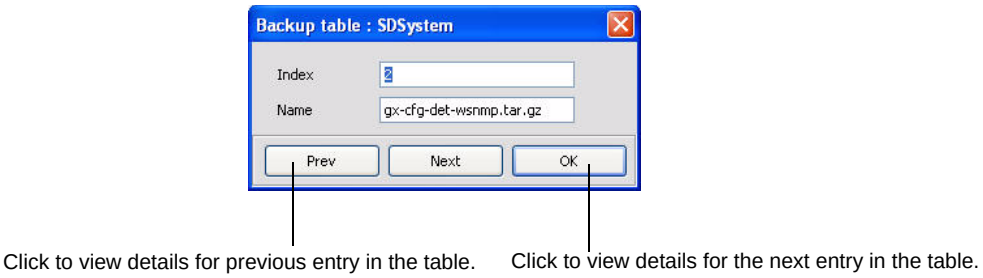
1. In the Software display, click the Backup tab. The table of backup files appears:



Viewing Details

To view details:

1. In the table, double-click the name of a specific backup file. The Backup table detail window appears:



2. Click Prev and Next to scroll forward and backward through all the Backup table entry details.
3. Click **OK** to close the window.

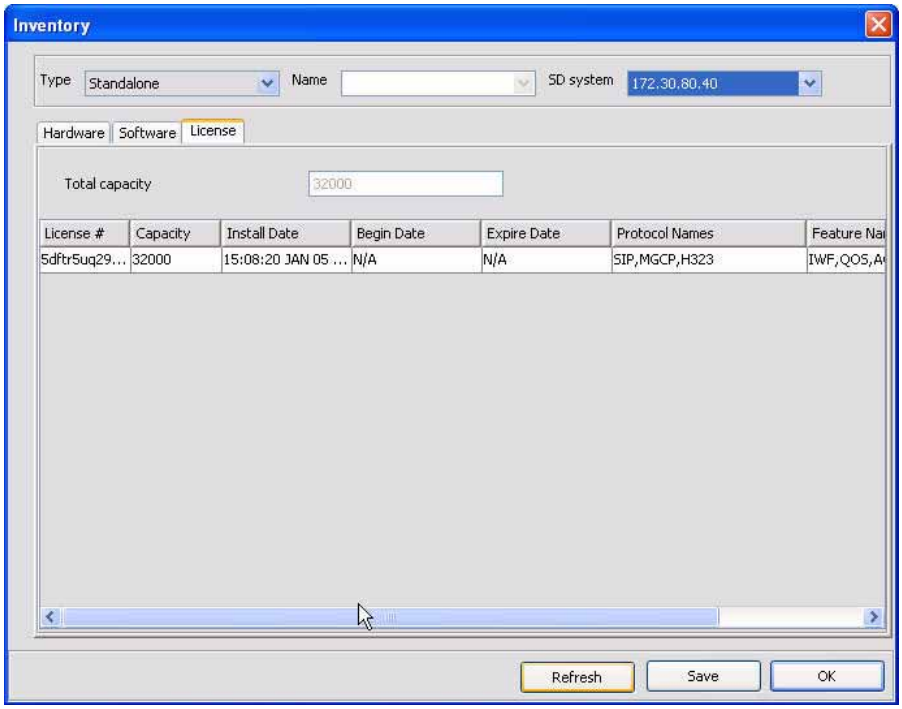
Viewing License Information

This section explains how to view inventory data for the licenses. All components of the Net-Net system software are licensed by Acme Packet, Inc. (In order to use these components and deploy their related services in your network, you must have a valid license for each of them.)

Accessing License Data

To access license data:

1. In the Inventory window, click the License tab. The license inventory data appears:



About the Total Capacity

The top section of the screen displays the total capacity for the Net-Net SBC, which comprises the maximum number of simultaneous sessions allowed by a Net-Net system for all combined protocols. If the Net-Net SBC had undergone several license upgrades, the value of each Capacity row adds up to the Total Capacity value.

For example:

About the License Data

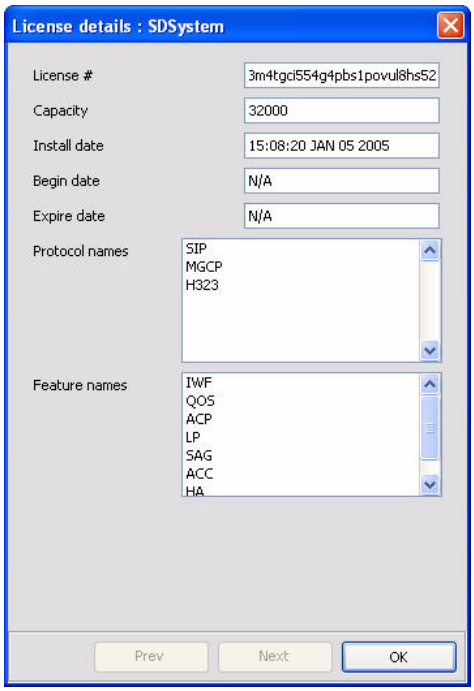
The following table defines the data displayed by Net-Net EMS for a standalone Net-Net SBC or for the Net-Net SBCs that belong to an HA pair:

Data	Description
License #	License number
Capacity	Maximum number of simultaneous sessions allowed by the Net-Net system for all combined protocols
Install date	Installation time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled.
Begin date	Installation time and date in the following format: hh:mm:ss month day year. Displays N/A if a license is not enabled.
Expire date	Expiration time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled.
Protocol names	All protocols licensed for this Net-Net SBC. Values are: • SIP • MGCP • H.323
Feature names	All features licensed for this Net-Net SBC. Values are: • Interworking (IWF) • Quality of Service (QoS) • Acme Control Protocol (ACP) • Local Policy (LP) • Session Agent Group (SAG) • ACC (allows the Net-Net system to create connections and send CDRs to one or more RADIUS servers) • High Availability (HA)

Viewing Details

To view details:

1. In the table, double-click the license row. The License details window appears:



2. Click **OK** to close the window.

8 Fault Management

Overview

This chapter contains information about fault management using Net-Net EMS. Fault management involves the following:

- Network event log
- Alarm monitoring and reporting
- System log

The information about events, alarms, and syslog is based on the Acme Packet® standard and proprietary Management Information Bases (MIBs). For more information about the events, alarms, and MIBs, see the *Net-Net MIB Reference Guide*. For information about Net-Net SBC logging, see the *Logs* chapter in the *Net-Net EMS 4000 Configuration Guide*.

About the Relationship of Traps to Events and Alarms

All SNMP traps from nodes managed by Net-Net EMS appear as events in the Network events window. Only a subset of traps are considered to be alarms, which appear in the Alarms window. In general, the Net-Net EMS characterization of alarms matches that of the Net-Net SBC. See the *Net-Net MIB Reference Guide* for more information.

Verifying Net-Net SBC Configuration

You should verify that the Net-Net SBCs for which you want to view fault management information have the following information configured:

- Simple Network Management Protocol (SNMP) communities
- MIB contact
- Trap receivers
- Syslog events

  These features are necessary to use Acme Packet's Net-Net EMS to manage Net-Net SBCs. They provide important monitoring and system health information that contribute to a robust deployment of the Net-Net system.

  You can also configure the optional syslog server. Syslogs conform to the standard used for logging servers and processes as defined in RFC 3164.

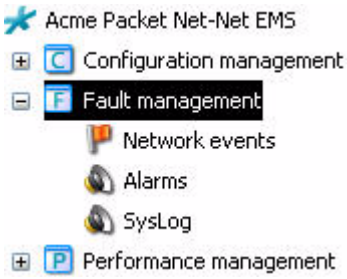
See the *System Configuration* chapter of the *Net-Net EMS 4000 Configuration Guide* for complete information about these parameters.

Accessing Fault Management Information

This section explains how to access the Net-Net SBC fault information displayed by Net-Net EMS.

To access fault management information:

1. In the Navigation tree, click the plus sign (+) next to `Fault management` to expand it. For example:



   From here you can choose the type of information you want to view. See the following sections for specific information.

Viewing Event Information

This section explains how to access and view event information. Events are caused by actions that generate one or more of the following:

- Alarms
- Entries in a log file
- SNMP traps

For more information about events, refer to the *Net-Net MIB Reference Guide*.

Event Severity

There are eight severity levels ranging from the highest, Emergency to the lowest severity of Debug.

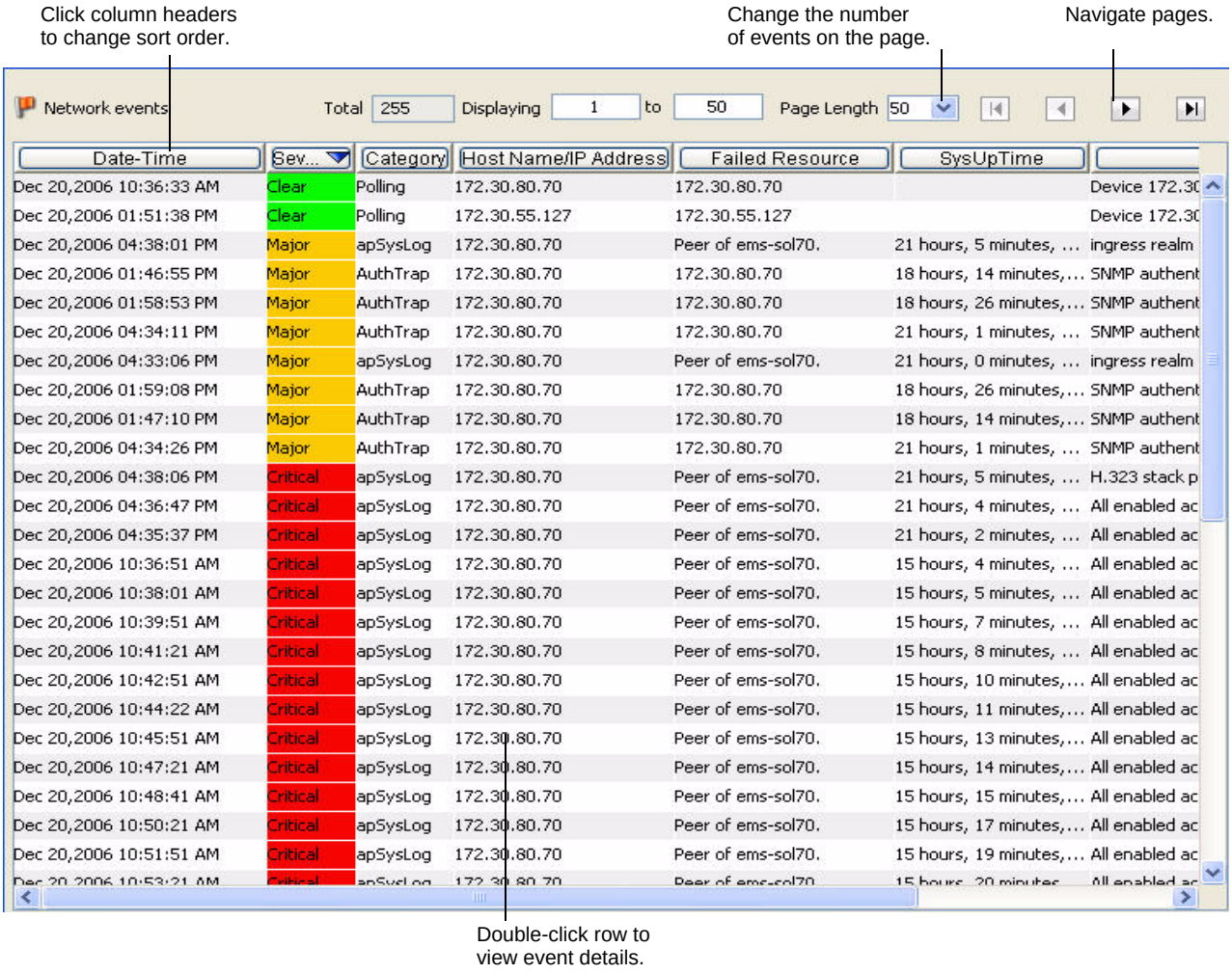
syslog Numerical Code	syslog Severity	Acme Packet Log Enumeration
0	Emergency (system is unusable)	EMERGENCY (0)
1	Alert (action must be taken immediately)	CRITICAL (1)
2	Critical (critical conditions)	MAJOR (2)
3	Error (error conditions)	MINOR (3)
4	Warning (warning conditions)	WARNING (4)
5	Notice (normal but significant condition)	NOTICE (5)
6	Informational (informational messages)	INFO (6)
7	Debug (debug level messages)	TRACE (7) DEBUG (8) DETAIL (9)

Accessing Event Information

To access event information:

1. In the Net-Net EMS navigation tree, click the plus sign (+) to expand `Fault management`.
2. Click `Network events`.

   The list of network events appears in the right pane. For example:

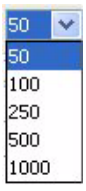


Changing Number of Events on the Page

By default, 50 events are shown per page in the Network events view.

To change the number of events displayed:

1. At the top of the Network events window, click the down arrow for `Page Length`. The drop down list of values appears.



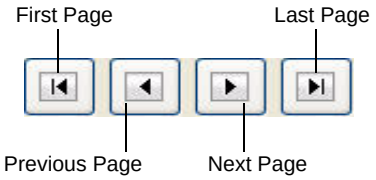
2. Click the number you want to apply.

Navigating Pages

To navigate through multiple pages:

1. Use the navigation arrows located at the top of the Network events window to navigate through multiple pages.

   Clicking navigation icons display the desired page, such as the first page, previous page, next page, and the last page of Events list view. For example:



Sorting Events

By default, the events in the Events List View are displayed in the order of precedence based on the Date/Time and Event ID and in descending order. Events are assigned IDs and these are based on the date and time they are generated. Hence these two properties are interrelated. This order can be changed using the **Sorting** option.

To sort events:

1. In the Events List View, click the column header for the column you want to change the sort order.

   When you click the column header for the first time, the column is sorted in ascending order. Clicking the same column header again sorts the column in descending order. The up and down arrows in the headers indicate ascending and descending order, respectively.

   For example, if you need to sort the events based on its status, click the **Severity** column header. This sorts the events based on its severity and the default order of precedence is Critical, Major, Minor, Warning, Clear, and info. For descending order of the same column, click the **Severity** column header again.

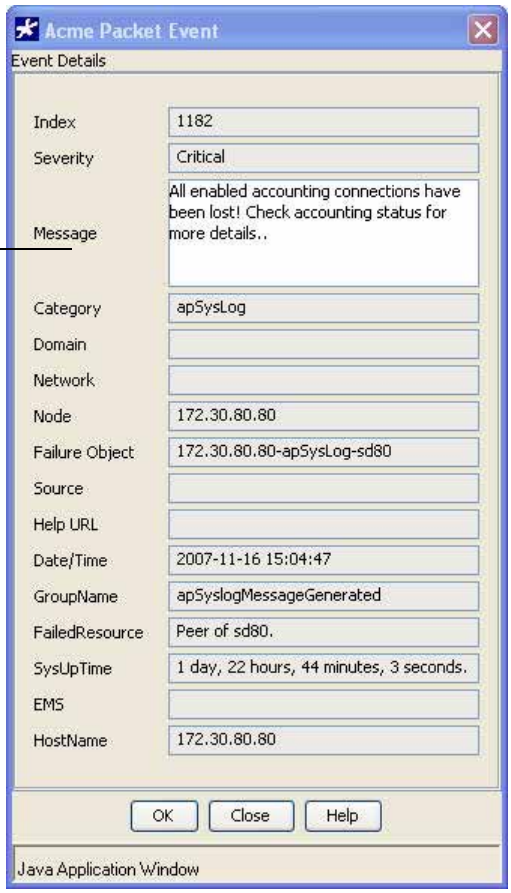
Viewing Event Details

You can access details about the event.

To view event details:

1. Double-click the table row for the event you want to view.

   The Event Details dialog box appears. For example:



2. Review the information and click **OK** to close the dialog box.

   The following table contains descriptions of the information in the dialog box.

Event Category	Description
Index	Unique ID created for the generated event
Severity	Severity level of event: • Critical • Major • Minor • Clear • Warning • Info
Message	Message associated with the event
Category	Category to which the event belongs

Event Category	Description
Domain	Domain-specific information which is based on the physical location, functional categorization, or logical categorization of the source of the event
Network	Network to which the event belongs
Node	Node to which the event belongs. For example, if the event is for an interface, the node value is specified as the interface parent node.
Failure Object	Specific entity in the source that has failed and is primarily responsible for the event
Source	Exact source of the event
Help URL	URL for locating the help documentation on clicking the Help button in the same dialog box
Date/Time	Date and time the event was generated
GroupName	Name of the group to which the event belongs
Failed Resource	Resource responsible for the event
SysUpTime	System's up time in hours, minutes, and seconds
EMS	Element Management System
HostName	Name of the host from which the alarm was generated

Viewing Alarm Information

This section explains how to view information about alarms. Alarms play a significant role in determining overall health of the system. For additional information about alarms, see the *Acme Packet MIB Reference Guide*.

About Alarms

An alarm is triggered when a condition or event happens within either the Net-Net system's hardware or software. Alarms contain an alarm code, a severity level, a textual description of the event, and the time the event occurred.

Alarm Categories

The alarms displayed in the Net-Net EMS fall into the following categories:

Category	Description
apSysLog	Associated with the proprietary Acme Packet ap-slog.mib, which provides a method of gathering syslog messages generated by the Net-Net system via SNMP
apSysMgmt	Associated with the proprietary Acme Packet ap-smgmt.mi, which provides a means of gathering information about the status of the Net-Net system
AuthTrap	Associated with the standard authenticationFailure trap. The SNMPv2 agent received a protocol message that was not properly authenticated.
ColdStart	Associated with the standard coldStart trap. The SNMPv2 agent is reinitializing itself and its configuration may have been altered.
DoS	Proprietary trap generated by Acme Packet Denial of Service protection

Category	Description
EMS-HA	Generated by the Net-Net EMS in a Net-Net EMS failover situation
License	Associated with the proprietary Acme Packet ap-license.mib, which provides information about the status of your Net-Net licenses
LinkDown	Associated with the standard linkDown trap. The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the up state to the down state. The ifOperStatus value indicates the other state.
LinkUp	Associated with the standard linkUp trap. The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the down state to the up state. The ifOperStatus value indicates the other state.
Monitor	Associated with the proprietary Acme Packet ap-env-monitor.mib, which gathers information about fan speed, voltage, temperature, and power supply for the Net-Net system. It also sends out traps when status changes occur
Polling	Generated by the Net-Net EMS to indicate ability to reach the Net-Net SBC
Reboot	Proprietary version of the standard coldStart trap

Alarm Severities

The following table lists the alarm severities.

Alarm Severity	Description
Emergency	Requires immediate attention. If you do not attend to this condition immediately, there could be physical, permanent, and irreparable damage to your Net-Net system.
Critical	Requires attention as soon as it is noted. If you do not attend to this condition immediately, there may be physical, permanent, and irreparable damage to your Net-Net system.
Major	Functionality has been seriously compromised. As a result, this situation might cause loss of functionality, hanging applications, and dropped packets. If you do not attend to this situation, your Net-Net system will suffer no physical harm, but it will cease to function.
Minor	Functionality has been impaired to a certain degree. As a result, you might experience compromised functionality. There will be no physical harm to your Net-Net system. However, you should attend to this type of alarm as soon as possible in order to keep your Net-Net system operating properly.
Warning	Some irregularities in performance. This condition describes situations that are noteworthy, however, you should attend to this condition in order to keep your Net-Net system operating properly. For example, this type of alarm might indicate the Net-Net system is running low on bandwidth and you may need to contact your Acme Packet customer support representative to arrange for an upgrade.

Default Alarm Severity Color Codes

The severity levels for the alarms are color coded with the following defaults. (You can change the defaults, see *Configuring Severity Color-Coding*.)

- red- emergency
- red - critical
- gold - major
- yellow - minor

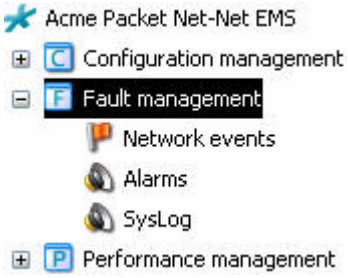
- blue - warning
- green -clear

Remapping Alarm Severities

You can override the default severity levels for alarms.

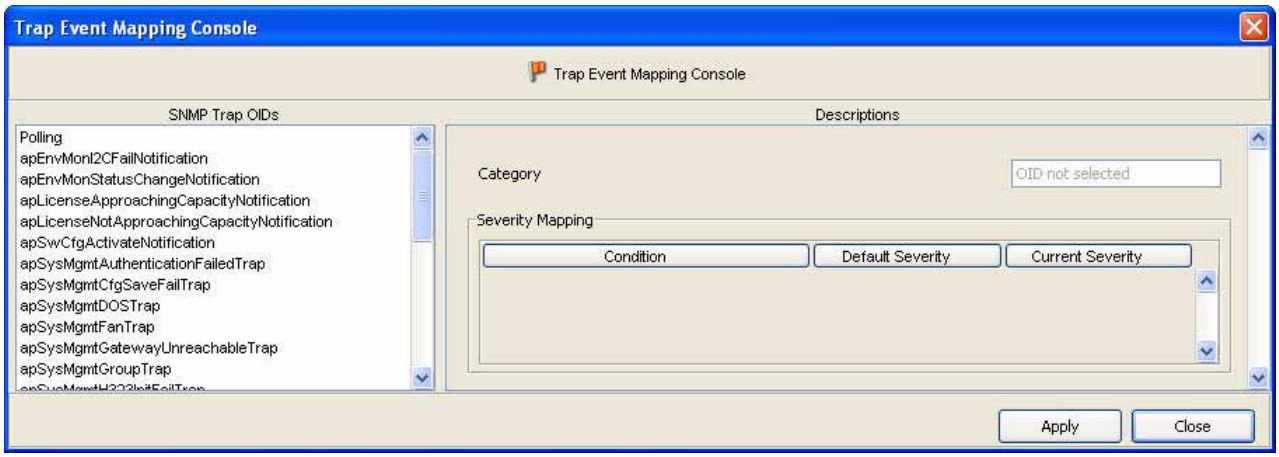
To remap alarm severities:

1. In the Navigation tree, click the plus sign (+) next to `Fault management` to expand it. For example:

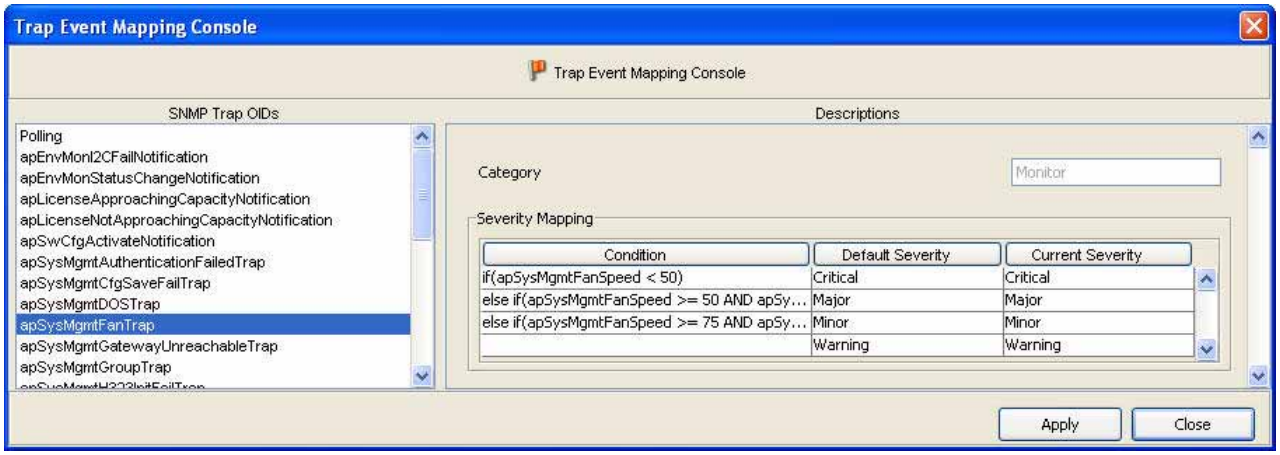


2. Right-click Network events to access the Trap Event Mapping option.

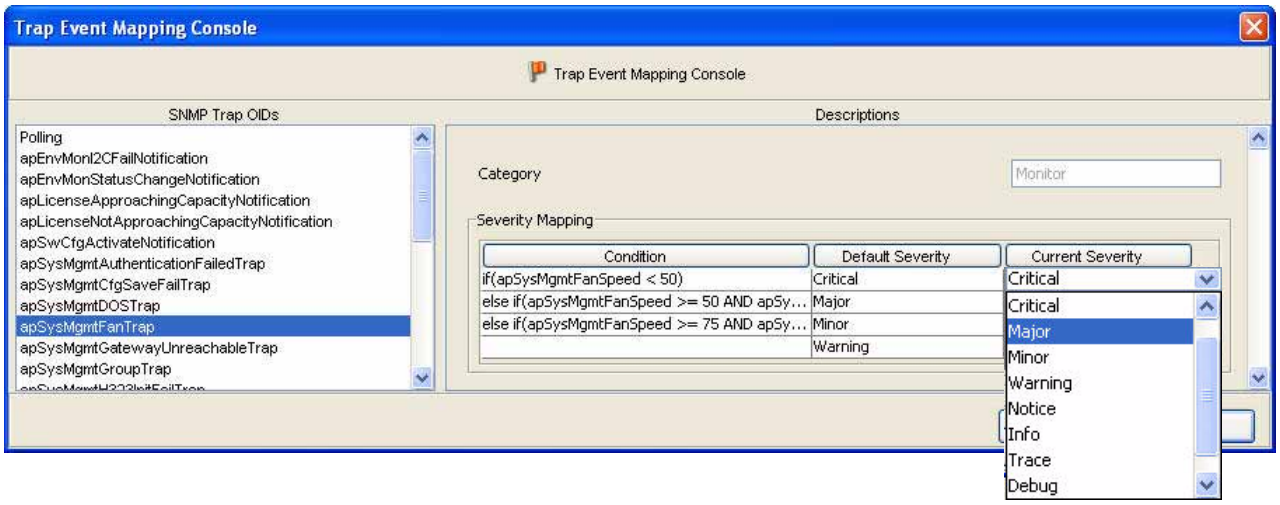
3. Click Trap Event Mapping. The Trap Event Mapping console appears:



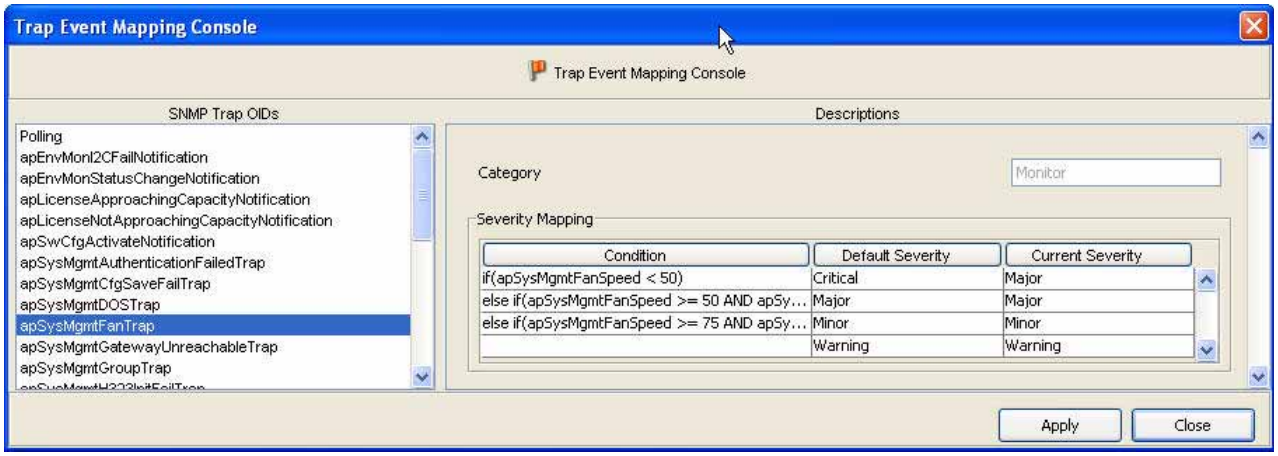
4. Choose the trap event you want to modify in the left pane. The information for that trap event appears in the Severity Mapping area.



5. Click the row of the condition you want to modify in the Current Severity column. A drop-down list of severity levels appears.



6. Click the new severity level in the drop-down list to select it. The new level appears in the Current Severity column.



7. Repeat for each condition you want to modify and click **Apply**. The new value will apply to all subsequent client displays.
8. Repeat steps for each trap event you want to modify.

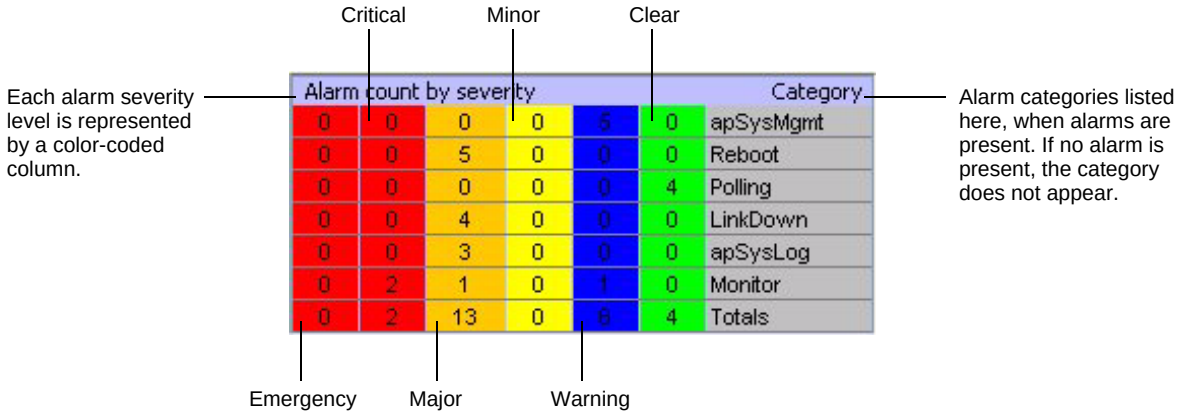
Alarm Count by Severity Table

You can access alarm information by using the Alarm count by severity table. (You can also access alarm information by choosing the Alarms option from the Fault Management category. See *Displaying the Alarm View* for details.)

The Alarm count by severity table displays a summary of all alarms generated, by alarm severity and by category. The table appears in the lower left pane of the Net-Net EMS GUI. The summary displays the number of alarms that are generated under various categories and severity levels. This table is automatically refreshed every 30 seconds.

Each row in the Alarm count by severity table corresponds to a specific category of alarms. The number of rows correspond to the number of alarm categories. The last row provides the total number of alarms for each severity level.

For example:



The Alarm count is based on the severity. When a new alarm is generated, the count is updated automatically and, if necessary, its category is added to the display.

You can click a table cell to display a list of alarms in the Alarm view, in the right pane. (See *Displaying the Alarm View* for details.) An asterisk appears in the cell to provide a visual cue as to which filter you have applied to the alarm display.

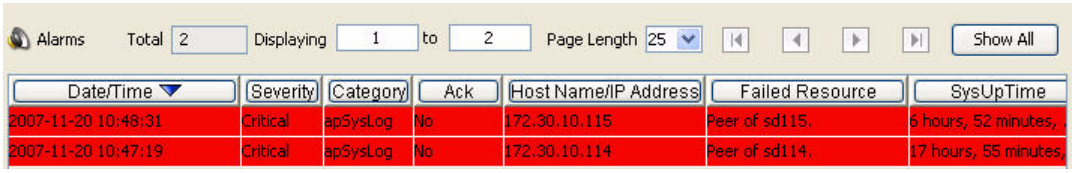
Viewing Alarms by Severity for a Specific Category

To view all alarms by category:

1. Click the count corresponding to the specific category of the alarms you want to view.

   For example, if you want to view all the Critical alarms for the asSyslog category, click the count in the red column and in the asSyslog row.

   An asterisk appears next to the count to provide a visual cue as to which filter you have applied to the alarm display. The Alarm view appears in the right pane, displaying the two Critical alarms that belong to the asSyslog category. For example:



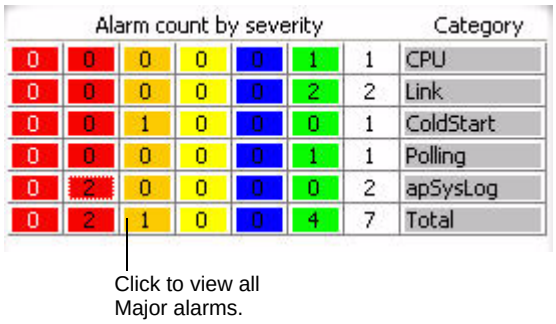
Viewing All Alarms by Severity

You can view a list of all alarms that belong to a specific severity level.

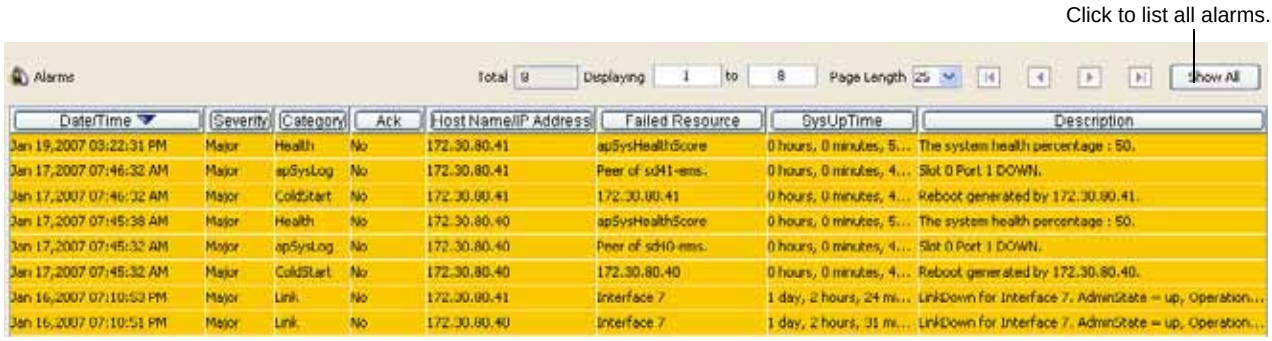
To view all alarms by severity:

1. From the Alarm count by severity table, click the count in the Total row that corresponds to the specific severity of the alarms you want to view.

   For example, if you want to view all Major alarms (8 in the following example), click the count in the gold column and in the Totals row.



An asterisk appears next to the count to provide a visual cue as to the type of alarms you are viewing. The Alarm view appears in the right pane, displaying all Major alarms. For example:



2. Click **Show All** to display all alarms or click a different cell in the Alarm count by severity table to display a different set of alarms.

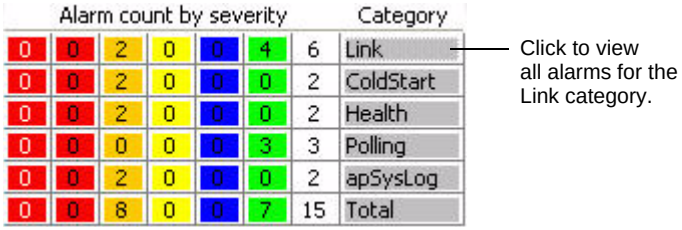
Viewing Alarms by Category

You can view a list of all alarms that belong to a specific severity level.

To view all alarms by severity:

1. From the Alarm count by severity table, click the count in the Total row that corresponds to the specific severity of the alarms you want to view.

   For example, if you want to view all Monitor alarms, click the Monitor cell in the Category column.



   An asterisk appears next to the count to provide a visual cue as to the type of alarms you are viewing. The Alarm view appears in the right pane, displaying all alarms belonging to the Monitor category. For example:

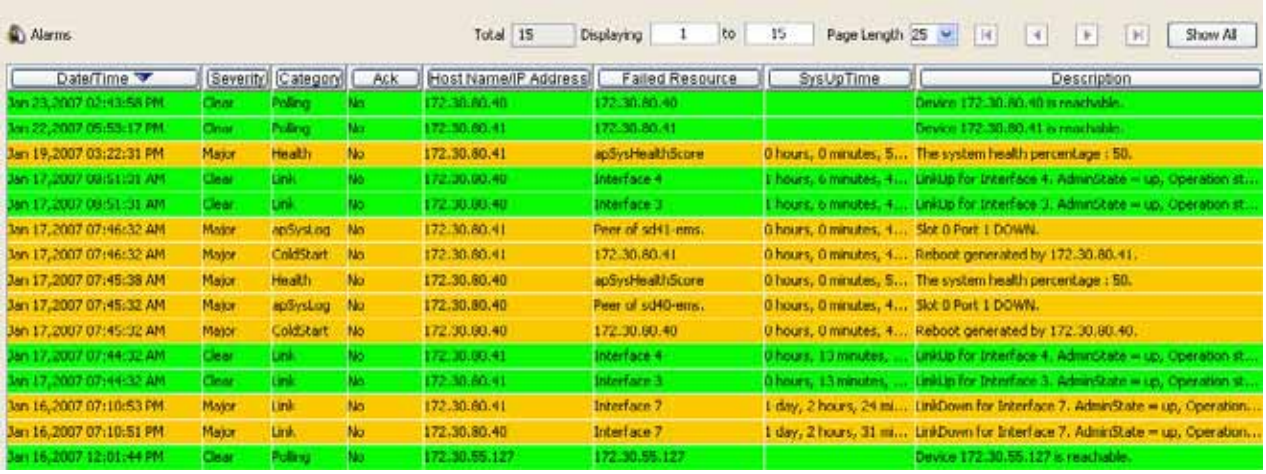
2. Click **Show All** to display all alarms in the right pane or click a different cell in the Alarm count by severity table to display a different set of alarms.

Displaying the Alarm View

The Alarm view is a list of alarms that is displayed in the right pane. You can generate this list of alarms by:

- Clicking `Alarms` under the Fault Management function
- Clicking the Totals category in the Alarm count by severity table. You can also change what is displayed in the list of alarms by clicking cells in the alarm severity table.

The following example shows the Alarm view:



The following table describes the information displayed in the list of alarms.

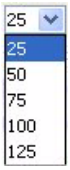
Options	Description
Date-Time	Date and time the alarm was generated
Severity	Current alarm severity level
Category	Category to which the alarm belongs
Ack	Whether an alarm has been acknowledged
Host name/IP address	Specific host name or IP address from which this alarm was generated
Failed Resource	Resource responsible for the alarm
SysUpTime	System's up time in hours, minutes, and seconds
Description	Description of the alarm

Changing Number of Alarms on the Page

By default, 25 alarms are shown per page in the Alarm view.

To change the number of alarms displayed:

1. At the top of the Alarms window, click the down arrow for `Page Length`. The drop down list of values appears.



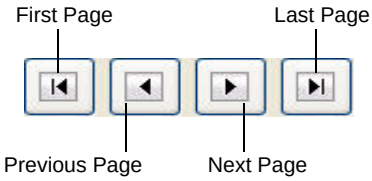
2. Click the number you want to apply.

Navigating Pages

To navigate through multiple pages:

1. Use the navigation arrows located at the top of the Alarms window to navigate through multiple pages.

   Clicking navigation icons display the desired page, such as the first page, previous page, next page, and the last page of Alarms list view. For example



Sorting Alarms

By default, in the Alarms view the alarms are displayed in the order of precedence based on time and in descending order. This order can be changed using the **Sorting** option.

To sort alarms:

1. In the Alarms view, click the column header for the column you want to change the sort order.

   When you click the column header for the first time, the column is sorted in ascending order. Clicking the same column header again sorts the column in descending order. The up and down arrows in the headers indicate ascending and descending order respectively.

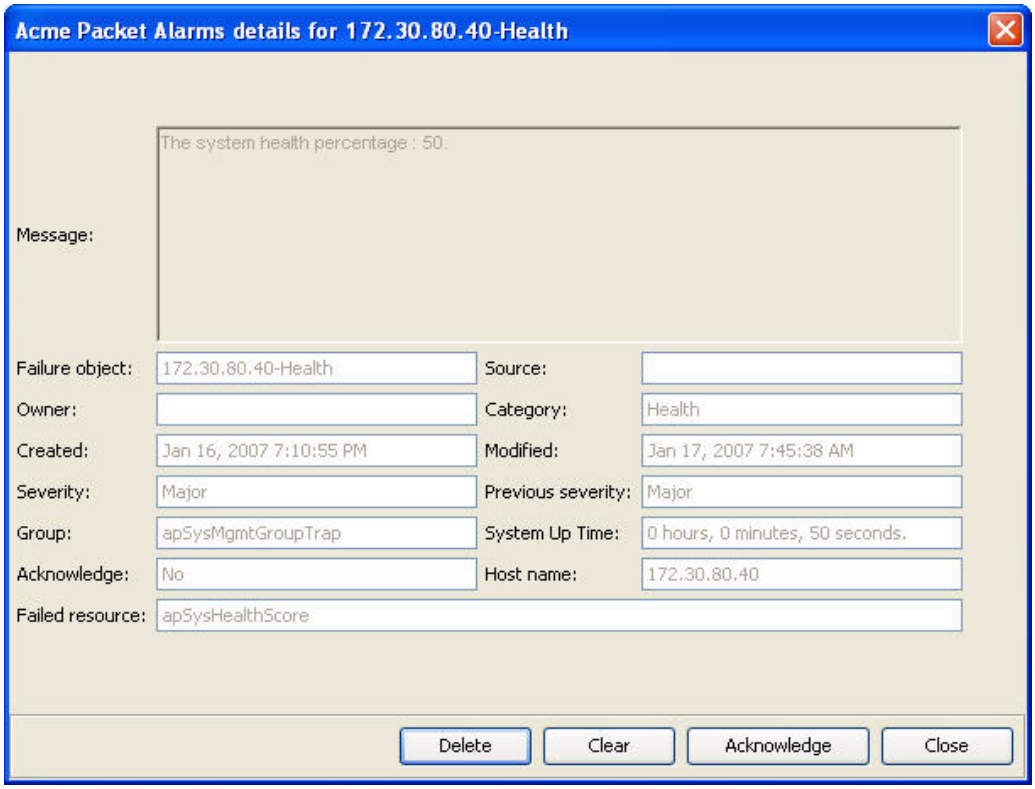
   For example, if you need to sort the alarms based on its severity, click the **Severity** column header. This sorts the alarms based on its severity and the default order of precedence is Critical, Major, Minor, Warning, Clear, and info. For descending order of the same column, click the **Severity** column header again.

Viewing Alarm Details

You can view alarm details for a specific alarm.

To view alarm details:

1. With the Alarm view displayed, double-click a row in the table to access alarm details. The Alarm details dialog box appears:



The following table describes the information displayed in the Alarm details window.

Options	Description
Message	Message associated with the alarm
Failure object	Specific entity in the source that has failed and is primarily responsible for the alarm
Owner	Owner associated with the alarm
Created	Date and time the alarm was created
Severity	Current severity of alarm: • Emergency • Critical • Major • Minor • Warning • Clear
Group	Name of group to which the alarm belongs

Options	Description
Acknowledge	Acknowledge an alarm. The alarm acknowledgment status is displayed on the Alarm view window.
Failed resource	Failed resource that generated the alarm
Source	Source of the alarm
Category	Category to which the alarm belongs
Modified	Date and time the alarm was last modified
Previous severity	Previous severity of the alarm
System Up Time	Length of time the system has been operational
Host name	Name of the host being managed

Acknowledging Alarms

Users with the appropriate privileges can acknowledge alarms by clicking Acknowledge on the Alarms details window. When you acknowledge an alarm the Acknowledge, Owner, and Modified fields are updated. The Acknowledge button toggles to the Unacknowledge button.

Clearing Alarms

Users with the appropriate privileges can clear alarms by clicking Clear on the Alarms details window. The user is prompted to confirm clearing the alarm and the alarm severity is updated to Clear. If the Severity is Clear, the Clear and Acknowledge buttons are disabled.

Deleting Alarms

Users with the appropriate privileges can delete alarms by clicking Delete in the Alarms details window. The user is prompted to confirm deleting the alarm and the alarm is removed from the Net-Net EMS display and database for all Net-Net EMS users.

Configuring Alarm Email List

Net-Net EMS can trigger automatic e-mail notification when reporting alarms for certain severities. Users with the appropriate privileges can configure alarm e-mail addresses for each severity.

To configure an alarm email list:

1. Right-click Alarms in the Fault management area of the Net-Net EMS navigation pane.
2. Choose Alarm E-mail Console. The console appears.
3. Click the checkboxes of the alarm severities for which you want to attach an email address.
4. Enter up to six email addresses you want to attach to the alarm severity. Separate multiple email addresses with a comma.
5. Click **Apply**.

Using the Audible Alarm System

The Net-Net EMS audible alarm system lets you activate an audible alarm sound that will play when an alert (the trap event associated specifically with an alarm) is received by Net-Net EMS from a Net-Net SBC.

About the Audible Alarm System

The audible alarm system lets you associate sounds with the different alarm severity levels, and set the sound alarm frequency and number of repetitions. The audible alarm system provides the tools necessary for a Net-Net EMS client to interact with the sounding alarms. Once activated, the audible alarm system checks the alarm statistics during each configured cycle, looking for new or modified alarms. Once it detects alarms, it sends them for processing. Finally, it plays the sound wave for a specific alarm severity (if you have configured an alarm sound for that severity level).

> **Note:** A delay of up to 5 seconds can sometimes occur between the time an alarm is updated on the screen and the time the alarm sounds. A discrepancy between the Net-Net EMS client and server system times, can increase the delay. Acme Packet recommends ensuring the system times are the same on both.

How the Audible Alarm System Works

You configure the audible alarm system to choose the alarm severity levels for which you want audible alarms to sound. You then activate the audible alarm system. Alarms detected after activation will cause the configured alarms to sound.

If alarms of different severity levels (for which you configured alarm sounds) are detected, only the alarm with the greater severity will sound. Alarm priorities from highest to lowest are critical, major, minor, warning.

About the Audio Files

The audible alarm system comes with four alarm sound.wav files. Each sound is specific to the severity it represents. You can find these files in the ADVENTNET_HOME/conf directory.

- Audio_Critical.wav: critical severity alarms
- Audio_Major.wav: major severity alarms
- Audio_Minor.wav: minor severity alarms
- Audio_Warning.wav: warning severity alarms

Substituting WAV Files

You can substitute your own .wav files for those supplied with Net-Net EMS.

1. Create an alarm sound wav file. For example, NewCriticalAlarm.wav.
2. In the ADVENTNET_HOME/conf directory, rename the existing Audio_Critical.wav to Original_Audio_Critical.wav to create a backup of the original file.
3. Copy the new wav file to the ADVENTNET_HOME/conf directory and rename it to Audio_Critical.wav.

   The new critical alarm sound will now be played after you activate the audible alarm system.

Using the Audible Alarm Console

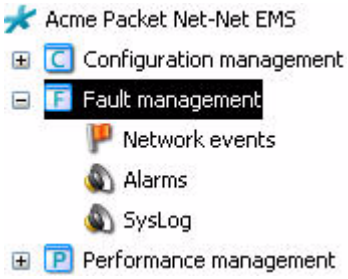
You activate, deactivate, and configure alarm sound characteristics through the Audible Alarm console. The configuration settings are only are valid for the current session. When you exit the session, the alarm sound settings revert to the default values.

> **Note:** If a time difference exists between the client and server systems, either the alarms do not sound or are not synchronized with the trap generator.

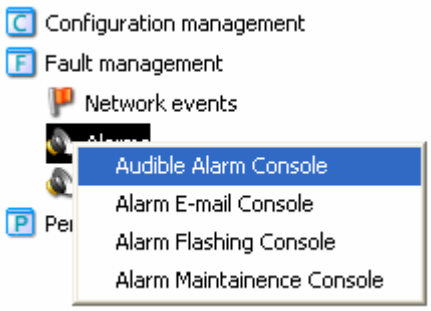
Accessing the Audible Alarm Console

To access the Audible Alarm console:

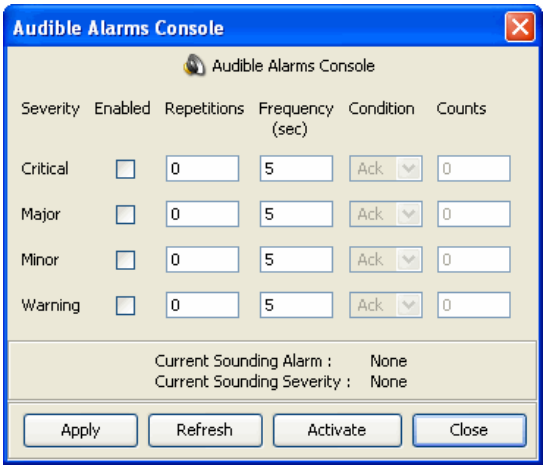
1. In the Navigation tree, click the plus sign (+) next to `Fault management` to expand it. For example:



2. Right-click Alarms to display the Audible Alarm Console option.



3. Click Audible Alarm Console to select it. The Audible Alarm Console appears.



> **Note:** The Condition options are currently not supported.

Configuring Audible Alarms

After you enter your configuration values, you must click **Apply** to apply your configuration and then click **Activate** to active the Audible Audio Alarm console.

> **Note:** Acme Packet recommends setting the frequency to accommodate the sounding time of the alarm .wav file chosen. You want to ensure the alarm sound plays in its entirety. For example, if a .wav file sound runs for 10 seconds, enter a value greater than 10 seconds, so that sound file plays completely.

To configure audible alarms:

1. Click the checkbox in the Enabled column for each alarm severity to which you want to associate an audible alarm.
2. Enter a value that represents the number of times the alarm will sound. Providing a number greater than zero causes the alarm sound to be repeated for the number of repetitions requested. For example, enter the number 10 to cause the severity alarm to sound 10 times and then stop.

   The default value of zero (0) means that once a alarm sound starts, it will continue indefinitely until the end user stops it by either deselecting the checkbox and clicking Apply button, or clicking the Deactivate button to stop the audible alarm system.
3. Enter a value in seconds that represents the frequency of the alarm sound and accommodates the sounding time of the alarm .wav file chosen. The default value of 5 seconds means that the alarm sound plays every 5 seconds and the the sounding time of the file is less than 5 seconds.

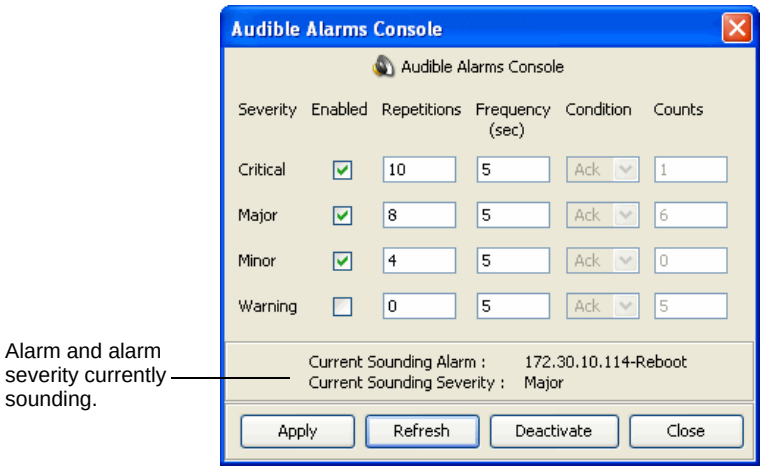
   Note: Do not enter a value of 2 seconds or less for frequency.
4. Click **Apply** to apply the values you entered.
5. Click **Activate** to start the audible alarm system. The button toggles to Deactivate. The next alarm detected that has been configured for an audible alarm, will cause the audible alarm to sound.

Viewing Alarm Information

You can click **Refresh** to display the most current valid configuration. Use Refresh if the Audible Alarms console has been active for a lengthy period of time to ensure the correct information is displayed.

The Count column displays the total number of alarms for each severity level currently in the system. The Audible Alarm console displays the counts after you activate the audible alarm system.

The console displays the name of the alarm sounding, as well as its severity. This information is not updated until you activate the audible alarm system and an alarm is sounding.



Note: If multiple alarms of the same severity are present and causing the alarm to sound, only one of those alarms is chosen at random and noted in the display.

Clearing the Audible Alarm

To clear the audible alarm:

1. Open the Audible Alarm console.
2. Perform one of the following:
   - Click **Deactivate** (recommended)
   - Deselect the Enabled checkbox for the specific alarm severity and click **Apply**.
3. Click **Close** to exit the console.

Alarm Handling

The information Net-Net EMS displays in the alarms table includes the severity level of the alarm (Severity column) and whether the alarm has been acknowledged (Ack column). The severity levels for the alarms are color coded, all Critical alarms are red, Major alarms are gold, and so on. (See *Viewing Alarm Information* in the *Net-Net EMS User Guide* for details about the alarm display.)

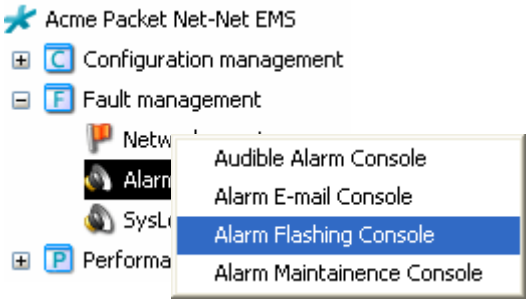
You can control the visual display of unacknowledged alarms by configuring alarm flashing based on severity level. Each alarm of the severity level you configure, has its entry in the Severity column continuously change from the assigned severity color to a white background, and back, at a specified interval. The alarm will flash until it is acknowledged, or you configure the flashing to stop.

Configuring Flashing Alarms

To configure flashing alarms:

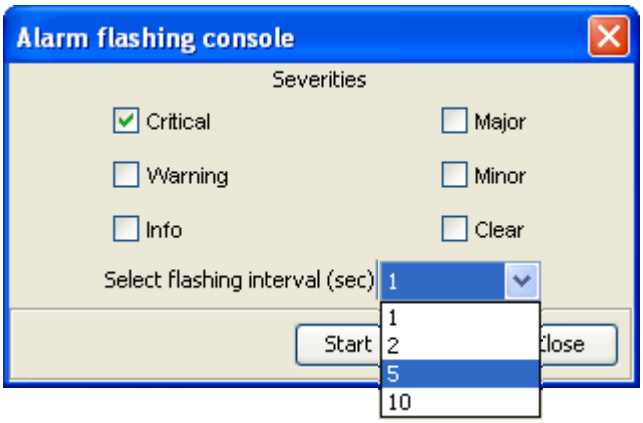
1. Click the plus sign (+) next to Fault management in the navigation pane to expand it.

2. Right-click Alarms. A pop-up list of options appears.
3. Click Alarm Flashing Console to choose it.



The Alarm flashing console appears.

4. **Severities**—Choose the severity levels of the alarms you want to flash by clicking the checkboxes. For example, if you want alarms with the severity level of Critical to flash, click the Critical checkbox. You can choose any or all of the severity levels.
5. **Select flashing interval (sec)**—Choose the interval in seconds at which you want the alarms to flash from the drop-down list.



6. Click **Start Flashing**. The button toggles to **Stop Flashing**.
7. Click **Close**. The flashing starts immediately. The background color in the Severity column changes from its assigned color to white and back again for the specified interval. For example, the Critical alarm's red background has changed to white:

Date/Time	Severity	Category	Ack	Host Name/IP Address	Failed Resource	SysUpTime	
Mar 27,2007 04:45:01 PM	Critical	apSysLog	No	172.30.10.114	Peer of sd114.	1 hours, 5 minutes, 4...	All
Mar 27,2007 04:44:58 PM	Critical	apSysLog	No	172.30.10.115	Peer of sd115.	2 hours, 14 minutes, ...	All
Mar 27,2007 03:51:45 PM	Major	Gateway	No	172.30.10.113	gateway 4.4.4.4 unreac...	0 hours, 48 minutes, ...	Gat
Mar 27,2007 03:43:46 PM	Warning	Session a...	No	172.30.10.113	sip-sa2	0 hours, 40 minutes, ...	SA
Mar 27,2007 03:43:46 PM	Warning	Session a...	No	172.30.10.113	sip-sa1	0 hours, 40 minutes, ...	SA
Mar 27,2007 03:43:46 PM	Warning	Session a...	No	172.30.10.113	sip-sa	0 hours, 40 minutes, ...	SA
Mar 27,2007 03:43:32 PM	Warning	CPU	No	172.30.10.113	apSysCPUUtil	0 hours, 40 minutes, ...	The

Stopping Alarms from Flashing

You can stop the alarm flashing by using the Alarm flashing console or by acknowledging the alarm.

Using the Alarm Flashing Console

1. Access the Alarm flashing console.
2. Click **Stop Flashing**. The button toggles to **Start Flashing**.
3. Click **Close**.

Acknowledging Alarms

Users with the appropriate privileges can acknowledge alarms by clicking **Acknowledge** on the Alarms details window. When you acknowledge an alarm, the the Acknowledge, Owner, and Modified fields are updated. The Acknowledge button toggles to the Unacknowledge button. (See *Viewing Alarm Details* in the Fault Management chapter of the *Net-Net EMS 6User Guide* for details.)

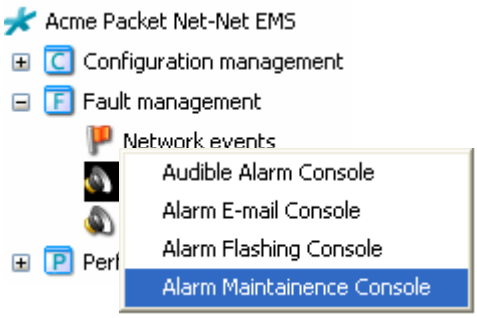
Saving and Deleting Selected Alarms

You can filter selected alarms to choose the ones you want to save or delete. You can select alarms using one, some, or all of the selection criteria. For example, you can select alarms for a specific IP address during a specified date-time range.

Configuring Alarm Selection

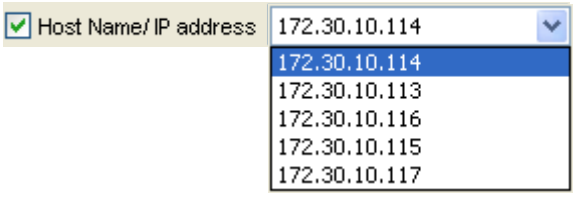
To configure alarm selection:

1. Click the plus sign (+) next to Fault management in the navigation pane to expand it.
2. Right-click Alarms. A pop-up list of options appears.
3. Click Alarm Maintenance Console to choose it.



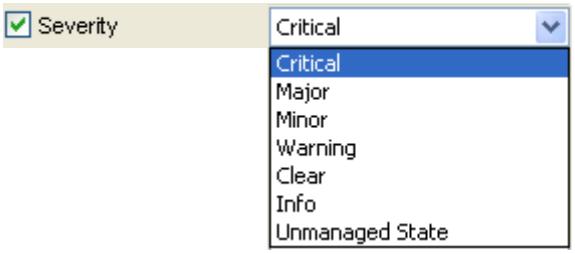
The Alarm maintenance console appears. Choose the alarm filtering method by clicking any or all of the checkboxes.

4. **Host Name/IP address**—Click the checkbox to select alarms based on hostname or IP address. The drop-down list is activated.
5. Choose the hostname or IP address from the drop-down list.

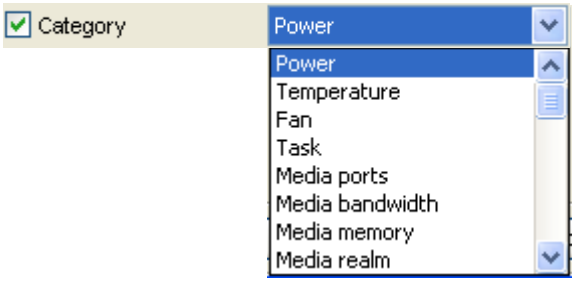


6. **Severity**—Click the checkbox to select alarms based on severity. The drop-down list is activated.

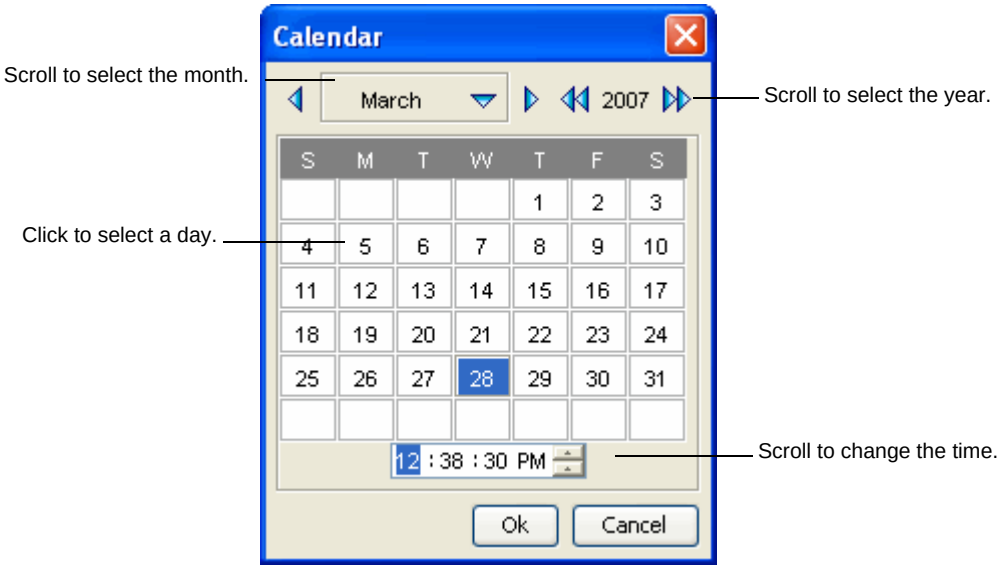
7. Choose the severity level from the drop-down list.



8. **Category**—Click the checkbox to select alarms based on category. The drop-down list is activated.
9. Choose the category from the drop-down list.

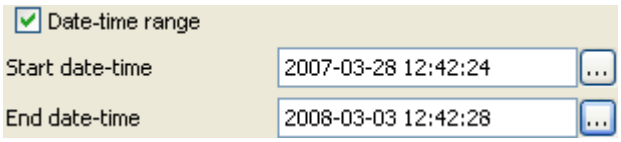


10. **Date-time range**—Click the checkbox to select alarms based on a date-time range. The Start date-time and End date-time textboxes are enabled.
11. **Start date-time, End date-time**—Click ... to access the Calendar:



12. Choose the month and the year by using the arrows to scroll to the needed options.
13. Choose the day by clicking the appropriate cell.
14. Choose the time by scrolling up or down in the time textbox.

15. Click **OK** to exit the Calendar and apply the values.



You can now save or delete alarms.

Saving Alarms

To save alarms:

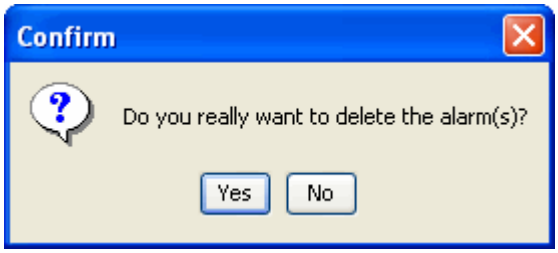
1. In the Alarm maintenance console, click **Save**. You are prompted to save the alarms text file (.txt). The file name is Alarms-date time.txt. For example:

   `Alarms-2007-03-28 12-51-54.txt`
2. Edit the default file name to change it.
3. Choose the location to which you want to save your alarm file.
4. Save the file.

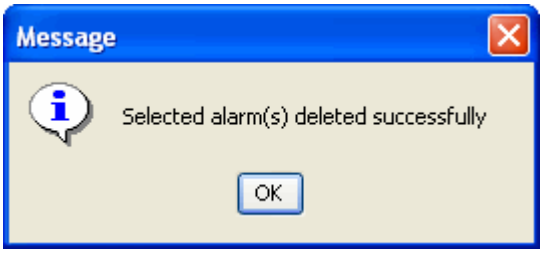
Deleting Alarms

To delete alarms:

1. In the Alarm maintenance console, click **Delete**. A confirmation message appears.



2. Click **Yes** to continue the deletion. A message that alarms were deleted successfully appears.



3. Click **OK**.

   The alarms you selected for deletion are removed from the Alarms display.

Viewing Syslog Information

This section explains how to view the syslog messages generated for the discovered devices. Each Net-Net SBC generates syslog messages. These message can be stored internally within the device or forwarded to an external entity. If the syslog server's IP address is set to 0.0.0.0, logs are stored internally within the device. If the IP address is set to an EMS server, the logs are saved in the database.

Syslog Message Example

The following example shows one of the possible syslog messages. For more information and additional examples, see the *Net-Net MIB Reference Guide*.

Hardware Monitor Failure Trap Example

The following is an example of an `apSyslogMessageGenerated` trap caused by the failure of the Net-Net system's environmental sensor. This generated a Critical-level alarm.

```
==============PACKET CAPTURED================
DLC: Ethertype=0800, size=307 bytes
IP:  D=[10.0.1.27] S=[10.0.2.233] LEN=273 ID=317
UDP: D=162 S=161  LEN=273
SNMP: ----- Simple Network Management Protocol (Version 2) -----
   SNMP:
   SNMP: SNMP Version = 2
   SNMP: Community    = public
   SNMP: Command      = SNMPv2-trap
   SNMP: Request ID   = 1
   SNMP: Error status = 0 (No error)
   SNMP: Error index  = 0
   SNMP:
   SNMP: Object = {1.3.6.1.2.1.1.3.0} (sysUpTime.0)
   SNMP: Value  = 5145 hundredths of a second
   SNMP:
   SNMP: Object = {1.3.6.1.6.3.1.1.4.1.0} (internet.6.3.1.1.4.1.0)
   SNMP: Value  = {1.3.6.1.4.1.9148.3.1.2.0.1}
   SNMP:
   SNMP: Value  = type
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.5.1}
(enterprise.9148.3.1.1.2.3.1.5.1)
   SNMP: Value  = Hardware monitor failure! Unable to monitor fan speed and
temperature!
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.6.1}
(enterprise.9148.3.1.1.2.3.1.6.1)
   SNMP: Value  = 50 (time ticks)
   SNMP:
ADDR  HEX                                                ASCII
0000: 00 d0 09 6e a0 0c 00 08 25 01 00 70 08 00 45 00 | .Ð.n ...%..p..E.
0010: 01 25 01 3d 00 00 40 11 60 88 0a 00 02 e9 0a 00 | .%.=..@.`ˆ...é..
```

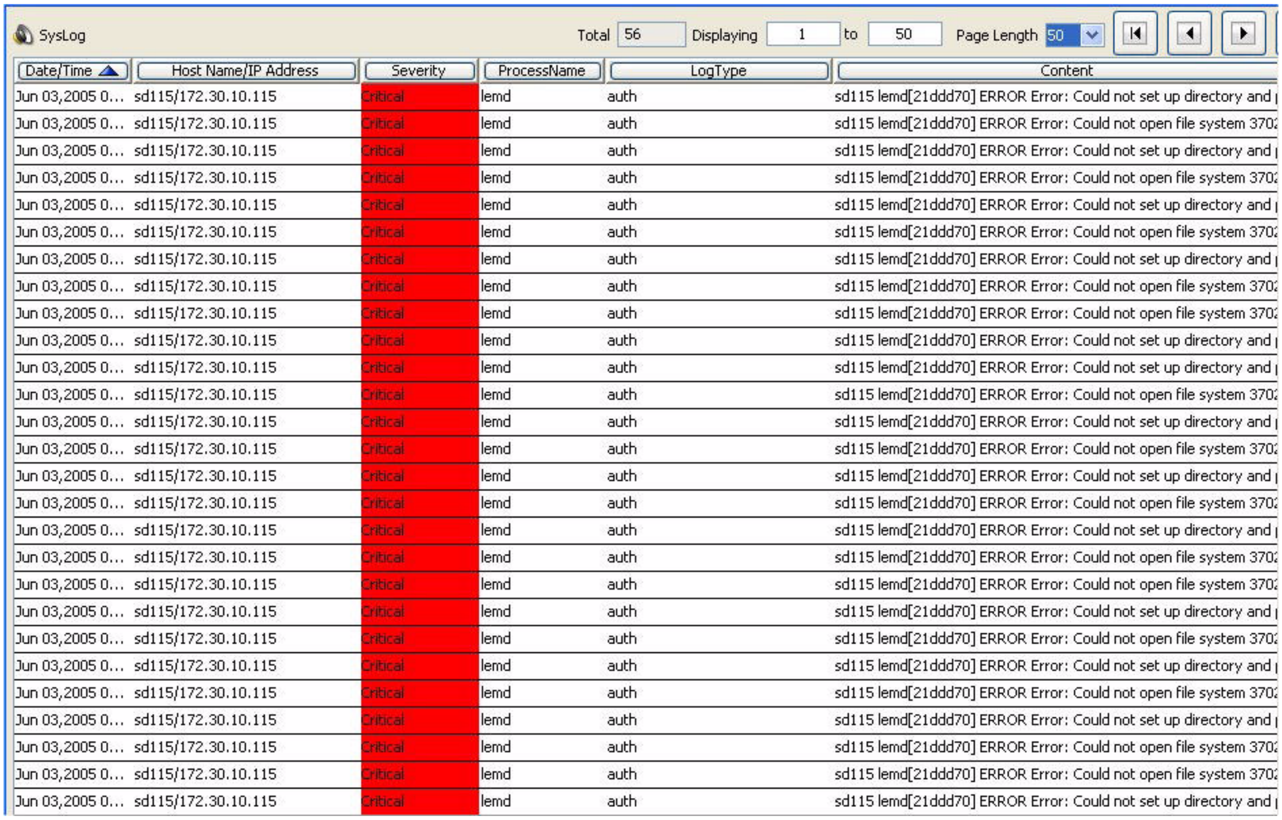
```
0020: 01 1b 00 a1 00 a2 01 11 fd 08 30 82 01 05 02 01 | ...¡.¢..ý.0,....
0030: 01 04 06 70 75 62 6c 69 63 a7 81 f7 02 01 01 02 | ...public§_÷....
0040: 01 00 02 01 00 30 81 eb 30 0e 06 08 2b 06 01 02 | .....0_ë0...+...
0050: 01 01 03 00 43 02 14 19 30 1a 06 0a 2b 06 01 06 | ....C...0...+...
0060: 03 01 01 04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 | ........+....Ç<.
0070: 01 02 00 01 30 1d 06 0f 2b 06 01 04 01 c7 3c 03 | ....0...+....Ç<.
0080: 01 01 02 03 01 02 01 04 0a 61 63 6d 65 73 79 73 | .........acmesys
0090: 74 65 6d 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 | tem0...+....Ç<..
00a0: 01 02 03 01 03 01 02 01 02 30 17 06 0f 2b 06 01 | .........0...+..
00b0: 04 01 c7 3c 03 01 01 02 03 01 04 01 04 04 74 79 | ..Ç<..........ty
00c0: 70 65 30 59 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | pe0Y..+....Ç<...
00d0: 02 03 01 05 01 04 46 48 61 72 64 77 61 72 65 20 | ......FHardware
00e0: 6d 6f 6e 69 74 6f 72 20 66 61 69 6c 75 72 65 21 | monitor failure!
00f0: 20 55 6e 61 62 6c 65 20 74 6f 20 6d 6f 6e 69 74 |  Unable to monit
0100: 6f 72 20 66 61 6e 20 73 70 65 65 64 20 61 6e 64 | or fan speed and
0110: 20 74 65 6d 70 65 72 61 74 75 72 65 21 30 14 06 |  temperature!0..
0120: 0f 2b 06 01 04 01 c7 3c 03 01 01 02 03 01 06 01 | .+....Ç<........
0130: 43 01 32                                        | C.2
============SAME PACKET RECEIVED BY SNMP TEST TOOL================
Tue Nov 11 17:09:50 2003  SNMPv2c trap from [10.0.2.233]
   sysUpTime.0 :  (5145) type TimeTicks
   snmpTrapOID.0 : apSyslogMessageGenerated (1.3.6.1.4.1.9148.3.1.2.0.1)
type ObjectID
   apSyslogHistFrom.1 :  (ACMEPACKET) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistLevel.1 :  (2) type SyslogLevel, indexed by
apSyslogHistIndex
   apSyslogHistType.1 :  (type) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistContent.1 :  (Hardware monitor failure! Unable to monitor
fan speed and temperature!) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistTimestamp.1 :  (50) type TimeStamp, indexed by
apSyslogHistIndex
```

Displaying Syslog Messages

By default the syslog message display is started and you can access the syslog message view. You can stop and re-start the syslog message display at any time.

To display the syslog view:

1. Under the Fault Management category, click `SysLog`. The syslog view appears in the right pane. For example:



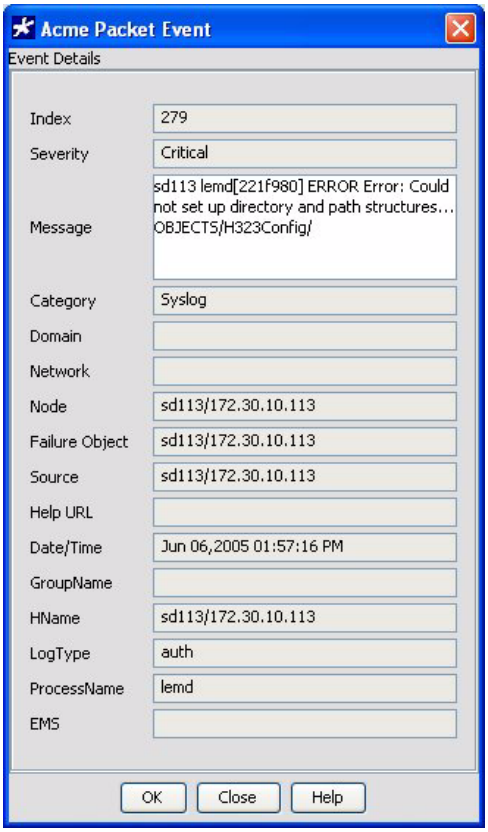
Date/Time	Host Name/IP Address	Severity	ProcessName	LogType	Content
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not open file system 370
Jun 03,2005 0...	sd115/172.30.10.115	Critical	lemd	auth	sd115 lemd[21ddd70] ERROR Error: Could not set up directory and

Viewing Details

You can view the details for a syslog message.

To view the syslog details:

1. In the SysLog view, double-click the row of the syslog message you want to view. The Event Details window appears:



2. Review the information and click **OK** to apply the changes and close the dialog box.

The following table contains descriptions of the information contained in the dialog box.

Event Category	Description
Index	Unique ID created for the generated event
Severity	Severity level of event • All • Emergency • Critical • Major • Minor • Clear • Warning • Notice • Info • Trace • Debug
Message	Message associated with the event
Category	Category to which the event belongs
Domain	Domain-specific information which is based on the physical location, functional categorization, or logical categorization of the source of the event
Network	Network to which the event belongs
Node	Node to which the event belongs. For example, if the event is for an interface, the node value is specified as the interface parent node.
Failure Object	Specific entity in the source that has failed and is primarily responsible for the event
Source	Exact source of the event
Help URL	URL for locating the help documentation on clicking the Help button in the same dialog box
Date/Time	Date and time the event was generated
GroupName	Name of the group to which the event belongs
HName	Name of the host from which the alarm was generated
Log Type	Type of log
ProcessName	Name of the process that generated the log
EMS	

Stopping Syslog Message Display

You can stop the display of syslog messages.

To stop the syslog message display:

1. Under Fault Management, right-click `SysLog`. A list of options appears.
2. From the list, click **Stop**. The Stop option toggles to Start option and the Confirm message appears:

3. Click **Yes** to stop the syslog message display. The disabled successfully message appears.

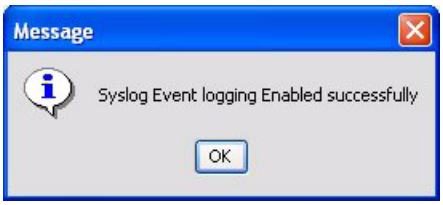
4. Click **OK** to clear the message.

Starting Syslog Message Display

To start the syslog message display:

1. Under Fault Management, right-click `SysLog`. A list of options appears.
2. From the list, click **Start**. The Start option toggles to Stop option and the Confirm message appears:

3. Click **Yes** to start the syslog message display. The enabled successfully message appears.



4. Click **OK** to clear the message.

Sorting Syslog Messages

By default, the syslog messages in the Syslog view are displayed in the order of precedence based on the Date/Time and in descending order. This order can be changed using the Sorting option.

To sort events:

1. In the Syslog view, click the column header for the column you want to change the sort order.

   When you click the column header for the first time, the column is sorted in ascending order. Clicking the same column header again sorts the column in descending order. The up and down arrows in the headers indicate ascending and descending order respectively.

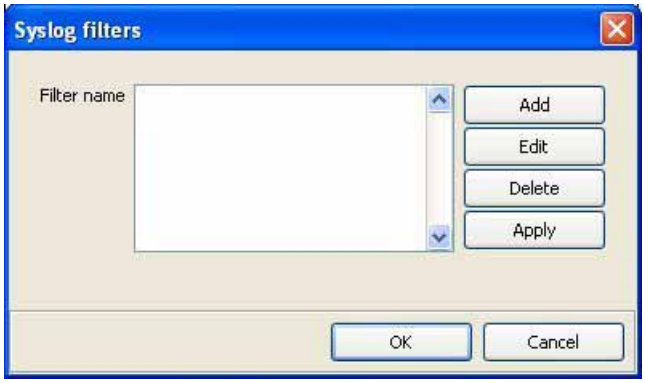
Filtering Syslog Messages

You can create filters to apply to the syslog view to focus on the syslog messages that meet specific criteria. That criteria can be as broad as filtering syslog messages on all severity levels or as narrow as filtering on severity level, date and time range, and process.

Accessing the Syslog Filter Dialog Box

To access the Syslog filters dialog box:

1. Under Fault Management, right-click `Syslog`. A list of options appears.
2. Click `Syslog filter` to select it. The Syslog filters dialog box appears:



Note: You can also choose `Syslog filter` from the Display filter option in the toolbar.

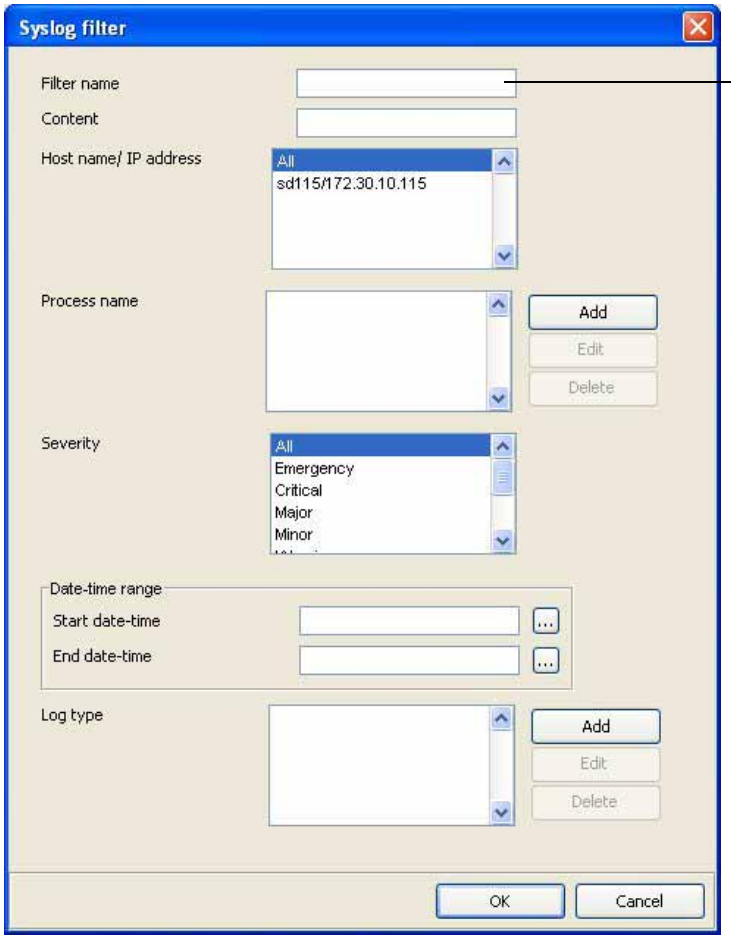
From here you can add or edit, then apply filters, as well as delete filters.

Adding New Syslog Filters

You can add new filters to use to filter the syslog messages.

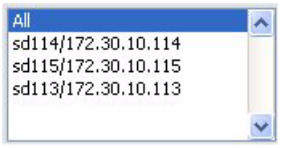
To add syslog filters:

1. Click **Add**. The Syslog filter dialog box appears:



From here you enter the criteria by which you want to filter the syslog messages. The only required information is a name for the filter. You can create a filter that operates on Content and Process name, or on Severity, or just on Host Name or IP address.

2. **Filter name**—*Required*. Enter a name for the filter. For example, filter1.
3. **Content**—Enter the text of the log message to filter by Content field. All messages that have Content fields that contain this text will be displayed.
4. **Host name/IP address**—Choose one or more host names or IP addresses (or all) from the list. All discovered Net-Net SBCs appear in the list. For example:



You can choose multiple values.

- Use CTRL+click to select multiple non-contiguous values
- Use SHIFT+click to select multiple contiguous values
- Click **All** to filter on all discovered Net-Net SBCs

All messages generated by the selected host names or IP addresses will be displayed.

5. **Process name**—Enter the name (or names of multiple processes) that generated the log.

   5a. Click **Add**. The Process name dialog box appears:

   5b. Enter the name of the process that generated the log. The following table lists the processes:

Process	Description
algd	MGCP processes
berpd	Berpd process or the redundancy health process. Used for storing health messages and events and for determining whether a switchover is required.
brokerd	Platform-level processes, for example various host tasks related to communicating with the network processors and/or the CAM. Brokerd also forwards messages from the IP fragmenter, which currently takes part in the SIP NAT process, through sysmand to the acmelog (the overall system log).
cliTelnet	ACLI Telnet sessions, if your system access method is Telnet
console	ACLI console functions
h323d	H.323 processes
lemd	Local element manager (or local database server) processes, pertains to remote retrievals of and writing of configuration data
mbcd	Application flow manager processes, such as the creating, updating, and removing media NAT entries
radd	Accounting daemon for RADIUS. It serves as a RADIUS client to the outside world. Also serves as a place to concentrate RADIUS records from various signaling protocol tasks running on the Net-Net SBC.

Process	Description
sipd	SIP process; how the Net-Net system's SIP proxy is processing messages
sysmand	System manager process, which is currently responsible for writing the system log (acmelog), dispatching commands to other application tasks, and starting the application-level code

5c. Click **OK**.

The process name is added to the list and the Edit and Delete buttons are activated.

5d. Enter another process name following steps 5a through 5c or click **Cancel**. All process names appear in the list. For example:

All messages that have the specified process names are displayed.

6. **Severity**—Choose the severity level from the drop-down list. You can choose multiple values.

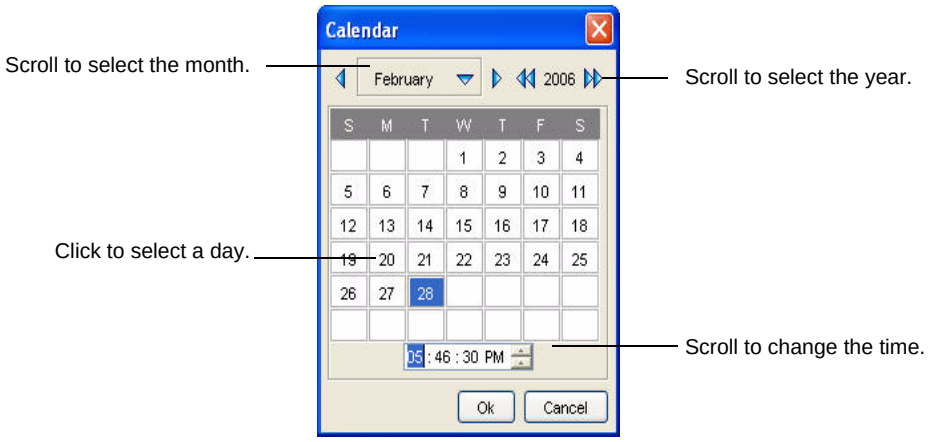
- Use CTRL+click to select multiple non-contiguous values
- Use SHIFT+click to select multiple contiguous values
- Click **All** to include all severity levels

For example:

7. **Date-time range**—Enter the start date and time and end date and time.

7a. **Start date-time** and **End date-time**—Click the box next to the textboxes to access a calendar. For example:

The Calendar appears:



7b. Choose the month, and the year, for the date by scrolling to the month and year you need.

7c. Choose the day by clicking the appropriate cell.

7d. Choose the time by scrolling up or down in the time textbox.

Only syslog messages within that date-time range will be displayed.

8. **Log type**—Add the log types upon which you want to filter.

8a. Click **Add**. The Log type dialog box appears:

8b. Enter the text that identifies the log type.

8c. Click **OK**.

The log type is added to the list and the Edit and Delete buttons are activated.

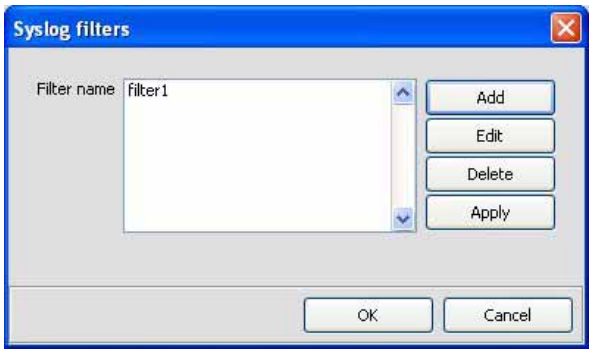
8d. Enter another log type following steps 8a through 8c or click **Cancel**. All log types appear in the list. For example:

8e. Choose the log types from the list for which you want to filter.

- Use CTRL+click to select multiple non-contiguous values
- Use SHIFT+click to select multiple contiguous values
- Click **all** to include all log types

All messages for those specified log types are displayed.

9. After you enter all filter criteria, click **OK**. The filter name appears in the Syslog filters list:



10. Click the filter name to select it and click **Apply**. The Confirmation screen appears:

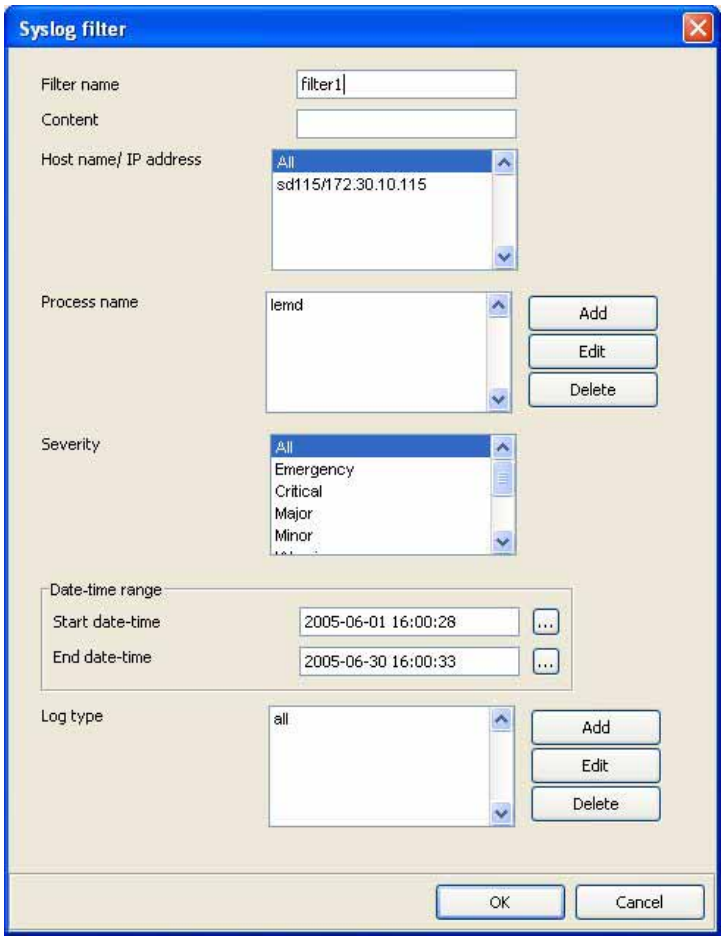
11. Click **Yes** to apply the filter.

Editing Syslog Filters

You can edit an existing filter to change or add filtering criteria.

To edit syslog filters:

1. Click **Edit**. The Syslog filter dialog box appears:

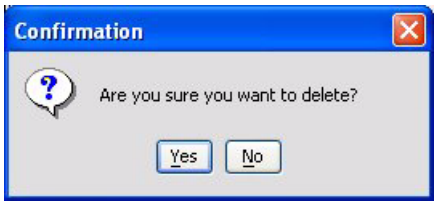


2. Follow the instructions in *Adding New Syslog Filters* to edit or add criteria.

Deleting Filters

To delete filters:

1. In the Syslog filters list, click the name of the filter you want to delete.
2. Click **Delete**. A confirmation message appears:



3. Click **Yes** to delete the file.

Viewing Registration Cache Information

You can use Net-Net EMS to access the registration cache for the SIP, H.323, and MGCP protocols to query and clear entries. You can run an endpoint audit to determine if endpoints are reachable and able to respond to signaling messages.

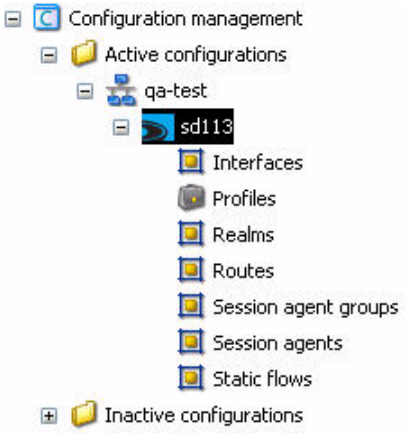
How It Works

You can query and clear entries in each cache using predefined grouping methods among others. You can group cache entries by user (endpoint) or IP address range.

Accessing the Registration Cache

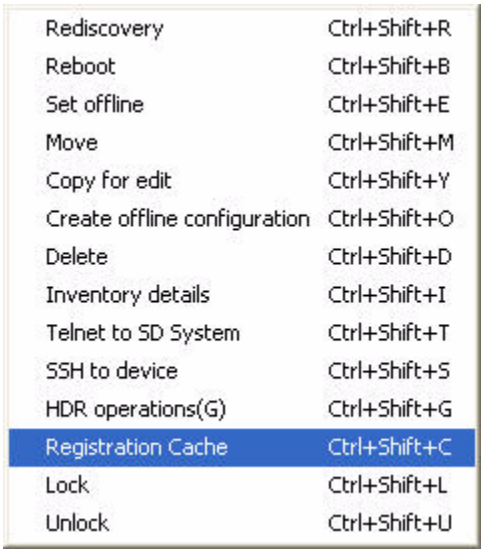
To access the registration cache:

1. In the Active configurations area, right click a Net-Net SBC.



   A pop-up list of options appears.

2. Click Registration Cache to select it.



   The Registration Cache window appears. You can view, audit, and clear registration cache information for SIP, MGCP, and H.323 protocols.

Working with SIP Registration Caches

To display the SIP registration caches:

1. In the Cache Type area, click SIP.

   The SIP commands and registration cache table appear. From here you can show, clear, and audit.

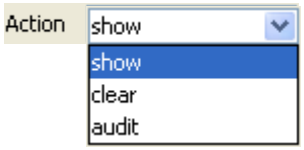
IP Address

Displays the Net-Net SBC's SIP process registration cache for a specified IP address. The IP address value can be a single IP address, a wildcarded IP address value that has an asterisk (*) as its final character, or just the asterisk itself as the wildcard.

> ***Note:*** *This command is only available if you configure the reg-via-key option in the SIP interface prior to endpoint registration. The reg-via-key option keys all registered endpoints by IP address and username.*

To display the SIP process registration cache for an IP address.

1. **Action**—Choose show from the Action drop-down list.



2. **Type**—Choose by-ip from the Type drop-down list.

3. **Expression**—Enter the IP address value or an IP address range in the form n.n.n.n/nn in the Expression textbox. You can use the asterisk as a wildcard.

4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).

   You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

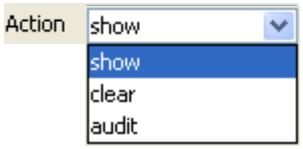
Users

Displays the Net-Net SBC's SIP process registration cache for a specified phone number or for a user name. The **<endpoint>** portion of the command you enter depends on how the SIP endpoint is registered. For example, an endpoint might be registered as `7815551234@10.0.0.3` or as `username@10.0.0.3`. The value preceding the at-sign (@) is what you enter for the **<endpoint>**.

The phone number can be a single number (such as `7815551234`) or a single number wildcarded by placing an asterisk (*) (such as `7815551*`) at the end of the phone number. The user name can be a single name (such as `user`), or a single name wildcarded by using an asterisk at the end of the user name (such as `us*`).

You can prefix the expression with sip: or sips: to specify whether the search for the endpoint should be over the secure connection (TLS) or not.

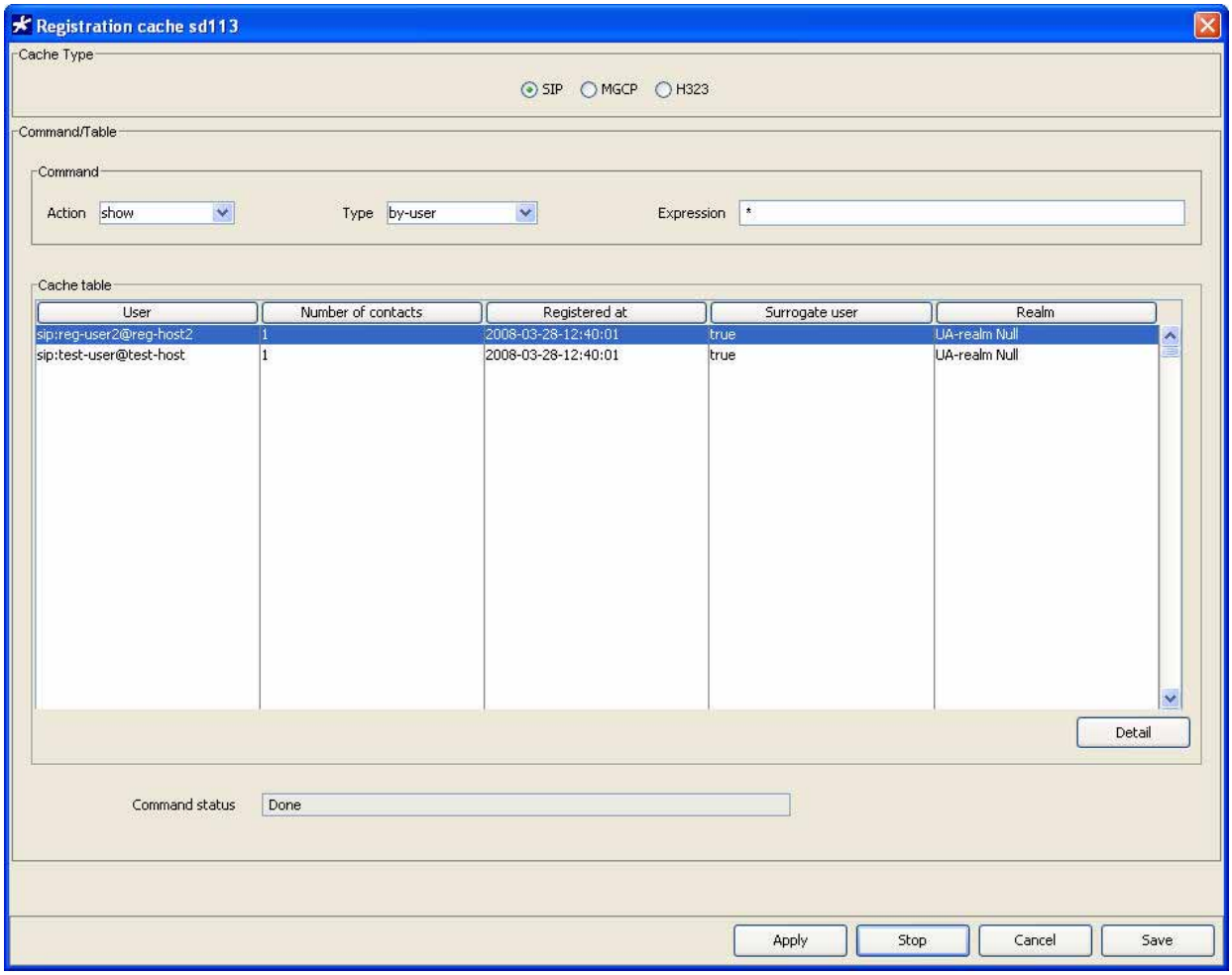
1. **Action**—Choose show from the Action drop-down list.



2. **Type**—Choose by-user from the Type drop-down list.

3. **Expression**—Enter the user name or phone number in the Expression textbox. You can use the asterisk as a wildcard.

4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).



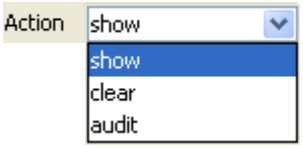
You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Realm

Displays the calls that have registered through a specified ingress realm. The output is sorted alphabetically by the realm name which will be shown first in the output.

To display the SIP process registration cache for a realm:

1. **Action**—Choose show from the Action drop-down list.



2. **Type**—Choose by-realm from the Type drop-down list

3. **Expression**—Enter the name of the realm whose registration cache information you want to view or use the asterisk as a wildcard.

4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).

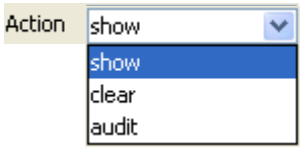
   You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Registrar

Displays formation for calls that use a specific registrar.

To display the SIP process registration cache for a registrar:

1. **Action**—Choose show from the Action drop-down list.



2. **Type**—Choose by-register from the Type drop-down list

3. **Expression**—Enter the IP address of the registrar whose registration cache information you want to view or use the asterisk as a wildcard

4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).

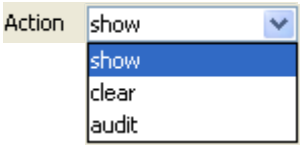
   You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Route

Display information for calls by their Internet-routable IP address. This allows you to view the endpoints associated with public addresses.

To display the SIP process registration cache for a route:

1. **Action**—Choose show from the Action drop-down list.



2. **Type**—Choose by-route from the Type drop-down list

3. **Expression**—Enter the IP address whose registration cache information you want to view or use the asterisk as a wildcard

4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).

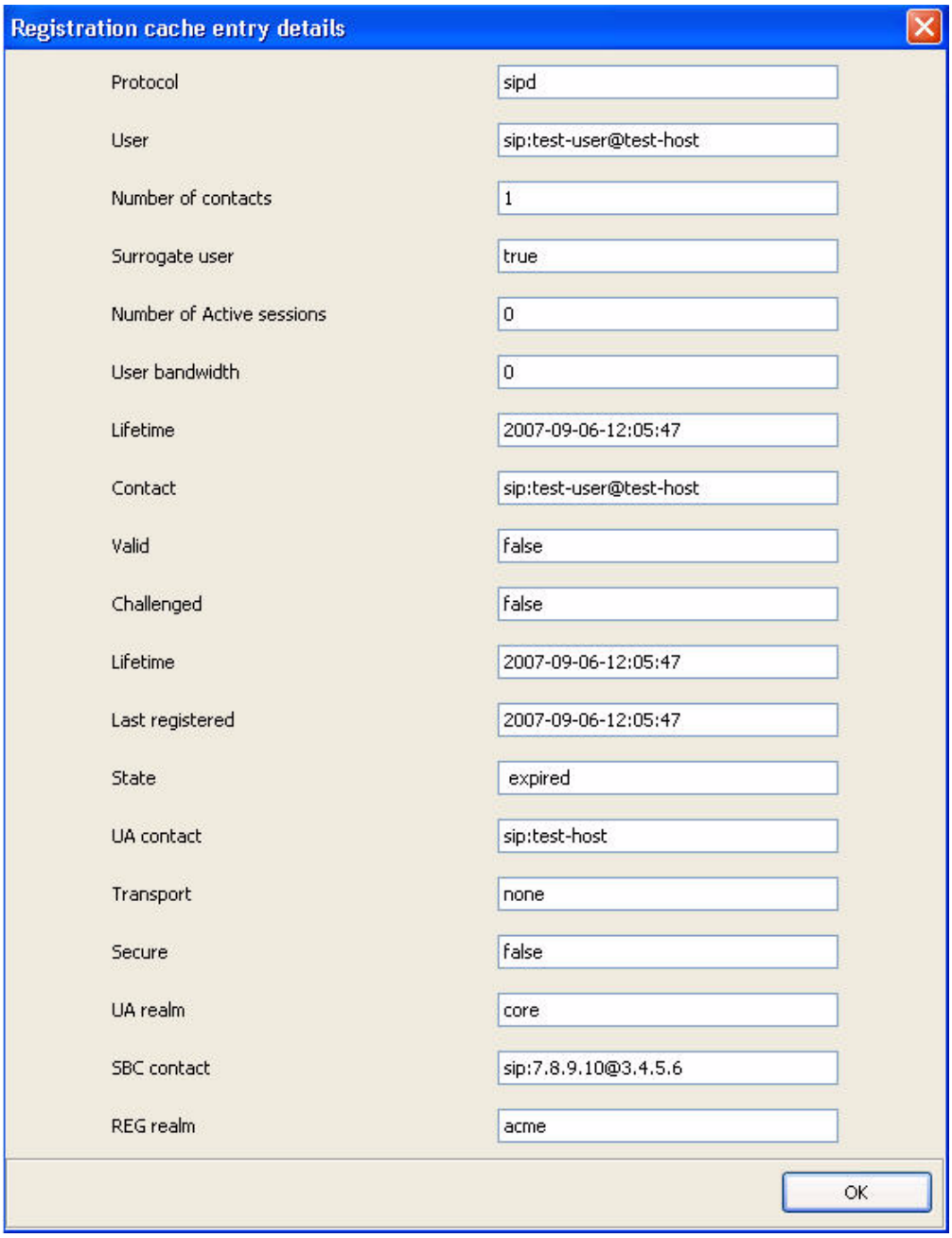
   You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Command Status

The Command status textbox displays the commands you issue. For example:

Viewing Registration Cache Details

You can right-click an entry in the Cache table or click a row to select it and then click Detail to access additional details. The Registration cache entry details window appears.



Clearing the SIP Registration Cache

To clear the SIP process registration cache:

1. **Action**—Choose clear from the Action drop-down list.

2. **Type**—Choose all or by-user from the Type drop-down list.

   - **all**—Clears all SIP registrations in the cache
   - **by-user**—Clears the Net-Net SBC's SIP process registration cache of a particular phone number or user name

   Note: You cannot wildcard values for commands to clear the SIP registration cache.

3. **Expression**—If clearing by user, enter a phone number or a user name.
4. Click **Apply**.

Auditing the SIP Registration Cache

To audit the SIP process registration cache:

1. **Action**—Choose audit from the Action drop-down list.
2. **Type**—Choose by-ip or by-user from the drop-down list.
   - **by-ip**—Audits a specified IP address in the SIP registration cache.
   - **by-user** —Audits a specific user by specifying the user name or phone number in the SIP registration cache.

   Note: Note that you cannot wildcard values for commands to audit the SIP registration cache. Expired entries are automatically cleared.

3. **Expression**—Enter an IP address for or phone number or a user name.
4. Click **Apply**.

Working with the H.323 Registration Cache

To work with H.323 registration caches:

1. In the Cache Type area, click H323.

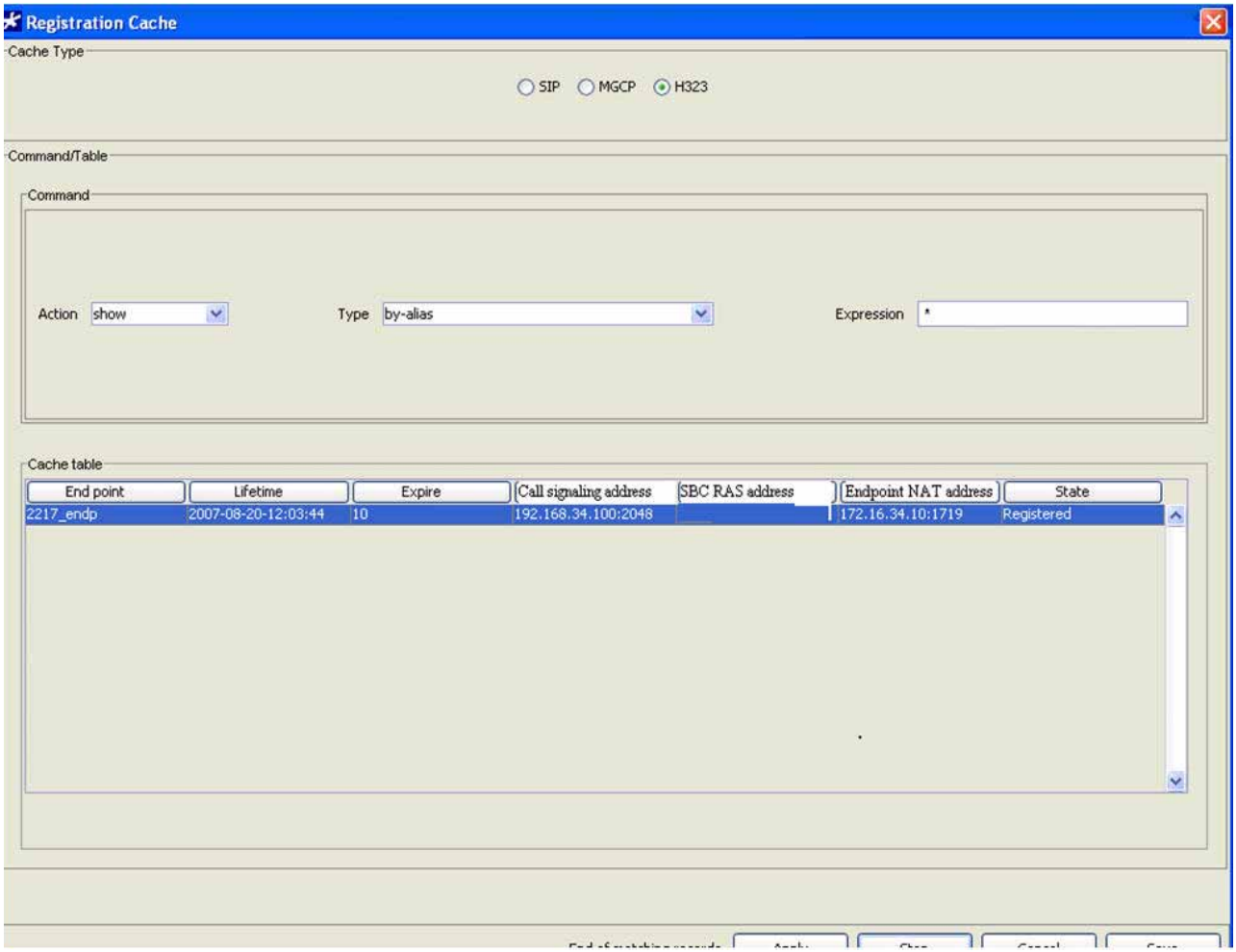
   The H.323 commands and registration cache table appear. From here you can show, clear, and audit registration cache entries.

Displaying the H.323 Registration Cache

To display the H.323 cache entries:

1. **Action**—Choose show from the Action drop-down list.
2. **Type**—Choose by-alias from the Type drop-down list to display the H.323 registration cache for a particular alias.

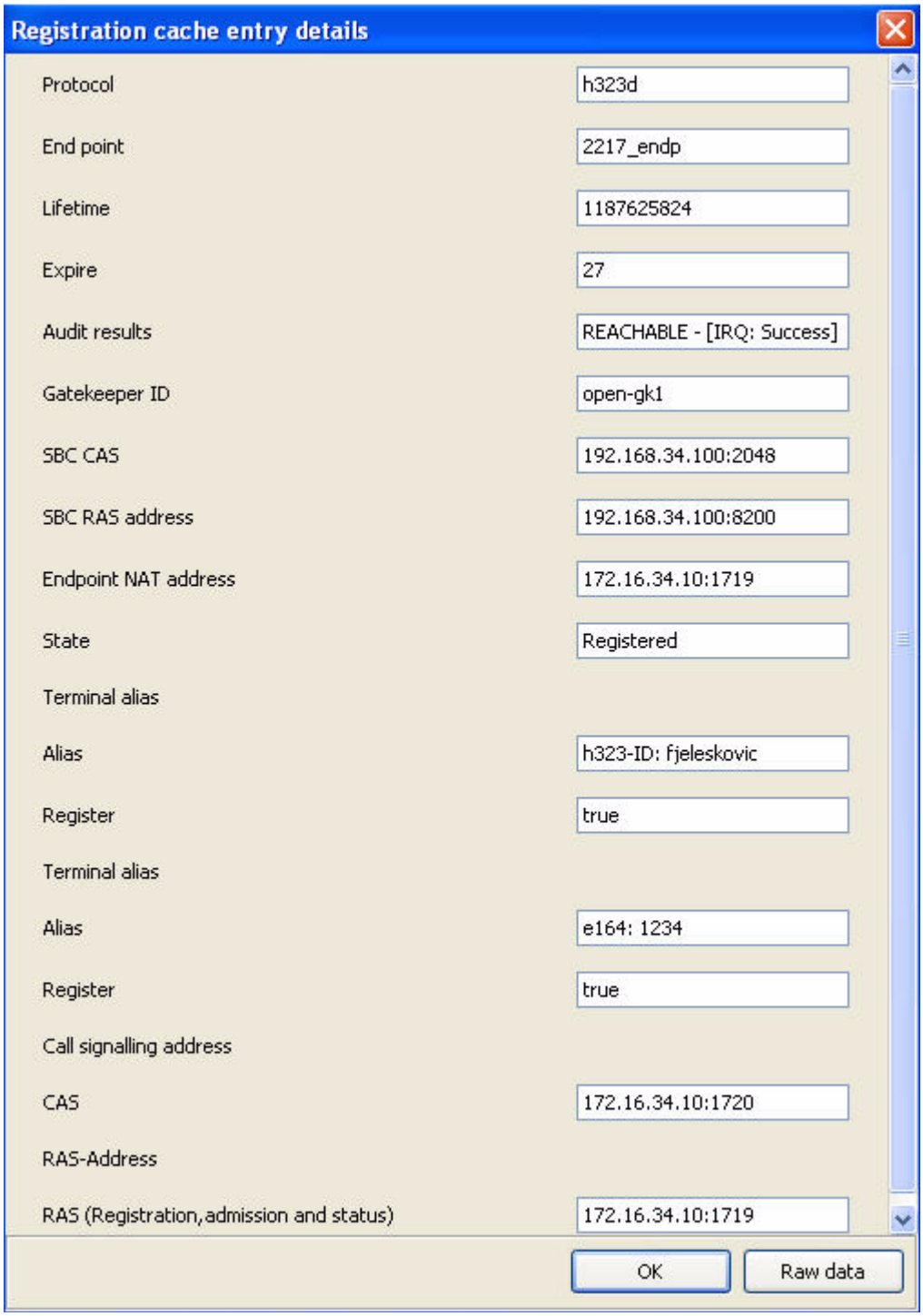
3. **Expression**—Enter use a phone number or terminal identifier. You can wildcard the value by using an asterisk (*) as the final character in the terminalAlias string.
4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).



You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Viewing Registration Cache Details

You can right-click an entry in the Cache table or click a row to select it and then click Detail to access additional details. The Registration cache entry details window appears.



Clearing the H.323 Registration Cache

To clear the H.323 process registration cache:

1. **Action**—Choose clear from the Action drop-down list.

2. **Type**—Choose all or by-alias from the Type drop-down list.
3. **Expression**—If by-alias, enter a phone number or terminal identifier.

   Note: You cannot wildcard values to clear the H.323 registration cache.

4. Click **Apply**.

Auditing the H.323 Registration Cache

To audit the H.323 process registration cache:

1. **Action**—Choose audit from the Action drop-down list.
2. **Type**—Choose by-alias from the drop-down list.
3. **Expression**—Enter enter a phone number or terminal identifier.
4. Click **Apply**.

Working with MGCP Registration Caches

To work with MGCP registration caches:

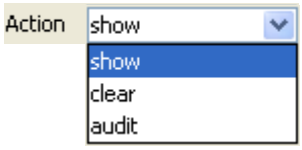
1. In the Cache Type area, click MGCP.

   The MGCP commands and registration cache table appear. From here you can show, clear, and audit registration cache entries.

Displaying the MGCP Registration Cache

To display the MGCP registration cache entries:

1. **Action**—Choose show from the Action drop-down list.

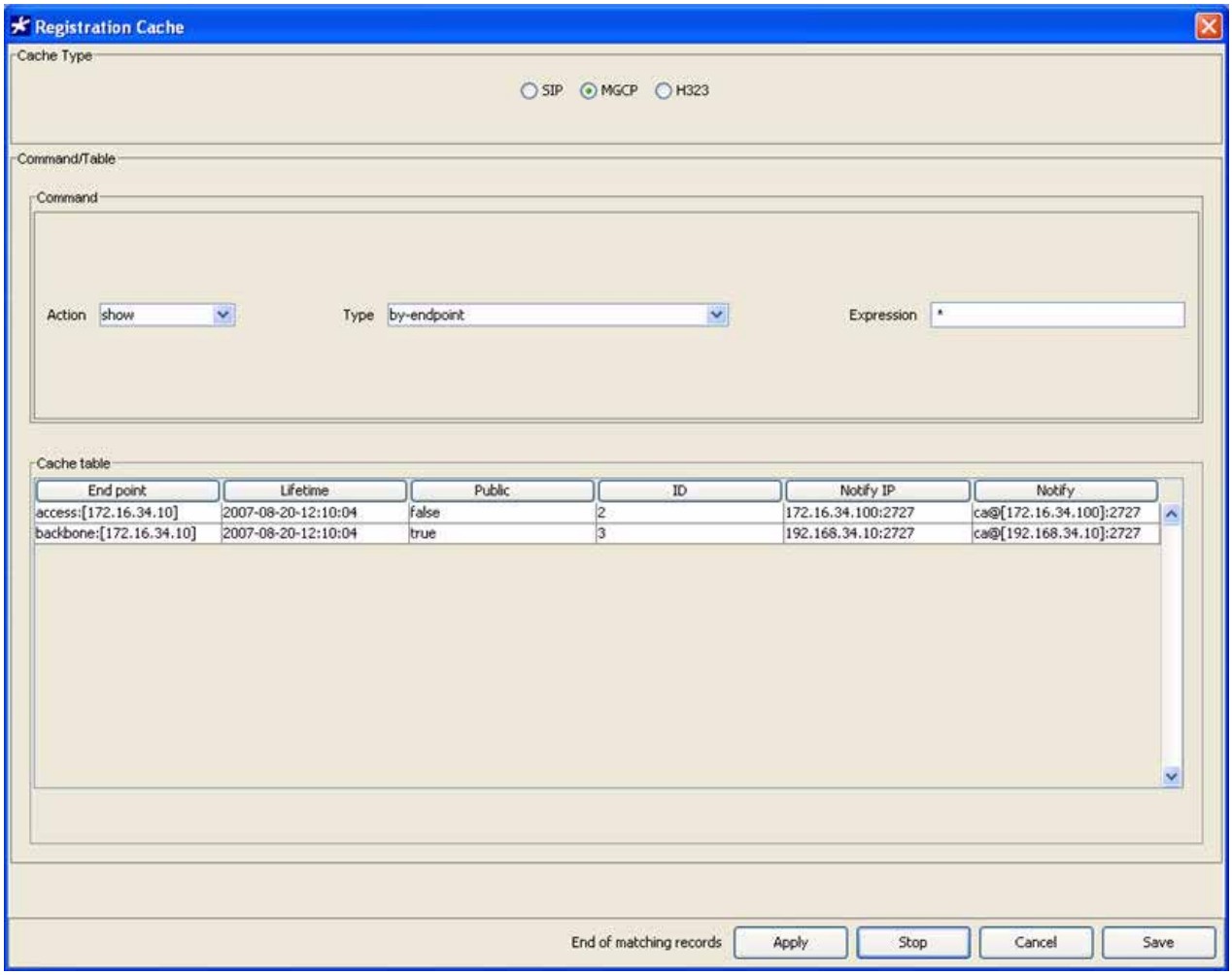


2. **Type**—Choose by-endpoint from the Type drop-down list.
3. **Expression**—Enter one of the following arguments:
   - realm_id:local_name@host
   - realm_id:host
   - local_name@host
   - host

   In these arguments, values are defined as follows:
   - realm_id—Name of a realm named in the MGCP configured; only complete realm names are accepted; entry must end with a colon (:)
   - local_name—Local name of the endpoint; must end with the at-sign (@)

- host—Can be an FQDN, IP address, or IP address enclosed in square brackets ([]); wildcarded by using an asterisk (*) at the end to refer to multiple hosts; using the square brackets for in IP address value is optional

4. Click **Apply**. The Apply button grays out while Net-Net EMS processes the command. A message is displayed in the Command status textbox once processing completes and the Cache table displays the results (if any).



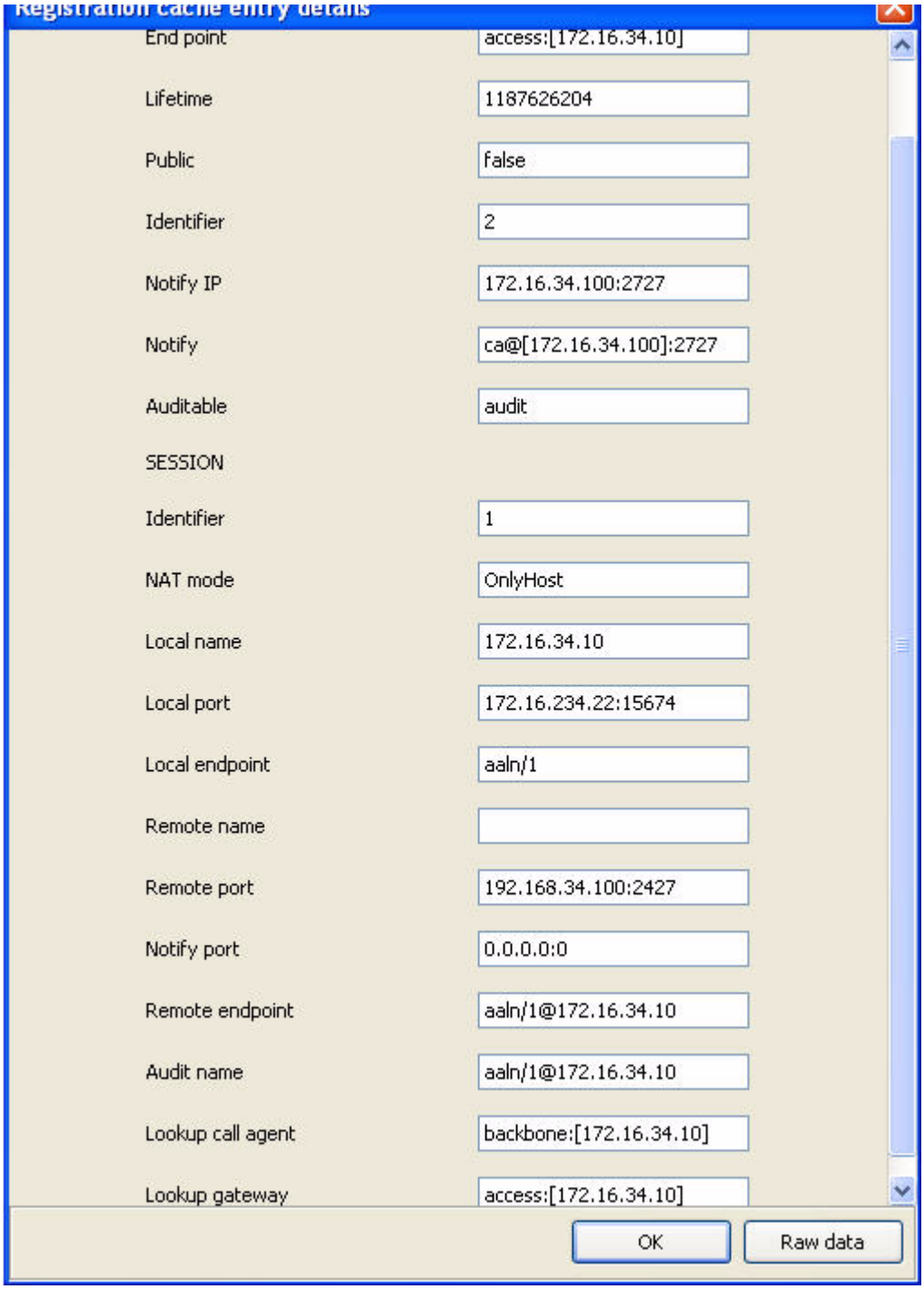
You can view the known details of the cache table entries. See Viewing Registration Cache Details for step-by-step instructions.

Command Status

The Command status textbox displays the commands you issue. For example:

Viewing Registration Cache Details

You can right-click an entry in the Cache table or click a row to select it and then click Detail to access additional details. The Registration cache entry details window appears.



Clearing the MGCP Registration Cache

To clear the MGCP process registration cache:

1. **Action**—Choose clear from the Action drop-down list.

2. **Type**—Choose all or by-endpoint from the Type drop-down list.
   - **all**—Clears all MGCP registrations in the registration cache.
   - **by-endpoint**—Clears the MGCP registration cache of a particular endpoint. You enter this command with one of the following arguments:

     realm_id:local_name@host

     realm_id:host

     In these arguments, values are defined as follows:
     - realm_id—Name of a realm named in the MGCP configured; only complete realm names are accepted; entry must end with a colon (:)
     - local_name—Local name of the endpoint; must end with the at-sign (@)
     - host—Can be an FQDN, IP address, or IP address enclosed in square brackets ([]); wildcarded by using an asterisk (*) at the end to refer to multiple hosts; using the square brackets for in IP address value is optional
3. **Expression**—If clearing by endpoint, enter the endpoint information.
4. Click **Apply**.

Auditing the MGCP Registration Cache

To audit the MGCP process registration cache:

When you audit the MGCP registration cache, the Net-Net SBC sends an audit endpoint message (AUEP) to the MGCP endpoint to determine leachability, and a reply is expected from the endpoint.

MGCP audit messages are only sent to the endpoints in private realms. Requests sent to public realms are rejected and error messages are returned.

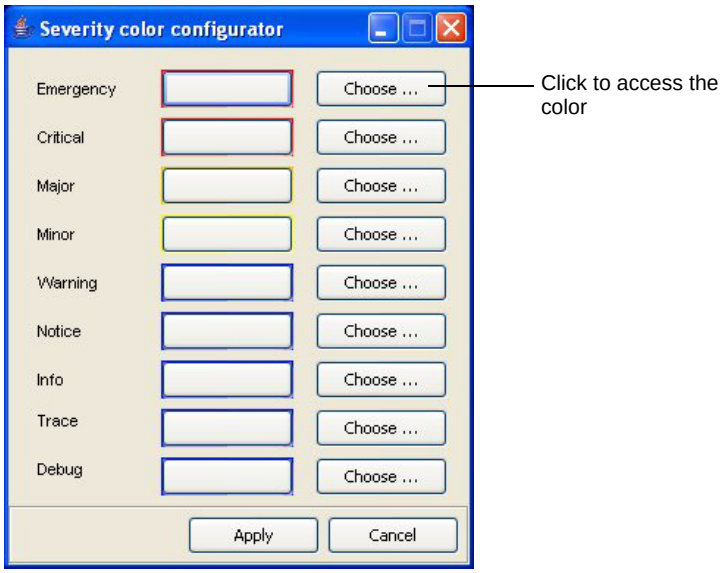
1. **Action**—Choose audit from the Action drop-down list.
2. **Type**—Choose by-endpoint from the drop-down list.
3. **Expression**—Enter the endpoint information.
4. Click **Apply**.

Configuring Severity Color-Coding

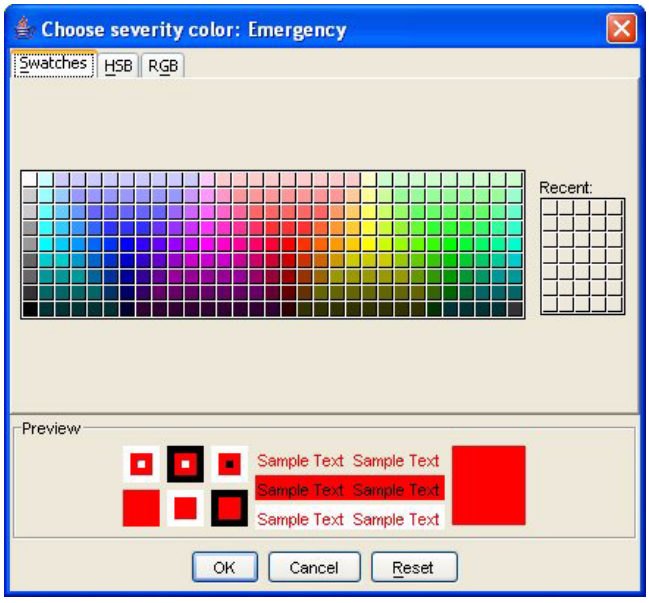
You can configure the colors used to indicate the different severity levels.

To configure colors:

1. Right-click Fault Management and choose Severity configurator from the option list. The Severity color configurator dialog box appears:



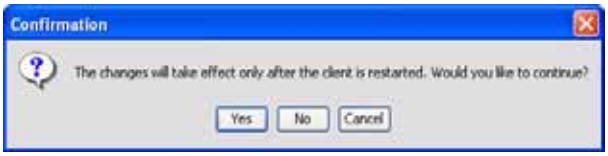
2. Choose the color you want for each severity level by clicking **Choose**. The Choose severity color window appears:



3. Edit the current color, hue/saturation/brightness (HSB) values, and red/green/blue (RGB) values by following the steps in the appropriate section.

   After you make your edits and click **OK** in the Choose severity color window, you return to the Severity color configurator window. From there you can apply your edits.

4. Click **OK** to apply your changes. The Confirmation message appears:



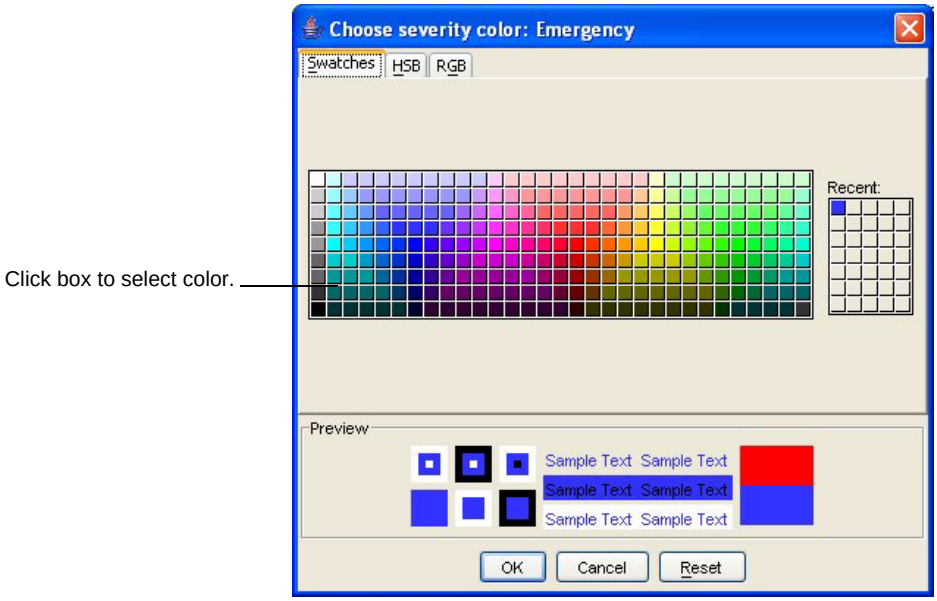
5. Click **Yes** to apply the changes and clear the message.
6. Exit the Severity color configurator.
7. Restart Net-Net EMS to apply your changes.

Choosing a New Color

To choose a new color:

1. In the Choose severity color window, ensure the **Swatches** tab is selected.
2. Click a box in the color grid to select a new color.

   The Preview section of the window displays your color choice and the Recent grid displays the color in the top left block. For example:



3. View your changes in the preview section of the window.

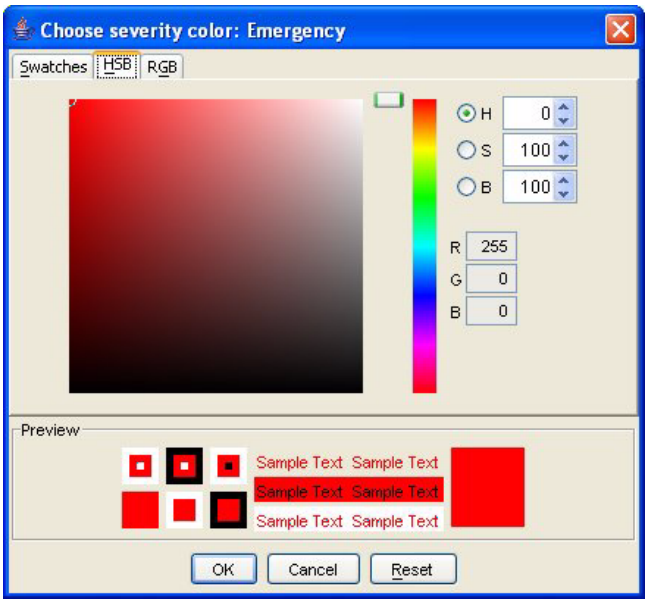
   From here you can edit the HSB values and/or the RGB values, or you can click **OK** to return to the Severity color configurator window.

Editing HSB Values

To edit HSB values:

1. Click the HSB tab.

   The HSB tab contains a color palette, text entry boxes for hue (H), saturation (S), and brightness (B) and display boxes for red (R), green (G), and blue (B) values. For example:



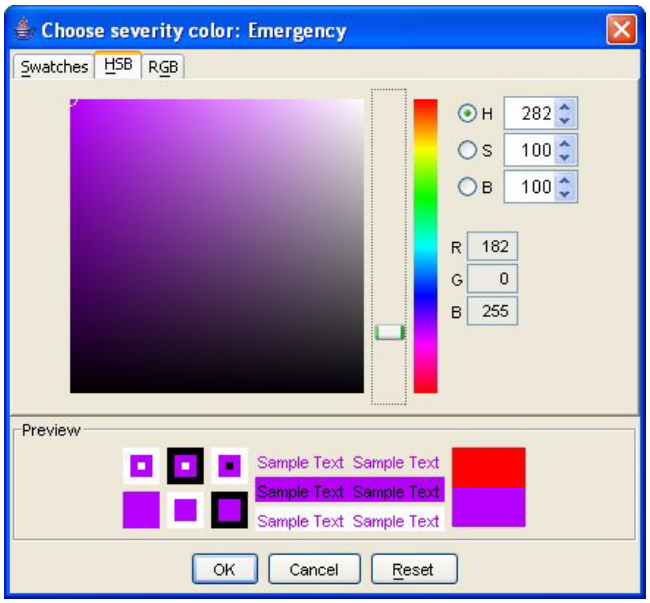
   - RGB (red, green, and blue): a system for representing the colors in your display. Red, green, and blue are combined in various proportions to produce any color in the visible spectrum. Levels of red, green, and blue can each range from 0 to 100 percent of full intensity. Each level is represented by the range of decimal numbers from 0 to 255 (256 levels for each color). The total number of available colors is 256 x 256 x 256, or 16,777,216 possible colors.
   - HSB (hue, saturation, and brightness): aspects of color in the RGB scheme. All possible colors can be specified according to hue, saturation, and brightness.

2. Edit the values for hue, saturation,- and brightness by using one of the following methods:

   2a. Selecting from color palette. Left-click and hold the mouse button while moving the icon in the color palette to select a color.

   2b. Entering specific values. For example, edit the value for hue (H) by clicking the H radio button for the value to select it. Enter a new value.

The R, G, and B values change to reflect the changes made to H, S, or B. Also the slide next to the color bar moves to reflect your edits. For example:



3. View your choice in the preview section of the window.

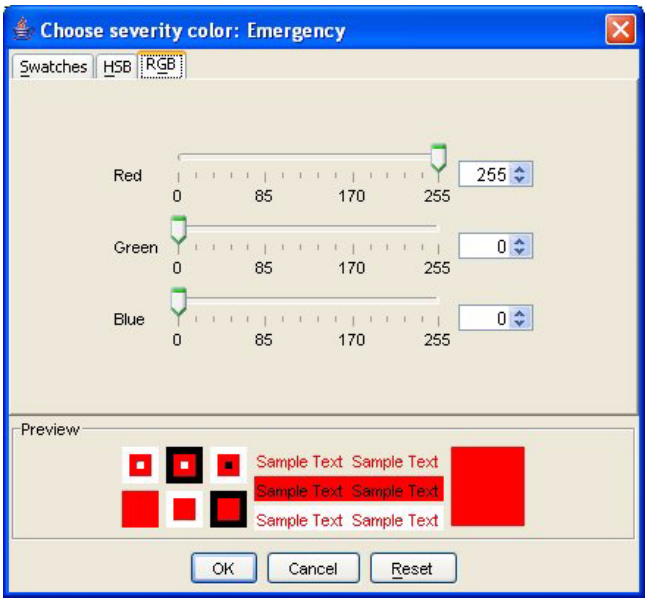
   From here you can edit the RGB values or you can click **OK** to return to the Severity color configurator window.

Editing RGB Values

To edit RGB values:

1. Click the RGB tab.

   The RGB tab contains three sliders to use for changing the values. The values display in the boxes next to each slider. For example:

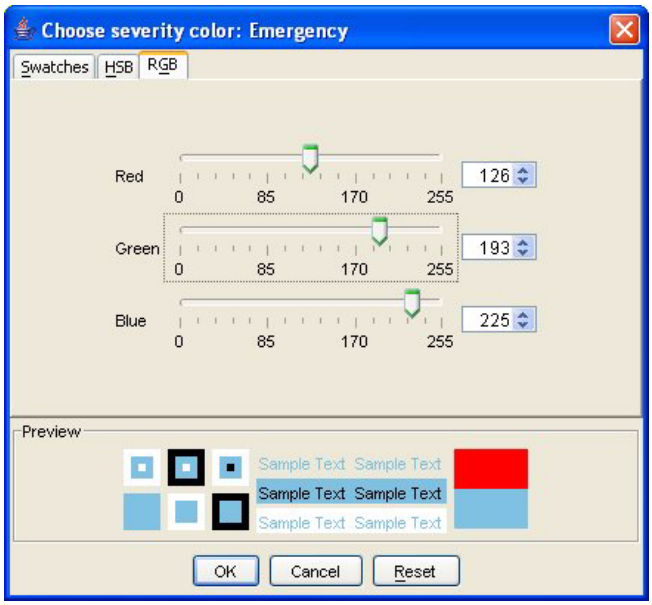


   RGB (red, green, and blue) is a system for representing the colors in your display. Red, green, and blue are combined in various proportions to produce

any color in the visible spectrum. Levels of red, green, and blue can each range from 0 to 100 percent of full intensity. Each level is represented by the range of decimal numbers from 0 to 255 (256 levels for each color). The total number of available colors is 256 x 256 x 256, or 16,777,216 possible colors.

2. Left-click on the slider's bar and move it to the value you want or enter a value in the display box next to the slider.

   The new values display next to the slider and the new color displays in the Preview section. For example:



3. View your choice in the preview section of the window.
4. Click **OK** to apply your changes and return to the Severity color configurator window. From there you can apply your changes.

9 Performance Management

Introduction

This chapter describes the Net-Net EMS performance management component. Performance management involves monitoring your Net-Net SBCs by collecting necessary data from each of them. The performance is measured based on various factors, such as number of bytes of data received/sent (over a period) by a particular interface of a device, the interface's current bandwidth in bits per second, and so on.

The Net-Net EMS displays performance data for your discovered Net-Net SBCs. It displays the statistical and state information provided by the Net-Net SBC software (in the form of MIBs).

In Net-Net EMS, performance management statistics are only gathered for display when you access a Performance management screen or when you click the Refresh button. To preserve data, you must save it to a file by using the Save button.

> **Note:** You need to configure the SNMP community parameter on the Net-Net SBCs for which you want to view performance data. See the *Net-Net EMS 4000 Configuration Guide* and the *Net-Net ACLI Reference Guide* for details.

Accessing Performance Management Information

This section explains how to access the performance management information. The Performance management node is located in the EMS navigation pane's (left pane) hierarchical tree of nodes.

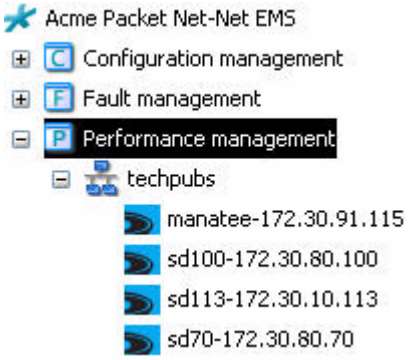
Listed under the Performance management node is a set of domains, each of which contains a list of Net-Net SBCs. The domains and Net-Net SBCs listed under Performance management always matches the list of Net-Net SBCs currently in the Active configuration category (located under the Configuration management node). Any additions and deletions to the Active configuration list of nodes is reflected in the Performance management list.

In the Performance management list, each member of an HA pair is listed individually, which differs from the display in the Active configuration area (where members of an HA pair are treated as a single managed device). You can view performance data for each of the Net-Net SBC systems that belong to the pair.

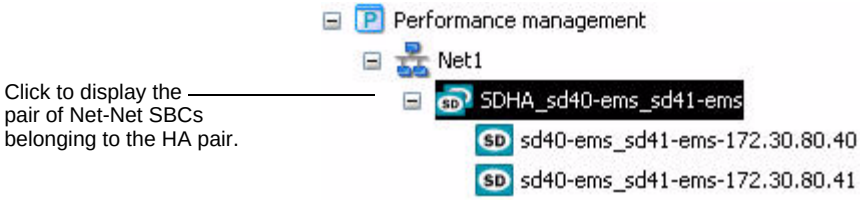
To access performance management information:

1. Click the plus (+) sign next to Performance Management to expand the category.

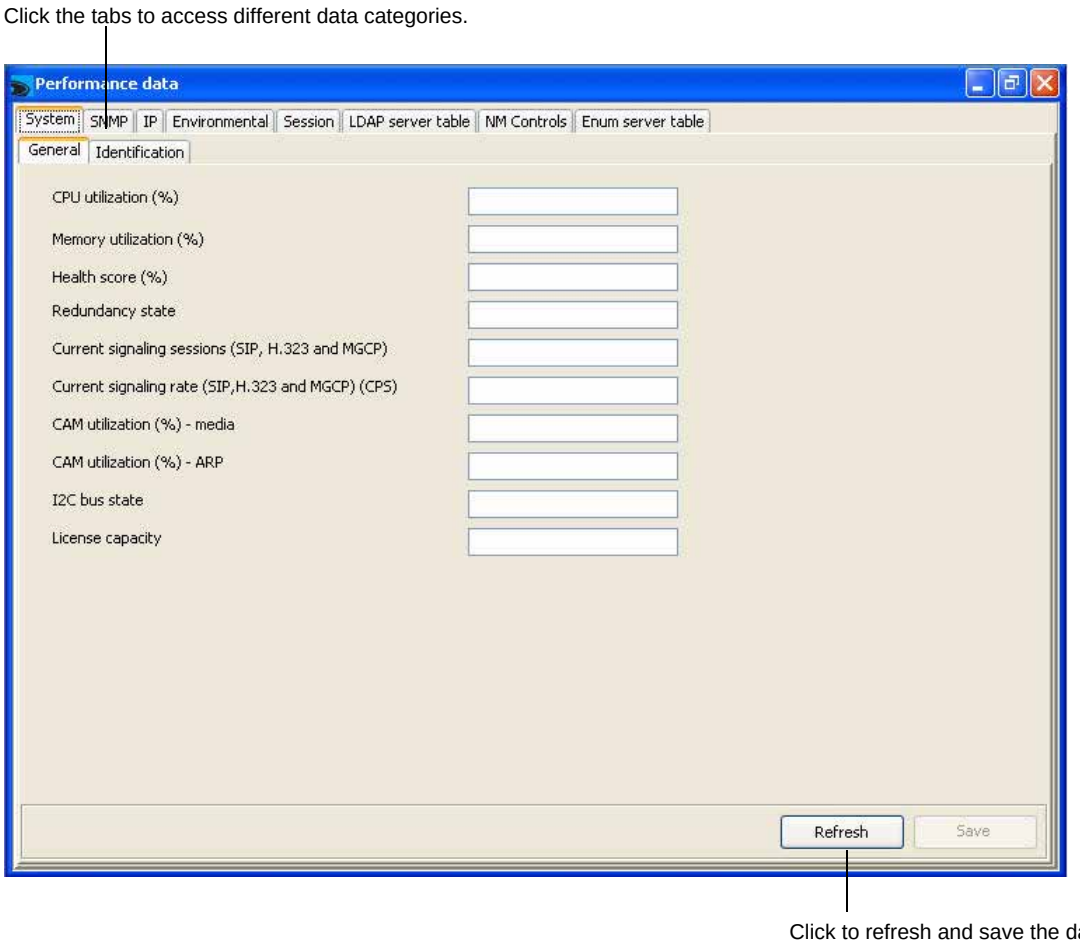
   A list of domain names appears. These are the same domain names that appear under the Configuration category.



2. Click the plus (+) sign next to a domain name to expand it.
3. If accessing Net-Net SBCs that belong to an HA pair, click the + sign next to the name of the HA pair. For example:



4. Click the name of the Net-Net SBC for which you want to view performance data. The performance data for the Net-Net SBC appears in the right pane. For example



5. Access data by clicking the tabs across the top of the performance data window.

Refreshing Data

You can refresh the statistics displayed on each screen by clicking **Refresh**.

Saving Data

You can save the data displayed on each screen to a text file in comma separated format.

To save data to a file:

1. With the data displayed, click **Save**.

   A Save window opens with a file name in the following format:

   <stats screen name>-<tab name>-<date> <hh-mm-ss>.txt

   For example:

   System-General-2007-06-10 13-53-21.txt

2. Click **Save** to save the file and close the window.

Viewing System Information

This section explains the system performance information displayed by the Net-Net EMS.

Accessing System Data

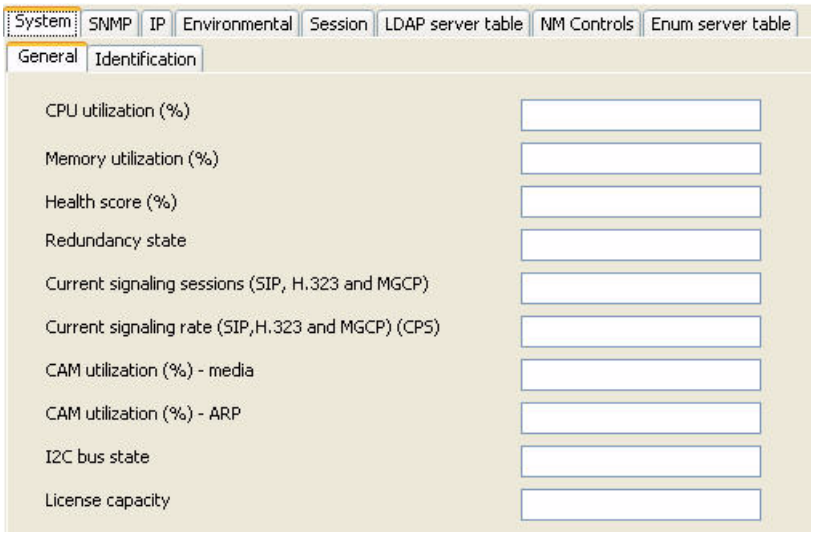
To access System data:

1. Click the System tab in the Performance data screen. System performance data for the category General appears by default.
2. Click the Identification tab to view data that identifies this Net-Net SBC.

General

To access General data:

1. In the System window, click the General tab. The general system data appear:



The following table defines the data displayed by Net-Net EMS:

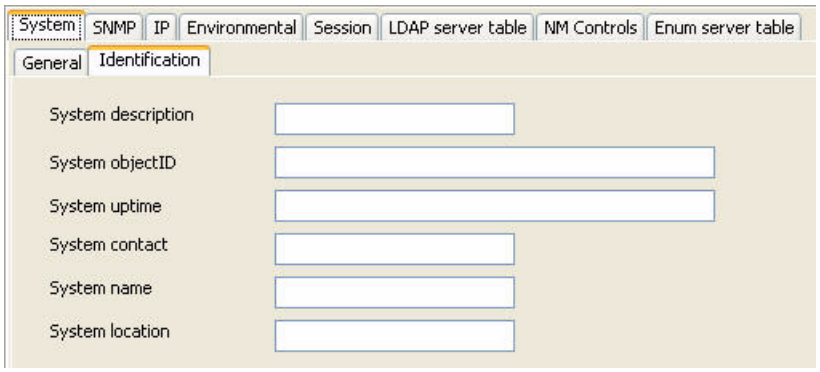
Data	Description
CPU utilization (%)	Percentage of CPU utilization
Memory utilization (%)	Percentage of memory utilization
Health score (%)	System health percentage, with a system health percentage value of 100 (100%) being the healthiest
Redundancy state	For Net-Net HA pairs, information about this Net-Net SBC's state. Values are: • active • standby
Current signaling sessions (SIP, H.323, and MGCP)	Total number of global concurrent sessions at the moment
Current signaling rate (SIP, H.323, and MGCP) (CPS)	Number of global calls per second

Data	Description
CAM utilization (%) - media	Percentage of NAT table in Content Addressable Memory (CAM) utilization
CAM utilization (%) - ARP	Percentage of ARP table (in CAM) utilization
I2C bus state	State of the environmental monitor located in the chassis. Values are: • normal • not functioning
License capacity	Remaining license capacity

Identification

To access Identification data:

1. In the System window, click the Identification tab. The system identification data appears:



The following table defines the data:

Data	Description
System description	Textual description of the entity. This value includes the full name and version identification of the system's hardware type, software operating-system, and networking software.
System objectID	Vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining what kind of box is being managed.
System uptime	Time (in hundredths of a second) since the network management portion of the system was last re-initialized.
System contact	Textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.
System name	Administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.
System location	Physical location of this node. If the location is unknown, the value is the zero-length string.

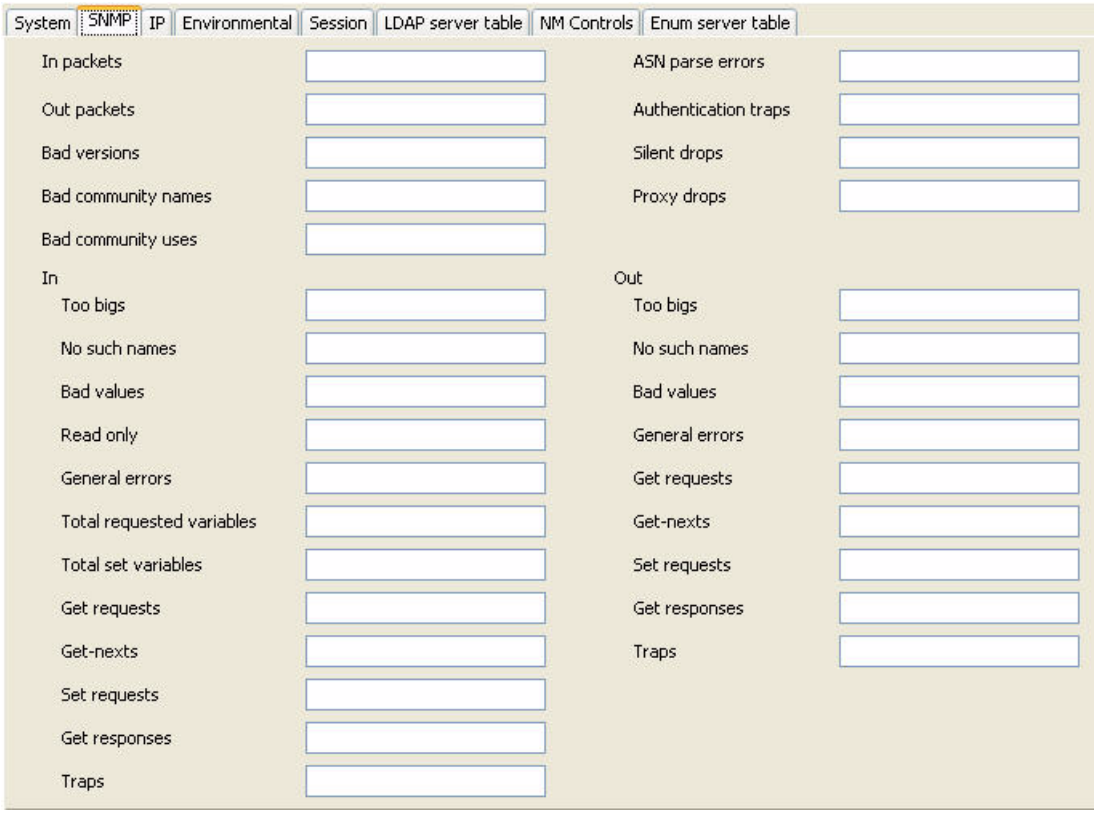
Viewing SNMP Information

This section describes the SNMP performance data displayed by the Net-Net EMS.

Accessing SNMP Data

To access SNMP data:

1. In the Performance data window, click the SNMP tab. The following data appear:



The following table defines the information displayed:

Data	Description
In Packets	Total number of messages delivered to the SNMP entity from the transport service
Out packets	Total number of SNMP messages passed from the SNMP protocol entity to the transport service
Bad versions	Total number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version
Bad community names	Total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity

Data	Description
Bad community uses	Total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message
ASN parse errors	Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages
Authentication traps	Indicates whether the SNMP entity is permitted to generate `authenticationFailure` traps
Silent drops	Total number of `GetRequest-PDUs`, `GetNextRequest-PDUs`, `GetBulkRequest-PDUs`, `SetRequest-PDUs`, and `InformRequest-PDUs` delivered to the SNMP entity that were silently dropped. They were dropped because the size of a reply containing an alternate `Response-PDU` with an empty `variable-bindings` field was greater than either a local constraint or the maximum message size associated with the originator of the request.
Proxy drops	Total number of `GetRequest-PDUs`, `GetNextRequest-PDUs`, `GetBulkRequest-PDUs`, `SetRequest-PDUs`, and `InformRequest-PDUs` delivered to the SNMP entity which were silently dropped. They were dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a timeout) such that no `Response-PDU` could be returned.
In	
Too bigs	Total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is *tooBig*.
No such names	Total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is *noSuchName*.
Bad values	Total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is *badValue*.
Read only	Total number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is *readOnly*. Note: Generating an SNMP PDU that contains the value readOnly in the error-status field is a protocol error. This value is provided to detect incorrect implementations of SNMP.

Data	Description
General errors	Total number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is *genErr*
Total requested variables	Total number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs
Total set variables	Total number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP set-Request PDUs
Get requests	Total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol entity
Get-nexts	Total number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP protocol entity
Set requests	Total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP protocol entity
Get responses	Total number of SNMP Get-Responses that have been accepted and processed by the SNMP protocol entity
Traps	Total number of SNMP Trap PDUs that have been accepted and processed by the SNMP protocol entity
Out	
Too bigs	Total number of SNMP PDUs generated by the SNMP protocol entity and for which the value of the error-status field is *tooBig*
No such names	Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is *noSuchName*
Bad values	Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is *badValue*
General errors	Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is *genErr*
Get requests	Total number of SNMP Get-Request PDUs generated by the SNMP protocol entity
Get-nexts	Total number of SNMP Get-Next PDUs generated by the SNMP protocol entity
Set requests	Total number of SNMP Set-Request PDUs generated by the SNMP protocol entity

Data	Description
Get responses	Total number of SNMP Get-Responses generated by the SNMP protocol entity
Traps	Total number of SNMP Trap PDUs generated by the SNMP protocol entity

Viewing IP Information

This section describes the IP data displayed by Net-Net EMS.

Accessing IP Data

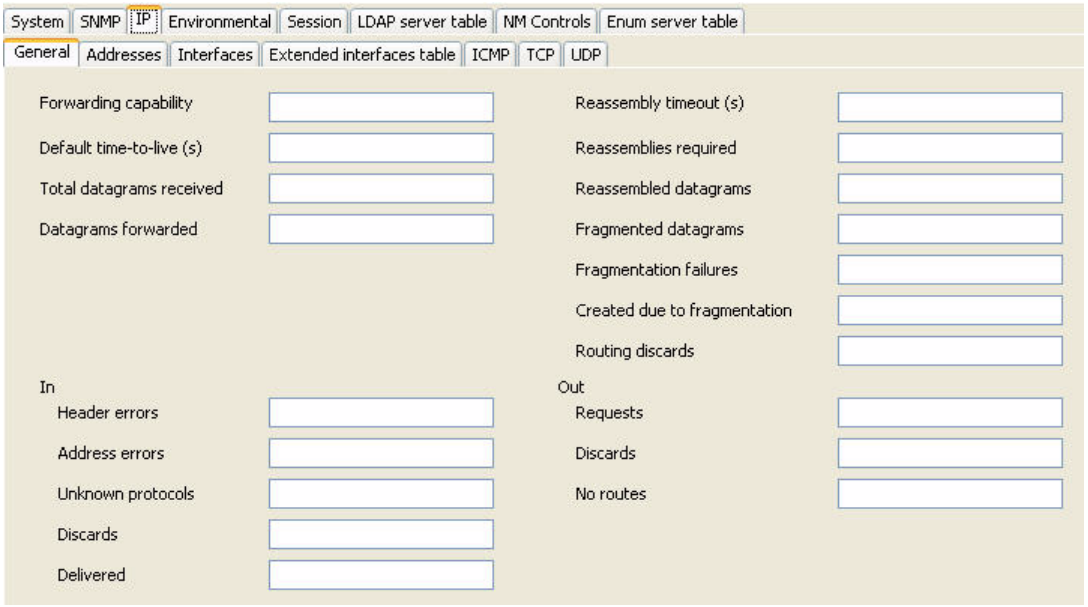
To access IP data:

1. In the Performance data window, click the IP tab. The IP performance data appears for the following categories:
   - General: general performance data
   - Addresses: information about this Net-Net SBC's IP addressing
   - Interfaces: information about the Net-Net SBC's interfaces. Each interface is thought of as being attached to a *subnetwork*.
   - ICMP: information about this Net-Net SBC and Internet Control Message Protocol (ICMP)
   - TCP: information about this Net-Net SBC's existing TCP connections
   - UDP: information about this Net-Net SBC's UDP end-points, upon which a local application is currently accepting datagrams

General

To access General data:

1. In the IP window, click the General tab. The following data appears:



The following table defines the data displayed:

Data	Description
Forwarding capability	Indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host). Note that for some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a *badValue* response if a management station attempts to change this object to an inappropriate value.
Default time-to-live(s)	Default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol
Total datagrams received	Total number of input datagrams received from interfaces, including those received in error
Datagrams forwarded	Number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP gateways, this counter includes only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
Reassembly timeout(s)	Maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity
Reassemblies required	Number of IP fragments received which needed to be reassembled at this entity
Reassembled datagrams	Number of IP datagrams successfully re-assembled
Fragmented datagrams	Number of IP datagrams that have been successfully fragmented at this entity
Fragmentation failures	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be (for example, because their Don't Fragment flag was set)
Created due to fragmentation	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity
Routing discards	Number of routing entries that were discarded although they were valid. A reason for discard could be to free up buffer space for other routing entries.
Header errors	Number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on
Address errors	Number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example., 0.0.0.0) and addresses of unsupported Classes (for example., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Unknown protocols	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol

Data	Description
Discards	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). (Note that this counter does not include any datagrams discarded while awaiting re-assembly.)
Delivered	Total number of input datagrams successfully delivered to IP user-protocols including Internet Control Message Protocol (ICMP)
Requests	Total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. (Note that this counter does not include any datagrams counted in `ipForwDatagrams`.)
Discards	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). (Note that this counter would include datagrams counted in `ipForwDatagrams` if any such packets met this (discretionary) discard criterion.)
No routes	Number of IP datagrams discarded because a route could not be found to transmit them to their destination. Note that this counter includes any packets counted in `ipForwDatagrams` which meet this "no-route" criterion. (This includes any datagrams which a host cannot route because all of its default gateways are down.)

Addresses

To access Address data:

1. In the IP window, click the Address tab. The following data appears:

System | SNMP | IP | Environmental | Session | LDAP server table | NM Controls | Enum server table

General | Addresses | Interfaces | Extended interfaces table | ICMP | TCP | UDP

Index	Address	Netmask	Broadcast address	Max reassembly size
3	2.0.0.0	255.0.0.0	1	65535
5	64.215.70.147	255.255.255.248	1	65535
2	127.0.0.1	255.0.0.0	1	65535
1	172.30.80.70	255.255.0.0	1	65535
5	204.245.18.226	255.255.255.240	1	65535
14	204.245.18.228	255.255.255.240	1	65535
14	204.245.18.229	255.255.255.240	1	65535
14	204.245.18.230	255.255.255.240	1	65535
13	208.51.25.6	255.255.255.128	1	65535
13	208.51.25.24	255.255.255.128	1	65535
13	208.51.25.43	255.255.255.128	1	65535
13	208.51.25.113	255.255.255.128	1	65535
13	208.51.25.124	255.255.255.128	1	65535
5	208.51.25.125	255.255.255.128	1	65535

The following table defines the information displayed for the Net-Net system's control and maintenance interfaces (such as wancom and loopback):

Data	Description
Index	Index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of `ifIndex`.
Address	IP address to which this entry's addressing information pertains
Netmask	Subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the host bits set to 0.
Broadcast address	Value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value is 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.
Max reassembly size	Size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface

Interfaces

To access Interfaces data:

1. In the IP window, click the Interfaces tab. The following data appears:

System | SNMP | IP | Environmental | Session | LDAP server table | NM Controls | Enum server table

General | Addresses | Interfaces | Extended interfaces table | ICMP | TCP | UDP

Index	Name	Description	Type	MTU	Speed	Physical address	Admin status	Operatio
1	wancom0	wancom0	ethernetCsmacd	1500	100000000		up	up
2	lo0	lo0	softwareLoopback	32768	100000000		up	up
3	wancom1	wancom1	ethernetCsmacd	1500	100000000		up	down
5	CustomerInt...	CustomerInterface	ethernetCsmacd	1500	100000000		up	down
6			ethernetCsmacd	1500	100000000		down	down
7			ethernetCsmacd	1500	100000000		down	down
8			ethernetCsmacd	1500	100000000		down	down
9			ethernetCsmacd	1500	100000000		down	down
10			ethernetCsmacd	1500	100000000		down	down
11			ethernetCsmacd	1500	100000000		down	down
12			ethernetCsmacd	1500	100000000		down	down
13	sp0	sp0	ethernetCsmacd	1500	100000000		up	up
14	sp1	sp1	ethernetCsmacd	1500	100000000		up	up

The following table defines the information displayed for the Net-Net system's control and maintenance interfaces (such as wancom and loopback):

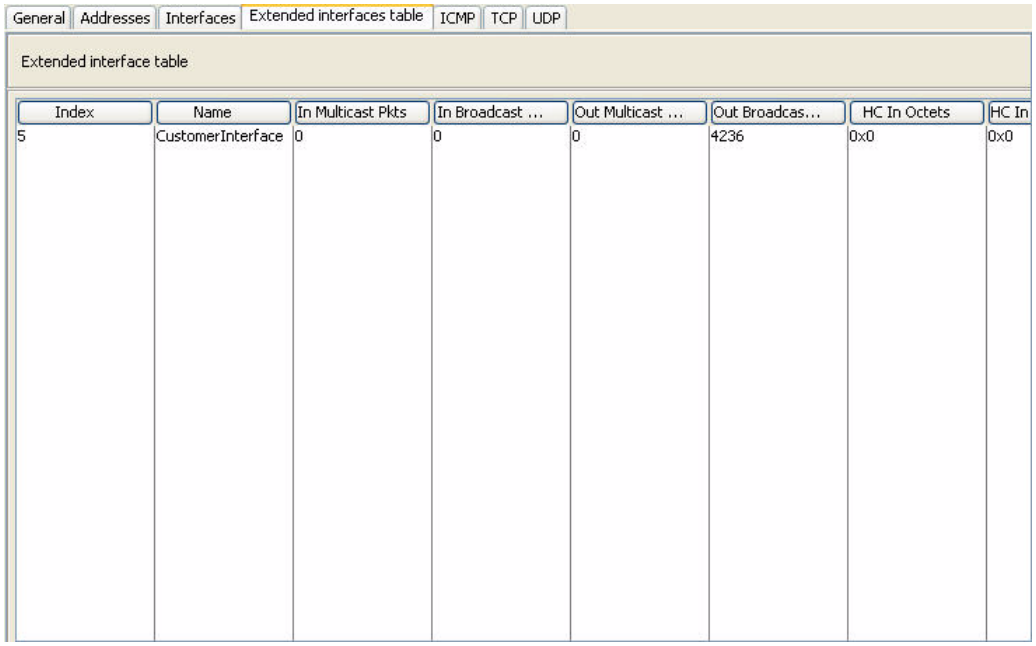
Data	Description
Index	Unique value for each interface. Value has a range between 1 and the value of ifNumber and must remain constant at least from one re-initialization of the entity's NMS to the next re-initialization.
Description	Textual string containing information about the interface. This string includes the name of the manufacturer, the product name, and the version of the hardware interface.
Type	Information about the type of interface, distinguished according to the physical/link protocol(s) immediately *below* the network layer in the protocol stack
MTU	Size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces that transmit network datagrams, this is the size of the largest network datagram that can be sent on the interface.
Speed	Estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where an accurate estimation cannot be made, it contains the nominal bandwidth.
Physical address	Interface's address at the protocol layer immediately *below* the network layer in the protocol stack. For interfaces which do not have such an address (for example, a serial line), it contains an octet string of zero length.
Admin status	Current administrative state of the interface. Values are: • up • down • testing
Operational status	Current operational state of the interface. Values are: • up • down • testing
Last change time	Value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then it contains a zero value.
In	
Octets	Total number of octets received on the interface, including framing characters
Unicast pkts	Number of subnetwork-unicast packets delivered to a higher-layer protocol
Non-Unicast pkts	Number of non-unicast (for example, subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol
Discards	Number of inbound packets which were chosen to be discarded although no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Data	Description
Errors	Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
Out	
Octets	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent
Unicast pkts	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent
Non-Unicast pkts	Total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent
Discards	Number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Errors	Number of outbound packets that could not be transmitted because of errors
Specific media	Returns a reference to MIB definitions specific to the particular media being used to realize the interface. For example, if the interface is realized by an ethernet, then the value of this object refers to a document defining objects specific to Ethernet. If this information is not present, its value should be set to the OBJECT IDENTIFIER {0 0}, which is a syntactically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.

Extended Interfaces

To access extended interfaces data:

1. In the IP window, click the Extended interfaces tab. The following data appears:



The following table defines the information displayed for the Net-Net 9000's media interfaces:

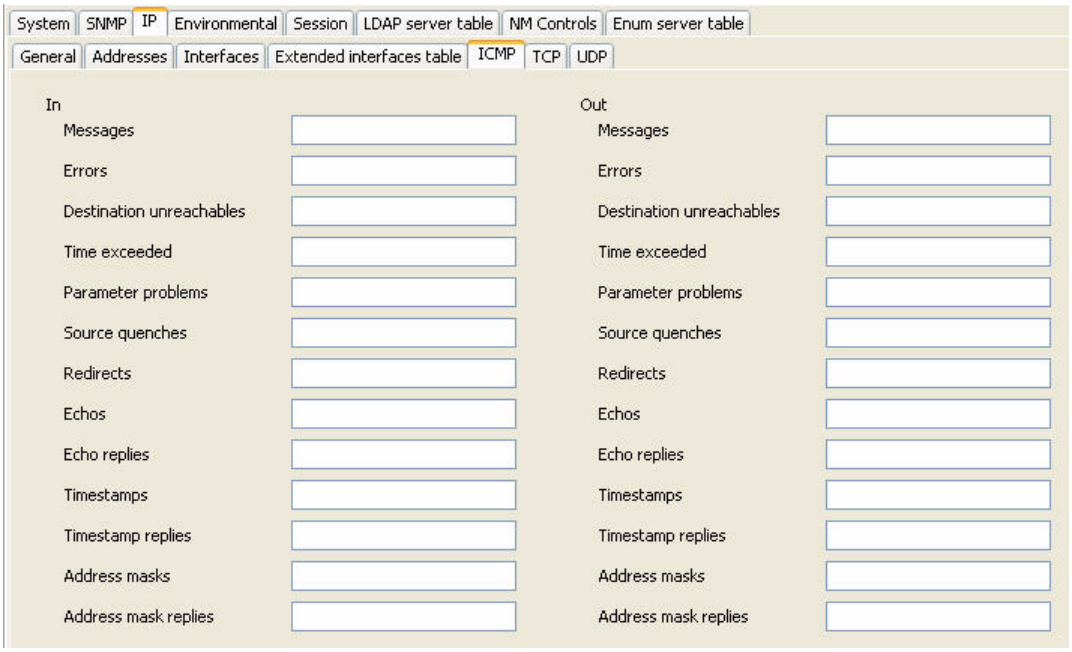
Data	Description
Index	Unique value for each interface. Value has a range between 1 and the value of ifNumber and must remain constant at least from one re-initialization of the entity's NMS to the next re-initialization.
Name	Textual string containing the name of the interface. The name is the one assigned by the local device. It could be a text name or a port number, depending on the interface naming syntax of the device.
In	
Multicast Pkts	Number of packets delivered from this layer to a higher layer that were addressed to a multicast address. For a MAC layer protocol, it includes both group and functional addresses.
Broadcast Pkts	Number of packets delivered by this layer to a higher level that were addressed to a broadcast address
Out	
Multicast Pkts	Number of packets that higher-level protocols requested be transmitted that were addressed to a multicast address at this layer, including those discarded or not sent
Broadcast Pkts	Number of packets higher-level protocols requested to be transmitted that were addressed to a broadcast address at this layer, including those discarded or not sent
HC in	

Data	Description
Octets	Total number of octets received on the interface, including framing characters
Ucast Pkts	Number of packets delivered by this layer to a higher layer that were not addressed to a multicast or broadcast address at this layer
Multicast Pkts	Number of packets delivered by this layer to a higher layer that were addressed to a multicast address at this layer. For a MAC layer protocol, this includes both group and functional addresses.
Broadcast Pkts	Number of packets delivered by this layer to a higher layer that were addressed to a broadcast address at this layer
HC out	
Octets	Total number of octets transmitted out of the interface, including framing characters
Ucast Pkts	Total number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast or broadcast address at this layer; including those discarded or not sent
Multicast Pkts	Total number of packets that higher-level protocols requested be transmitted that were addressed to a multicast address at this layer, including those discarded or not sent. For a MAC layer protocol, this includes both the group and functional addresses.
Broadcast Pkts	Total number of packets that higher-level protocols requested be transmitted that were addressed to a broadcast address at this layer; including those discarded or not sent
LinkUpDownTrap Enable	Indicates whether linkUp/linkDown traps should be generated for this interface. The value should be enabled(1) for interfaces that do no operate on top of any other interface and disabled(2) otherwise.
High Speed	Estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If a value of n is reported, the speed of the interface is in the range of n-500,00 to n+499,999. For interfaces that do no vary in bandwidth or for those where no accurate estimation can be made, a nominal bandwidth is given.
Promiscuous Mode	If the interface only accepts packets/frames addressed to this station, the value is false(2). If the interface accepts all packets/frames transmitted on the media, the value is true(1). This object has a true(1) value only on certain types of media. This values does not affect the reception of broadcast and multicast packets/frames by the interface.
Connector Present	If the interface layer has a physical connector, the value is true(1). Otherwise it is false(2)
Alias	Provides a location in which a non-volatile interface-naming value can be stored. This lets a network manager give one or more interfaces their own unique names, regardless of any interface-stack relationship.
Counter Discontinuity Time	Value of sysUpTime on the most recent occasion at which one or more of this interface's counters suffered a discontinuity

ICMP

To access ICMP data:

1. In the IP window, click the ICMP tab. The following data appears:



The following table defines the information displayed:

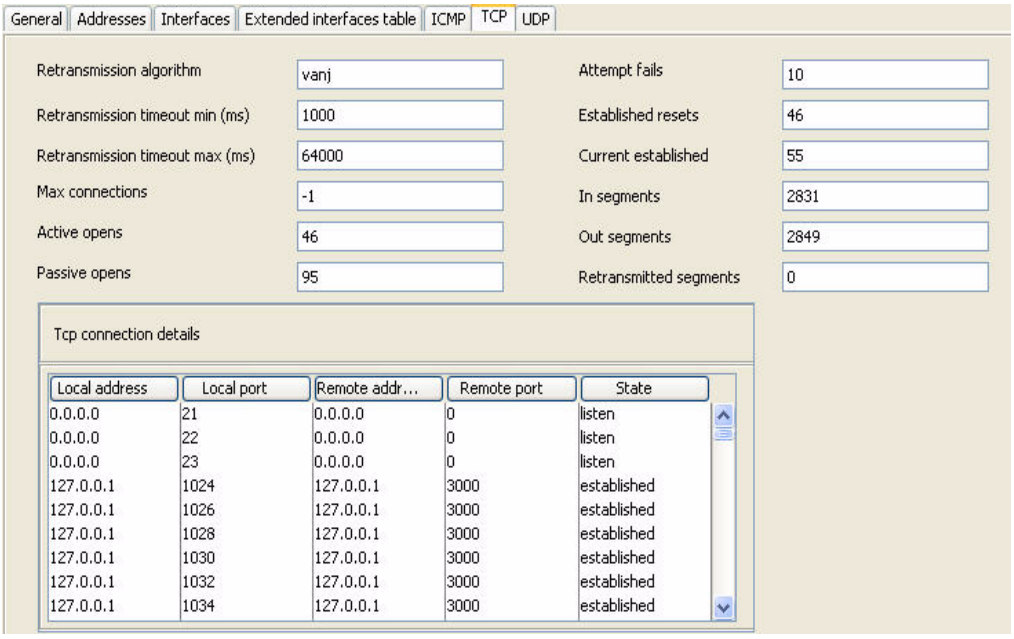
Data	Description
In	
Messages	Total number of ICMP messages which the Net-Net SBC received. (Note that this counter includes all those counted by `icmpInErrors`.)
Errors	Number of ICMP messages which the Net-Net SBC received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on)
Destination unreachables	Number of ICMP Destination Unreachable messages received
Time exceeded	Number of ICMP Time Exceeded messages received
Parameter problems	Number of ICMP Parameter Problem messages received
Source quenches	Number of ICMP Source Quench messages received
Redirects	Number of ICMP Redirect messages received
Echoes	Number of ICMP Echo (request) messages received
Echo replies	Number of ICMP Echo Reply messages received
Timestamps	Number of ICMP Timestamp (request) messages received
Timestamp replies	Number of ICMP Timestamp Reply messages received
Address masks	Number of ICMP Address Mask Request messages received
Address mask replies	Number of ICMP Address Mask Reply messages received
Out	

Data	Description
Messages	Total number of ICMP messages which the Net-Net SBC attempted to send. (This counter includes all those counted by `icmpOutErrors`.)
Errors	Number of ICMP messages which the Net-Net SBC did not send due to problems discovered within ICMP such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
Destination unreachables	Number of ICMP Destination Unreachable messages sent
Time exceeded	Number of ICMP Time Exceeded messages sent
Parameter problems	Number of ICMP Parameter Problem messages sent
Source quenches	Number of ICMP Source Quench messages sent
Redirects	Number of ICMP Redirect messages sent
Echoes	Number of ICMP Echo (request) messages sent
Echo replies	Number of ICMP Echo Reply messages sent
Timestamps	Number of ICMP Timestamp (request) messages sent
Timestamp replies	Number of ICMP Timestamp Reply messages sent
Address masks	Number of ICMP Address Mask Request messages sent
Address mask replies	Number of ICMP Address Mask Reply messages sent

TCP

To access TCP data:

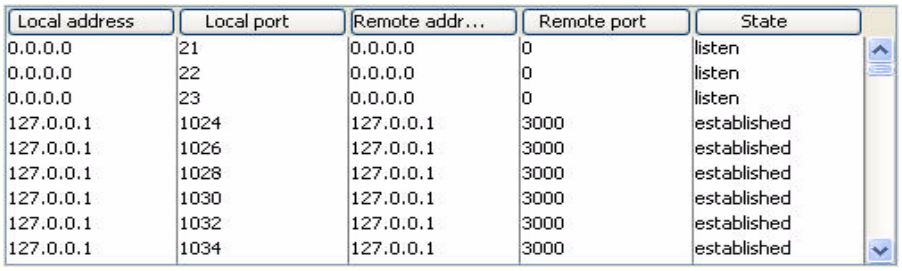
1. In the IP window, click the TCP tab. The following data appears:



The following table defines the information displayed:

Data	Description
Retransmission algorithm	Algorithm used to determine the timeout value used for retransmitting unacknowledged octets
Retransmission timeout min (ms)	Minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is `rsre`, an object of this type has the semantics of the LBOUND quantity described in RFC 793.
Retransmission timeout max (ms)	Maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is `rsre`, an object of this type has the semantics of the UBOUND quantity described in RFC 793.
Max connections	Total number of TCP connections the Net-Net SBC supports. In entities where the maximum number of connections is dynamic, this object contains the value -1.
Active opens	Number of times TCP connections made a direct transition to the SYN-SENT state from the CLOSED state
Passive opens	Number of times TCP connections made a direct transition to the SYN-RCVD state from the LISTEN state
Attempt fails	Number of times TCP connections made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections made a direct transition to the LISTEN state from the SYN-RCVD state
Established resets	Number of times TCP connections made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state
Current established	Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT
In segments	Total number of segments received, including those received in error. This count includes segments received on currently established connections
Out segments	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets
Retransmitted segments	Total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets

You can scroll through a list of connections displayed in the bottom section of the screen.



Local address	Local port	Remote addr...	Remote port	State
0.0.0.0	21	0.0.0.0	0	listen
0.0.0.0	22	0.0.0.0	0	listen
0.0.0.0	23	0.0.0.0	0	listen
127.0.0.1	1024	127.0.0.1	3000	established
127.0.0.1	1026	127.0.0.1	3000	established
127.0.0.1	1028	127.0.0.1	3000	established
127.0.0.1	1030	127.0.0.1	3000	established
127.0.0.1	1032	127.0.0.1	3000	established
127.0.0.1	1034	127.0.0.1	3000	established

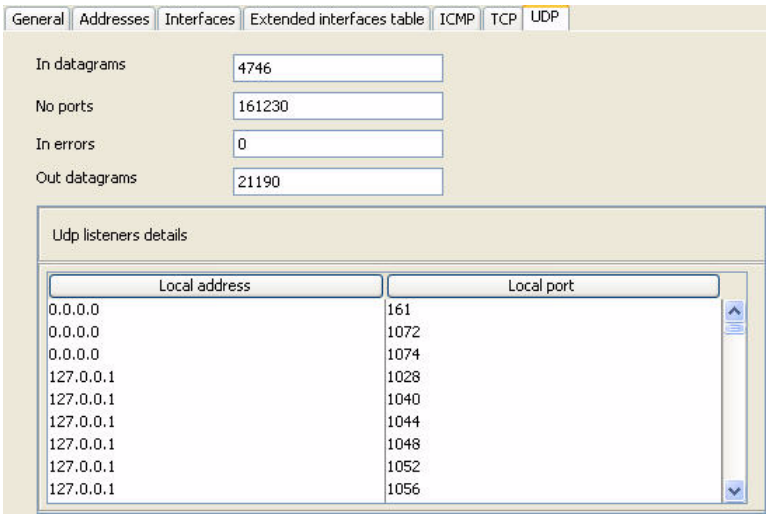
The following table defines the information displayed:

Data	Description
Local address	Local IP address for this TCP connection. In the case of a connection in the listen state, the value is 0.0.0.0.
Local port	Local port number for this TCP connection
Remote address	Remote IP address for this TCP connection
Remote port	Remote port number for this TCP connection
State	State of this TCP connection. Values are: • closed • listen • established

UDP

To access UDP data:

1. In the IP window, click the UDP tab. The following data appears:



The following table defines the information displayed:

Data	Description
In datagrams	Total number of UDP datagrams delivered to UDP users
No ports	Total number of received UDP datagrams for which there was no application at the destination port
In errors	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port
Out datagrams	Total number of UDP datagrams sent from this Net-Net SBC
Listeners	
Local address	Local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value is 0.0.0.0.
Local port	Local port number for this UDP listener

Viewing Environmental Information

This section describes the environmental information displayed by Net-Net EMS.

Accessing Environmental Data

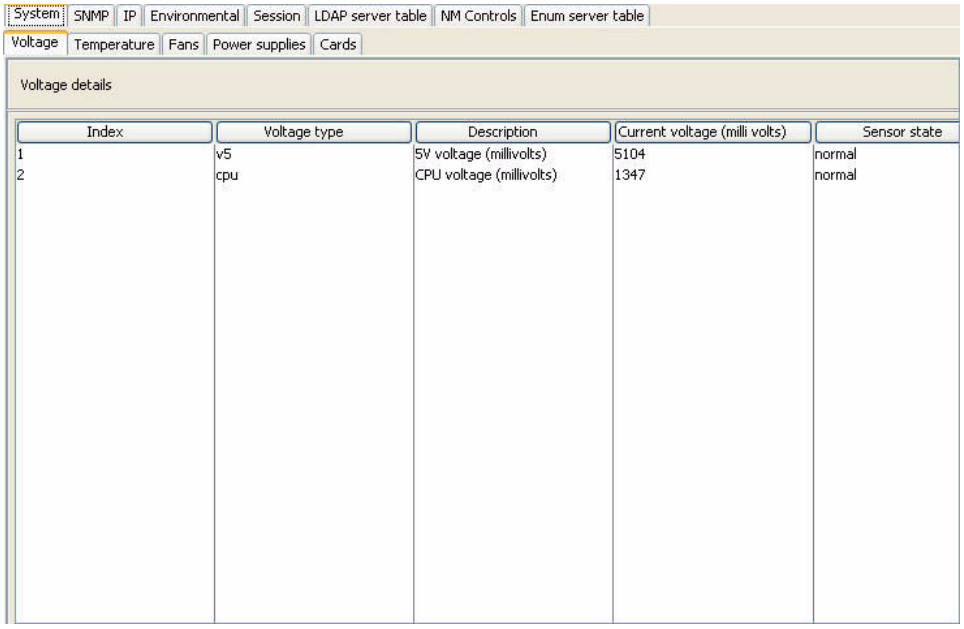
To access environmental data:

1. From the Performance data window, click the Environmental tab. Data for the following categories appears:
   - Voltage
   - Temperature
   - Fans
   - Power supplies
   - Phy cards

Voltage

To access Voltage data:

1. In the Environmental window, click the Voltage tab. The following data appears:



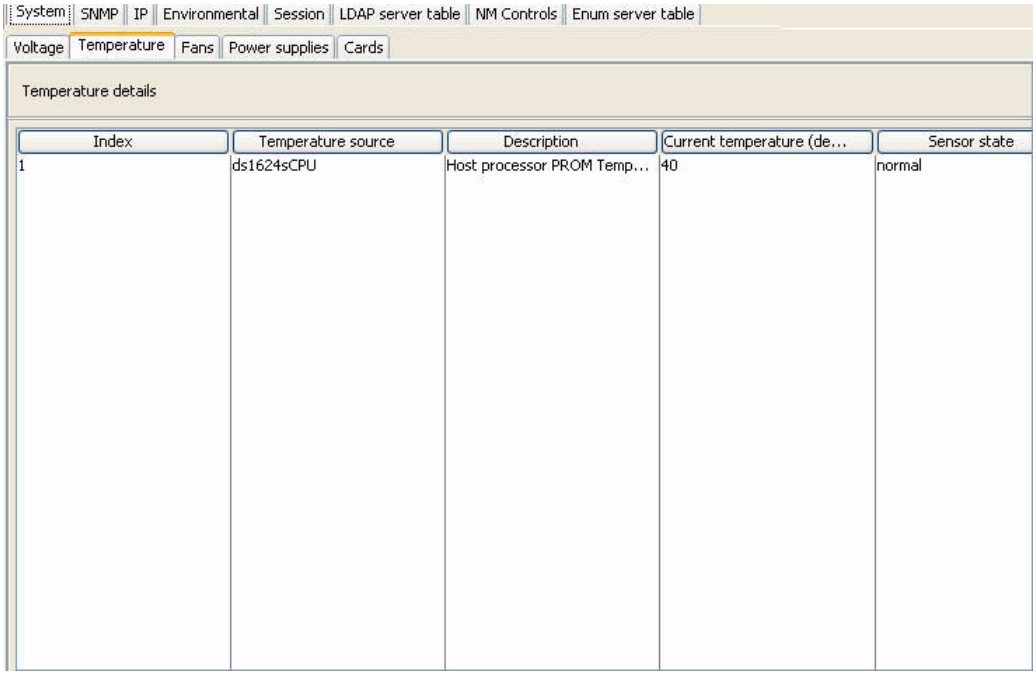
The following table defines the information displayed:

Data	Description
Index	A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Voltage type	Value which indicates the sensor monitoring voltage. Values are: • v2p5- 2.5v sensor. This monitors L3 cache core voltage, micro-processor and co-processor I/O voltage, and Field-Programmable Gate Array (FPGA) memories I/O voltage. • v3p3 - 3.3V sensor. This monitors general TTL supply rail, control logic, micro-processor; micro-processor and co-processor; and SDRAM voltage. • v5 - 5V sensor. This monitors fans and micro-processor core voltage regulator. • CPU sensor. This monitors CPU voltage and micro-processor core voltage.
Description	Description of the entity being monitored for voltage. Values are: • 2.5V voltage (millivolts) • 3.3V voltage (millivolts) • 5V voltage (millivolts) • CPU voltage (millivolts)
Current voltage (millivolts)	Current voltage measurement, in millivolts, if available. A value of -1 indicates that the monitor cannot obtain a value.
Sensor state	Current state of the voltage for the device being monitored. Values are: **Host Processor 7450 and 7455** • normal range: 1.55v to 1.65v • minor range: 1.4v to 1.55v or 1.65v to 1.8v • shutdown range: <1.4v or >1.8v **Host Processor 7457** Version 1.0 • normal range: 1.35v to 1.45v • minor range: 1.00v to 1.35v or 1.45v to 1.6v • shutdown range: <1.0v or >1.6v Version 1.1 and later • normal range: 1.25v to 1.35v • minor range: 1.00v to 1.25v or 1.35v to 1.6v • shutdown range: <1.0v or >1.6v

Temperature

To access Temperature data:

1. In the Environmental window, click the Temperature tab. The following data appears:



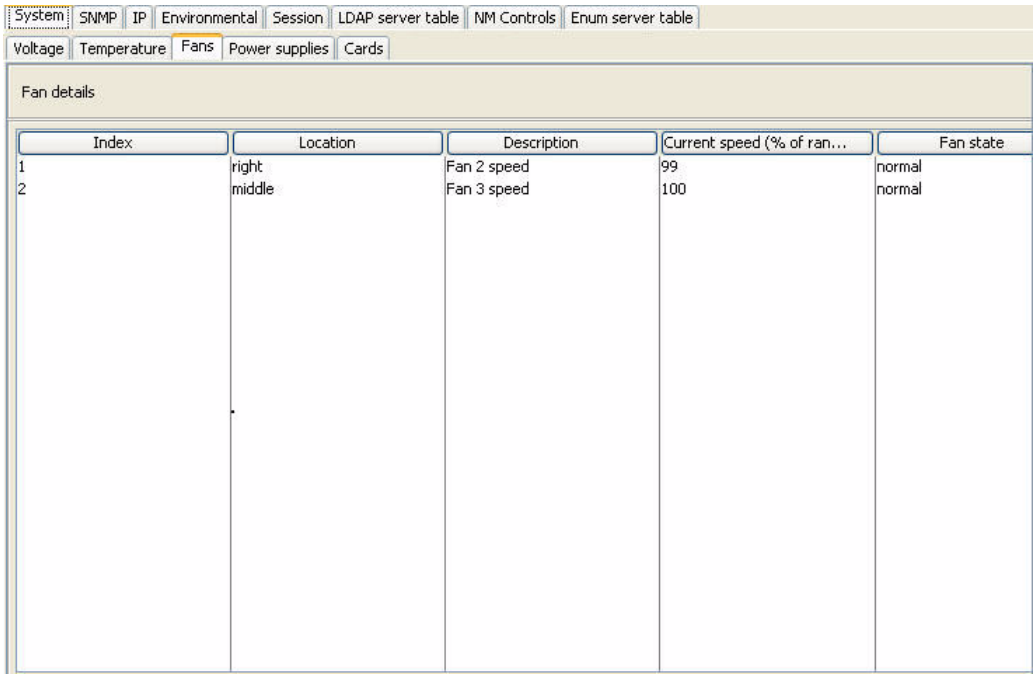
The following table defines the information displayed:

Data	Description
Index	A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Temperature source	Indicates the entity being monitored for temperature.
Description	Description of the temperature being monitored.
Current temperature (degrees Celsius)	The current temperature of the main board PROM in Celsius.
Sensor state	Current state of the temperature which can have one of the following values: • initial: temperature is at its initial state • normal: temperature is normal • minor alarm: temperature is greater than or equal to 53 degrees Celsius and less than 63 degrees Celsius • major alarm: temperature is greater than or equal to 63 degrees Celsius and less than 73 degrees Celsius • critical alarm: temperature is greater than 73 degrees Celsius • shutdown: system should be shutdown immediately • not present: temperature sensor does not exist • not functioning: temperature sensor is not functioning properly • unknown: cannot obtain information due to an internal error

Fans

To access fan data:

1. In the Environmental window, click the Fans tab. The following data appears:



The following table defines the information displayed:

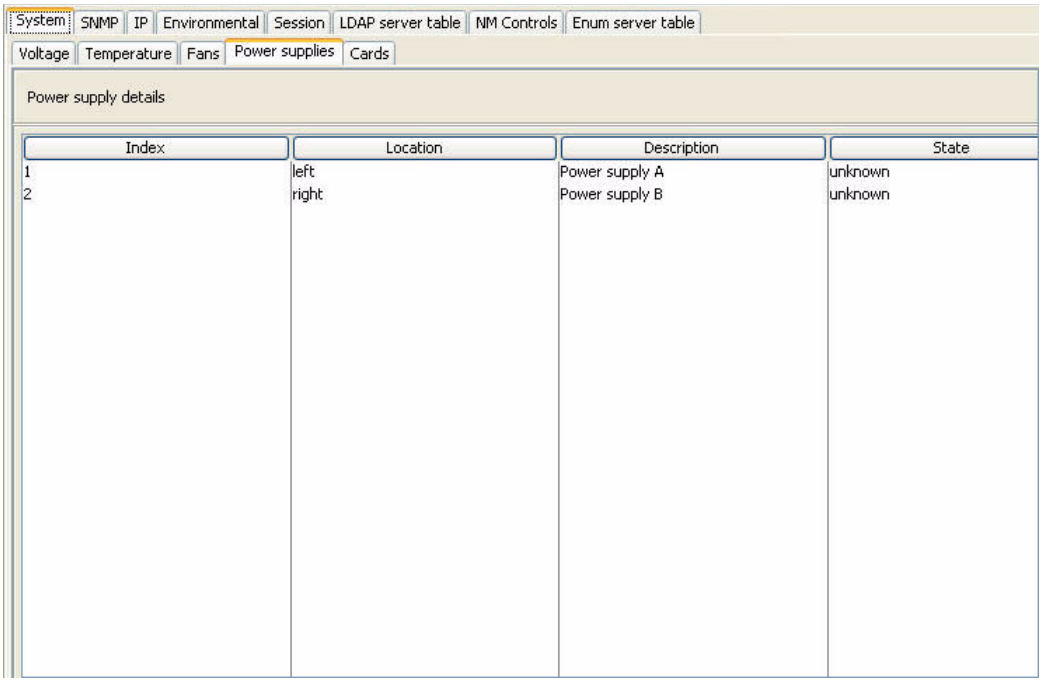
Data	Description
Index	A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Location	Location of the fan. Values are: • left fan • middle fan • right fan
Description	Description of the fan. Values are: • fan 1 • fan 2 • fan 3

Data	Description
Current speed (% or range)	Current measurement of fan speed in percentage
Fan state	Current state of the fan speed. Values are: • initial: fan speed is at its initial state • normal: fan speed is normal • minor: fan speed is between 75% and 90% of the full fan speed • major: fan speed is between 50% and 75% of the full fan speed • critical: fan speed is less than 50% of the full fan speed • shutdown: system should be shutdown immediately • not present: fan sensor does not exist • not functioning: fan sensor is not functioning properly • unknown: cannot obtain information due to an internal error

Power Supplies

To access Power supplies data:

1. In the IP window, click the Power supplies tab. The following data appears:



The following table defines the information displayed:

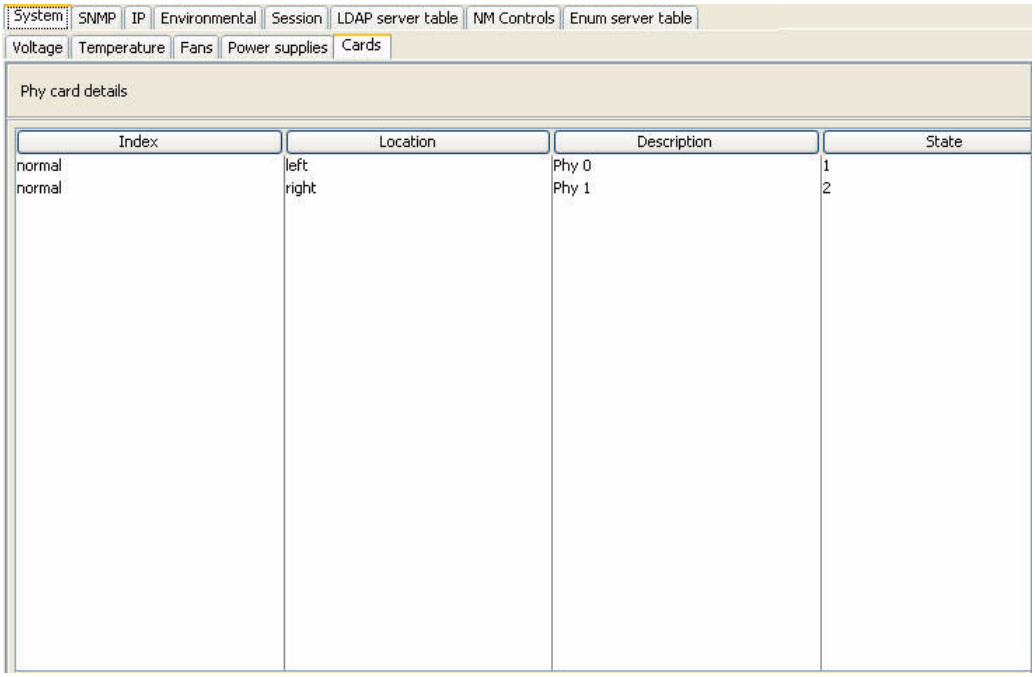
Data	Description
Index	A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Location	Location of the power supply. Values are: • Left power supply (A) • Right power supply (B)

Data	Description
Description	Description of the power supply. Values are: • Power supply A • Power supply B
State	Current state of the power supply. Values are: • normal: the power supply is normal • unknown: the power supply sensor does not exist

Cards

To access card data:

1. In the IP window, click the Cards tab. The following data appears:



The following table defines the information displayed:

Data	Description
Index	A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Location	Location of the phy card. Values are: • left phy card (Phy 0) • right phy card (Phy 1)
Description	Description of the phy card. Values are: • Phy 0 for the left phy card • Phy 1 for the right phy card
State	The current state of the phy card. Values are: • normal: state of the phy card is normal • unknown: phy card is not present

Viewing Session Information

This section describes the session data displayed by the Net-Net EMS.

Accessing Session Data

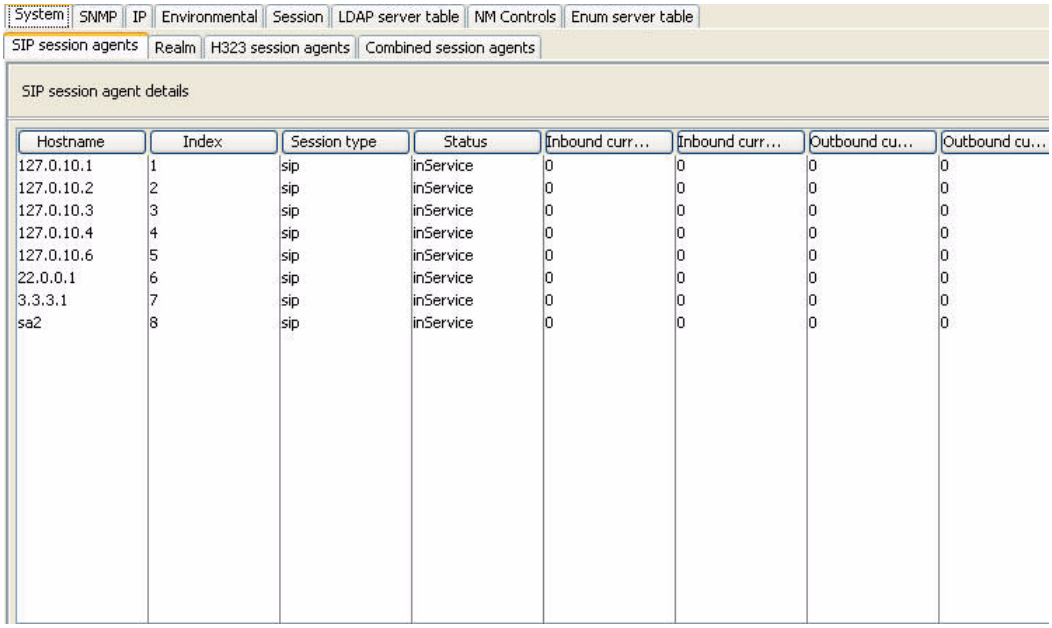
To access Session data:

1. From the Performance data screen, click the Session tab. Session data for the following categories appears:
   - SIP session agents
   - H.323 session agents
   - Combined session agents
   - Realm

SIP Session Agents

To access SIP session agent data:

1. In the Session window, click the SIP session agents tab. The following data appears:



Hostname	Index	Session type	Status	Inbound curr...	Inbound curr...	Outbound cu...	Outbound cu...
127.0.10.1	1	sip	inService	0	0	0	0
127.0.10.2	2	sip	inService	0	0	0	0
127.0.10.3	3	sip	inService	0	0	0	0
127.0.10.4	4	sip	inService	0	0	0	0
127.0.10.6	5	sip	inService	0	0	0	0
22.0.0.1	6	sip	inService	0	0	0	0
3.3.3.1	7	sip	inService	0	0	0	0
sa2	8	sip	inService	0	0	0	0

The following table defines the information displayed:

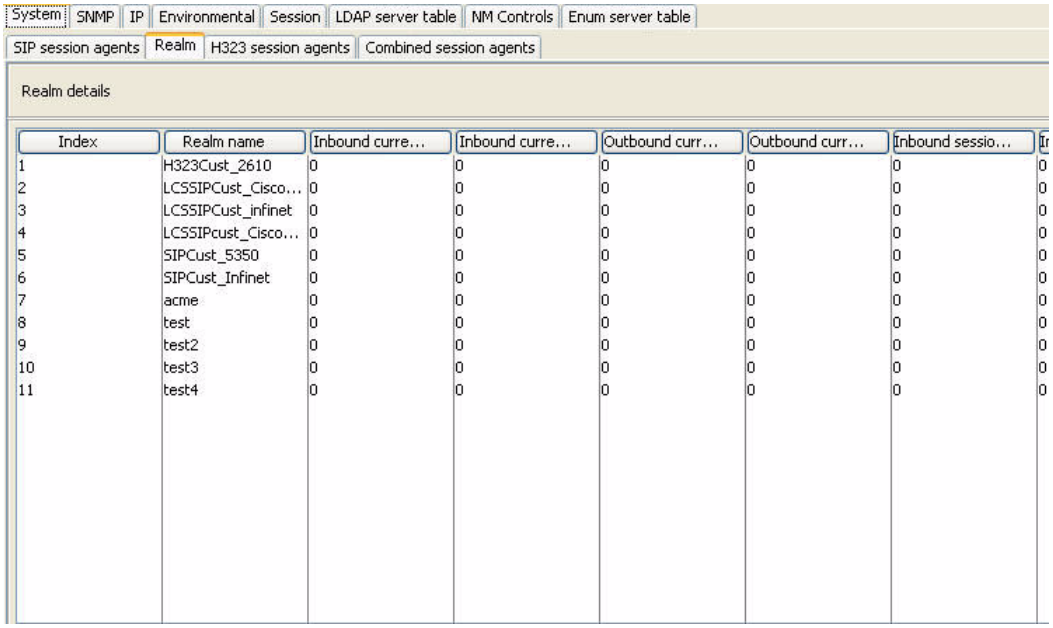
Data	Description
Hostname	The hostname of the session agent for which the following statistics are being calculated
Index	A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1.
Session type	The type of the specified session agent, SIP

Data	Description
Status	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound	
Current active sessions	Number of current active inbound sessions
Current session rate (CPS)	Current inbound session rate in CPS
Outbound	
Current active sessions	Number of current active outbound sessions
Current session rate (CPS)	Current outbound session rate in CPS
Period-based statistics	
Inbound	
Session admitted	Total number of inbound sessions during the period
Session not admitted	Total number of inbound sessions rejected due to insufficient bandwidth
Highest number concurrent sessions	Highest number of concurrent inbound sessions during the period.
Average session rate (CPS)	Average rate of inbound sessions during the period in CPS
Outbound	
Sessions admitted	Total number of outbound sessions during the period
Sessions not admitted	Total number of outbound sessions rejected because of insufficient bandwidth
Highest number concurrent sessions	Highest number of concurrent outbound sessions during the period
Average session rate	Average rate of outbound sessions during the period in CPS
Period-based statistics	
Max burst rate (in+out) (CPS)	Maximum burst rate of traffic measured during the period (combined inbound and outbound)
Total seizures	Total number of seizures during the period
Total answered sessions	Total number of answered sessions during the period
Answer/Seizure ratio (%)	The answer-to-seizure ratio, expressed as a percentage.For example, a value of 90 would represent 90%, or .90.
Average one-way signaling latency (ms)	Average observed one-way signaling latency during the period
Maximum one-way signaling latency (ms)	Maximum observed one-way signaling latency during the period

Realm

To access Realm data:

1. In the Session window, click the Realm tab. The following data appears:



Index	Realm name	Inbound curre...	Inbound curre...	Outbound curr...	Outbound curr...	Inbound sessio...	In
1	H323Cust_2610	0	0	0	0	0	0
2	LCSSIPCust_Cisco...	0	0	0	0	0	0
3	LCSSIPCust_infinet	0	0	0	0	0	0
4	LCSSIPcust_Cisco...	0	0	0	0	0	0
5	SIPCust_5350	0	0	0	0	0	0
6	SIPCust_Infinet	0	0	0	0	0	0
7	acme	0	0	0	0	0	0
8	test	0	0	0	0	0	0
9	test2	0	0	0	0	0	0
10	test3	0	0	0	0	0	0
11	test4	0	0	0	0	0	0

The following table defines the information displayed:

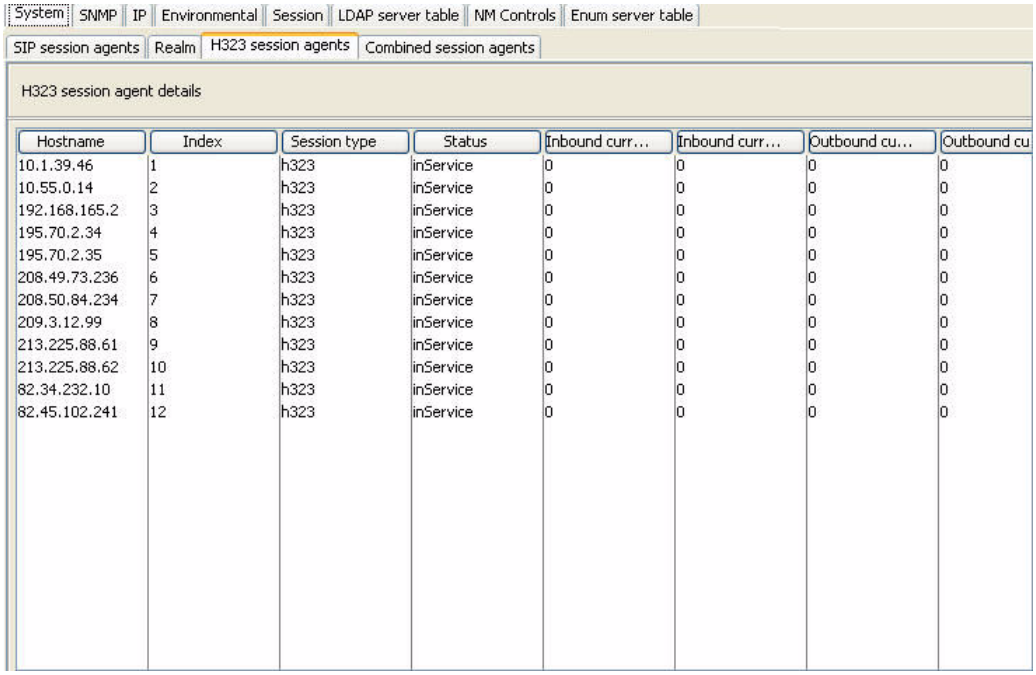
Data	Description
Realm name	The name of the realm for which the following statistics are being calculated
Index	A monotonically increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1.
Inbound	
Current active sessions	Number of current active inbound sessions
Current session rate (CPS)	Current Inbound Session rate in CPS
Outbound	
Current active sessions	Number of current active outbound sessions
Current session rate (CPS)	Current outbound session rate in CPS
Period-based statistics	
Inbound	
Session admitted	Total number of inbound sessions during the period
Session not admitted	Total number of inbound sessions rejected due to insufficient bandwidth
Highest number concurrent sessions	Highest number of concurrent inbound sessions during the period
Average session rate (CPS)	Average rate of inbound sessions during the period in CPS
Outbound	

Data	Description
Sessions admitted	Total number of outbound sessions during the period
Sessions not admitted	Total number of outbound sessions rejected because of insufficient bandwidth
Highest number concurrent sessions	Highest number of concurrent outbound sessions during the period
Average session rate	Average rate of outbound sessions during the period in CPS
Period-based statistics	
Max burst rate (in+out) (CPS)	Maximum burst rate of traffic measured during the period (combined inbound and outbound)
Total seizures	Total number of seizures during the period
Total answered sessions	Total number of answered sessions during the period
Answer/Seizure ratio (%)	The answer-to-seizure ratio, expressed as a percentage
Average one-way signaling latency (ms)	Average observed one-way signaling latency during the period
Maximum one-way signaling latency (ms)	Maximum observed one-way signaling latency during the period

H.323 Session Agents

To access H.323 session agent data:

1. In the Session window, click the H.323 session agents tab. The following data appears:



Hostname	Index	Session type	Status	Inbound curr...	Inbound curr...	Outbound cu...	Outbound cu
10.1.39.46	1	h323	inService	0	0	0	0
10.55.0.14	2	h323	inService	0	0	0	0
192.168.165.2	3	h323	inService	0	0	0	0
195.70.2.34	4	h323	inService	0	0	0	0
195.70.2.35	5	h323	inService	0	0	0	0
208.49.73.236	6	h323	inService	0	0	0	0
208.50.84.234	7	h323	inService	0	0	0	0
209.3.12.99	8	h323	inService	0	0	0	0
213.225.88.61	9	h323	inService	0	0	0	0
213.225.88.62	10	h323	inService	0	0	0	0
82.34.232.10	11	h323	inService	0	0	0	0
82.45.102.241	12	h323	inService	0	0	0	0

The following table defines the information displayed:

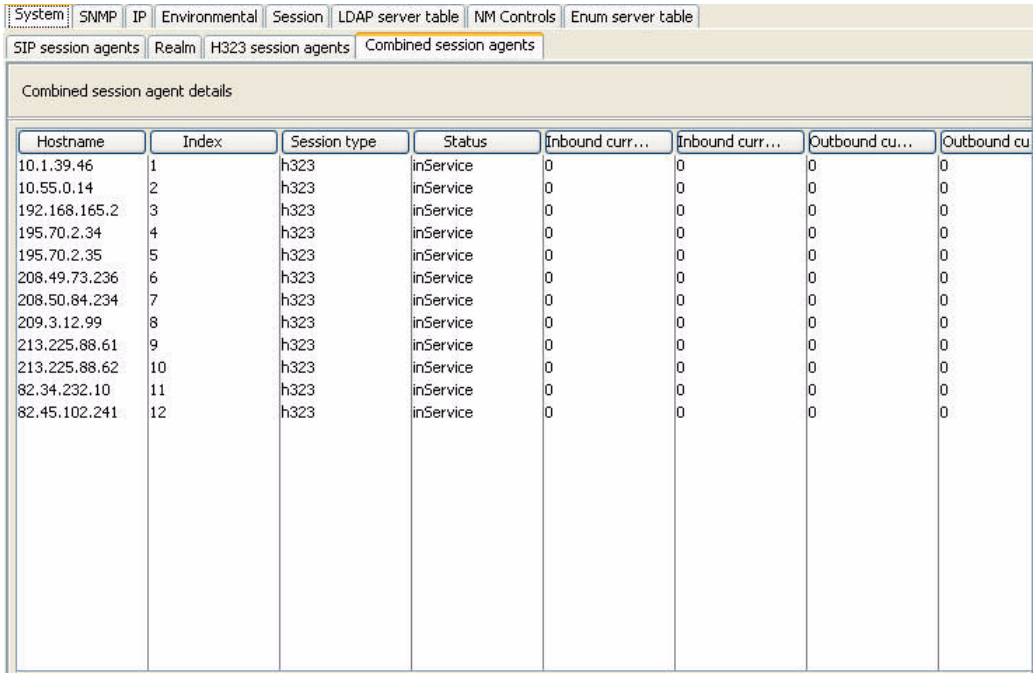
Data	Description
Hostname	The hostname of the session agent for which the statistics are being calculated
Index	A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1.
Session type	The type of the specified session agent, H.323
Status	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound	
Current active sessions	Number of current active inbound sessions
Current session rate (CPS)	Current Inbound Session rate in CPS
Outbound	
Current active sessions	Number of current active outbound sessions
Current session rate (CPS)	Current outbound session rate in CPS
Period-based statistics	
Inbound	
Session admitted	Total number of inbound sessions during the period
Session not admitted	Total number of inbound sessions rejected due to insufficient bandwidth
Highest number concurrent sessions	Highest number of concurrent inbound sessions during the period
Average session rate (CPS)	Average rate of inbound sessions during the period in CPS
Outbound	
Sessions admitted	Total number of outbound sessions during the period
Sessions not admitted	Total number of outbound sessions rejected because of insufficient bandwidth
Highest number concurrent sessions	Highest number of concurrent outbound sessions during the period
Average session rate	Average rate of outbound sessions during the period in CPS
Period-based statistics	
Max burst rate (in+out) (CPS)	Maximum burst rate of traffic measured during the period (combined inbound and outbound)
Total seizures	Total number of seizures during the period
Total answered sessions	Total number of answered sessions during the period

Data	Description
Answer/Seizure ratio (%)	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90.
Average one-way signaling latency (ms)	Average observed one-way signaling latency during the period
Maximum one-way signaling latency (ms)	Maximum observed one-way signaling latency during the period

Combined Session Agents

To access Address data:

1. In the Session window, click the Combined session agents tab. The following data appears:



Hostname	Index	Session type	Status	Inbound curr...	Inbound curr...	Outbound cu...	Outbound cu
10.1.39.46	1	h323	inService	0	0	0	0
10.55.0.14	2	h323	inService	0	0	0	0
192.168.165.2	3	h323	inService	0	0	0	0
195.70.2.34	4	h323	inService	0	0	0	0
195.70.2.35	5	h323	inService	0	0	0	0
208.49.73.236	6	h323	inService	0	0	0	0
208.50.84.234	7	h323	inService	0	0	0	0
209.3.12.99	8	h323	inService	0	0	0	0
213.225.88.61	9	h323	inService	0	0	0	0
213.225.88.62	10	h323	inService	0	0	0	0
82.34.232.10	11	h323	inService	0	0	0	0
82.45.102.241	12	h323	inService	0	0	0	0

The following table defines the information displayed:

Data	Description
Hostname	The hostname of the session agent for which the following statistics are being calculated
Index	A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1.
Session type	The type of the specified session agent, SIP or H.323

Data	Description
Status	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound	
Current active sessions	Number of current active inbound sessions
Current session rate (CPS)	Current Inbound Session rate in CPS
Outbound	
Current active sessions	Number of current active outbound sessions
Current session rate (CPS)	Current outbound session rate in CPS
Period-based statistics	
Inbound	
Session admitted	Total number of inbound sessions during the period
Session not admitted	Total number of inbound sessions rejected due to insufficient bandwidth
Highest number concurrent sessions	Highest number of concurrent inbound sessions during the period
Average session rate (CPS)	Average rate of inbound sessions during the period in CPS
Outbound	
Sessions admitted	Total number of outbound sessions during the period
Sessions not admitted	Total number of outbound sessions rejected because of insufficient bandwidth
Highest number concurrent sessions	Highest number of concurrent outbound sessions during the period
Average session rate	Average rate of outbound sessions during the period in CPS
Period-based statistics	
Max burst rate (in+out) (CPS)	Maximum burst rate of traffic measured during the period (combined inbound and outbound)
Total seizures	Total number of seizures during the period
Total answered sessions	Total number of answered sessions during the period
Answer/Seizure ratio (%)	The answer-to-seizure ratio, expressed as a percentage.For example, a value of 90 would represent 90%, or .90.
Average one-way signaling latency (ms)	Average observed one-way signaling latency during the period
Maximum one-way signaling latency (ms)	Maximum observed one-way signaling latency during the period

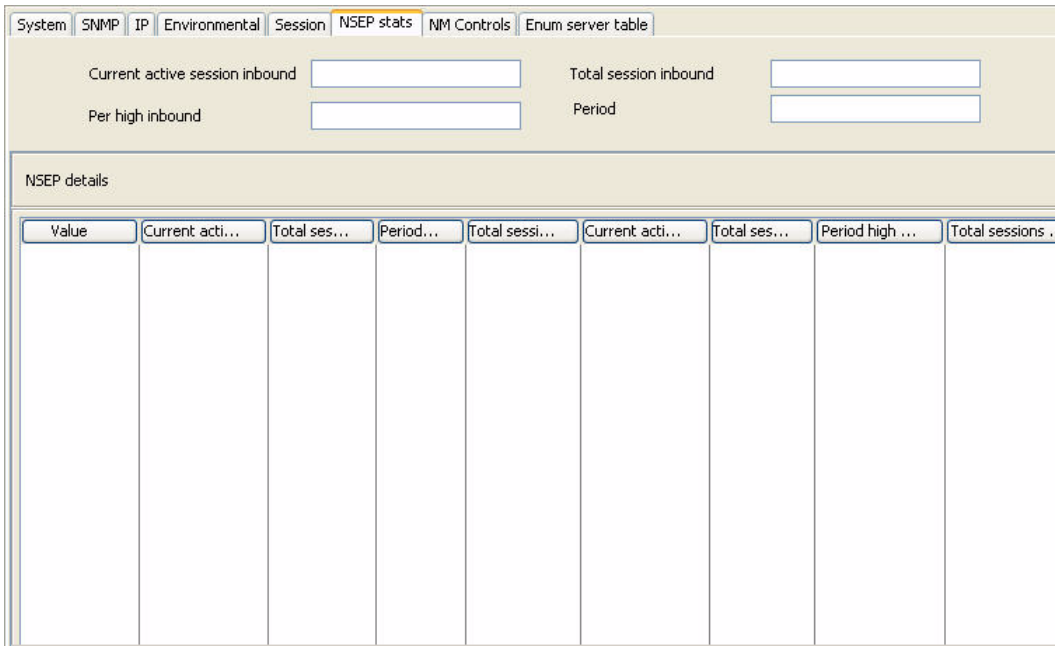
Viewing NSEP Information

This section describes the NSEP data displayed by the Net-Net EMS.

Accessing NSEP Data

To access NSEP data:

1. From the Performance data screen, click the NSEP tab. Data for the following categories appears:



The following table defines the information displayed:

Data	Description
Value	Specific value used for indexing
Current active sessions inbound	Number of current active NSEP sessions
Total sessions inbound	Total number of inbound NSEP sessions during the period
Period high inbound	Highest number of concurrent inbound NSEP sessions during the period
Total sessions not admitted inbound	Total number of inbound NSEP sessions rejected
Current active sessions outbound	Number of current active outbound NSEP sessions
Total sessions outbound	Total number of outbound NSEP sessions during the period
Period high outbound	Highest number of concurrent outbound NSEP sessions during the period
Total sessions not admitted outbound	Total number of outbound NSEP sessions rejected

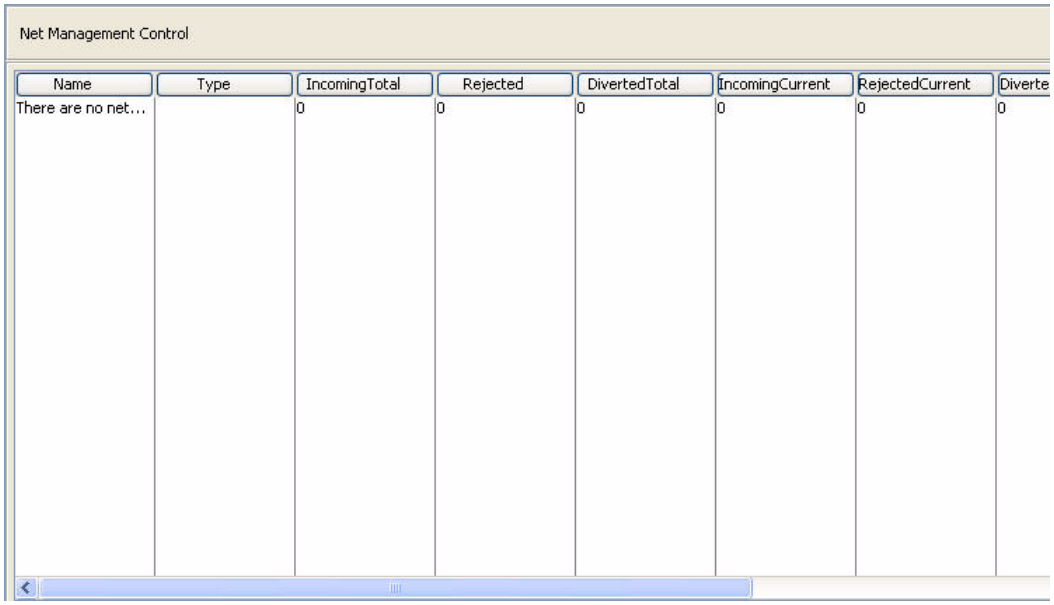
Viewing Network Management Controls Information

This section describes the network management (NM) control data displayed by the Net-Net EMS.

Accessing NM Control Data

To access NM control data:

1. From the Performance data screen, click the NM Controls tab. Session data for the following categories appears:



The following table defines the information displayed:

Data	Description
Name	Name of the network management control
Type	Type of network management control
Incoming Total	Total number of incoming calls that match a destination identifier
Rejected Total	Total number of incoming calls that are rejected
Diverted Total	Total number of incoming calls that are diverted
Incoming Current	Number of incoming calls during the current period that match a destination identifier
Rejected Current	Number of incoming calls that are rejected during the current period
Diverted Current	Number of incoming calls diverted during the current period
Incoming Period Max	Maximum number of incoming calls during a period that match a destination identifier
Rejected Period Max	Number of the maximum incoming calls rejected in a period
Diverted Period Max	Number of the maximum incoming calls diverted in a period

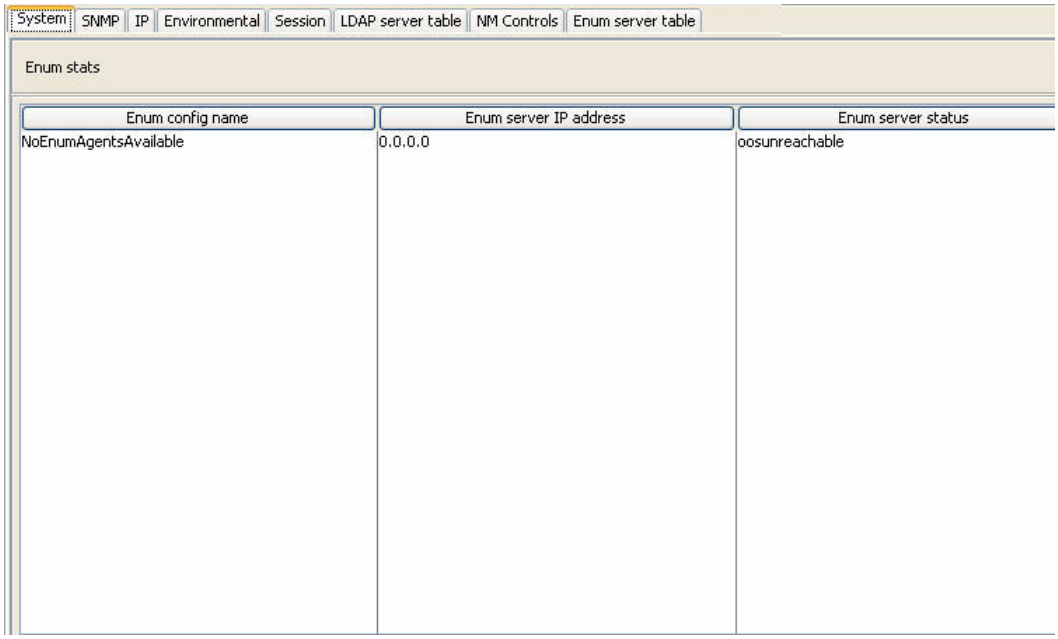
Viewing ENUM Server Table Information

This section describes the ENUM server table data displayed by the Net-Net EMS.

Accessing ENUM Server Table Data

To access ENUM server table data:

1. From the Performance data screen, click the ENUM server table tab. ENUM server table data for the following categories appears:



The following table defines the information displayed:

Data	Description
Enum config name	Name of the ENUM configuration
Enum server IP address	IP address for the ENUM server
Enum server status	Status of the ENUM server